



NCC-ES

SPAIN CYBERSECURITY
COORDINATION CENTRE



 **incibe**

INSTITUTO NACIONAL DE
CIBERSEGURIDAD

DIGITAL-EC3C-2024-DEPLOY-CYBER-06- ENABLINGTECH

SPAIN

LAND OF CYBERSECURITY

Call 1: Aplicaciones Novedosas de IA y Otras Tecnologías Habilitadoras para Centros de Operaciones de Seguridad (SOC).

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH

Objetivo

- ❖ Desarrollar una tecnología habilitadora, como la Inteligencia Artificial (IA), para SOC's nacionales y plataformas transfronterizas de estos.
- ❖ Estas tecnologías deben fortalecer capacidades para analizar, detectar y prevenir amenazas e incidentes cibernéticos, mientras se apoya la producción de inteligencia de alta calidad sobre amenazas cibernéticas

Alcance

- ❖ Desarrollo y despliegue de sistemas y herramientas para la ciberseguridad basados en tecnologías para la detección y mitigación de amenazas, recuperación de incidentes, análisis y compartición de datos
- ❖ Actividades: detección de patrones, creación de Inteligencia de Amenazas Cibernéticas (CTI), respuesta a incidentes, mitigación de amenazas de malware, identificación y gestión de vulnerabilidades, reducción de ataques y protección de datos sensibles

Stakeholder Objetivo

- ❖ Actores públicos y privados (o consorcios de ambos) que pueden apoyar la detección de amenazas cibernéticas y el intercambio de CTI



Cofinanciado por
la Unión Europea



Indicadores Clave de Rendimiento (KPIs)

- ❖ Número de entidades beneficiadas de los fondos
- ❖ Intensidad de intercambio de información entre entidades
- ❖ Número de servicios de Inteligencia Artificial y tecnologías habilitadoras desplegadas para la detección de incidentes de seguridad digital
- ❖ Número de actividades organizadas para colaboración, comunicación, concientización, entrenamiento e intercambio de información en la implementación de los servicios y herramientas de Inteligencia Artificial.

Resultado esperado

- ❖ Despliegue de IA y Tecnologías Clave Avanzadas para SOC's, herramientas para la creación, análisis y procesamiento de CTI que permitan operaciones más rápidas y escalables de SOC's, y servicios o fuentes de CTI europeas originales

Presupuesto: 30M€. Financiación: 50%. Simple grants

Call 2: Fortalecimiento de las capacidades de ciberseguridad de las PYMEs europeas en línea con los requisitos y obligaciones de la CRA

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA

Objetivo

- ◆ Apoyar a las PYMEs europeas, especialmente micro y pequeñas empresas, para fortalecer sus capacidades de ciberseguridad y apoyar la implementación del Reglamento propuesto sobre la Ley de Ciberresiliencia (CRA).

Alcance

- ◆ Distribuir subvenciones de financiación en cascada a PYMEs europeas para apoyar el cumplimiento con los requisitos y obligaciones de la CRA.
- ◆ Incluye la creación de una plataforma abierta con recursos relacionados con la CRA, la realización de capacitaciones y la promoción de buenas prácticas y casos de uso de cumplimiento de la CRA

Stakeholder Objetivo

- ◆ Autoridades nacionales de ciberseguridad, centros de competencia, Centros de Coordinación Nacionales, entidades privadas y otros stakeholders relevantes con capacidad de agregar demanda de beneficiarios finales y lanzar licitaciones para adquisiciones en el espacio del mercado de ciberseguridad

Indicadores Clave de Rendimiento (KPIs)

- ❖ Número de PYMEs beneficiadas de la financiación,
- ❖ Actividades de sensibilización, número de talleres, sesiones de formación y eventos, recursos publicados para apoyar el cumplimiento de la CRA,
- ❖ Servicios de evaluación de riesgos, visitantes mensuales de la plataforma en línea, casos de uso relacionados con el cumplimiento de la CRA y mejores prácticas desarrolladas y difundidas,
- ❖ Contribuciones a la estandarización relacionada con la CRA.

Resultado esperado

- ❖ Apoyo financiero para PYMEs y otros stakeholders para el cumplimiento de la CRA, plataforma abierta con recursos relacionados con la CRA, talleres, eventos, intercambio de experiencias, y contribuciones a la estandarización de la CRA

Presupuesto: 22M€. Financiación: 100% consorcio; 50% tercero apoyado. Grants for Financial Support



Cofinanciado por
la Unión Europea



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Call 3: Herramientas para el cumplimiento de los requisitos y obligaciones de la CRA (Cyber Resilience Act)

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA

Objetivo

- ❖ Apoyar la implementación de la CRA a través de herramientas que faciliten y automaticen los procedimientos internos de cumplimiento con un enfoque especial en las PYMEs europeas

Alcance

- ❖ Diseño y desarrollo de herramientas para facilitar y automatizar el cumplimiento de la CRA, con un enfoque en herramientas automáticas que aseguren el alineamiento con los requisitos esenciales de ciberseguridad de la CRA y las obligaciones de documentación.

