



Imagem de Pete Linforth por Pixabay

## Perceção da População sobre Cibersegurança

# Índice

<b>1</b>	<b>Metodologia</b>	<b>3</b>
<b>2</b>	<b>Análise Global</b>	<b>6</b>
<b>3</b>	<b>Síntese</b>	<b>22</b>

1

# Metodologia

# Metodologia

4

No âmbito do **Barómetro APAV – INTERCAMPUS**, realizou-se em 2020 uma nova edição com vista a aferir a perceção da população sobre Cibersegurança.

- Frequência de acesso à internet;
- Atividades que realiza online
- Perceções sobre cibersegurança
- Perceções sobre cibercrime
- Estruturas de apoio a vítimas de cibercrime

A recolha de dados foi realizada com base num questionário elaborado pela APAV, composto maioritariamente por perguntas fechadas.

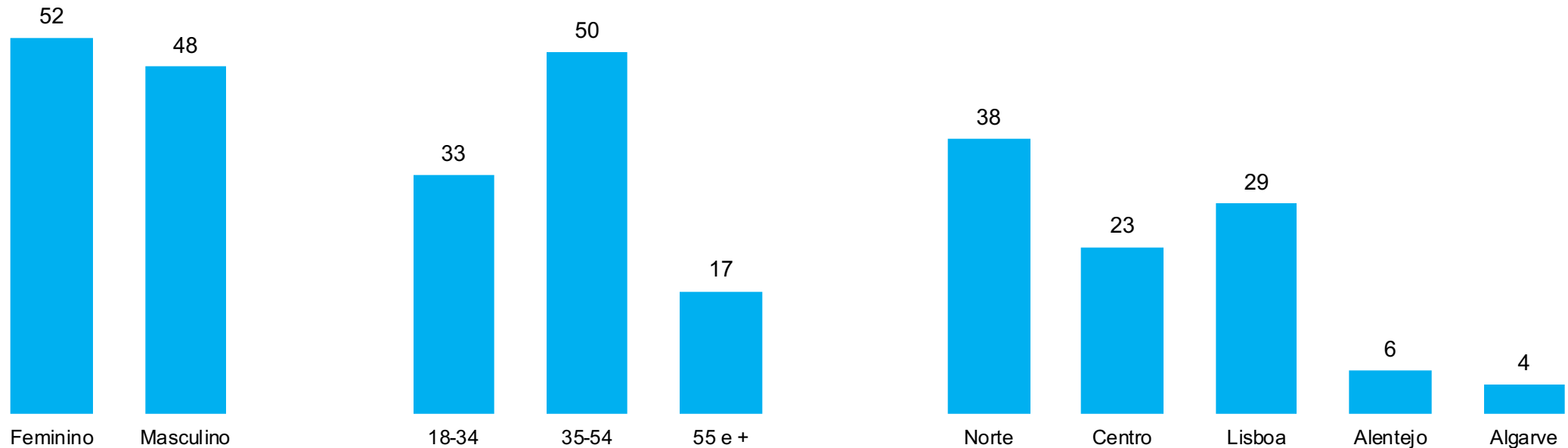
A informação foi recolhida através de entrevistas online, junto de um painel de internautas, no período entre 27 de Fevereiro e 08 de Março de 2020.



# Metodologia

5

A amostra global foi de n=591 entrevistas com a seguinte distribuição em termos de Género, Idade e Região.



