**La IA puede ser una amenaza, pero también una aliada para proteger las identidades**

* **El 34% de los directivos europeos teme el phishing impulsado por IA, mientras que el 87% ya usa esta tecnología para reforzar la seguridad de identidades**
* **Solo el 34% confía en su proveedor de identidad y casi la mitad ha sufrido pérdidas económicas por robo de identidad**
* **Aunque el 88% ve esencial el MFA resistente al *phishing*, solo el 32% confía en él; el 70% busca consolidar proveedores para reducir complejidad**

**Madrid, 3 de septiembre de 2025. –** La inteligencia artificial puede ser tanto una ventaja como un riesgo, según **el nuevo informe de Cisco DUO “**[**2025 State of Identity Security**](https://resources.duo.com/explore/assets/2025-state-of-identity-security-report?utm_medium=web-referral&utm_source=blog&utm_campaign=2025-state-of-identity-security-ebook)**”**, basado en encuestas a **325 responsables de TI y seguridad en Europa**, entre otros. El dato más destacado es que **el 34%** de los directivos considera que **el phising impulsado por IA será una de las principales amenazas** para la identidad digital en 2025. Sin embargo, al mismo tiempo, **la IA también está ayudando a modernizar la protección de las identidades**. De hecho, **el 87% de las empresas europeas** ya están impulsando soluciones de seguridad específicos en sus redes para frenar los ataques basados en IA.

**Riesgos para la seguridad de la identidad**

Aunque los directivos reconocen la importancia de la seguridad de la identidad, existen grandes brechas en cuanto a confianza y ejecución. Según el informe, **solo un 34% de los directivos europeos creen que su proveedor de identidad actual (IdP)** puede prevenir ataques a las identidades. Esto se debe, entre otros factores, a la complejidad de los sistemas y a la falta de transparencia sobre posibles vulnerabilidades.

Un **96% de los directivos afirma que una infraestructura de identidad compleja compromete la seguridad global de su organización.** Además, **el 88% reconoce que no tiene una visión completa de los riesgos de identidad dentro de su empresa**. No es de extrañar: de media, los equipos de TI y seguridad utilizan **cinco herramientas diferente para resolver** un problema relacionado con la identidad.

Las consecuencias pueden ser costosas. Un 48% de los responsables de la toma de decisiones ha sufrido pérdidas económicas debido al robo de identidad. Como respuesta a esta amenaza, **el 76% ya ha aumentado su inversión en seguridad** de identidad de cara a 2025.

**Phising constante y brechas en MFA**

La amenaza constante del phising subraya la necesidad de una i**mplementación segura de autenticación multifactor (MFA)**. No obstante, aunque el 88% de los directivos considera esencial contra con MFA resistente al phising, s**olo el 32% confía plenamente en la eficacia de sus controles actuales frente a este tipo de ataques.**

No obstante, el 42% de las empresas europeas ya ha i**mplementado tokens FIDO2 para MFA resistente al phising.** Los tokens de hardware que cumplen con los estándares de la FIDO Alliance (Fast IDentity Online) se conectan al ordenador, por ejemplo, como una memoria USB, y ofrecen un alto nivel de seguridad porque la clave privada permanece en el dispositivo. Sin embargo, estos tokens suelen estar reservados para usuarios privilegiados debido al esfuerzo que implica **su gestión (59%), el coste del hardware (47%) y la necesidad de formación adicional (44%).** Al menos el 52% de los directivos quiere implantar el acceso sin contraseña, aunque prevén desafíos en la implementación.

**El 70% busca consolidar proveedores, también para mejorar la transparencia en tiempo real**

Existen varios obstáculos a la hora de proteger las identidades. Un 80% de los responsables de TI reconoce que **las soluciones de seguridad de identidad se añaden a la infraestructura como un complemento**, en lugar de integrarse desde el principio. Esto puede generar **costes adicionales, mayor complejidad y menor transparencia**. Para mejora esta situación, el 70% de los equipos está considerando activamente consolidar proveedores.

