AGÊNCIA DA UNIÃO EUROPEIA PARA A CIBERSEGURANÇA

# UMA EUROPA DE CONFIANÇA E COM CIBERSEGURANÇA

## Estratégia da ENISA

Junho de 2020

# UMA EUROPA DE CONFIANÇA E COM CIBERSEGURANÇA

AGÊNCIA DA UNIÃO EUROPEIA PARA A CIBERSEGURANÇA

# PREFÁCIO

**Durante mais de 15 anos, a ENISA – a Agência da UE para a Cibersegurança – desempenhou um papel fundamental ao permitir concretizar a ambição da UE de reforçar a confiança e a segurança digital na Europa, em conjunto com os Estados-Membros e as instituições e agências da UE. Ao aproximar as comunidades, a ENISA contribuiu com sucesso para fortalecer as capacidades de preparação e resposta da Europa a ciberincidentes.**

Simultaneamente, a digitalização da nossa economia e sociedade aumentou drasticamente, conforme demonstrado durante a crise da COVID-19, quando uma viragem coletiva e em massa para soluções de TI remotas foi essencial para manter muitas atividades a funcionar. Esta crise demonstrou o quanto os ciberinvasores se aproveitam da nossa dependência destas tecnologias. Também revelou como o cenário de ciberameaça se amplificou, passando de ataques a alvos para novas formas de ameaças em massa a milhões de empresas e cidadãos, incluindo um número crescente de incidentes sofisticados de ransomware (software de sequestro). O rápido desenvolvimento de produtos e serviços digitais, desde a nuvem e da videoconferência até ao 5G e à IA, também trouxe novos desafios a descobrir e enfrentar.

Com o seu mandato ininterrupto e agora reforçado com novas atribuições e capacidades, a ENISA está mais do que nunca vocacionada para desempenhar um papel preponderante na prestação de apoio à UE e aos seus Estados-Membros para que continuem a dar resposta a estes desafios, no dealbar de uma nova era para a cibersegurança na Europa.

No desempenho das sua funções, a ENISA com vista a antecipar tendências relevantes, captar e partilhar os conhecimentos especializados e a informação mais avançados, em benefício de todos. Apoiará a Comissão Europeia e os Estados-Membros na ajuda aos atores públicos e privados e aos cidadãos na prevenção e gestão dos riscos associados aos ciberincidentes. Com a implementação do enquadramento para a certificação de cibersegurança, a ENISA contribuirá para uma mudança de paradigma, melhorando o nível de segurança das soluções digitais implantadas na Europa e, desse modo, aumentando a possibilidade de escolha e de confiança de todos. Além disso, a Agência apoiará ativamente a comunidade operacional europeia de cibersegurança, cooperando estreitamente com a mesma e preparando-se para responder em conjunto quando o próximo ciberincidente de grande escala atingir a Europa.

No desempenho das novas funções que lhe foram conferidas, a abertura, a agilidade e a fiabilidade serão os principais motores das suas operações diárias, ao mesmo tempo que trabalha mais estreitamente com os Estados-Membros e a Comissão Europeia no alinhamento das abordagens. A ENISA também se esforçará por melhorar o seu impacto ambiental no contexto da atual crise climática e por criar um ambiente de trabalho socialmente responsável e inclusivo.

Este documento de estratégia, elaborado com o contributo de todo o pessoal da ENISA, dos membros do seu Conselho de Administração e do seu Grupo Consultivo num processo colaborativo e inclusivo, estabelece os objetivos claros que nortearão o trabalho da agência nos próximos anos para enfrentar os muitos desafios que se avizinham.

Pelo Conselho de Administração

**Jean-Baptiste Demaison**
Presidente do Conselho de Administração

**Krzysztof Silicki**
Vice-presidente do Conselho de Administração

# VISÃO

**Uma Europa de confiança e com cibersegurança**

# MISSÃO

A missão da Agência da União Europeia para a Cibersegurança (ENISA) é atingir um elevado nível comum de cibersegurança na União, em cooperação com a comunidade em geral. No cumprimento da sua missão funciona como centro de conhecimentos especializados em cibersegurança, recolhendo informação e disponibilizando assistência e aconselhamento técnico independente e de elevada qualidade aos Estados-Membros e organismos da UE em matéria de cibersegurança. Contribui para o desenvolvimento e a implementação da ciberpolítica da União.