Valores em %  
Base n=591

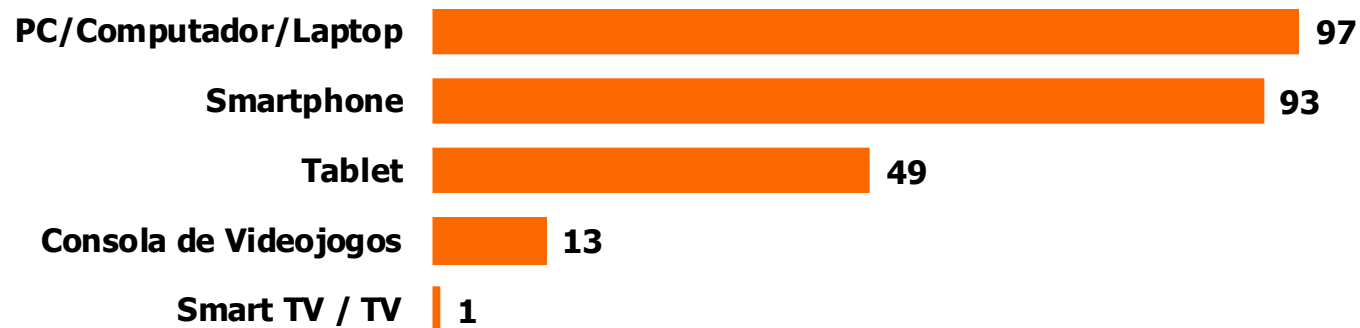
2

# Análise Global



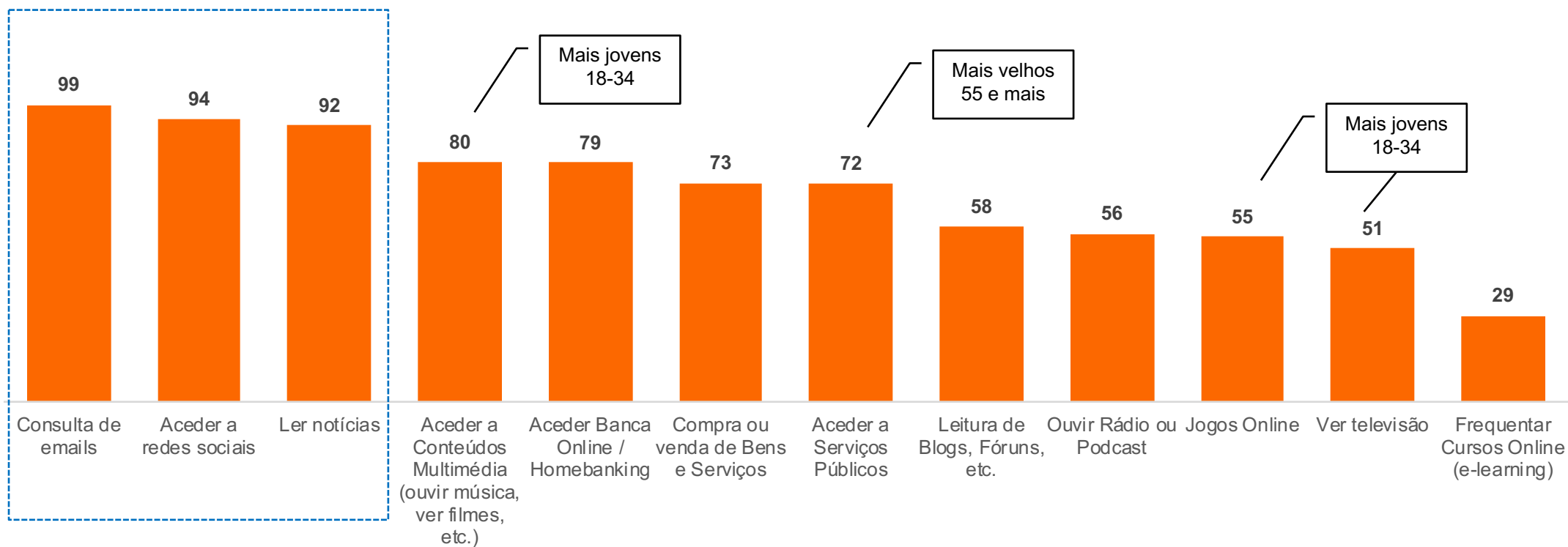
## Dispositivos e frequência de acesso à internet

7



Frequência de acesso	Está sempre ligado	Todos os dias ou quase todos os dias	Duas ou três vezes por semana	Uma vez por semana	Duas ou três vezes por mês	Com menor frequência
Em casa	60	37	2		0,3	0,2
No local de trabalho	50	29	5	0,7	0,2	2
Na escola / Universidade	12	10	3	0,3	0,3	1,4
Em qualquer local através do meu dispositivo móvel	37	42	10	2	0,8	6

# Atividades realizadas na internet



Valores em %  
Base n=591

P.2.1 Que atividades realiza ou já realizou na internet? RESPOSTA MÚLTIPLA

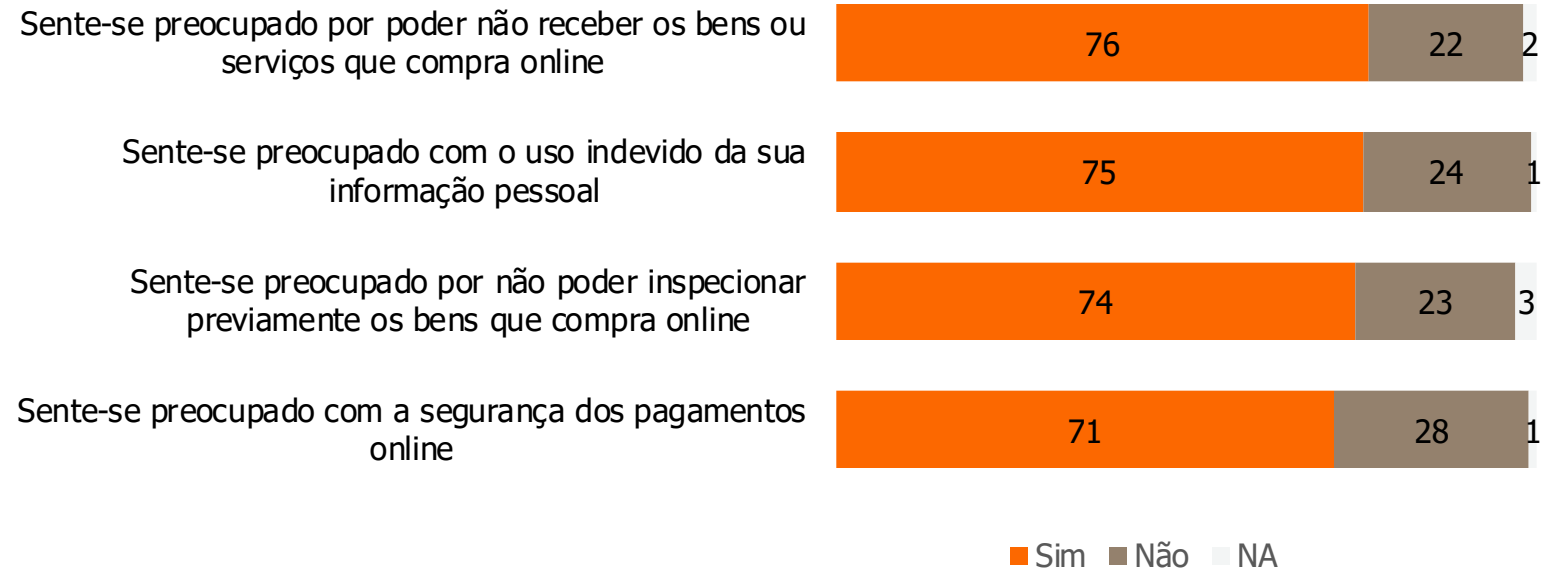




## Principais preocupações com compra / venda de bens e serviços e serviços de banca online / homebanking

9

**94%** Costuma realizar atividades online, nem que seja de vez em quando, como por exemplo, compra ou venda de bens ou serviços, serviços de banca online / Homebanking.

