DGEEC

DIREÇÃO-GERAL DE ESTATÍSTICAS DA EDUCAÇÃO E CIÊNCIA

A SEGURANÇA DAS TIC (CIBERSEGURANÇA) NA ADMINISTRAÇÃO PÚBLICA

Inquéritos à Utilização das Tecnologias da Informação e Comunicação na Administração Pública Central, Regional e nas Câmaras Municipais

- IUTICAP e IUTICCM 2022 -

DGEEC | Janeiro de 2024

Título
A SEGURANÇA DAS TIC (CIBERSEGURANÇA) NA ADMINISTRAÇÃO PÚBLICA - IUTICAP e IUTICCM 2022

Autor
Direção-Geral de Estatísticas da Educação e Ciência (DGEEC)
Direção de Serviços de Estatísticas da Ciência e Tecnologia e da Sociedade de Informação (DSECTSI)
Gonçalo Silva (recolha e apuramento de dados; relatório)
Ana Martins (Chefe de Equipa, relatório)
Catarina Carreira (Direção de Serviços, relatório)
Nuno Neto Rodrigues e Filomena Oliveira (Direção)

Edição
Direção-Geral de Estatísticas da Educação e Ciência (DGEEC)
Av. 24 de Julho, n.º 134
1399-054 Lisboa, PORTUGAL
Tel.: (+351) 213 949 200
E-mail: dgeec@dgeec.medu.pt
URL: https://www.dgeec.medu.pt
Imagem de capa: https://pixabay.com

ÍNDICE

| NOTA INTRODUTÓRIA

A Direção-Geral de Estatísticas da Educação e Ciência (DGEEC) divulga nesta publicação indicadores de Segurança das Tecnologias da Informação e Comunicação (TIC) apurados a partir dos Inquéritos à Utilização das Tecnologias da Informação e Comunicação de 2022, dirigidos à Administração Pública Central e Regional (IUTICAP) e às Câmaras Municipais (IUTICCM).

Os resultados do IUTICAP e do IUTICCM possibilitam a construção de indicadores de caracterização e evolução, em matéria de Sociedade de Informação e Tecnologias da Informação e Comunicação, na Administração Pública. Tratam-se de duas operações estatísticas realizadas com uma periodicidade anual e inscritas no Sistema Estatístico Nacional (SEN).

Os indicadores de Segurança das TIC (Cibersegurança) incluem componentes, tecnologias, serviços, recomendações e procedimentos aplicados em sistemas TIC, a fim de garantir a integridade, autenticidade, disponibilidade e confidencialidade dos dados e dos sistemas de informação, neste caso particular, dos Organismos da Administração Pública, nomeadamente:

- Tecnologias e aplicações de segurança das TIC utilizadas nos Organismos (ex.: segurança de redes e correio eletrónico, software antivírus, firewall).
- Medidas de segurança das TIC implementadas nos Organismos.
- Formação e consciencialização em matéria de segurança das TIC.
- Recursos afetos à realização de atividades de segurança das TIC.
- Incidentes de segurança das TIC.

Em termos de Cibersegurança na Administração Pública, salienta-se, em 2022, que:

- Relativamente à existência de uma estratégia para a segurança de informação, 63% dos Organismos da Administração Central, 60% das Câmaras Municipais, 59% dos Organismos da Região Autónoma (R.A) dos Açores e 38% dos Organismos da R.A. da Madeira indicaram ter uma estratégia definida e estruturada.

- Numa análise por regiões (NUTS II) verificou-se que, na Península de Setúbal, 89% das Câmaras Municipais implementaram uma estratégia para a segurança da informação e, na Grande Lisboa, foram 78%. De destacar que, a nível da NUTS III, a Região do Tâmega e Sousa, em termos percentuais, apresentou o valor mais elevado do país para este indicador (91%).

- Para a quase totalidade dos Organismos da Administração Pública que indicaram ter definida uma estratégia para a segurança da informação, esta encontrava-se de acordo com o Regulamento Geral da Proteção de Dados (RGPD) ou em fase de revisão para dar cumprimento ao mesmo. No que respeita ao Regime Jurídico da Segurança do Ciberespaço (RJSC), a percentagem é inferior, mas ainda assim a maioria indicou que a sua estratégia já se encontrava de acordo com este Regime ou estava em fase de revisão

- A quase totalidade dos Organismos utilizou software anti-vírus, firewall, filtros anti-spam e segurança de correio eletrónico como aplicações de segurança das TIC, com particular destaque para os dois primeiros que assumiram percentagens de 99% para as Câmaras Municipais e 98% para os Organismos da R.A. da Madeira.

- Em termos de medidas implementadas, a quase totalidade dos Organismos efetuou atualizações regulares do software e, mais de 90% dos Organismos da Administração Central, das Câmaras Municipais e da R.A dos Açores, implementaram medidas de controlo de acessos remotos às suas redes.

- As Câmaras Municipais foram as que mais indicaram ter necessidade elevada de reforço de competências em segurança das TIC (86%), destacando-se largamente dos restantes Organismos. Seguiram-se os Organismos da Administração Pública Central (70%) e os da R.A. dos Açores e da Madeira (55% e 47%, respetivamente).

• Neste âmbito, verifica-se que a totalidade das Câmaras Municipais das Regiões do Alto Minho, Ave, Terras de Trás-os-Montes, Beira Baixa, Península de Setúbal e Alentejo Litoral indicaram necessitar de reforçar as competências em segurança das TIC. Na maioria das restantes regiões os valores situam-se acima dos 60%.

• Relativamente à existência de problemas de segurança informática, foram os Organismos da Administração Central que detetaram o maior número de incidentes (21%), seguidos das Câmaras Municipais (16%) e dos Organismos da R.A. da Madeira e da R.A. dos Açores com 7% e 5%, respetivamente.

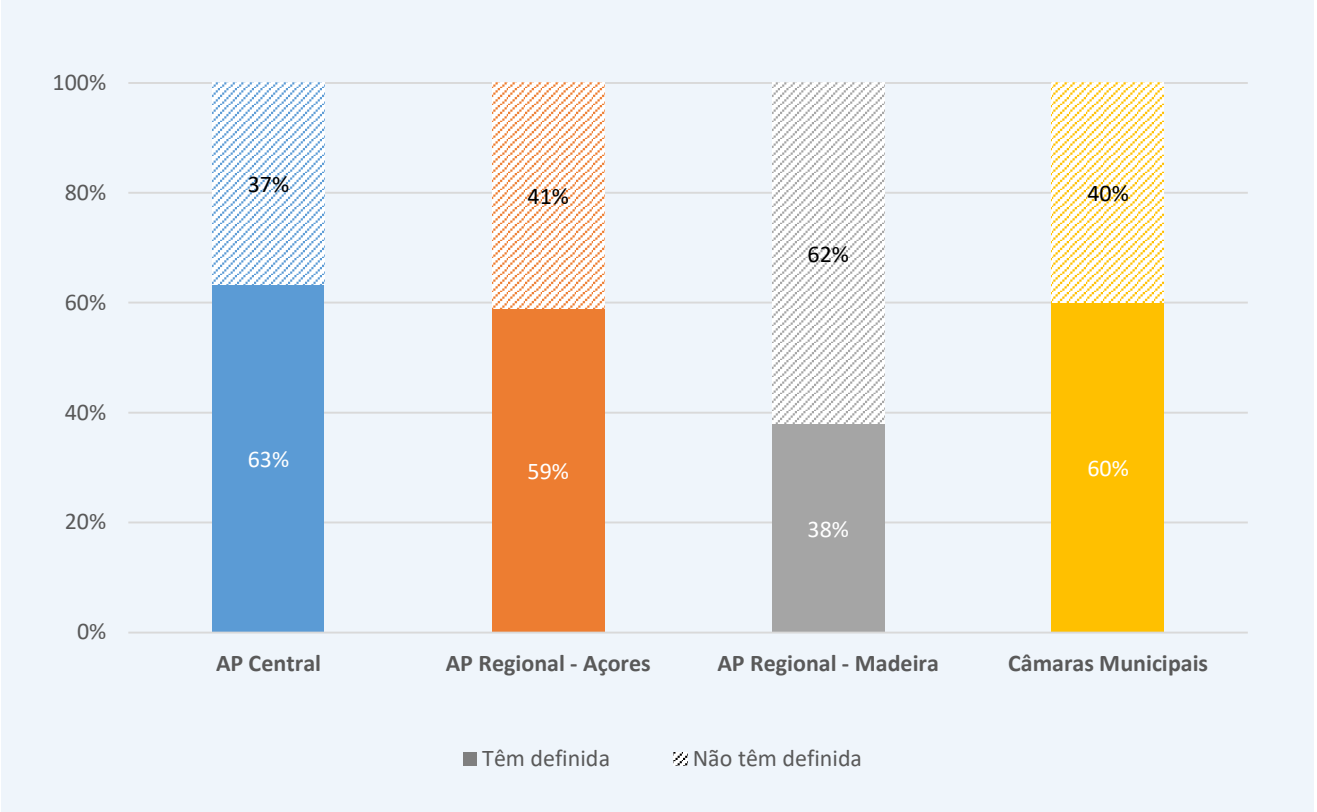
Os dados desta publicação apresentam alguns dos indicadores mais relevantes destas operações estatísticas, relativos a 2022, podendo os restantes ser consultados nos Sumários Estatísticos do IUTIC2022, na página da DGEEC.

