

CACADEMY

FORMAÇÃO AVANÇADA
EM CIBERSEGURANÇA

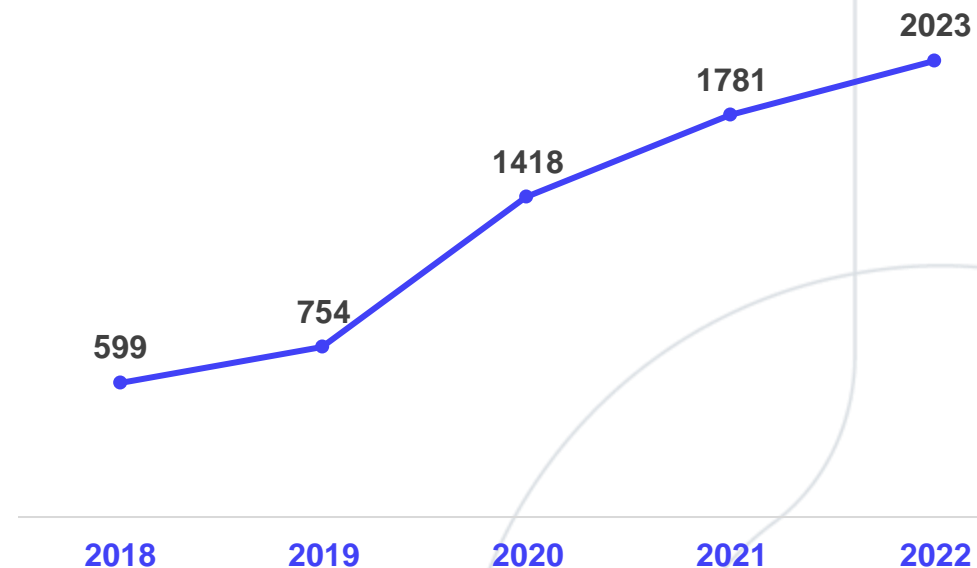
www.cncs.gov.pt



OS DESAFIOS DA CIBERSEGURANÇA

Os incidentes de cibersegurança são uma ameaça crescente ao funcionamento das organizações.

Ano	Total	Variação %
2018	599	+20
2019	754	+26
2020	1418	+88
2021	1781	+26
2022	2023	+14



Número de incidentes de cibersegurança no período 2018-2022 registados pelo CERT.PT

OS DESAFIOS DA CIBERSEGURANÇA

Os setores mais afetados, entre 2019 e 2022, foram: o setor Bancário (1251); as Infraestruturas digitais (825); os Prestadores de serviços de internet (663); a educação, ciência, tecnologia e ensino superior (546); a Administração local (308) e a Administração interna (222).

Nº de incidentes por setor anualmente - CERT.PT



Evolução do número de incidentes de cibersegurança na Administração Local (2019-2022)

OS DESAFIOS DA CIBERSEGURANÇA

O CNCS identificou ações gerais para mitigar os desafios à cibersegurança:



Formar mais recursos humanos para capacitar as organizações públicas e privadas.

