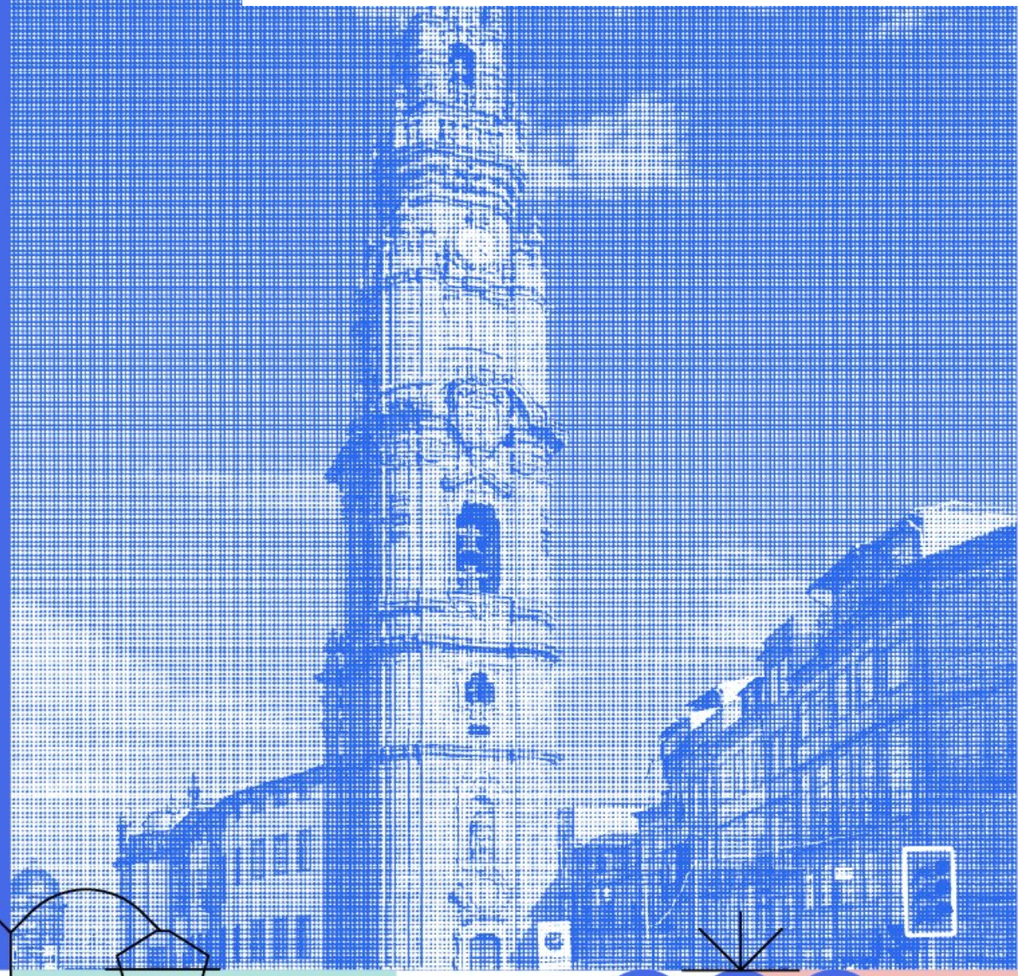
jornadas FCCN

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

NIS 2
Ensino Superior - e Agora!

Nuno Pires | npires@sp.ipl.pt



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

Evolução da Cibersegurança na UE

A jornada regulatória europeia na cibersegurança tem sido pautada por marcos importantes

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

jornadas FCCN

Da NIS à NIS 2: Cronologia dos Principais Diplomas

2016

Diretiva NIS (UE) 2016/1148

Medidas destinadas a alcançar um elevado nível comum de segurança das redes e dos sistemas de informação na União

2018

Regulamento de execução (UE) 2018/151

Estabelece normas de execução da Diretiva NIS aplicáveis a prestadores de serviços digitais

2018

Lei n.º 46/2018, RJSC

Estabelece o Regime Jurídico da Segurança do Ciberespaço, transpondo para o ordenamento jurídico português a Diretiva (UE) NIS

2021

Decreto-Lei n.º 65/2021

Regulamenta o Regime Jurídico da Segurança do Ciberespaço, definindo os requisitos de segurança e as regras para a notificação de incidentes.

2022

Regulamento n.º 183/2022

Regulamento que configura uma Instrução Técnica complementar ao Decreto-Lei n.º 65/2021 relativa a comunicações entre as entidades e o Centro Nacional de Cibersegurança

2022

Diretiva NIS 2 (UE) 2022/2555

Relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União

2025

Decreto-Lei n.º 125/2025

Aprova o Regime Jurídico da Cibersegurança, transpondo para o ordenamento jurídico português a Diretiva NIS 2 (UE) 2022/2555

Da NIS à NIS 2: Cronologia dos Principais Diplomas

Transposição da Diretiva NIS 2

O Decreto-Lei n.º 125/2025, de 4 de dezembro aprova o regime jurídico da Cibersegurança (RJC), transpondo a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, destinada a garantir um elevado nível comum de cibersegurança em toda a União.

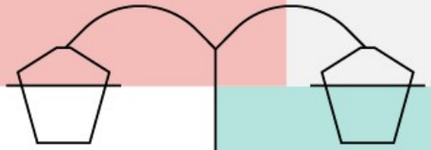
Entra em vigor 120 dias após publicação → **3 de abril de 2026**

jornadas FCCN

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

Requisitos e Diferenças

Principais diferenças face à Lei 46/2018 e DL 65/2021



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

Expansão do Âmbito de Aplicação

Legislação Anterior (Lei n.º 46/2018 e DL n.º 65/2021)

- Focada em **7 setores** considerados essenciais.
- Estes incluíam: **Energia, Transportes, Bancário, Infraestruturas do Mercado Financeiro , Saúde, Fornecimento e distribuição de Água, Infraestruturas Digitais**.
- Aplicado à Administração Pública de forma genérica
- O número de **entidades** identificadas enquanto **Operadores de Serviços Essenciais** era **na ordem das centenas.**

Nova Legislação (DL n.º 125/2025)

- O âmbito foi expandido drasticamente para **18 setores críticos**, abrangendo mais entidades e novos critérios (tamanho, criticidade, impacto).
- Novos setores incluem: **Gestão de Resíduos, Produção e Distribuição Alimentar, Indústria Transformadora, Produtos Químicos, Investigação e Desenvolvimento, Serviços Postais e de Estafetas, e Gestão de Resíduos**, entre outros.
- Nova classificação de entidades públicas relevantes do Grupo A ou B
- Esta expansão projeta um aumento para **uma ordem de milhares de entidades** abrangidas, enquanto entidades essenciais e importantes, incluindo inúmeras empresas de média e grande dimensão em novos domínios.

