MADRID | 4 DE JUNIO DE 2026

AWS SUMMIT

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.



DEV307

Criptografía Post-Cuántica en AWS: protegiendo datos contra ataques futuros

Robert Garcia Ventura

Data Architect
Keepler Data Tech

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Robert Garcia Ventura

DATA ARCHITECT + AWS COMMUNITY BUILDER

AWS community builder

- Data Architect en Keepler Part of Accenture
- AWS Subject Matter Expert
- 7x AWS certificaciones
- Trabajando con AWS desde 2018
- 7 años como AWS Community Builder



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.





“Entre el millón de sitios web principales, solo el 8,6% soporta mecanismos de intercambio de claves PQC híbridos.”

F5 Labs

2025 The State of Post-Quantum Cryptography (PQC) on the Web

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- Evolución de la computación cuántica
- Criptografía actual y sus riesgos
- Harvest Now Decrypt Later
- Estandarización de la criptografía post-cuántica
- Plan de migración de AWS hacia criptografía post-cuántica (PQC)

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Computación cuántica

la próxima gran revolución

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Evolución de la computación cuántica

1981

Richard Feynman propone la computación cuántica

1985

David Deutsh define la computadora cuántica universal

1994

Peter Shor crea el **algoritmo de Shor** (factorización de números)

1998

Primer ordenador cuántico funcional de **2 qubits**

2001

IBM & Stanford primera ejecución del **algoritmo Shor's** con el número 15 con **7 qubits**

2011

D-Wave Systems primer ordenador recocido cuántico comercial con **128 qubits**

2019

Google alcanza la **"Supremacía cuántica" con 53 qubits (Sycamore)**

Amazon Braket

2023

IBM Condor alcanza los **1121 qubits**

aws

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ordenadores cuánticos de terceros

AQT

IONQ

IQM

QuEra
Putting Quantum to Work

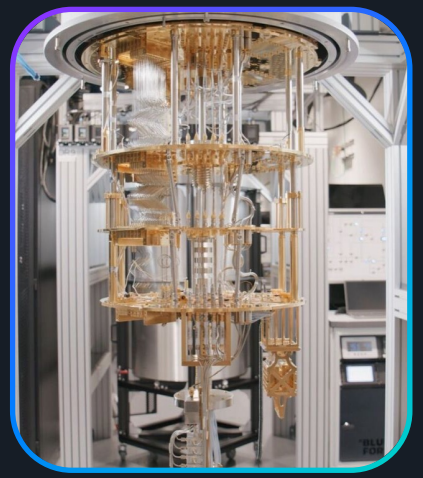
rigetti

Modo de reserva:
2,5k $ - 7k $ / hora

Amazon Braket

Futuros ordenadores cuánticos de AWS

aws



AWS Ocelot Quantum Chip

AWS Center for Quantum Computing

aws

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Criptografia actual

SIMÉTRICA	ASIMÉTRICA	FUNCIONES HASH
Clave única	Clave pública y privada	No reversible
Reversible	Reversible	SHA-256, PBKDF2
AES-128, AES-256	RSA, ECC, Diffie-Hellman	
Algoritmo de Grover	Algoritmo de Shor	

aws

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Harvest now decrypt later

X + **Y** > **Día Q**

¿Cuánto tiempo necesitas que tus datos permanezcan seguros?

¿Cuánto tiempo llevará migrar a criptografía post-cuántica?

¿Cuánto tiempo tardará en desarrollarse un super ordenador cuántico?

aws

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Estandarización de la Criptografía Post-Cuántica