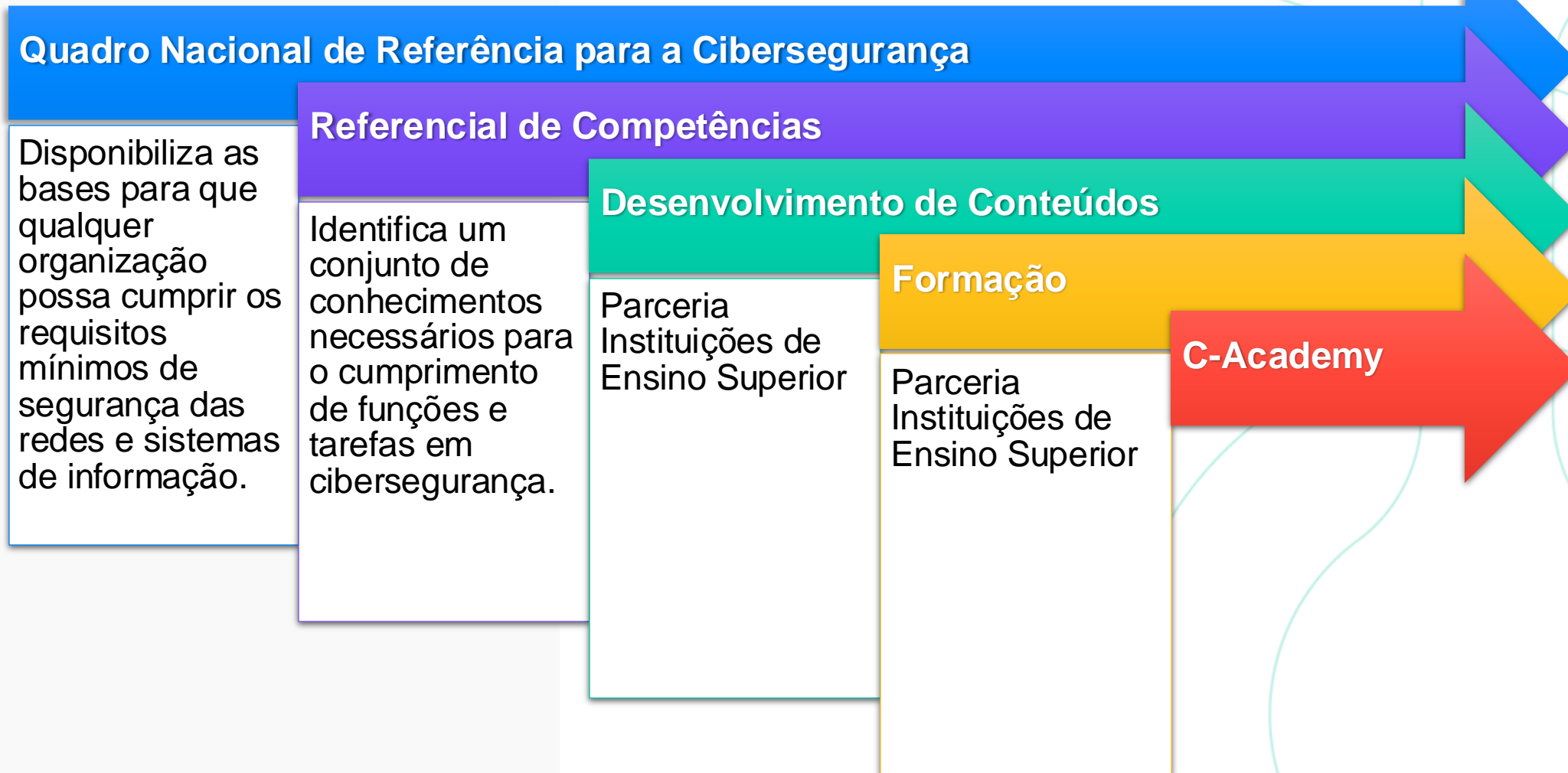


Criar mecanismos para a retenção dos profissionais ligados à cibersegurança na Administração Pública e nas empresas em Portugal.



Manter os conteúdos de boas práticas, os alertas e as políticas de cibersegurança atualizados com o conhecimento situacional do momento e os tutoriais de mitigação de riscos correspondentes.

ENQUADRAMENTO



O QUE É?

Um programa de formação para a administração pública e o sector privado que proporcionará competências avançadas a novos especialistas em cibersegurança.

Desenvolvido pelo Centro Nacional de Cibersegurança

Cofinanciado pela União Europeia no âmbito do Plano de Recuperação e Resiliência

OBJETIVOS C-ACADEMY

Abranger pelo menos 9800 formandos até ao primeiro trimestre de 2026

Alcançar uma distribuição geográfica que permita abranger todo o território nacional

INSTITUIÇÕES PARCEIRAS

Protocolos com Instituições de Ensino Superior para o desenvolvimento dos conteúdos e/ou implementação do programa de formação.

21 contratos com as seguintes Instituições de Ensino Superior Público:



Instituto Politécnico da Guarda
Instituto Politécnico de Bragança
Instituto Politécnico de Coimbra
Instituto Politécnico de Lisboa
Instituto Politécnico de Viana do Castelo
Instituto Politécnico de Viseu
Instituto Politécnico do Cávado e Ave
Instituto Politécnico do Porto

ISCTE - Instituto Universitário de Lisboa
Universidade da Beira Interior
Universidade da Madeira
Universidade de Aveiro
Universidade de Coimbra
Universidade de Évora
Universidade de Trás-os-Montes e Alto Douro
Universidade do Algarve
Universidade do Minho
Universidade do Porto
Universidade dos Açores
Universidade Nova de Lisboa
Faculdade de Ciências da Universidade de Lisboa