Lisboa, janeiro de 2024

Direção-Geral de Estatísticas da Educação e Ciência (DGEEC)
Direção de Serviços de Estatísticas da Ciência e Tecnologia e da Sociedade de Informação (DSECTSI)

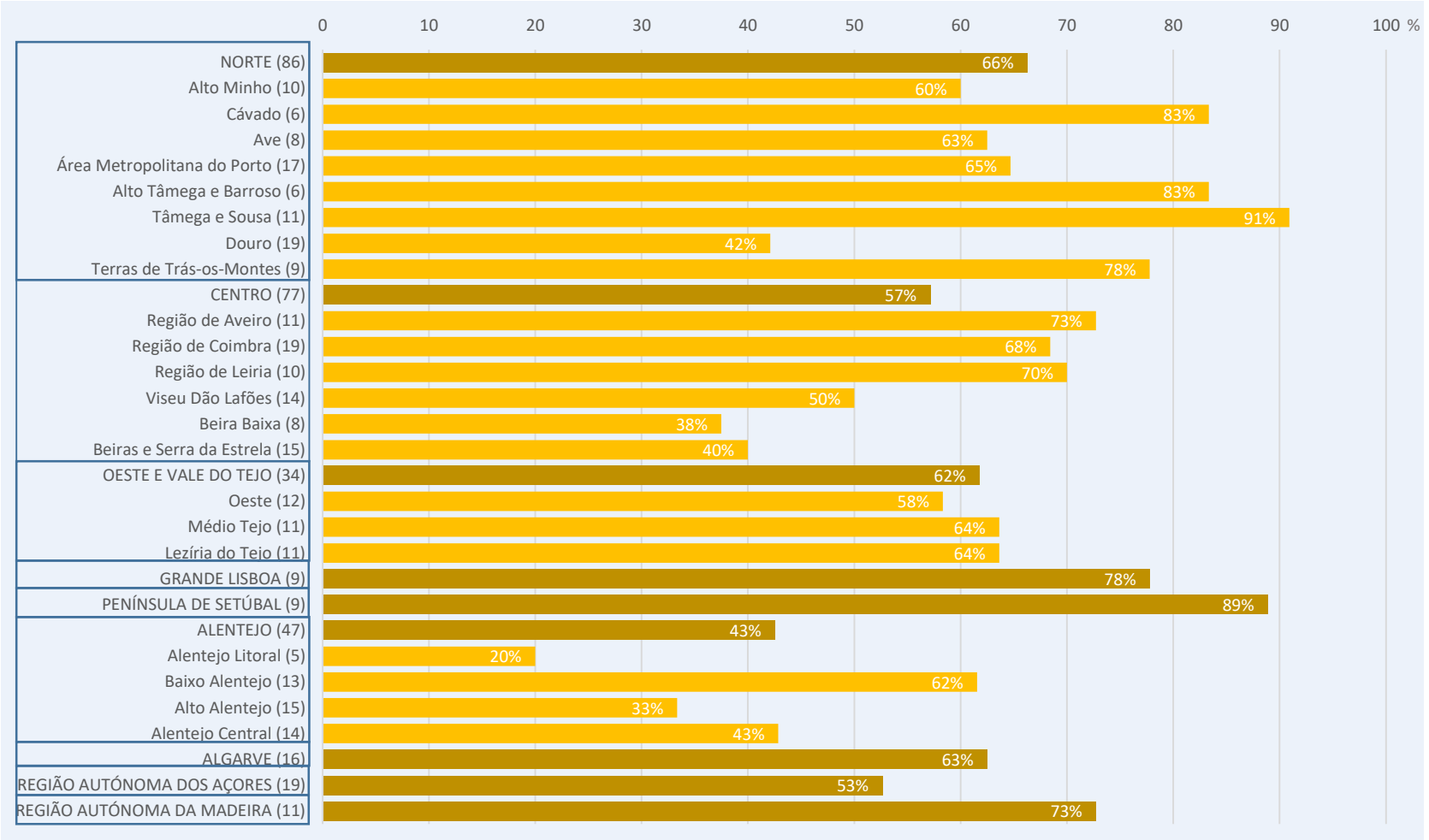
| INDICADORES DE CIBERSEGURANÇA NA ADMINISTRAÇÃO PÚBLICA EM 2022

Figura 1 - ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA QUE TÊM DEFINIDA UMA ESTRATÉGIA PARA A SEGURANÇA DA INFORMAÇÃO (%):



