A Cibersegurança na Saúde

Estado atual e perspectivas de futuro

Lino Santos
Centro Nacional de Cibersegurança

A Cibersegurança
hoje

A **transição digital** exige segurança

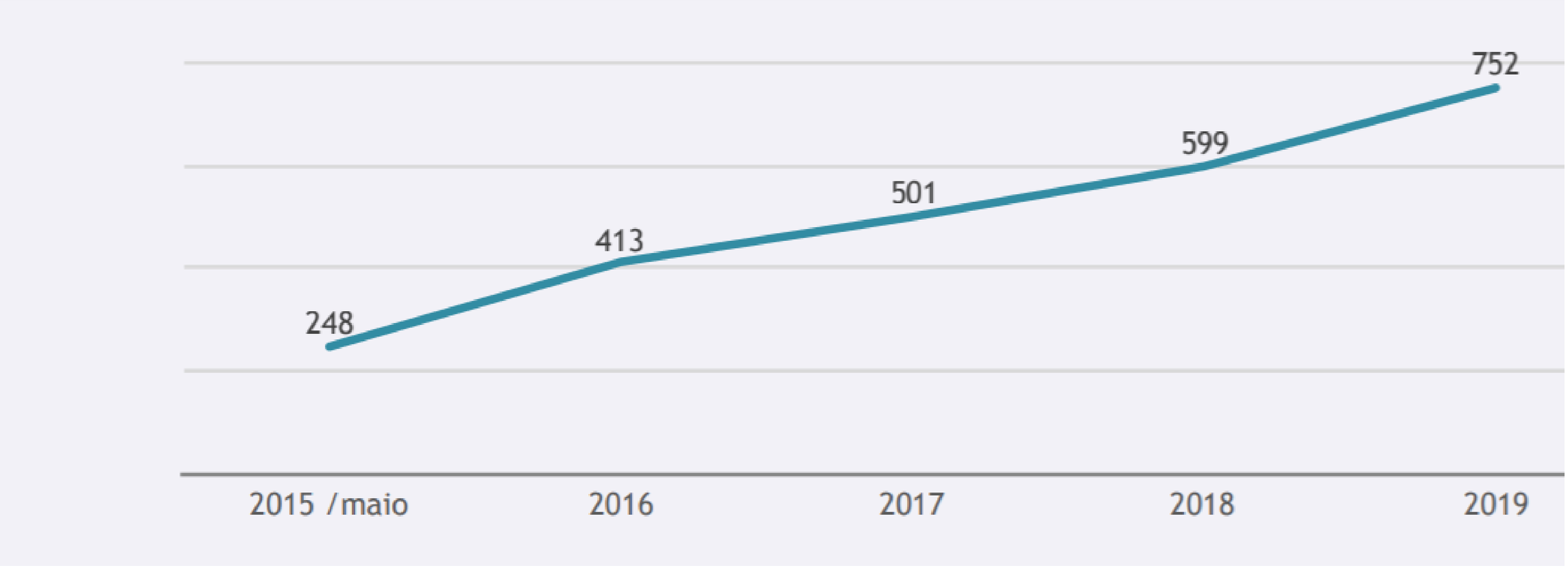
O digital como **substituição do presencial** aumenta os riscos

O digital cria **novas ameaças**

As **ameaças *offline* transferem-se** para o *online*

A cibersegurança é um **pilar** da democracia, da economia e da sociedade

Total de incidentes registados pelo CERT.PT
2015 -2019



Nota metodológica: esta tendência também é explicada pelo facto de o CNCS ter ganho mais conhecimento por parte da comunidade, logo esta tender a reportar mais incidentes.

