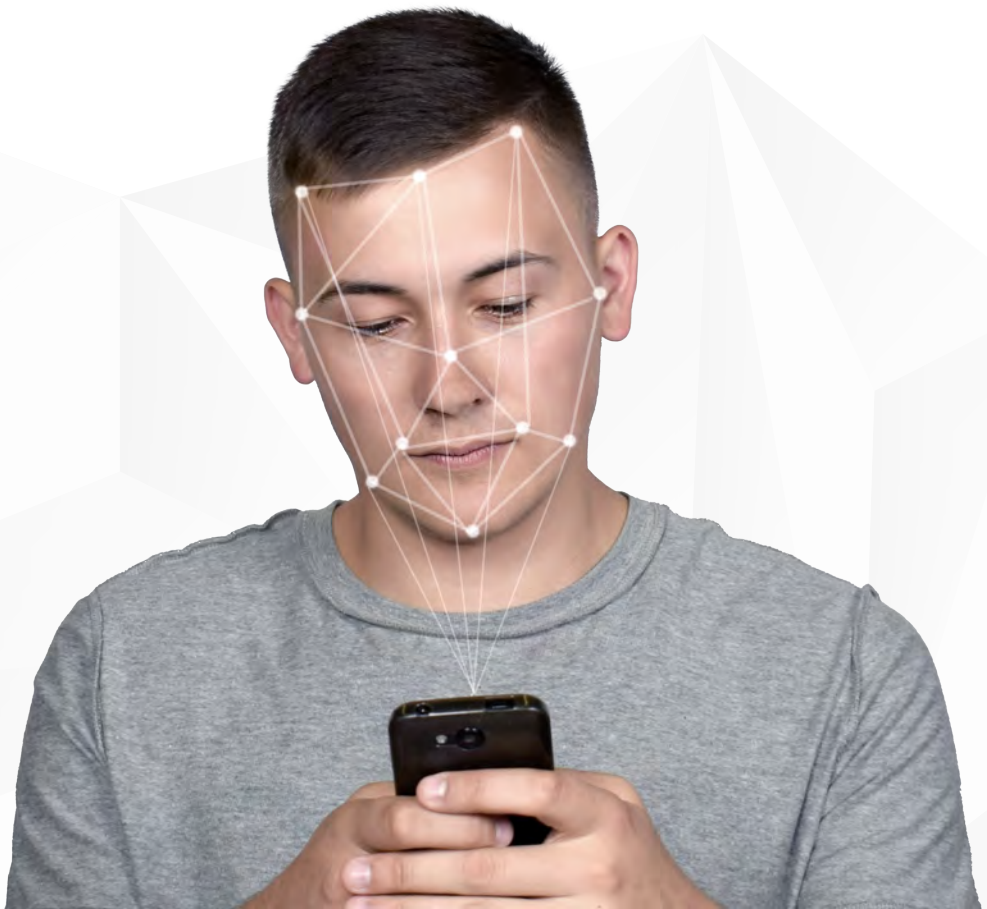
rekonpeople

Control de acceso biométrico:
qué es, ventajas, tipos y cómo implementarlo

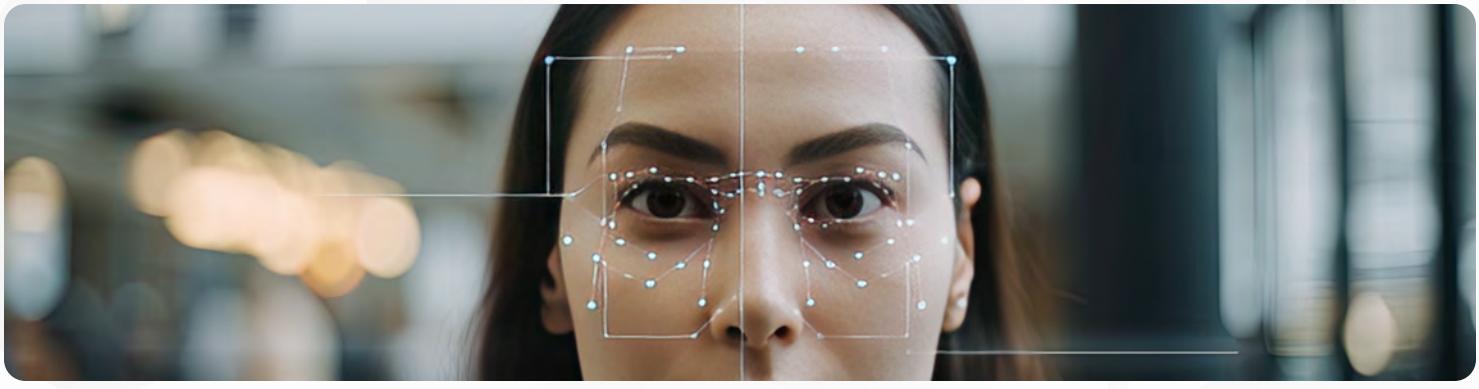
rekonpeople

Con tecnologías avanzadas que ofrecen mayor precisión, conveniencia y protección, los sistemas de **control de acceso biométrico** representan el futuro de la seguridad. Su efectividad se debe a que se basa en el uso de características físicas o conductuales únicas de cada individuo, lo que aumenta la precisión y reduce las posibilidades de fraude.

El **control de acceso biométrico** transformó la forma de gestionar la seguridad en todos los ámbitos, desde hogares y gobiernos a empresas y puestos laborales, sobre todo aquellos que se encuentran en lugares aislados o remotos. A continuación, ofrecemos un guía completa acerca de qué es, sus ventajas, los tipos disponibles, cómo elegir el sistema adecuado, los costos asociados, los retos y el futuro del control biométrico.



Índice



¿Qué es el control de acceso biométrico?

La verificación de acceso mediante biometría es un sistema de seguridad que verifica la identidad de las personas a través de características físicas para permitir o denegar el acceso a un lugar, dispositivo o sistema. A diferencia de los sistemas tradicionales basados en contraseñas o tarjetas, **el control biométrico es más seguro**, ya que las características físicas son difíciles de falsificar o compartir.

Definición y funcionamiento básico

El control de acceso biométrico es un sistema de seguridad que utiliza **las características físicas o comportamentales** únicas de una persona para verificar su identidad con el adjetivo de, por ejemplo, habilitar o rechazar el acceso o corroborar su asistencia.

Para su funcionamiento, el sistema primero registra los datos biométricos de una persona a través de un dispositivo de captura, como un escáner de huellas dactilares o una cámara para reconocimiento facial. **Los datos biométricos capturados se convierten en un patrón digital que se almacena en una base de datos segura.**

Estos datos no se guardan como una imagen, sino como un código cifrado que representa la característica biométrica.

Cuando una persona intenta acceder a una zona o sistema, sus datos biométricos se capturan nuevamente y se comparan con los patrones almacenados. Si hay una coincidencia, se concede el acceso; de lo contrario, se deniega.