Algoritmos fundamentales

Protocolos y redes

Marcos y normativas











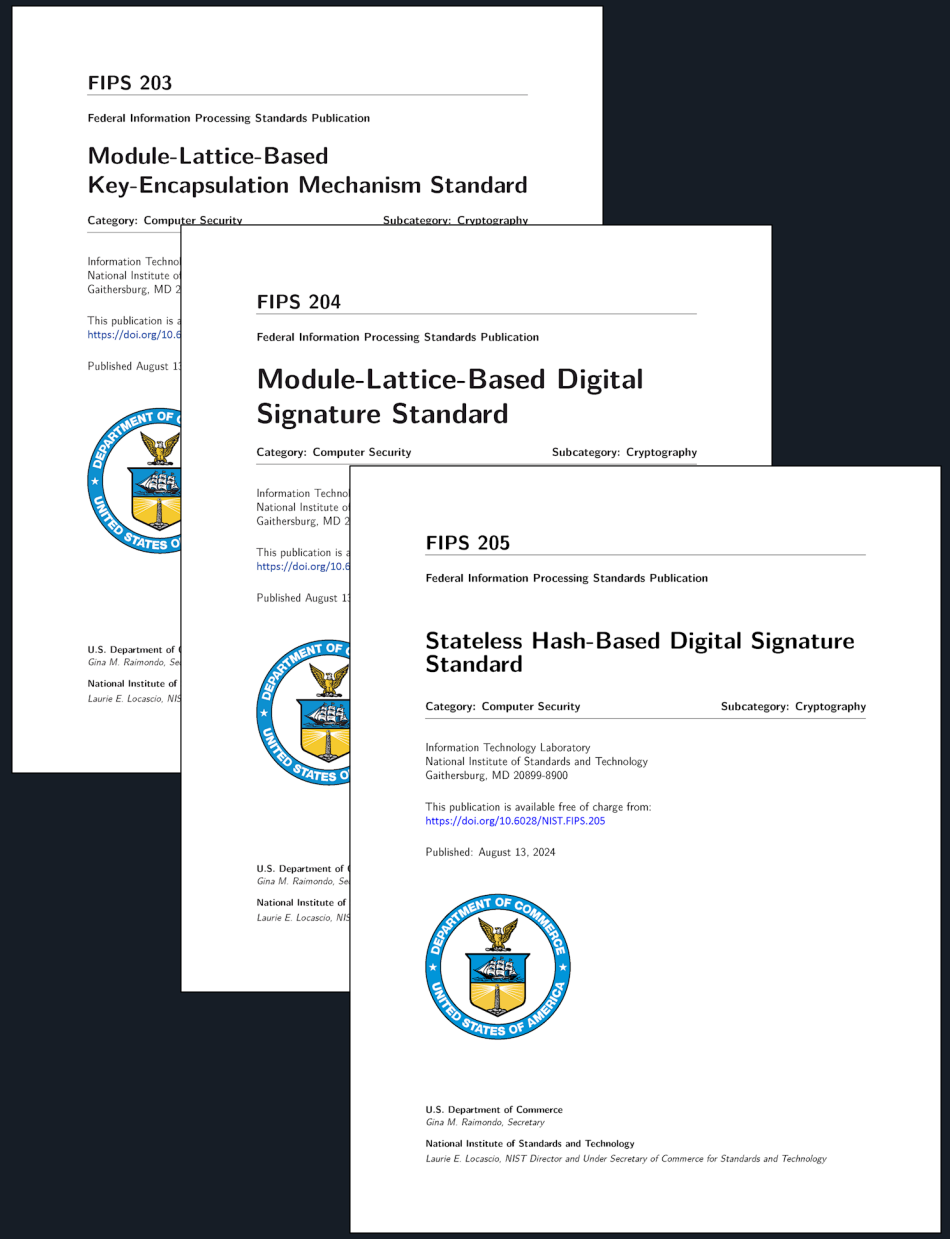


aws

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

- En Agosto de 2024, NIST publica 3 nuevos Federal Information Processing Standards (FIPS) definiendo algoritmos PQC para reemplazar los algoritmos de clave pública utilizados hoy
- Encapsulación de clave (Diffie-Hellman):
  - FIPS 203: ML-KEM (Kyber)
- Firma digital (RSA & ECC):
  - FIPS 204: ML-DSA (Dilithium)
  - FIPS 205: SLH-DSA (SPHINCS+)
- Próximamente:
  - FIPS 206: FN-DSA (FALCON)
  - FIPS 207: HQC-KEM (Hamming Quasi-Cyclic)



© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Librerias open source



OpenSSL

libssl

libcrypto

aws

s2n-tls

AWS-LC

1st FIPS 140-3 validación

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

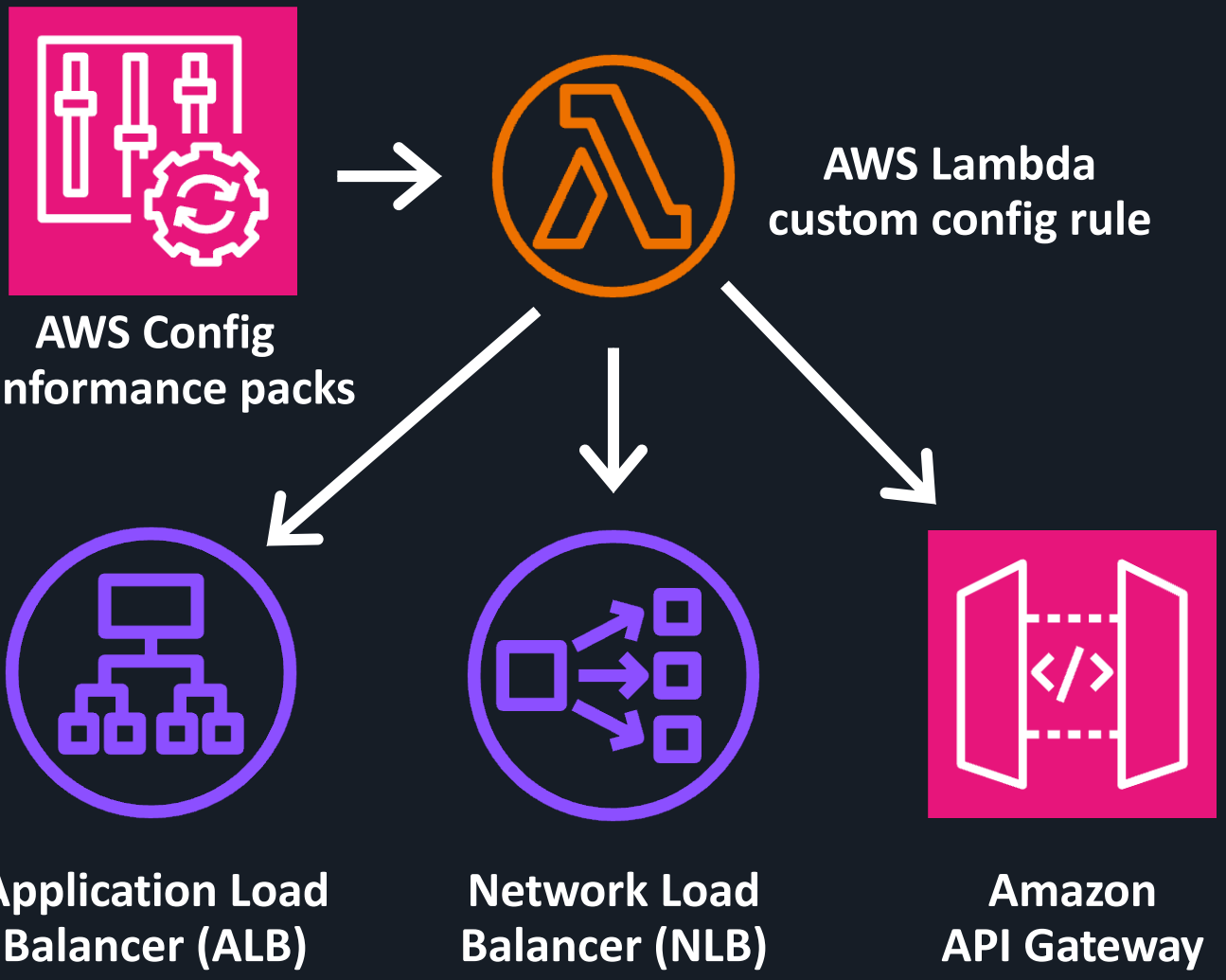
Plan de migración de AWS hacia criptografía post-cuántica (PQC)

Línea de trabajo 1

Inventario y planificación

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

PQC Readiness Scanner





AWS SAM

- Tier 1 — Totalmente preparado para PQC (TLS 1.3 con PQC)
- Tier 2 — Preparado para PQC pero compatible con versiones anteriores (TLS 1.2 + TLS 1.3 con PQC)
- Tier 3 — No preparado para PQC (TLS < 1.3 o sin PQC)

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Plan de migración de AWS hacia criptografía post-cuántica (PQC)

Línea de trabajo 1

Inventario y planificación

Línea de trabajo 2

Protección de datos en tránsito

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Endpoints de servicios de AWS con soporte ML-KEM



AWS Secrets Manager

04/2025



AWS Certificate Manager (ACM)

04/2025



AWS Key Management Service (KMS)

