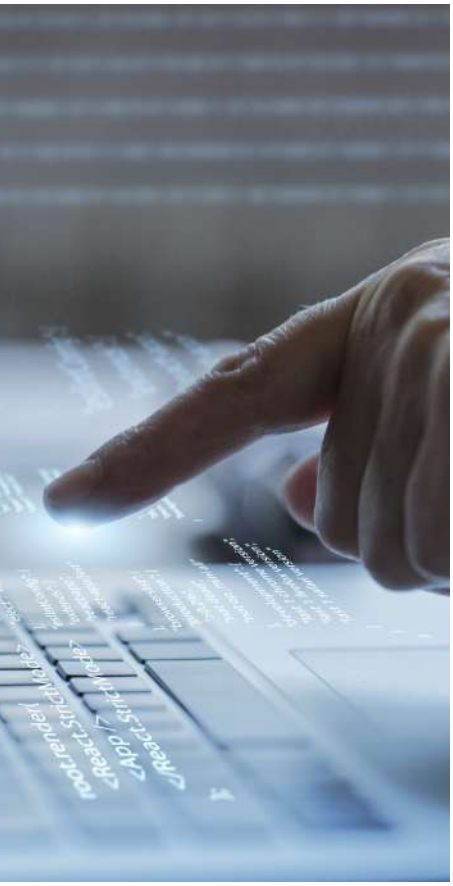
www.mexis.net

DEL PASSWORD AL RECONOCIMIENTO FACIAL: SALTO A LA SEGURIDAD DIGITAL AVANZADA



Durante décadas, la autenticación mediante usuario y contraseña ha sido el método predominante para acceder a sistemas y proteger información digital.

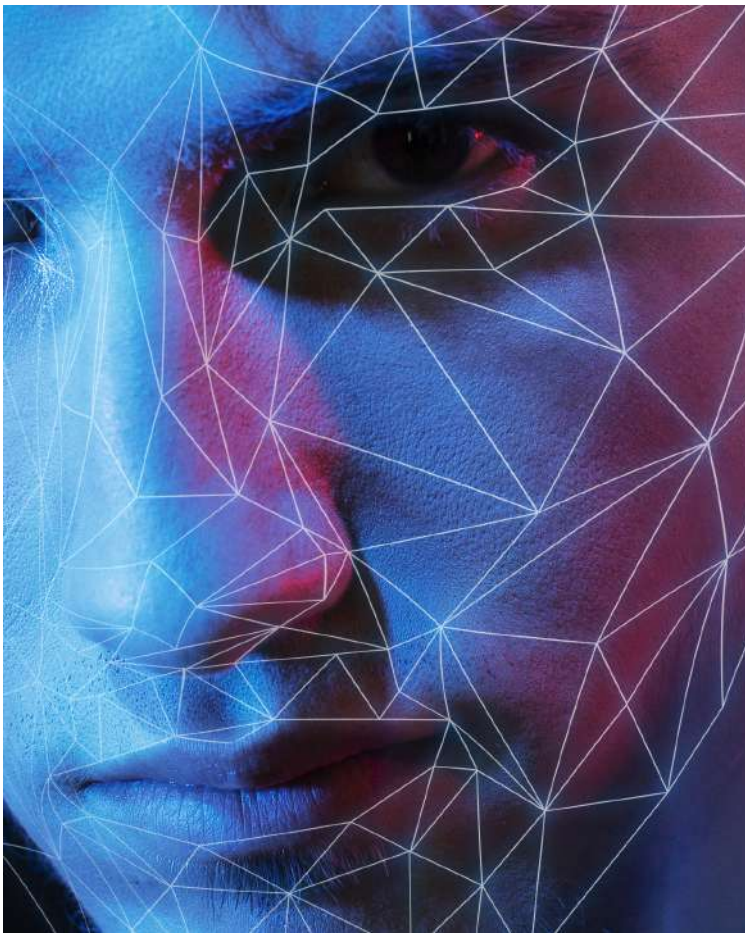
Sin embargo, en el contexto actual, con un ecosistema digital cada vez más complejo y amenazas sofisticadas, este sistema tradicional resulta insuficiente para garantizar la seguridad que requieren las organizaciones y los usuarios.