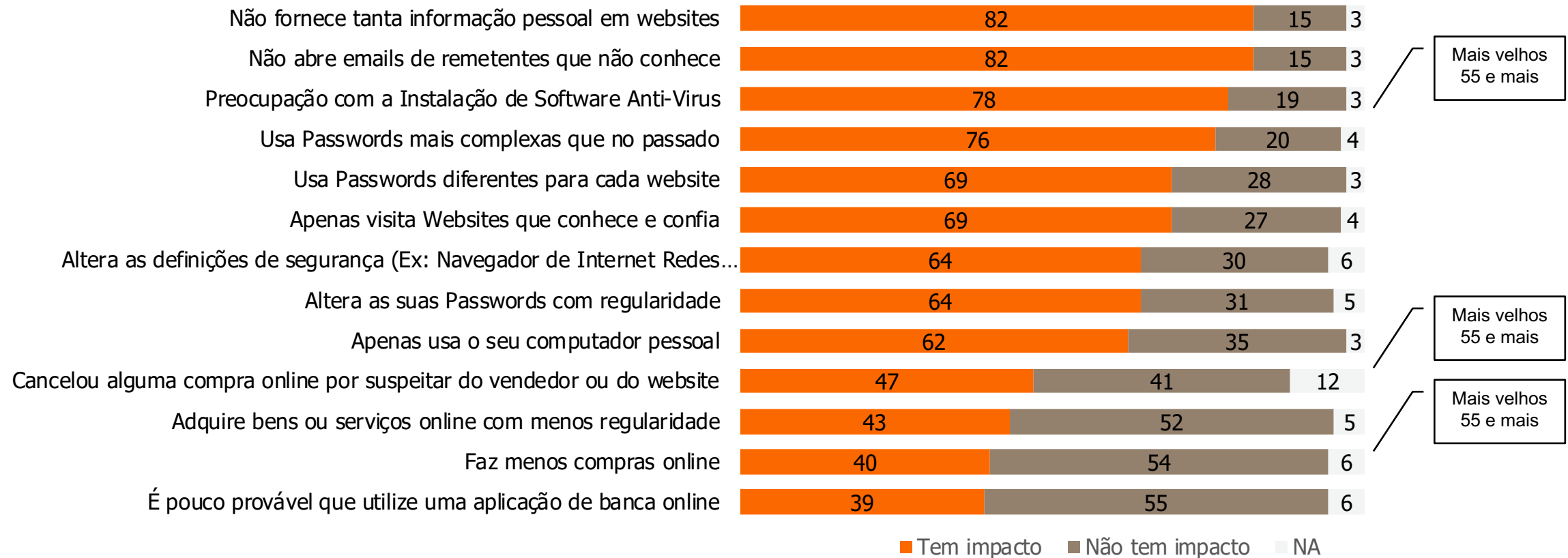


Valores em %  
Base n=556

P.3 Costuma realizar atividades online, nem que seja de vez em quando, como por exemplo, compra ou venda de bens ou serviços, serviços de banca online/Homebanking?  
P.3.1 – Quando realiza atividades online (compra ou venda de bens ou serviços, serviços de banca online/ Homebanking) sente alguma das seguintes preocupações?

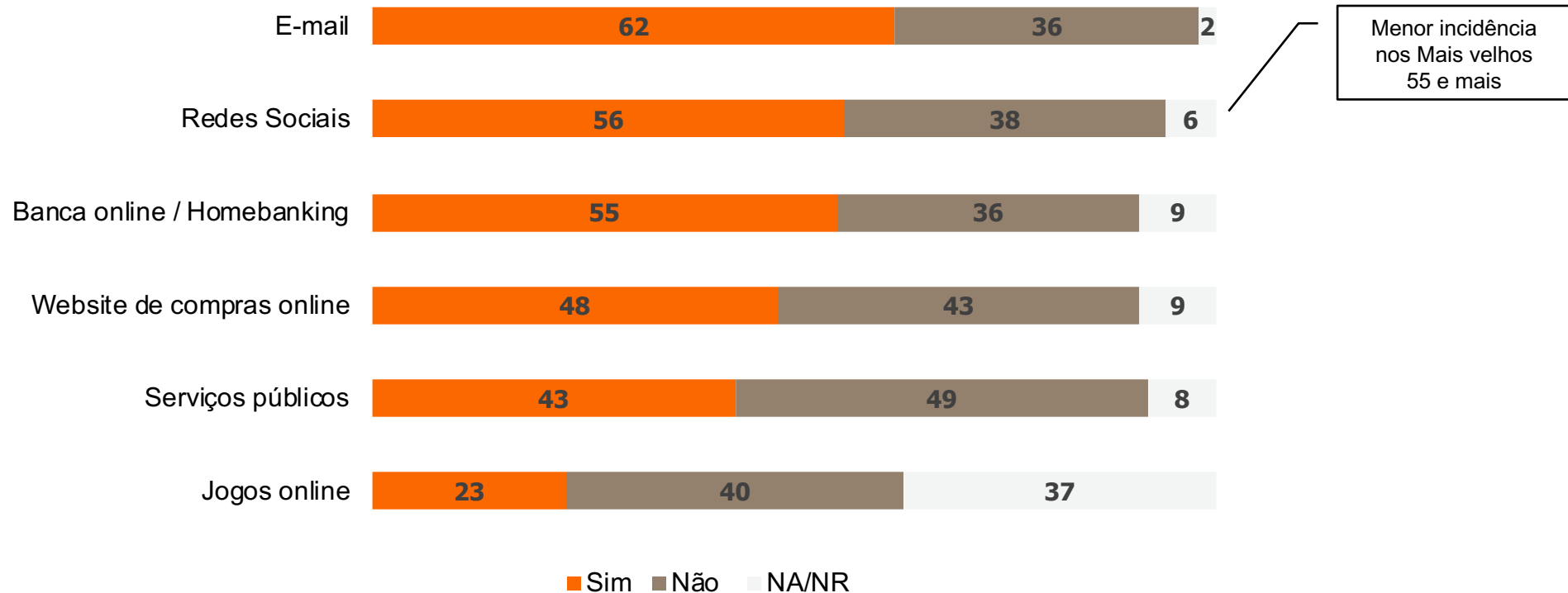
## Principais impactos na utilização de internet

