Elemento Humano - Formação e Prevenção

Mestrado em Auditoria

Auditoria a Sistemas de Informação e Tecnologias Aplicadas

Elemento Humano

Formação e Prevenção

Enquadramento

Os SI são fundamentais para o sucesso da Sociedade de Informação

Apatia, ignorância ou não consciência em relação à segurança e iliteracia tecnológica são as maiores ameaças

Elemento Humano

Formação e Prevenção

Enquadramento

Consciencialização é o ponto de partida

Necessidade de **Programas de capacitação de cidadãos** em cibersegurança

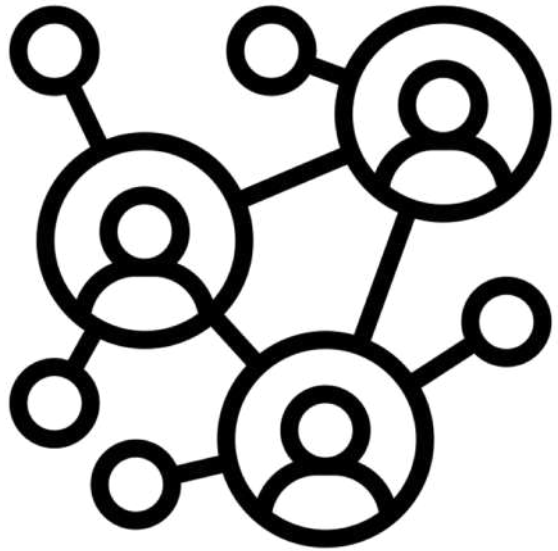
Elemento Humano

Formação e Prevenção

Enquadramento

Esta **componente humana** deve integrar toda a estratégia de cibersegurança.

Sem o **fortalecimento** do fator humano, a cibersegurança mantém-se **incompleta**.



Elemento Humano

Formação e Prevenção

Problema

Os utilizadores são frequentemente designados como "o elo mais fraco”

Os comportamentos de risco dos utilizadores são responsáveis por muitos ataques de cibersegurança

Alguns tipos de comportamento de risco resultam em falhas de segurança

Elemento Humano

Formação e Prevenção

Problema

Os **funcionários** podem ser considerados como a primeira linha de defesa da organização contra o cibercrime e incidentes de Cibersegurança

As organizações podem não conseguir eliminar completamente o risco de cibersegurança

Os incidentes de cibersegurança continuam a aumentar em frequência e sofisticação

Elemento Humano

Formação e Prevenção

Benchmarking

Bélgica - Parceria público-privada- ICC Bélgica, FEB, EY, Microsoft, L-SEC, B-CCENTRE e ISACA Bélgica

França - Agência Francesa de Segurança dos Sistemas de Informação - ANSSI

Reino Unido – Cyber Essentials - UK Government

EUA - Instituto Nacional de Ciência e Tecnologia (NIST)

Elemento Humano

Formação e Prevenção

Bons exemplos em Portugal

Centro Internet Segura – Portugal

Guarda Nacional Republicana (GNR) - CyberGNRation

Instituto de Informática, I.P

Jerónimo Martins

LIDL

....