O **Decreto-Lei n.º 125/2025** representa uma alteração fundamental, passando de uma abordagem seletiva de proteção de setores chave para uma cobertura abrangente que engloba entidades identificadas como essenciais e criticas possam ser alvo de ciberataques. Esta expansão reflete uma compreensão mais alargada das dependências intersetoriais e da necessidade de resiliência digital em todo o ecossistema nacional.

Reforço das Obrigações

Legislação Anterior (Lei n.º 46/2018 e DL n.º 65/2021)

- Medidas de segurança genéricas
- Mecanismos de supervisão com ausência de especificação do modo de atuação por tipo de entidade
- Referência genérica à formação de recursos humanos
- Coimas máximas até €50.000

Nova Legislação (DL n.º 125/2025)

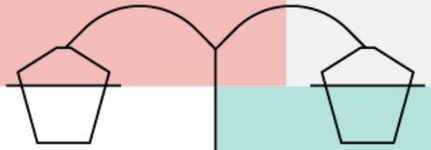
- Medidas de cibersegurança específicas e mínimas
- Mecanismo específicos de supervisão ex-ante (entidades essenciais) e ex-post (entidades importantes)
- Formação de recursos humanos obrigatória
- Medidas de cibersegurança relativas à cadeia de abastecimento
- Responsabilização dos Órgãos de Gestão, Direção e Administração
- Coimas máximas até €10M ou 2% do volume de negócios

jornadas FCCN

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

Qualificação de Entidades

Critérios e Mecanismos



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

Novas Categorias de Entidades

Entidades Essenciais

Grandes empresas, prestadores críticos e entidades da Administração Pública com elevada integração digital

Entidades Importantes

Médias empresas e outras entidades com impacto relevante mas não crítico

Entidades Públicas Relevantes

Administração Pública dividida em Grupo A (≥250 trabalhadores) e Grupo B (75-249 trabalhadores)

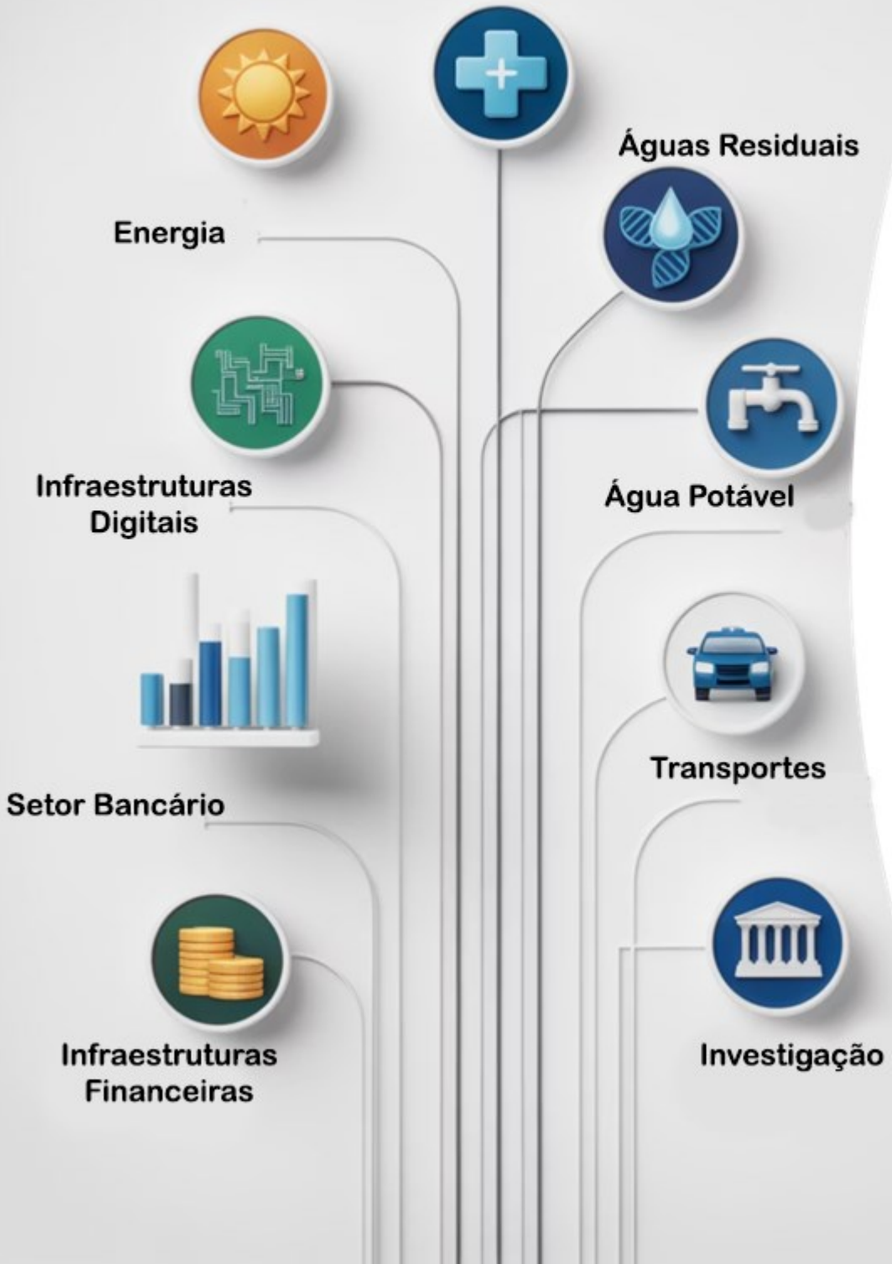
POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

Âmbito de Aplicação

jornadas FCCN

Setores Abrangidos

A legislação aplica-se a 18 setores críticos, incluindo:



Anexo I

1. Energia
2. Transportes
3. Setor bancário
4. Infraestruturas do mercado financeiro
5. Saúde
6. Água potável
7. Águas residuais
8. Infraestruturas digitais
9. Gestão de serviços de tecnologias da informação ou comunicação (entre empresas)
10. Espaço