10



## Alteração de Passwords nos últimos 12 meses

11



## Cibercrime

12

**24%** dos inquiridos

considera estar bastante bem informado sobre os riscos inerentes ao Cibercrime. 63% considera estar algo informado e 13% considera que está pouco ou nada informado.

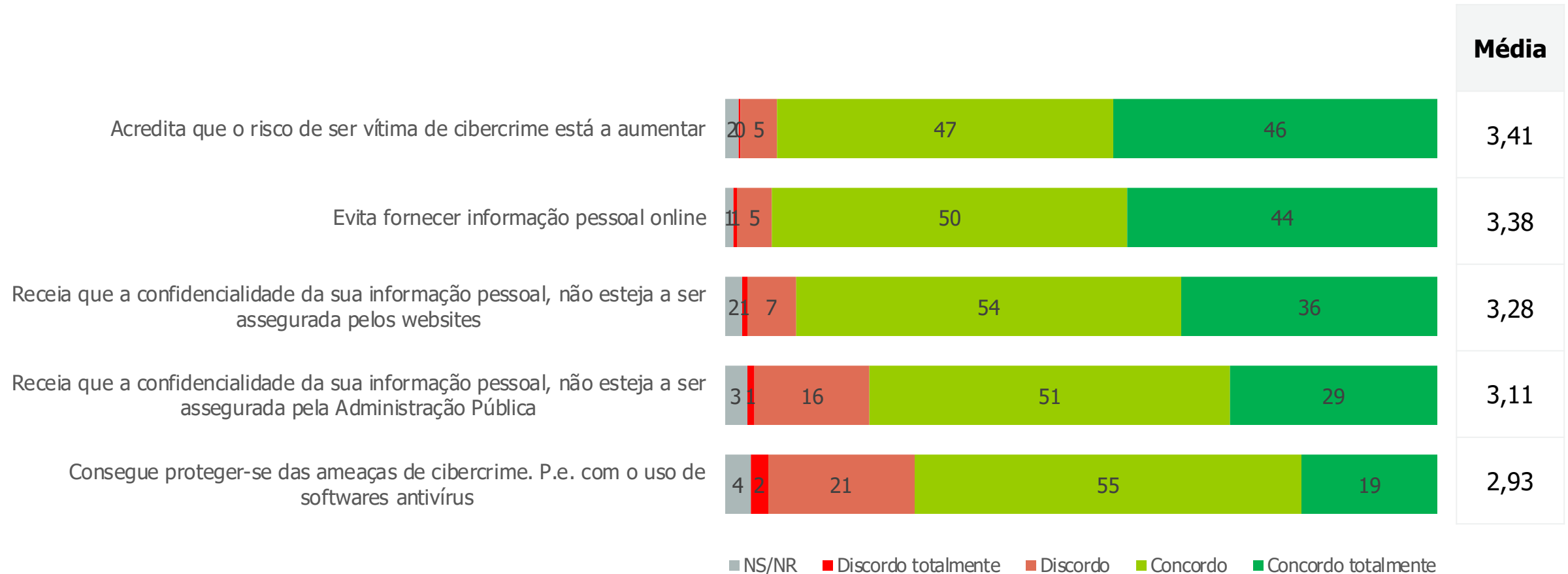
**Média 3,11**  
Escala de 1 a 4, ponto médio 2,5

São principalmente os “mais velhos” com 55 e mais anos de idade que se consideram menos bem informados (média 3,03)