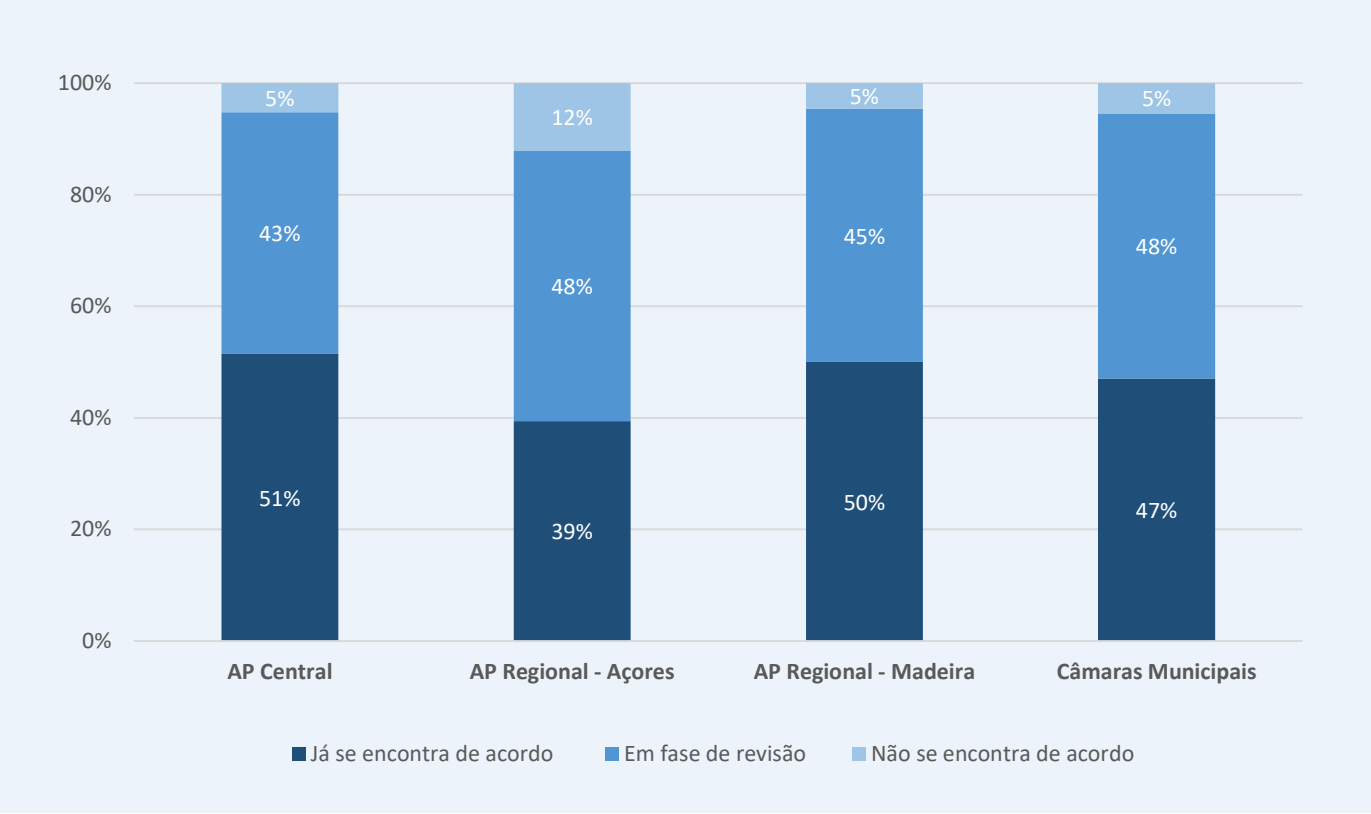
Fonte(s): DGEEC - Inquérito à Utilização das TIC na Administração Pública Central, Regional e Câmaras Municipais.

Figura 2 – CÂMARAS MUNICIPAIS QUE TÊM DEFINIDA UMA ESTRATÉGIA PARA A SEGURANÇA DA INFORMAÇÃO, POR NUTS[1] II E III (%):



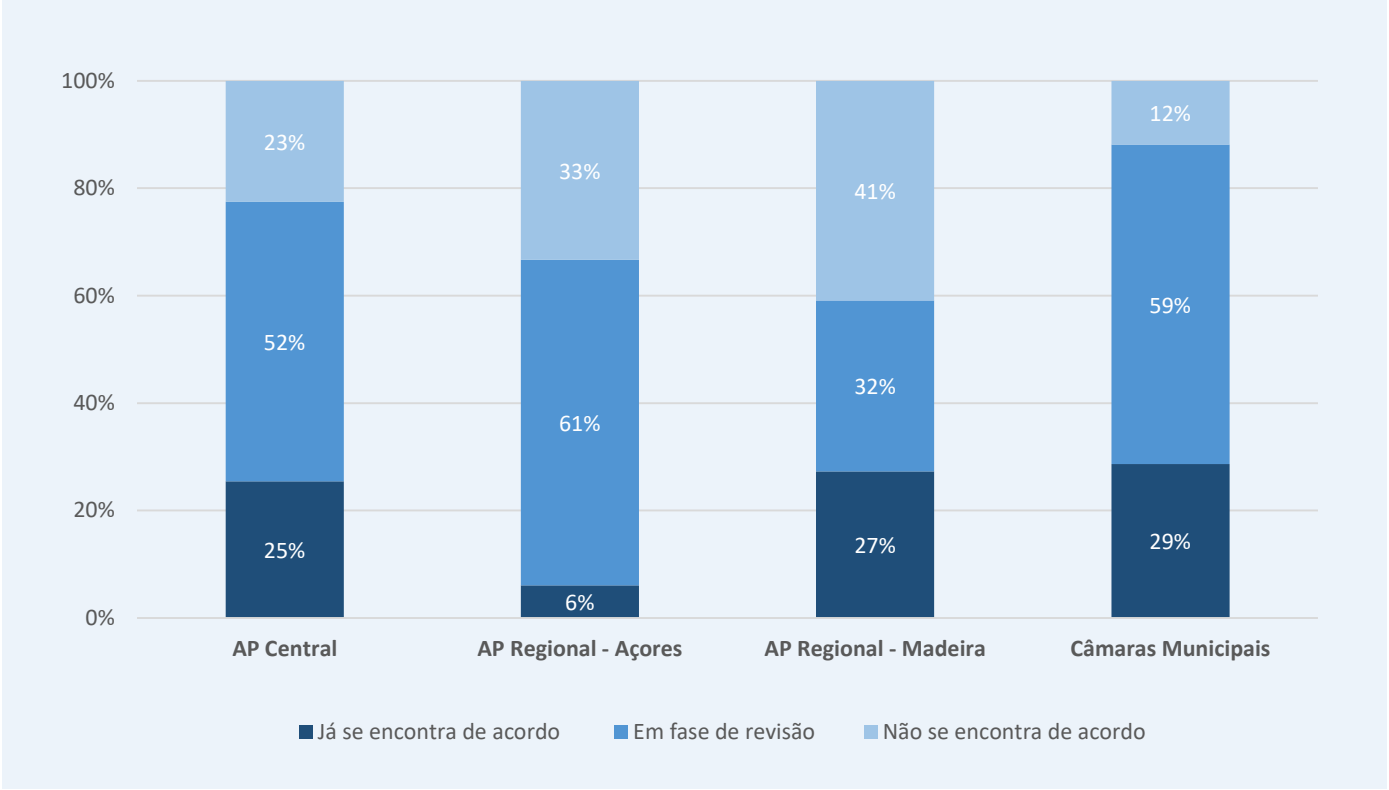
Nota(s):
[1] Nomenclatura das Unidades Territoriais para Fins Estatísticos (NUTS) 2024. Na figura, entre parêntesis, consta o número total de Câmaras Municipais na respetiva região.
- As percentagens são calculadas com base no N.º de Câmaras Municipais, na região (NUTS) correspondente.
Fonte(s): DGEEC - Inquérito à Utilização das TIC na Administração Pública Central, Regional e Câmaras Municipais.

Figura 3 - ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA QUE TÊM DEFINIDA UMA ESTRATÉGIA PARA A SEGURANÇA DA INFORMAÇÃO, POR TIPO DE CONFORMIDADE FACE AO REGULAMENTO GERAL DA PROTEÇÃO DE DADOS (RGPD) (%):



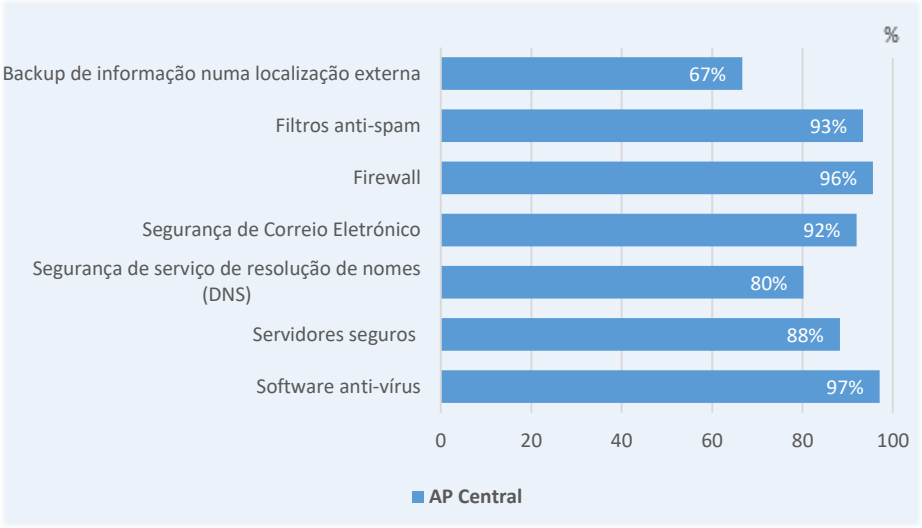
Fonte(s): DGEEC - Inquérito à Utilização das TIC na Administração Pública Central, Regional e Câmaras Municipais.