Anexo II

1. Serviços postais e de estafeta
2. Gestão de resíduos
3. Produção, fabrico e distribuição de produtos químicos
4. Produção, transformação e distribuição de produtos alimentares
5. Indústria transformadora
6. Prestação de serviços digitais
7. Investigação

Administração Pública

1. Entidades Públicas Relevantes grupo A e grupo B

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

jornadas FCCN

Critérios de Qualificação

Dimensão da Entidade

Médias empresas (≥50 trabalhadores e volume de negócios/balanço ≥€10M) ou superiores são automaticamente abrangidas

Setor de Atividade

Pertença a um dos 18 setores críticos definidos nos Anexos I e II da legislação

Criticidade do Serviço

Prestação de serviços essenciais para atividades sociais ou económicas críticas

Impacto de Perturbação

Potencial afetação da segurança pública, proteção pública ou saúde pública

Risco Sistémico

Capacidade de gerar riscos consideráveis, especialmente com impacto transfronteiriço

Importância Regional

Criticidade a nível nacional ou regional para o setor ou serviços interdependentes

As **pequenas empresas** (<50 trabalhadores e negócios/balanço <€10M) e **micro empresas** (<10 trabalhadores e negócios/balanço<€2M), estão **excluídas do cumprimento do presento decreto-lei** (salvo as enquadráveis em critérios específicos).

Critérios de Qualificação

Entidades Públicas Relevantes: Grupo A

- Serviços da administração direta do Estado, central e periférica, com **250 ou mais trabalhadores.**
- Serviços da administração direta das Regiões Autónomas, central e periférica, com **250 ou mais trabalhadores.**
- Entidades da administração indireta do Estado, com **250 ou mais trabalhadores.**
- Entidades da administração indireta das Regiões Autónomas, com **250 ou mais trabalhadores.**
- Entidades da administração autónoma, com **250 ou mais trabalhadores.**
- Entidades públicas empresariais que **excedam os limiares de médias empresas** (Recomendação 2003/361/CE da Comissão).
- Entidades administrativas independentes.
- Conselho Económico e Social, Provedoria de Justiça, e serviços técnicos e administrativos da Presidência da República, Assembleia da República, Tribunais, Conselho Superior da Magistratura, Conselho Superior dos Tribunais Administrativos e Fiscais, Conselho Superior do Ministério Público.

Critérios de Qualificação

Entidades Públicas Relevantes: Grupo B

- Serviços da administração direta do Estado, central e periférica, com **75 a 249 trabalhadores**.
- Serviços da administração direta das Regiões Autónomas, central e periférica, com **75 a 249 trabalhadores**.
- Entidades da administração indireta do Estado, com **75 a 249 trabalhadores**.
- Entidades da administração indireta das Regiões Autónomas, com **75 a 249 trabalhadores**.
- Entidades da administração autónoma, com **75 a 249 trabalhadores**.
- Entidades públicas empresariais qualificadas como **empresas médias** (Recomendação 2003/361/CE da Comissão).

jornadas FCCN

Âmbito de Aplicação

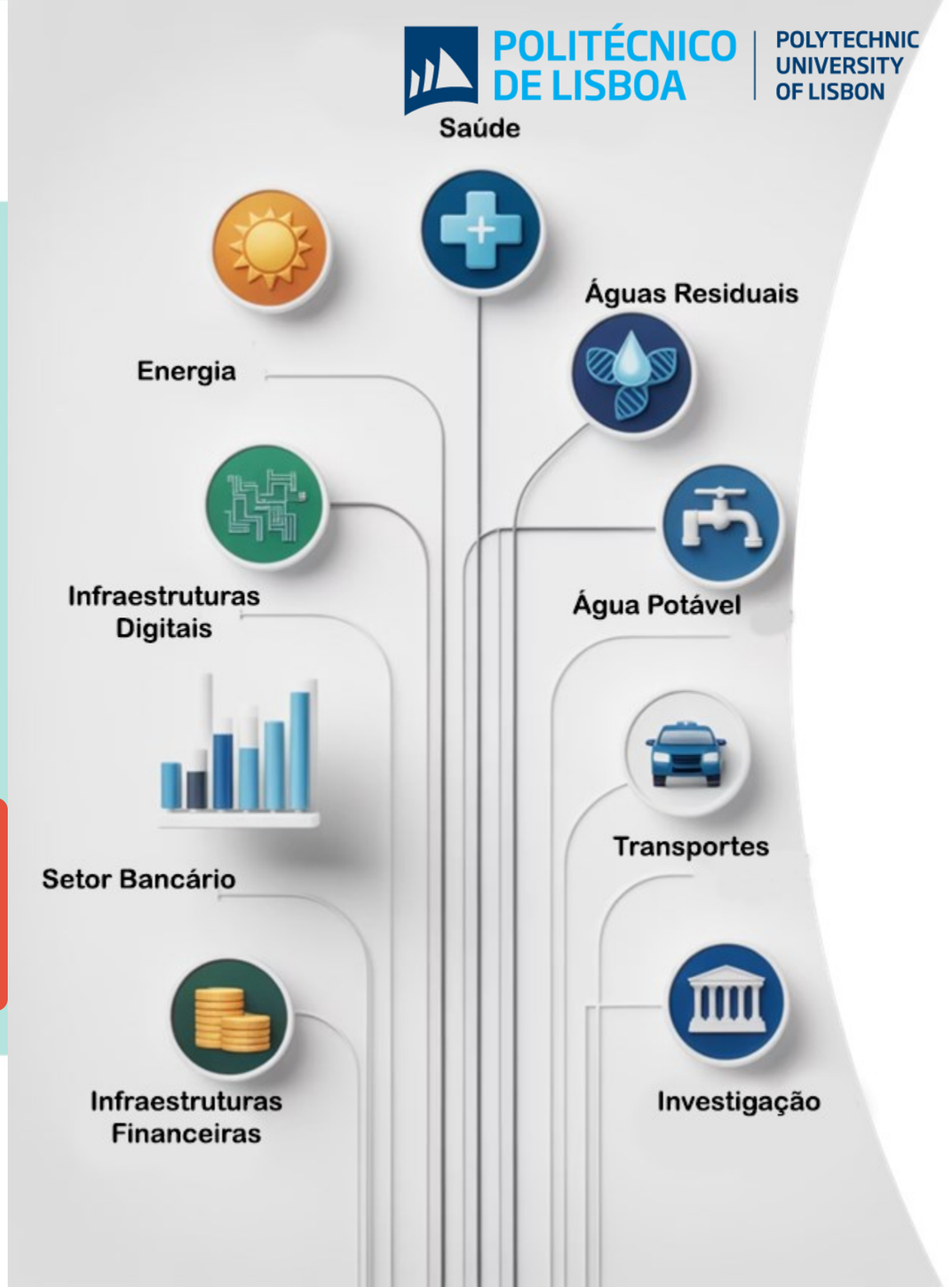
Entidades Abrangidas

Administração Pública:

- **(...)**
- **Instituições de Ensino Superior**

O Decreto-Lei n.º 125/2025 Artigo 3.º n.º 6

O presente decreto-lei aplica-se às instituições de ensino superior.

