BIOMETRÍA PARA LA GESTIÓN DE IDENTIDADES, UNA OPCIÓN EFICIENTE Y ÓPTIMA PARA EL USUARIO

BIOMETRÍA, ¿EL FUTURO DE LA GESTIÓN DE IDENTIDADES?

Si hay un elemento crítico en las operaciones empresariales actuales es la gestión de identidades y acceso de los usuarios, conocido habitualmente por sus siglas en inglés, IAM. Tradicionalmente, esta gestión se ha llevado a cabo con nombres de usuario y contraseñas, pero se ha demostrado que ya no es una forma eficaz por la cada vez más frecuente y efectiva actividad de los hackers. Frente a esta visión tradicional, la seguridad biométrica se consolida como una alternativa efectiva, sencilla de implementar y, sobre todo, con una mejor experiencia de uso.

La tecnología forma parte de todas y cada una de las actividades de los usuarios, tanto a nivel personal como profesional. Esta tecnología está en constante evolución, por lo que las prácticas y herramientas que han sido efectivas y eficientes durante un tiempo, pueden dejar de serlo frente a otras alternativas que aporten un mayor valor a los usuarios y las organizaciones. Y este es caso de la identificación de usuarios mediante nombre de usuario y contraseña, que ya no aporta la seguridad que necesitan las empresas e instituciones actuales, sobre todo por la actividad de los hackers, cada día más importante, efectiva y nociva.

En los últimos años, las violaciones de seguridad han aumentado de forma muy considerable y, según el Informe Cost of Data Breach Report de IBM, "las credenciales robadas o comprometidas no solo fueron la causa más común de filtración de datos, sino que, con 327 días, fueron las que mayor tiempo tomaron para ser identificadas". De hecho, según la firma, el promedio del coste de estas brechas de seguridad superaba los 150.000 dólares.

Las soluciones de Gestión de Identidad y Acceso (IAM) deben ser efectivas para gestionar y asegurar el acceso a información crítica dentro de las organizaciones solo por usuarios autorizados. Es, en definitiva, un marco habilitador de los procesos empresariales, políticas y tecnologías para la gestión de identidades digitales, permitiendo el acceso solo a aquellos usuarios realmente capacitados para ello.

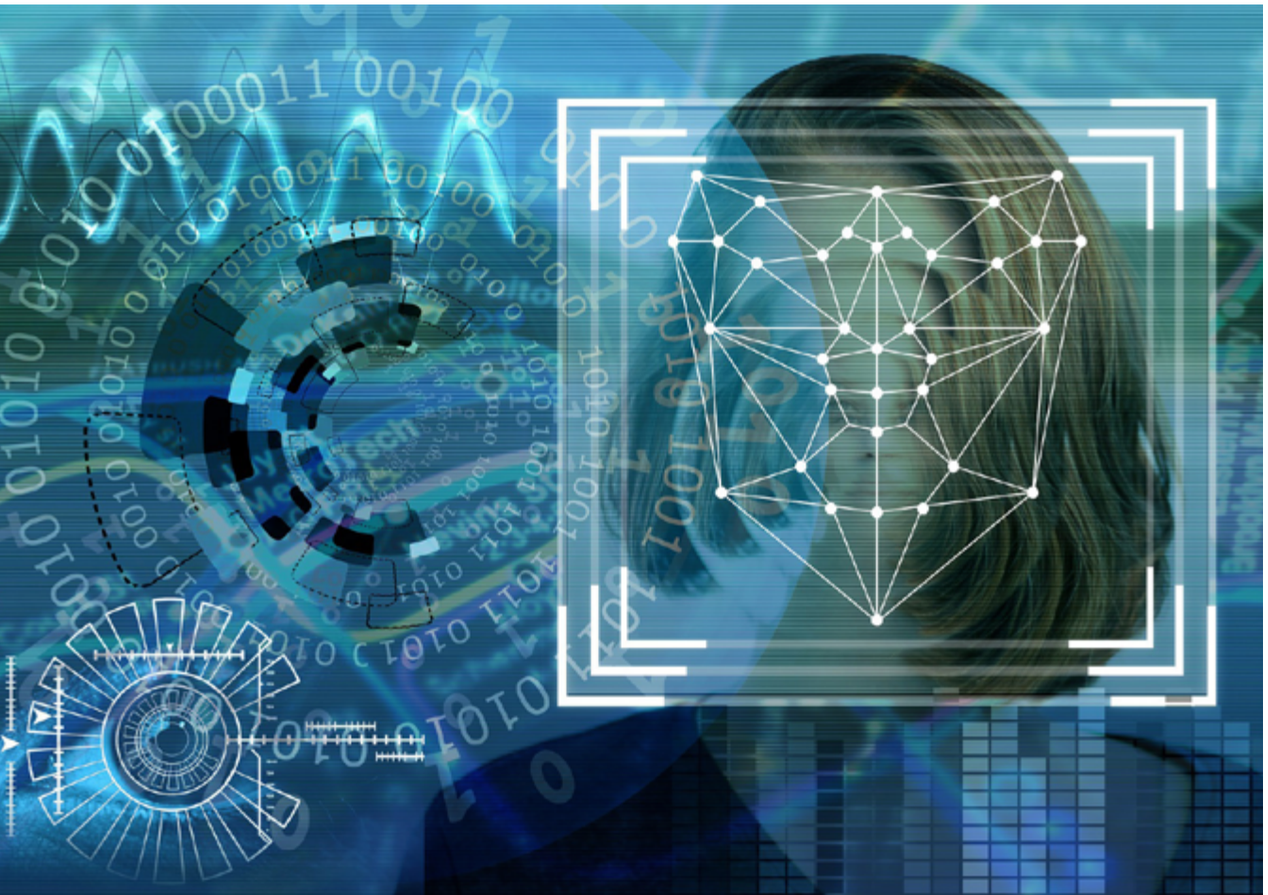
UNA NUEVA REALIDAD CADA DÍA MÁS PRESENTE

