Una nueva forma de verificación de la identidad está ayudando a las organizaciones a identificar verdaderamente a las personas en lugar de simplemente "emparejar" ciertos elementos que supuestamente posee o conoce el usuario

Identificar personas, eliminar el fraude y proteger la privacidad mediante la identificación como servicio (IDaaS)

Marzo 2023

B-FY ha querido contar con la opinión de IDC para abordar aspectos relevantes en el mundo empresarial actual. En este sentido, José A. Cano, Director de Análisis y Consultoría de IDC España, ha proporcionado respuestas a sus preguntas.

P1. ¿Se han planteado las empresas ir a enfoques más seguros, donde la verificación de identidad se realice de forma descentralizada, evitando el riesgo de robo masivo de credenciales, y disminuyendo prácticamente a cero la posibilidad de ataques basados en suplantación de identidad?

El uso cada vez más creciente de los datos para la mejora de la experiencia de usuario y el avance hacia una organización conducida por datos (*data driven company*), está condicionando la necesidad de abordar los retos asociados a la gestión de las herramientas y aplicativos de seguridad, así como facilitar el entorno de seguridad, de manera que se avance en la gestión de la privacidad y seguridad de los datos. En este contexto, los retos de desplegar, integrar, mantener y gestionar herramientas de seguridad dispares son una carga para los recursos finitos del equipo de seguridad, según afirman el 62% de las organizaciones europeas.

Esta pregunta tan simple como "¿Quién eres?" es quizás una de las más importantes en un momento en el que la gestión y verificación de la identidad digital se ha convertido en un elemento esencial para la supervivencia de los negocios. La progresiva digitalización de las organizaciones, el auge del comercio electrónico (en 2022 se realizaron hasta un 40% más de transacciones que en 2021) y el auge de la banca on line están siendo palancas de aceleración en las inversiones asociadas a tecnologías de verificación de la identidad digital.

El incremento exponencial en las ciberamenazas, especialmente aquellas asociadas con el uso ilegítimo de credenciales, fue responsable del 48% de las brechas de seguridad en 2021 (este tipo de amenazas está experimentando un crecimiento superior al 35% en 2022, según datos de ForgeRock), suponiendo unas pérdidas de más de 56.000 millones de euros, según datos de Protocol y Javelin respectivamente.

Por ello, muchas empresas están comenzando a explorar otros enfoques más seguros para la verificación de la identidad y protección de credenciales. La descentralización de la verificación de la identidad es una de las formas que las organizaciones están considerando en la actualidad. De hecho, el mercado de la gestión de identidad está en claro crecimiento en España (16.4% respecto al cierre de 2022) y con una senda de crecimiento en el periodo 2023-2026,

presentando un CAGR del 14.4%, impulsado principalmente por la parte de **autenticación avanzada** y la **gestión de identidad** en entornos B2C.

En cuanto al **tipo de despliegue**, hay que destacar que los despliegues en **cloud** van a crecer al **19%** mientras los **on premise** lo van a hacer al **3%,** lo que va a significar que **para el año 2026 el 64% del mercado va a basarse en arquitecturas en la nube**.

En esta búsqueda de la seguridad descentralizada, una de las soluciones más populares que se está explorando es la tecnología de cadena de bloques o Blockchain, que permite la verificación de identidad descentralizada y segura. En un sistema de identidad descentralizado basado en Blockchain, la información de identidad se almacena en una red de nodos descentralizados en lugar de en una base de datos centralizada. Esto significa que la información de identidad no se encuentra en un solo punto de vulnerabilidad, lo que la hace más difícil de comprometer.

Otra de las soluciones se basa en la biometría, ya que puede ser mucho más segura que las contraseñas tradicionales. La autenticación biométrica utiliza características físicas únicas, como la huella dactilar, el reconocimiento facial o la voz, para verificar la identidad del usuario, de forma que no es transferible (es decir, cada persona tiene acceso a un conjunto de datos biométricos únicos), lo que garantiza contra la suplantación de identidad, ya que es difícil falsificar o robar datos biométricos. De esta manera, se garantiza una alta seguridad y fiabilidad, maximiza la experiencia de usuario en un contexto donde la progresiva movilidad del trabajador requiere el acceso a infraestructura, dispositivos, aplicaciones y datos en múltiples ubicaciones, lo que dificulta la gestión de todos los mecanismos de gestión de la identidad de las organizaciones.

No obstante, a pesar del aumento de la seguridad, la eficacia y la comodidad, la autenticación biométrica y sus usos en aplicaciones digitales y tecnológicas también tiene hándicaps que requieren ser tratados de manera específica por las organizaciones. Más allá del riesgo de hackeo de una base de datos biométricas y el compromiso de la privacidad que puede limitar el uso de sistemas de reconocimiento facial, el coste de implementación de este tipo de sistemas se configura como el principal hándicap al que las empresas deben hacer frente en el proceso de implementación.

En este entorno, la evolución hacia la "identificación como servicio (IDaaS) puede cambiar por completo la forma en la que las empresas se enfrentan al reto de verificación del acceso de las personas tanto física como digital, utilizando los mecanismos de identificación biométrica de los dispositivos móvil, maximizando el customer journey y haciendo frente a los hándicaps asociados al uso de la información biométrica.

Q2. ¿La unificación del acceso físico y on line es una cuestión que se estén planteando las empresas en la actualidad?

La pandemia ha sido un punto de no retorno para las inversiones digitales, acelerando las de la trayectoria digital de muchas organizaciones. El 90% de las organizaciones de España reconocen que tener una estrategia digital es ahora una necesidad, ya que la tecnología es el principal motor para conseguir resultados empresariales y superar los retos de la empresa. De hecho, los datos de IDC apuntan que para el año 2023, una de cada dos empresas generará el 40% de sus ingresos mediante la venta de productos o servicios digitales.

