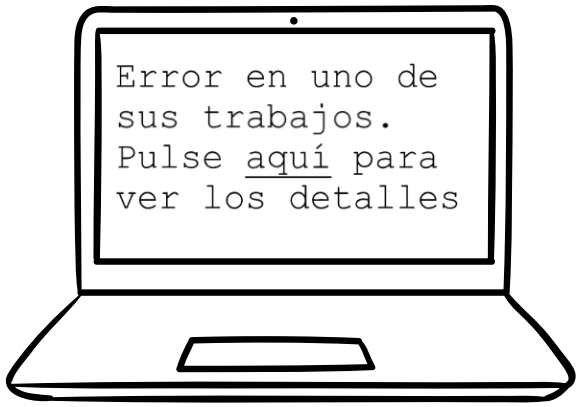
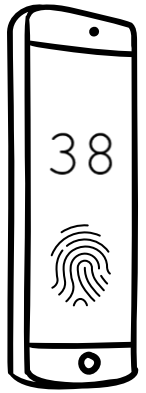
Ya tengo MFA ¿Es suficiente?

Julián de la Morena
Evangelino Valverde

JJ.TT. RedIRIS 2023

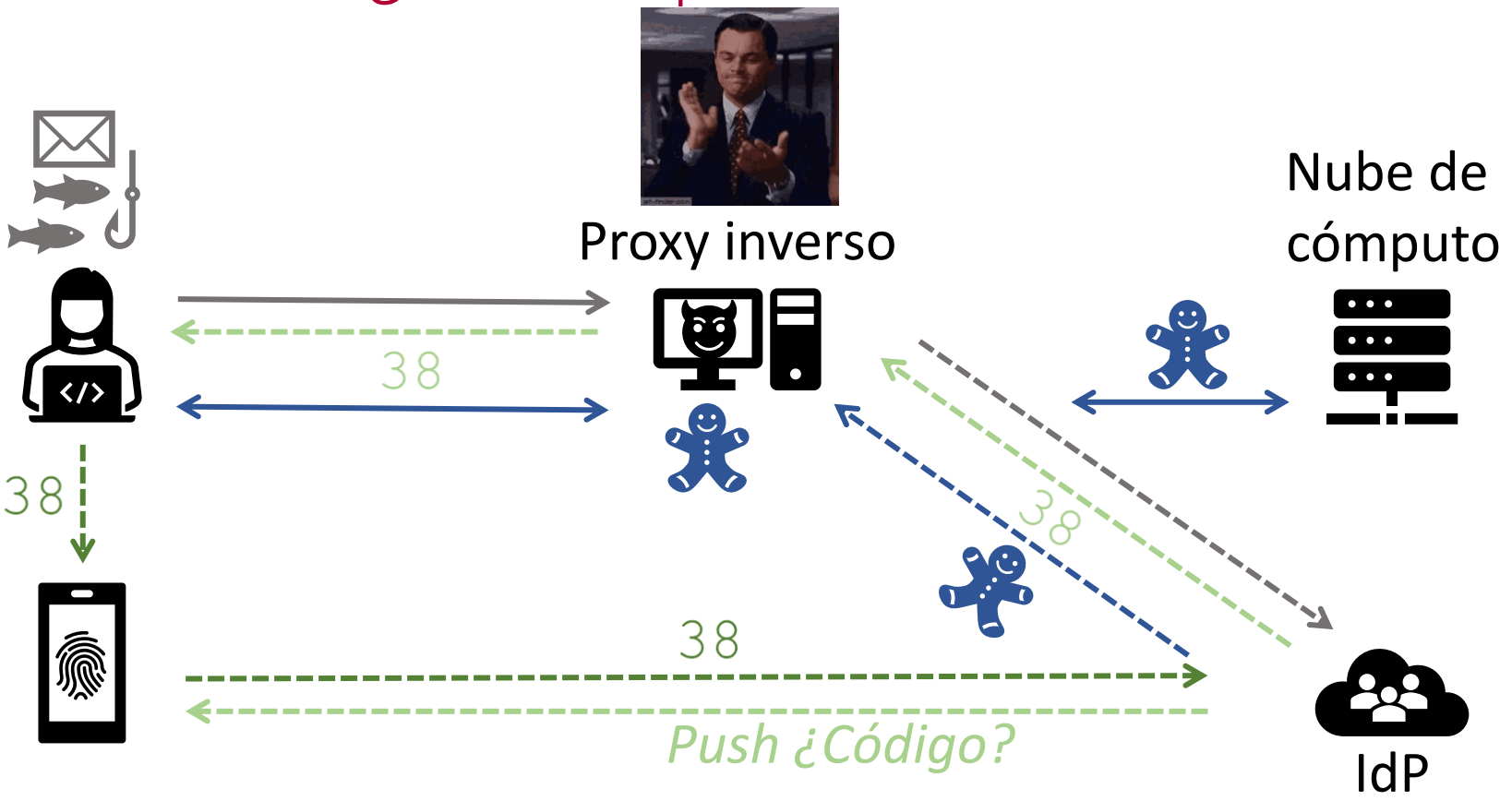
Elvira y la autenticación multifactor (MFA)