Recorrentemente o RASI sugere maior intervenção na sensibilização

Elemento Humano

Formação e Prevenção

Políticas Públicas

InCode 2030

Simplex +

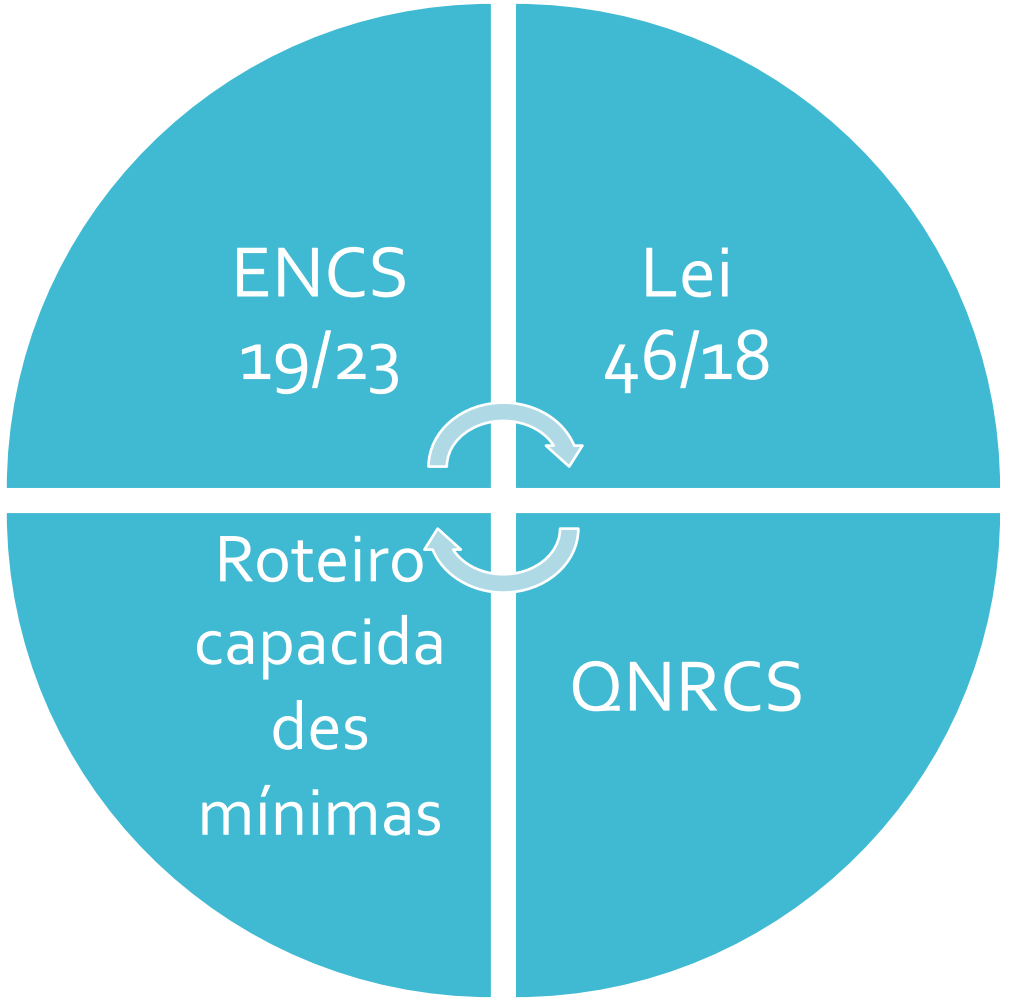
Estado da União 2017

Cyber Act

Elemento Humano

Formação e Prevenção

Políticas Públicas - contributo CNCS



Cadernos do Observatório (referência)

Elemento Humano

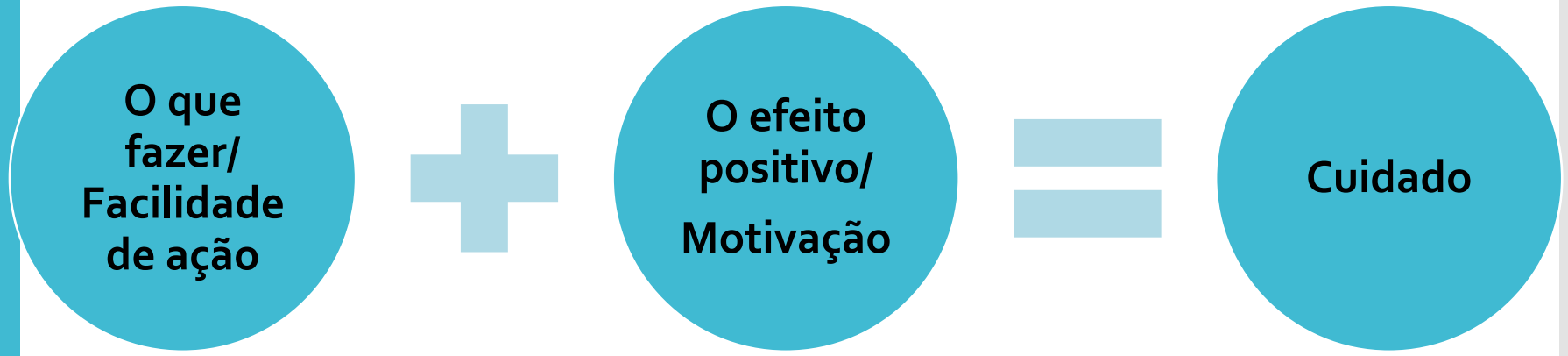
Formação e Prevenção

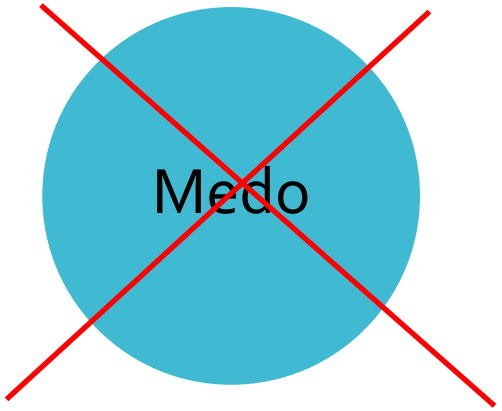
Considerando os bons estudos, o que fazer para fortalecer o elemento humano?

Elemento Humano

Formação e Prevenção

1. A sensibilização deve centrar-se nas **boas práticas** e no seu **efeito positivo** e não no medo.





Elemento Humano

Formação e Prevenção

Exemplo de **o que fazer** em relação à definições de privacidade do **Facebook.**

1º passo: no canto superior esquerdo, clicar em "Privacidade".