Por ello, lo "digital primero" debe significar "valor primero". Traducir las inversiones digitales en resultados de negocio es clave y esto requiere una convergencia de la tecnología y la estrategia empresarial, lo que exige transformar la forma en la que las empresas se enfrentan a la seguridad física como de aplicaciones y datos.

Las tecnologías de gestión de la identidad digital posibilitan **acreditar al usuario** durante todo el **customer journey**, una **identificación** que resulta crítica para proveer **servicios de valor añadido** y **banca contextual** asegurando una **buena experiencia de usuario,** alcanzando el equilibrio entre menos fricción y más seguridad (en las operaciones, onboarding, etc.) y garantizando un pleno **cumplimiento regulatorio**.

Sin embargo, la experiencia de identificación pasa en la mayoría de las ocasiones por el uso de múltiples contraseñas (en función del sitio al que se quiere acceder) el uso de tarjetas de acceso para acceder a un edificio, o el uso de la biometría centralizada si accede a un área restringida, entre otras situaciones. En estos casos, es muy complicado para las organizaciones identificar quién está accediendo a qué recursos si no tiene un único medio de identificación.

La progresiva convergencia entre la seguridad física y digital está impulsando la adopción de estrategias "*mobile-first*" en las organizaciones (aunque en la actualidad la adopción es aún lenta) en las que las aplicaciones móviles son la principal forma de acceso a servicios tanto físicos como digitales está cobrando cada vez más importancia, en un contexto de movilidad de empleados (hasta un 30% de los empleados están en movilidad en la actualidad según datos de IDC).

El uso de aplicaciones móviles ofrece una experiencia más personalizada y conveniente para los empleados y usuarios, lo que se traduce en mayor *engagement* del empleado o usuario con la organización, mejora la satisfacción de este y a su vez pueden aprovechar las capacidades de los dispositivos móviles, como la cámara y localización, incrementando así la experiencia de uso.

Q3. ¿Se han planteado las empresas ir más allá de ofrecer una app de uso alternativo a la web, y convertirla en el medio de acceso a sus servicios, tanto físicos como digitales?

En la actualidad, una persona media tiene más de 150 cuentas en línea que requieren contraseñas y dispone de 80 aplicaciones en su smartphone, a pesar de que únicamente utilice nueve de forma habitual. En este contexto, parece claro pensar que las superaplicaciones son una solución para consolidar todas las funciones y servicios que los empleados requieren en un solo lugar, en lugar de descargar diferentes aplicaciones para cada transacción, o crear una nueva contraseña para cada servicio.

En este sentido, si una empresa consigue convertir su aplicación móvil en la llave de acceso a todos los servicios, con una identificación descentralizada y convergente tanto en accesos físicos como digitales, estará mejorando enormemente la experiencia del usuario, mejorando también la seguridad de la empresa, y ganando un tiempo de exposición a la aplicación mucho más alto, pudiendo esto repercutir de manera muy positiva en mayores ventas, mejor fidelización del cliente, y menor exposición a fraudes.

Por ello, estas superaplicaciones pueden tener un impacto significativo en la identidad digital de los empleados, ya que más allá de las funcionalidades que recoge, recopilan diferentes tipos de datos sobre el empleado (nombre, dirección de correo electrónico, historial de navegación, actividad en redes sociales, entre otros datos).

Pensemos por ejemplo en una superaplicación que recopila datos de ubicación, historial de búsqueda y preferencias de compra, y de esta manera puede crear un perfil detallado del usuario que puede ser utilizado para personalizar la publicidad y el contenido en línea.

Sin embargo, esto también puede aumentar la preocupación por la privacidad de los usuarios y la posibilidad de que los datos sean utilizados de manera inapropiada o compartidos con terceros. O si la implementación de la autenticación biométrica no se realiza adecuadamente, puede haber riesgos de seguridad y privacidad asociados a la recopilación de datos biométricos.

Acerca del analista

José A. Cano, PhD. *Research & Consulting Director, IDC Spain*

Responsable de realizar investigaciones, proporcionar servicios de análisis y consultoría a las principales empresas tecnológicas y end-users en su proceso de transformación digital.

Con más de 17 años de experiencia en el mercado de TI y telecomunicaciones, antes de unirse a IDC trabajó en multinacionales como Deloitte, GAC Group, etc. así como la Administración Pública (Agencia de Innovación y Desarrollo de Andalucía IDEA).

José Antonio es Doctor Ingeniero de Telecomunicaciones por la Universidad de Valladolid y Master en Relaciones Internacionales y Comercio Exterior por INFOREM.

MENSAJE DEL PATROCINADOR

B-FY es una solución de identificación que utiliza las capacidades de reconocimiento biométrico de los teléfonos móviles, ofreciendo la máxima precisión en la identificación y la mayor seguridad a la privacidad de los datos de las personas.

B-FY es un servicio altamente eficaz, mucho más preciso que cualquier enfoque que utilice contraseñas. En cuanto a soluciones basadas en biometría tradicional, B-FY es más seguro, dado que su enfoque descentralizado neutraliza cualquier intento de suplantación de identidad con modelos de simulación biométrica, como por ejemplo el conocido deep fake, entre otros. Además, el modelo de B-FY potencia el concepto de identidad soberana, dado que la biometría de la persona a ser identificada siempre permanece en su teléfono móvil.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2022 IDC. Reproduction without written permission is completely forbidden.