Oferece uma oferta formativa diversificada

34 Formações

17 Percursos Formativos

6 Níveis de exigência

A – F

Em 21 Instituições de Ensino Superior

Por todo o país

Carga Horária

35 ou 70 horas

Atribuição de ECTS

Reconhecimento académico

Valor da Inscrição

50€ para formações de 35h, e
100€ para formações de 70h

OFERTA FORMATIVA

Nível A

_ FORMAÇÃO

50€

Mínimo 31 | Máximo 35 Formandos

Nível	Formação	Carga Horária
A	Fundamentos Básicos de Cibersegurança	35
A	Princípios Técnicos em Cibersegurança	35
A	Proteção e Privacidade de Dados	35
A	Formação em Cibersegurança para Executivos	35

Nível A**50€****Mínimo 31 | Máximo 35 Formandos****Online | Híbrido | Presencial**

Fundamentos de Cibersegurança

Esta formação destina-se a profissionais de diversas áreas fornece conceitos básicos mas completos a nível operacional de um contexto de trabalho, com vista a reforçar conhecimentos de cibersegurança e a deteção e evasão de ameaças de cibersegurança.

Pré-requisitos: Conhecimentos de Informática na ótica do utilizador, conhecimentos básicos de Internet e navegação com browsers.

35 Horas

Módulos Ministrados:

1. Legislação aplicada à cibersegurança

- Leis, regulamentos e boas práticas em relação à proteção de dados
- Leis e regulamentos relevantes para a cibersegurança

2. Introdução à Cibernética

- Terminologia Cibernética
- Leis Cibernéticas
- Leis aplicáveis à exploração Cibernética

3. Introdução à Ciberhigiene

- Boas práticas
- Conceitos de segurança da informação
- Normas e procedimentos de utilização das tecnologias da informação

4. Tecnologias Digitais

- Tipos de dados
 - Armazenamento de dados
 - Estratégias de pesquisa e gestão do conhecimento
 - Operações básicas de computadores
 - Plataformas colaborativas e redes sociais
-

Nível A**50€****Mínimo 31 | Máximo 35 Formandos****Híbrido | Presencial**

Proteção e Privacidade de Dados

Esta formação permite adquirir conhecimentos ao nível da capacidade de avaliar impacto de privacidade de dados, conhecimento de normas e regulamentos relacionados com vários tipos de dados sensíveis e críticos, como dados de saúde ou na indústria de cartões de pagamento; da legislação geral das áreas fundamentais da organização; perceção e comportamento aderente à ética profissional e pessoal, e sua relação com aspetos de cibersegurança.

Pré-requisitos: Ser capaz de utilizar computadores, a internet, telemóveis e outros serviços online como o correio eletrónico.

35 Horas

Módulos Ministrados:

- 1. Dados Pessoalmente Identificáveis e Sensíveis**
 - Normas e boas práticas de segurança e privacidade de dados pessoalmente identificáveis e de dados sensíveis
- 2. Avaliação de Impacto de Privacidade**
 - Métodos de avaliação de impacto de privacidade (e.g., DPIA - Data Protection Impact Assessment)
- 3. Cartões de Pagamento**
 - Normas de segurança da indústria dos cartões de pagamento (PCI)
- 4. Dados Pessoais de Saúde**
 - Normas de segurança para dados pessoais de saúde.
- 5. Ética na Cibersegurança**
 - Leis, regulamentos, políticas e ética relacionados com a cibersegurança e a privacidade

OFERTA FORMATIVA

Nível B

_ FORMAÇÃO

50€

Mínimo 27 | Máximo 30 Formandos

Nível	Formação	Carga Horária
B	Formação para Responsável de (Ciber)Segurança	35
B	Formação Intermédia em Cibersegurança	35

Nível B**50€****Mínimo 27 | Máximo 30 Formandos****Híbrido | Presencial**

Responsável em (Ciber)Segurança

Forma profissionais de cibersegurança para os dotar de um conjunto de competências necessárias para auxiliar na gestão da cibersegurança de empresas, nomeadamente, planos de cibersegurança, inventariação de ativos e análise de risco, notificação de incidentes e legislação associada.

Pré-requisitos: Possuir formação ou experiência profissional em área relacionada com as tecnologias de informação e comunicação, conhecimentos do funcionamento de sistemas operativos e de redes de comunicação, e conhecimentos técnicos ao nível da segurança dos sistemas de informação.