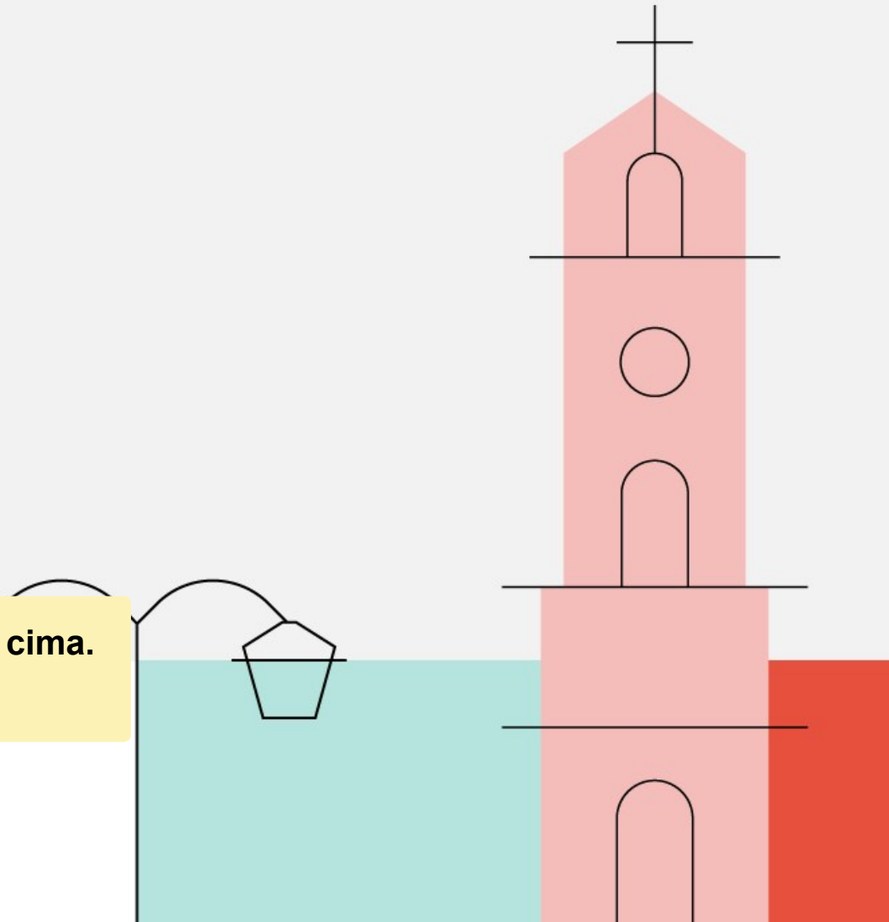


FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

Critérios de Qualificação

Instituições de Ensino Superior - Público

1. **Entidades Essenciais**
2. **Entidades Importantes**
3. **Entidades Públicas Relevantes – Grupo A**
4. **Entidades Públicas Relevantes – Grupo B**



⚠ **Se enquadrável simultaneamente em mais do que uma qualificação, é aplicada a ordem a cima.**

Ex.: Enquadrável como Essencial e Pública Relevante – qualificação será Entidade Essencial

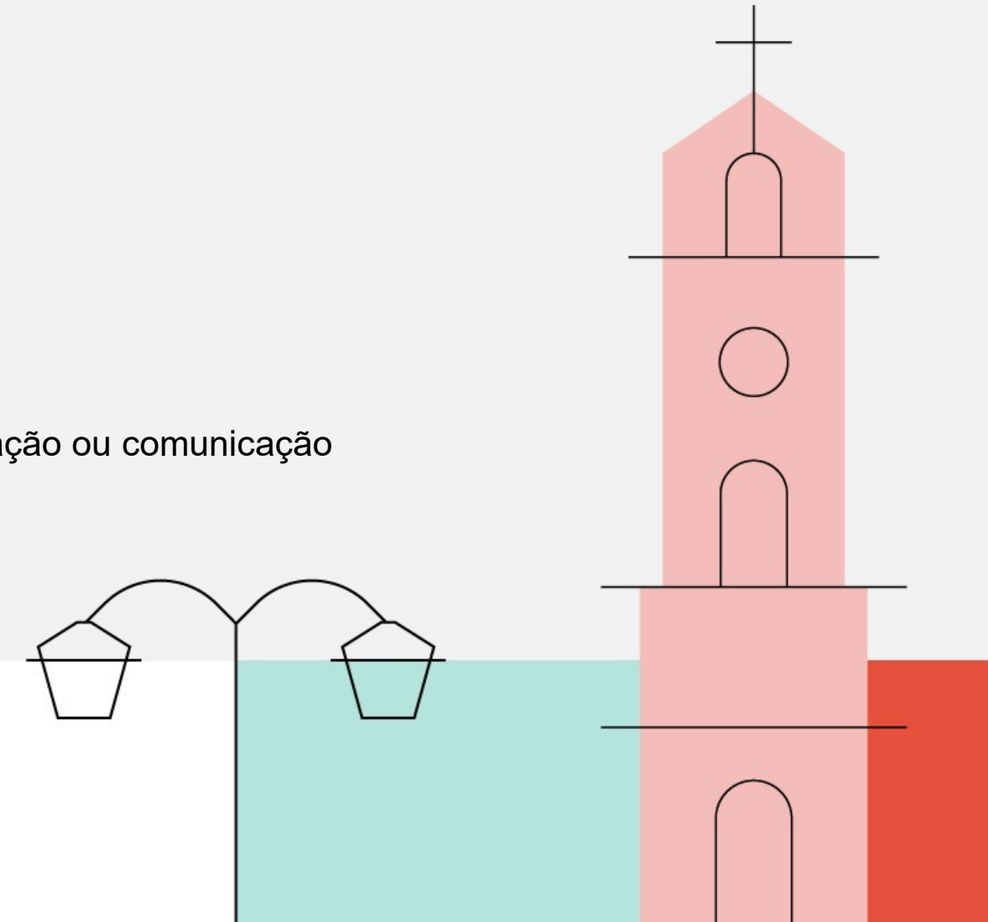
Critérios de Qualificação

Instituições de Ensino Superior - Público

- **Entidades Essenciais**

Anexo I - (≥ 250 trabalhadores)