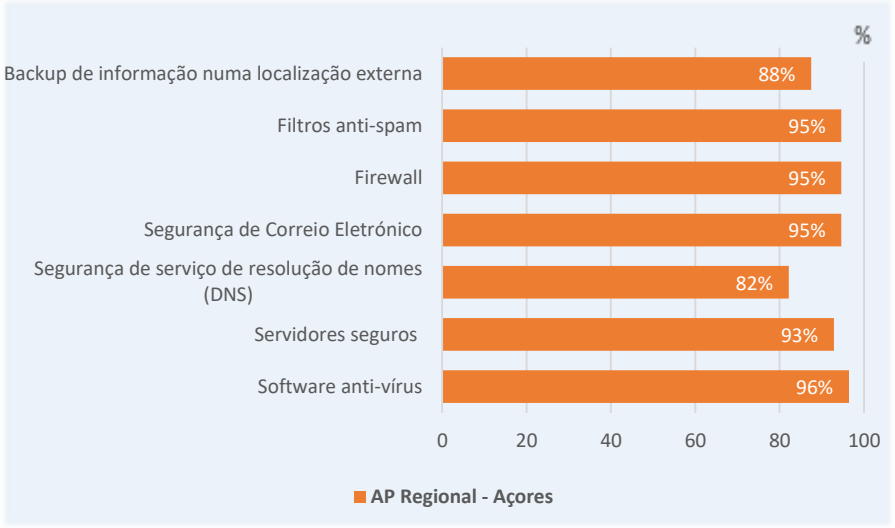
Figura 4 - ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA QUE TÊM DEFINIDA UMA ESTRATÉGIA PARA A SEGURANÇA DA INFORMAÇÃO, POR TIPO DE CONFORMIDADE FACE AO REGIME JURÍDICO DA SEGURANÇA DO CIBERESPAÇO (RJSC) (%):

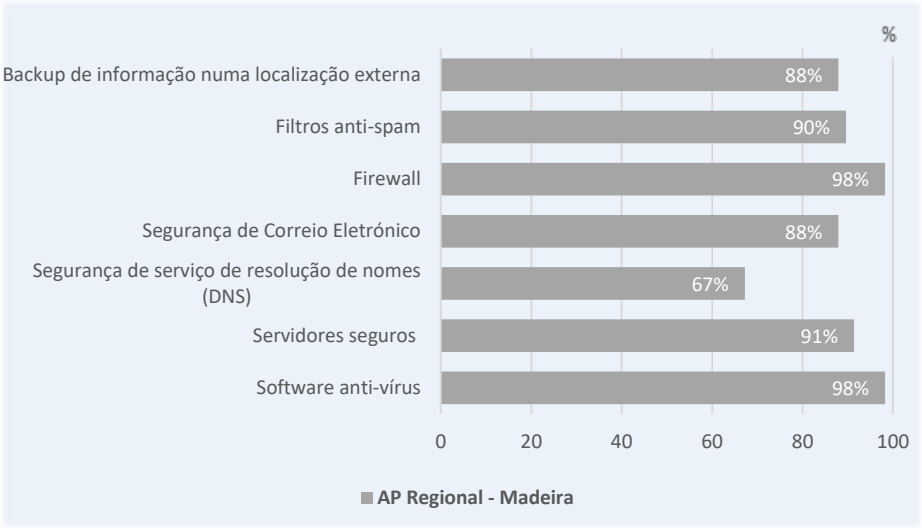


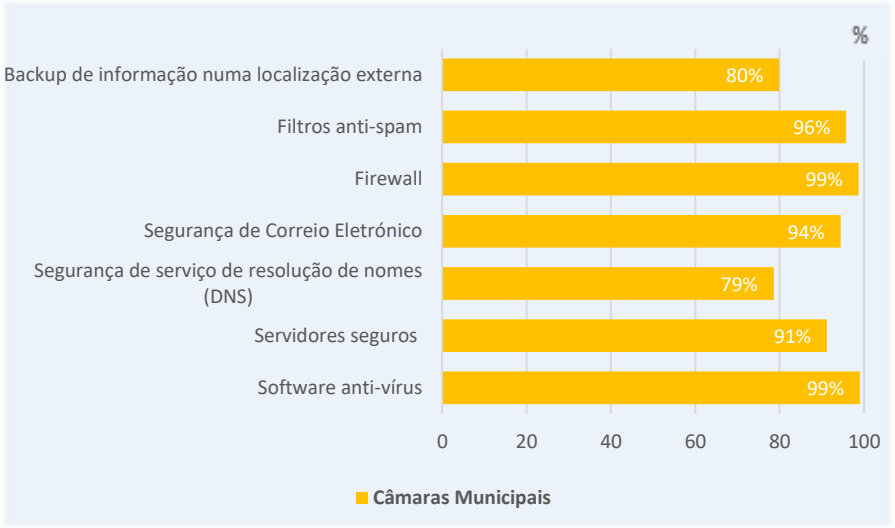
Fonte(s): DGEEC - Inquérito à Utilização das TIC na Administração Pública Central, Regional e Câmaras Municipais.

Figura 5 - ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA POR TIPO DE APLICAÇÕES DE SEGURANÇA DAS TIC UTILIZADAS (%):