Y es que, según el informe "Verizon Data Breach Investigations Report 2025", **el abuso de credenciales robadas fue el vector inicial en el 22% de las brechas de seguridad,** mientras que el factor humano, incluyendo errores y phishing, estuvo presente en el 60% de los casos.

Hacia una nueva norma: autenticación multifactor y biométrica

El informe "Ciberseguridad en el Edge: Innovación, riesgos y amenazas", elaborado por knowmad mood, pone de manifiesto esta transformación y destaca cómo **la autenticación multifactor (MFA) y los métodos biométricos se están consolidando como la nueva norma en materia de seguridad digital.**

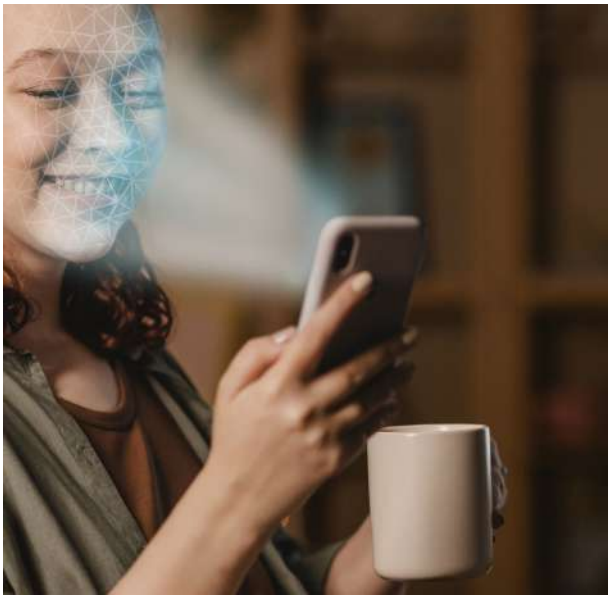
Este informe destaca que la autenticación multifactor (MFA) y **los métodos biométricos se están consolidando como el nuevo estándar de seguridad digital**, especialmente en entornos críticos y en aplicaciones que requieren altos niveles de protección. La MFA exige la combinación de varias formas de verificación, como una contraseña y una segunda forma de identificación, que puede ser un código temporal, un token físico o un dato biométrico, para otorgar acceso a sistemas sensibles. **Este enfoque dificulta enormemente los accesos no autorizados y los ataques** de suplantación de identidad.