16 días después…

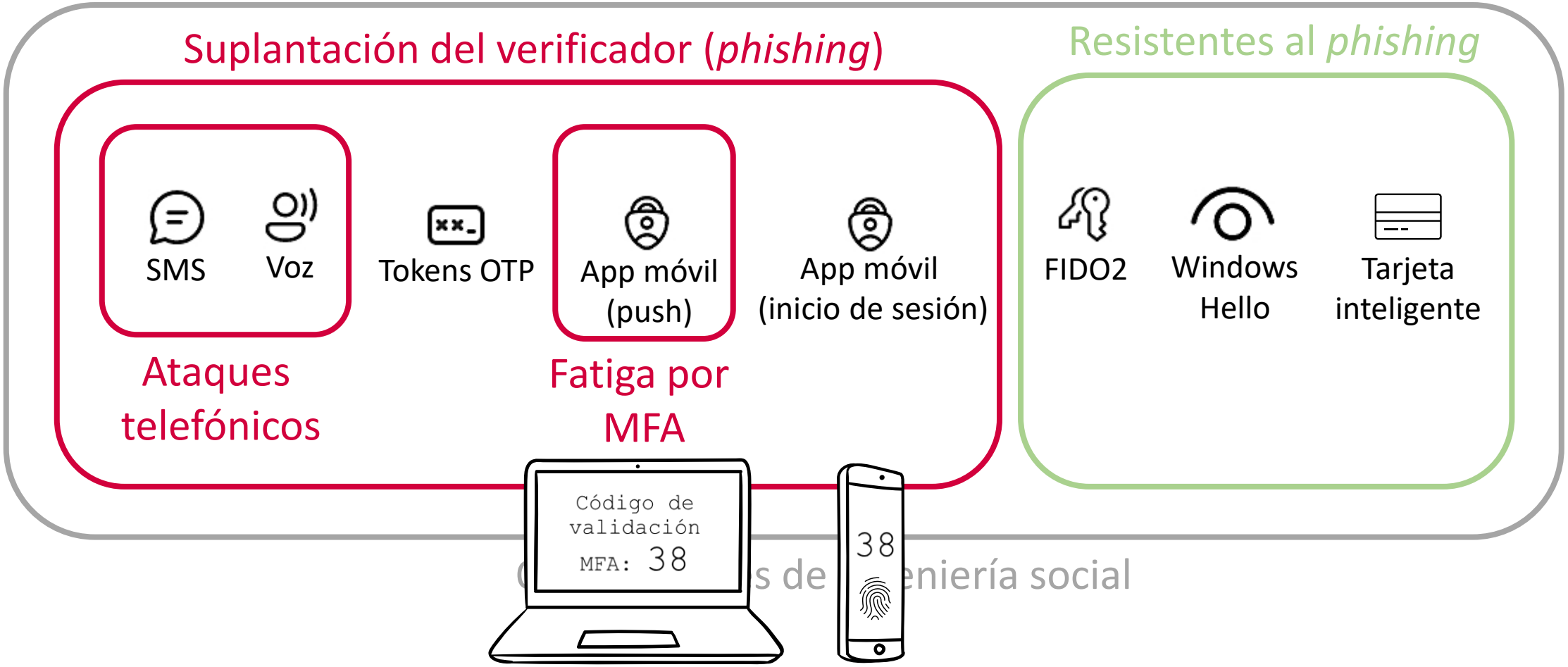
¿Qué le pasó a Elvira?