2º passo: na lista, restrinja quem pode ver as suas publicações, controle as publicações que o identificam, limite o público das publicações antigas, limite quem pode visualizar os seus amigos, limite a possibilidade de ser encontrado através de email e telefone e evite que as ferramentas de pesquisa fora do Facebook apresentem ligações para o seu perfil.

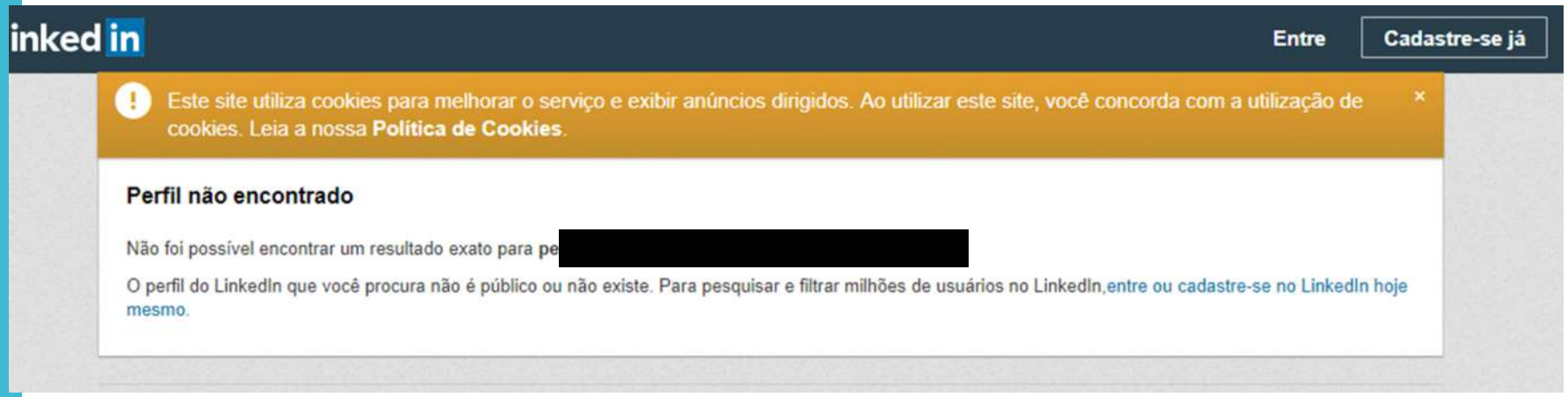
Definições e ferramentas de privacidade

A tua atividade	Quem pode ver as tuas publicações futuras?	Amigos	Editar
	Rever todas as tuas publicações e coisas em que te identificaram		Usar registo de atividade
	Limitar o público de publicações que partilhaste com amigos de amigos ou o Público?		Limitar publicações antigas
Como as pessoas podem encontrar-te e contactar-te	Quem pode enviar-te pedidos de amizade?	Todos	Editar
	Quem pode ver a tua lista de amigos? Não te esqueças: os teus amigos controlam quem pode ver a sua própria lista de amigos nas suas cronologias. Se as pessoas puderem ver a tua amizade noutra cronologia, vão poder vê-la no Feed de Notícias, nas pesquisas e noutros locais do Facebook. Se definires isto para Apenas eu, só tu vais poder ver a tua lista completa de amigos na tua cronologia. As restantes pessoas veem apenas os amigos em comum.	Apenas eu	Editar
	Quem pode encontrar-te através do endereço de e-mail que registaste?	Amigos	Editar
	Quem pode encontrar-te através do número de telemóvel que registaste?	Amigos	Editar
	Queres que as ferramentas de pesquisa fora do Facebook apresentem uma ligação para o teu	Não	Editar

Elemento Humano

Formação e Prevenção

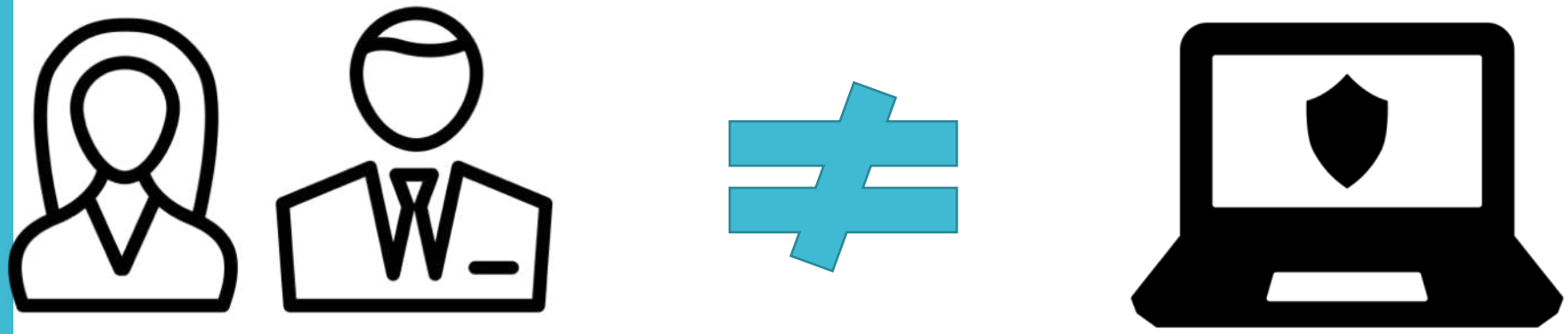
Exemplo de efeito positivo que se pode mostrar em relação a Linkedin (depois de tornar as definições de privacidade mais restritas).



