Cibersegurança e Indústria 4.0

Resultados de inquérito a trabalhadores e técnicos operacionais

Observatório de Cibersegurança
Centro Nacional de Cibersegurança
março de 2023

Introdução

O Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS), em colaboração com o Instituto Politécnico do Porto e o Compete 2020, lançou um inquérito aos técnicos operacionais e trabalhadores de organizações do âmbito da Indústria 4.0, sobre as políticas e as práticas de cibersegurança neste contexto. O questionário foi preenchido entre os dia 14 de julho e 7 de outubro de 2021.

O objetivo deste inquérito foi compreender a integração de políticas e práticas de cibersegurança num domínio tecnológico particularmente avançado e emergente, como é o da Indústria 4.0. As questões foram desenvolvidas por uma equipa do Instituto Politécnico do Porto, com o apoio do CNCS, e enviadas pelo Compete 2020 a uma lista de organizações elegíveis no âmbito de programas de financiamento para a Indústria 4.0.

Por Indústria 4.0 entendem-se os processos que “agregam tecnologias e métodos disruptivos” como “Big Data”, “Advanced Analytics”, “Cloud Computing” e “Internet das coisas (Internet of Things - IoT)”. Para uma compreensão mais aprofundada desta matéria e do tipo de organizações elegíveis, consultar a seguinte página.

O inquérito subdividiu-se em dois questionários diferentes. Um sobre a) “Políticas e Práticas de Cibersegurança dos Técnicos Operacionais”, dirigido a técnicos operacionais, e outro sobre b) “Práticas e a Consciência dos Trabalhadores acerca da Cibersegurança”, respondido pelos restantes trabalhadores das organizações abrangidas.

Índice

a. Políticas e Práticas de Cibersegurança dos Técnicos Operacionais na Indústria 4.0

Políticas e Práticas de Cibersegurança dos Técnicos Operacionais na Indústria 4.0

Caracterização

Atividade Económica	Número de respondentes	
Administração	1	0,4%
Agricultura, Silvicultura e Pescas	1	0,4%
Comércio	14	6%
Construção	12	5%
Energia e Ambiente	7	3%
Indústria Extrativa	6	3%
Indústria Transformadora	138	62%
Serviços	23	10%
Turismo	16	7%
Transportes	2	1%
Outro	1	0,4%
Não sabe	3	1%
Total	224	100%

Tamanho da organização	Número de trabalhadores	Número de respondentes	
Grande	250 ou mais	38	17%
Média	De 50 a 249	64	29%
Pequena	De 10 a 49	86	38%
Micro	Até 9	36	16%
Total		224	100%

Amostra global: n=224

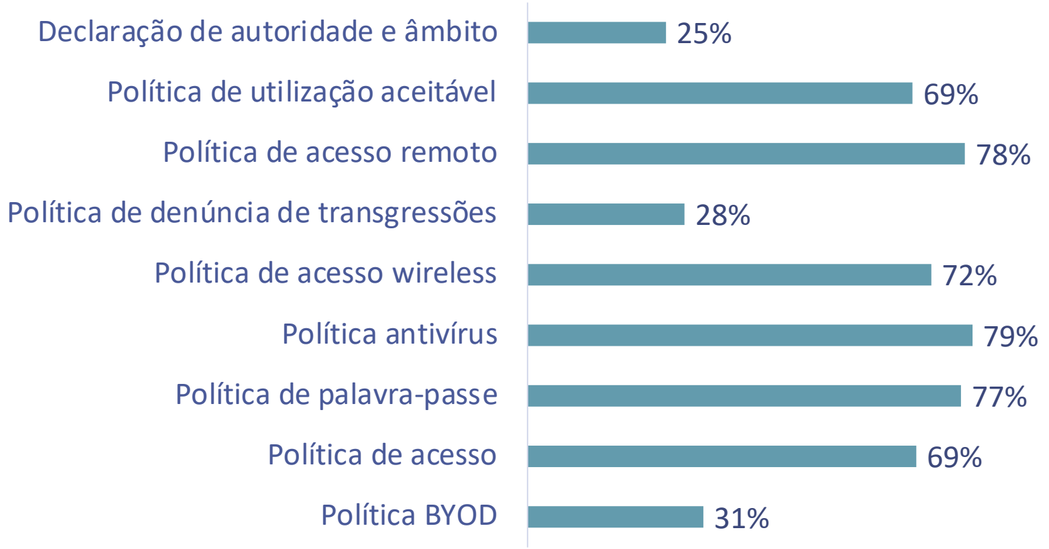
- 62% dos técnicos operacionais que participaram no questionário pertencem à indústria transformadora e 10% aos serviços;
- 67% dos técnicos operacionais que participaram no questionário pertencem a pequenas e médias empresas.

