QuantPaths

El futuro de la ciberseguridad

COMUNICACIONES POST CUÁNTICAS, GLOBALES Y
ULTRA-SEGURAS, EN UN ÚNICO LUGAR

EL PROBLEMA CON DISPOSITIVOS NO CIFRADOS

Su información es vulnerable a

DIFERENCIAS ENTRE SISTEMAS

Computación Binaria

✓ La unidad básica es el bit. Un bit sólo puede tener un valor al mismo tiempo: 1 o 0.

✓ Las computadoras clásicas tienen componentes como CPU, memoria RAM y pantalla.

✓ La programación binaria es adecuada para tareas cotidianas y complejas en diversos ámbitos como el científico y empresarial.

Computación Cuántica

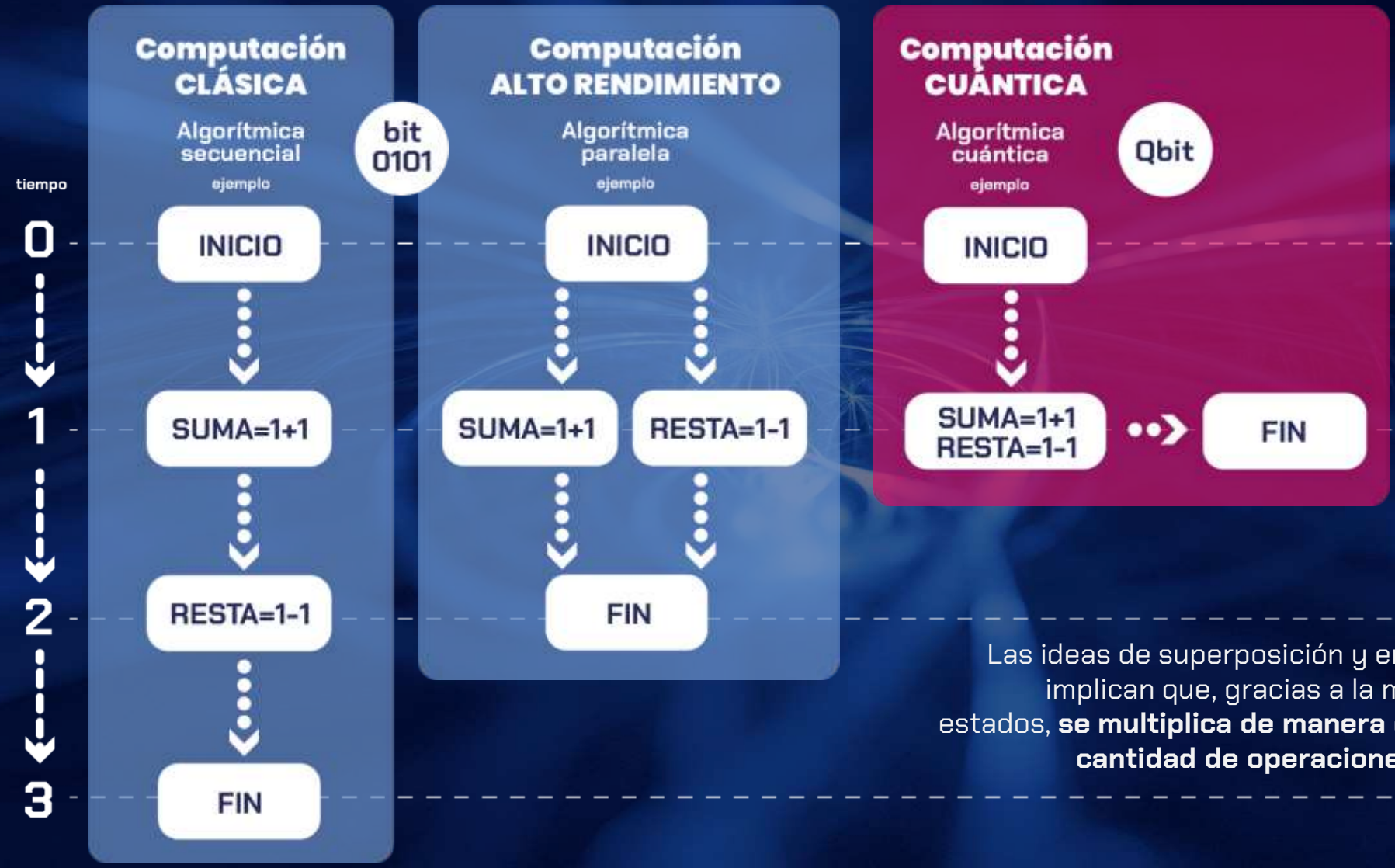
✓ La unidad de referencia es el cuanto.
Se expresa en cúbits.