Elemento Humano

Formação e Prevenção

2. Pouca relação entre **perfis específicos** (com base no género, classe, profissão, estilo de vida) e sensibilização para **comportamentos** mais ou menos seguros.



Elemento Humano

Formação e Prevenção

3. É mais eficaz as **organizações** **promoverem a adesão** à cibersegurança com **participação ativa** do que forçarem a conformidade com normas.

Participação e cocriação

Elemento Humano

Formação e Prevenção

Exemplo de **cocriação** usado no programa de **sensibilização** do CNCS.

Elemento Humano

Formação e Prevenção

4. A **cibersegurança** nas organizações só é percecionada como importante se **não colidir com o valor da produtividade**.

Elemento Humano

Formação e Prevenção

5. Sacrifica-se muitas vezes a **usabilidade a favor da segurança** – isso é negativo para o fator humano, devendo criar-se um **equilíbrio.**

Elemento Humano

Formação e Prevenção

6. As diferentes **áreas disciplinares**, desde as técnicas às sociais, devem **trabalhar em conjunto**, dialogando.

Que **tecnologia**?

Que **comportamento**?

Como **comunicar**?

Como **gerir**?

Que **lei**?

Como **reagir**?

Elemento Humano

Formação e Prevenção

7. O fator humano deve ser **articulado com as capacidades técnicas** – não basta fortalecer o humano, há soluções que são **técnicas**.

Por exemplo, um bom sistema de filtragem de ***spam*** deve acompanhar os cuidados comportamentais com o *email*.

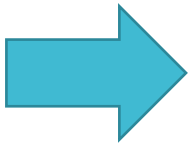
Pau Casals

Elemento Humano

Formação e Prevenção

8. É essencial **avaliar os resultados** das campanhas de **sensibilização**, usando vários métodos e adaptando a cada caso.

Observação;
Etnografia;
Inquéritos;
Entrevistas;
Análise de Dados



- Multinacionais
- PMEs
- Instituições públicas
- Infraestruturas críticas/ Serviços essenciais
- Espaço doméstico
- Espaço público

Elemento Humano

Formação e Prevenção

9. Alguns **conselhos** a vários **agentes**.

Políticos e gestores	• Valorizar a aquisição de competências e a aprendizagem por **exemplo**;
CISOs	• Reforçar as suas ***soft skills*** na relação com os outros trabalhadores;
CSIRTs/CERTs/ SOCs	• Ter esquipas **multidisciplinares** e investir no **desenvolvimento pessoal** dos trabalhadores – há muitos *burnouts* neste contexto;
Developers e seus educadores	• Promover a ***security by design*** e a obrigatoriedade desta componente na formação.

Elemento Humano

Formação e Prevenção

Balanço/

Que estratégias a partir daqui?

- Criar **conteúdos de sensibilização** com instruções sobre **o que fazer**;
- **Massificar** estes conteúdos;
- **Envolver** trabalhadores na criação de **normas**;
- Integrar **segurança nos KPIs**;
- Promover a **usabilidade** da segurança;
- Melhorar a **comunicação** entre departamentos;
- Valorizar ***soft skills*** e **sensibilizar chefias**;
- **Não negligenciar as soluções técnicas…**

Elemento Humano

Formação e Prevenção

Educação
Formação
Sensibilização
(capacitação)

Educação- aquisição e compreensão de conhecimentos, através das quais as competências são desenvolvidas

Formação – ensinar competências que permitam o desempenho de funções específicas

Capacitação- focar a atenção num problema onde é necessário a perceção e adequação de comportamento

Programas de capacitação em cibersegurança, robustos e transversais a todas as organizações e ao cidadão comum, são essenciais para abordar esta preocupação

Elemento Humano

Formação e Prevenção

Programa de capitação em cibersegurança

Planear, desenvolver e implementar um programa de capacitação em cibersegurança

Deve suportar as necessidades nacionais

Qual o **comportamento** que pretendemos fortalecer?