1. Energia
2. Transportes
3. Setor bancário
4. Infraestruturas do mercado financeiro
5. **Saúde**
6. Água potável
7. Águas residuais
8. Infraestruturas digitais
9. Gestão de serviços de tecnologias da informação ou comunicação (entre empresas)
10. Espaço



Critérios de Qualificação

Instituições de Ensino Superior - Público

- **Entidades Importantes**

Anexo I - (50 a 249 trabalhadores)

1. Energia
2. Transportes
3. Setor bancário
4. Infraestruturas do mercado financeiro
5. **Saúde**
6. Água potável
7. Águas residuais
8. Infraestruturas digitais
9. Gestão de serviços de tecnologias da informação ou comunicação (entre empresas)
10. Espaço

Anexo II - (≥ 50 trabalhadores)

1. Serviços postais e de estafeta
2. Gestão de resíduos
3. Produção, fabrico e distribuição de produtos químicos
4. Produção, transformação e distribuição de produtos alimentares
5. Indústria transformadora
6. Prestação de serviços digitais
7. **Investigação**

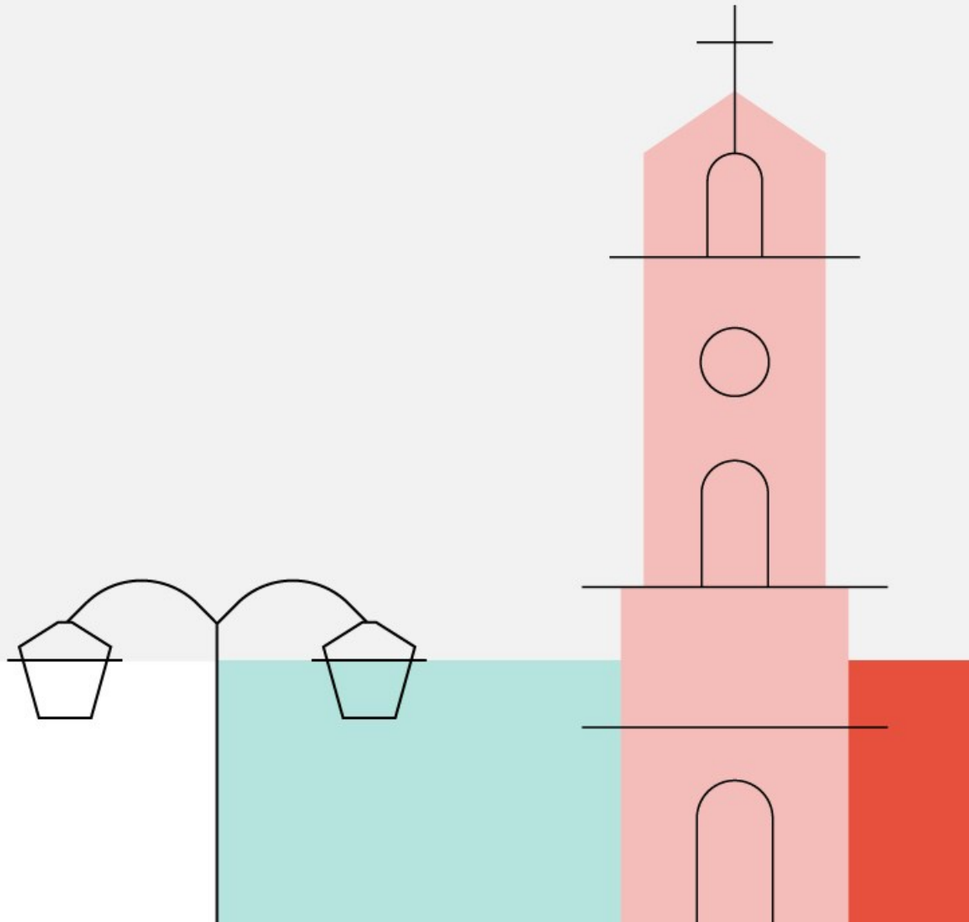
Critérios de Qualificação

Instituições de Ensino Superior - Público

- **Entidades Públicas Relevantes**

Grupo A - **(≥ 250 trabalhadores)**

Grupo B - **(75 a 249 trabalhadores)**



Critérios de Qualificação

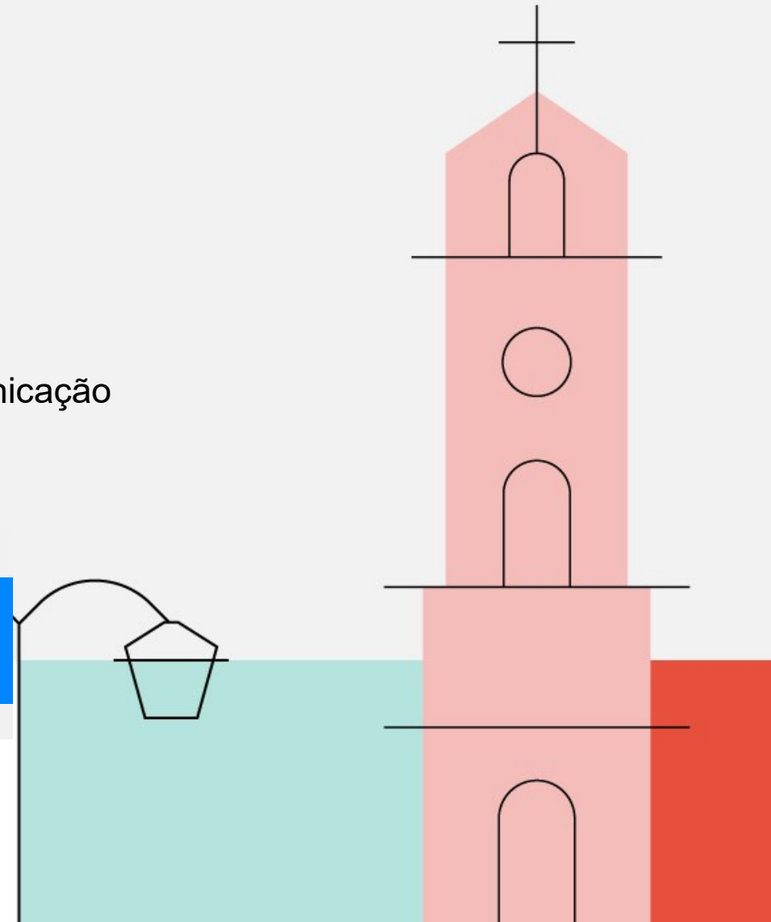
Instituições de Ensino Superior - Privado