35 Horas

Módulos Ministrados:

1. **Legislação aplicável à Cibersegurança**
2. **Frameworks CIS, COBIT, ISO/IEC, NIST,**
3. **Análise e gestão de risco**
4. **Ferramenta Monarc**
5. **Medidas técnicas e organizativas**
6. **Auditoria e monitorização da Cibersegurança**
7. **Inventário de ativos**
8. **Gestão de incidentes de cibersegurança**
9. **Política de Segurança da Informação (PSI)**
10. **Plano de Segurança**
11. **Relatório Anual de Cibersegurança**
12. **Plano para conformidade com o RJSC**
13. **Esquema de certificação QNRCS**
14. **Selo de maturidade digital da cibersegurança**

OFERTA FORMATIVA

Nível C

_ FORMAÇÃO 35h|50€ 70h|100€

Mínimo 22 | Máximo 25 Formandos

Nível	Formação	Carga Horária
C	Fundamentos de Redes de Computadores	35
C	Segurança de Redes	35
C	Gestão de Dados em Cibersegurança	70
C	Gestão de Informação em Cibersegurança	35
C	Criptologia	70
C	Dispositivos de Rede e Funcionalidades	35
C	Programação para Desenvolvimento de Software	70
C	Segurança de Sistemas	35
C	Sistemas de Gestão de Bases de Dados	35
C	Técnicas de Análise de Ataques	70
C	Tecnologias de Aplicações Web	35

OFERTA FORMATIVA

Nível D

_FORMAÇÃO 35h|50€ 70h|100€

Mínimo 22 | Máximo 25 Formandos

Nível	Formação	Carga Horária
D	Manutenção e Análise de Redes	35
D	Legislação, Política e Gestão de Ativos no Contexto da Cibersegurança	35
D	Princípios e Metodologias de Gestão de Risco	35
D	Administração de Sistemas em Rede	70
D	Engenharia de Software Seguro	70
D	Gestão de Risco Orientado à Organização	35
D	Metodologias para Tolerância a Falhas	70
D	Protocolos de Resposta a Incidentes	35
D	Segurança Aplicada a Sistemas de Informação	35

OFERTA FORMATIVA

Nível E

_FORMAÇÃO 35h|50€ 70h|100€

Mínimo 22 | Máximo 25 Formandos

Nível	Formação	Carga Horária
E	Recolha e Análise Forense de Dados	35
E	Ciberdefesa e Princípios Legislativos	35
E	Legislação Aplicada à Análise Forense	35
E	Fundamentos de Auditoria	35
E	Liderança Organizacional e Gestão de Recursos Humanos no Contexto da Cibersegurança	35
E	Organização Aplicada a Cibersegurança	35
E	Planeamento e Metodologias de Defesa	70

OFERTA FORMATIVA

Nível F

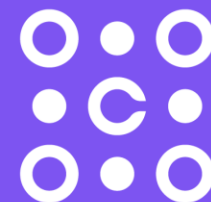
_FORMAÇÃO 35h|50€ 70h|100€

Mínimo 18 | Máximo 20 Formandos

Nível	Formação	Carga Horária
F	Gestão de Conhecimentos a Nível Organizacional no Contexto da Cibersegurança	35

O QUE É?

Um **selo de distinção** que marca o compromisso da organização com a qualificação e requalificação de recursos humanos, procurando a excelência na área da cibersegurança.



COMPROMISSO
CACADEMY

O QUE É?

Uma parceria que permite às organizações escolher a formação que pretendem e usufruir de turmas reservadas exclusivamente para os formandos identificados pela organização.



A **C-Academy** disponibiliza formação e identifica Instituições de Ensino Superior para ministrar as formações.



O **parceiro** angaria os formandos para as formações pretendidas.

Nomear um ponto de contacto

Identificar os formandos para pelo menos 3 turmas C-Academy até dezembro de 2025

Garantir a inscrição dos formandos

BENEFÍCIOS



Reforço da cibersegurança da organização, setor ou região



Valorização do Capital Humano



Reforço do compromisso com a organização e com a comunidade



Reconhecimento público na promoção da cibersegurança, com o recebimento do selo Compromisso C-Academy



Formações em cibersegurança certificadas e de elevada qualidade



Formadores altamente qualificados



Canal de comunicação privilegiado com a C-Academy, sendo disponibilizado um gestor de conta



Acesso a uma divulgação estruturada e com orientações definidas

Para esclarecer dúvidas, contacte:
C-Academy@cncs.gov.pt

www.cncs.gov.pt



Financiado pela
União Europeia
NextGenerationEU