Este tipo de control de acceso se utiliza en diferentes entornos, desde edificios corporativos hasta dispositivos electrónicos, ya que **es más seguro que métodos tradicionales como contraseñas o tarjetas de acceso.**

Tipos de biometría utilizados en el control de acceso

En el acceso controlado por biometría, se utilizan diversas tecnologías para identificar a las personas. Los principales tipos de biometría empleados son:

Huella dactilar, el cual utiliza el patrón único de las huellas dactilares para identificar a una persona.

Reconocimiento facial, para lo que se escanea el rostro analizando puntos clave como la distancia entre los ojos, la forma de la nariz y el contorno facial.

Reconocimiento de iris, el cual se considera uno de los métodos más seguros, ya que analiza el patrón único del iris del ojo, que es casi imposible de replicar.

También existen análisis de la geometría de la mano, el reconocimiento de voz, del patrón de las venas de la mano o el dedo, reconocimiento de firma y hasta reconocimiento de la dinámica de tecleo, que analiza la velocidad y el ritmo al presionar las teclas.

Los sistemas biométricos no solo garantizan seguridad, sino que **también pueden medir la productividad de los empleados** al controlar su tiempo de entrada, salida y actividad.

Ventajas de los sistemas biométricos en seguridad

Las ventajas que presenta el control biométrico son variadas. Por un lado, **garantiza la confiabilidad al reducir la posibilidad de fraude** evitando que personas no autorizadas o incluso niños trabajen.

También puede **reducir costos, al automatizar los procesos de registro,** reduciendo los recursos necesarios para el registro y el control de tiempo y asistencia, y aportar una **solución eficiente** en sectores de agroindustria, construcción, minería, y manufactura, **donde la gestión de grandes plantillas de empleados y cumplimiento normativo son críticos.**

Precisión y reducción de errores humanos

Los datos biométricos son únicos para cada persona, lo que **elimina las posibilidades de duplicación o errores de identidad.** Esto asegura una mayor precisión en la autenticación, además de reducir significativamente el margen de error que podría surgir al gestionar manualmente sistemas de contraseñas o tarjetas.