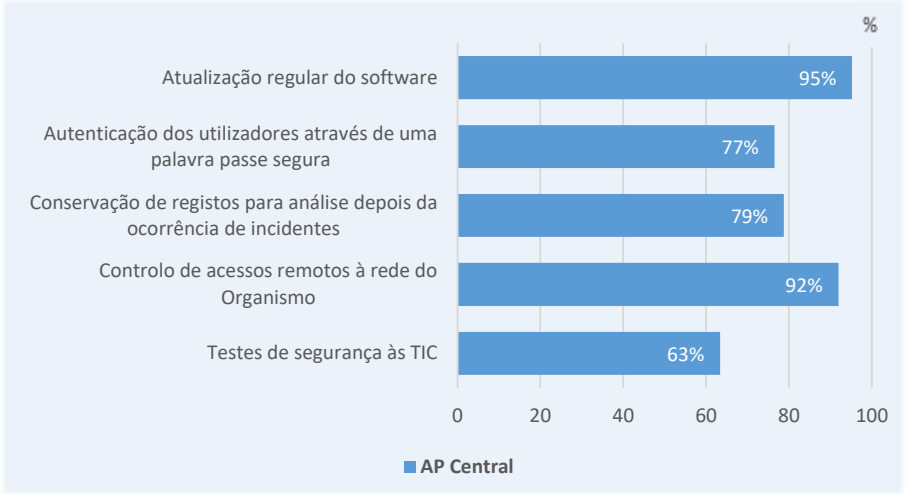


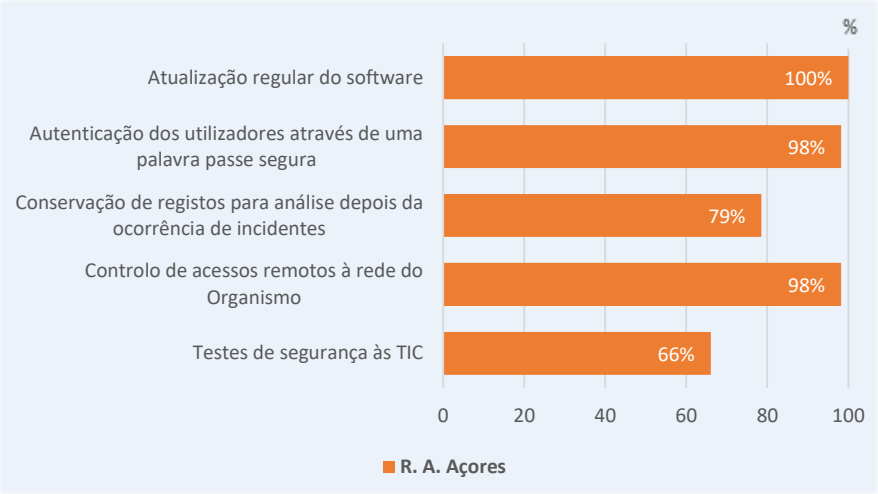


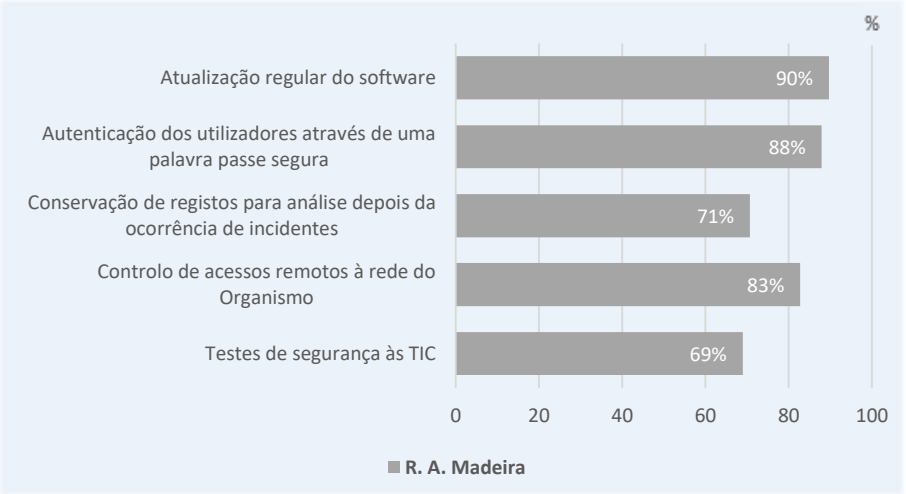


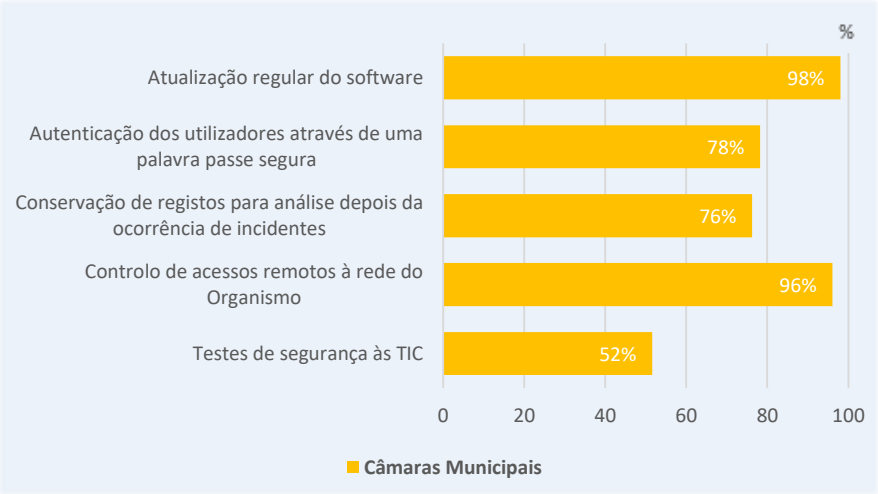
Fonte(s): DGEEC - Inquérito à Utilização das TIC na Administração Pública Central, Regional e Câmaras Municipais.

Figura 6 - ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA POR TIPO DE MEDIDAS DE SEGURANÇA DAS TIC IMPLEMENTADAS (%):