Sin embargo, como ya hemos mencionado, los métodos tradicionales de autenticación de identidad, como

LAS SOLUCIONES DE GESTIÓN DE IDENTIDAD Y ACCESO (IAM) DEBEN SER EFECTIVAS PARA GESTIONAR Y ASEGURAR EL ACCESO A INFORMACIÓN CRÍTICA DENTRO DE LAS ORGANIZACIONES SOLO POR USUARIOS AUTORIZADOS

contraseñas y nombres de usuario, se muestran ineficaces contra los niveles y eficiencia de los ciberataques actuales. Con lo que era necesario poner sobre la mesa una alternativa que sirviera para reemplazar estos elementos. Así, la tecnología de autenticación biométrica ha surgido como una de las propuestas más efectivas para la IAM, dado que se basa en características fisiológicas o comportamentales únicas, como huellas dactilares, reconocimiento facial y escaneo del iris, para verificar la identidad de un usuario, y esto provoca que sea una opción más segura que la autenticación basada en contraseñas tradicionales, ya que no es factible que los hackers repliquen datos biométricos de otra persona.

LA TECNOLOGÍA DE AUTENTICACIÓN BIOMÉTRICA HA SURGIDO COMO UNA DE LAS PROPUESTAS MÁS EFECTIVAS PARA LA IAM, DADO QUE SE BASA EN CARACTERÍSTICAS FISIOLÓGICAS O COMPORTAMENTALES ÚNICAS, COMO HUELLAS DACTILARES, RECONOCIMIENTO FACIAL Y ESCANEO DEL IRIS



Y las cifras de las consultoras respaldan esta percepción. Así, según los datos que maneja la consultora MarketsandMarkets, el mercado mundial de autenticación e identificación biométrica, situado en torno a los 42.900 millones de dólares en 2022, podría suponer hasta 82.900 millones en 2027, lo que supone un incremento anual medio del 14,1%, un incremento que, según el análisis de la consultora no se centra en un único sector económico, sino que se apoyaría en una creciente demanda de este tipo de soluciones en diferentes segmentos económicos y verticales industriales.

VENTAJAS QUE APORTA LA BIOMETRÍA A IAM

Como decíamos, la tecnología biométrica es altamente efectiva para asegurar los sistemas de IAM. De hecho, una reciente investigación de Biometrics Institute señalaba que el uso de la tecnología biométrica reduce de manera destacada el riesgo de violaciones de seguridad y robo de datos, y mejora la seguridad general de los sistemas de IAM.