04/2025



AWS Payment Cryptography

11/2025



Amazon Simple Storage Service (S3)

11/2025

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Clientes con soporte PQC

- **Clientes con soporte nativo o configurable**
  - **AWS SDK Go ≥ 1.24 (runtime Go 1.24+)**
  - **Node.js ≥ 22.20 LTS / ≥ 24.9 (OpenSSL 3.5 embebido)**
  - **AWS SDK Rust (publicados después de 29/08/2025)**
- **Clientes dependientes del sistema (OpenSSL ≥ 3.5)**
  - **AWS CLI (depende del OpenSSL del sistema)**
  - **AWS SDK Python (boto3)**
  - **AWS SDK PHP**
  - **AWS SDK .NET (Linux/macOS)**

aws



AWS Certificate Manager (ACM)



AWS Secrets Manager



AWS Key Management Service (KMS)



Amazon Simple Storage Service (S3)

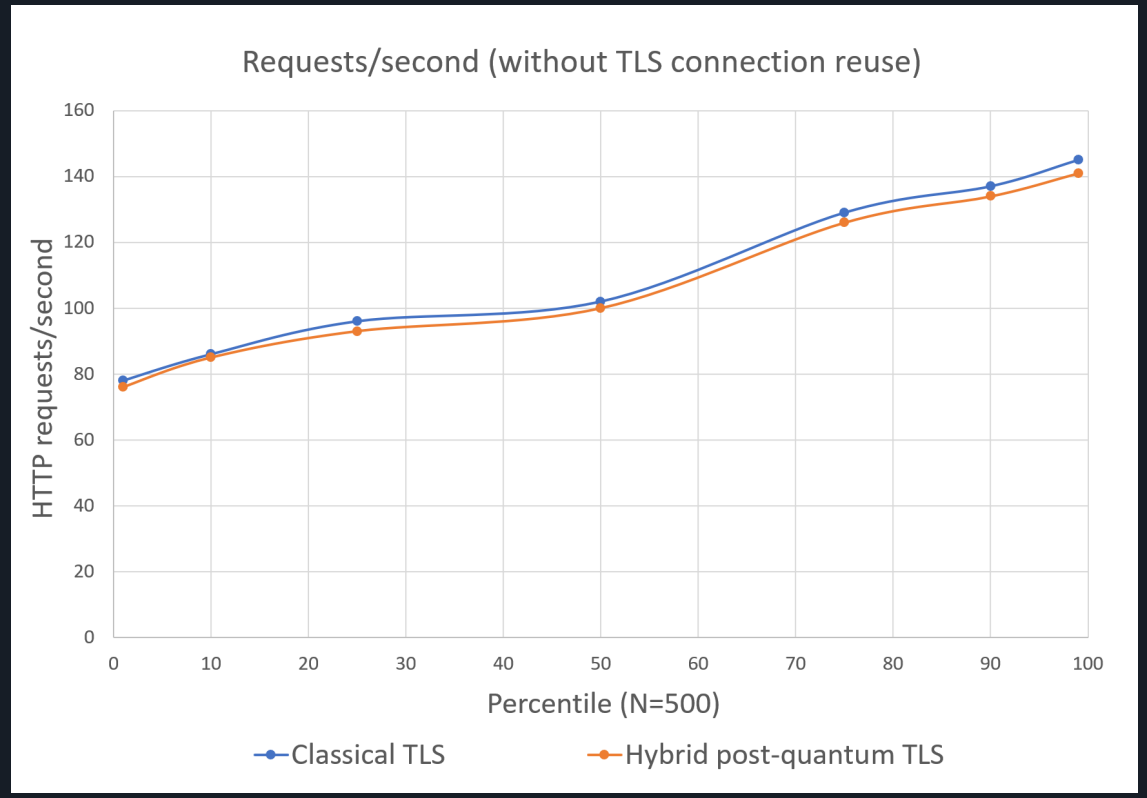


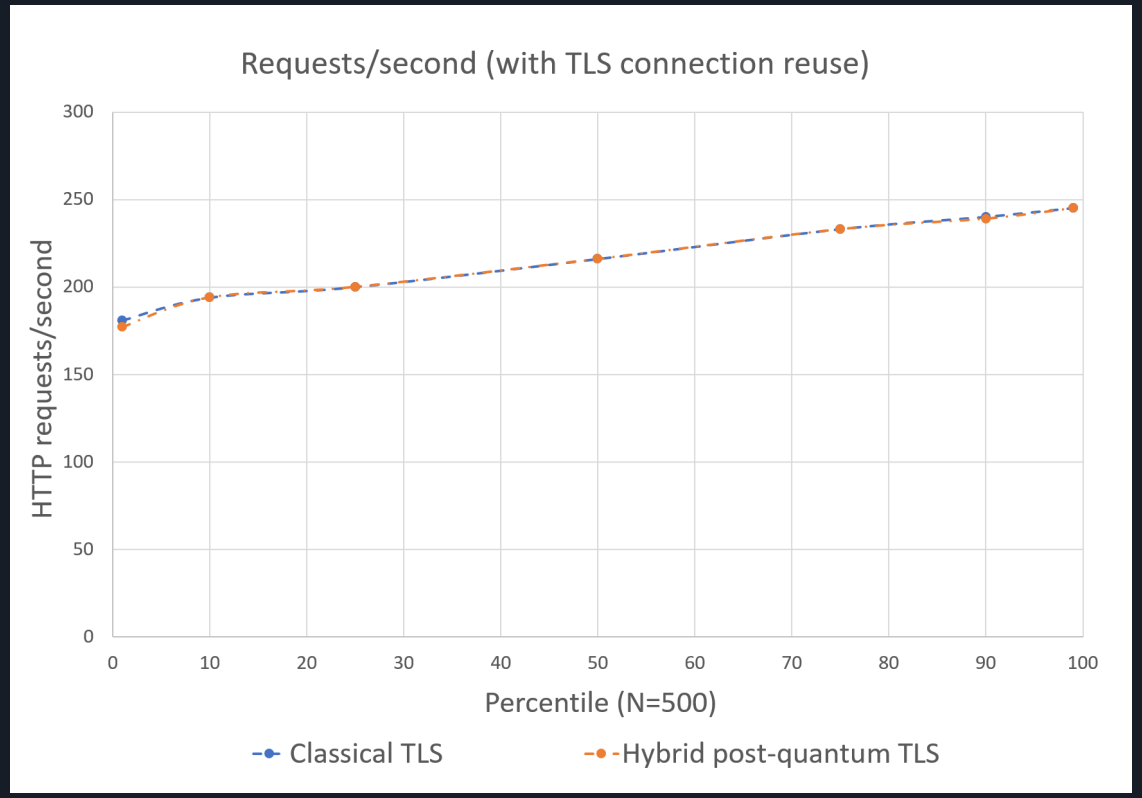
AWS Payment Cryptography

aws

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Rendimiento de TLS clásico vs TLS híbrido





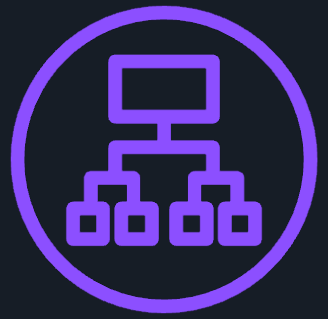
TLS PQC: ~–2.3% TPS
(108.7 TPS a 106.2 TPS)

~ 1600 bytes
80-150 microseg

TLS PQC: ~–0.05% TPS
(216.1 TPS a 216.0 TPS)

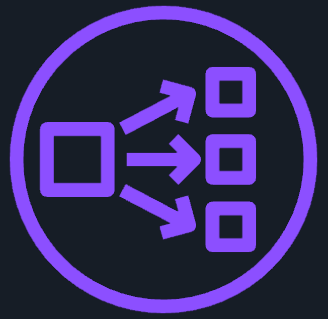
© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Servicios de AWS con soporte ML-KEM opcional



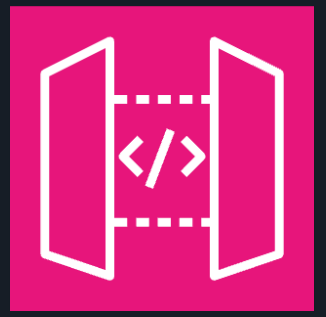
Application Load Balancer (ALB)

11/2025



Network Load Balancer (NLB)