Políticas e Práticas de Cibersegurança dos Técnicos Operacionais na Indústria 4.0

Política de cibersegurança

Política de cibersegurança na Indústria 4.0 e papel do Técnico Operacional (TO), Portugal, 2021 (segundo TO)

1.3. Elementos presentes nessa Política de cibersegurança, na Indústria 4.0, Portugal, 2021 (segundo TO)



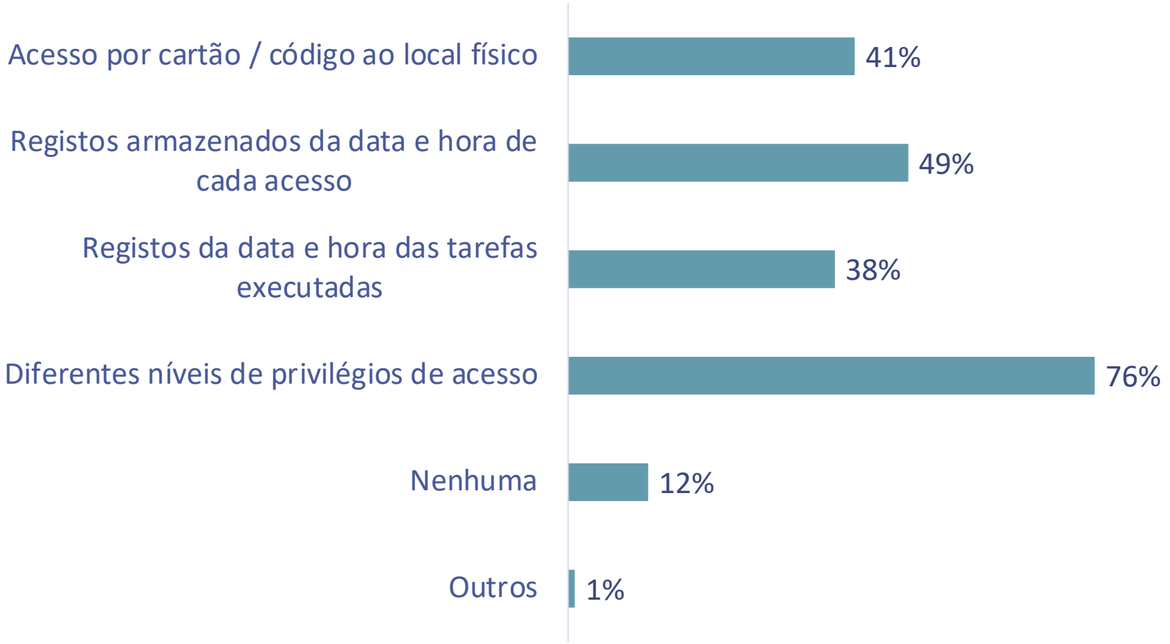
- 75% dos técnicos operacionais afirmam que as suas organizações implementam uma política de cibersegurança;
- As políticas relacionadas com o antivírus (79%), com o acesso remoto (78%) e com a palavra-passe (77%) são os aspetos mais presentes nas respostas dadas.