Así, son varias las ventajas que aporta la biometría a IAM, y algunas de las más destacadas son:

➤ **Facilita el acceso en cualquier lugar.** En la actualidad las personas necesitan todo el tiempo sus identidades para utilizar servicios y recursos. En ese sentido, requieren acceso a cualquier plataforma sin límites utilizando sus identificaciones, eliminando así las barreras para que los clientes ingresen a la plataforma en cualquier momento y lugar.

➤ **Favorece la conexión entre las distintas partes.** La transformación digital que está produciéndose cada vez entre más organizaciones, obliga a la necesidad de que las personas, las aplicaciones y los dispositivos se mantengan conectados unos con otros. Y, como era de esperar, todos estos procesos traen consigo algunas amenazas de seguridad.

➤ **Mejora la productividad.** IAM por biometría automatiza el ingreso de nuevo personal y te facilita el acceso a todos los componentes del

sistema con el que funciona la empresa. Esto permite reducir tiempos en la entrega de accesos para que comiencen a producir de inmediato.

➤ **Optimiza la experiencia del usuario**. Recordar tantos nombres de usuario y contraseñas para acceder a las redes sociales, a las entidades bancarias y a demás servicios en Internet se convierte en un reto para las personas. Con IAM por biometría se obtiene una identidad que brinda acceso a diferentes sistemas.

LOS USUARIOS PREFIEREN SISTEMAS DE AUTENTICACIÓN BIOMÉTRICA

Un informe de Transparency Market Research apunta que la industria biométrica mundial elevará sus ingresos hasta superar los 136.000 millones en 2031, lo que representan un incremento medio anual por encima del 13%.

La clave puede encontrarse en una **encuesta publicada por PYMNTS**, que confirma más de uno de cada tres usuarios está dispuesto a utilizar métodos de autenticación biométrica. De hecho, uno de cada dos afirma estar preparado para decir adiós a las contraseñas. Unos datos que coinciden con los de otra **encuesta publicada por VISA**, según la cual, en EE.UU. más del 85% de los usuarios de consumo tiene interés en usar la biometría para identificarse o para realizar pagos, mientras que 7 de cada 10 piensan que es más sencillo que otros métodos, y casi la mitad cree que es más seguro que las contraseñas.

También son coincidentes los datos del **informe de Servicios de Identidad Digital de iProov**, que indican que el 55% de los encuestados ya utiliza biometría, ya sea reconocimiento facial o reconocimiento de huellas dactilares, para desbloquear sus dispositivos móviles.

➤ **Incrementa la rentabilidad:** La autenticación biométrica hace que no sea necesario emitir y reemplazar continuamente tokens de autenticación ni restablecer contraseñas olvidadas. Además, ayuda a prevenir las pérdidas económicas debido a violaciones de seguridad, la implementación de hardware o los gastos asociados al envío de mensajes de texto (SMS) cada vez que se requiere autenticación.

➤ **Se trata de una solución escalable:** La autenticación biométrica puede escalar fácilmente para satisfacer las necesidades de las grandes organizaciones, lo que la convierte en una solución ideal para empresas con muchos empleados. ■

MÁS INFO +

» Cost of Data Breach Report

» Next generation biometric technologies market

COMPARTIR EN REDES SOCIALES

#ENTREVISTA

Nuestra estrategia es brindar nuestra innovación, tecnología y protocolo de acceso, como marca blanca para la institución

RODRIGO JIMÉNEZ, MANAGING DIRECTOR DE B-FY

La gestión de identidades es uno de los elementos clave en la seguridad de las empresas e instituciones, y uno de los puntos de entrada de los atacantes. Utilizando la biometría se ofrece una solución más amigable con los usuarios y más robusta desde el punto de vista de la seguridad. Para ver cómo afronta este reto B-FY, hemos hablado con su Managing Director en nuestro país.

¿Cuáles son los principales problemas de seguridad a los que se enfrentan las empresas? ¿Cómo ha ido evolucionando esta realidad en los últimos meses/años?

Según informes recientes de empresas de ciberseguridad, los robos tanto de datos personales como de contraseñas se están disparando. El informe anual Global Digital Fraud Trends de TransUnion (publicado en marzo de 2022) revela que entre 2019 y 2021, el crecimiento en la tasa de sospecha de fraude digital a escala global aumentó en un 52,2 %. La mayor parte de los ataques parten del robo de bases de datos y venta de identidades o credenciales.