- **Entidades Essenciais**

  Anexo I - (≥ 250 trabalhadores)

1. Energia
2. Transportes
3. Setor bancário
4. Infraestruturas do mercado financeiro
5. Saúde
6. Água potável
7. Águas residuais
8. Infraestruturas digitais
9. Gestão de serviços de tecnologias da informação ou comunicação (entre empresas)
10. Espaço

Entidades Importantes - se não enquadráveis como essenciais



Exemplo

Instituições de Ensino Superior - Público

Enquadramento	Setor	≥ 250 trabalhadores	50 – 249 trabalhadores	Entidades Públicas Relevantes Grupo A	Entidades Públicas Relevantes Grupo B
Anexo 1	(ex.) Saúde	Essencial	Importante		
Anexo 2	(ex.) Investigação	Importante	Importante		
Por Omissão	N/A			≥ 250 trabalhadores	75 – 249 trabalhadores

Instituições de Ensino Superior - Privado

Enquadramento	Setor	≥ 250 trabalhadores	50 – 249 trabalhadores	Grupo A	Grupo B
Anexo 1	(ex.) Saúde	Essencial	Importante		
Por Omissão	N/A	Importante	Importante		

Procedimento de Qualificação

Identificação e Registo Inicial

As entidades identificam-se e mantêm os seus dados atualizados numa plataforma eletrónica do **CNCS**, no prazo de 60 dias após a disponibilização da mesma.

Qualificação Automática

Para a maioria das a qualificação pelo **CNCS** é efetuada com base na informação fornecida na plataforma, resultando num mecanismo mais direto.

Qualificação Específica

Para casos mais complexos, a qualificação do **CNCS** é comunicada com 60 dias de antecedência e revista a cada dois anos, exigindo fundamentação do **CNCS** e audiência prévia da entidade.

Notificação da Qualificação

Após a qualificação, o **CNCS** (ou as autoridades setoriais competentes) notifica a entidade sobre a sua qualificação no prazo máximo de 30 dias.

Regulamentação e Conformidade

As regras de funcionamento da plataforma eletrónica serão definidas através de regulamento emitido pelo **CNCS**.

Este procedimento de qualificação não dispensa as entidades abrangidas, de cumprir com o dever de registo previsto no artigo 35.º

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

jornadas FCCN

Plataforma CNCS

Dados Essenciais para Registo: Nome, NIF, endereço, Correio eletrónico, gamas de endereços IP, números de telefone, número de trabalhadores, setor do Anexo I ou II (se aplicável), Estados-Membros da UE onde os serviços são prestados (se aplicável).

Autoidentificação

Submissão de um formulário digital com os dados essenciais para iniciar o processo de registo.

Qualificação

Análise dos dados pelo CNCS e comunicação da decisão de qualificação ou exclusão.

Acesso à Plataforma

Acesso da entidade à plataforma disponibilizado, com perfis atribuídos aos utilizadores da entidade.

Comunicação de obrigações

Submissão de relatórios, notificações de incidentes e comunicação de vulnerabilidades.

MY CIBER https://myciber.gov.pt

Monitorização

Visualização de indicadores e dashboards sobre o estado dos registos e atividades da entidade.

Gestão de alertas

Receção de notificações formais do CNCS por email, SPNE e na área de trabalho da plataforma.

Artigo 35.º - Todas as entidades essenciais, importantes e públicas relevantes devem registar-se na plataforma eletrónica do **CNCS** para garantir a sua identificação completa e facilitar a gestão da cibersegurança nacional.

jornadas FCCN

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

Responsabilidades dos Órgãos de Gestão, Direção e Administração

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

jornadas FCCN

Obrigações dos Órgãos de Gestão

A nova legislação estabelece responsabilidades claras e incontornáveis para Órgãos de Gestão, Direção e Administração das entidades essenciais e importantes.

Aprovação de Medidas

Aprovar as medidas de gestão dos riscos de cibersegurança adotadas pela organização.

Supervisão

Supervisionar a aplicação efetiva das medidas de gestão dos riscos de cibersegurança.

Cumprimento

Assegurar o cumprimento das medidas de supervisão e execução impostas pelas autoridades.

Formação

Garantir ações de formação regulares em cibersegurança para promover cultura interna.

Medidas de Cibersegurança

Artigo 27.º - Entidades Essenciais e Importantes devem adotar medidas de cibersegurança, considerando a sua matriz de risco, abrangendo as seguintes áreas:

Tratamento de Incidentes

Gestão eficaz de incidentes de cibersegurança.

Continuidade das Atividades

Inclui gestão de cópias de segurança, recuperação de desastres e gestão de crises.

Segurança da Cadeia de Abastecimento

Foco na segurança das relações com fornecedores e prestadores de serviços diretos.

Segurança de Redes e Sistemas de Informação

Desde a aquisição e desenvolvimento até à manutenção, incluindo tratamento de vulnerabilidades.

Avaliação de Eficácia

Políticas e procedimentos para avaliar a performance das medidas de gestão de riscos.

Ciber-Higiene e Formação

Práticas básicas e formação contínua em cibersegurança para todos os colaboradores, incluindo os Órgãos de Gestão, Direção e Administração.

Medidas de Cibersegurança

Artigo 33.º - Entidades Públicas Relevantes devem adotar as medidas de cibersegurança definidas pelo **CNCS**.

Dever de Cumprimento

As Entidades Públicas Relevantes são obrigadas a cumprir as medidas de cibersegurança estabelecidas pelo **CNCS**.