“Over 10,000 Organizations Targeted in AiTM Phishing Campaign That Circumvents MFA”
spiceworks.com, 14/07/2022

Imagen: From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud, Microsoft, 2022

¿Existe algún tipo de MFA seguro?



¿Por qué algunos métodos son resistentes al *phishing*?

Factores en paralelo

SMS

Voz

Tokens OTP

App móvil (push)

App móvil (inicio de sesión)

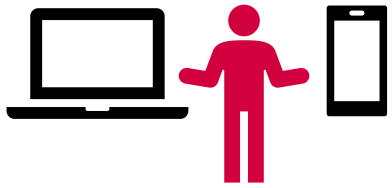
Factores en serie

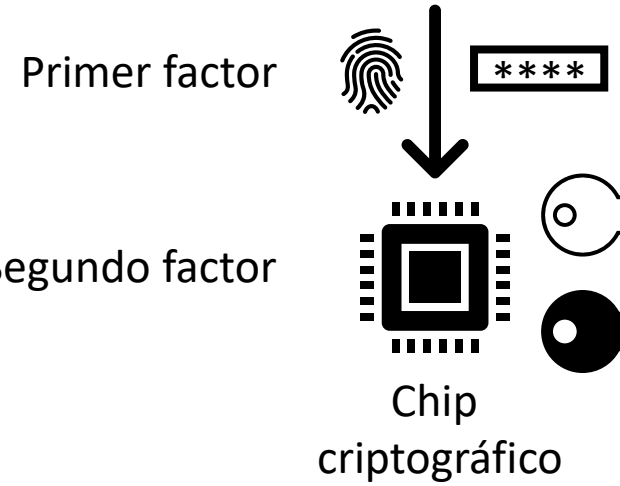
FIDO2

Windows Hello

Tarjeta inteligente

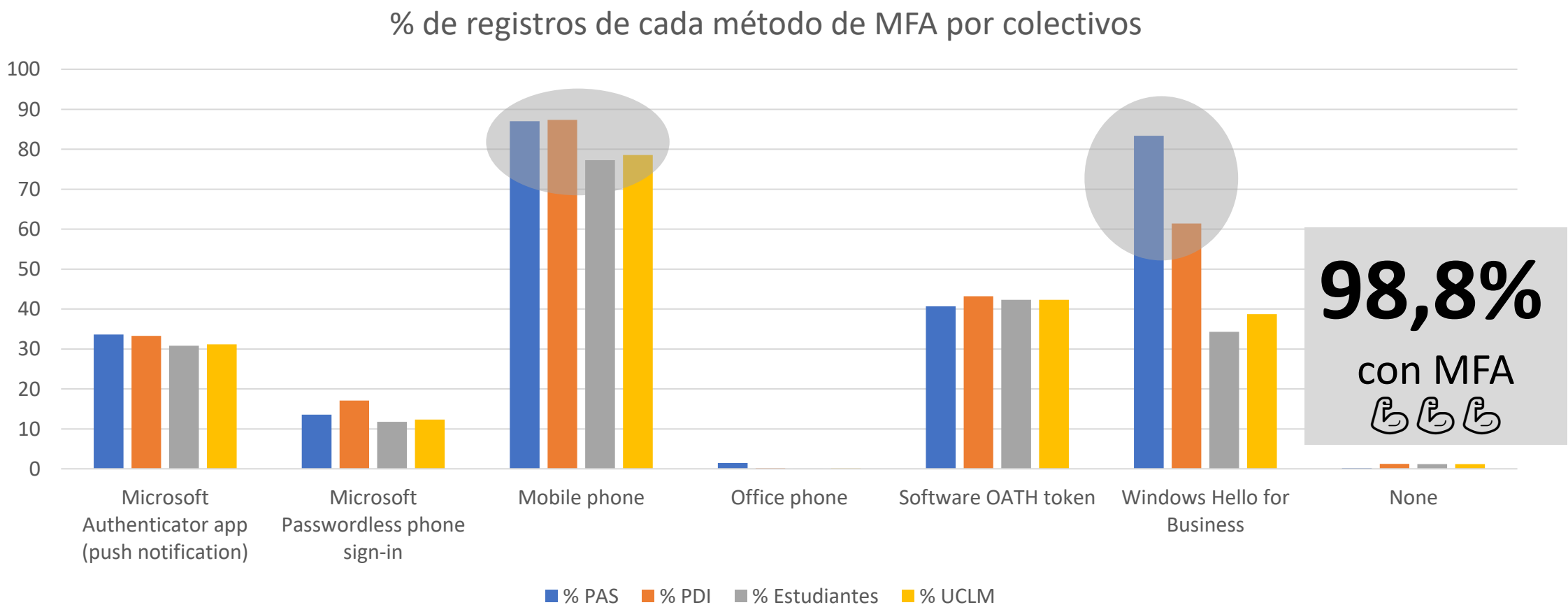
El usuario es el nexo entre factores





¿MFA en vuestras organizaciones?

Grado de implantación en la UCLM



PAS (1.670) + PDI (3.213) + Estudiantes (33.157) = 38.040

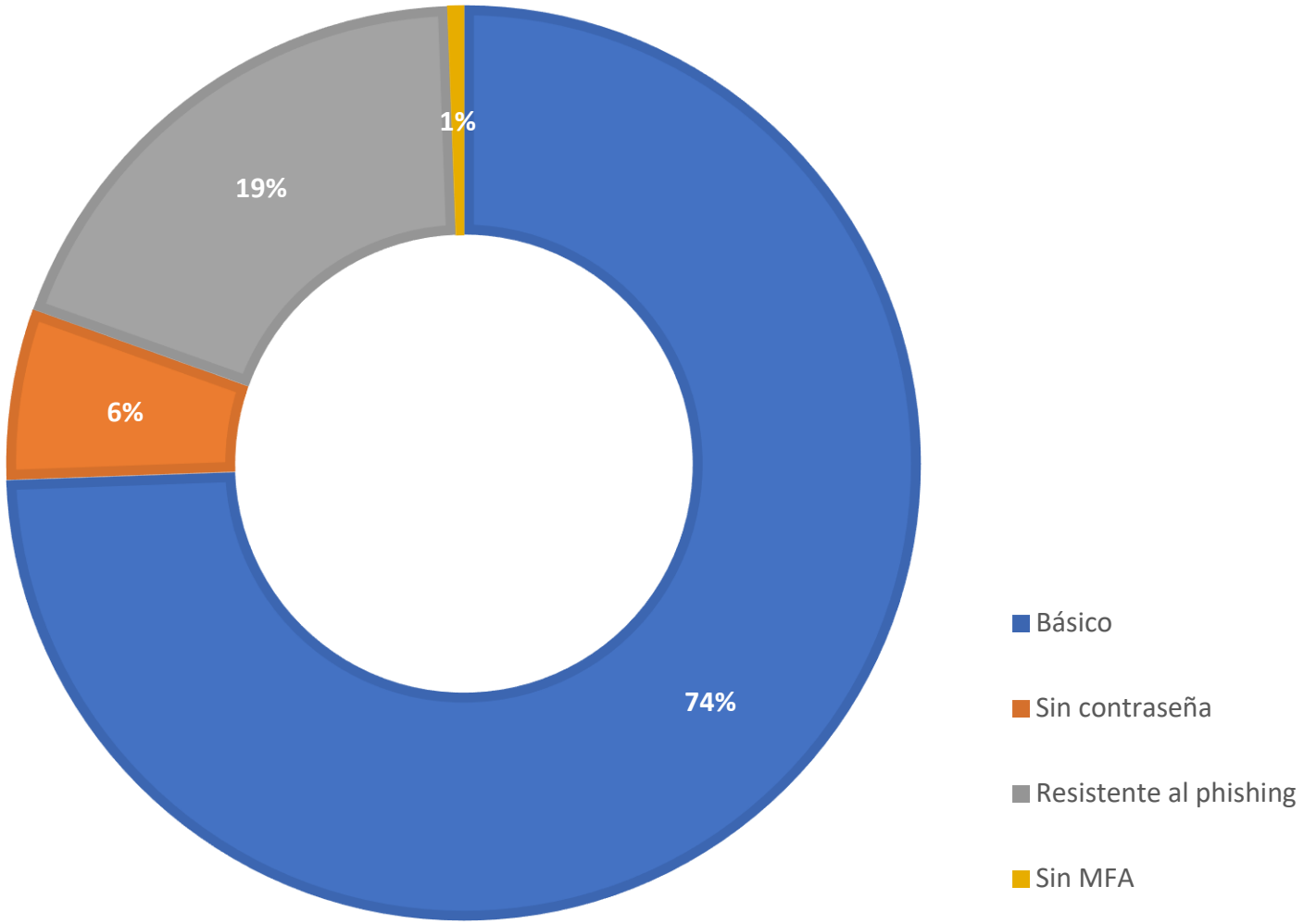
Calidad de los métodos de MFA registrados

