agefe

ASSOCIAÇÃO EMPRESARIAL DOS SETORES ELÉTRICO, ELETRODOMÉSTICO, ELETRÓNICO E DAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

RISCOS DE CIBERSEGURANÇA EM *ENDPOINT DEVICES*

Guia Prático para Dispositivos
de Computação, Impressão e Mobilidade

ÍNDICE

ENDPOINT DEVICES - Não sendo pacífica a tradução da expressão para português (dispositivos de utilização final vs. dispositivos terminais), opta-se pela utilização neste Guia do termo original, em inglês, que não suscita dúvidas. Naturalmente, quando é utilizado o termo dispositivo, referimo-nos a um *endpoint device*.

I. FUNDAMENTOS DA EDIÇÃO DESTE GUIA

I. Fundamentos da edição deste guia

A AGEFE - Associação Empresarial dos Setores Elétricos, Eletrodomésticos, Eletrónico e das Tecnologias da Informação e Comunicação é uma associação empresarial multissectorial que representa em Portugal as Indústrias de equipamento elétrico, eletrónico e eletrodoméstico, e que integra como sector autónomo, entre outros, o das empresas que operam no nosso País na área dos equipamentos e tecnologias da informação, impressão e comunicação (TIC).

Nessa qualidade, a AGEFE é membro de várias associações europeias, entre as quais a APPLiA, a associação europeia da indústria de eletrodomésticos, e a DIGITALEUROPE, a associação de referência da indústria das tecnologias digitais na Europa.

No quadro das suas atribuições estatutárias, e em estrita conformidade com as regras da concorrência, a AGEFE estuda os assuntos que interessem às suas associadas, nas áreas de atividade que representa, divulga e defende posições sobre os mesmos, e coopera com os poderes públicos nos processos preparatórios da regulamentação e das medidas de política pública com impacto naquelas áreas, tendo em vista pugnar pelo desenvolvimento sustentável dos sectores representados.

Consequentemente, ao congregar no seu seio um número muito significativo das empresas diretamente envolvidas nas questões relacionadas com a segurança no ciberespaço (**cibersegurança**), em especial daquelas que atuam em Portugal no sector das TIC, a AGEFE entende que no âmbito da sua atividade lhe compete analisar este tema, com estrito respeito pelas regras da concorrência, as quais aliás incorpora no seu Código de Conduta nesta matéria.

A AGEFE entende ter também a responsabilidade social de transmitir ao poder político e às autoridades administrativas as posições comuns das suas associadas, cujo conhecimento das questões relativas à segurança dos equipamentos e serviços que disponibilizam no mercado é, naturalmente, muito profundo.

A AGEFE assume-se como um *stakeholder* empenhado na implementação do **Quadro Nacional de Referência para a Cibersegurança (QNRCS)** e na articulação deste com o Plano de **Ação para a Transição Digital**.

Importa mencionar que este Guia é o resultado de um Grupo de Trabalho criado pelo Conselho Setorial para este efeito, e a cujos membros a AGEFE agradece reconhecidamente.

A AGEFE esclarece também que a adoção deste documento foi precedida da divulgação prévia, para apreciação do seu conteúdo, a todas as empresas suas associadas do sector de Eletrónica e TIC em 2020, cuja relação consta em anexo.

II. INTRODUÇÃO

II. Introdução

A **cibersegurança** é um dos temas essenciais ao desenvolvimento do Mundo Digital, pois só ela pode proporcionar aos cidadãos, à economia e aos governos, a **CONFIANÇA** indispensável à digitalização de processos e procedimentos que até há bem pouco eram realizados em meio analógico.

Neste pressuposto, importa sublinhar, como adiante se demonstra, que é necessário e urgente que, sem descurar as infraestruturas críticas, seja dada maior atenção aos *endpoint devices*, que são a porta de entrada para a grande maioria dos ciberataques[2], e a origem de mais de um quarto das quebras de segurança[3].