Após implementar

Avaliação e Feedback

Gerir a mudança

Elemento Humano

Formação e Prevenção

Desenvolver o Programa de capacitação em Cibersegurança para Cidadãos

Uma organização **é tão mais segura**, do ponto de vista da segurança dos SI e da informação, quanto mais consciente dos riscos estiveram os trabalhadores da mesma

Educar, formar, capacitar, consciencializar e sensibilizar os colaboradores e os cidadãos para os comportamentos adequados a uma cultura organizacional de cibersegurança **é a base** para fortalecer as organizações.

Elemento Humano

Formação e Prevenção

É imperativo que os **Estados respondam**

O E-Learning - método de aprendizagem comumente utilizado e massificado

Os incidentes de cibersegurança não discriminam organizações nem cidadãos

Elemento Humano

Formação e Prevenção

O fator humano, nomeadamente os comportamentos, são **fundamentais** e **transversais**, devendo ser tomados em linha de conta na cibersegurança

Todos os segmentos da sociedade (funções profissionais) necessitam de consciencialização

Foco nas **competências de cibersegurança** que qualquer trabalhador ou cidadão **deve possuir**

Elemento Humano

Formação e Prevenção

	Organizativa /Gestão	Económica	Legal	Técnica	Comportamental
Alta direção/ Administração	A	M	M	B	A
Direção intermédia	M	A	M	B	A
Gestor técnico (TIC)	B	B	B	A	A
Gestor Funcional (área financeira, recursos humanos, compras, logística, …)	B	M	A	M	A
Funcionário / cidadão			B	B	M

Legenda: A – Alto, M- Médio, B- Baixo

Elemento Humano

Formação e Prevenção

Políticas Públicas

É imperativo que os **Estados** **respondam:**

Estratégia Nacional de Segurança do Ciberespaço 2019-2023

InCode2030

SIMPLEX +

Regime Juridico de Segurança do Ciberespaço

Quadro Nacional de Referência para a Cibersegurança

Roteiro para Capacidades Mínimas de Cibersegurança

Elemento Humano

Formação e Prevenção

ENSC 2019-2023

O que é?

Aprovada no anexo da **Resolução do Conselho de Ministros n.º 92/2019**, de 5 de junho

Responder à evolução tecnológica ocorrida entre 2015 e 2019

"tornar Portugal um país mais **seguro e próspero**, através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade"

Elemento Humano

Formação e Prevenção

ENSC 2019-2023

O que é?

Plano de Ação cuja responsabilidade de coordenação da elaboração, do acompanhamento da execução e da sua revisão é atribuída ao CNCS, "em articulação e estreita cooperação com todas as entidades com responsabilidade no âmbito da segurança do ciberespaço"

O Plano de Ação criou oportunidades de reflexão, **aproximar pessoas e organizações**, clarificar objetivos, promover alinhamento, fomentar a apropriação e responsabilização, definir e reorientar prazos, identificar boas práticas e casos de sucesso.

Elemento Humano

Formação e Prevenção

ENSC 2019-2023

O que é?

Compete ao **Conselho Superior de Segurança do Ciberespaço** "elaborar anualmente, ou sempre que necessário, relatório de avaliação da execução da Estratégia Nacional de Segurança do Ciberespaço" (Lei n.º 46/2018 de 13 de agosto)

Elemento Humano

Formação e Prevenção

ENSC
2019-2023

Objetivos Estratégicos

Objetivo estratégico 1 — Maximizar a resiliência

Fortalecer e garantir a resiliência digital nacional potenciando a inclusão e a colaboração em rede de forma a salvaguardar a segurança do ciberespaço de interesse nacional face às ameaças que possam comprometer ou provocar a disrupção das redes e sistemas de informação essenciais à sociedade

Elemento Humano

Formação e Prevenção

ENSC

2019-2023

Objetivos Estratégicos

Objetivo estratégico 2 — Promover a inovação

Fomentar e potenciar a capacidade nacional de inovação afirmando o ciberespaço como um domínio de desenvolvimento económico, social, cultural e de prosperidade

Elemento Humano

Formação e Prevenção

ENSC

2019-2023

Objetivos Estratégicos

Objetivo estratégico 3 — Gerar e garantir recursos

Contribuir para obter e garantir a alocação de recursos adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço

Elemento Humano

Formação e Prevenção

ENSC 2019-2023

Eixos de Intervenção

Eixo 1 — Estrutura de segurança do ciberespaço

Eixo 2 — Prevenção, educação e sensibilização

Eixo 3 — Proteção do ciberespaço e das infraestruturas

Eixo 4 — Resposta às ameaças e combate ao cibercrime

Eixo 5 — Investigação, desenvolvimento e inovação

Eixo 6 — Cooperação nacional e internacional

Elemento Humano

Formação e Prevenção

InCode2030

Criação de novas competências digitais orientadas para o futuro e para as novas oportunidades

Lançado pelo XXI Governo, 2017

Programa integrado de **competências digitais**, que pretende que Portugal responda a três principais desafios, entre 2017-2030:

Elemento Humano

Formação e Prevenção

InCode2030

"Garantir a literacia e a inclusão digitais para o exercício pleno da cidadania

Estimular a empregabilidade e especialização em tecnologias e aplicações digitais para a qualificação do emprego e uma economia de maior valor acrescentado

Produzir novos conhecimentos nas áreas digitais em cooperação internacional".