(CNCS, 2020a)

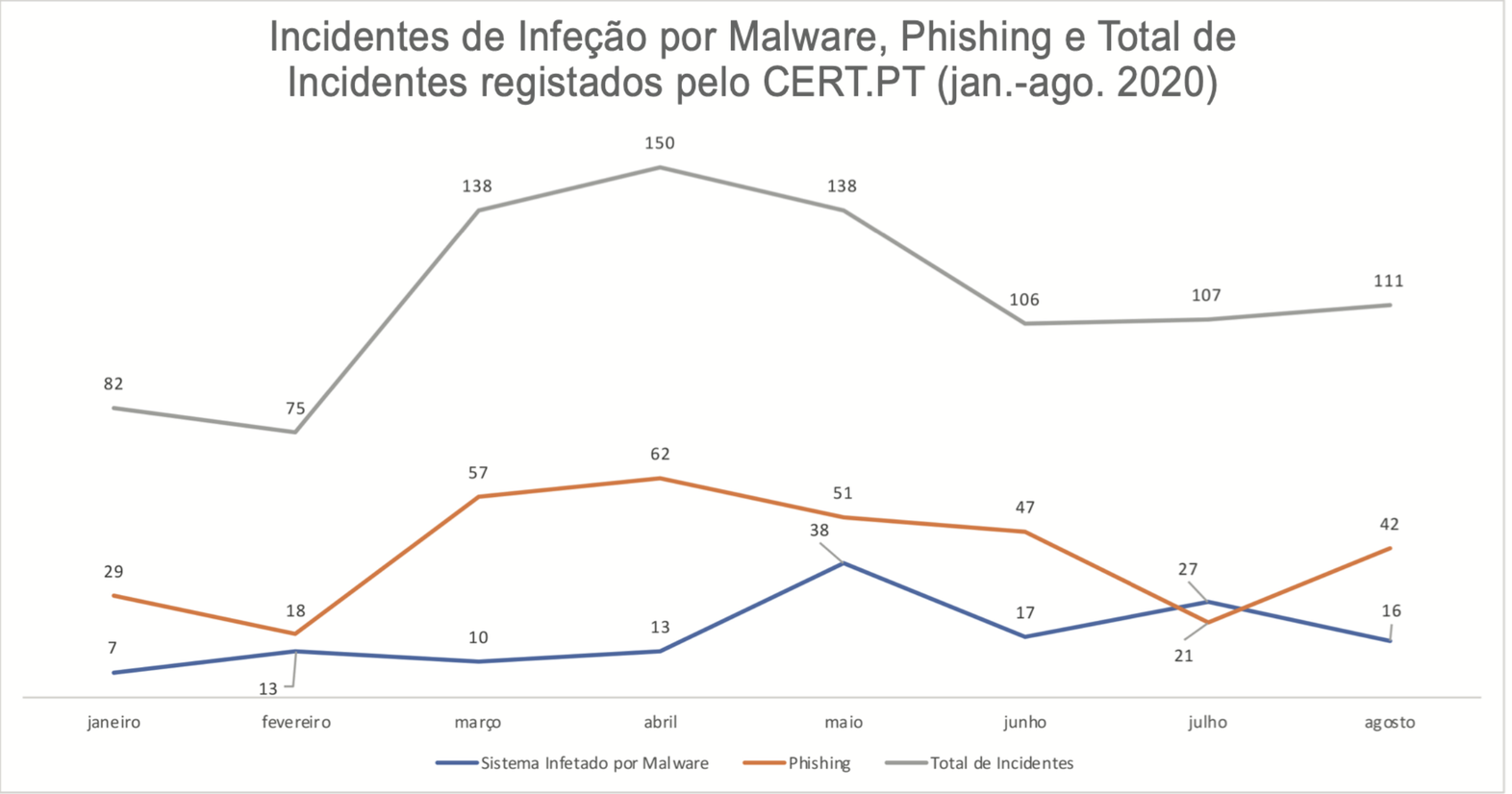
Tipos de incidentes registados pelo CERT.PT
2018-2019

Relevância clara do ***phishing*** e da **infeção por *malware***

2018				2019				Ordenação	
RK	Tipo	N°	%	RK	Tipo	N°	%	Tendência absoluta	Lugar RK
1°	*Phishing*	176	29	1°	*Phishing*	236	31	+	=
2°	Infeção *(malware)*	132	22	2°	Infeção *(malware)*	123**	16	-	=
3°	Distribuição *(malware)*	71	12	3°	Compromisso de Conta	95	13	+	+
4°	*Scan*	54	9	4°	Exp. de vuln. (intrusão)	58	8	+	+
5°	Exp. de vuln. (intrusão)	40	7	5°	Distribuição *(malware)*	55	7	-	-
6°	Tentativa de *login*	25	4	6°	Tentativa de *login*	30	4	+	=
7°	Compromisso de Conta	21	4	7°	*Scan*	28	4	-	-
8°	Exp. de vuln. (tentativa de intrusão)	19	3	8°	DoS/DDoS	27	4	+	+
9°	SPAM	15	3	9°	Utilização ilegítima de nome de terceiros	19	3	+	+
10°	*Blacklist*	12	2	10°	Exp. de vuln. (tentativa de intrusão)	18	2	-	-