Según el Microsoft Digital Defense Report, entre julio de 2020 y junio de 2021, el mundo fue testigo del florecimiento de la economía del ciberdelito que registró un fuerte aumento. Este informe afirma que la ciberdelincuencia es un mercado maduro que sigue creciendo, tanto en tamaño como en sofisticación, mientras que los ciberdelincuentes cambian continuamente "de táctica, valiéndose de los eventos actuales para aprovecharse de objetivos vulnerables y avanzar en su actividad a través de nuevos canales". De acuerdo con el mismo estudio, el robo de identidad real aumentó un 81% en todas las industrias en el mismo período.

Los métodos de los ciberdelincuentes son cada vez más agresivos y, en los últimos tiempos, se orientan con mayor frecuencia a PYMES e individuos que, a diferencia de las grandes corporaciones, no tiene los medios o la capacidad de defenderse. El método de autenticación de identidad basado en usuario y contraseña es el eslabón más débil –el método menos seguro, en otras palabras– en todo el esquema de ciberseguridad.

> "B-FY OFRECE UNA SOLUCIÓN INNOVADORA, QUE CREA UN NUEVO PROTOCOLO DE ACCESO UTILIZANDO LA CAPACIDAD BIOMÉTRICA DEL DISPOSITIVO MÓVIL DEL USUARIO, SIN USO DE CONTRASEÑAS, NI ENVÍO DE PATRONES BIOMÉTRICOS POR INTERNET"

Los sistemas tradicionales de seguridad basados en la autenticación del conocimiento están demostrando ser ineficientes contra el cibercrimen. Además, los usuarios se ven abrumados por la necesidad de hacer seguimiento a un sinfín de contraseñas, que, según un estudio reciente, no son menos de 100 por persona. Como es de esperar, nadie va a memorizar 100 contraseñas distintas. Al final las personas terminan reutilizando un pequeño grupo de contraseñas para todos esos servicios. Además, en muchos de los casos, las contraseñas serán muy básicas, es decir, fácilmente vulnerables.

Por otro lado, los sistemas de seguridad de autenticación multifactor (MFA) se ponen a prueba todos los días. Aunque MFA es bueno, muchas de las implementaciones actuales son vulnerables, consumen mucho tiempo de los usuarios y son difíciles de implementar para las empresas.

¿Qué retos, tanto de seguridad como normativos, tienen que afrontar las empresas actualmente?

Para el 83% de las empresas, según el informe Cost of a data breach 2022 de IBM, la cuestión no es si se producirá una filtración de datos, sino cuándo. A escala global, el coste total medio de una filtración de datos ronda los 4,35 millones de dólares. Si hablamos de EE.UU., el coste se duplica, para llegar a los 9,44 millones de dólares, según este mismo informe.

Para las empresas, tener procesos seguros de identificación y autenticación son fundamentales tanto para el alta de nuevos clientes y empleados, así como para la prestación de servicios. Así, el uso de la tecnología biométrica para la autenticación de identidad se está convirtiendo rápidamente en la solución preferida de las empresas. No obstante, existen algunas preguntas fundamentales que las empresas deben hacerse antes de abordar cualquier proyecto que involucre datos biométricos. Para los usuarios, mantener la privacidad de sus datos también es una gran preocupación. Alrededor del 74% de los usuarios de Internet en los EE.UU. están

más preocupados que nunca por su privacidad en línea y el 79% de los usuarios de Internet de todo el mundo sienten que han perdido por completo el control sobre sus datos personales.

También en el frente del consumidor, la investigación de KPMG Corporate data responsibility: Bridging the consumer trust gap informa de que alrededor del 47% de los encuestados señaló estar preocupado por la posibilidad de que sus datos fueran hackeados, mientras que el 51% estaba preocupado porque pudieran venderlos.

Por lo tanto, dado que la vida se vuelve cada vez más digital, asegurar los datos de los usuarios no es solo una cuestión económica, sino una cuestión de confianza. La de los usuarios en relación con cómo las empresas que recopilan su información personal pueden usarla o mantenerla segura.