25%

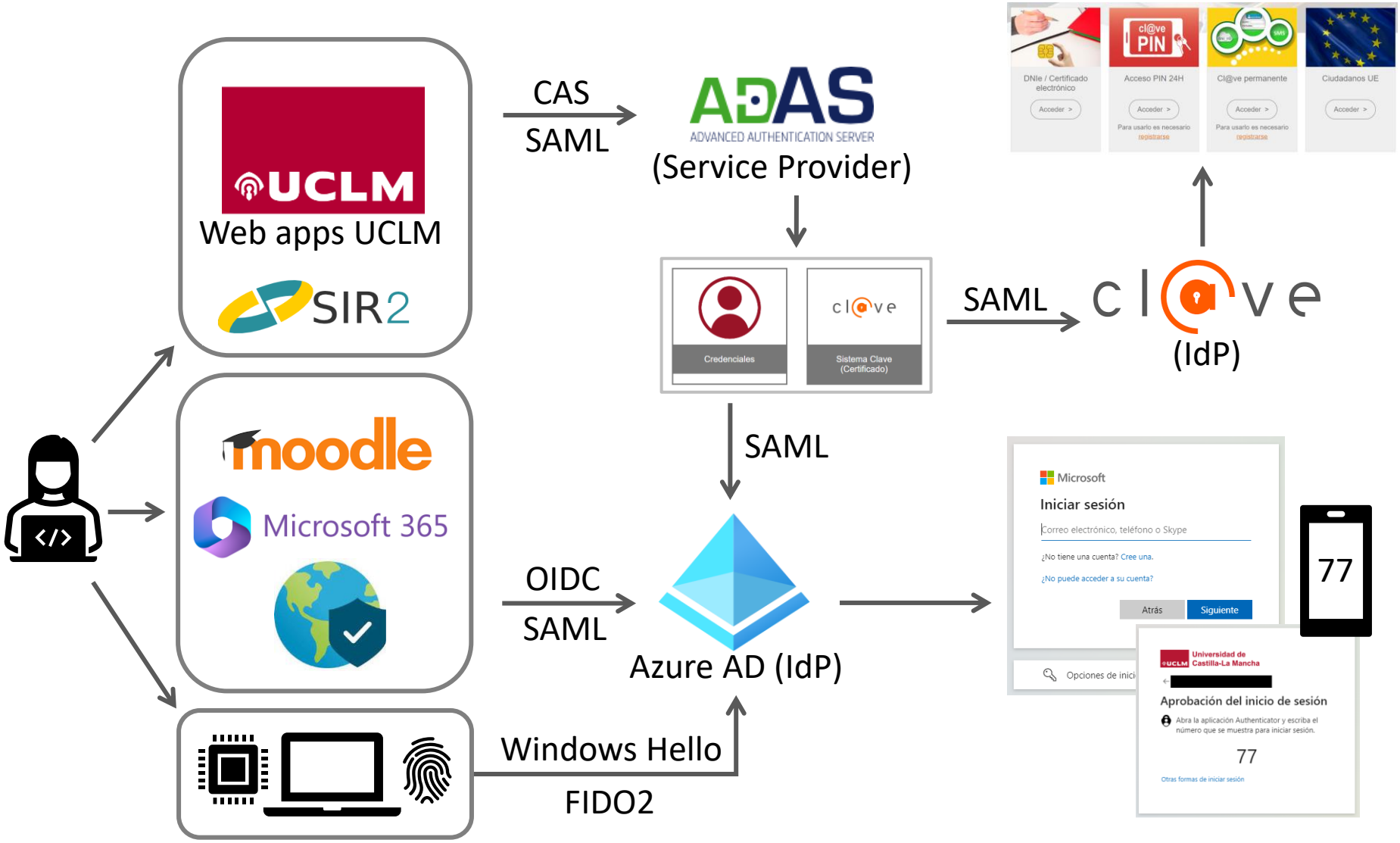
de métodos sin contraseña (👍 usabilidad)