11/2025



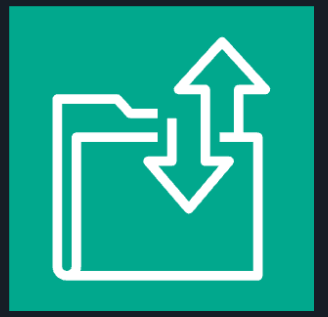
Amazon API Gateway

11/2025



Amazon CloudFront

09/2025



AWS Transfer Family for SFTP

05/2025
06/2023*

aws

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Políticas de seguridad en ALB, NLB y API Gateway

Security policies	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-TLS13-1-3-2021-06	Yes	No	No	No
ELBSecurityPolicy-TLS13-1-3-PQ-2025-09	Yes	No	No	No
ELBSecurityPolicy-TLS13-1-2-2021-06	Yes	Yes	No	No
ELBSecurityPolicy-TLS13-1-2-PQ-2025-09	Yes	Yes	No	No
ELBSecurityPolicy-TLS13-1-2-Res-2021-06	Yes	Yes	No	No
ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09	Yes	Yes	No	No
ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06	Yes	Yes	No	No
ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09	Yes	Yes	No	No
ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06	Yes	Yes	No	No
ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09	Yes	Yes	No	No
ELBSecurityPolicy-TLS13-1-1-2021-06	Yes	Yes	Yes	No
ELBSecurityPolicy-TLS13-1-0-2021-06	Yes	Yes	Yes	Yes
ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	Yes	Yes	Yes	Yes
ELBSecurityPolicy-TLS-1-2-Ext-2018-06	No	Yes	No	No
ELBSecurityPolicy-TLS-1-2-2017-01	No	Yes	No	No
ELBSecurityPolicy-TLS-1-1-2017-01	No	Yes	Yes	No
ELBSecurityPolicy-2016-08	No	Yes	Yes	Yes

Security policy	Supported TLS versions	Supported ciphers
SecurityPolicy_TLS13_1_2_FIPS_PFS_PQ_2025_09	TLS1.3 TLS1.2	**TLS1.3** • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 **TLS1.2** • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384
SecurityPolicy_TLS13_1_2_PFS_PQ_2025_09	TLS1.3 TLS1.2	**TLS1.3** • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 **TLS1.2** • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384
SecurityPolicy_TLS13_1_2_PQ_2025_09	TLS1.3 TLS1.2	**TLS1.3** • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 **TLS1.2** • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

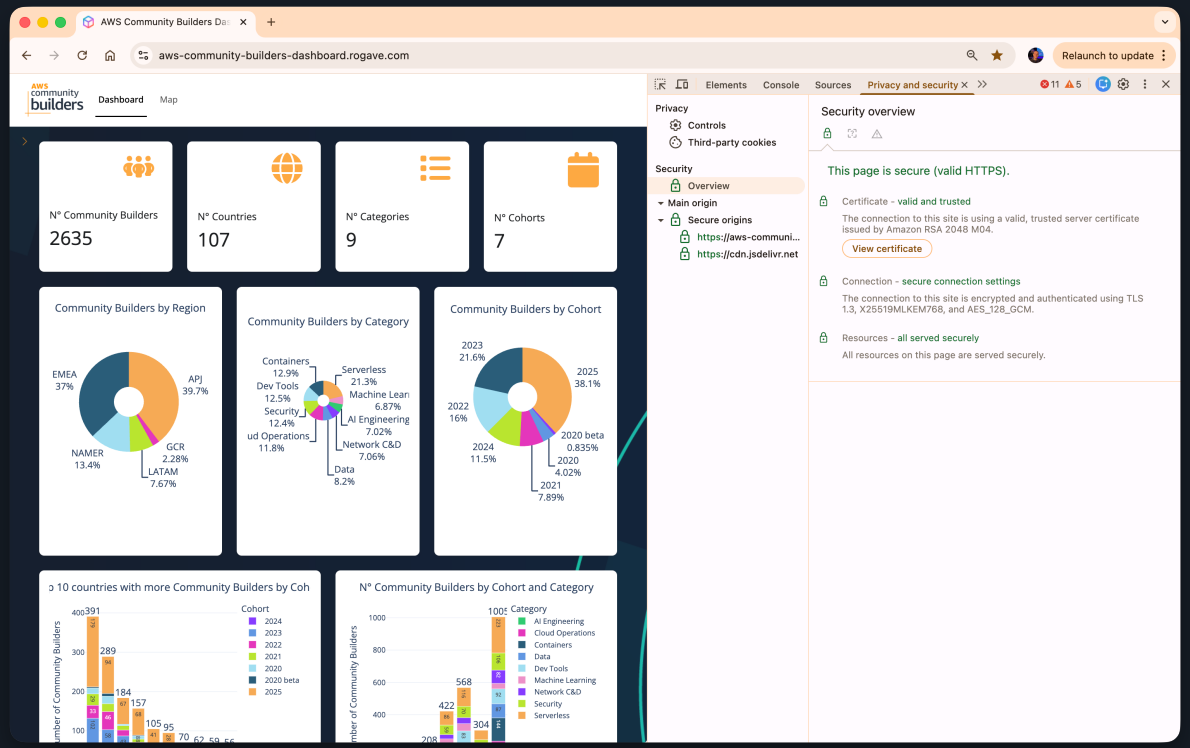
Criptografía híbrida en Amazon CloudFront