A diferencia de contraseñas o tarjetas de acceso que pueden ser olvidadas o extraviadas, **las características biométricas siempre están "disponibles",** evitando problemas como la pérdida de llaves o el olvido de códigos.

Mayor seguridad frente a sistemas tradicionales

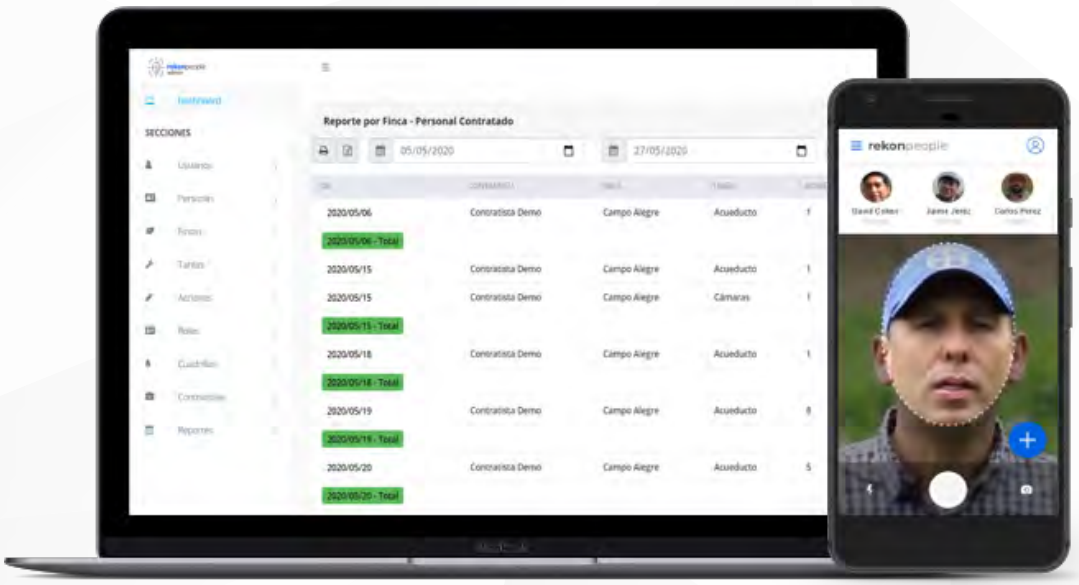
Dado que las características biométricas son únicas y difíciles de falsificar, la gestión de acceso por biometría ofrece un nivel de seguridad superior en comparación con contraseñas o tarjetas. Esto hace que sea mucho más complicado para un intruso acceder a áreas restringidas, y **reduce el riesgo de suplantación de identidad.**

Los sistemas biométricos permiten un monitoreo constante y preciso de quién entra y sale de una instalación. Esto permite a las empresas y organizaciones identificar cualquier actividad inusual o intentos de acceso no autorizados en tiempo real. Además, pueden combinarse con otros métodos de autenticación, como la verificación de dos factores (biometría y PIN, por ejemplo), lo que añade una capa extra de seguridad y minimiza el riesgo de accesos fraudulentos.

La tecnología biométrica de control de acceso también puede emplearse mediante aplicaciones móviles, así, los empleados pueden **registrar su entrada y salida directamente desde su dispositivo móvil.**

Adicionalmente, estos **sistemas de asistencia móvil** pueden utilizar geolocalización para garantizar que el empleado se encuentre en el lugar correcto cuando marque su asistencia -lo que evita posibles fraudes o errores-, o el GPS del teléfono para realizar un seguimiento de la ubicación del empleado cuando marca su entrada o salida.

Esto es útil para empresas que gestionan **equipos de trabajo remoto** o que requieren que sus empleados se desplacen, como personal de ventas o técnicos de servicio en campo.