✓ Una computadora cuántica es un cubículo sellado con una estructura metálica y un entramado de cables, operado desde ordenadores convencionales externos.

✓ Está **diseñada para operaciones de gran envergadura y complejidad**, como ciberseguridad y el big data.

✓ Es extremadamente sensible a las condiciones ambientales, requiere temperaturas cercanas a -273 °C y aislamiento del campo magnético terrestre para funcionar correctamente.

DIFERENCIAS ENTRE SISTEMAS



Las ideas de superposición y entrelazamiento implican que, gracias a la multiplicidad de estados, **se multiplica de manera exponencial la cantidad de operaciones simultáneas realizables.**

IMPLICACIONES DE LA

Computación Cuántica

La computación cuántica ofrece oportunidades económicas y científicas significativas.

Sin embargo, también acelera la aparición de nuevos riesgos de seguridad, especialmente la posibilidad de romper la encriptación de clave pública, esencial para la seguridad del sector financiero y las comunicaciones gubernamentales.

La consecuencia de no estar preparado para la tecnología cuántica es dejar expuesto sus secretos.

OPORTUNIDADES Y RIESGOS DE LA

Computación Cuántica

40% de las organizaciones están tomando medidas proactivas para comprender las amenazas cuánticas*.

Evaluación del riesgo cuántico

El 40% de las organizaciones han comenzado a tomar medidas.

Vigilancia ante amenazas

Muchas organizaciones están vigilantes ante amenazas como "Cosechar Ahora, Desencriptar Después".