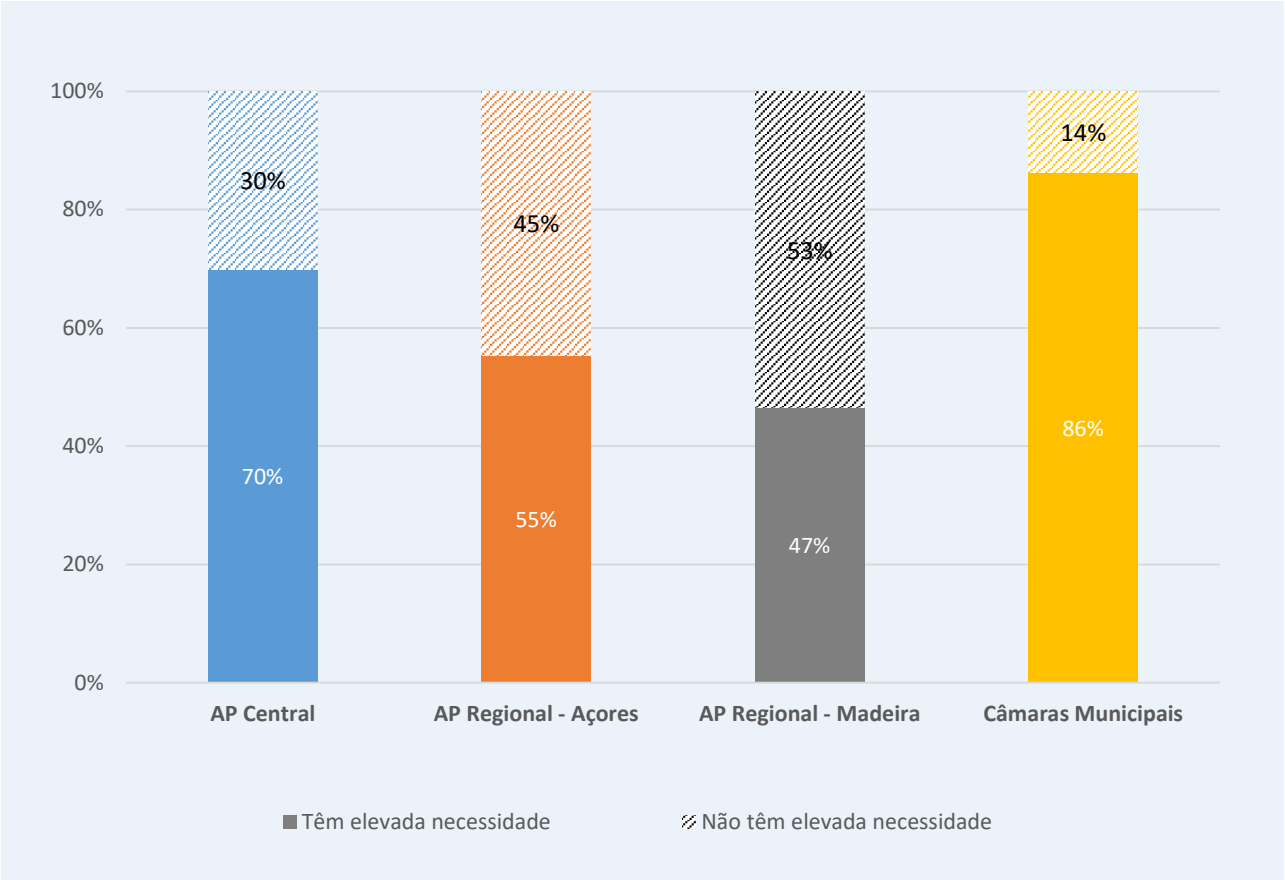






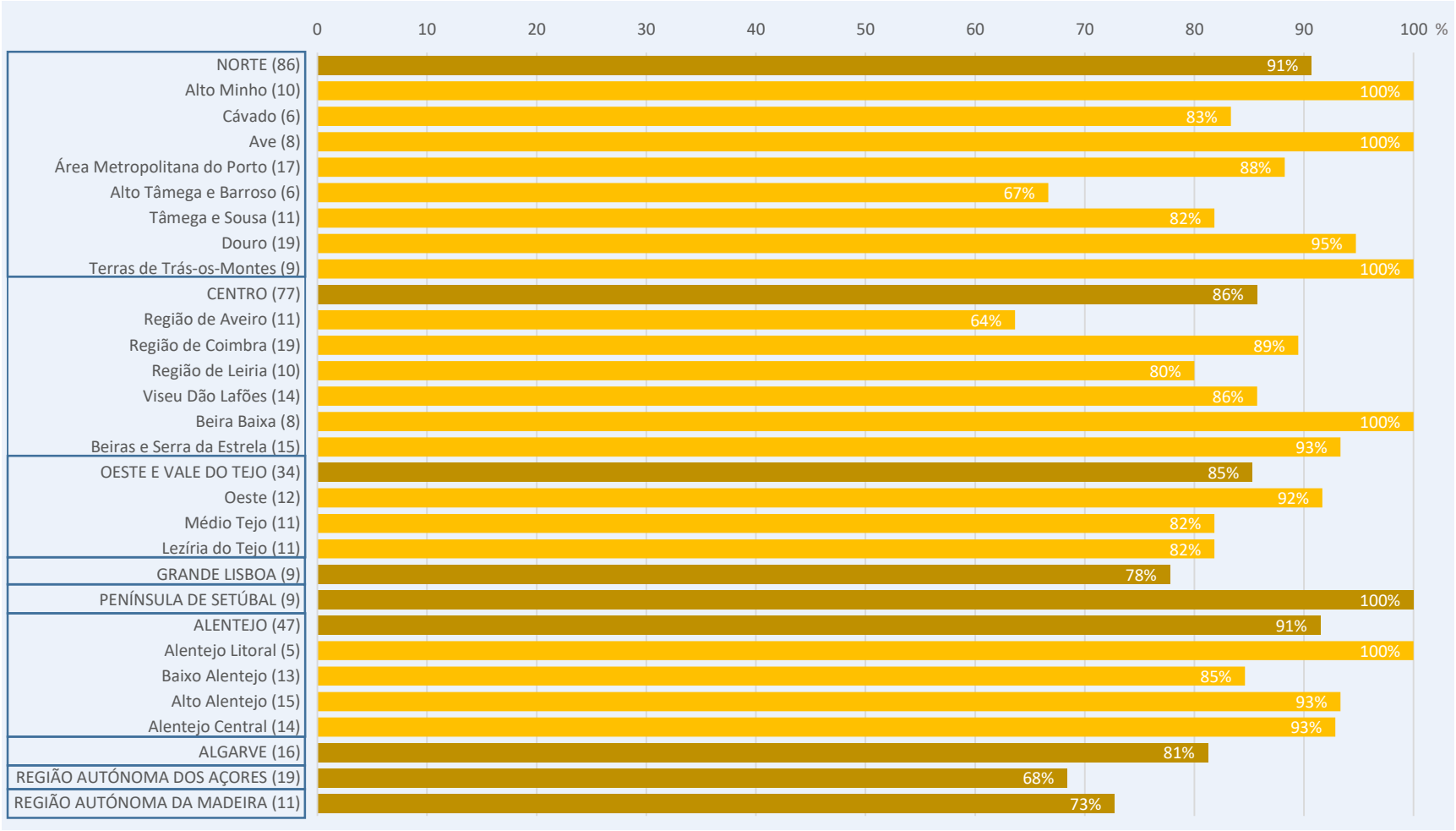
Fonte(s): DGEEC - Inquérito à Utilização das TIC na Administração Pública Central, Regional e Câmaras Municipais.

Figura 7 - ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA QUE INDICARAM TER ELEVADA NECESSIDADE DE REFORÇO DE COMPETÊNCIAS EM SEGURANÇA DAS TIC (%):



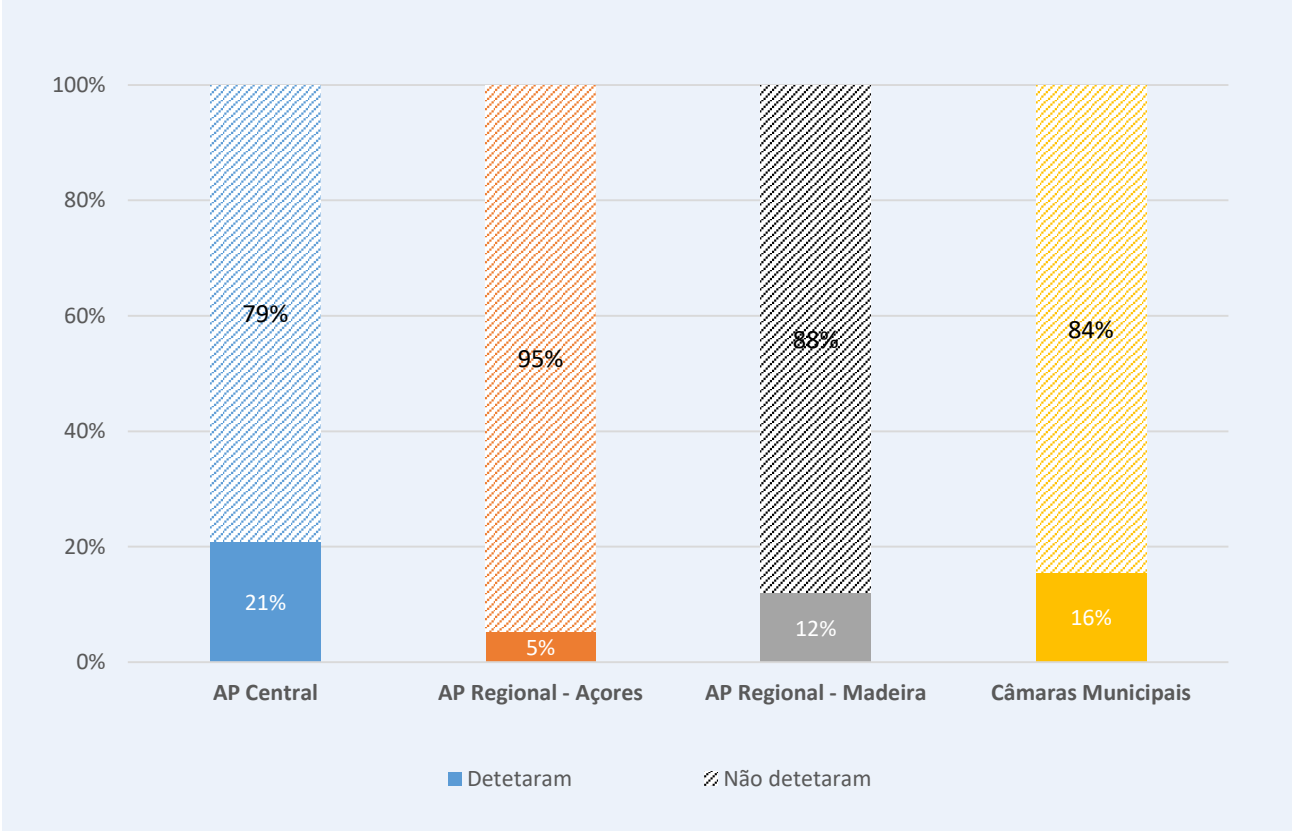
Fonte(s): DGEEC - Inquérito à Utilização das TIC na Administração Pública Central, Regional e Câmaras Municipais.