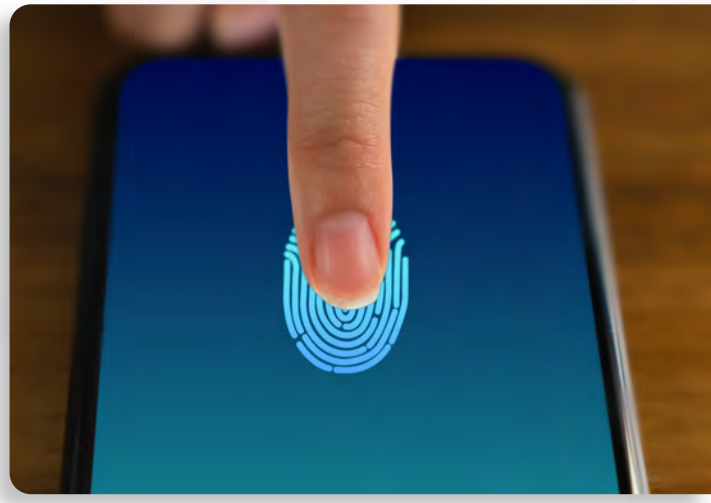


Tipos de tecnología biométrica para control de accesos

Existen varios tipos de tecnologías biométricas utilizadas para el control de acceso, cada una basada en características físicas o conductuales únicas de los usuarios.

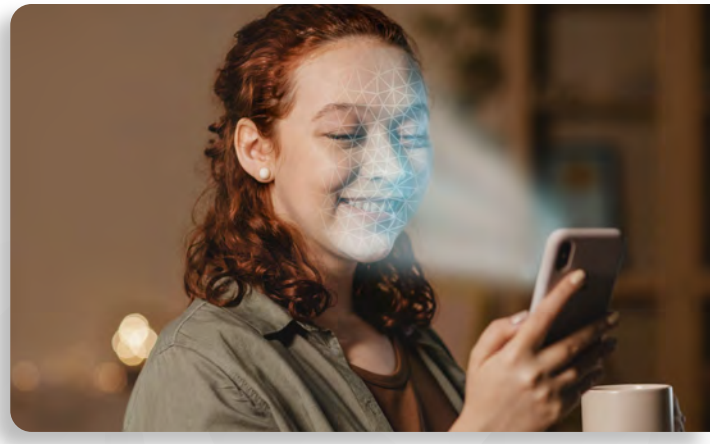
Lectura de huellas digitales

El reconocimiento biométrico por huellas digitales es uno de los sistemas más comunes y utilizados para control de acceso y autenticación. Este método **analiza los patrones únicos de las huellas dactilares de una persona para verificar su identidad,** pero puede presentar algunos **problemas relacionados con la presencia de suciedad en los dedos,** mojados o desgastados debido a que requiere del contacto físico entre la persona y el dispositivo de control.



Reconocimiento facial

Para el reconocimiento facial se utilizan cámaras avanzadas para identificar a una persona mediante la geometría de su rostro, analizando puntos clave como la distancia entre los ojos, la forma de la nariz y el contorno facial. **No es invasivo, es rápido y preciso, y al no requerir contacto físico con el dispositivo la hace más higiénica y cómoda de usar.**



Escaneo de iris

En el reconocimiento de iris se analizan patrones en el iris de una persona que son únicos, lo que **ofrece una gran precisión,** casi imposible de replicar, por lo que se considera uno de los métodos más seguros.

¿Cómo elegir el sistema de control de acceso biométrico adecuado?

Elegir el sistema de control de acceso biométrico adecuado depende de varios factores que deben ser evaluados según las necesidades específicas de seguridad, comodidad y presupuesto de la organización.

Factores clave a considerar

1. Primero es necesario **identificar el nivel de riesgo de los espacios** que se protegerán. Por ejemplo, una oficina con información confidencial requerirá un sistema más seguro (como reconocimiento de iris o venas), mientras que una entrada general puede utilizar un sistema más accesible como reconocimiento facial o huella dactilar.

2. El **tamaño de la base de usuarios** es decisivo a la hora de elegir un sistema de control de acceso biométrico. Si la empresa o instalación tiene muchos empleados, se deberá elegir un sistema que pueda gestionar grandes volúmenes de datos biométricos sin afectar el rendimiento. Por ejemplo, algunos sistemas de reconocimiento facial o de huellas dactilares están diseñados para manejar miles de usuarios.