CNCS

(CNCS, 2020a)



Durante o 2º trimestre, o *phishing* foi o tipo de incidente mais registado pelo CERT.PT. O 2º tipo de incidente mais registado durante esse período foi o sistema infetado por *malware*. Contudo, à medida que se aproximou o período de férias, o *phishing* diminuiu. Com a entrada no mês de julho, verificaram-se mais incidentes referentes a sistema infetado por *malware* do que a *phishing*. Em agosto, a tendência inverteu-se para uma situação semelhante a junho.

Atitudes e comportamentos
Portugal

Menos portugueses do que a média da UE a sentirem-se **muito bem informados** sobre os riscos de cibercrime: 11% na UE e 2% em Portugal, em 2019 (EC, 2020)

Menos portugueses que afirmam ser capazes de se **proteger** o suficiente do cibercrime, em 2019 – menos 8 pp (45%) e menos 9 pp na média da UE (52%) do que em 2018 (EC, 2020)

Maior **preocupação** dos portugueses com o cibercrime, em contraciclo com a UE. P. ex.: a preocupação com a fraude em cartão bancário ou em banco *online* aumentou 10 pp (74%), a média da UE desceu 3 pp (67%), entre 2018 e 2019 (EC, 2020)

Portugal é o país da UE no qual mais pessoas **NÃO** **alteraram alguma *password*** no ano anterior, em 2019: 48%, enquanto a média da UE é 31% (EC, 2020)

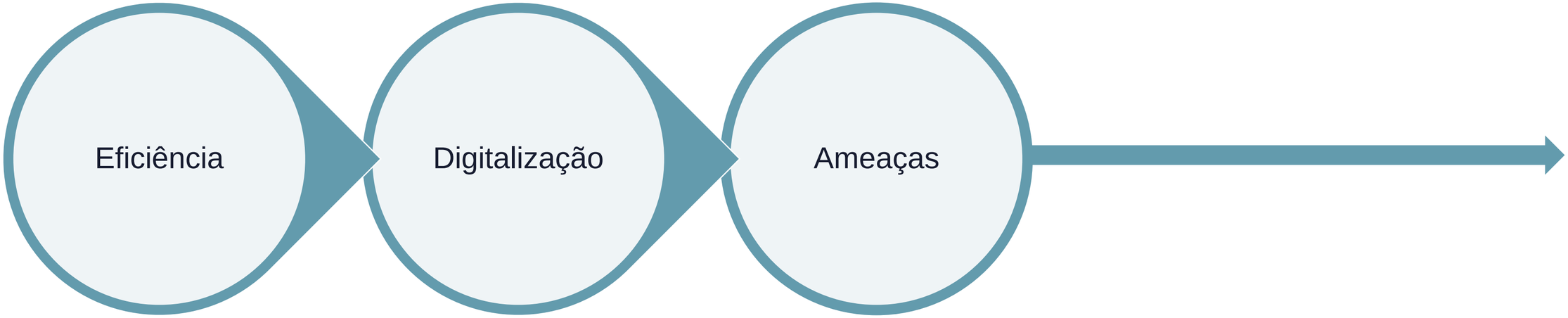
Poucas empresas portuguesas **com seguro** contra incidentes de segurança em TIC – 10%, contra 21% da média da UE (Eurostat, 2020)