# Perceções sobre Cibercrime

Até que ponto concorda com as seguintes afirmações

13



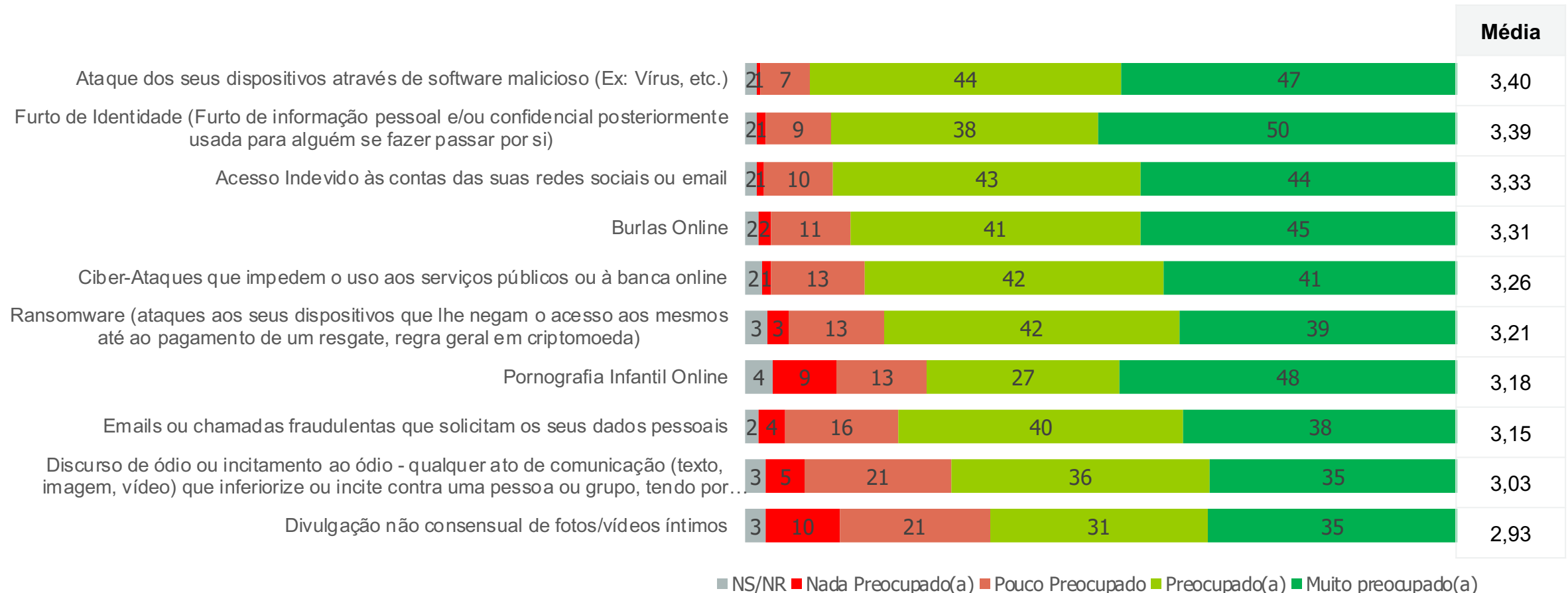
Valores em %  
Base n=591

P.6 Até que ponto concorda com as seguintes informações  
Escala de 1 a 4, 1 = discordo totalmente e 4 = concordo totalmente, ponto médio 2,5

# Perceções sobre Cibercrime

## Até que ponto está preocupado com...

14

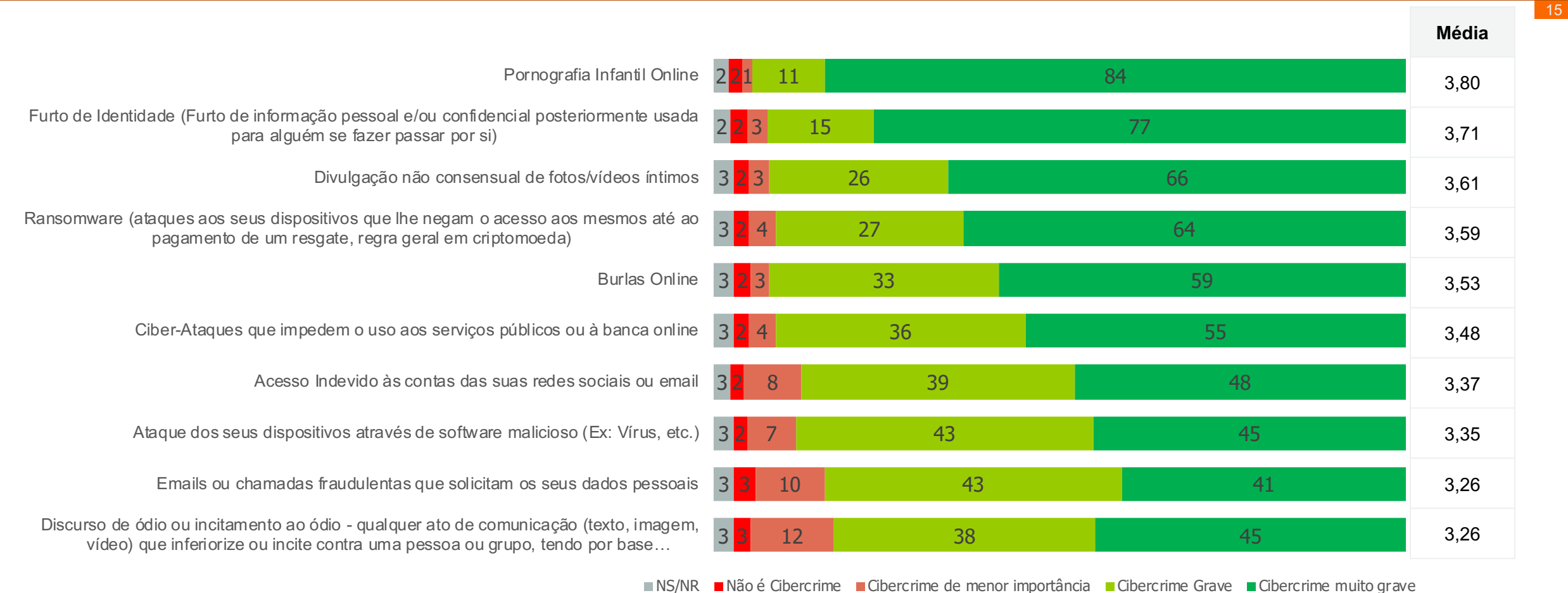


Valores em %  
Base n=591

P.7 – O Cibercrime pode incluir diferentes tipos de atividade criminosa. Até que ponto está preocupado(a) em ser vítima ou viver algum dos seguintes tipos de situação?  
Escala de 1 a 4, 1 = discordo totalmente e 4 = concordo totalmente, ponto médio 2,5

# Perceções sobre Cibercrime

Até que ponto considera que as seguintes situações podem ser consideradas cibercrime...