Políticas e Práticas de Cibersegurança dos Técnicos Operacionais na Indústria 4.0

Política de cibersegurança

1.3.1. Elementos da política de palavra-passe na Indústria 4.0, Portugal, 2021 (segundo TO)

1.3.2. Elementos da política de acesso na Indústria 4.0, Portugal, 2021 (segundo TO)



1.3.3. Entre os 31% respondentes que assinalaram "Política BYOD", quase metade detalharam que os trabalhadores podem utilizar dispositivos pessoais na sua instituição:

49 %

- A complexidade é o elemento mais presente na política de palavra-passe (87%); os diferentes níveis de privilégio de acesso, o elemento mais presente na política de acesso (76%); e, entre as políticas que têm referência a BYOD (31%), para 49% dos respondentes permite-se que os colaboradores usem os seus dispositivos pessoais na instituição a que pertencem.

Políticas e Práticas de Cibersegurança dos Técnicos Operacionais na Indústria 4.0

Verificação de novos operadores

Verificação de aspetos biográficos de novos operadores na Indústria 4.0 e aspetos verificados, Portugal, 2021 (segundo TO)

3. O TO tem um *briefing* de sensibilização em cibersegurança preparado para realizar aos novos operadores:

34%

- Segundo 31% dos técnicos operacionais, as organizações em causa verificam aspetos biográficos dos novos operadores;
- A segurança social (78%) e os registos profissionais (65%) são os aspetos mais verificados;
- 34% dos técnicos operacionais têm um *briefing* de sensibilização de cibersegurança preparado para os novos operadores.

Políticas e Práticas de Cibersegurança dos Técnicos Operacionais na Indústria 4.0

Estimar os custos de um incidente

Estimativa dos custos da recuperação da automação no caso de incidente, por tamanho da organização, na Indústria 4.0, Portugal, 2021 (segundo TO)

Tamanho da organização	Número de trabalhadores	Custo médio (euros)	% de Respondentes
Micro	até 9	16 867	38%
Pequena	de 10 a 49	66 266	14%
Média	de 50 a 249	14 014	33%
Grande	250 ou mais	83 333	14%
Total			9%

4. É capaz de estimar o custo de recuperação da automação no caso de uma interrupção provocada por um incidente:

9%

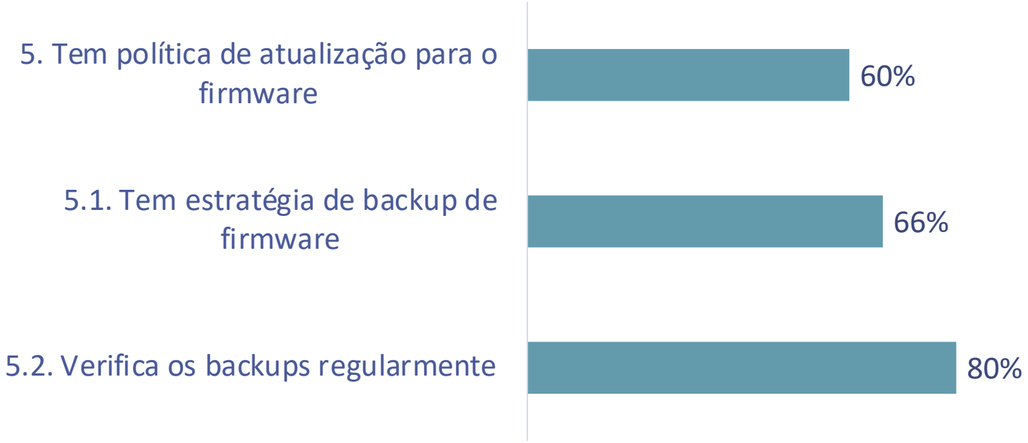
- Para apenas 9% dos técnicos operacionais as suas organizações são capazes de estimar o custo de recuperação de um incidente;
- Entre estes, resulta que as grandes empresas têm custos mais elevados (média de cerca de 83 mil euros), mas também têm menos capacidade de estimativa do que as micro e médias empresas (para estas os custos são em média de 66 mil euros).

CNCS Observatório de Cibersegurança P.PORTO COMPETE 2020

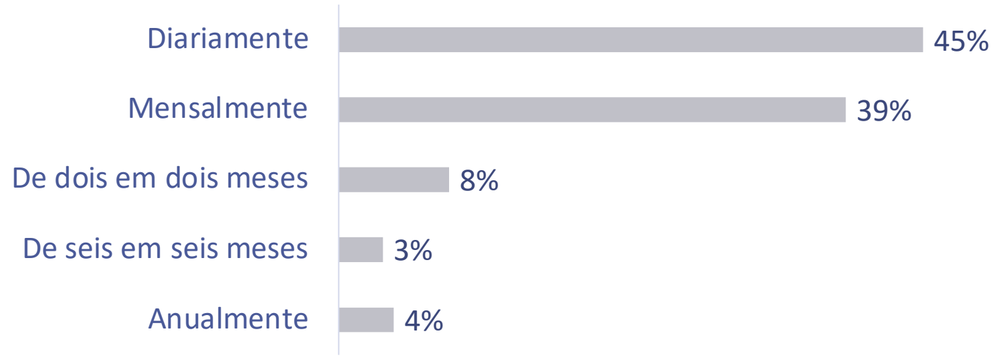
Políticas e Práticas de Cibersegurança dos Técnicos Operacionais na Indústria 4.0

Política de *firmware*

Política de atualização de *firmware* nos sistemas de automação, na Indústria 4.0, Portugal, 2021 (segundo TO)



5.2.1. Frequência com que verificam os *backups* de *firmware*



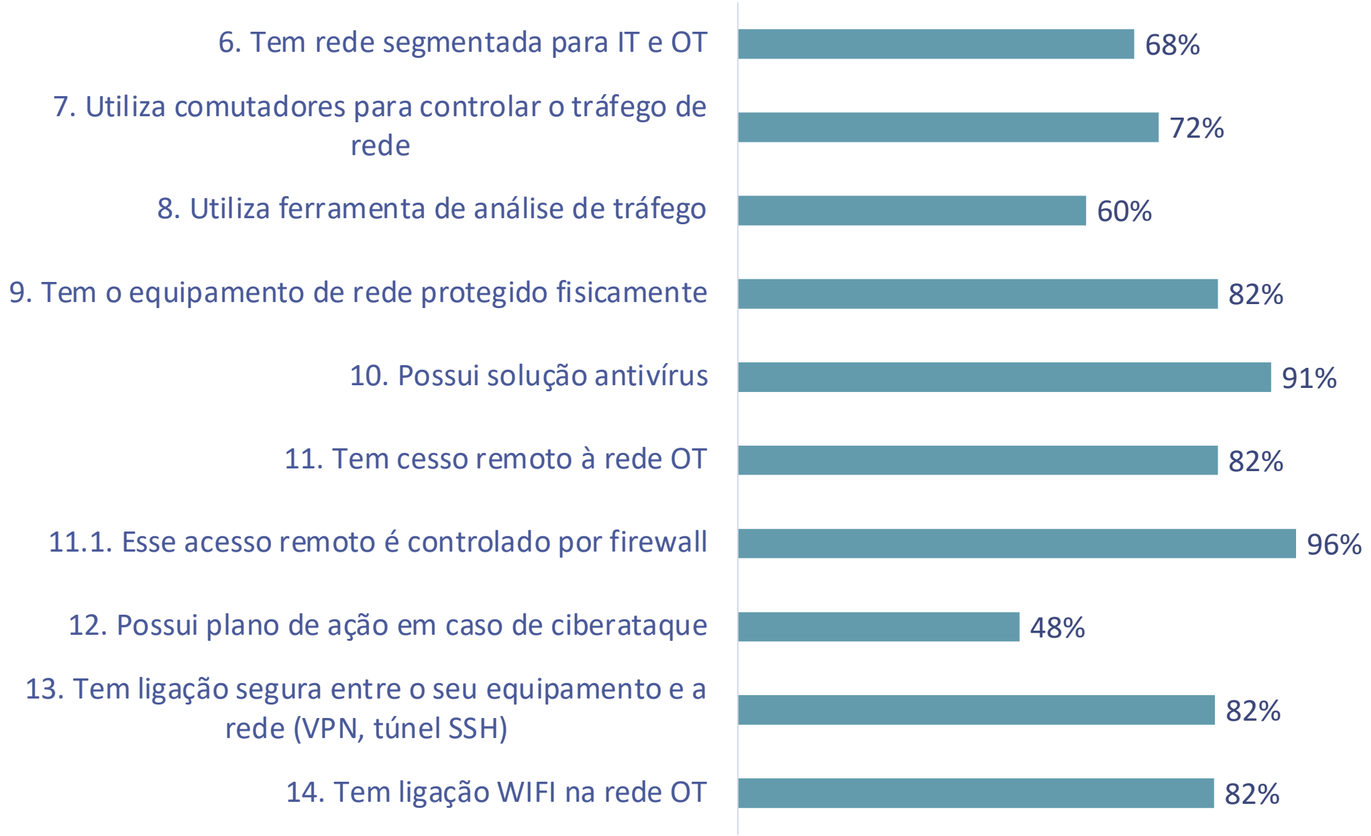
- 60% dos técnicos operacionais afirma que a organização tem política de atualização do *firmware*;
- Destes, 66% afirmam ter estratégia de *backup* de *firmware*. E destes, 80% verificam-nos regularmente (45% fazem-no diariamente).

CNCS Observatório de Cibersegurança P.PORTO COMPETE 2020

Políticas e Práticas de Cibersegurança dos Técnicos Operacionais na Indústria 4.0

Tecnologias e processos

Tecnologias e processos com relação à cibersegurança na Indústria 4.0, Portugal, 2021 (segundo TO)



- 91% dos técnicos operacionais afirma que a sua organização possui solução antivírus e, 82%, que tem o equipamento de rede protegido fisicamente, bem como ligação segura entre equipamento e rede;
- 68% dos técnicos operacionais afirma que a sua organização tem rede segmentada para IT e OT;
- Apenas 48% dos técnicos operacionais afirma que a organização possui plano de ação em caso de ciberataque.

b. Práticas e a Consciência dos Trabalhadores acerca da Cibersegurança na Indústria 4.0

Práticas e a Consciência dos Trabalhadores acerca da Cibersegurança na Indústria 4.0

Caracterização

Atividade Económica	Número de respondentes	
Administração	8	1%
Agricultura, Silvicultura e Pescas	4	1%
Comércio	43	7%
Construção	45	8%
Energia e Ambiente	15	3%
Indústria Extrativa	4	1%
Indústria Transformadora	361	61%
Serviços	61	10%
Transportes	1	0%
Turismo	31	5%
Outro ou não sabe	18	3%
Total	591	100%

Tamanho da organização	Número de trabalhadores	Número de respondentes	
Grande	250 ou mais	135	23%
Média	De 50 a 249	215	36%
Pequena	De 10 a 49	187	32%
Micro	Até 9	54	9%
Total		591	100%

