

L.R. MADRID

Ante los riesgos asociados a la rápida evolución de la tecnología, Grupo Logalty crea soluciones innovadoras con el objetivo de garantizar la seguridad jurídica de las operaciones entre entidades y personas, especialmente en sectores altamente expuestos como la banca o los seguros. Conversamos con José Luis Martínez, director general adjunto y responsable de estrategia y desarrollo de negocio.

¿Cómo han evolucionado las amenazas de fraude con la IA y los deepfakes?

Los fraudes han cambiado radicalmente. Antes requerían habilidades avanzadas, pero ahora la IA facilita la creación de deepfakes realistas con solo unas muestras de voz o imagen. Esto permite estafas como el robo de cuentas bancarias, engaños en verificación facial y fraudes telefónicos. Además, el phishing es ahora más creíble, natural y personalizado, sin errores sospechosos, lo que dificulta su detección incluso por usuarios experimentados.

La IA también falsifica documentos con gran precisión, generando identidades, pasaportes o extractos bancarios falsos de cero, además de modificar en cuestión de segundos documentos escaneados, lo que aumenta el riesgo en entornos digitales y presenciales.

¿Cómo combate Grupo Logalty estos riesgos sin que llegue a afectar a la experiencia del usuario?

El reto es equilibrar seguridad y experiencia de usuario: los procesos complejos ahuyentan a los usuarios, pero los simples son vulnerables. Soluciones como la autenticación multifactor –que combina contraseñas, biometría, códigos enviados al móvil o aplicaciones externas–, la detección de vida en tiempo real para evitar fraudes mediante deepfakes, y el uso de inteligencia artificial para identificar patrones anómalos o inconsistencias visuales, ayudan a reforzar la seguridad de los sistemas.

Sin embargo, cuantos más elementos se integran, más se puede ver comprometida la fluidez y sencillez del proceso. Para resolverlo, desde Grupo Logalty, hemos desarrollado Very-ID, una tecnología innovadora que garantiza protección sin comprometer la experiencia del usuario.



LOGALTY

José Luis Martínez director general adjunto de Grupo Logalty. Responsable de estrategia y desarrollo de negocio

«Pasamos de validar documentos a verificar datos en fuentes oficiales»

Grupo Logalty es la LegalTech y RegTech líder en el mercado ibérico, especializada en identificación digital, certificación y contratación electrónica

¿Qué hace a Very-ID una herramienta eficaz y en qué sectores destaca?

Leemos el chip del DNI, pasaporte y TIE. Es una forma muy segura de verificación, ya que extrae datos directamente del chip, que son oficiales e inalterables, y los compara con otros elementos de verificación en tiempo real para proporcionar

una autenticidad garantizada. Además, mejora la experiencia del usuario al evitar el ingreso manual de información.

Su ámbito de aplicación es muy amplio. En el sector financiero facilita la apertura de cuentas y combate el blanqueo de capitales; en salud previene suplantaciones que pueden comprometer la se-

guridad de los pacientes y generar pérdidas económicas; y en logística permite verificar la identidad en la entrega de paquetes o mercancías. También impulsa la digitalización en la administración pública, al evitar la presentación de documentos físicos, y reduce el fraude en sectores como el inmobiliario o el educativo, acelerando procesos como contratos o matrículas.

¿Cómo transforma Fuentes Fiables la forma en que compartimos información personal?

Hoy en día, muchas verificaciones aún dependen de documentos físicos o digitales, con riesgos de suplantación o fraude. Para asegurar que una persona o empresa es quien dice ser y su información es veraz, entran en juego las fuentes oficiales de confianza. En Grupo Logalty apostamos por validar datos desde fuentes auténticas, como Agencia Tributaria, Seguridad Social, Registros, Banco de España o la Policía. Con Fuentes Fiables, las entidades pueden verificar información en tiempo real en bases oficiales de manera recurrente, reduciendo fraude y burocracia. Es un cambio de paradigma: pasar de validar documentos a confirmar datos directamente en las fuentes que los generan.

¿Qué papel juegan estas tecnologías en la protección de las



Hoy en día la confianza digital es determinante para las transacciones en línea

empresas frente a posibles responsabilidades legales?

Las empresas deben cumplir con normativas de seguridad, privacidad y prevención del fraude, como el Reglamento General de Protección de Datos (GDPR), la Ley de Servicios Digitales y regulaciones específicas en sectores financieros y administrativos. Su incumplimiento puede conllevar sanciones económicas, demandas civiles e incluso consecuencias penales en casos de fraude o blanqueo.

Tecnologías como Very-ID y Fuentes Fiables ayudan a minimizar riesgos legales al asegurar la identidad de los usuarios. Generamos trazabilidad y evidencia legal al registrar el proceso de verificación y autenticación, permitiendo que las empresas demuestren el cumplimiento legal en auditorías o litigios. También ayudamos a cumplir normativas KYC (Know Your Customer) y AML (Anti-Money Laundering), evitando clientes fraudulentos en sectores como banca, seguros y administraciones públicas, especialmente en procesos críticos como firma de contratos digitales o solicitud de créditos y becas.

¿Cómo contribuyen estas soluciones a generar confianza en un entorno digital donde la desinformación y la suplantación son cada vez más comunes?

La desinformación y la suplantación de identidad avanzan con la IA y los deepfakes, por lo que la confianza digital es determinante en las transacciones en línea. Very-ID y Fuentes Fiables refuerzan esta confianza con verificación de identidad en tiempo real. Very-ID extrae datos del chip de documentos oficiales, lo que evita fraudes en procesos críticos y reduce el riesgo de suplantación con credenciales verificadas. Fuentes Fiables obtiene datos directamente de entidades oficiales, garantizando fuentes seguras y verificables. Ambas fortalecen la reputación de las organizaciones que las implementan, promoviendo seguridad entre sus clientes y socios y diferenciándose de competidores que no cuentan con estos mecanismos.