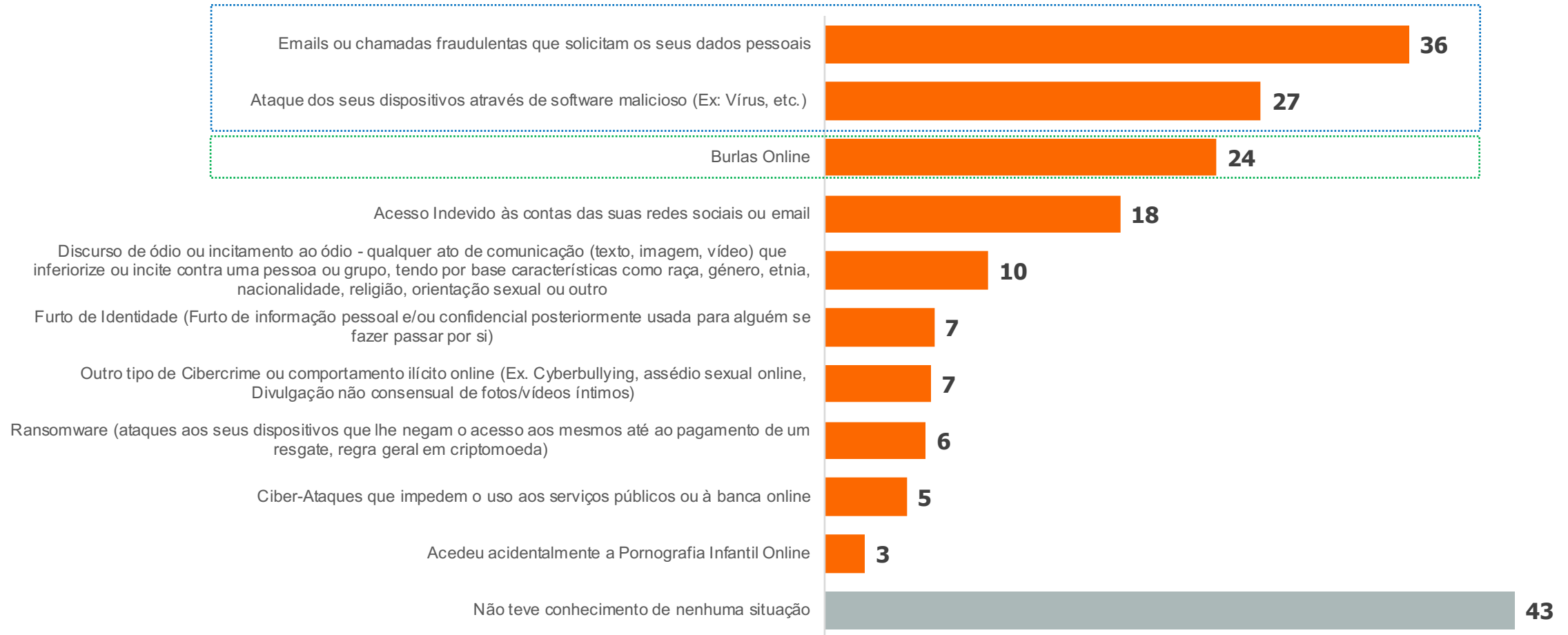
Valores em %  
Base n=591

P.8 Indique por favor até que ponto considera que as seguintes situações podem ser consideradas cibercrime? Vamos usar uma escala de 1 a 4, 1 = não é cibercrime e 4 = cibercrime muito grave, ponto médio 2,5

# Perceções sobre Cibercrime

Nos últimos três anos algum dos seus familiares, amigos ou conhecidos tiveram conhecimento ou foram vítimas de...

16



Valores em %  
Base n=591

P.9 Nos últimos três anos algum dos seus familiares, amigos ou conhecidos tiveram conhecimento ou foram vítimas de algum deste tipo de situações? (REGISTE TODOS OS QUE SE APLICAM)



# Perceções sobre Cibercrime

Nos últimos três anos foi vítima ou viveu algumas das seguintes situações...

17



# Perceções sobre Cibercrime

## Ações que tomou

18

Ações que tomou...	Situações que experienciou...			
	Ataque dos seus dispositivos através de software malicioso (Ex: Vírus, etc.)	Burlas Online	Acesso Indevido às contas das suas redes sociais ou email	Emails ou chamadas fraudulentas que solicitam os seus dados pessoais
Instalação de antivírus	45			
Formatação / Reparo / Limpeza do computador	15			
Contactar especialista Informático	11			
Bloqueio do Computador / Bloqueio da conta	3			
Ignorar mensagens ou chamadas / Não fornecer dados / Apagar mensagens / Spam	3	7	4	55
Denúncia: à Polícia / ao website / às entidades responsáveis	3	32	16	12
Utilização / Atualização de Sistemas de bloqueio (Firewall)	3			
Informar ao banco / Cancelar de cartões e pagamentos		15		
Aumentar cuidados, segurança, atenção		3	5	
Alterar palavras-passe			51	
Cancelar contas			9	
Bloqueio: E-mails, Mensagens, Chamadas, Websites suspeitos				13

