

# TECNOLOGÍA SOBERANA Y PROTECCIÓN POSTCUÁNTICA

Colaboración para  
una sanidad resiliente

**Darragh Kelly**

*Product Marketing Manager*

SOBERANÍA COMO CAPACIDAD DE MANTENER LA OPERACIÓN

# DEPENDENCIA TECNOLÓGICA Y CONTINUIDAD ASISTENCIAL

≈ 70%

del mercado europeo de  
ciberseguridad cubierto por  
proveedores no europeos

*ECSSO, 2025 ≈ 65% en análisis interno  
del catálogo CPSTIC*

Licencia

Actualización

Nube

Soporte

Operación

**El riesgo no es el origen de la tecnología.**  
Es **carecer de control, alternativas o  
capacidad de sustitución.**

**¿Podríamos mantener la operación si una capacidad crítica dejara de estar disponible?**

CONTEXTO SANITARIO

# LOS ENTORNOS SANITARIOS AMPLIFICAN LAS DEPENDENCIAS TECNOLÓGICAS

**IT + IoT + OT + IoMT**

Tecnologías y ciclos de vida muy distintos

**10 – 15+ años**

Equipos médicos difíciles de actualizar o sustituir



**La importancia de la visibilidad**

CPI INCIBE · COLABORACIÓN APLICADA

# UN CYBERSOC ADAPTADO AL ENTORNO SANITARIO



Impulso mediante Compra Pública de Innovación



Liderazgo e integración del proyecto CyberSOC



OpenNAC-Health: visibilidad, contexto y actuación



Colaboración público-privada y privada-privada sobre necesidades reales del sector.

# DEL CONOCIMIENTO SANITARIO A LA CAPACIDAD DE ACTUAR

## QUÉ DESARROLLAMOS

### IoT

Identificación y perfilado adaptados al entorno clínico

### DICOM / HL7

Comprensión de comunicaciones de imagen médica

### Datos reales

POCs y validación de casos de uso sanitarios

## IMPACTO

### VISIBILIDAD AGNÓSTICA

Múltiples mecanismos para ampliar cobertura y reducir puntos ciegos

### DE LA VISIBILIDAD A LA ACCIÓN

Contexto convertido en segmentación, acceso y control desde la red

**Cerrar el gap entre conocer el entorno y poder actuar.**

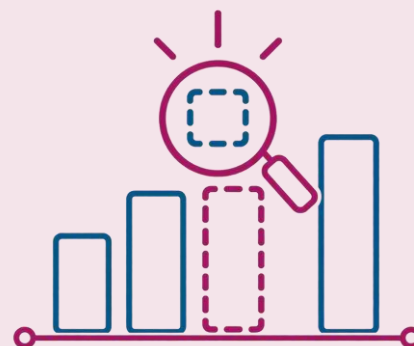
# GARTNER: CERRAR EL GAP ENTRE VISIBILIDAD Y ACCIÓN



## VISIBILIDAD Y CONTEXTO

Identificar y comprender  
el entorno

Monitorización · contexto · priorización



GAP DEL MERCADO



## CAPACIDAD DE ACTUACIÓN

Segmentar, controlar el acceso  
y responder desde la red

Control · contención · respuesta

La **monitorización**, por sí sola, **no mejora la resiliencia operativa**.

**Cerrar el gap entre conocer el entorno y poder actuar.**

# UNA NUEVA NECESIDAD EXIGE INNOVACIÓN Y COLABORACIÓN

## 01 NUEVA NECESIDAD

### Transición postcuántica

Proteger los datos sensibles de hoy frente a las amenazas del futuro.



## 02 NUEVA EXIGENCIA DE INNOVACIÓN

### Adaptar tecnología existente

Incorporar protección postcuántica sin sustituir toda la infraestructura.



## 03 NUEVA COLABORACIÓN

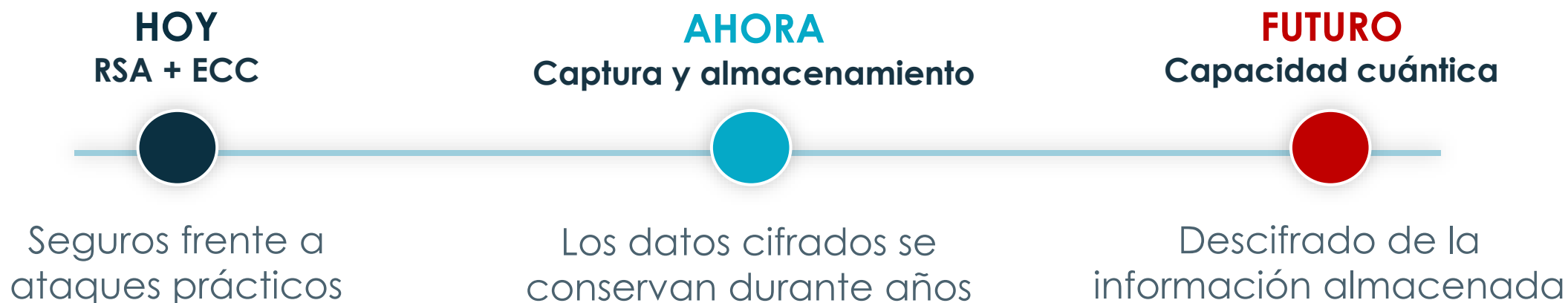
### Trabajo con el CCN

Desarrollar y validar una respuesta aplicable a entornos críticos.