Además, la visibilidad en tiempo real del comportamiento de identidades y dispositivos es fundamental para que los equipos de seguridad y TI puedan tomar decisiones informadas. De hecho, **el 53% de las empresas ya ha integrado completamente la telemetría de identidad y dispositivos.**

*“Las empresas necesitan soluciones de identidad modernas que prioricen la seguridad sin sacrificar la experiencia del usuario”,* señala **Andreu Vilamitjana, director general de Cisco para España y Portugal.** *“Solo una gestión de identidades y accesos (IAM) orientada a la seguridad en la red corporativa garantiza una protección sólida de la identidad frente a ataques basados en IA”,* continúa diciendo.

El informe ***“2025 State of Identity Security: Challenges and Strategies from IT and Security Leaders”*** ha sido elaborado por Cisco Duo. Duo y Cisco Identity Intellignce ayudan a equipos globales a comprender el complejo apanorma de la gestión de identidades, ofreciendo administración de identidades simplificadas y centrada en l aseguridad, MFA resistente al ohising sin fricciones y telemtría unificada de identidades.

Más información disponible en este [blog;](https://duo.com/blog/research-insights-4-trends-reshaping-identity-security-in-2025) El estudio global completo puede consultarse [aquí](https://resources.duo.com/explore/assets/2025-state-of-identity-security-report?utm_medium=web-referral&utm_source=blog&utm_campaign=2025-state-of-identity-security-ebook); Las infografías con los datos globales están disponibles [aquí](https://resources.duo.com/duo-library/challenge-strategies-leaders-infographic).

**\*\*\*\*\*\***

**Acerca de Cisco**

Cisco (NASDAQ: CSCO) es el líder tecnológico mundial que está revolucionando la forma en que las organizaciones se conectan y protegen en la era de la IA. Durante más de 40 años, Cisco ha conectado al mundo de forma segura. Con sus soluciones y servicios basados en IA líderes en el mercado, Cisco ayuda a sus clientes y partners y a las comunidades a impulsar la innovación, mejorar la productividad y reforzar su resiliencia digital. Con el propósito como eje central, Cisco mantiene su compromiso de crear un futuro más conectado e inclusivo para todos. Descubre más en [news-blogs.cisco.com/emea/es](https://news-blogs.cisco.com/emea/es/) / [The Network](https://newsroom.cisco.com/) y síguenos en X en [@Cisco](https://twitter.com/Cisco).

Cisco y el logotipo de Cisco son marcas comerciales o marcas registradas de Cisco y/o sus filiales en Estados Unidos y otros países. Puede encontrarse un listado de las marcas comerciales de Cisco en [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Las marcas comerciales de terceros mencionadas son propiedad de sus respectivos dueños. El uso de la palabra partner no implica una relación de asociación entre Cisco y cualquier otra empresa.

**Para obtener más información:**

[Cisco España](http://www.cisco.com/c/es_es/index.html)

Ariadna Hernández, Directora de Comunicación

ariahern@cisco.com

[Team Lewis](http://www.teamlewis.com/es)

Nina Janmaat

Tel: 91 926 62 82

E-mail: [nina.janmaat@teamlewis.com](https://u7367035.ct.sendgrid.net/ls/click?upn=u001.Poj1F9nGI3M2MniuU7PQfHkhhPWBGNMvJNbO4EAPce7FZsG5EkSnvtC4C-2Bbopr5xEBh2_SiyBeK-2BfnHBbngR9woVGj7kRQLNS3P4mppV2ugZVmGzp6eimV3JlPAchLJPgLumUNF6q-2Fb5U-2B2myvsSO5npwhKNQNdKATaLBpSdmcbNwEzc5DxJTrlAilyfOjvkz-2FfEE2AkrUsZlxHwlSo-2FxffBn985WVd9G1c1IFL8r6Di-2FiDML4sHJb1T1Nb23K-2Bt4147T9JXTs1n7n-2BlmwN-2BTcznReQ-3D-3D)

Juan Ortiz

Tel: 91 926 67 05

E-mail: juan.ortiz@teamlewis.com