Regulamentação do CNCS

O **CNCS** define, por regulamento, as medidas de cibersegurança, adaptadas à proporcionalidade e ao grupo da entidade.

Sujeição a Supervisão e Execução

Estas entidades estão sujeitas às medidas de supervisão e execução previstas na nova legislação.

Anexo IV do Regulamento do RJC (em consulta pública até 22/04)

Medidas de cibersegurança para Entidades Públicas Relevantes Grupo B.

Medidas de cibersegurança para Entidades Públicas Relevantes Grupo A (cumulativas com as aplicadas ao Grupo B).

Contraordenações Muito Graves

(artigo 61.º)

Incluem incumprimento de medidas de cibersegurança, deveres de notificação e obrigações de responsáveis.

€10M

Entidades Essenciais

Até €10M ou 2% do volume de negócios anual mundial (pessoas coletivas)

€7M

Entidades Importantes

Até €7M ou 1,4% do volume de negócios anual mundial (pessoas coletivas)

€4M

Públicas Relevantes A

€16.000 a €4M(pessoas coletivas)

€350K

Públicas Relevantes B

€8.000 a €350K (pessoas coletivas)

€350 a €200.000

(pessoas singulares)

€500 a €16.000

(pessoas singulares)

Contraordenações Graves

(artigo 62.º)

Incluem incumprimento de ordens vinculativas, violação de suspensões e falta de registo.

€5M	€3.5M	€2.5M	€225K
Entidades Essenciais	**Entidades Importantes**	**Públicas Relevantes A**	**Públicas Relevantes B**
Até €5M ou 1% do volume de negócios anual mundial (pessoas coletivas)	Até €3.5M ou 0,7% do volume de negócios anual mundial (pessoas coletivas)	€10.000 a €2.5M(pessoas coletivas)	€5.000 a €225K (pessoas coletivas)

€250 a €125.000	€375a €10.000
(pessoas singulares)	(pessoas singulares)

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

jornadas FCCN

Contraordenações Leves

(artigo 63.º)

Incluem utilização indevida de grafismo, marca de certificação, omissão ou prestação de informação falsa.

€45K

Pessoas Coletivas

De €875,00 a €45.000,00

€3.75K

Pessoas Singulares

De €250,00 a €3.750,00

Negligência: As contraordenações referidas no n.º 1 do artigo 61.º, no n.º 1 do artigo 62.º e nas alíneas a) e b) do n.º 1 do artigo 63.º, são igualmente puníveis a título negligente, sendo os limites mínimos e máximos das coimas reduzidos a metade.

Responsabilidade Individual

⚠ Responsabilidade

Os titulares dos Órgãos de Gestão, Direção e Administração podem responder por ação ou omissão, com dolo ou culpa grave, pelas infrações previstas no decreto-lei.

Não Delegável

A responsabilidade e poderes necessários para o cumprimento destas obrigações **não podem ser delegados**, exceto num dos titulares dos órgãos de gestão, direção e administração.

Consequências

Responsabilidade civil e penal | Coimas até €200.000

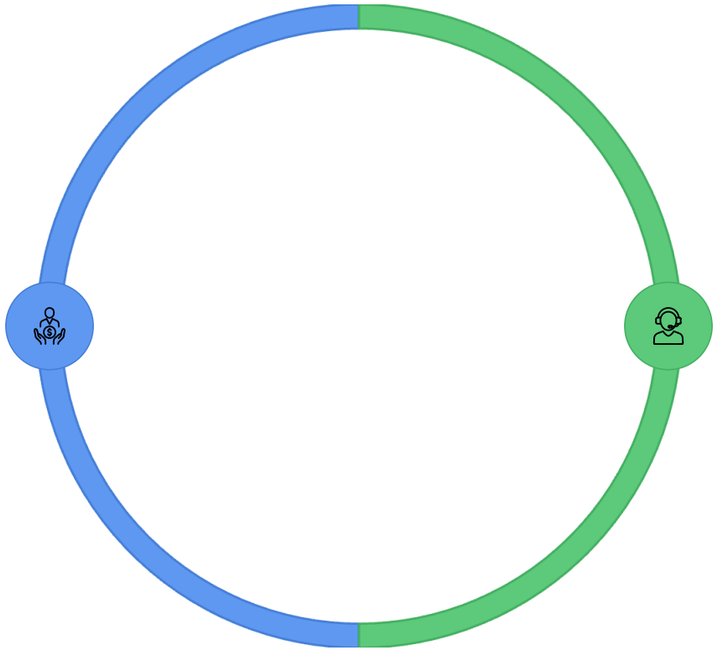
Interdição temporária de funções | Danos reputacionais

Recursos Humanos Obrigatórios

Responsável de Cibersegurança

Responda organicamente e de forma direta aos Órgãos de Gestão

Propõe medidas, presta informações e coordena ações.



Ponto de Contacto Permanente

Nível operacional e técnico e resposta a incidentes.

Pode ser uma pessoa ou equipa

As entidades devem assegurar que dispõem de meios de contacto principais e alternativos para a comunicação com o CNCS

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

jornadas FCCN

Formação e Sensibilização

Órgãos de Gestão, Direção e Administração

Formação sobre responsabilidades legais, gestão dos riscos estratégicos e tomada de decisão em cibersegurança

Equipas Técnicas

Formação especializada em tecnologias de segurança, resposta a incidentes e análise de ameaças

Colaboradores

Sensibilização para ciber-higiene, *phishing*, engenharia social e boas práticas de segurança

⚠ **A legislação exige ações de formação regulares para todos os níveis da organização, incluindo os Órgãos de Gestão, Direção e Administração.**

Produção de efeitos | Artigo 10.º do DL 125/2025

Medidas de cibersegurança

Ao que se referem o n.os 1 e 2 do artigo 27.º

Cadeia de abastecimento

Ao que se refere o artigo 28.º

Gestão do risco residual

Ao que se refere o artigo 29.º

Relatório anual

Ao que se refere o artigo 30.º

Medidas de cibersegurança aplicáveis às entidades públicas relevantes

Ao que se refere o artigo 33.º

Contraordenações muito graves

Ao que se referem as alíneas b), c) e f) do n.º 1 do artigo 61.º

Obs.: que resultam diretamente dos aqui apresentados

⚠ **24 meses após a publicação da regulamentação referida nos artigos 8.º, 14.º, 26.º, 31.º, 32.º e 83.º**

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

jornadas FCCN

Próximos Passos

01

Avaliação de lacunas

Identificar diferenças entre estado atual e requisitos legais.