Elemento Humano

Formação e Prevenção

InCode2030

A crescente exigência das competências digitais para o exercício de diferentes profissões obriga a que na população ativa, variáveis como a **aprendizagem**, a **produtividade** e a **competitividade** estejam cada vez mais dependentes das TIC.

Elemento Humano

Formação e Prevenção

SIMPLEX +

Eixo da Inclusão e da Qualificação

Objetivo primordial - facilitar a vida dos cidadãos e das empresas no relacionamento com a Administração Pública

O programa visa

alterar processos e **simplificar** e/ou **eliminar procedimentos** pouco eficientes que se encontrem inseridos nas leis e regulamentos que agora vigoram.

Através de **referenciais** e de **ferramentas** para os atingir

Referenciais

- Quadro Nacional de Referência para a Cibersegurança
- Quadro de Avaliação das Capacidades de Cibersegurança

Ferramentas

- Ferramenta Web de Autoavaliação
- Roteiro para as Capacidades Mínimas

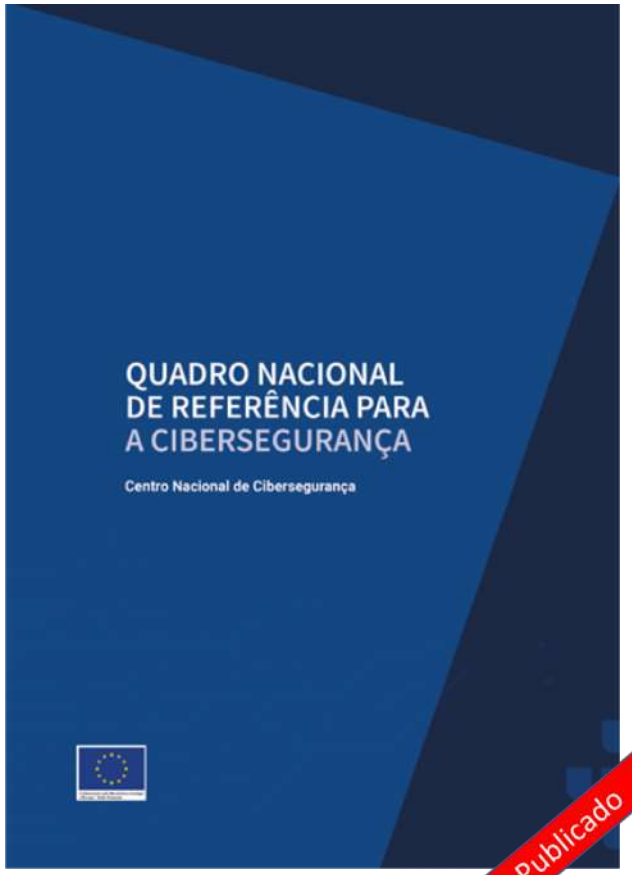
Quadro Nacional de Referência para a Cibersegurança

Disponibiliza medidas de segurança que traduzem objetivos;

Referencia exemplos e orientações;

Não é uma lista de controlo de ações a realizar;

É um suporte ao processo de gestão do risco de cibersegurança.



https://www.cncs.gov.pt/content/files/cncs_qnrcs_[illegible].pdf

Quadro Nacional de Referência para a Cibersegurança

Objetivos de cibersegurança a atingir

Quadro de Avaliação das Capacidades de Cibersegurança

Inicial

Intermédio

Avançado

Para cada uma das **103 medidas** traduzidas nos **5 objetivos** de segurança, foram identificados **3 níveis de capacidade**

https://www.cncs.gov.pt/content/files/cncs_quadrodeavaliacao_3.pdf

Quadro de Avaliação das Capacidades de Cibersegurança

Inicial

Iniciativas ad-hoc, predominam ações **isoladas** e **pouco formais**.