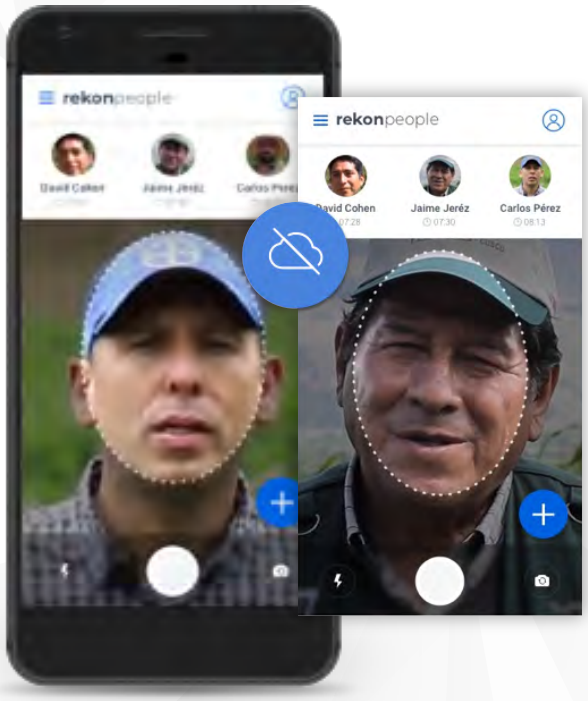
3. Otro factor clave es considerar las condiciones ambientales, si el sistema estará expuesto a condiciones externas (polvo, humedad, luz brillante, etc.) es importante elegir un sistema que sea resistente o que no se vea alterado por estas implicancias.

4. Por último, se deberá tener en cuenta la capacitación de los empleados sobre el sistema de reconocimiento elegido. Es aconsejable optar por una solución con una **interfaz de usuario intuitiva y un diseño sencillo.**

En Rekonpeople Desarrollamos una app que revolucionará el control de asistencia y la gestión empresarial.

Conoce una solución que cuenta con tecnología avanzada de reconocimiento facial, que permitirá identificar a cada empleado de manera precisa, eliminando cualquier posibilidad de fraude. Además, ofrece un control exacto de los horarios de ingreso, en ubicaciones específicas sin margen de error.

Esta aplicación puede funcionar incluso sin conexión a internet y no requiere infraestructura adicional, ya que el único componente necesario para su funcionamiento es un teléfono celular. Esto representará un gran ahorro de presupuesto y optimización de tiempo para las compañías.



Compatibilidad con otros sistemas de seguridad

Los sistemas biométricos se pueden integrar con sistemas tradicionales de control de acceso, como lectores de tarjetas o teclados numéricos. Esta combinación ofrece una doble autenticación, aumentando la seguridad.

Los sistemas biométricos pueden conectarse a sistemas de automatización para controlar puertas, luces y otras funciones dentro de un edificio cuando un usuario autorizado ingresa o sale.

Instalación de sistemas biométricos

La instalación de sistemas biométricos requiere una planificación cuidadosa para garantizar su compatibilidad con otros sistemas de seguridad, su eficacia operativa y su capacidad para escalar y manejar los datos de forma segura.

Aspectos técnicos a tener en cuenta

Los sistemas deben ser capaces de procesar datos biométricos rápidamente para e**vitar demoras o congestión,** especialmente en áreas de alto tráfico.

La precisión es crítica. Los sistemas deben tener un **bajo índice de falsos positivos** y negativos para asegurar que solo las personas autorizadas tengan acceso.

Es esencial **asegurarse de que el sistema pueda escalar** a medida que crece la empresa o aumentan los usuarios. Esto incluye la capacidad de agregar más lectores biométricos o aumentar la cantidad de datos almacenados.

Los datos biométricos deben ser encriptados, tanto en su almacenamiento como durante la transmisión, para evitar que sean interceptados o manipulados. En muchos países, los datos biométricos están sujetos a regulaciones de privacidad, por lo que es importante cumplir con la normativa local para evitar problemas legales.

Los dispositivos deben contar con una interfaz intuitiva, facilitando su uso tanto para los administradores como para los usuarios finales. La capacidad de enrolar rápidamente a los usuarios es importante para que el sistema sea práctico.

Requerimientos de infraestructura

La mayoría de los sistemas biométricos requieren una conexión a la red para sincronizar datos y operar de manera efectiva. Esto implica contar con una infraestructura de red confiable, tanto cableada como inalámbrica, dependiendo del sistema.

Pero **existen sistemas modernos que gestionan datos biométricos desde una plataforma en la nube** que permiten reducir infraestructura y complejidad, y que funcionan en lugares sin internet o energía eléctrica y, aún así, brindan información en tiempo real.

Algunos sistemas de reconocimiento facial o de iris, requieren espacio específico para las cámaras y sensores, al contrario de las aplicaciones móviles que se pueden utilizar desde los propios teléfonos.

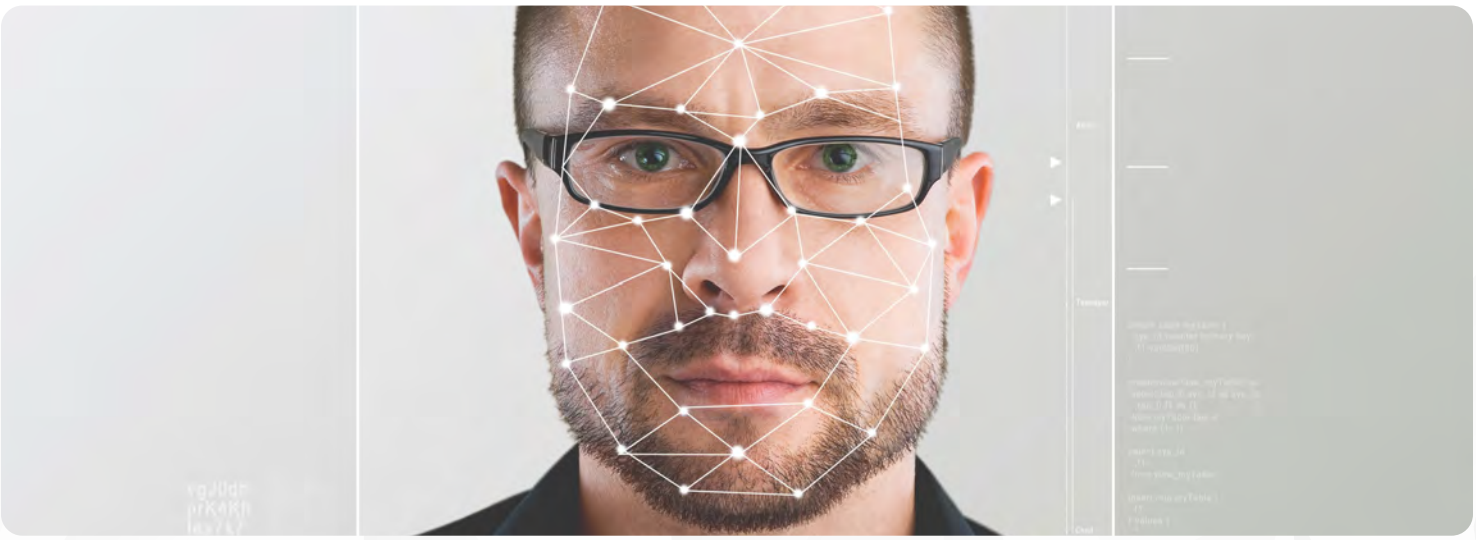
Costos asociados al control de acceso biométrico

El control de acceso biométrico implica una inversión inicial profunda, ya que implica contar con nuevos dispositivos o software según cada tecnología.

Inversión inicial y mantenimiento

La inversión inicial de los sistemas de control de acceso biométricos, implican incorporar dispositivos como escáneres, un software especializado para gestionar y almacenar los datos biométricos y la conexión a red y luego contar con la actualización del software y reemplazo de equipos.

Sin embargo, actualmente existen soluciones que brindan facilidad, seguridad, y eficiencia en la gestión de personal, sin necesidad de infraestructura adicional, lo que reduce los costos de inversión. El reconocimiento facial desde dispositivos móviles, es una opción óptima, **con una implementación rápida y sin necesidad de inversiones** en infraestructura.



Comparativa con sistemas tradicionales

Comúnmente puede pensarse que los sistemas tradicionales son más económicos de implementar, pero a largo plazo, el control biométrico ofrece mayores ahorros gracias a sus **ventajas en seguridad y eficiencia.**

Este tipo de tecnología elimina costos recurrentes, como la reposición de tarjetas de acceso por pérdida o daño, lo que compensa con creces la inversión inicial.

Casos de uso de control de acceso biométrico

La verificación de acceso mediante biometría se utiliza en una amplia gama de escenarios gracias a su capacidad para ofrecer una **seguridad avanzada, precisión en la identificación y una solución eficiente** en sectores donde por la localización y grandes plantillas de empleados son críticos.

Empresas y oficinas

En entornos empresariales, la biometría se utiliza para garantizar que **solo empleados autorizados puedan acceder a áreas sensibles,** y gestionar el control de asistencia.