Base n=120

Base n=69

Base n=57

Base n=179

Valores em %

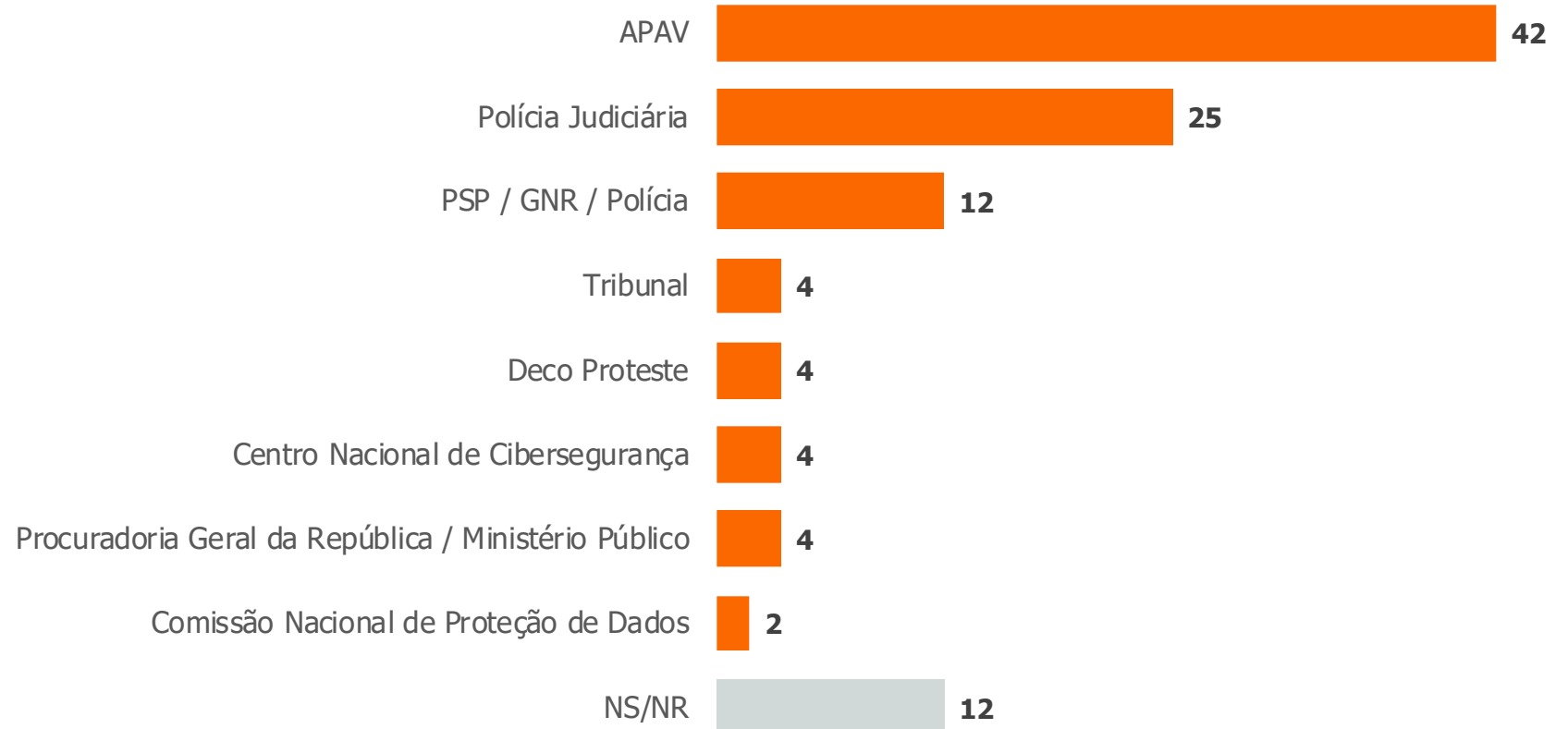
P.10.1 Se foi vítima de alguma(s) das situações anteriormente descritas que ações tomou?  
Referências com 3% ou mais

# Perceções sobre Cibercrime

## Estruturas de apoio a vítimas de cibercrime

19

Apenas **10%** dos inquiridos declara ter conhecimento de alguma estrutura em Portugal que preste Apoio a Vítimas de Cibercrime



Valores em %  
Base n=57

P.12 Conhece alguma Estrutura em Portugal que preste Apoio a Vítimas de Cibercrime?  
P.12.1 Qual ou quais as estruturas que conhece em Portugal que prestam Apoio a Vítimas de Cibercrime?

# Perceções sobre Cibercrime

## Estruturas de apoio a vítimas de cibercrime

# 17%

do total da amostra tem conhecimento da linha Internet Segura e entendem que presta apoio para...



# 7%

já contactou ou conhece alguém que tenha contactado com a linha Internet Segura, procurando apoio para...

	Valores absolutos
Apoio tendo sido vítima de cibercrime (Ex: vítima de cyberbullying, divulgação não consensual de imagens e vídeos, burla online, furto de identidade, acesso ilegítimo, etc.)	4
Apoio na remoção de conteúdos ilegais Online (Pornografia Infantil, Discurso de Ódio, Incitamento à Violência)	3
Pedidos de ações de sensibilização	1
Ajuda técnica	3
Base	(7)

Valores em %  
Base n=98

Base n=7

P.13 Tem conhecimento da Linha Internet Segura?