Intermédio

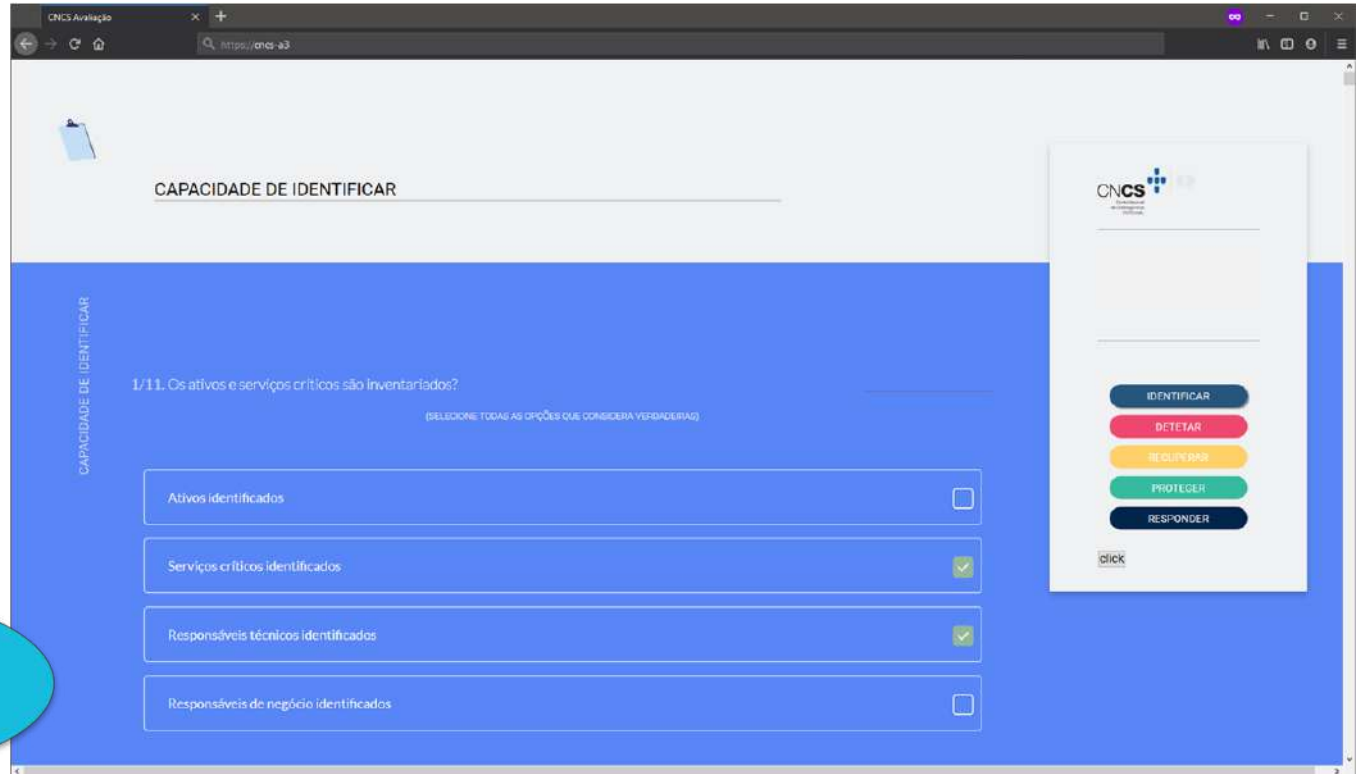
Atende-se à **maioria dos casos e necessidades,** as medidas são atingidas **formalmente**.

Avançado

Envolve a **monitorização contínua** dos controlos, **avaliação** e **revisão** recorrentes, **melhoria proativa**.

Ferramenta Web de Autoavaliação

Pretende ser um instrumento para, através de uma **plataforma *online***, aferir o **estado** de uma organização em termos de cibersegurança, considerando o QNRCS e o QACC.