Además, es una excelente solución para corporaciones multinacionales con operaciones distribuidas en varias sedes, para que los empleados puedan acceder a áreas específicas en cada oficina utilizando reconocimiento facial o huella dactilar, **centralizando la gestión de seguridad** y mejorando la experiencia del personal.

Instalaciones industriales y gubernamentales

En el sector industrial, el control de acceso biométrico no solo garantiza un control estricto sobre quién puede acceder a determinadas áreas por motivos de **seguridad y prevención de riesgos laborales.**

Además, las soluciones basadas en la nube, que no requieren conexión continua, son las únicas capaces de operar en espacios de trabajo amplios en zonas rurales. Estas áreas suelen **carecer de infraestructura adecuada y no tienen acceso a Internet,** computadoras, o incluso suministro eléctrico, lo que hace que dichas soluciones sean fundamentales.

Dependencias gubernamentales, como oficinas de defensa, organismos de seguridad y agencias de inteligencia, utilizan la biometría para permitir solo el acceso de personal autorizado. Esto es especialmente crucial en áreas donde se maneja información clasificada.

Retos y desafíos del control de acceso biométrico

El control de acceso biométrico, a pesar de sus numerosas ventajas, puede enfrentar una serie de retos y desafíos en su implementación y operación. Estos desafíos abarcan aspectos técnicos, legales, éticos y operativos.

Protección de datos personales y privacidad

El uso de datos biométricos, como huellas dactilares, reconocimiento facial o escaneo de iris, implica la captura y almacenamiento de información personal extremadamente sensible. **La violación de estos datos puede tener consecuencias graves,** ya que, a diferencia de una contraseña, los datos biométricos no pueden ser fácilmente cambiados si se ven comprometidos.

Las organizaciones deben **cumplir con leyes de privacidad y protección de datos,** como el GDPR en Europa o la Ley Federal de Protección de Datos Personales en México, para garantizar el almacenamiento seguro de esta información. Es crucial implementar cifrado robusto y soluciones de seguridad avanzadas para evitar filtraciones o hackeos.

Fallos en el reconocimiento biométrico

A diferencia de los sistemas tradicionales que son fácilmente vulnerables con controles débiles como listas en papel, la perdida o el intercambio de tarjetas de entrada entre empleados (lo que permite la entrada de personas no autorizadas), y hasta el trabajo infantil, los sistemas de reconocimiento biométricos son más efectivos.

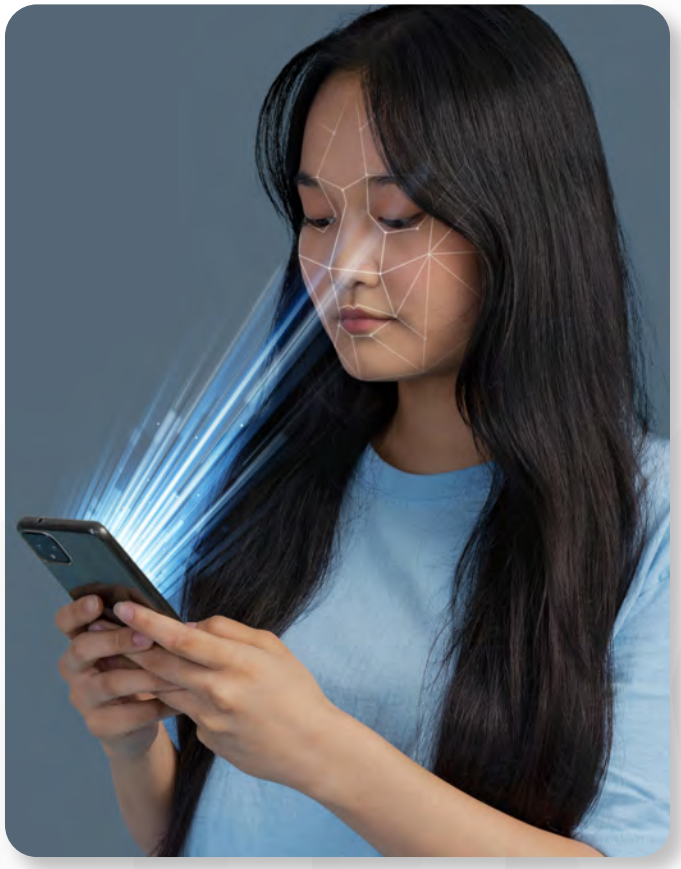
Y si bien puede haber falsos positivos o negativos en la identificación biométrica, especialmente en sistemas con usuarios no cooperativos o condiciones ambientales adversas, siguen siendo una opción óptima, por ejemplo, con una implementación rápida y sin necesidad de inversiones en infraestructura, **el sistema de reconocimiento facial biométrico logra un control correcto con una eficiencia del 99.9%.**