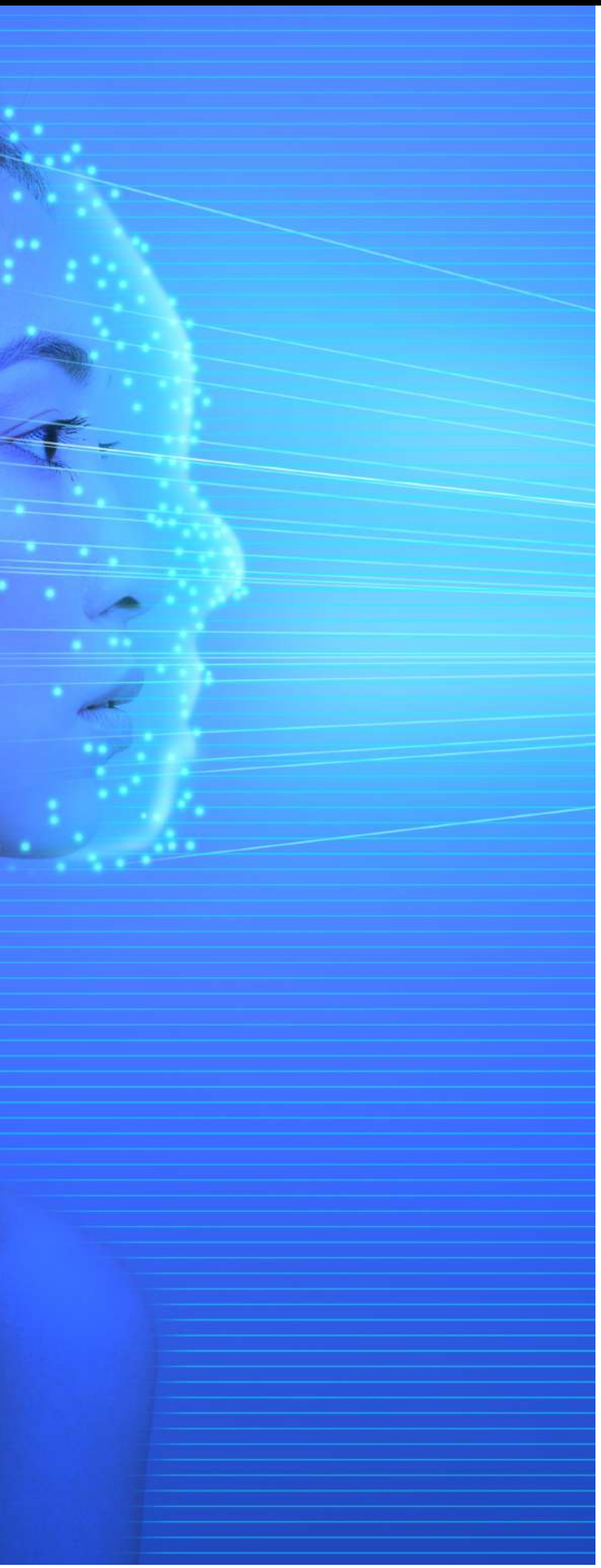


Los métodos biométricos, como el **reconocimiento facial, la huella dactilar o el escaneo del iris, se están integrando de forma creciente en dispositivos móviles, sistemas bancarios y plataformas corporativas**. Según el informe, la MFA y la biometría "son una protección más que reduce significativamente el riesgo de acceso no autorizado y ataques de suplantación de identidad", aportando tanto seguridad como una experiencia de usuario más ágil y cómoda.

Zero Trust y automatización: pilares de la defensa moderna

Bajo el principio de "nunca confiar, siempre verificar", **Zero Trust exige que todos los usuarios, incluidos los empleados, verifiquen su identidad antes de cada acceso a recursos críticos**, utilizando mecanismos como la MFA, la verificación del dispositivo y la segmentación de la red. Este enfoque es especialmente relevante ante el auge del trabajo remoto y la necesidad de proteger el acceso a infraestructuras distribuidas.





La automatización se presenta como otro elemento clave, ya que permite a los equipos de ciberseguridad gestionar grandes volúmenes de incidentes sin intervención manual, reducir el tiempo de respuesta y centrarse en amenazas complejas. **Las herramientas automatizadas incorporan funciones de detección, generación de alertas y respuesta inicial**, añadiendo una capa fundamental de protección ante ataques a gran escala.