Em desenvolvimento

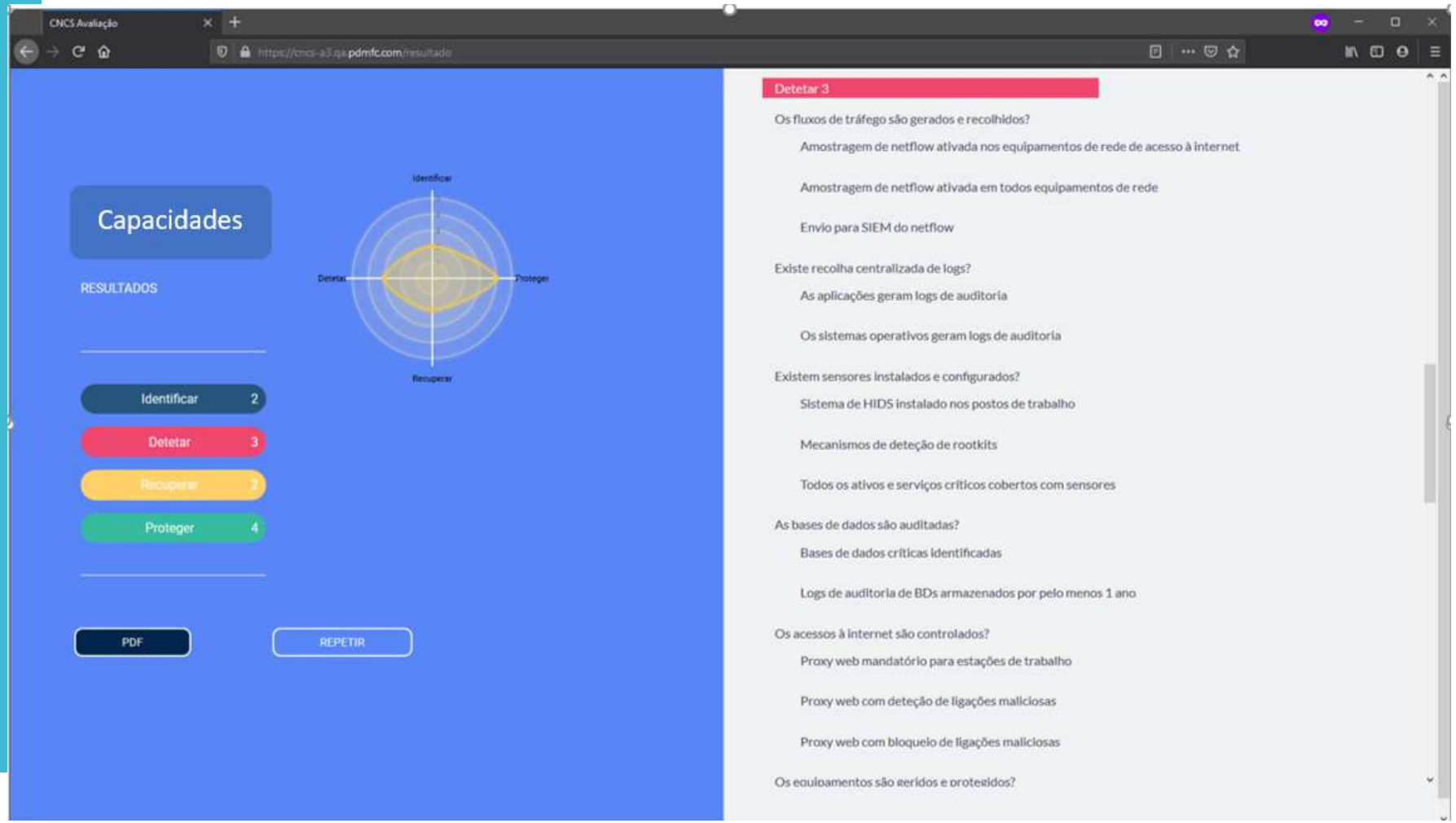
Ferramenta Web de Autoavaliação

Funcionamento do *website*

Resposta a questões

Verificação de conformidade

Resultados



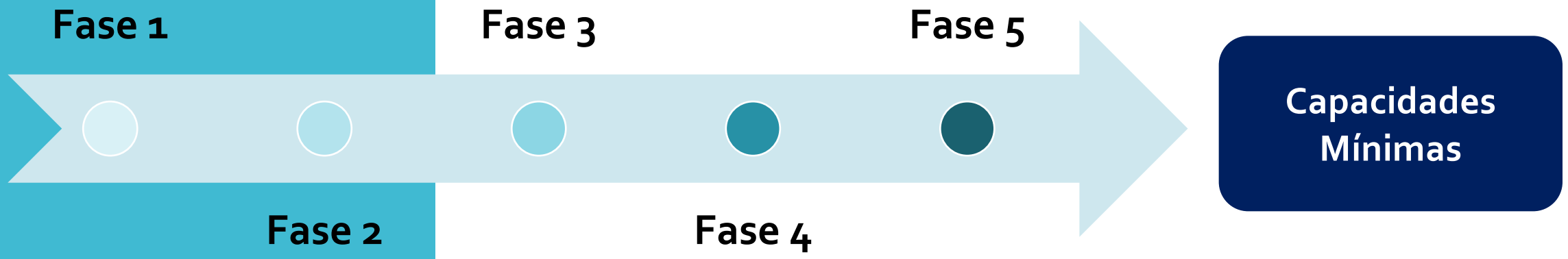
Roteiro para Capacidades Mínimas de Cibersegurança

- Este roteiro permite o **desenvolvimento progressivo** de cada uma das organizações relativamente ao seu grau de capacidades, percorrendo um conjunto de fases numeradas **de 1 a 5**

- Corresponde **aos primeiros passos** para uma organização estar em conformidade com os níveis mínimos de cibersegurança.

https://www.cncs.gov.pt/content/files/cncs_roteiro_capacidades_minimas_ciberseguranca.pdf

Roteiro para Capacidades Mínimas de Cibersegurança



Em cada uma das fases, são identificadas ações necessárias para as capacidades mínimas, articulando com o QNRCS, numa lógica de **progressão guiada**.

Conclusões

A Cibersegurança deve ser uma prioridade para as organizações;

A disponibilização de referenciais e ferramentas aumentam a capacidade das organizações;

Os referenciais servem para mapear as principais competências a adquirir;

As ferramentas têm o propósito de guiar as organizações no processo de aquisição dessas competências.