En los últimos años, casi todos los países del mundo han emitido algún tipo de regulación para proteger la privacidad de los datos. Estas leyes profundizan en cómo se recopila la información, cómo se informa a los interesados y qué control tiene un interesado sobre su información una vez que se transfiere.

> "EL CIBERATAQUE Y EL FRAUDE ONLINE SON UNA AMENAZA REAL Y CRECIENTE EN TODAS LAS EMPRESAS, INSTITUCIONES DE CUALQUIER VERTICAL, TANTO EN ESPAÑA, COMO EN EL EXTRANJERO"
>
> **RODRIGO JIMÉNEZ,**
> Managing Director de **B-FY**

¿Cuál es la respuesta que ustedes les dan para afrontar estos retos?
Como hemos visto, RGPD se considera un estándar en lo que respecta a la protección de datos, incluidos los datos biométricos. Uno de los pilares sobre los que se asienta esta empresa es proteger a las personas frente al fraude y proteger su identidad. El protocolo de identificación de B-FY ha sido diseñado de acuerdo con las directivas europeas de privacidad de datos, cuidando al máximo la privacidad del usuario y la de la empresa. Al utilizar el sistema B-FY para identificar a sus usuarios, nuestros clientes integran nuestro servicio a través de una librería en su aplicación. B-FY no recopila ni almacena datos biométricos de los usuarios.

Para verificar la identidad del usuario, B-FY solo necesita su correo electrónico y su número de teléfono, asociándose el dispositivo a una sola persona. Los datos de registro (teléfono y correo electrónico) se almacenan en una base de datos, que se encuentra en una red estanca solo accesible desde la propia plataforma B-FY. El factor biométrico del usuario está asociado al dispositivo que ha registrado como suyo, y sus datos quedan siempre bajo su control y custodia.

¿Cuál es el elemento diferencial de B-FY para ayudar a las empresas? ¿Cuál es vuestra estrategia de negocio?
Nuestra misión es identificar personas, eliminar el fraude y proteger la privacidad. Hemos vistos desde hace varios años, el auge del smartphone a nivel mundial, y sobre todo la mejora y robustez de la tecnología biométrica que vienen en estos dispositivos. Se predice que para el 2024, un 65% de todas las identificaciones de los individuos procederán de la capacidad biométrica del móvil. Segundo, el crecimiento de las aplicaciones móviles por parte de las instituciones. También ha ocurrido el aumento de los ciberataques por robos de credenciales o fraude de ID y el endurecimiento de las leyes de protección de datos y privacidad del usuario, sobre todo en Europa.

Por ello, B-FY lanzó al mercado, en 2022, una solución innovadora, creando un nuevo protocolo de acceso, utilizando la capacidad biométrica del dispositivo móvil del usuario, sin uso de contraseñas, ni envío de patrones biométricos por internet. Nuestra estrategia es brindar nuestra innovación, tecnología y protocolo de acceso, como marca blanca para la institución. De tal forma que, para el usuario final, esto sea transparente, y vea a la institución, ofreciendo este servicio a todos sus clientes finales, a través de su App móvil.

Cualquier usuario: el cliente, empleado, colaboradores, dirección, equipos de seguridad y tecnología, podrán usar su dispositivo móvil para identificarse de forma segura, sin uso de contraseñas, usando la App de la institución como herramienta omnicanal, tanto para accesos a espacios físicos como digitales. B-FY es una solución de identificación como servicio que aplica el principio identity-first (identificar siempre a la persona antes

de dar acceso al servicio). La identificación veraz de la persona autorizada es el punto más importante del modelo zero-trust. B-FY utiliza la biometría que los usuarios poseen en sus dispositivos móviles para poder identificarse verazmente, eliminando la necesidad de patrones biométricos en servidores centralizados, contraseñas y tarjetas de acceso, para obtener acceso a los servicios a la cual están autorizados, todo ello mediante un método muy simple y escalable.

Nuestro modelo de acceso con biometría descentralizada evita el riesgo de las soluciones basadas en biometría centralizada, que almacenan los patrones biométricos de los usuarios en sus servidores, provocando un alto riesgo para la protección de privacidad de los usuarios y la suplantación de identidad por parte de los ciberatacantes.