Menos informação + Insegurança
+ Preocupação + Inação

Agentes de ameaças mais relevantes atualmente
Portugal

- Agentes Estatais
- Cibercriminosos
- Hacktivistas

O contexto da Saúde
que faz surgir novas e velhas ameaças



Rapidez
Acesso
Monitorização ativa
Robotização/Remotização
Prevenção/Predição

Integração de Sistemas
Telemedicina
Wearables
Inteligência Artificial

Confidencialidade
Integridade
Disponibilidade

Vulnerabilidades
como pontos críticos da transição digital

Exploração das **vulnerabilidades do humano** através da engenharia social

Sistemas complexos e interdependentes com **componentes vulneráveis**

Necessidade de **operação contínua** limita reação a incidentes

Necessária **especialização** na configuração de dispositivos médicos

Incompatibilidade entre os **ciclos de vida** do IT e dos dispositivos médicos

Deficiente **processo de aquisição**

Cibersegurança na Saúde
Desafios presentes e futuros

Tecnologia

Zero-Trust
Anti-negação de serviço
Anti-perda de dados
Security-by-Design
Certificação de produtos

Processos

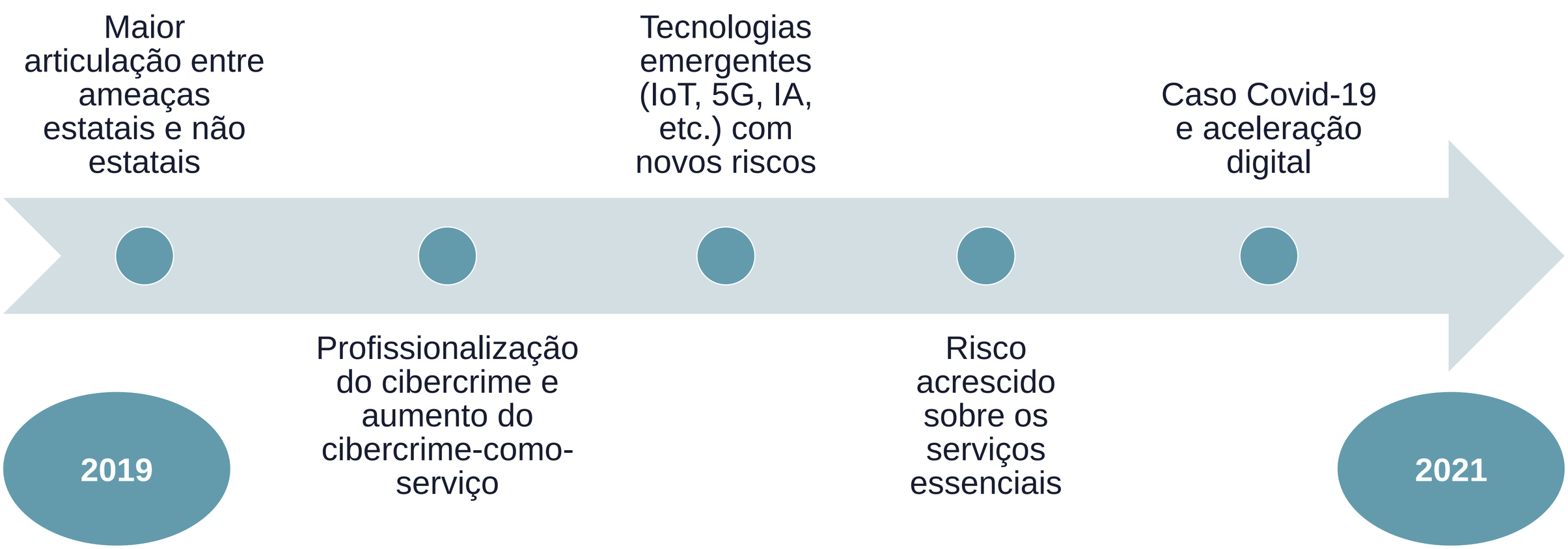
Transparência no tratamento de dados
Security-by-Design
Mecanismos de recuperação
Mecanismos de continuidade de atividade
Certificação de serviços