Figura 8 – CÂMARAS MUNICIPAIS QUE INDICARAM TER ELEVADA NECESSIDADE DE REFORÇO DE COMPETÊNCIAS EM SEGURANÇA DAS TIC, POR NUTS[1] II E III (%):



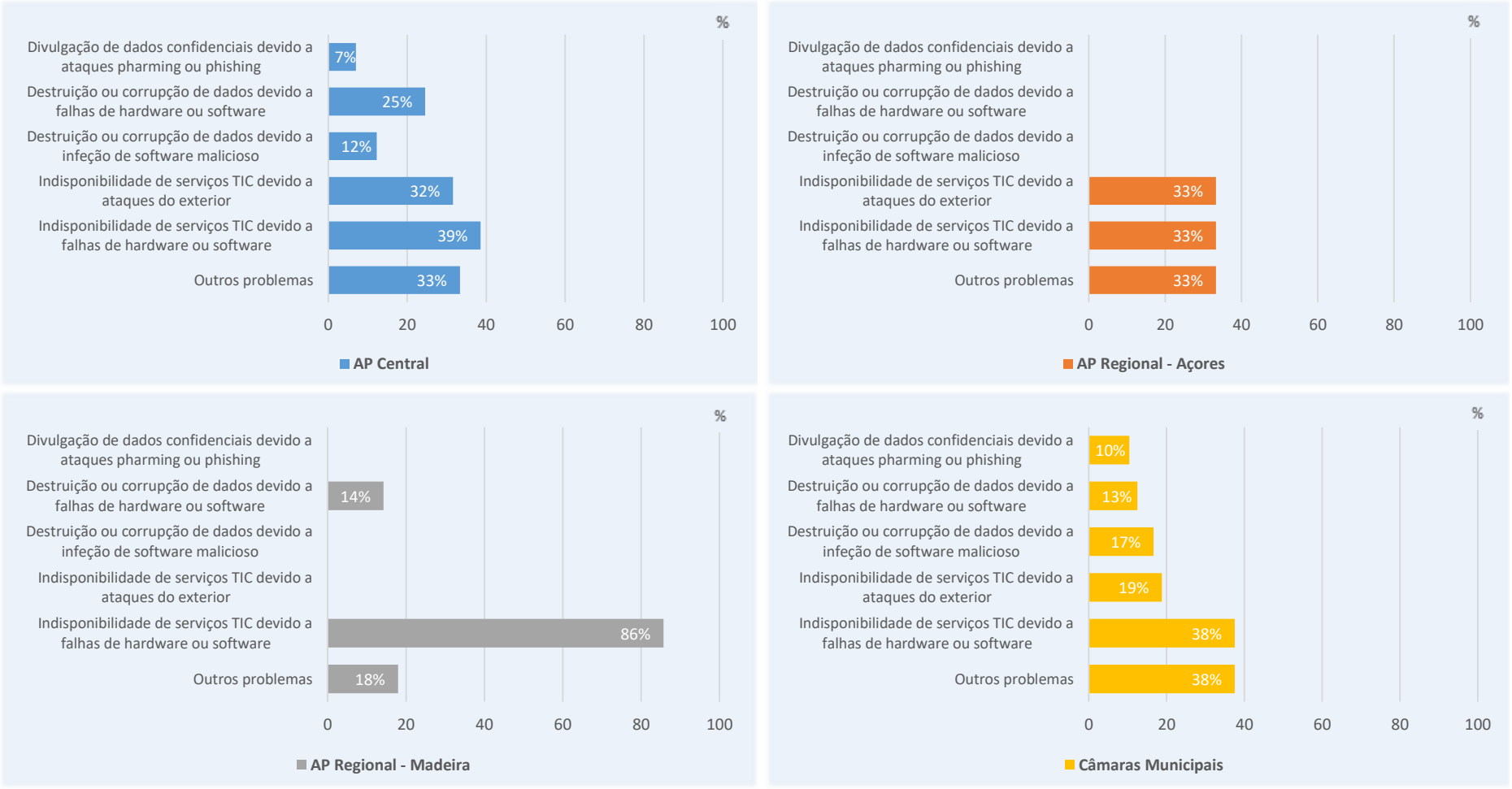
Nota(s):
[1] Nomenclatura das Unidades Territoriais para Fins Estatísticos (NUTS) 2024. Na figura, entre parêntesis, consta o número total de Câmaras Municipais na respetiva região.
- As percentagens são calculadas com base no N.º de Câmaras Municipais, na região (NUTS) correspondente.
Fonte(s): DGEEC - Inquérito à Utilização das TIC na Administração Pública Central, Regional e Câmaras Municipais.

Figura 9 - ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA QUE DETETARAM PROBLEMAS DE SEGURANÇA INFORMÁTICA[2] (%):



Nota (s): [2] Os dados deste indicador reportam ao ano anterior ao de referência do inquérito.
Fonte(s): DGEEC - Inquérito à Utilização das TIC na Administração Pública Central, Regional e Câmaras Municipais.

Figura 10 - ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA QUE DETETARAM PROBLEMAS DE SEGURANÇA INFORMÁTICA, POR TIPO DE CONSEQUÊNCIA DE SEGURANÇA DAS TIC VERIFICADA[3] (%):



Nota (s): [3] Os dados deste indicador reportam ao ano anterior ao de referência do inquérito.
Fonte(s): DGEEC - Inquérito à Utilização das TIC na Administração Pública Central, Regional e Câmaras Municipais.

| NOTA METODOLÓGICA

Os dados apresentados têm por base o Inquérito à Utilização de Tecnologias da Informação e da Comunicação na Administração Pública Central (IUTICAP) e o Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Câmaras Municipais (IUTICCM), realizados pela DGEEC - Direção-Geral de Estatísticas da Educação e Ciência.

O IUTICAP e o IUTICCM são instrumentos de notação do Sistema Estatístico Nacional (Lei n.º 22/2008 de 13 de maio) de resposta obrigatória, registados no Instituto Nacional de Estatística, IP. São realizados anualmente e os seus resultados possibilitam a construção de indicadores de caracterização e evolução, em matéria de Sociedade de Informação e Tecnologias da Informação e Comunicação, na Administração Pública.

Nos questionários IUTICAP e IUTICCM existem questões de resposta múltipla, pelo que os dados apresentados na maioria dos quadros refletem as várias opções selecionadas pelas entidades inquiridas.