Consequentemente, neste Guia sistematiza-se, numa perspetiva operacional, o que de essencial existe de forma avulsa e muito dispersa sobre a **cibersegurança** dos *endpoint devices*, procurando-se desta forma contribuir para a prossecução dos objetivos estratégicos do País neste domínio, consubstanciados no QNRCS e no Plano de Ação para a Transição Digital.

a. *Endpoint devices*

Endpoint devices, tecnicamente "nós de extremidade", são dispositivos conectados a uma Rede de Área Local ou a uma Rede de Longa Distância, que permitem estabelecer comunicações através dessa mesma rede. Este Guia aborda os *endpoint devices* que são terminais de dados, nas categorias de impressão, mobilidade e computação.

CATEGORIA	DISPOSITIVOS
Computação	• Computadores de Secretária • Computadores Portáteis • Estações de Trabalho (*workstations*) • Terminais
Impressão	• Dispositivos de impressão • Dispositivos multifuncionais (cópia, impressão, digitalização e *fax*)
Mobilidade	• *Smartphones* • *Tablets* • Híbridos (dispositivos que não são nem um computador portátil nem um *tablet*) • *Chromebooks* • Relógios inteligentes (*smartwatches*)

[2] - No estudo da Forrester *The State of Data Security and Privacy: 2018 to 2019*, realizado por Heidi Shey e Enza Iannopollo é apontado que os endpoint devices estão na origem de 70% dos ciberataques.
[3] - SANS - *Endpoint Security Survey* aponta que estes dispositivos estão na origem de 28% das quebras de segurança verificadas em 2018.l

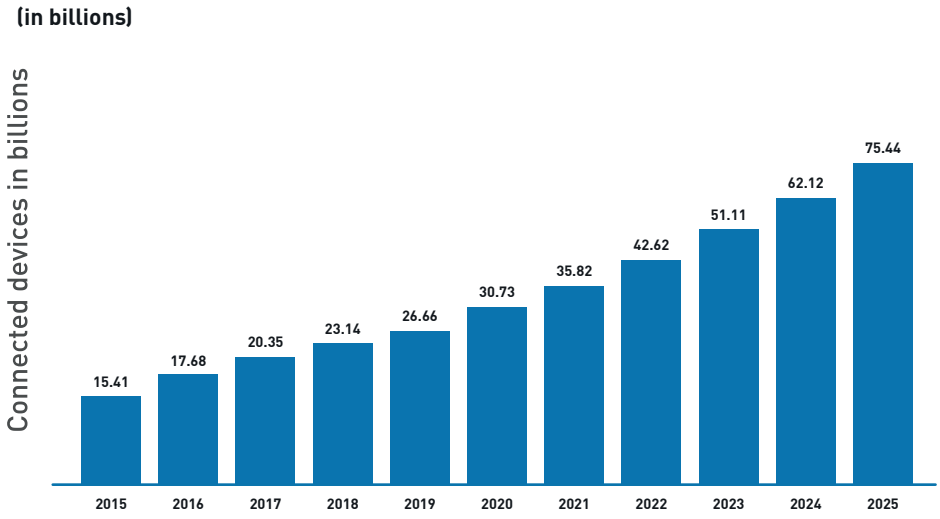
Todos estes dispositivos, por armazenarem dados das organizações, são na maioria dos casos o primeiro ponto de entrada nas redes corporativas. A pesquisa independente recente *The Third Annual Ponemon Institute Study on the State of Endpoint Security*[4], conclui que a frequência dos ataques através de *endpoint devices* está a aumentar (com 68% dos inquiridos a responderem ter sofrido mais ciberataques no último ano).

É, assim, fundamental que os decisores públicos em Portugal reconheçam a crescente importância da proteção dos dispositivos *endpoint*, que a indústria já disponibiliza, concretizando esta necessidade e incorporando-a nos critérios de valorização e de exigência, nos procedimentos de adjudicação e avaliação legalmente estabelecidos.

b. Situação e riscos globais de cibersegurança

O Fórum Económico Mundial no seu recente relatório *The Global Risk Report 2020* refere que, atualmente, mais de 50% da população mundial tem acesso à internet, que se regista um aumento diário de conexões avaliado em cerca de um milhão de novas pessoas, e que dois terços dos habitantes do planeta dispõem de um dispositivo móvel.

