



México ante el Día Internacional de las Telecomunicaciones: el reto de la inclusión digital y el fraude de identidad

Según el Instituto Federal de Telecomunicaciones, más de 90 millones de mexicanos son vulnerables a fraudes digitales como el SIM Swapping si no activan medidas de seguridad adicionales que no dependan exclusivamente de su red celular.

El gobierno impulsa la campaña del registro telefónico nacional para asociar una identidad a una línea móvil, hasta ahora solo 18.7% de las 145 millones líneas móviles han sido vinculadas.

Las soluciones de verificación de la identidad mediante biometría de Identity.io se consolidan como un nuevo estándar de seguridad para entidades públicas y privadas y para la población, facilitando la integración digital y mitigando los efectos de la suplantación y robo de identidad.

México encara la celebración del próximo Día Internacional de las Telecomunicaciones, que tendrá lugar el próximo 17 de mayo, con un sector en evolución que se enfrenta al importante reto de lograr una mayor inclusión social y digital, especialmente para los segmentos de la población más desfavorecida, y a la necesidad de mitigar los riesgos que supone el fraude digital, especialmente el causado por el robo y la suplantación de identidad.

Así, de acuerdo con los datos recogidos en un reciente estudio presentado por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), casi 16 millones de mexicanos podrían sufrir fraude digital en 2026, teniendo en cuenta el incremento del 18% previsto sobre los 13.5 millones de casos registrados el año pasado. A esto se suma un factor crítico de protección contra fenómenos como el SIM Swapping, al alza en México. Según el Instituto Federal de Telecomunicaciones, el 95,5% de los usuarios de telefonía del país, esto es, más de 90 millones de personas, corren peligro de sufrir fraudes digitales por suplantación de su línea celular si no activan medidas de seguridad adicionales que no pasen por la verificación de identidad mediante SMS o llamadas telefónicas.

A esto se suma el debate en torno al Registro Nacional de Usuarios de Telefonía Móvil (PANAUT), que buscaba vincular líneas móviles con la identidad de los usuarios mediante datos personales y biométricos. Aunque el proyecto enfrentó cuestionamientos constitucionales y fue invalidado por la Suprema Corte de Justicia de la Nación, dejó sobre la mesa un punto crítico para el sector: la necesidad de contar con mecanismos robustos de identificación para reducir delitos como la extorsión y el fraude telefónico. Hoy, la discusión ha evolucionado hacia modelos más sofisticados y menos intrusivos, donde la verificación biométrica descentralizada, desde el propio dispositivo del usuario, podría ofrecer un equilibrio entre seguridad, privacidad y viabilidad operativa para operadores y reguladores.

En un contexto en el que se estima que el 95% de los puntos de venta físicos solo requieren de una copia de una identificación (INE) para obtener un duplicado de la SIM que abra las puertas a todo tipo de suplantaciones de identidad, las soluciones de verificación biométrica, como las desarrolladas por Identity.io, están emergiendo como un habilitador clave para este nuevo entorno, al colaborar



directamente en la prevención del fraude digital mediante la reducción de los casos de robo o suplantación de la identidad.

Así las cosas, el proceso para poder aprovechar todo el potencial de la tecnología biométrica, se inicia en el onboarding, donde el usuario captura mediante su propio teléfono móvil sus huellas dactilares o sus rasgos faciales. Estas credenciales digitales se almacenan en el celular bajo los protocolos de seguridad más exigentes del mundo, y a partir de ese momento, pueden utilizarse para validar la identidad del usuario mediante consulta a una base de datos centralizada (1:N) y garantizar que la persona que lleva a cabo un determinado trámite es quien realmente dice ser (1:1). Además, las soluciones diseñadas por Identy.io permiten la emisión de códigos QR biométricos (BioCode), que el usuario puede presentar y que contienen su información personal, lo que le permite controlar en todo momento qué datos comparte, cuándo y con quién, así como almacenar todos sus datos críticos en una billetera digital (ID Wallet) bajo los estándares de encriptación más estrictos.

A diferencia de la verificación biométrica de la identidad con la que ya cuentan muchos celulares en el mercado, las soluciones de Identy.io almacenan las credenciales digitales del usuario en el terminal después de haber comparado sus huellas digitales o sus rasgos faciales contra una base de datos oficiales. Los celulares, por su parte, no llevan a cabo esta comprobación, y solo verifican que las huellas o el rostro del usuario coinciden con los que se utilizó en su momento en la puesta en marcha del dispositivo.

Las soluciones propietarias de Identy.io cuentan, además, con interfaces claras y sencillas de utilizar, que se valen de la prueba de vida pasiva (passive liveness) para poder determinar si una persona que intenta validar su identidad en un determinado servicio es real y no un doble digital. Todo ello, sin necesidad de llevar a cabo movimientos definidos previamente -parpadear un número determinado de veces o girar la cabeza de una determinada forma, por ejemplo-, sino que el sistema analiza factores como los movimientos sutiles de la piel del usuario o cómo se refleja la luz en él para descartar aquellos casos en los que pueda existir un caso de suplantación de identidad.

Según Jesús Aragón, CEO de Identy.io, "El sector de las telecomunicaciones se enfrenta en la actualidad a la necesidad de proteger a los usuarios frente al fenómeno del fraude digital, que anualmente causa miles de millones de pesos de pérdidas en el país, pero al mismo tiempo, a la extensión de los servicios digitales a aquellas personas que, hasta el momento, no han podido contar con ellos por vivir en áreas desfavorecidas o alejadas de los grandes núcleos urbanos del país. Con motivo del Día Internacional de las Telecomunicaciones, desde Identy.io hacemos un llamado para que la tecnología, que debería ser un factor de integración, no pierda esta vocación y ofrezca la posibilidad de que millones de personas puedan comenzar a llevar a cabo sus trámites y gestiones con las administraciones públicas y las entidades bancarias. Es exactamente esto lo que proponemos con nuestras soluciones de biometría sin contacto desde el celular del usuario: por un lado poder garantizar la máxima seguridad en cualquier trámite y, a su vez, ofrecer el máximo alcance de la digitalización entre la población".

La tecnología que ha desarrollado Identy.io se encarga de la captura de las 10 huellas dactilares con prueba de vida pasiva. Este sistema ofrece una gran fiabilidad en casi cualquier condición de iluminación y procesa todos los datos de forma local en el propio celular del usuario, solo necesitando



para ello un modelo con una cámara básica y un flash, y sin que sea necesario contar con una conexión a Internet en ese momento.

Sobre Identy.io

Con sede en EEUU y sedes en Brasil, México, Colombia, España e India, Identy.io es la referencia mundial en verificación de identidad digital mediante el uso de biometría móvil sin contacto. En Identy.io creemos en la autenticación multifactor, a la vez que abogamos por la necesidad de sustituir los métodos tradicionales de verificación de identidad mediante contraseñas, tokens u OTPs (One Time Password, por sus siglas en inglés), que no garantizan la identidad del usuario.

En Identy.io trabajamos con instituciones para garantizar la identidad en sus procesos de negocio mediante el uso de biometría sin contacto desde los dispositivos móviles de los usuarios. Nuestra protección de la autenticación física (liveness) hace que la biometría sea segura y desplegable a gran escala. Para más información, visite <https://identity.io>