CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Cibersegurança: tendências e desafios atuais (PME)

Pedro Xavier Mendonça
(CNCS)

OBJETIVO DA APRESENTAÇÃO

Mostrar a **importância da cibersegurança** para as PME e o **contexto de ameaças** que as pode afetar.

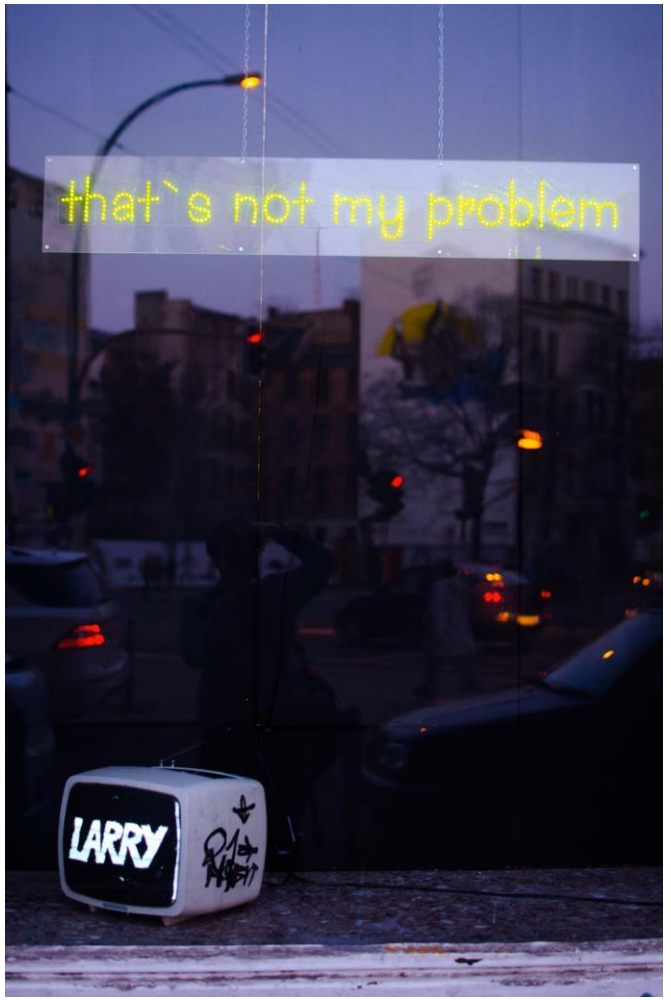
CIBERSEGURANÇA NAS PME

"Ninguém se interessa por mim!"

"Não tenho nada de valor!"

"Quem não deve não teme!"

"Vão furtar o quê?!"



Aneta Pawlik

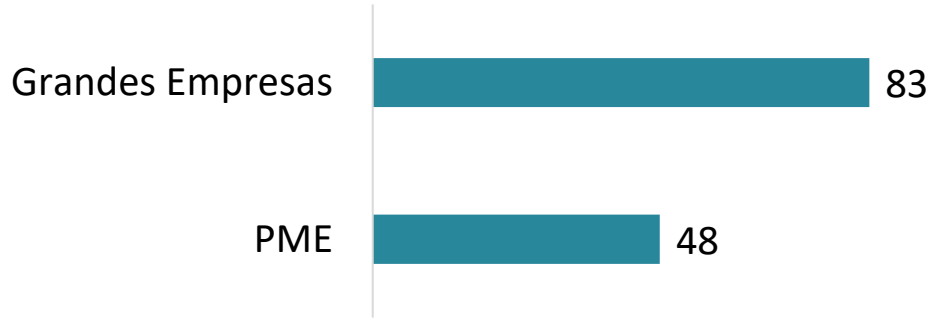
DESIGUALDADE NA CIBERSEGURANÇA

Há uma crescente **desigualdade entre empresas** na capacitação para a cibersegurança, nomeadamente entre PME e grandes empresas:

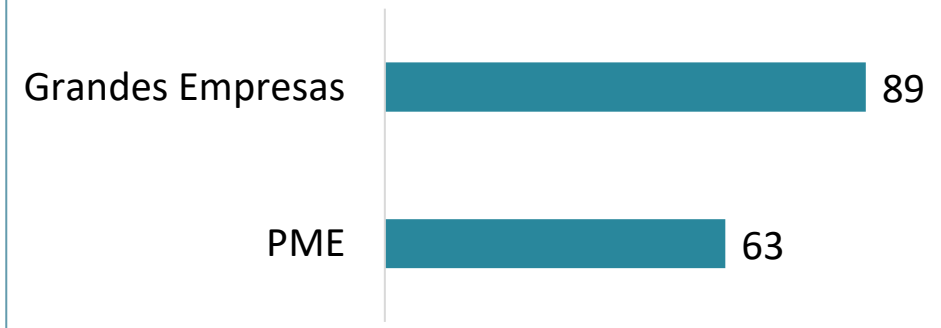
– **90% dos executivos** inquiridos pelo WEF consideram que este é um **problema urgente.**