O nosso objetivo é reforçar a confiança na economia conectada, aumentar a resiliência e a confiança das infraestruturas e dos serviços da União e garantir a segurança digital da nossa sociedade e dos nossos cidadãos. Aspiramos a ser uma organização ágil, ambiental e socialmente responsável e centrada nas pessoas.

# VALORES

**Mentalidade comunitária**
A ENISA trabalha com as comunidades, respeitando as suas competências e os seus conhecimentos especializados, e promove sinergias e confiança para melhor cumprir a sua missão.

**Excelência**
A ENISA visa alcançar no seu trabalho o nível de competência técnica mais avançado, mantém níveis operacionais da mais elevada qualidade e avalia o seu desempenho para alcançar uma melhoria contínua através da inovação e previsão.

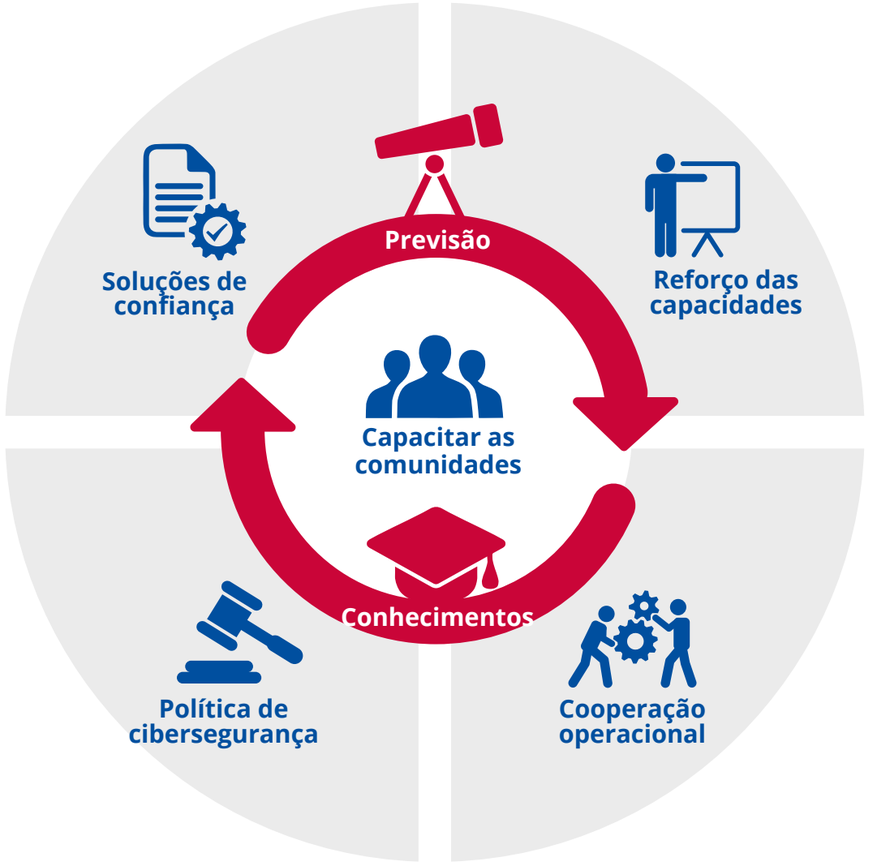
**Integridade/ética**
A ENISA respeita os princípios éticos e as regras e obrigações relevantes da UE nos seus serviços e no seu ambiente de trabalho, garantindo justiça e inclusão.

**Respeito**
A ENISA respeita os direitos e os valores fundamentais europeus em todos os seus serviços e no seu ambiente de trabalho, bem como as expectativas das partes interessadas.

**Responsabilidade**
A ENISA assume responsabilidades garantindo, assim, a integração das dimensões social e ambiental nas práticas e procedimentos.

**Transparência**
A ENISA adota procedimentos, estruturas e processos abertos, factuais e independentes, limitando, assim, o preconceito, a ambiguidade, a fraude e a falta de tranparência.

# OBJETIVOS ESTRATÉGICOS



# OE1

## Objetivo estratégico

# COMUNIDADES CAPACITADAS E ENVOLVIDAS EM TODO O ECOSSISTEMA DE CIBERSEGURANÇA

## Contexto

A cibersegurança é uma responsabilidade partilhada. A Europa esforça-se por implementar um enquadramento de cooperação transetorial abrangente. A ENISA desempenha um papel fundamental na promoção da cooperação ativa entre as partes interessadas no domínio da cibersegurança nos Estados-Membros e nas instituições e agências da UE. Esforça-se por garantir a complementaridade dos esforços comuns, agregando valor às partes interessadas, explorando sinergias e utilizando de forma eficaz os conhecimentos especializados e os recursos em cibersegurança limitados. As comunidades devem ser capacitadas para ampliar o modelo de cibersegurança.