Stakeholder Objetivo

- ❖ PYMEs europeas, pero otros solicitantes están permitidos

Indicadores Clave de Rendimiento (KPIs)

- ❖ Número de herramientas para facilitar y automatizar el cumplimiento de la CRA
- ❖ Cobertura de los requisitos esenciales de la CRA por las herramientas
- ❖ Actividades de sensibilización y formación, casos de uso de cumplimiento de la CRA y mejores prácticas
- ❖ Número de empresas y productos beneficiados por las herramientas desarrolladas

Resultado esperado

- ❖ Herramientas para simplificar y automatizar el cumplimiento de la CRA, incluyendo aquellas que aseguren la alineación con los requisitos esenciales de ciberseguridad de la CRA y las obligaciones de documentación

Presupuesto: 8M€. Financiación: 50% subvenciones de apoyo; PYMES 75%. SME Support Actions



Cofinanciado por
la Unión Europea



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Call 4: Implementación de Criptografía Post-Cuántica (PQC) en sistemas de sectores industriales



NCC-ES
SPAIN CYBERSECURITY
COORDINATION CENTRE

incibe_
INSTITUTO NACIONAL DE
CIBERSEGURIDAD

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY

Objetivo

- ❖ Habilitar la adopción de PQC en sectores industriales como automotriz, automatización, finanzas, sistemas de control o energía
- ❖ Integrar de manera fluida sistemas, equipos, componentes, protocolos y tecnologías de red PQC en redes de seguridad digital y comunicación existentes

Alcance

- ❖ Propuestas enfocadas en la integración de un protocolo PQC estandarizado en redes de seguridad digital y comunicación en los sectores mencionados considerando necesidades específicas de estos.
- ❖ Incluye el desarrollo o adaptación del software/hardware requerido y la validación de la solución en un demostrador a gran escala.

Stakeholder Objetivo

- ❖ Empresas de Criptografía Post-Cuántica, actores industriales, incluyendo PYMEs y startups, y actores relevantes en el proceso de integración y estandarización de PQC



Cofinanciado por
la Unión Europea



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Indicadores Clave de Rendimiento (KPIs)

- ❖ Número de entidades beneficiadas de los fondos
- ❖ Intensidad de intercambio de información entre entidades
- ❖ Número de servicios PQC desarrollados o adaptados
- ❖ Número de actividades organizadas para sensibilización y mejores prácticas en la transición a PQC

Resultado esperado

- ❖ Validación de sistema PQC y tecnología PQC lista para despliegue generalizado en sectores industriales
- ❖ Protección a largo plazo de activos críticos,
- ❖ Seguridad de la información a largo plazo y continuidad operativa ante la llegada de computadoras cuánticas,
- ❖ Listas de verificación y planes de migración para PQC

Presupuesto: 22,25M€. Financiación: 50%. Simple grants

Call 5: Estandarización y concienciación sobre la transición europea a la criptografía post-cuántica

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STANDARDPQC

Objetivo

- ❖ Fortalecer los esfuerzos de Europa en la transición a la criptografía post-cuántica (PQC) apoyando actividades de estandarización europeas e internacionales, elaborando un mapa de ruta industrial europeo para la migración a PQC y aumentando la conciencia sobre los esfuerzos de PQC

Alcance

- ❖ Propuestas con esfuerzos concretos de estandarización dentro de foros europeos e internacionales.
- ❖ Incluye la creación de un mapa de ruta de migración a PQC, la promoción de la conciencia y comprensión de los logros europeos en PQC, y la identificación de necesidades de formación e infraestructura para avanzar en el desarrollo de PQC.

Stakeholder Objetivo

- ❖ Empresas de estandarización de PQC, jugadores industriales, incluyendo PYMEs y startups, y actores relevantes en el proceso de estandarización de PQC



Cofinanciado por
la Unión Europea



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Indicadores Clave de Rendimiento (KPIs)

- ❖ Número de eventos, talleres, consultas con stakeholders y white paper
- ❖ Número de actividades de estandarización europeas e internacionales
- ❖ Actividades de sensibilización y participación de stakeholders
- ❖ Servicios de difusión de investigación

Resultado esperado

- ❖ Contribuciones a estándares y regulaciones europeas e internacionales en PQC
- ❖ Talleres, white papers y otras actividades para apoyar sinergias entre diferentes sectores en la transición a PQC
- ❖ Mapa de ruta europeo para la migración a PQC
- ❖ Desarrollo de estándares para sistemas criptográficos híbridos

Presupuesto: 1M€. Financiación: 100%. Coordination and Support Actions



Cofinanciado por
la Unión Europea



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Call 6: Hoja de ruta para la transición de las administraciones públicas europeas a una era de criptografía post-cuántica

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-TRANSITIONEUPQC

Objetivo

- ❖ Desarrollar una hoja de ruta para la transición de las administraciones públicas a la criptografía post-cuántica (PQC), con un papel destacado para las agencias de seguridad nacional. Esto debe incluir un inventario de sistemas a reemplazar, el cronograma y los aspectos técnicos y legales de la migración a PQC en las administraciones públicas

Alcance

- ❖ Reunir agencias de seguridad nacional, administraciones públicas relevantes y otros stakeholders, incluyendo expertos en PQC.
- ❖ Coordinación de esfuerzos a nivel nacional y europeo para lograr resultados impactantes que conduzcan a la adopción de PQC en las administraciones públicas europeas.

Stakeholder Objetivo

- ❖ Agencias de seguridad nacional y otras administraciones públicas involucradas en el desarrollo de una hoja de ruta para la transición a PQC

Indicadores Clave de Rendimiento (KPIs)

- ❖ Hoja de ruta para la transición a PQC
- ❖ Número de actividades colaborativas que involucran a stakeholders de agencias de seguridad nacional y otras administraciones públicas
- ❖ Actividades de sensibilización y participación de stakeholders entre las administraciones públicas

Resultado esperado

- ❖ Hoja de ruta para la transición de la administración pública europea a PQC
- ❖ Talleres, white papers y otras actividades para apoyar sinergias entre agencias de seguridad nacional y administraciones públicas
- ❖ Colaboraciones entre administraciones públicas respecto a la transición a PQC

Presupuesto: 0,75M €. Financiación: 100%. Coordination and Support Actions

NCC-ES INCIBE

Edificio INCIBE. Av. José Aguado 41.

24005 León. España

Tel: +34 987 877 189

nccspain@incibe.es