2

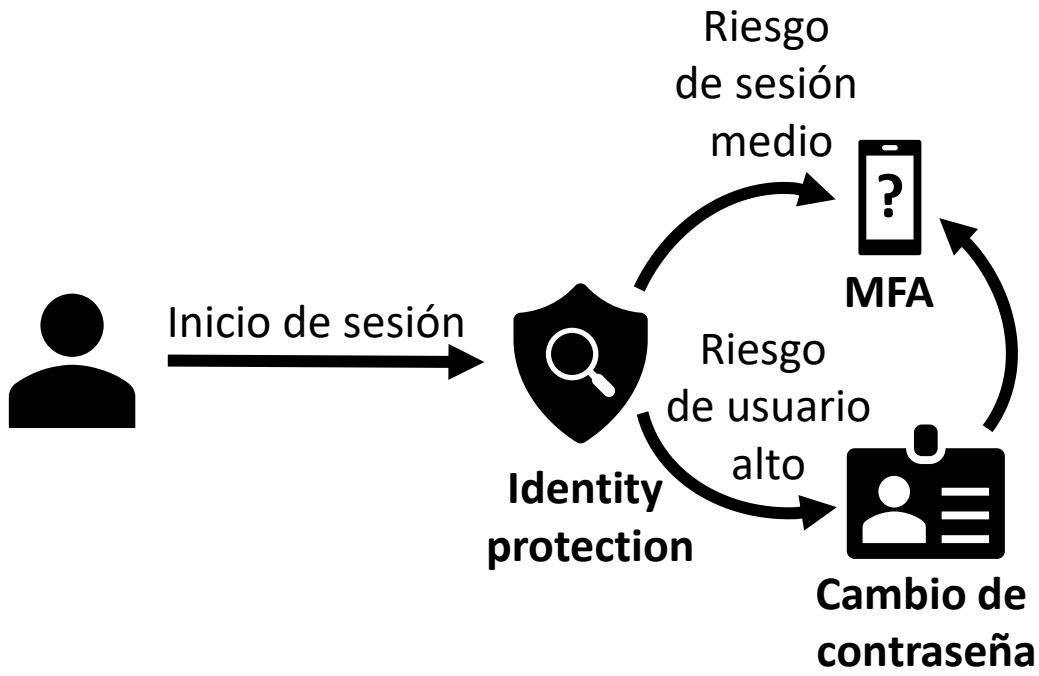
media de métodos de MFA registrados por usuario (👍 redundancia)



¿Cómo lo hemos implementado?