## O que queremos alcançar

- Um acervo de conhecimentos de ponta a nível da UE sobre conceitos e práticas de cibersegurança, que desenvolva a cooperação entre os principais atores no domínio da cibersegurança, promova os ensinamentos aprendidos e os conhecimentos especializados da UE e crie novas sinergias.
- Um ciberecossistema capacitado que abranja as autoridades dos Estados-Membros, as instituições, as agências e os organismos da UE, as associações, os centros de investigação e as universidades, a indústria, os atores privados e os cidadãos, que desempenham o seu papel para tornar a Europa segura em termos cibernéticos.

# OE2

**Objetivo estratégico**

# A CIBERSEGURANÇA COMO PARTE INTEGRANTE DAS POLÍTICAS DA UE

## Contexto

A cibersegurança é a pedra angular da transformação digital e a sua necessidade é transversal a todos os setores devendo, por conseguinte, ser tida em consideração num amplo espetro de políticas e iniciativas. A cibersegurança não deve estar circunscrita a uma comunidade especializada de peritos técnicos. A cibersegurança deve, portanto, ser integrada em todos os domínios de política da UE. É essencial evitar a fragmentação e fomentar uma abordagem coerente que, ao mesmo tempo, tenha em conta as especificidades de cada setor.

## O que queremos alcançar

- Aconselhamento e apoio proativos a todos os atores relevantes a nível da UE, integrando a dimensão da cibersegurança no ciclo de vida do desenvolvimento de políticas através de orientações técnicas viáveis e específicas.
- Estruturas de gestão de risco de cibersegurança implantadas em todos os setores e acompanhadas durante todo o ciclo de vida da política de cibersegurança.

# OE3

**Objetivo estratégico**

# COOPERAÇÃO EFICAZ ENTRE OS ATORES OPERACIONAIS DA UNIÃO EM CASO DE CIBERINCIDENTES EM MASSA

## Contexto

Os benefícios da economia e da sociedade digitais europeias só podem ser plenamente alcançados com a premissa da cibersegurança. Os ciberataques não conhecem fronteiras. Todos os estratos sociais podem ser afetados e a União deve estar pronta para responder a ciberataques (em grande escala e transfronteiriços) e a cibercrises em massa. As interdependências transfronteiriças realçaram a necessidade de uma cooperação eficaz entre os Estados-Membros e as instituições da UE para uma resposta mais rápida e uma coordenação adequada dos esforços a todos os níveis (estratégico, operacional, técnico e de comunicações).

## O que queremos alcançar

- Apoio contínuo, transfronteiriço e transversal à cooperação entre os Estados-Membros, bem como com as instituições da UE. Em particular, tendo em conta os potenciais incidentes e crises em grande escala, apoiar o reforço da cooperação técnica operacional, política e estratégica entre os principais atores operacionais, a fim de possibilitar uma resposta atempada, a partilha de informações, o conhecimento da situação e a comunicação no âmbito de crises na União.
- Tratamento técnico abrangente e rápido de pedidos dos Estados-Membros para facilitar as necessidades técnicas e operacionais na gestão de incidentes e crises.

# OE4

## Objetivo estratégico

# COMPETÊNCIAS E CAPACIDADES DE PONTA EM CIBERSEGURANÇA NA UNIÃO EUROPEIA

## Contexto

A frequência e sofisticação dos ciberataques estão a aumentar a um ritmo acentuado, ao mesmo tempo que a utilização de infraestruturas e tecnologias de TIC por parte de indivíduos, organizações e setores se intensifica. As necessidades de conhecimento e competências em cibersegurança excedem a oferta. A UE deve investir no desenvolvimento de competências e talentos em cibersegurança a todos os níveis, desde os não especialistas aos profissionais altamente qualificados. Os investimentos devem centrar-se não só em aumentar o conjunto de competências em cibersegurança nos Estados-Membros, mas também em garantir que as diferentes comunidades operacionais possuem a capacidade adequada para lidar com o panorama das ciberameaças.

## O que queremos alcançar

- Alinhamento das competências, da experiência profissional e das estruturas de ensino no domínio da cibersegurança para atender às necessidades cada vez maiores de conhecimentos e competências em cibersegurança na UE.
- Um nível de base elevado de sensibilização e de competências em matéria de cibersegurança em toda a UE e, mesmo tempo, a integração da cibersegurança em novas disciplinas.
- Competências bem solidificadas e testadas com a capacidade adequada para lidar com o contexto de ameaça em constante evolução na UE.