(WEF, 2024)

Empresas com **política de segurança para as TIC** definida ou revista nos últimos dois anos, Portugal, 2022 (%)



Empresas que **sensibilizaram os seus empregados** para as obrigações de segurança nas TIC, Portugal, 2022 (%)



(Eurostat, 2022)

CNCS Centro Nacional de Cibersegurança PORTUGAL

ECONOMIA DA CIBERSEGURANÇA EM PORTUGAL

Aspetos positivos (2021)

- **Existem pelo menos 144 empresas** que oferecem serviços de cibersegurança;
- Os profissionais de cibersegurança são **relativamente novos e com formação** elevada;
- Verifica-se um **aumento da cooperação** entre empresas com a criação de mais Comunidades de Cibersegurança.

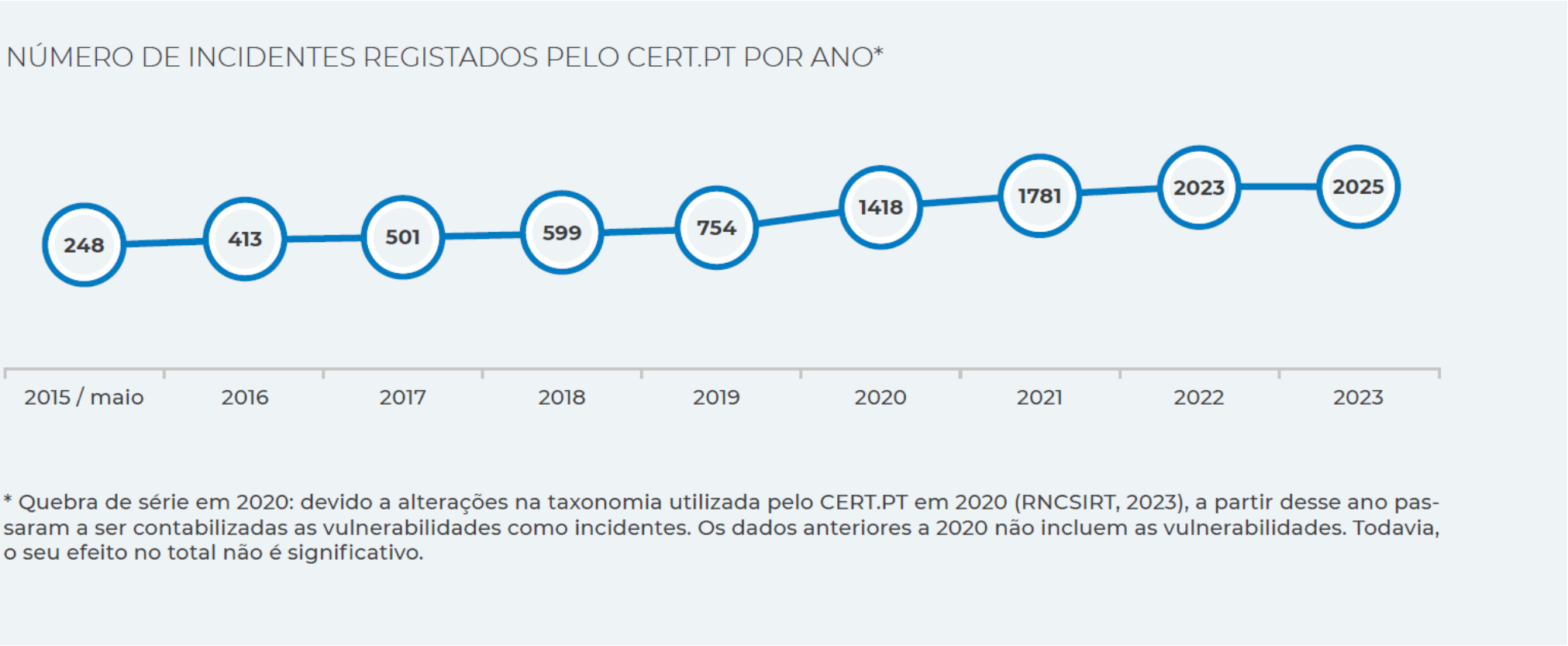
Problemas que persistem (2021 e 2022)

- Pouco mais de um terço das PME tem um **orçamento abaixo dos 3000 euros** em cibersegurança;
- Pelo menos **uma em cada seis PME tem dificuldades em contratar** profissionais de cibersegurança;
- As razões principais são a **escassez de profissionais** (para 78%) e **o seu elevado custo** (para 57%).