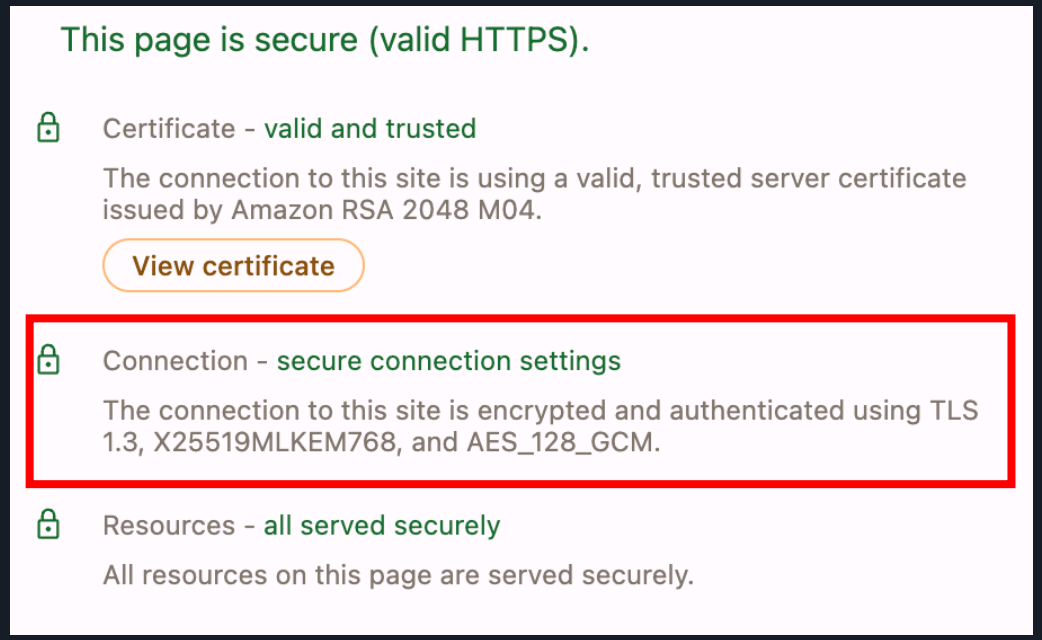


Security policy
TLSv1.2_2021



Security policy
TLSv1.3_2025





Elliptic Curve Diffie-Hellman (ECDH) + ML-KEM

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Plan de migración de AWS hacia criptografía post-cuántica (PQC)

Línea de trabajo 1

Inventario y planificación

Línea de trabajo 2

Protección de datos en tránsito

Línea de trabajo 3

Firmas y certificados de larga duración

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Servicios de AWS con soporte ML-DSA



AWS Key Management Service (KMS)

06/2025



AWS Private Certificate Authority (Private CA)

10/2025



AWS CloudHSM

(Preview)

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Plan de migración de AWS hacia criptografía post-cuántica (PQC)



Línea de trabajo 1

Inventario y planificación

Línea de trabajo 2

Protección de datos en tránsito

Línea de trabajo 3

Firmas y certificados de larga duración

Línea de trabajo 4

Certificados y Autenticación

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Servicios de AWS con soporte ML-DSA para CA



AWS Private Certificate Authority (Private CA)

10/2025

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.

¡Gracias!

LinkedIn

Please complete the session survey

© 2026, Amazon Web Services, Inc. or its affiliates. All rights reserved.