Integración con software de gestión

La **integración de sistemas de acceso biométrico** con software de gestión y administrativo puede llevar la eficiencia y la seguridad en las empresas al ofrecer una solución robusta para mejorar la seguridad, la eficiencia y el monitoreo continuo dentro de las organizaciones.

Conexión con software administrativo

La integración con software de gestión ofrece ventajas como control de acceso centralizado. A través de un ERP o un software de gestión de recursos humanos (HRMS), es posible gestionar quién tiene acceso a diferentes áreas de la empresa o plataformas digitales, basándose en roles y permisos.



El software de gestión puede **actualizar permisos de acceso biométrico de forma automática,** por ejemplo, si un empleado cambia de departamento o rol dentro de la empresa.

El uso de biometría no solo es útil para el control de acceso físico, sino que también se puede integrar con software de **gestión de horarios y soluciones de acceso remoto** que permite que el registro de entradas y salidas mediante biometría se refleje automáticamente en el sistema de control horario.

También, para los empleados que trabajan de forma remota, la biometría puede utilizarse como un **segundo factor de autenticación** en soluciones VPN o software de acceso remoto.

Monitoreo y auditoría en tiempo real

Integrar sistemas biométricos con software de monitoreo y auditoría permite a las empresas **supervisar en tiempo real quién accede a las instalaciones** o a los sistemas internos, lo que fortalece la seguridad y garantiza el cumplimiento normativo.

Toda actividad registrada por los sistemas biométricos puede ser auditada. Por ejemplo, **es posible generar informes de quién accedió a qué áreas y cuándo.** Estos datos pueden ser revisados regularmente o ante incidentes de seguridad.

Futuro del control de acceso biométrico

El futuro de la verificación de acceso mediante biometría está marcado por la evolución tecnológica, la adopción creciente en diversos sectores y el surgimiento de nuevas aplicaciones.

A medida que la biometría continúa integrándose en sistemas de seguridad más complejos, se espera que juegue un papel aún más importante en garantizar la seguridad física y digital de personas y organizaciones.

Tendencias emergentes

El uso de inteligencia artificial y machine learning está transformando el control de acceso biométrico. Estos avances permitirán a los sistemas aprender y mejorar con el tiempo, ajustando los algoritmos para **reducir la tasa de errores, mejorar la precisión** y adaptarse a cambios en las características físicas de las personas (como el envejecimiento o lesiones).

La expansión de redes 5G y la interconexión de dispositivos mediante el Internet de las Cosas (IoT) permitirán la integración de sistemas biométricos en más lugares y con mayor rapidez. Los sistemas de acceso biométrico podrán comunicarse en tiempo real con plataformas de seguridad, gestionando el acceso de manera más eficiente y permitiendo respuestas inmediatas ante situaciones de emergencia.

Perspectivas de crecimiento del control de acceso biométrico

El mercado global de biometría ha crecido exponencialmente en los últimos años.
Impulsados por la pandemia de COVID-19, las **soluciones biométricas sin contacto,** como el reconocimiento facial y de iris, están ganando tracción.

Sin dudas, en América Latina, la **biometría se presenta como una solución cada vez más relevante en el ámbito de la seguridad y la autenticación.** Con un mercado regional valuado en alrededor de USD 5,2 mil millones en 2023 y con proyecciones de crecimiento sostenido a una tasa anual compuesta del 12,30 % hasta 2032, el creciente interés y adopción de esta tecnología es evidente.

En México, por ejemplo, el uso de control biométrico ha sido impulsado por el sector bancario y gubernamental: 78% de usuarios de tecnología digital está dispuesto a compartir datos biométricos.

Mientras tanto, en Colombia, el uso de biometría se está extendiendo en sectores como la salud y la seguridad pública: la Corte Suprema podrá acceder a bases de datos biométricos de la Registraduría para validar identidades en juicios y audiencias. En Argentina, el control biométrico ha ganado popularidad en sectores como la banca, telecomunicaciones, administración pública y aeropuertos.

rekonpeople

rekonpeople.com