RIESGO POSTCUÁNTICO

# EL RIESGO YA HA COMENZADO

HARVEST NOW, DECRYPT LATER (HNDL)



En sanidad, la **información clínica** puede conservar su sensibilidad durante décadas

**La fecha es incierta. La exposición de los datos ya ha comenzado.**

EL CCN Y LA UE YA HAN MARCADO EL CAMINO A SEGUIR

# ¿POR QUÉ EMPEZAR AHORA?

## 01 CCN-TEC 009

Recomendaciones para la transición a criptografía post-cuántica

Marco operativo nacional que define los pasos para preparar la transición a la criptografía poscuántica.

## 02 Recomendación EU 2024/1101

Coordinated Implementation Roadmap — Post-Quantum Cryptography

Hoja de ruta europea con fases de inventario, pilotos y migración obligatoria para los sectores regulados.

## 03 NIS Cooperation Group

Guidelines on Post-Quantum Cryptography — Coordinated EU Transition

Directrices para implementar PQC en infraestructuras críticas y planificar la transición con antelación.

## TIMELINE DEFINIDO POR LA UE

**2024 – 2025**

Inventario criptográfico

**2026**

Pilotos en entornos críticos

▲ HOY

**2027 – 2029**

Implementación progresiva

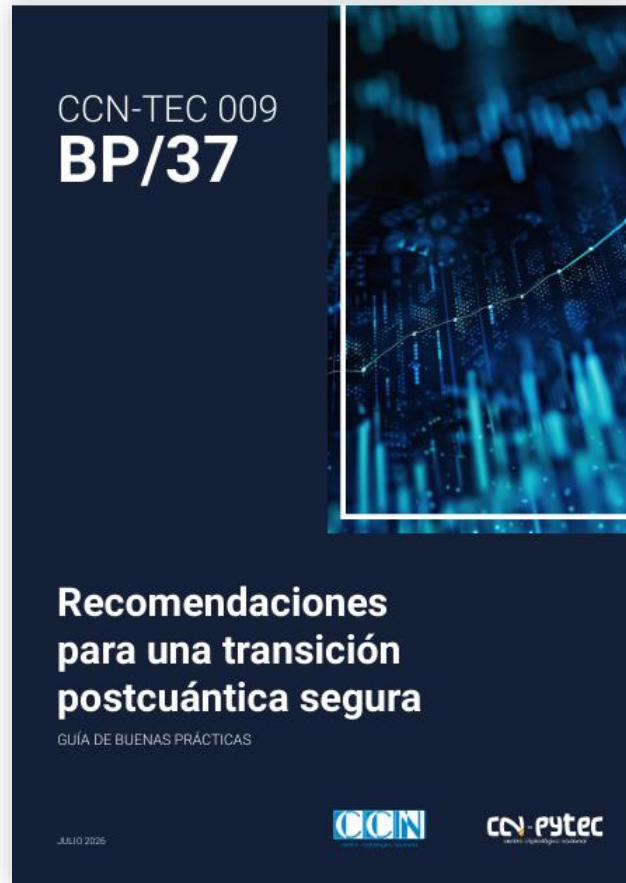
**2030 – 2035**

Migración obligatoria

Actuar ahora neutraliza el HNDL mientras el cambio sigue siendo económico: proteger los datos de larga vida antes de que exista capacidad cuántica.

PASOS PARA INICIAR LA TRANSICIÓN, SEGÚN EL CCN.

# CÓMO ABORDAR LA TRANSICIÓN



- 01  Comenzar cuanto antes
- 02  Inventariar los activos criptográficos
- 03  Evaluar riesgos y priorizar
- 04  Adoptar soluciones híbridas
- 05  Diseñar con cripto-agilidad

**CCN-TEC 009** — Recomendaciones para una transición postcuántica segura, Centro Criptológico Nacional (julio 2026).

Identidad, postura, políticas y visibilidad antes de conectarte.

# CÓMO PROTEGEMOS HOY

01

**Identidad  
verificada**

02

**Autenticación  
MFA / 2FA**

03

**Validación de  
postura**

04

**Motor de  
políticas ONE**

05

**Túnel cifrado**

Wireguard - WG



Kernel module  
+ user-space tools



Kernel-mode driver  
+ user-space



Native client +  
Go implementation



NetworkExtension  
sandbox integration



Managed daemon  
architecture

COLABORACIÓN CON EL CCN

# UNA TRANSICIÓN POSTCUÁNTICA DESPLEGABLE POR SOFTWARE

## COMUNICACIONES SEGURAS



Un atacante debe romper **las dos**: la curva clásica + el algoritmo de retículos.

Una solución software para proteger hoy y preparar la criptografía de mañana.

VISIÓN DE PRODUCTO

# OPENNAC ENTERPRISE: CONOCER, CONTROLAR Y PROTEGER

- 01** **Visibilidad y contexto**  
IT, IoT, OT e IoMT
- 02** **Segmentación y Control de Acceso**  
Políticas aplicadas de manera automática y centralizada a capa 2
- 03** **Comunicaciones seguras**  
WireGuard + preparación postcuántica



*On-premise · independiente del fabricante de red · licenciamiento sencillo y transparente*

**Ver todo. Entender el contexto. Controlar el acceso. Proteger las comunicaciones.**

# TECNOLOGÍA SOBERANA Y PROTECCIÓN POSTCUÁNTICA

Colaboración para  
una sanidad resiliente

**Darragh Kelly**

*Product Marketing Manager*



Crear un mundo mejor, más eficiente, seguro y sostenible

LO HACEMOS POSIBLE

[cipherbit@oesia.com](mailto:cipherbit@oesia.com)