Retos y oportunidades en la adopción de nuevas tecnologías de autenticación

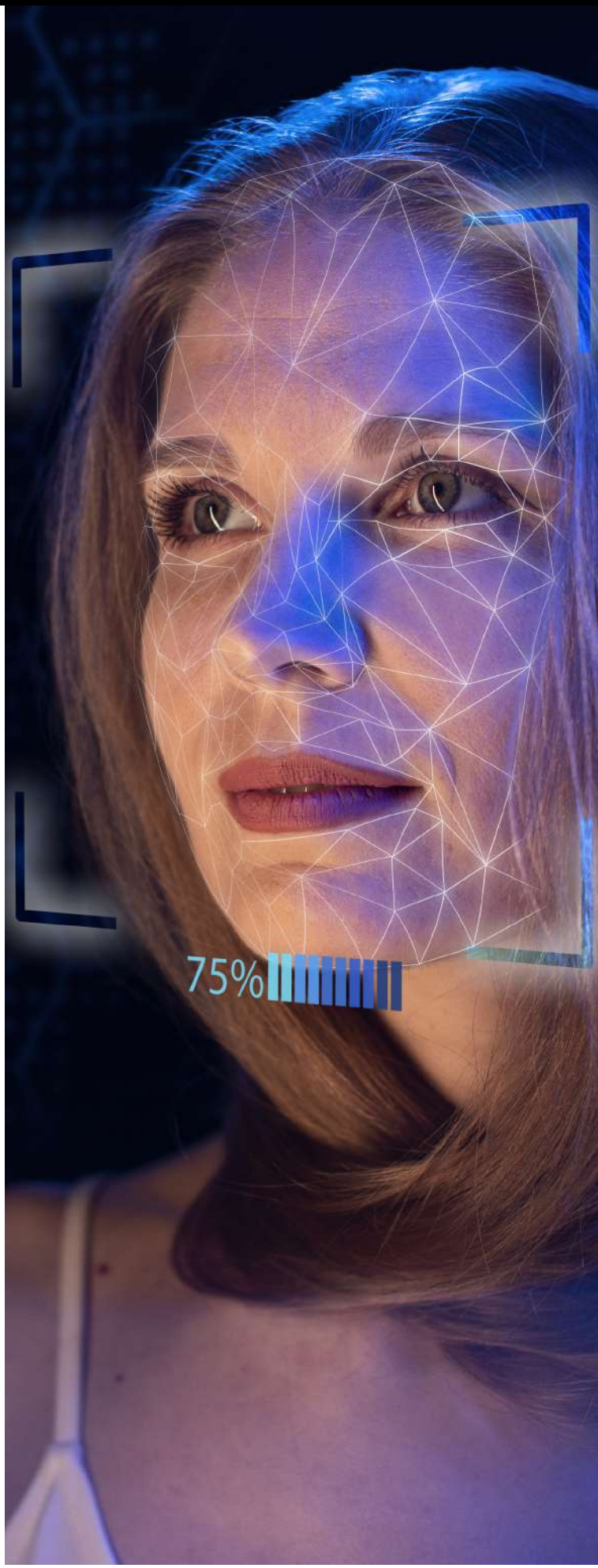
A pesar de sus ventajas, **la adopción de MFA y biometría implica desafíos importantes**. El informe señala que la privacidad y la protección de los datos biométricos requieren estrictos protocolos y el cumplimiento de normativas como el Reglamento General de Protección de Datos (RGPD) en Europa. Además, **la integración de estas tecnologías en infraestructuras existentes demanda inversión, planificación y la garantía de compatibilidad y usabilidad para los usuarios.**

El crecimiento de dispositivos IoT en sectores como la industria, la salud y el hogar también amplía la superficie de ataque, haciendo imprescindible la autenticación robusta, el cifrado y la gestión de identidades para evitar que estos dispositivos se conviertan en puntos de entrada para los atacantes.

Gobernanza, resiliencia y capacitación: una visión integral

El informe de knowmad mood aboga por una visión integral de la ciberseguridad, donde la gobernanza de datos, la resiliencia cibernética y la capacitación continua de los empleados son factores decisivos. **La gobernanza de datos ayuda a mantener el control de los activos digitales y a cumplir con las regulaciones de privacidad y seguridad**, mientras que la resiliencia cibernética permite a las organizaciones resistir y recuperarse rápidamente de incidentes, minimizando el impacto operativo y reputacional.

"El futuro de la ciberseguridad pasa por dejar atrás la dependencia exclusiva de la contraseña. La autenticación multifactor y la biometría no solo fortalecen la defensa contra accesos no autorizados, sino que también facilitan una experiencia de usuario más fluida y segura", afirma Roberto Liesa, Head of Cloud & Cybersec Alliance de knowmad mood.



Fuente de información: cybersecuritynews