# OE5

**Objetivo estratégico**

# ELEVADO NÍVEL DE CONFIANÇA EM SOLUÇÕES DIGITAIS SEGURAS

## Contexto

Os produtos e serviços digitais implicam benefícios e riscos, sendo que os riscos devem ser identificados e mitigados. No processo de avaliação da segurança das soluções digitais e da garantia da sua fiabilidade, é essencial adotar uma abordagem comum, com o objetivo de encontrar um equilíbrio entre as necessidades societais, de mercado, económicas e de cibersegurança. Uma entidade neutra que funcione de forma transparente aumentará a confiança do cliente nas soluções digitais e no ambiente digital mais alargado.

## O que queremos alcançar

- Um ambiente ciberdigital seguro em toda a UE, onde os cidadãos podem confiar em produtos, serviços e processos de TIC através da implantação de sistemas de certificação em áreas tecnológicas essenciais.

# OE6

## Objetivo estratégico

# PREVISÃO DOS DESAFIOS EMERGENTES E FUTUROS EM CIBERSEGURANÇA

## Contexto

Várias novas tecnologias, ainda a dar os primeiros passos ou perto de serem integradas, beneficiariam com a utilização de métodos de previsão. Através de um processo estruturado que permita o diálogo entre as partes interessadas, os decisores políticos e os legisladores podem definir estratégias de atenuação precoces que melhorem a resiliência da UE às ameaças de cibersegurança, bem como encontrar soluções para dar resposta aos desafios emergentes.

## O que queremos alcançar

- Compreender tendências e padrões emergentes utilizando cenários de previsão e futuros que contribuam para mitigar os desafios cibernéticos das nossas partes interessadas.
- Avaliação antecipada dos desafios e riscos da adoção e adaptação às opções futuras emergentes, colaborando, ao mesmo tempo, com as partes interessadas no desenvolvimnento de estratégias de mitigação adequadas.

# OE7

## Objetivo estratégico

# INFORMAÇÕES DE CIBERSEGURANÇA EFICIENTES E EFICAZES E GESTÃO DE CONHECIMENTO PARA A EUROPA

## Contexto

A energia que alimenta o moinho da cibersegurança é a informação e o conhecimento. Para que os profissionais de cibersegurança sejam eficientes na perseguição dos nossos objetivos, trabalhem num ambiente em constante mudança – em termos de desenvolvimentos digitais e de atores — e dêem resposta aos desafios do nosso tempo, precisamos de um processo contínuo de recolha, organização, síntese, análise, comunicação e manutenção de informações e conhecimentos sobre cibersegurança. Todas as fases são essenciais para garantir que a informação e o conhecimento sejam partilhados e disseminados no ecossistema de cibersegurança da UE.

## O que queremos alcançar

- Informação partilhada e gestão do conhecimento para o ecossistema de cibersegurança da UE de forma acessível, personalizada, oportuna e aplicável, com metodologia, infraestruturas e ferramentas adequadas, bem como métodos de garantia de qualidade conjugados para alcançar a melhoria contínua dos serviços.

## ACERCA DA ENISA

A Agência da União Europeia para a Cibersegurança, ENISA, é a agência da União dedicada à obtenção de um elevado nível comum de cibersegurança na Europa. Estabelecida em 2004 e reforçada pelo Regulamento Cibersegurança da UE, a Agência da União Europeia para a Cibersegurança contribui para a ciberpolítica da UE, reforça a fiabilidade dos produtos, serviços e processos de TIC com sistemas de certificação da cibersegurança, coopera com os Estados-Membros e os organismos da UE e ajuda a Europa a preparar-se para os desafios cibernéticos de amanhã. Através da partilha de conhecimentos, do reforço das capacidades e da sensibilização, a Agência trabalha em colaboração com as suas principais partes interessadas para reforçar a confiança na economia conectada, aumentar a resiliência da infraestrutura da União e, em última análise, manter a segurança digital da sociedade e dos cidadãos europeus. Pode encontrar mais informações sobre a ENISA e o seu trabalho em www.enisa.europa.eu

TP-02-20-759-PT-C

**ENISA**
Agência da União Europeia para a Cibersegurança

**Delegação de Atenas**
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Grécia

**Delegação de Heraclião**
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Grécia

enisa.europa.eu