(CNCS, 2022)

CNCS Centro Nacional de Cibersegurança PORTUGAL

TOTAL DE INCIDENTES REGISTADOS PELO CERT.PT
2015 -2023

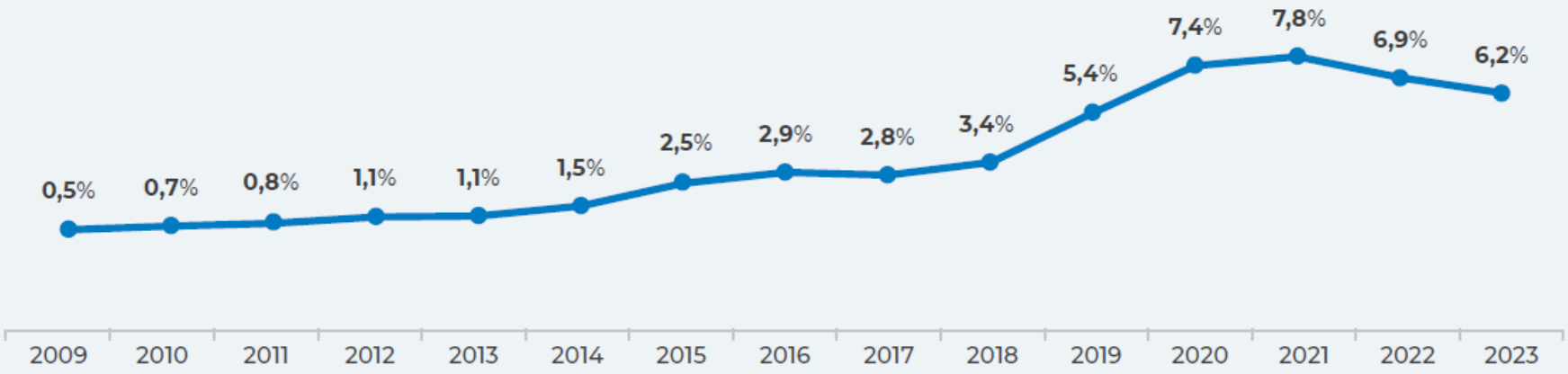


Fonte: CERT.PT

(CNCS, 2024)

CRIME E CIBERCRIME PARTICIPADO EM PORTUGAL
2009-2023

PERCENTAGEM DE CRIMES RELACIONADOS COM A INFORMÁTICA EM RELAÇÃO AO TOTAL DE CRIMES REGISTADOS PELAS AUTORIDADES POLICIAIS*



*Os crimes relacionados com a informática incluem os crimes informáticos juntamente com a burla informática/comunicações e a devassa por meio de informática. Verifica-se uma quebra de série em 2022: crimes antes registados como "burla informática/comunicações" passaram a ser registados como "abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento" (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

Fonte: DGPJ

(CNCS, 2023)

O FATOR HUMANO NA CIBERSEGURANÇA
extorsões e fraudes

Em 2023, pelo menos **45%** dos incidentes registados pelo CERT.PT envolvem diretamente o **fator humano.**

As **PME continuam a ser um dos principais alvos** de cibercriminosos que têm como objetivo obter ganhos económicos através de **extorsões** e **fraudes**.

O ***ransomware*** é também uma preocupação, nomeadamente pelo impacto.

São preocupantes os casos de **comprometimento de *email* empresarial**, com *phishing*, CEO Fraud, entre outros.

RANSOMWARE
modi operandi mais frequentes

Recolha de credenciais de acesso: bases de dados, *phishing*, força-bruta → **Comprometimento** de contas → Escalar para privilégios de **administrador** → **Instalação** de *malware*

Outros *modi operandi*

Exploração de vulnerabilidades
Comprometimento de acesso remoto (RDP)
Emails com anexos e *links* com *malware*

CEO FRAUD (BEC)
modi operandi mais frequentes

Recolha de credenciais de acesso: bases de dados, *phishing*, força-bruta → **Comprometimento** de conta de fornecedor → Recolha de informação sobre **contexto** de *emails* → **Pedido de pagamento** a cliente para novo IBAN

Outros *modi operandi*

Personificação de entidade fornecedora e clientes – *typosquatting*
Personificação de empregado para alterar destino do vencimento
Personificação de superior hierárquico a requisitar cartões de oferta

CADEIA DE ATAQUE DA ENGENHARIA SOCIAL

1. Recolha de informação

2. Criação de "(pre)texto"

3. Escolha de vetores de ataque

4. Ataque

5. Benefício

(Adaptado de Hadnagy, 2018)

CNCS Centro Nacional de Cibersegurança PORTUGAL

O QUE FAZER?