Con B-FY, se elimina la necesidad de enviar, almacenar, comparar datos sensibles de los usuarios, que finalmente pueden ser robados y utilizados posteriormente para atacar a las instituciones. De esta forma, los ciberatacantes se ven desarmados de su método usual de ataque, que es a través del robo de credenciales y de suplantación de identidad. La solución omnicanal de B-FY, a través de la App de la institución, permite una excelente experiencia de usuario englobando todos los casos de uso más frecuentes en una empresa. B-FY permite identificar clientes finales, empleados, personal externo, equipo de dirección, equipos de seguridad e IT, para poder darles acceso a servicios y espacios tanto físicos como digitales, utilizando tecnología de vanguardia que deja fuera a los ciberacriminales y evita fraudes por suplantación de identidad.

> “CON B-FY SE ELIMINA LA NECESIDAD DE ENVIAR, ALMACENAR, COMPARAR DATOS SENSIBLES DE LOS USUARIOS, QUE FINALMENTE PUEDEN SER ROBADOS Y UTILIZADOS POSTERIORMENTE PARA ATACAR A LAS INSTITUCIONES”

¿Cuál es el perfil adecuado de cliente con el que suelen trabajar?
B-FY utiliza la biometría que los usuarios poseen en sus dispositivos móviles para poder identificarse verazmente, eliminando la necesidad de patrones biométricos en servidores centralizados, contraseñas y tarjetas de acceso, para obtener acceso a los servicios a la cual están autorizados, todo ello mediante un método muy simple y escalable.

Todas aquellas empresas que dispongan de una estrategia de seguridad de nivel crítico y una fuerte orientación al cliente y en concreto, que dispongan de una aplicación móvil como oferta fundamental de servicio para sus clientes finales, corresponden con el perfil de clientes que buscamos.

¿Qué verticales de negocio son las que más foco ponen en la seguridad?
En líneas generales, son las grandes corporaciones, instituciones y multinacionales las que están más preparadas ante posibles ataques o fraudes. Estas disponen de mayores recursos financieros y humanos para establecer una robusta estrategia de seguridad, junto con un equipo interno especializado en ciberseguridad. Esto es así en todos los sectores donde operan y en diferentes verticales.

Por la misma razón, las PYMES, tanto en España como en el extranjero, son las que ofrecen mayor vulnerabilidad ante posibles ataques o fraudes, al disponer de menores recursos económicos y de personal experto en seguridad, para poder afrontar estos nuevos retos de posibles ataques o fraude.

El ciberataque y el fraude online son una amenaza real y creciente en todas las empresas, instituciones de cualquier vertical, tanto en España, como en el extranjero. No obstante, desde B-FY, tenemos un foco especial a los sectores de Finanzas, Salud, Educación, Energía y Telecomunicaciones que responden a un alto índice de criticidad en la seguridad y a la vez disponen de una importante estrategia de servicios y atención al cliente a través de sus aplicaciones móviles. ■

¿POR QUÉ LA BIOMETRÍA ES UNA SOLUCIÓN ESENCIAL EN LA EVOLUCIÓN DE IAM PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN?

RODRIGO JIMÉNEZ
Managing Director de B-FY

La IAM abarca la autenticación, autorización, gestión de usuarios y en este artículo, exploraremos cómo la tecnología biométrica se ha convertido en una solución esencial para abordar los desafíos actuales en ciberseguridad y protección de datos personales.

La Gestión de Identidad y Acceso (IAM) se ha convertido en un componente esencial de las operaciones empresariales modernas debido a la creciente amenaza de ciberataques, la necesidad de cumplir con regulaciones de privacidad de datos, la complejidad de las infraestructuras tecnológicas, el aumento de la movilidad y el trabajo remoto de los empleados, así como la búsqueda de experiencias de usuario mejoradas y la protección de la privacidad del usuario.

MEJORAR LA AUTENTICACIÓN

A medida que los métodos tradicionales de autenticación, como contraseñas y nombres de usuario, se han vuelto cada vez más vulnerables a los ciberataques, la tecnología de autenticación biométrica ha surgido como una de las soluciones más efectivas para la IAM.

La tecnología biométrica se basa en características únicas y difíciles de replicar, como huellas dactilares, reconocimiento facial y escaneo del iris, para verificar la identidad de un usuario.