Mitigación de riesgos gracias al MFA

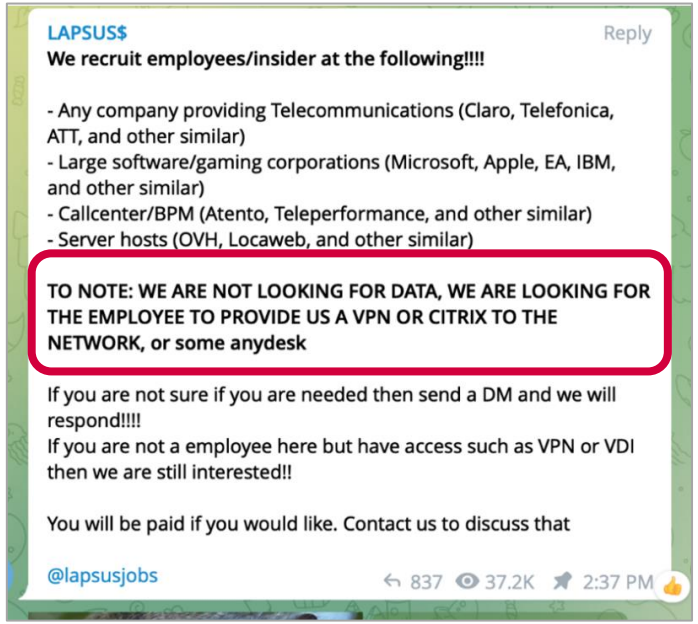


¿Es suficiente MFA para proteger la identidad?

Over 10,000 Organizations Targeted in AiTM Phishing Campaign That Circumvents MFA

Microsoft discovered an AiTM phishing campaign that involved attackers bypassing multi-factor authentication safeguards.

Sumeet Wadhwani Asst. Editor, Spiceworks Ziff Davis July 14, 2022



LAPSUS$ Reply

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs 837 37.2K 2:37 PM

ars TECHNICA

THE HITS KEEP COMING —

LastPass says employee's home computer was hacked and corporate vault taken

Already smarting from a breach that stole customer vaults, LastPass has more bad news.

DAN GOODIN - 2/28/2023, 2:01 AM

Recuerda: el atacante no quiere tus credenciales, quiere tus privilegios

Fuentes: spiceworks.com, 14/07/2022, Ars Technica (2023), Krebs on Security (2022)

Entonces… ¿Cómo podríamos ayudar a Elvira?

Asegurándonos de que el sistema de acceso es tan cómodo que no tiene que buscar atajos que comprometan su seguridad

Verificando la conformidad de su equipo antes de concederle acceso a recursos críticos

Exigiéndole métodos de MFA resistentes al *phishing* para acceder a recursos críticos

No todos los métodos de MFA son igual de buenos, pero cualquiera es mucho mejor que ninguno

Referencias

- All your creds are belong to us! - Microsoft Community Hub
- Phishing-Resistant MFA Does Not Mean Un-Phishable (linkedin.com)
- From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud | Microsoft Security Blog
- LastPass says employee's home computer was hacked and corporate vault taken | Ars Technica
- A Closer Look at the LAPSUS$ Data Extortion Group – Krebs on Security
- NIST SP 800-63 Digital Identity Guidelines
- Cómo alcanzar el nivel 3 de garantía del autenticador (AAL3) de NIST con Azure Active Directory - Microsoft Entra | Microsoft Learn