Pessoas

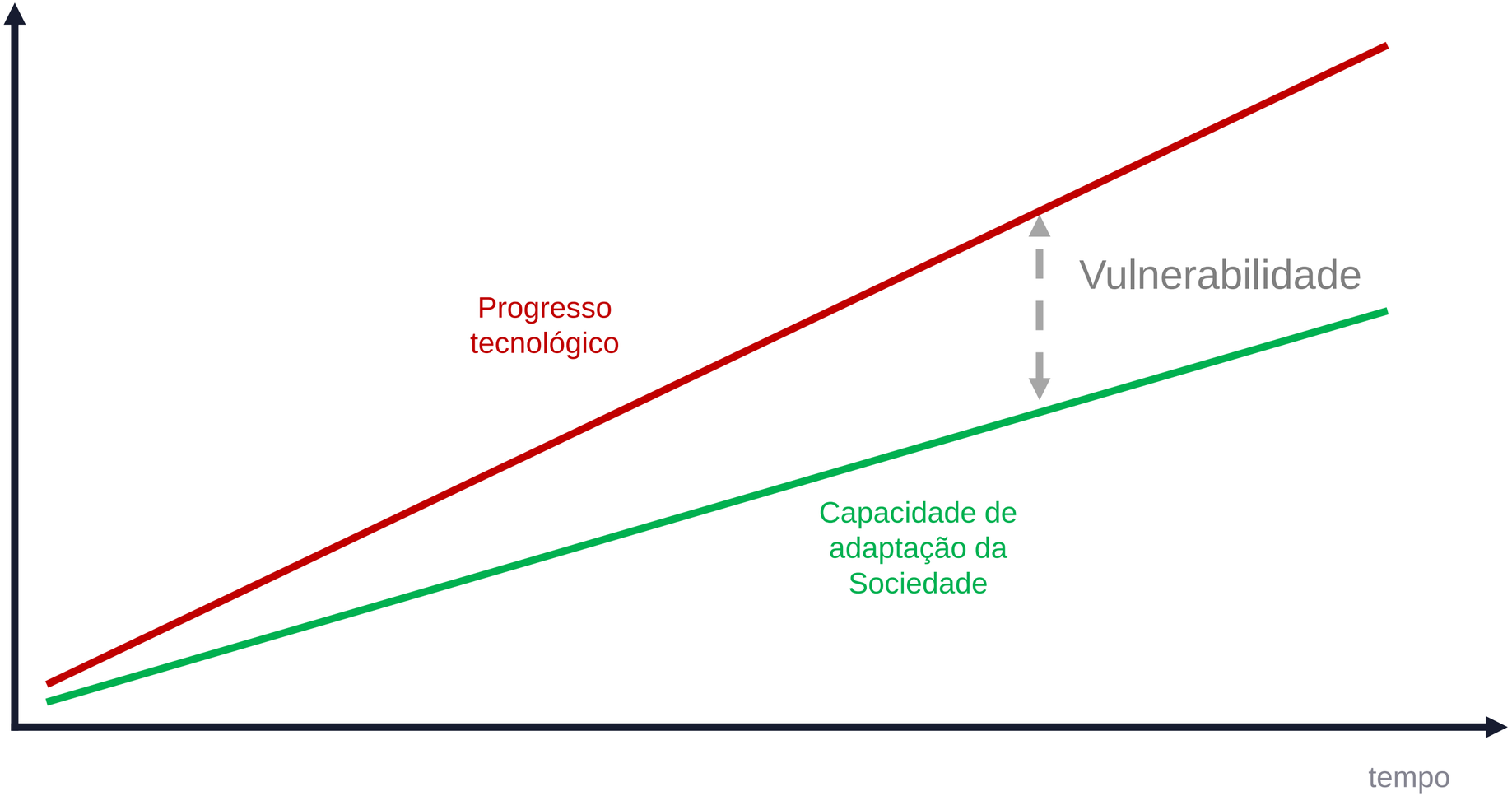
Competências de cibersegurança em todo o pessoal