Esta tecnología ofrece una ventaja significativa en términos de seguridad. Es prácticamente imposible que alguien pueda replicar los datos biométricos de otra persona. Según un informe de MarketsandMarkets, se espera que el mercado global de autenticación e identificación biométrica crezca a una tasa anual compuesta del 14,1%, alcan-

zando los 82,900 millones de dólares en 2027 debido a la creciente demanda de sistemas seguros de autenticación e identificación en diversas industrias.

IMPLEMENTACIÓN DE MEJORES PRÁCTICAS

A pesar de sus ventajas, la tecnología biométrica también enfrenta desafíos. Para aprovechar al máximo su potencial, las organizaciones deben implementar las mejores prácticas:

- **Evaluaciones de riesgos.** Se deben realizar evaluaciones periódicas de riesgos para identificar posibles vulnerabilidades en el sistema.
- **Almacenamiento seguro de datos biométricos.** Los datos biométricos deben almacenarse y cifrarse de manera segura para proteger la privacidad de los usuarios.
- **Políticas claras y transparencia.** Se deben proporcionar políticas y pautas claras para el uso de la tecnología biométrica, y los usuarios deben tener la opción de optar por no utilizarla si tienen preocupaciones sobre la privacidad.

VENTAJAS DE LA BIOMETRÍA EN IAM

La investigación ha demostrado que la tecnología biométrica es altamente efectiva para asegurar los sistemas de IAM. Un estudio del Biometrics Institute reveló que el uso de la tecnología biométrica puede reducir significativamente el riesgo de violaciones de seguridad y robo de datos, mejorando la seguridad general de los sistemas IAM. Algunas de las ventajas clave de la biometría sobre los métodos tradicionales de IAM incluyen:

> “OFRECEMOS UNA ALTERNATIVA RENTABLE Y ALTAMENTE SEGURA A LOS MÉTODOS TRADICIONALES DE IAM, LO QUE PERMITE A LAS ORGANIZACIONES MEJORAR LA SEGURIDAD Y LA EXPERIENCIA DEL USUARIO”
>
> **RODRIGO JIMÉNEZ,** Managing Director de **B-FY**

1. **Mayor seguridad.** La autenticación biométrica es inherentemente más segura que las contraseñas, que pueden ser hackeadas o robadas.
2. **Experiencia del usuario mejorada.** La autenticación biométrica es más rápida y conveniente para los usuarios, eliminando la necesidad de recordar contraseñas o llevar tokens de autenticación.
3. **Rentabilidad.** La autenticación biométrica puede ser más rentable a largo plazo al evitar la emisión y el reemplazo continuo de tokens de autenticación y la recuperación de contraseñas olvidadas.
4. **Escalabilidad.** La autenticación biométrica puede escalar fácilmente para satisfacer las necesidades de organizaciones de todos los tamaños.

LA SOLUCIÓN DE B-FY

En B-FY, nuestra principal preocupación es proteger a las personas y su identidad. Nuestro sistema utiliza la biometría para autenticar a los usuarios de manera segura y eficiente, eliminando la necesidad de contraseñas que pueden ser hackeadas o robadas. Además, no almacenamos patrones biométricos del usuario, lo que garantiza la privacidad.

Nuestra solución es fácil de usar y se integra sin problemas en las operaciones de nuestros clientes. Ofrecemos una alternativa rentable y altamente segura a los métodos tradicionales de IAM, lo que permite a las organizaciones mejorar la seguridad y la experiencia del usuario. La tecnología biométrica descentralizada que utilizamos garantiza la protección de los datos de los usuarios y la prevención de ciberataques.

En un mundo digital en constante evolución, la tecnología biométrica se ha convertido en un pilar fundamental para la Gestión de Identidad y Acceso. Con B-FY, estamos comprometidos a brindar una solución de IAM que sea segura, eficiente y orientada al usuario, ayudando a las organizaciones a abordar los desafíos actuales y futuros de seguridad y privacidad de datos. ■

MÁS INFO +

- State of Biometrics
- Biometric systems market

La ciberdelincuencia en España representa el 15,6% de los hechos delictivos*.

No dejes que los ciberdelincuentes acaben con tu negocio.

b°FY

Identify Individuals, Eliminate Fraud, Protect Privacy.

b-fy.com

* Informe sobre la Criminalidad en España 2021.