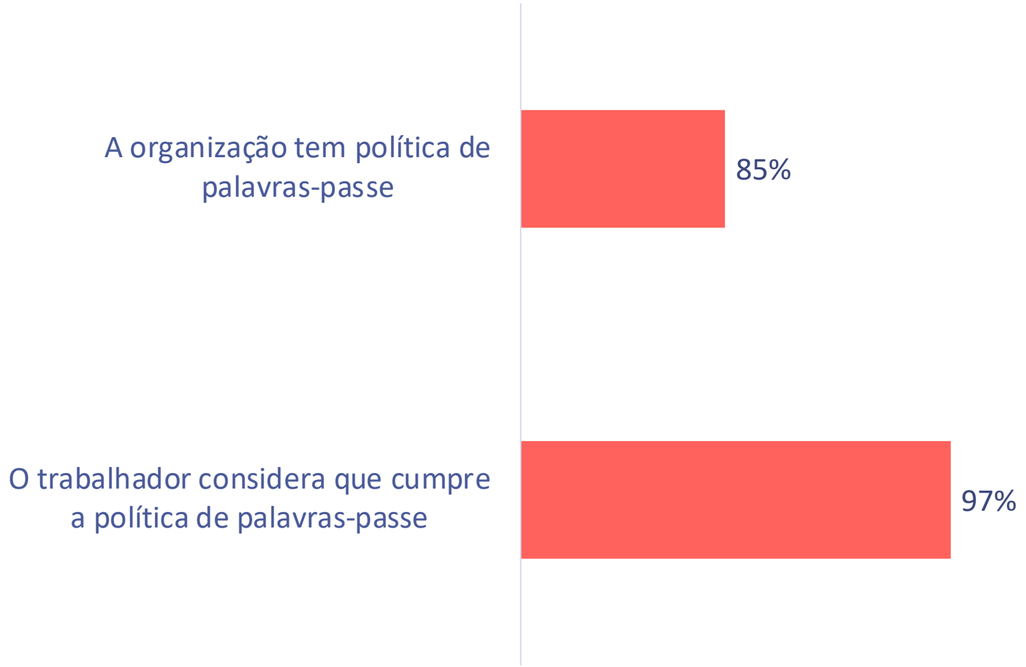
Amostra global: n=591

- 61% dos trabalhadores pertence a entidades da indústria transformadora e 10% dos serviços;
- 68% dos trabalhadores pertence a entidades que são pequenas e médias empresas.

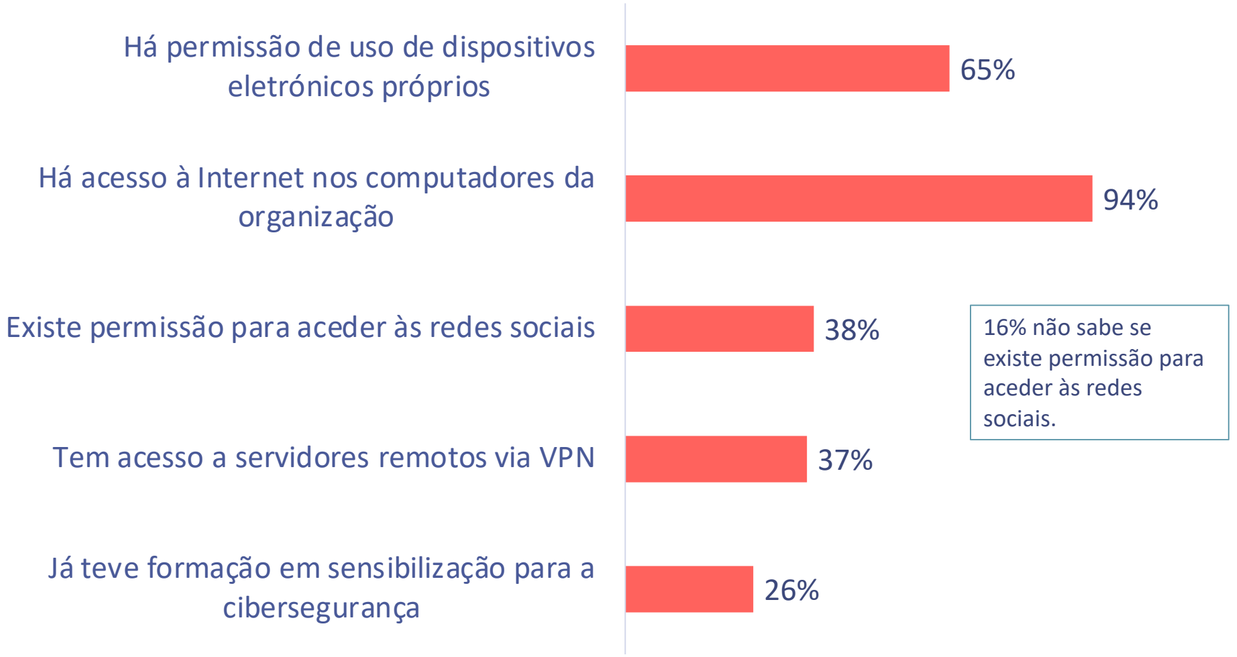
Práticas e a Consciência dos Trabalhadores acerca da Cibersegurança na Indústria 4.0