Identificar – inventariar quais os ativos críticos para a organização

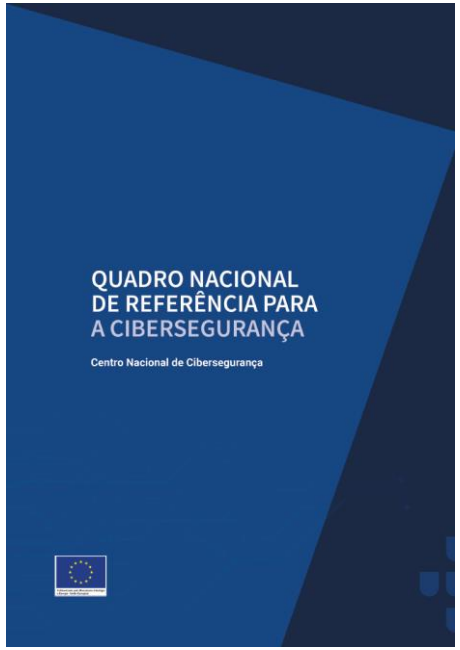
Guardar – fazer *backups* regulares

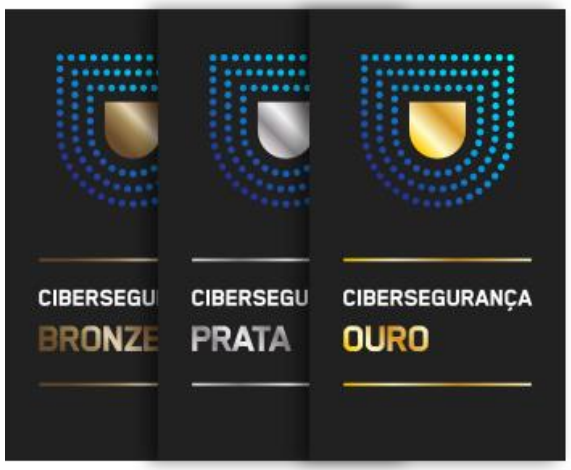
Multiplicar – aplicar o múltiplo fator de autenticação

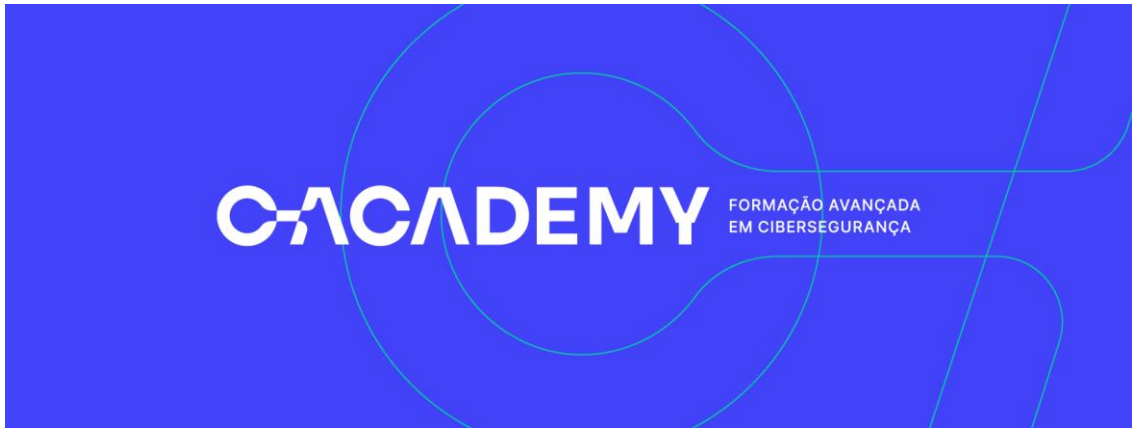
Atualizar – manter os sistemas atualizados

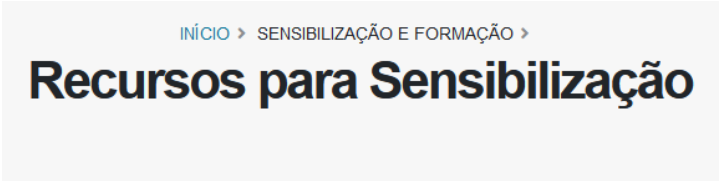
Formar – disponibilizar sensibilização e treino aos empregados

INSTRUMENTOS CNCS









CNCS
Centro Nacional de Cibersegurança
PORTUGAL

OBRIGADO

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt | (+351) 210 497 400