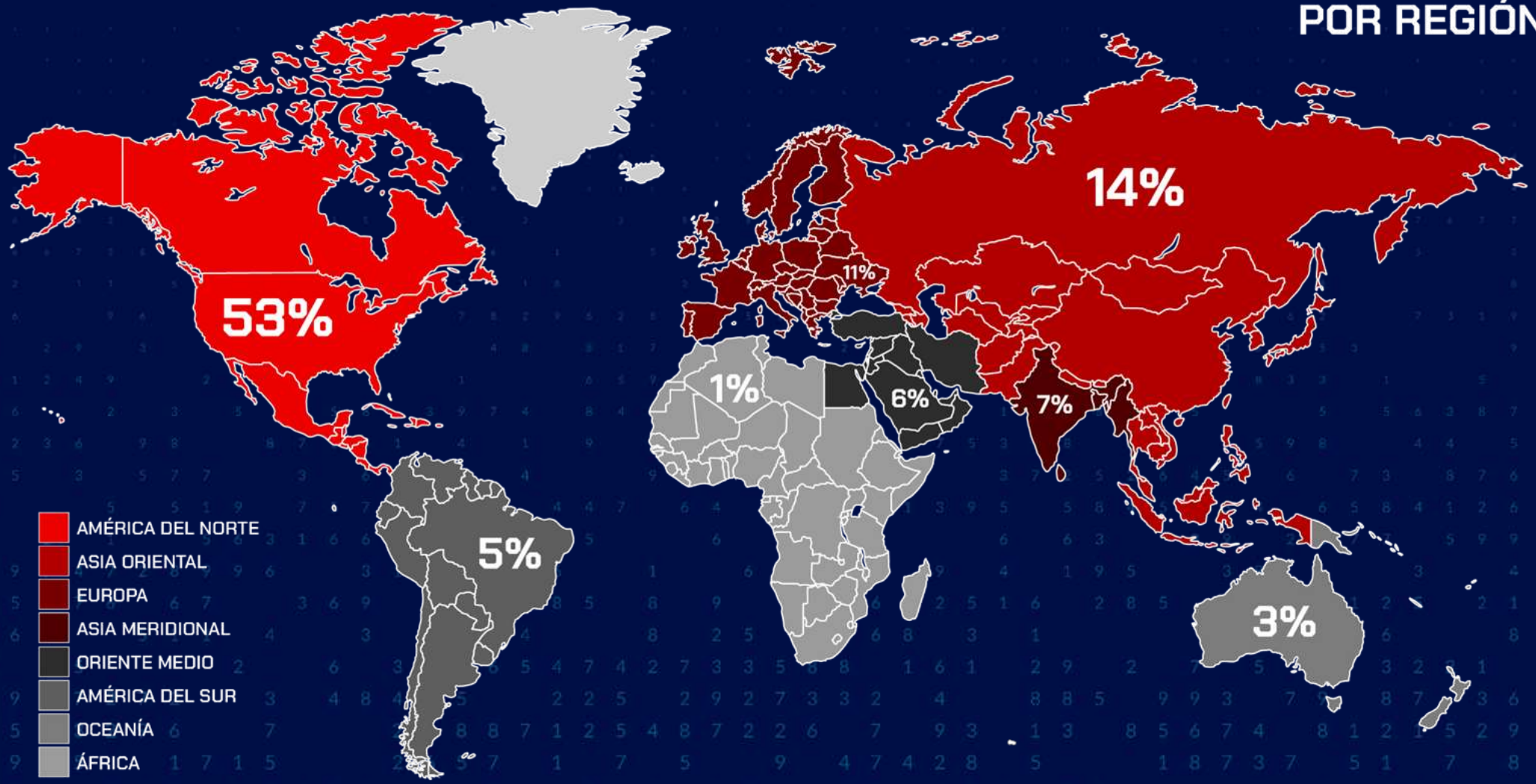
Recomendaciones y estándares

Se han realizado múltiples esfuerzos para impulsar la acción, incluyendo recomendaciones del Grupo de Expertos en Ciberseguridad del G7 y la publicación de estándares de algoritmos de criptografía post-cuántica por el NIST.

*Fuente: Global Cybersecurity Outlook 2025, WEF & Accenture

ESTADO DEL ARTE EN CIBERSEGURIDAD 2025

INTRUSIONES INTERACTIVAS POR REGIÓN



Fuente: Repositorio Europeo de Accidentes Cibernéticos

ESTADO DEL ARTE EN CIBERSEGURIDAD 2025

Presente y futuro de la computación cuántica

Todas las grandes empresas tecnológicas están involucradas en el desarrollo de esta tecnología, como **IBM** o **Google**, hasta el punto de prototipar "modelos de sobremesa".

Pero el mundo 'real' aún queda muy lejano, pues los prototipos son muy primarios y los inconvenientes de su sensibilidad a las condiciones ambientales reducen mucho su aplicación práctica.

Aunque parece claro que la aplicación de la computación cuántica quedará circunscrita a ámbitos muy específicos de nuestro mundo que, por su complejidad, necesitan de equipos informáticos súper potentes, se postula como una **poderosa aliada en ciberseguridad**, como demuestran algunos desarrollos de encriptación de datos, como el **Quantum Key Distribution (QKD)**.

RETOS A RESOLVER

Baja seguridad de datos

✓ Los métodos de cifrado son cada vez **más vulnerables.**

✓ Sólo hay una forma de estar seguro en la era **post cuántica.**

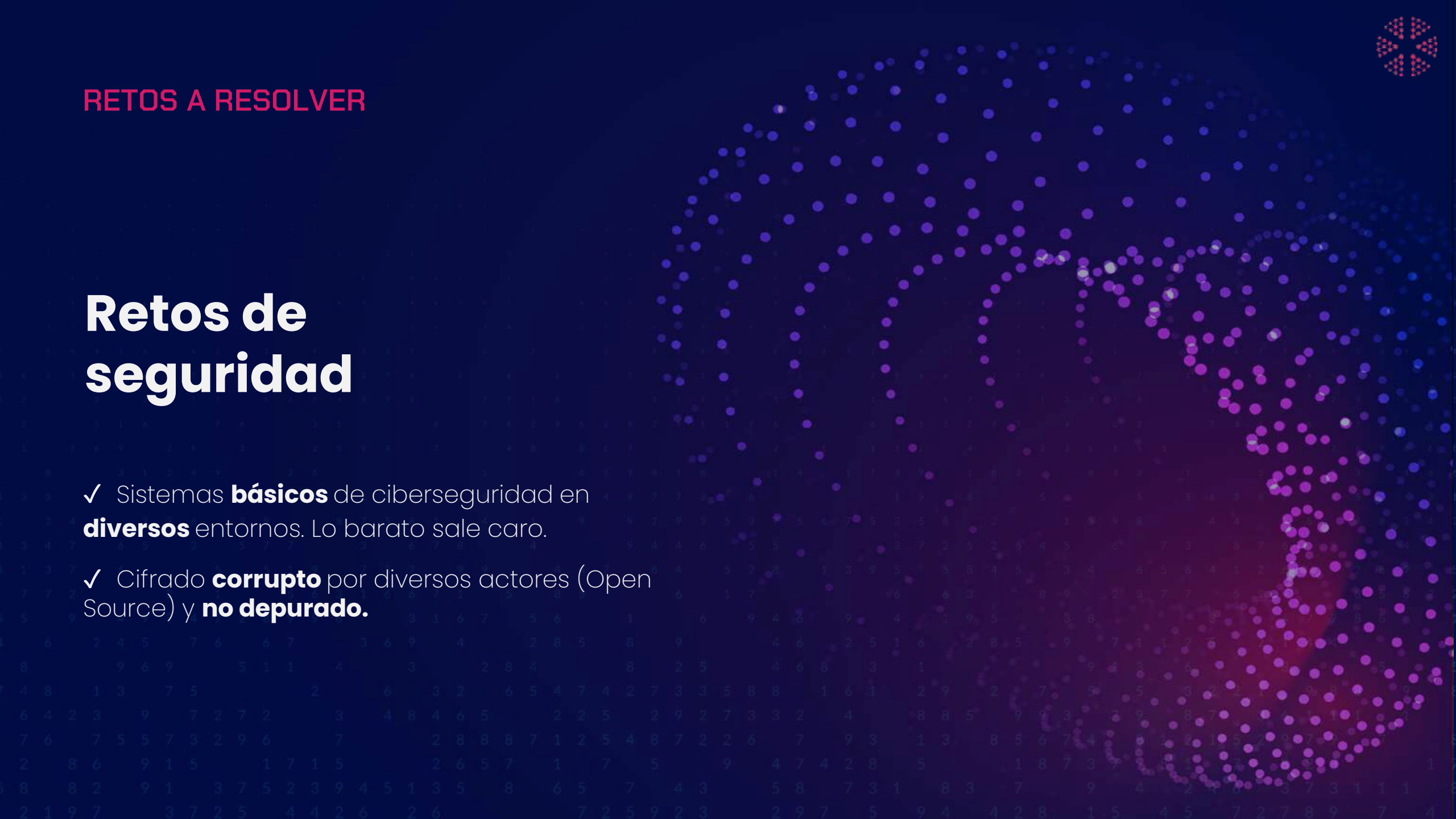
✓ La oferta actual está en sus **primeras fases.**

RETOS A RESOLVER

Retos de seguridad

✓ Sistemas **básicos** de ciberseguridad en **diversos** entornos. Lo barato sale caro.

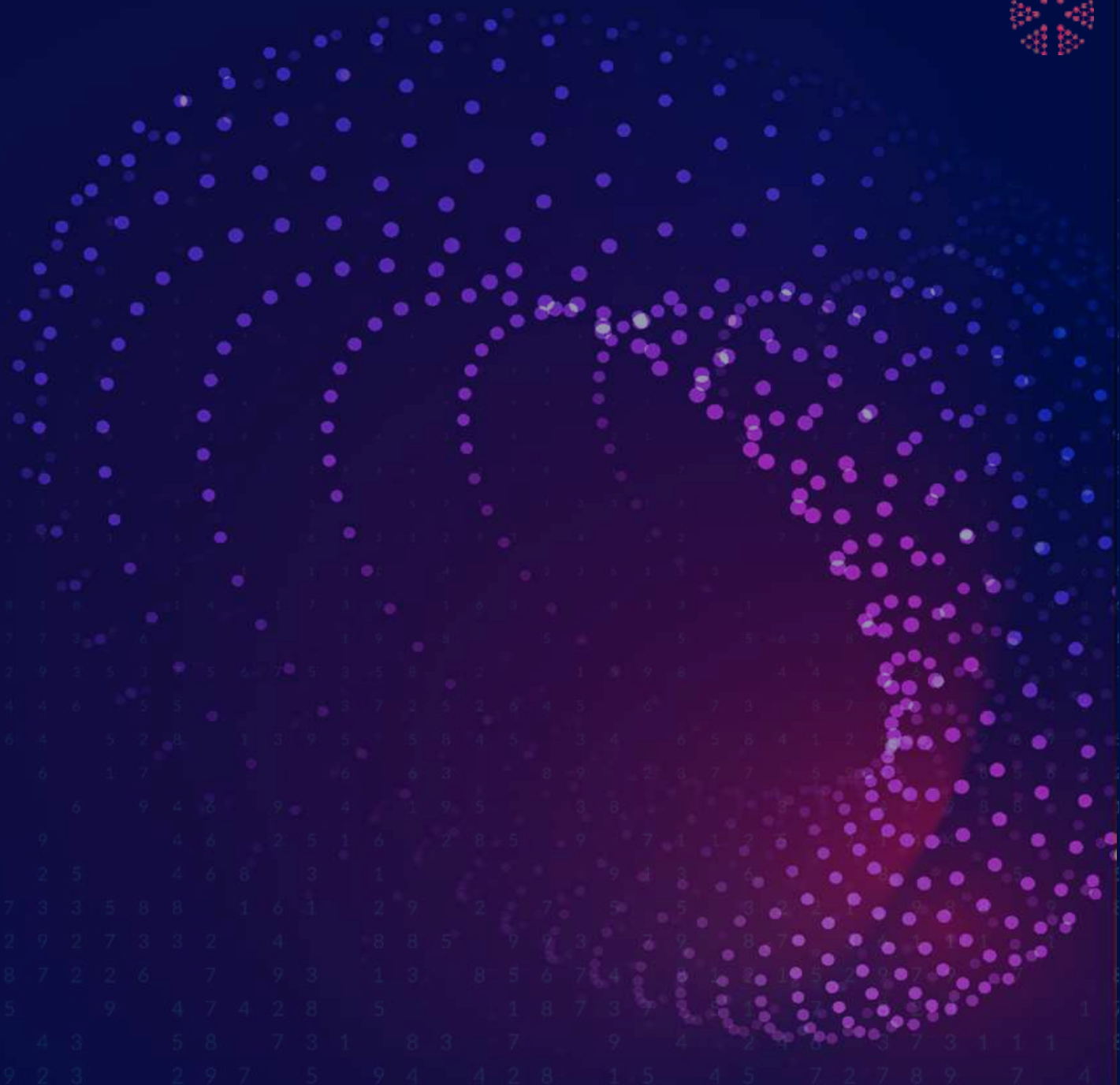
✓ Cifrado **corrupto** por diversos actores (Open Source) y **no depurado.**



RETOS A RESOLVER

Carencia de ofertas fiables

- ✓ Oferta **reducidas** de sistemas y dispositivos.
- ✓ Falta de apoyo y servicios **consultativos.**
- ✓ Opciones **limitadas** de aplicaciones de ciberseguridad certificadas.



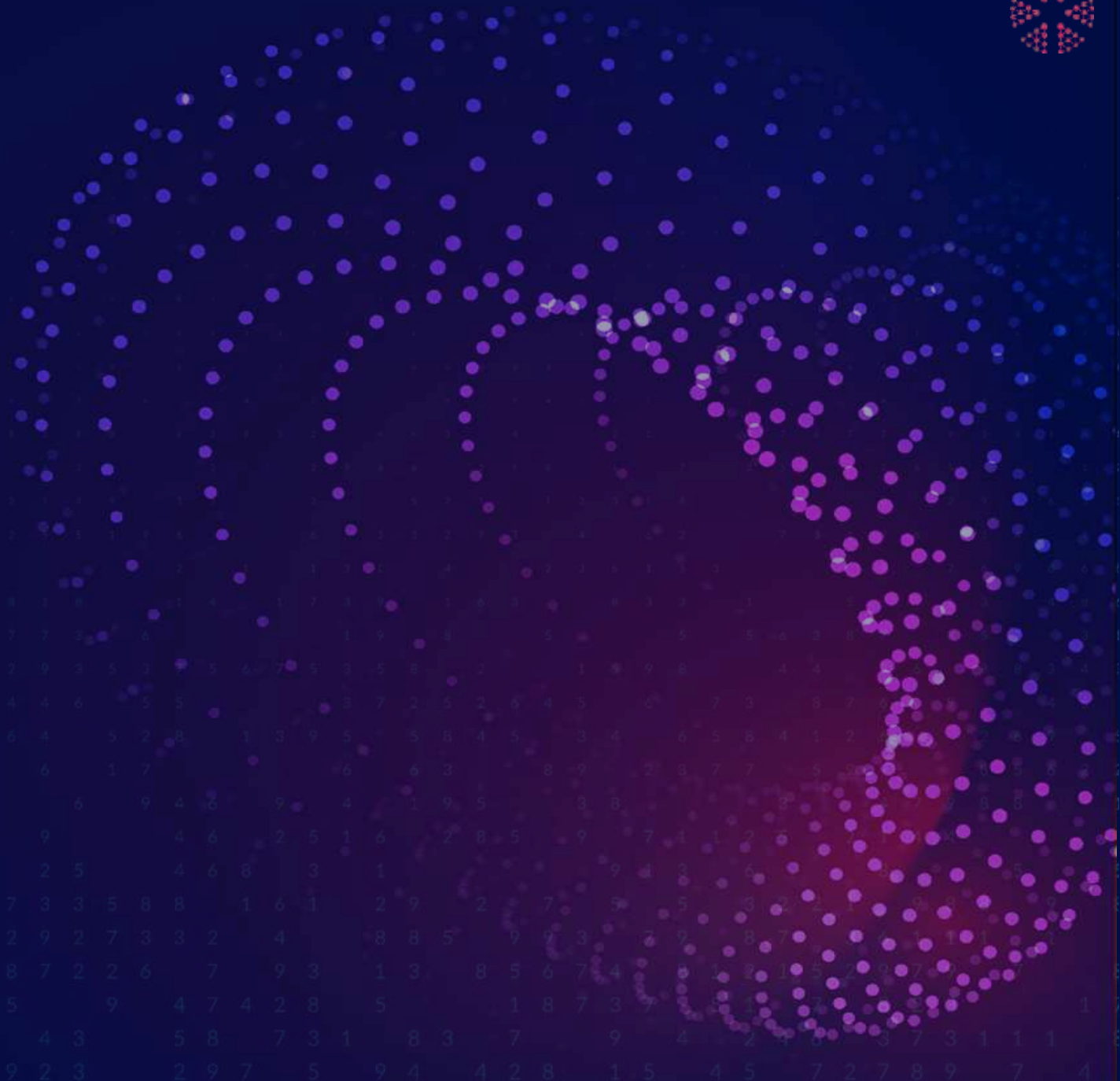
RETOS A RESOLVER

Vulnerabilidad del sistema

La **ciber resiliencia** es cada vez más difícil de mantener debido:

✓ La creciente sofisticación de los ataques

✓ La falta de recursos y capacidades para implementar medidas de seguridad efectivas.



QUIÉNES SOMOS

QuantPaths

La organización de Ciberseguridad que consulta, desarrolla y ofrece soluciones para implementar seguridad de datos bajo cifrado con protección post cuántica.

Dispositivos

Compatibles con la licencia de MSQuantum (mensajería cifrada) que incluye el teléfono.

Aplicaciones

Para mejorar la seguridad de comunicación como correo cifrado, almacenamiento encriptado.

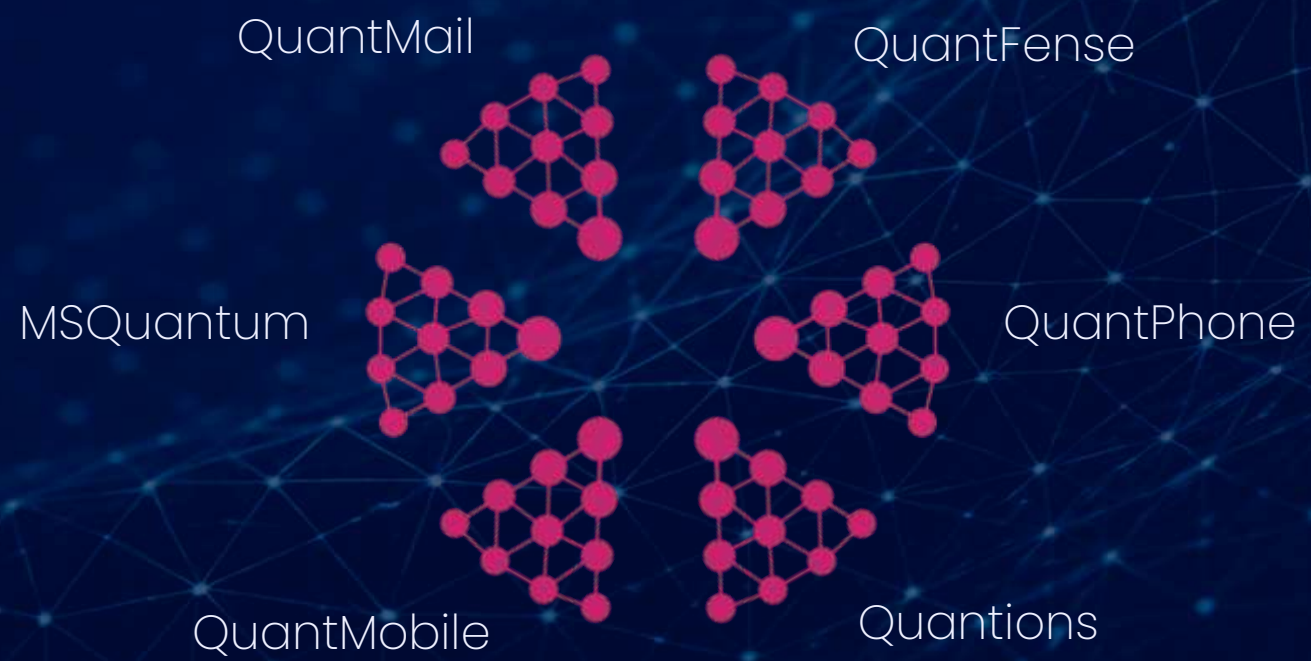
Entorno IT

Consultoría en mejores prácticas de seguridad e implementación de productos de encriptación post cuántica, realizando todo de manera global con tu departamento IT.

NUESTRA GAMA DE

Soluciones

Nuestra cartera incluye consultoría de ciberseguridad, habilitación de algoritmos basados en IA y desarrollo de productos con seguridad post cuántica.



VENTAJAS DE

Nuestra oferta

Nuestro enfoque se basa en capas de seguridad que permiten:

- Control de todos los datos exclusivo para el usuario
- Sin riesgo de accesos no autorizados
- Equipo técnico especializado y soporte directo al cliente.

NUESTRO

Producto

Un dispositivo sin igual, certificado por:

BlackBerry

Cifrado con **infraestructura post cuántica** que protege las comunicaciones móviles, con cobertura global.

- ✓ Sin competencia actual en materia de certificaciones
- ✓ Interfaz intuitiva y sencilla
- ✓ Infraestructura bajo red post cuántica certificada
- ✓ Comunicación con apps cifradas sin riesgo de ataques cibernéticos

NUESTROS ALIADOS EN

Academia

DE MONTFORT UNIVERSITY LEICESTER

Gracias en nombre de

QuantPaths

¿Le interesa una demo?
Escríbanos:

info@quantpaths.com

Teléfono:
+57 321 225 00 10

www.quantpaths.com

Acceda a la presentación