Como se evidencia no gráfico em baixo, o número de *endpoint devices* conectados, que em 2015 era pouco superior a 15 mil milhões, deverá crescer para mais de 75 mil milhões em 2025!



Evolução de dispositivos conectados (Internet of Things (IoT) entre 2015 e 2025 — Statista

[4] - https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf

Este aumento exponencial, ano após ano, do número de *endpoint devices* conectados, que levará a um incremento superior a 500% deste número em apenas uma década, resulta essencialmente do seguinte:

- Crescimento significativo do número de *smartphones* (vendas mundiais em 2020 de 1.5 mil milhões de unidades - Statista), *tablets, smartwatches* ou computadores vendidos globalmente;

- Crescente penetração destes dispositivos em mercados emergentes e bastante povoados como a China, a Índia ou o Paquistão;

- Aparecimento de um conjunto de novos dispositivos conectados à internet, como as *Smart Home Appliances* (frigoríficos, máquinas de lavar roupa, aspiradores ou *Smart TVs*);

- Desenvolvimento e conexão de uma enorme multiplicidade de sensores e câmaras utilizados por entidades governamentais, empresas e particulares, para os mais diversos fins.

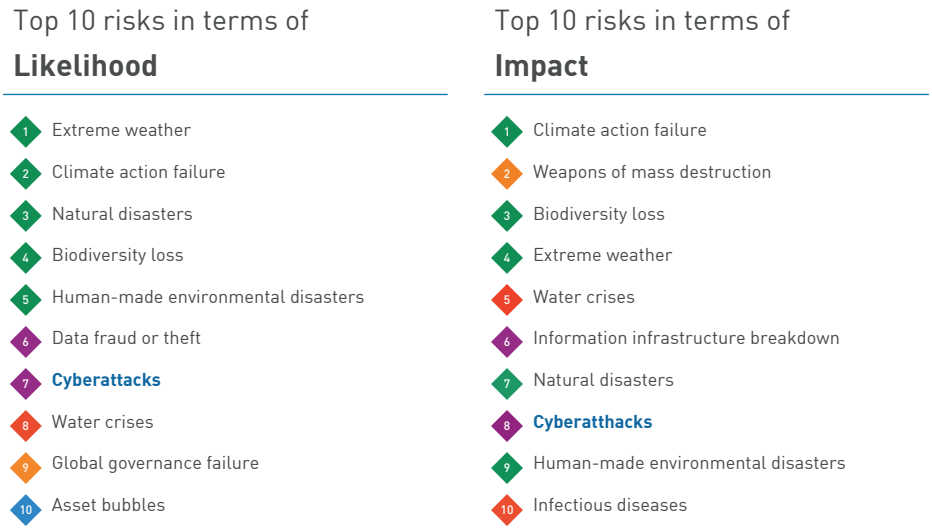
Este crescimento exponencial dos *endpoint devices* vai ser ainda mais acelerado com a implementação da nova geração de redes de comunicação móveis (5G)[5], que se irá tornar o elemento catalisador de outras tecnologias, como a *Cloud Computing*[6], a Inteligência Artificial[7], a Condução Autónoma (veículos autónomos e conectados) e a IoT[8], que serão a base tecnológica das cidades inteligentes, e de muita da atividade humana no futuro.

Torna-se, pois, óbvia a razão pela qual a segurança do ciberespaço é certamente **um dos maiores desafios que se colocam à segurança dos cidadãos, das organizações, e mormente, dos próprios Estados.**

Tal como é óbvia a importância que deve ser dada à **cibersegurança dos *endpoint devices***, os quais, como se referiu atrás, estão na origem da grande maioria dos ciberataques, e de mais de um quarto das quebras de segurança.

Num inquérito muito recente do Fórum Económico Mundial a diversos líderes mundiais, cujos resultados constam do seu relatório atrás mencionado, os ciberataques figuram no TOP 10 das maiores ameaças que a humanidade enfrenta, quer quanto à sua probabilidade de ocorrência, quer quanto ao seu impacto.

[5] - A introdução comercial em Portugal da 5G está prevista para o próximo ano.
[6] - *Cloud data Processing and Storage*
[7] - *Predictive Models and Machine Learning*
[8] - "Internet das Coisas": dispositivos inteligentes e conectados



Top 10 Risks by Likelihood | Global Risks Report — World Economic Forum

Os líderes mundiais entrevistados apontam que a conjugação dos riscos decorrentes da falta de segurança do ciberespaço, com a ausência de um quadro regulatório à escala global destas tecnologias e de uma normalização que permita a sua certificação à mesma escala, põe em causa a possibilidade de se poder aproveitar na plenitude todo o potencial das tecnologias de nova geração.

c. Aspectos da cibersegurança na UE

A União Europeia tem vindo a manifestar preocupação com o impacto económico, político e social das condições de segurança no ciberespaço, e dos correspondentes riscos, que rapidamente poderão atingir uma escala inaceitável.

Nesse sentido, foi adotado em 2019 o **Regulamento de Cibersegurança da UE**, que veio renovar e fortalecer o mandato da **Agência da União Europeia para a Cibersegurança (ENISA)**, e sobretudo estabelecer, a partir dela, uma estrutura de certificação da UE para produtos, serviços e processos digitais das TIC.

Apesar de já existirem na UE vários esquemas de certificação de segurança para produtos das TIC, o desenvolvimento de uma **estrutura comum de certificação** em **cibersegurança** para toda a Europa é essencial para reforçar o mercado único europeu.

Na verdade, só ela pode minimizar o risco de fragmentação do ciberespaço, com o aparecimento de normas e certificações diferentes, competitivas entre si. Pelo menos, no próprio espaço europeu.

Através da APPLiA e da DIGITALEUROPE, que integram o **SCCG** - *Stakeholder Cybersecurity Certification Group da ENISA*, a AGEFE tem vindo a acompanhar de perto os desenvolvimentos dos trabalhos relativos à criação daquela estrutura comum de certificação o último dos quais foi a abertura em 2 de julho da consulta pública sobre a primeira proposta para o novo **Regime Europeu de Certificação de Cibersegurança** (*Common Criteria based European candidate cybersecurity certification scheme*).

Uma nota final quanto à política da União Europeia em matéria de **cibersegurança** para destacar que esta faz parte dos **objetivos do plano de recuperação apresentado pela Comissão Europeia para relançar as economias dos Estados membros**, e ultrapassar a crise provocada pela pandemia.

III. CIBERSEGURANÇA EM PORTUGAL

III. Cibersegurança em Portugal

a. Quadro regulamentar

Em Portugal, na sequência da transposição da Diretiva da Segurança das Redes e dos Sistemas de Informação[9], pela Lei n.º 46/2018, foi publicada a Estratégia Nacional de Segurança do Ciberespaço 2019-2023[10], que define o enquadramento, os objetivos e as linhas de ação do Estado em matéria de segurança do ciberespaço.

Em meados de 2019, o **Centro Nacional de Cibersegurança** (CNCS) publicou o QNRCS, tendo por objetivo proporcionar *"às organizações um guia de cibersegurança que sistematiza um conjunto de medidas para as problemáticas mais relevantes da atualidade"*, disponibilizando as bases para que se possam cumprir *"os requisitos mínimos de segurança da informação recomendados."*

Ora, apesar de indicar claramente os processos e procedimentos de **cibersegurança**, pela sua natureza, o QNRCS faz uma abordagem genérica da questão dos requisitos de **cibersegurança** do *hardware* — o que levanta dificuldades do ponto de vista operacional a quem, não sendo especialista, pretende tomar decisões informadas para o implementar.

Com este Guia, dirigido a todos os decisores, públicos ou privados, não especialistas em matéria de **cibersegurança**, a AGEFE procura colmatar a ausência de informação prática sobre as especificações técnicas dos *endpoint devices* nesse domínio, através do arrolamento dos respetivos normativos, complementan do assim o próprio QNRCS.

b. Situação e riscos nacionais

Se o panorama internacional relativamente à **cibersegurança** é extremamente desafiante para as organizações, o ciberespaço português não é excepção, tal como se constata pelas infografias do Relatório Cibersegurança em Portugal: Riscos & Conflitos, de Junho de 2020, do **Observatório de Cibersegurança** do CNCS a seguir reproduzidas:

[9] - Directiva (EU) 2016/1148, transposta pela Lei n.º 46/2018
[10] - RCM n.º 92/2019

Empresas e indivíduos em Portugal reconhecem menos do que na UE sofrer incidentes de cibersegurança, em 2019 (Eurostat).

8% DAS EMPRESAS PORTUGUESAS (13% NA UE)

27% DOS INDIVÍDUOS PORTUGUESES (37% NA UE)

Durante 2019, as Infraestruturas Digitais (ID), os Prestadores de Serviços de Internet (PSI), a Educação, Ciência, Tecnologia e Ensino Superior (ECTES) e a Banca são os setores e áreas governativas mais afetados por incidentes e com mais observáveis identificados (CERT.PT).

19% DOS INCIDENTES EM ID

18% DOS INCIDENTES EM PSI

9% DOS INCIDENTES EM ECTES

8% DOS INCIDENTES NA BANCA

Entre 2018 e 2019 houve um aumento no número de incidentes registados e no número de vulnerabilidades identificadas pelo CERT.PT (CERT.PT).

+26% DE INCIDENTES

+139% DE VULNERABILIDADE

Atores e Incidentes | Relatório Cibersegurança em Portugal — Observatório de Cibersegurança

Assinala-se que o Relatório Sociedade 2019 do mesmo Observatório refere que Portugal possui indicadores preocupantes no que diz respeito à sensibilidade da população sobre as melhores práticas a adotar, quando comparados com a média europeia, designadamente **em relação ao uso de** *passwords*:

POUCA MUDANÇA DE COMPORTAMENTO EM RELAÇÃO AO USO DE PASSWORDS, APESAR DAS PREOCUPAÇÕES

13% EM PT
29% NA UE

utilizam diferentes passwords para diferentes websites*

12% EM PT
27% NA UE

utilizam passwords mais complexas que no passado*

16% EM PT
21 % NA UE

alteram a password regularmente*

* Em 2018

Comportamentos | Relatório Sociedade 2019 — Observatório de Cibersegurança

c. Impacto do surto pandémico na cibersegurança

Não é pois de estranhar ler na Nota Informativa Covid-19: Cibercrime em tempo de pandemia, do Gabinete Cibercrime da Procuradoria-Geral da República, que as denúncias de cibercrime têm aumentado no decurso dos anos, desde 2016, sem excepções. Tal como se compreende que a mesma Nota Informativa destaque que tais denúncias registaram entre 1 de janeiro e 31 de maio de 2020 um **aumento de 38% face às recebidas em todo o ano de 2019**.

O surto pandémico gerado pela SARS-CoV-2 teve, e continua a ter, um impacto profundo na vida das pessoas, famílias e comunidades, tal como nas organizações, nas quais, com a adoção massiva do teletrabalho, aumentou significativamente o risco de ameaças cibernéticas. Segundo o último Boletim (n.º 3/2020) do Observatório de Cibersegurança do CNCS, neste ano, o número de incidentes registados pelo CERT.PT[11] aumentou 34% no 2º trimestre face ao 1.º, e 124% em relação ao período homólogo do ano anterior.

O enorme incremento dos riscos imediatos para a **cibersegurança** das organizações, públicas e privadas, no contexto da crise pandémica, encontra explicação sobretudo no seguinte:

1. A manutenção dos processos críticos de negócio através do teletrabalho é em geral priorizada em detrimento das políticas de segurança dos sistemas ou ferramentas, assegurando-se apenas que o colaborador se mantém operacional;
2. O número de colaboradores em teletrabalho cresceu exponencialmente e, consequentemente, também o número de dispositivos com acesso a informação crítica;
3. A pressão gerada sobre as equipas de IT, para assegurarem a operacionalidade de colaboradores remotos aumentou. Neste contexto, verificaram-se mudanças significativas nas infraestruturas de IT, o que levou a que o espaço para ciberataques aumentasse proporcionalmente.
4. A própria cadeia de valor das organizações é impactada, na medida em que os seus prestadores de serviços de segurança *(outsourced operations centers, firewall management teams,* entre outros) viram também a sua capacidade operacional afetada, originando dificuldades acrescidas à capacidade de reação a ataques.
5. As organizações e os seus colaboradores não estavam preparados para mudarem as suas operações de forma tão drástica. Com a mudança do físico para o virtual, o grau de dependência nas tecnologias de acesso remoto cresceu significativamente, crescendo em paralelo também a criticidade e o impacto de ciberataques ou interrupções de IT para as organizações. Adicionalmente, foi solicitada aos colaboradores a utilização de tecnologias, *endpoint devices* e aplicações com os quais aqueles não estavam familiarizados, o que incrementa o risco / exposição a ciberataques.

[11] - Serviço do CNCS que coordena a resposta a incidentes envolvendo entidades do Estado, operadores de serviços essenciais, operadores de infra-estruturas críticas nacionais e prestadores de serviços digitais.

d. A cibersegurança e a administração pública

A preocupação do Estado com a **cibersegurança** tem vindo a ser evidenciada na produção legislativa e no trabalho desenvolvido pelo Gabinete Nacional de Segurança, através das atividades do **Centro Nacional de Cibersegurança**, e mais recentemente com o Plano de Ação para a Transição Digital, do qual a Digitalização do Estado é um dos três pilares.

Ora, segundo o relatório do IDC *IT Endpoint Security Survey 2019*, 49,4% das organizações inquiridas (privadas e governamentais) consideram a segurança do *endpoint* como secundária, não sendo abordada de forma estratégica e holística.

Por outro lado, a Verizon no seu relatório de 2019 *Data Breach Investigations Report* aponta que em 2018 cerca de 16,4% das quebras de seguranças provocadas por ciberataques ocorreram na Administração Pública.

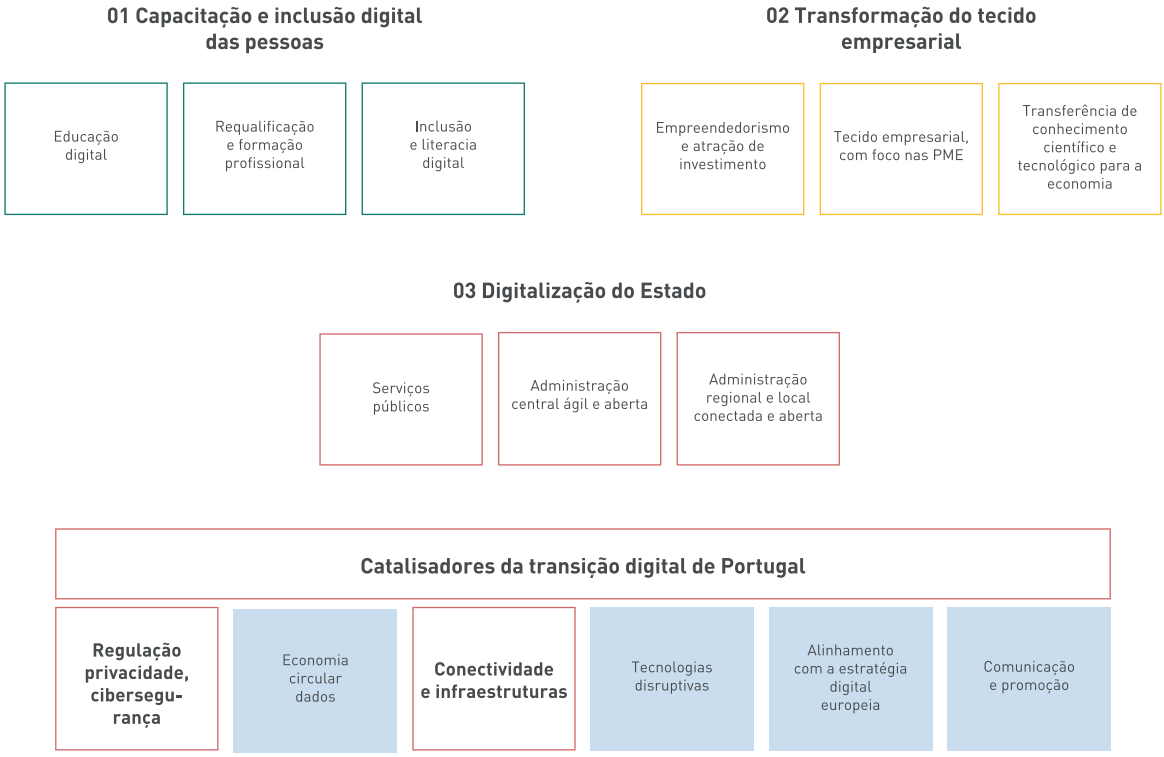
Em Portugal, no mesmo ano, o IUTIC - Inquérito à Utilização das Tecnologias da Informação, da Comunicação, da Direcção-Geral de Estatísticas da Educação e Ciência, chega praticamente à mesma percentagem (16%).

É de salientar que, computando os dados do estudo da Verizon supracitado, verificamos que **a taxa de conversão de ciberataques em quebras de segurança na Administração Pública é superior à do sector de *Media & Entertainment.***

IV. O PLANO DE AÇÃO PARA A TRANSIÇÃO DIGITAL E A CIBERSEGURANÇA

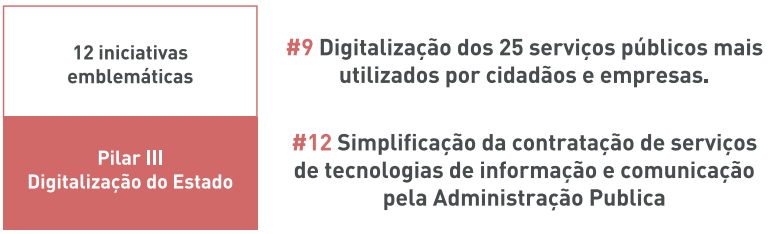
IV. O Plano de Ação para a Transição Digital e a Cibersegurança

Neste quadro de enormes desafios tecnológicos foi publicada, a 21 de Abril de 2020, a Resolução do Conselho de Ministros n.º 30/2020, que aprovou o Plano de Ação para a Transição Digital, o qual reflete a estratégia definida para esta transição e condensa a visão do Governo neste domínio, materializada numa estrutura que contempla três pilares principais de atuação, e seis catalisadores transversais àqueles, que no seu conjunto constituem os instrumentos de aceleração da transição digital em Portugal.



Apresentação do Plano de Ação para a Transição Digital | Ministério da Economia e Transição Digital

A própria Resolução do Conselho de Ministros n.º 30/2020, que aprovou este Plano de Ação, integra um conjunto de 57 iniciativas, das quais, pelo seu grau de criticidade, são também desde logo aprovadas **12, consideradas prioritárias e emblemáticas.**



A simplificação dos processos de contratação pública inerentes à prestação de serviços e aquisição de bens no âmbito das TIC, pela Administração Pública, é efetivamente uma medida que dá resposta a uma necessidade premente, e desde há muito identificada: um *"procedimento de contratação mais ajustado à natureza dos bens e serviços a adquirir"*.