	Designação da operação estatística	Âmbito	População-alvo	Universo inquirido	Taxa de resposta	Periodicidade	Método de inquirição	Período de referência dos dados	Recolha dos dados
1. Administração Pública Central	Inquérito à Utilização de Tecnologias da Informação e da Comunicação na Administração Pública Central (IUTICAP)	Inquérito censitário aos organismos da Administração Pública Central (em Portugal Continental).	Organismos da Administração Central (exceto fundos de segurança social), constituídos em pessoas coletivas, com exceção das empresas públicas sob controlo de uma unidade da Administração Central ou Regional, Universidades, Estabelecimentos de ensino, Estabelecimentos hospitalares e estruturas temporárias.	273	100%	Anual	Inquérito on-line.	Dados referentes ao momento da inquirição, exceto os relativos aos recursos financeiros, recursos humanos, comércio eletrónico, Big Data e problemas de segurança informática, que se reportam ao ano anterior ao de referência.	De setembro de 2022 a fevereiro de 2023

2. Administração Pública Regional	Inquérito à Utilização de Tecnologias da Informação e da Comunicação na Administração Pública Regional (IUTICAP)	Inquérito censitário aos Organismos da Administração Pública Regional (Governo Regional da Madeira e Governo Regional dos Açores).	Organismos da Administração Regional (exceto fundos de segurança social), constituídos em pessoas coletivas, com exceção das empresas públicas sob controlo de uma unidade da Administração Central ou Regional, Universidades, Estabelecimentos de ensino, Estabelecimentos hospitalares e estruturas temporárias.	R.A. Açores = 56 R.A. Madeira = 58	R.A. Açores = 100% R.A. Madeira = 100%	Anual	Inquérito on-line.	Dados referentes ao momento da inquirição, exceto os relativos aos recursos financeiros, recursos humanos, comércio eletrónico, Big Data e problemas de segurança informática, que se reportam ao ano anterior ao de referência.	De setembro de 2022 a janeiro de 2023
3. Câmaras Municipais	Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Câmaras Municipais (IUTICCM)	Inquérito censitário realizado anualmente junto das Câmaras Municipais do continente e regiões autónomas.	Câmaras Municipais (Continente, Açores e Madeira).	308	100%	Anual	Inquérito on-line.	Dados referentes ao momento da inquirição, exceto os relativos aos recursos financeiros, recursos humanos, comércio eletrónico, Big Data e problemas de segurança informática, que se reportam ao ano anterior ao de referência.	De setembro de 2022 a dezembro de 2022

| SIGLAS E SINAIS CONVENCIONAIS

- **AP** Administração Pública
- **TIC** Tecnologias de Informação e Comunicação
- **R.A.** Região Autónoma
- **-** Dado nulo
- **NUTS** Nomenclatura das Unidades Territoriais para Fins Estatísticos
- **RGPD** Regulamento Geral da Proteção de Dados
- **RJSC** Regime Jurídico da Segurança do Ciberespaço

| GLOSSÁRIO

BACKUP

Cópia de segurança ou sistema replicado que pode substituir um que se encontre em funcionamento.

CIBERSEGURANÇA

Conjunto de meios e tecnologias que visa proteger programas, computadores redes e dados de danos e intrusão ilícita, garantindo três aspetos importantes: integridade confidencialidade e disponibilidade.

CORREIO ELETRÓNICO

Sistema que permite o envio de mensagens por computadores inseridos em redes de comunicação ou por outro tipo de equipamento de comunicações. O correio eletrónico é uma versão informatizada dos serviços de correspondência interna ou dos serviços postais. As mensagens poderão incluir voz, gráficos, imagens e outras informações.

ENCRIPTAÇÃO

Utilização de uma cifra na conversão de uma mensagem original numa mensagem não inteligível (criptograma) que não permita a sua leitura por pessoas não autorizadas.

FILTRO ANTI-SPAM

Filtro de segurança que analisa o texto de uma mensagem eletrónica a fim de obter a probabilidade de ela ser ou não indesejável. Uma vez identificada, a mensagem pode ser, automaticamente, apagada ou movida para um local à parte.

FIREWALL

Equipamento usado em redes informáticas que protege uma rede interna do acesso externo de utilizadores não autorizados.

INTRUSÃO

Tentativa de contornar os controlos de segurança de um sistema de informação, por meios tais como espionagem, vírus, vermes, cavalos de troia, entre outros.

PALAVRA-PASSE DE UTILIZAÇÃO ÚNICA

Palavra-passe que apenas pode ser utilizada uma vez, evitando assim que alguém que a intersete a possa utilizar novamente com sucesso.

PALAVRA PASSE

Encadeamento de carateres introduzidos por um utilizador com a finalidade de verificar a sua identidade numa rede de trabalho ou num computador pessoal.

PHARMING

Crime informático que consiste na colocação de informação falsa num servidor de nomes de domínio (DNS server) e que implica o redireccionamento de um pedido feito pelo utilizador na Web para um destino diferente do pretendido, embora o seu programa de navegação continue a mostrar o sítio Web correto.

PHISHING

Crime informático que consiste na distribuição em massa de mensagens de correio eletrónico com ligações para falsos sítios Web de instituições bancárias ou outras, com pedidos de atualização de dados pessoais dos clientes.

RANSOMWARE

Software malicioso (malware) que infeta o sistema informático do utilizador e manipula o sistema infetado, de uma forma que a vítima não pode utilizá-lo (parcial ou totalmente), e os dados armazenados no mesmo. Geralmente, a vítima recebe uma nota de chantagem por pop-up, pouco tempo depois, pressionando-a a pagar um resgate (daí o nome) para voltar a ter acesso total ao sistema e aos ficheiros.

REDE VIRTUAL PRIVADA (VPN)

Rede usada por uma empresa ou grupo privado para efetuar ligações entre sítios, para comunicações de voz ou dados, como se fossem linhas dedicadas entre tais locais. O equipamento usado fica nas instalações do operador de telecomunicações públicas e faz parte integrante da rede pública, mas tem o software disposto em partições para permitir uma rede privada genuína.

Secure HTTP

Uma extensão do protocolo HTTP que permite o envio em segurança de dados pela World Wide Web.

SERVIDOR

Computador ou programa que providencia um determinado serviço a um outro programa, a que se chama cliente, que pode correr noutro computador.

Notas: um programa que serve páginas segundo o protocolo HTTP é um servidor Web e um programa que disponibiliza caixas de correio eletrónico para serem consultadas pelos utilizadores é um servidor de correio eletrónico. Uma máquina (hardware) pode correr vários servidores ao mesmo tempo, pois na prática cada serviço é gerido por um programa (servidor) separado.

SERVIDOR SEGURO

Servidor que permite aos utilizadores encriptar informação de modo a facilitar o comércio eletrónico (por exemplo os dados dos cartões de crédito).

SOFTWARE

Conjunto de meios não materiais (em oposição a hardware) que servem para o tratamento automático da informação e permitem o «diálogo» entre o homem e o computador.

SOFTWARE ANTIVÍRUS

Programa informático desenhado para detetar e dar resposta a programas mal-intencionados como os vírus informáticos. A resposta pode consistir no bloqueio do acesso aos ficheiros infetados, na remoção dos ficheiros ou sistemas infetados ou na informação ao utilizador da deteção de um programa infetado.

SPAM

Utilização abusiva da Internet para enviar mensagens irrelevantes ou inconvenientes a um ou mais grupos de discussão ou listas de distribuição, em violação deliberada ou acidental da etiqueta da Internet.

TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO (TIC)

Ramo da ciência da computação e da sua utilização prática que tenta classificar, conservar e disseminar a informação. É uma aplicação de sistemas de informação e de conhecimentos em especial aplicados nos negócios e na aprendizagem. São os aparelhos de hardware e de software que formam a estrutura eletrónica de apoio à lógica da informação.

VÍRUS

Um vírus causa muitas vezes danos ou distúrbios e pode ser ativado por um dado acontecimento, tal como a ocorrência de uma data predeterminada.

DGEEC | PUBLICAÇÕES

A SEGURANÇA DAS TIC (CIBERSEGURANÇA) NA ADMINISTRAÇÃO - IUTICAP e IUTICCM 2022

Av. 24 de Julho, n.º134
1399-054 Lisboa PORTUGAL
Tel.: (+351) 213 949 200