INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER

Criptografía Poscuántica

https://is3coalition.org/

Youth LACIGF 2025

11 de octubre de 2025

João Moreno Rodrigues Falcão

Sobre IS3C

- Despliegue de estándares de Internet
- Cuatro informes y dos guías prácticas
- Cinco grupos de trabajo activos

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER

Sobre mí

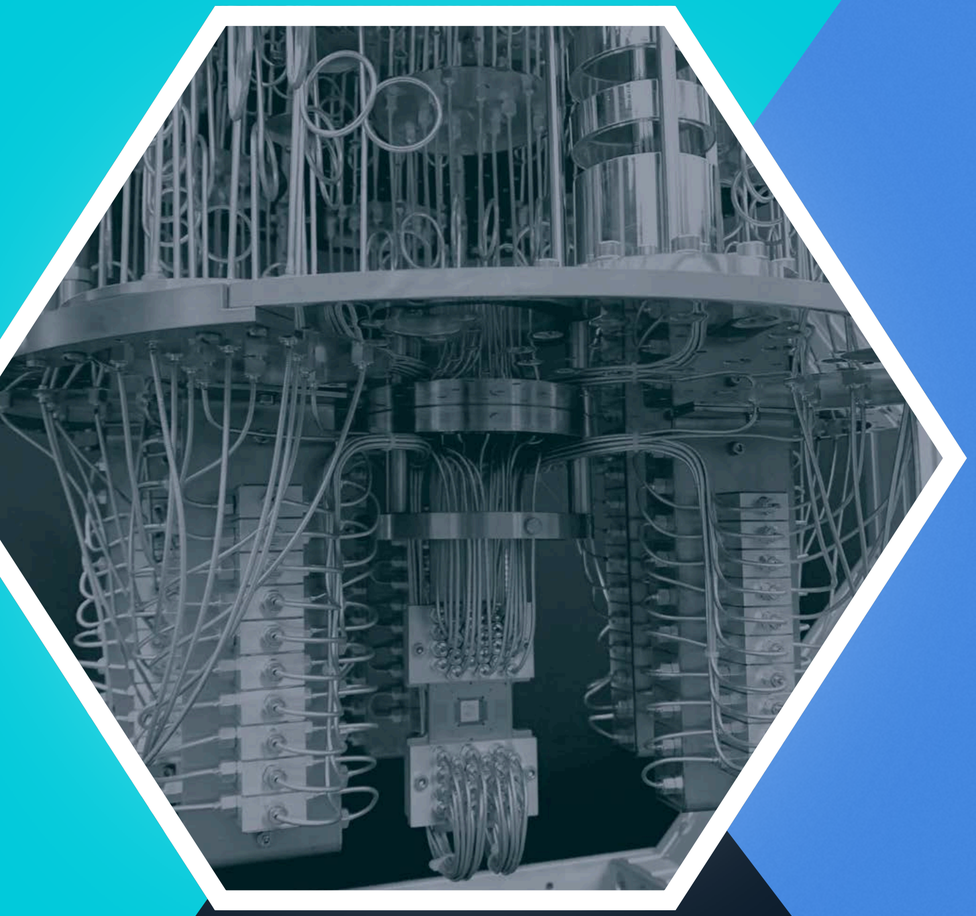
João Moreno Rodrigues Falcão

- Ingeniero eléctrico
- Investigador en criptografía
- Profesional de ciberseguridad
- Consultor en políticas públicas
- Participante del comité del YouthLACIGF 2025, 2024, 2023 y 2022

LinkedIn

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER



Agenda

- Políticas públicas en ciberseguridad
- Criptografía poscuántica
- Computación cuántica y nuestro objectivo
- Proximos pasos

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER

Políticas públicas en ciberseguridad

2024

El problema

Presentación de los riesgos y oportunidades

2025

Investigación

Como el mundo esta trabajando eso

2026

Involucramento

Buscar personas clave para contruir estratégias

2027

Atuación

Actuar en los foros necesários

¿Qué es criptografía poscuántica?

Criptografía y problemas matemáticos

La criptografía se basa en problemas matemáticos: si son demasiado complejos para los ordenadores actuales, seguimos seguros.

Factorización y logaritmo discreto

La criptografía asimétrica que sustenta la autenticación e integridad actuales depende de estos dos problemas.

El computador cuántico

Aprovechando la superposición cuántica, un computador cuántico potente puede resolver estos problemas con facilidad.

Criptografía poscuántica - PQC

Son protocolos que usan otros problemas matemáticos para garantizar la seguridad en el futuro.

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER

¿Internet Segura?

- **RSA y ECC: llaves públicas**

  Serán vulnerables ante computadoras cuánticas de gran escala.

- **Autenticación y integridad**

  Dependen en gran medida de protocolos inseguros frente a la computación cuántica, su seguridad se derrumba.

- **Es necesario una transición**

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER

Recomendaciones de nuestra investigación

Preparación

- Inventario criptográfico
- Apoyo regulatorio
- Coordinación global

Transición

- Sistemas híbridos compatibles
- Migración por fases
- Garantizar la interoperabilidad

Retos futuros

- Costos operativos
- Interoperabilidad
- Brecha cuántica
- Impacto ambiental
- Tiempo limitado

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER

Colaboración

- Definición de algoritmos
- Creación de programas pilotos
- Acción conjunta entre registros, operadores, gobiernos y academia

Únete a IS3C

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)

MAKING THE INTERNET MORE SECURE AND SAFER

ICANN LAC DNS FORUM

¡GRACIAS!

João Moreno Rodrigues Falcão

Visitanos
https://is3coalition.org/

Nuestros reportes