02

Plano de Implementação

Desenvolver roteiro com prioridades, recursos e prazos.

03

Designação de Responsáveis

Nomear Responsável de Cibersegurança e Ponto de Contacto.

04

Registo e Qualificação

Inscrever na plataforma do **CNCS** e confirmar qualificação.

05

Implementação de Medidas

Executar medidas de cibersegurança mínimas e específicas.

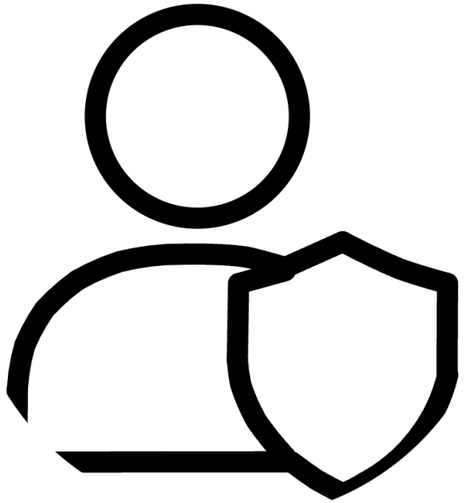
06

Monitorização e Melhoria

Acompanhar conformidade e promover melhoria continua.

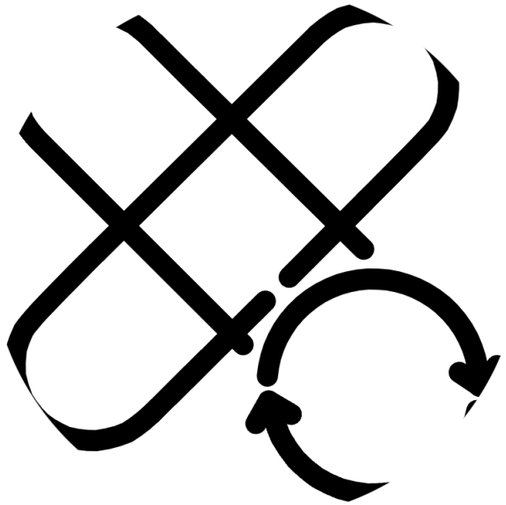
⚠ **Os Órgãos de Gestão, Direção e Administração devem liderar este processo, garantindo recursos adequados e compromisso organizacional com a cibersegurança.**

Proteção e Resiliência



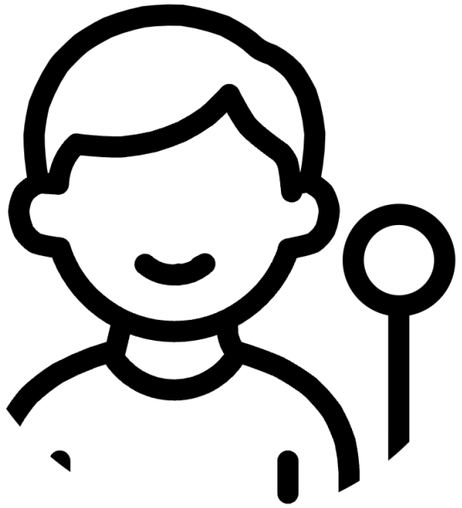
Redução de Riscos

Implementação sistemática de medidas de cibersegurança reduz significativamente a probabilidade e impacto de incidentes



Capacidade de Recuperação

Planos de continuidade e recuperação garantem retoma rápida das operações após incidentes



Deteção Precoce

Sistemas de monitorização permitem identificar e responder a ameaças antes que causem danos significativos

jornadas FCCN

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

Para informações mais detalhadas:

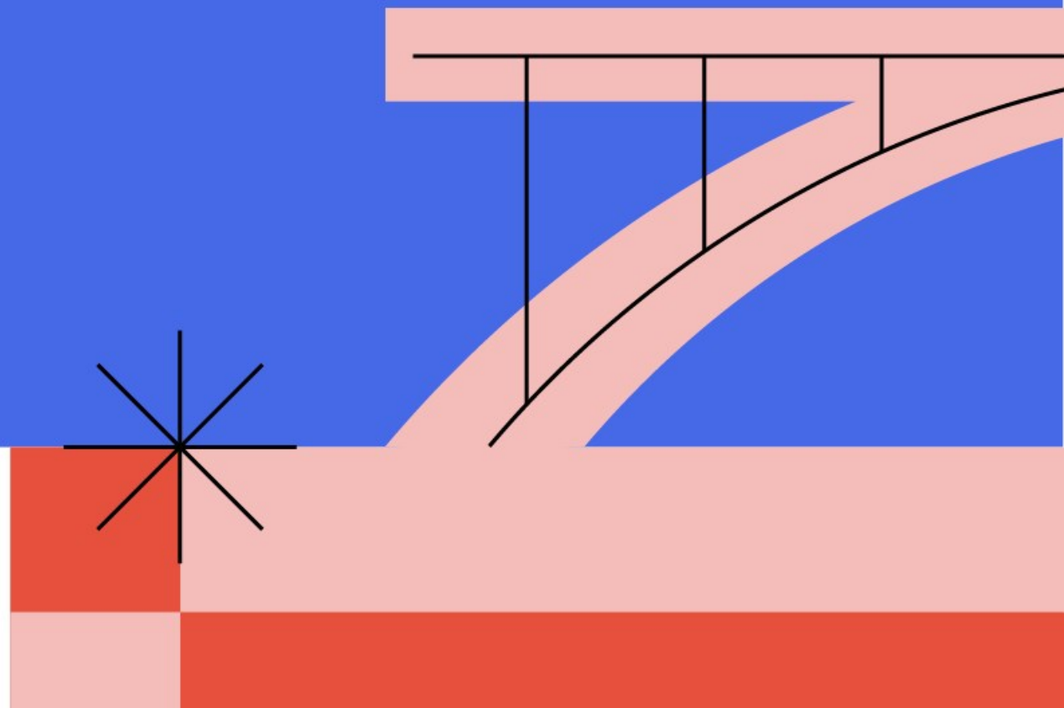
CNCS / C-Academy: Formação gratuita - Roteiro NIS 2

https://www.c-academy.pt

Obrigado!

Nuno Pires | npires@sp.ip.pt

jornadas.fccn.pt | fccn.pt



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | U.PORTO | U.PORTO FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO