

PORTUGAL PROTEGE 21|27

Mostra dos Fundos Europeus do Programa Portugal Protege 21|27

Fundos europeus apoiam projetos estratégicos nas áreas da segurança interna, gestão das fronteiras e política de vistos

O Programa Portugal Protege 21|27 disponibiliza oportunidades de financiamento europeu para o desenvolvimento de projetos que contribuam para reforçar a segurança interna, melhorar a gestão das fronteiras e responder aos desafios associados à prevenção e investigação criminal e ao combate ao crime organizado.

Através do Fundo para a Segurança Interna (FSI) e do Instrumento de Apoio Financeiro à Gestão das Fronteiras e à Política de Vistos (IGFV), são apoiados investimentos destinados, entre outros objetivos, à modernização de equipamentos e sistemas, à adoção de novas soluções tecnológicas, ao reforço das capacidades operacionais e à cooperação entre entidades nacionais e europeias.

Neste contexto, a Secretaria-Geral do Ministério da Administração Interna, enquanto entidade responsável pela gestão destes instrumentos, desempenha um papel fundamental na divulgação das oportunidades de financiamento e no acompanhamento dos beneficiários, contribuindo para transformar os recursos europeus em projetos com impacto concreto na segurança e na proteção das fronteiras.

A importância destes apoios esteve em destaque na Mostra dos Fundos Europeus do Programa Portugal Protege 21|27, promovida pela SGM AI, a 15 de setembro, em Cascais, sob o mote «Fronteiras Seguras, Europa Protegida».

Através de exposições, demonstrações operacionais e de uma conferência estratégica, a iniciativa deu a conhecer projetos financiados pelo FSI e pelo IGFV e reuniu forças e serviços de segurança, especialistas, académicos e representantes de instituições nacionais e europeias para refletir sobre temas como as fronteiras inteligentes, a prevenção e investigação criminal, o combate ao crime organizado e os desafios futuros da segurança interna.

A Mostra permitiu, assim, dar visibilidade aos resultados concretos do financiamento europeu e ao potencial do Portugal Protege 21|27 para apoiar novos projetos e investimentos, reforçando as capacidades nacionais e contribuindo para uma Europa mais segura, resiliente e preparada para enfrentar ameaças emergentes.

Consulte o Programa [aqui](#)



DIGITAL-ECCC-2027-DEPLOY-CYBER-11-DUALUSE

Dual-use technologies

OBJETIVOS

Este aviso surge no âmbito, da necessidade de dar relevância, às tecnologias de dupla utilização que emergiram como um pilar fundamental para enfrentar tanto as ameaças à cibersegurança como as necessidades mais amplas de ciberdefesa. A integração de tecnologias civis e militares avançadas sob uma estrutura unificada é crucial para reforçar a resiliência em infraestruturas críticas, garantindo a segurança dos dados. Além disso, o combate ao cibercrime e às ameaças híbridas contribuirá para a manutenção da estabilidade social.

O objetivo é reforçar a cooperação entre as esferas civil e de defesa no que diz respeito a projetos, serviços, competências e aplicações de dupla utilização em cibersegurança.

Resultados Esperados

- Estrutura de Partilha de Dados Segura;
- Sistemas de Alerta Antecipado (EWS);
- Programas de Formação Colaborativa;
- Sistemas Integrados de Detecção de Ameaças;
- Normas de segurança intersectoriais;
- Colaboração e integração das partes interessadas.

BENEFICIÁRIOS

São considerados beneficiários todas as entidades interessadas nas esferas da Cibersegurança Civil e da Defesa, com o objetivo de fomentar colaborações conjuntas que visem o desenvolvimento de sistemas, ferramentas e tecnologias concretas. Este aviso pode incorporar entidades, como empresas industriais, Ministérios e Agências de Defesa, Ministérios da Administração Interna, PME e startups e atores relevantes que desempenham um papel nas esferas europeias de Cibersegurança Civil e Defesa.

Consórcio

A composição de consórcios multinacionais não é obrigatória para este tema, mas contribuirá positivamente para o impacto da ação.

DOTAÇÃO GLOBAL

10.000.000,00€

DOTAÇÃO POR PROJETO

3.000.000,00€ a 5.000.000,00€
(3 projetos)

PRAZO

14 de janeiro de 2027

COFINANCIAMENTO

50%

FONTE

Comissão Europeia

[consultar programa](#)

NOTA IMPORTANTE: Recomenda-se a verificação da informação diretamente nos Avisos Oficiais, que prevalece sobre qualquer síntese ou resumo.

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG

Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements

OBJETIVOS

O objetivo deste aviso é apoiar o ecossistema europeu no reforço das suas capacidades de cibersegurança e na implementação do quadro regulamentar, em conformidade com: a regulamentação de Ciber-Resiliência (CRA), a Diretiva NIS 2, a RGPD- General Data Protection Regulation, a DORA- Digital Operational Resilience Act, a Lei da Cibersegurança, Regulamento Europeu da Inteligência Artificial, tornando as Entidades mais resilientes, com uma abordagem mais homogênea. Além disso, e em consonância com o Plano de Educação Digital, que enfatiza o desenvolvimento de competências digitais cruciais para a economia moderna, e em apoio de iniciativas como a Academia de Competências em Cibersegurança, devem também ser promovidas atividades relacionadas com os desafios da cibersegurança. Estas iniciativas visam colmatar a escassez de competências em cibersegurança e desenvolver uma força de trabalho capaz de satisfazer as exigências regulamentares e operacionais. Ao proporcionar formação prática, atrair jovens profissionais e incentivar a diversidade na área, estes esforços são vitais para a capacidade da Europa de responder às ameaças cibernéticas em evolução e de cumprir a nova legislação. Além disso, estas atividades promovem a igualdade de oportunidades e aumentam a consciencialização sobre a cibersegurança entre as gerações futuras, contribuindo para os objetivos estratégicos mais amplos da Europa no domínio digital.

Resultados Esperados

- Implementação de orientações, processos normalizados ou manuais;
- Desenvolvimento e implementação de ferramentas, sensibilização e incentivo no âmbito da Cibersegurança;
- Apoio a mecanismos que reduzam a carga administrativa para as entidades;
- Estabelecimento de canais de comunicação seguros que permitam a cooperação e a iniciativas de partilha de informação;
- Apoio à organização de reuniões/workshops regulares para identificar boas práticas em setores específicos ou áreas emergentes;
- Apoio ao desenvolvimento de cursos de formação;
- Contributo para a normalização da Cibersegurança;
- Promoção da certificação;
- Desenvolvimento de programas e materiais de formação, incluindo ferramentas para colaboração e intercâmbio transnacional, com o objetivo de melhorar as competências dos participantes;
- Criação de programas de benchmarking;
- Implementação de programas de intercâmbio e de bolsas de estudo.

BENEFICIÁRIOS

- Empresas PME
- Start up
- Autoridades dos Estados-membros
- Equipas de resposta a Incidentes de Segurança Informática
- Centros de Operações de Segurança
- Operadores de Serviços Essenciais
- Prestadores de Serviços Digitais
- Centros de Partilha e Análise de Informação
- Intervenientes que desempenham um papel na implementação da Lei da Resiliência Cibernética

Consórcio

A composição de consórcios multinacionais não é obrigatória para este aviso, mas contribuirá positivamente para o impacto da ação.

DOTAÇÃO GLOBAL

20.000.000,00€

DOTAÇÃO POR PROJETO

3.000.000,00€ a 5.000.000,00€
(5 projetos)

PRAZO

14 de janeiro de 2027

COFINANCIAMENTO

50%

FONTE

Comissão Europeia



[consultar programa](#)

NOTA IMPORTANTE: Recomenda-se a verificação da informação diretamente nos Avisos Oficiais, que prevalece sobre qualquer síntese ou resumo.

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-CYBERAI cybersecure tools, technologies and services relying on AI

OBJETIVOS

Este aviso, aborda as tecnologias baseadas em IA (incluindo a IA generativa) para as autoridades nacionais e as autoridades competentes, incluindo os Centros Nacionais e Transfronteiriços de Cibersegurança, CSIRTs - Computer Security Incident Response Teams, organismos públicos e entidades privadas abrangidas pela diretiva NIS 2, NCCs - National Coordination Centres. Estas desempenham um papel fundamental no fornecimento de capacidade operacional central aos ecossistemas europeus de cibersegurança. Podem também fornecer dados de entrada primários para ferramentas e soluções de cibersegurança baseadas em IA/ML, o que pode reforçar a capacidade destas autoridades para analisar, detetar e prevenir ciberameaças e incidentes, e para apoiar a produção de informação de alta qualidade sobre ciberameaças. Em particular, a adoção da IA generativa poderá representar um desafio e uma oportunidade para os processos e aplicações de cibersegurança.

Estas tecnologias têm como objetivo permitir uma criação e análise mais eficazes de Inteligência de Ciberameaças (CTI), a automatização de processos em larga escala, bem como um processamento mais rápido e escalável de CTI e a identificação de padrões que permitam uma deteção e tomada de decisão rápidas.

Resultado Esperado

- Implementação de Inteligência Artificial e de diversas tecnologias alimentadas por IA como facilitadores para Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs e outros.
- Novas ferramentas de cibersegurança baseadas em IA que foram desenvolvidas, testadas e validadas em condições relevantes e disponibilizadas para Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs e outros.
- Melhor partilha de informação e colaboração entre os Centros Cibernéticos Nacionais e Transfronteiriços, CSIRTs, NCSCs, NIS SPOCs e outras partes interessadas relevantes, apoiada por CTI produzidos por ferramentas alimentadas por IA.
- Ferramentas para a automatização de processos de cibersegurança como a criação, análise e processamento de CTI, para potenciar as operações dos Cyber Hubs.
- Feeds ou serviços CTI europeus originais.
- Garantir que as soluções seguras de IA mais avançadas e inovadoras são desenvolvidas e implementadas para os setores NIS.
- Soluções e ferramentas de IA seguras, em conformidade com a legislação da UE. Promover a mitigação dos riscos associados ao uso indevido da IA por atores mal-intencionados, com foco na ética da IA e na implementação segura.
- Contributo para a normalização e certificação de tecnologias de IA ciberseguras e fiáveis.

BENEFICIÁRIOS

Fornecedores de tecnologia, operadores de Cyber Hubs, instituições de investigação e académicas, entidades de cibersegurança, setor público, entidades da Diretiva NIS 2, setor privado, outras partes interessadas relevantes que apoiam a implementação de soluções de IA ciberseguras.

DOTAÇÃO GLOBAL

15.000.000,00€

DOTAÇÃO POR PROJETO

3.000.000,00€ a 5.000.000,00€
(4 projetos)

PRAZO

14 de janeiro de 2027

COFINANCIAMENTO

50%

FONTE

Comissão Europeia

[consultar programa](#)



NOTA IMPORTANTE: Recomenda-se a verificação da informação diretamente nos Avisos Oficiais, que prevalece sobre qualquer síntese ou resumo.



DIGITAL-ECCC-2027-DEPLOY-CYBER-11-REGCABH Regional Cable Hubs

OBJETIVOS

O objetivo deste aviso é apoiar a criação progressiva de Centros Regionais de Cabos, um por bacia marítima da UE, cuja função será reforçar concretamente a deteção de ameaças e a segurança operacional em torno destas infraestruturas estratégicas.

Esta ação visa, assim, apoiar a implementação de processos, ferramentas e serviços para a deteção e análise de ameaças emergentes, de forma a estabelecer uma consciência situacional quase em tempo real para proteger os cabos submarinos. A ação inclui a capacidade de agregar dados e informações de segurança de todas as fontes disponíveis (incluindo sistemas estabelecidos como o Sistema Marítimo Integrado, ou CISE, ou Centros Nacionais de Cibersegurança) e analisá-los de forma automatizada. A ação apoiará também o estabelecimento de uma função de notificação de incidentes e de um procedimento para a partilha de informações entre as autoridades nacionais competentes.

Resultados Esperados

Os centros regionais de cabos submarinos contribuirão para melhorar e consolidar a consciência situacional coletiva e as capacidades de deteção, apoiando o desenvolvimento de capacidades operacionais para garantir a segurança e a resiliência dos cabos submarinos.

Os centros devem atuar como um ponto central que permita uma maior integração de dados e informação relevantes para o ambiente de segurança dos cabos, possibilitando a divulgação de informação sobre ameaças e a deteção de incidentes à escala regional e entre um conjunto diversificado de intervenientes nacionais, conforme designado por cada Estado-membro (por exemplo, Centros Nacionais, CSIRTs).

Os centros devem permitir uma troca rápida de informações, mesmo que classificadas, entre as autoridades participantes num determinado centro. Para o efeito, as autoridades participantes devem estabelecer procedimentos de cooperação e partilha de informações.

Além disso, os centros regionais de cabos submarinos podem também beneficiar de soluções adicionais para a vigilância e proteção de cabos submarinos e para a deteção de atividades maliciosas. Por exemplo, a consciência situacional obtida através da recolha e análise de dados de sensores marítimos in situ, bem como de imagens de satélite relevantes ou capacidades de drones submarinos.

BENEFICIÁRIOS

Autoridades públicas competentes de, pelo menos, dois Estados-membros envolvidos na bacia marítima relevante. Outras entidades públicas ou privadas relevantes podem participar, se necessário, para a implementação.

As propostas podem incluir a expansão de projetos existentes de Centros Regionais de Cabos financiados em chamadas anteriores deste tema para outros Estados-membros.

DOTAÇÃO GLOBAL

5.000.000,00€

DOTAÇÃO POR PROJETO

2.500.000,00€

(+/- 2 projetos)

PRAZO

14 de janeiro de 2027

COFINANCIAMENTO

70%

FONTE

Comissão Europeia

[consultar programa](#)

NOTA IMPORTANTE: Recomenda-se a verificação da informação diretamente nos Avisos Oficiais, que prevalece sobre qualquer síntese ou resumo.

Comissão Europeia lança consulta pública sobre o futuro das Parcerias Europeias no Horizonte Europa 2028-2034

A Comissão Europeia (CE) abriu uma consulta pública para recolher contributos sobre o futuro das Parcerias Europeias no próximo Programa-Quadro de Investigação e Inovação (2028-2034).

As Parcerias Europeias são instrumentos estratégicos que reúnem a CE, os Estados-membros, a indústria, organizações de investigação e outros parceiros, com o objetivo de mobilizar investimento público e privado, promover o desenvolvimento de tecnologias e soluções inovadoras e responder aos principais desafios da União Europeia.

Esta é uma oportunidade para empresas, centros de investigação, universidades e entidades públicas partilharem a sua visão sobre a mobilização de investimento, o reforço da competitividade do ecossistema europeu e a aceleração da chegada da inovação ao mercado. Os contributos serão importantes para identificar prioridades e definir as áreas temáticas que poderão integrar o futuro portefólio de Parcerias Europeias.

A consulta contribuirá para a avaliação de impacto da Comissão Europeia, que servirá de base à preparação do futuro Single Basic Act para as Joint Undertakings, de eventuais atos legislativos relativos a iniciativas ao abrigo do artigo 185.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e à definição do futuro portefólio de Parcerias Europeias no Horizonte Europa 2028-2034.

i A consulta pública está aberta a toda a comunidade de investigação e inovação até 16 de outubro. As respostas podem ser submetidas em qualquer uma das 24 línguas oficiais da União Europeia.

 A consulta pública está disponível [aqui](#).



Contactos

Equipa Multidisciplinar de Captação de Financiamento
para as Entidades MAI

Rua de São Mamede, n.º 23
1100-533 Lisboa

Telefone +351 213 409 000

emcf@sg.mai.gov.pt

www.sg.mai.gov.pt