CNCS

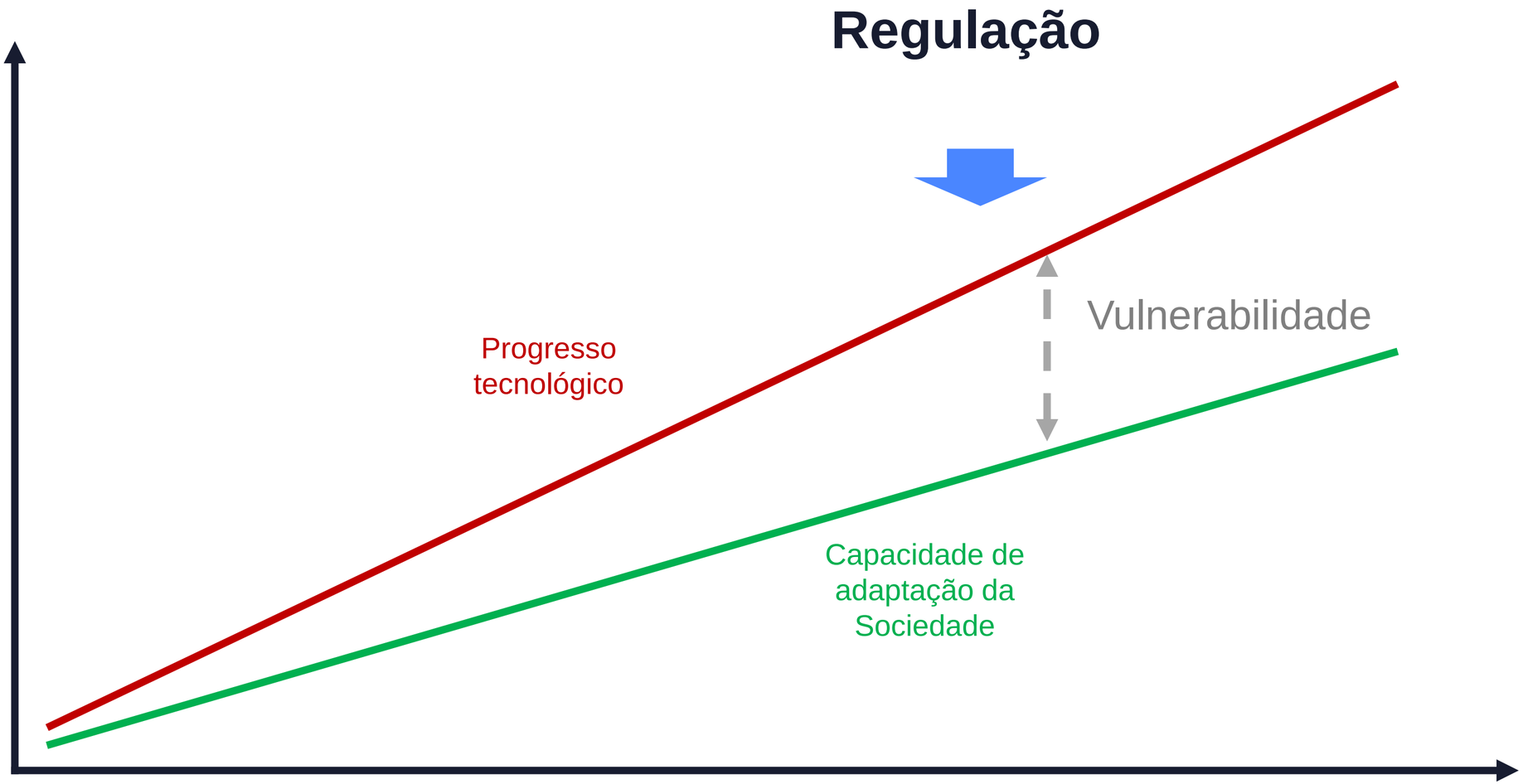
Tendências globais



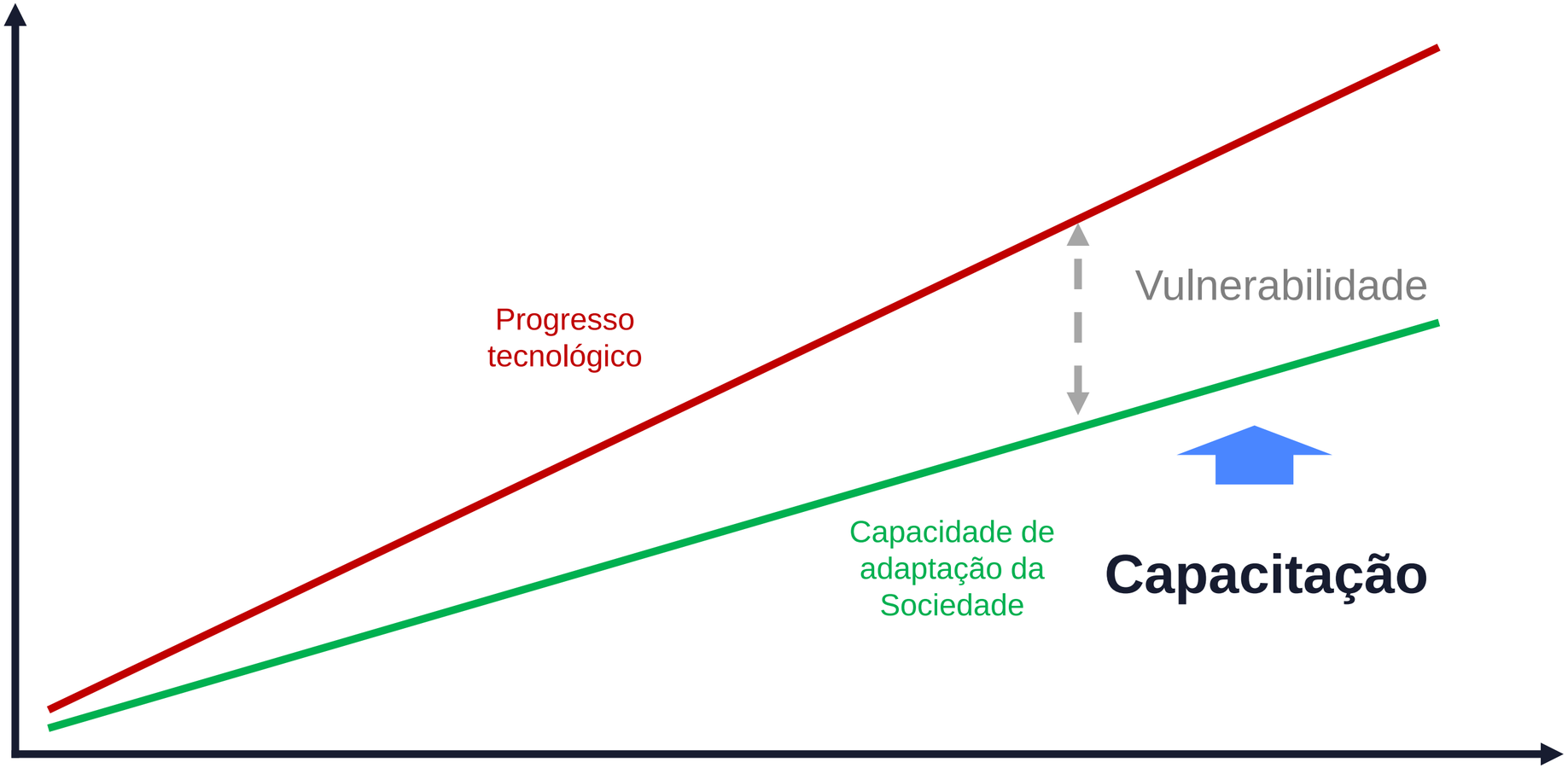
Vulnerabilidade da sociedade



Medidas de mitigação



Medidas de mitigação



Desafios
o que fazer

Normalizar a cibersegurança

Qualificar os profissionais

Influenciar as lideranças

Educar a comunidade

Regular os Serviços Essenciais

Segurança *by* ***design***

Envolver os ***stakeholders***

Integrar as **novas tecnologias**

Naturalizar a cibersegurança, não como um problema que se resolve mas como um **risco** que se gere

Transformar a cibersegurança num ativo estratégico

CNCS

Referências

CNCS (2020a) *Relatório Cibersegurança em Portugal – Riscos e Conflitos*. Observatório de Cibersegurança, Centro Nacional de Cibersegurança.

CNCS (2020b) *Boletim 03/2020*. Observatório de Cibersegurança, Centro Nacional de Cibersegurança.

EC (2020) *Special Eurobarometer 499: Europeans' Attitudes Towards Cyber Security*. Brussels: European Commission

Eurostat (2020a) *Security incidents and consequences*. Code: isoc_cisce_ic.

MP (2020) *Nota Informativa COVID 19: cibercrime em tempo de pandemia*, Ministério Público, Procuradoria-Geral da República, Gabinete de Cibercrime.

RASI (2020) *Relatório Anual de Segurança Interna 2019*. Sistema de Segurança Interna.

ENISA (2020) Good practices for the security of Healthcare services