P.14A No seu entender que tipo de apoio presta a Linha Internet Segura? (Questão aberta)

P.14B Já contactou a Linha Internet Segura ou conhece alguém que o tenha feito? P.14A No seu entender que tipo de apoio presta a Linha Internet Segura?

P.15 Que tipo de apoio procurou e/ou caso o apoio tenha sido procurado por terceiro qual o tipo de apoio prestado?

## Monitorização da atividade online de crianças e jovens

**35%** dos inquiridos  
declara ter alguma criança ou  
jovem, com menos de 16  
anos de idade, à sua guarda  
ou cuidado

**74%**  
Monitorizo a  
atividade  
online da  
criança / jovem

**58%**  
Discuto a  
temática dos  
riscos online  
com a criança /  
jovem

**45%**  
O tempo que a  
criança / jovem  
passa online  
está limitado

**42%**  
Uso controlos  
parentais no meu  
navegador de  
internet

Valores em %  
Base n=208

P.11A – O(a) Sr.(a) tem alguma criança ou jovem, com menos de 16 anos de idade à sua guarda ou cuidado?  
P.11B Pensando especificamente no tipo de situação online (pornografia infantil, cyberbullying, grooming – assédio sexual de menores para fins sexuais, Etc.) que coloca em risco crianças e jovens (idades inferiores a 16 anos), que medidas de segurança adotou para garantir que a criança ou jovem que tem à sua guarda e cuidado não seja vítima deste tipo de situações? (REGISTE TODOS OS QUE SE APLICAM)

3

# Síntese

# Análise Síntese

23

Praticamente a totalidade da amostra acede á internet a partir de PC's / Computador / Laptop ou Smartphone, sendo que, uma grande maioria está sempre ligado em casa (60%), no local de trabalho (50%) ou em qualquer local (37%).

As atividades mais realizadas são a consulta de e-mail, o acesso a redes sociais e a leitura de notícias.

94% realiza ou já realizou compra / venda de bens e/ou serviços e / ou serviços de banca online.

No que concerne às principais preocupações com a utilização de internet, mais de três quartos refere que não fornece informação pessoal, não abre e-mails de remetentes desconhecidos, preocupa-se com a utilização de antivírus e usa passwords mais complexas. No entanto, apenas sensivelmente metade dos inquiridos alterou as suas passwords nos últimos 12 meses.

13% dos inquiridos, com maior incidência no escalão etário mais elevado, considera que está pouco ou nada informado sobre os riscos do Cibercrime vs 24% que considera estar bastante bem informado. Mais de metade considera ter alguma informação.

# Análise Síntese

24

E-mails ou chamadas fraudulentas, ataques aos dispositivos por meio de softwares maliciosos e burlas online são as situações mais referenciadas com experiência pessoal ou de familiares, amigos e /ou conhecidos.

Apenas 17% tem conhecimento (98 inquiridos) refere conhecer a Linha Internet Segura, à qual 7 indivíduos declaram já ter usado ou conhecer quem tenha usado.

De entre os inquiridos que têm crianças ou jovens com menos de 16 anos a seu cargo (208), a monitorização da atividade online da criança é a ação mais adotada como medida de segurança, sendo que 42% refere também usar controlos parentais no browser de internet.



# Cibercrime

## Alguns exemplos atuais

25

### Cuidado! Não instale a aplicação COVID-19 Tracker

O Centro Nacional de Cibersegurança alerta para não confiar nem instalar a aplicação COVID-19 Tracker no telemóvel. Trata-se de um "esquema de ransomware para equipamentos Android", que, após a sua instalação, "bloqueia o dispositivo e exige um resgate" em bitcoins.

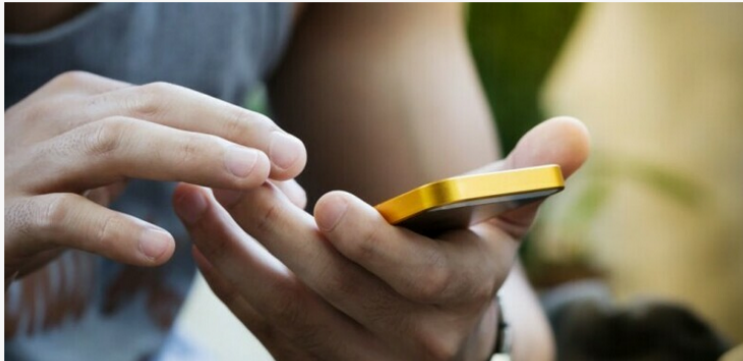
Susete Henriques  
18 Março 2020 — 01:39



#### TÓPICOS

- Cibercrime
- COVID-19
- País

#### Relacionados



O CNCS alerta ainda para esquemas de fraude digital partilhados por e-mail ou em redes sociais, que divulgam iniciativas de 'crowdsourcing' para a recolha de donativos para falsas campanhas de compra de material médico ou de proteção pessoal.

Perigosos são ainda "SMS enviados a informar que, de acordo com a lei, estão a ser aplicadas medidas extraordinárias para o combate à Covid-19 e que todos os cidadãos nacionais serão vacinados, sendo garantido um reembolso dos custos pelo governo. Para tal, bastaria pagar uma determinada quantia indicada no SMS e através do registo no link enviado seriam posteriormente ressarcidos".

Campanhas de "phishing" - através de email, SMS ou das redes sociais - a coberto da imagem de entidades oficiais como a Organização Mundial de Saúde, a UNICEF ou centros de investigação e laboratórios do setor da saúde, com conteúdos alusivos à pandemia.

Neste caso, existem anexos que uma vez usados permitem a captação de dados pessoais, ou a infeção dos computadores.