Políticas de cibersegurança

1. Políticas de Palavras-passe na Organização de Indústria 4.0, Portugal, 2021 (segundo trabalhadores)



2. Políticas de Cibersegurança nas Organizações da Indústria 4.0, Portugal, 2021 (segundo trabalhadores)



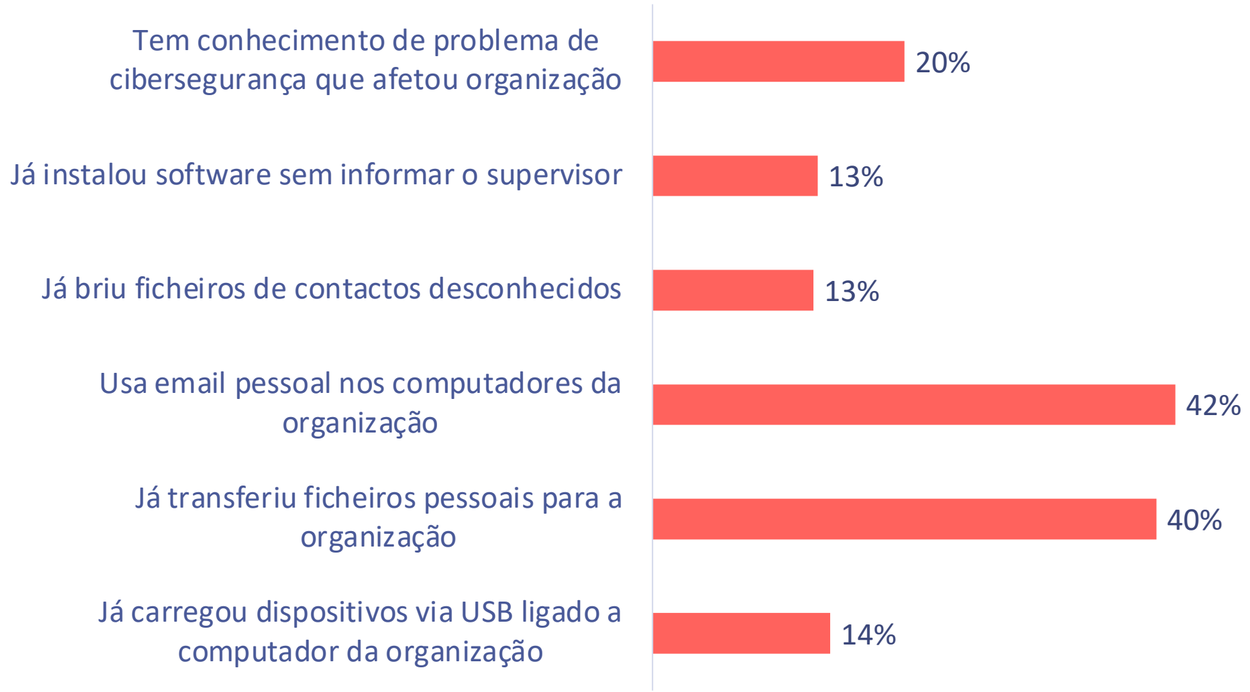
- 85% dos trabalhadores admite que as suas organizações possuem política de palavras-passe;
- Para 65% dos trabalhadores existe permissão para o uso de dispositivos próprios e para 38% permissão para uso de redes sociais (16% não sabe);
- Apenas 26% referem que beneficiaram de ações de sensibilização em cibersegurança.

CNCS Observatório de Cibersegurança P.PORTO COMPETE 2020

Práticas e a Consciência dos Trabalhadores acerca da Cibersegurança na Indústria 4.0

Práticas e vulnerabilidades de cibersegurança

3. Práticas e vulnerabilidades de Cibersegurança nas Organizações da Indústria 4.0, Portugal, 2021 (segundo trabalhadores)



- 20% dos trabalhadores tem conhecimento de um problema de cibersegurança que a organização já sofreu;
- 42% dos trabalhadores afirma que usa o *email* pessoal nos computadores da organização e 40% já transferiu ficheiros pessoais para a organização;
- 13% já instalou *software* sem informar o supervisor e, com a mesma percentagem, já abriu ficheiros de contactos desconhecidos.

c. Destaques 1/2

Segundo **75% dos técnicos operacionais as suas organizações implementam uma política de cibersegurança**, predominando aspetos relacionados com o antivírus, o acesso remoto e a palavra-passe (sendo a complexidade destas a exigência mais presente);

Para **31% dos técnicos operacionais, as suas organizações verificam aspetos biográficos dos novos operadores**, predominando como aspetos verificados a segurança social e os registos profissionais;

34% dos técnicos operacionais têm um *briefing* de sensibilização de cibersegurança preparado para os novos operadores;

Para **9% dos técnicos operacionais, as suas organizações são capazes de estimar o custo de recuperação de um incidente: as grandes empresas têm custos mais elevados** na recuperação de um incidente (média de cerca de **83 mil euros**), seguidas das empresas médias (cerca de 66 mil euros).

De acordo com **60% dos técnicos operacionais, as suas organizações possuem uma política de atualização de *firmware*** (e 66% destes refere que existe uma estratégia de *backup* desse *firmware*).

82% dos técnicos operacionais refere que a sua organização tem o equipamento de rede protegido fisicamente e 68% que a rede para IT e para OT se encontra segmentada.

Apenas **48% dos técnicos operacionais afirma que a organização possui plano de ação** em caso de ciberataque.

Destaques 2/2

Segundo **85% dos restantes trabalhadores, as organizações em causa possuem políticas de palavras-passe**.

Para **65% destes trabalhadores há permissão para o uso de dispositivos próprios** e para **38% permissão para usar redes sociais** (mas 16% não sabem).

Apenas **26% dos trabalhadores admite ter beneficiado de ações de sensibilização** em cibersegurança nas suas organizações.

20% dos trabalhadores admite ter conhecimento de um problema de cibersegurança que a organização já sofreu.

42% dos trabalhadores afirma que usa o *email* pessoal nos computadores da organização e 40% que já transferiu ficheiros pessoais para a organização.

13% dos trabalhadores já instalou *software* sem informar o supervisor.

d. Nota metodológica

O inquérito sobre a Indústria 4.0 e a Cibersegurança foi desenvolvido por uma equipa do Instituto Politécnico do Porto (IPP), com o apoio do Observatório de Cibersegurança do CNCS e do Compete 2020. Os questionários foram criados pelo IPP, integrados numa plataforma de inquéritos *online* do CNCS e disseminados pelo Compete 2020, via *email*, junto de entidades elegíveis no âmbito do financiamento à Indústria 4.0.

O inquérito foi constituído por dois questionários de perguntas fechadas e respondido entre os dias 14 de julho e 7 de outubro de 2021. Um dos questionários foi dirigido aos técnicos operacionais e o outro aos trabalhadores das organizações. Devido ao caráter anónimo do processo, não é possível identificar o rácio de respondentes por organização. Por isso, cada resposta deve ser lida com base na perspetiva do respondente e não como representante única de uma organização.

Obtiveram-se 224 respostas no questionário aos técnicos operacionais 591 no questionário aos restantes trabalhadores destas organizações.

Para mais detalhe sobre a metodologia adotada, contactar cncs@cncs.gov.pt.

Abreviaturas

BYOD	Bring Your Own Device
IT	Information Technology
OT	Operational Technology
SSH	Secure Shell
TO	Técnico Operacional
VPN	Virtual Private Network