Esta medida é de extrema importância, tanto mais quanto, conforme é apontado neste Plano de Ação, é propósito que a mesma simplificação, *"para além de garantir a celeridade e continuidade exigidas por estes,* ***garanta o cumprimento atempado dos objetivos nacionais em matéria de transição digital*** *(destacado nosso)."*

Com efeito, não seria coerente que, no quadro da mencionada simplificação do procedimento de contratação na área das TIC, a **cibersegurança**, enquanto catalisador transversal do Plano de Ação para a Transição Digital, não viesse a ser sempre considerada e valorizada, como requisito de base — em maior ou menor grau face ao tipo de dispositivo e de utilização que lhe vai ser dada, mas sempre um requisito.

Na verdade, tendo presente o objetivo geral de reforçar a digitalização dos serviços públicos, concretamente dos 25 mais utilizados por cidadãos e empresas, a que se refere a medida #9, se não for acautelada a **cibersegurança** dos dispositivos em que assenta, o risco de ciberataques que se venham a traduzir em quebras de segurança em áreas críticas aumentará significativamente.

Por outro lado, há que ter em atenção que a segurança se inicia no próprio utilizador do *endpoint device*, que deve estar sensibilizado para o risco que corre e ter formação adequada neste domínio, incluindo o conhecimento das funcionalidades de proteção incorporadas nativamente no dispositivo.

Salienta-se também que outro dos catalisadores transversais do Plano de Ação, a "Conectividade e infraestrutura", ao possibilitar uma ampla conexão, através do incremento da disponibilização de redes *Wi-Fi*, obriga a garantir a segurança em múltiplas e distintas redes, muitas delas públicas.

Deste modo, o alargamento da conexão reforça consideravelmente a importância da proteção dos *endpoint devices*, na medida em que são a forma primária de acesso às redes por parte do utilizador, e de um modo geral são **tendencialmente o elo mais fraco, não pela ausência de tecnologia de proteção, mas sim pela pouca sensibilização e exigência neste domínio.**

O sucesso do Plano de Ação para a Transição Digital, que se deseja, não está pois relacionado apenas com a capacidade de execução por parte dos agentes e entidades nele envolvidos. É indispensável que estes tenham **CONFIANÇA** nos meios que lhes são disponibilizados para o implementarem — o que só medidas de **cibersegurança**, a começar nos próprios dispositivos que utilizam, lhes poderão assegurar.

a. O QNRCS e os *endpoint devices*

A segurança do ecossistema de informação depende de todos os seus componentes tecnológicos, processos/procedimentos e do factor humano. E neste contexto a segurança dos *endpoint devices* é particularmente relevante, uma vez que são estes dispositivos que fazem o interface "homem-máquina".

No **Quadro Nacional de Referência para a Cibersegurança** os *endpoint devices* (computadores, *tablets*, impressoras, multifuncionais, *smartphones*, etc.) são abordados como ativos tecnológicos de um sistema de informação, e como tal deverão ser incluídos na estratégia das organizações para reduzir/gerir o risco e mitigar o impacto de qualquer incidente associado às ciberameaças.

O QNRCS propõe um conjunto de boas práticas/medidas de segurança, concretizadas em exemplos de implementações tecnológicas, processuais ou outras. Estão agrupadas em cinco objetivos de segurança; Identificar, Proteger, Detetar, Responder e Recuperar, com uma ou mais categorias e subcategorias.

São identificadas 102 medidas de segurança que abrangem todo o ecossistema de um sistema de informação, do conjunto das quais identificámos as mais relevantes no domínio dos *endpoint devices*.

As medidas deste Quadro relacionadas com os *endpoint devices* são elencadas a seguir, tendo presente que o propósito deste Guia é habilitar todos os envolvidos na implementação daquele Quadro de Referência com um conjunto de informações específicas que facilitam e complementam a sua concretização.

Não obstante este propósito, a informação que é dada numa perspectiva utilitária neste Guia deve ser complementada com outras boas práticas/medidas de segurança sempre que existam integrações com outros sistemas.

OBJETIVO	CATEGORIA	SUBCATEGORIA	DENOMINAÇÃO
IDENTIFICAR	ID.GA - Gestão de ativos	ID.GA-1	Os dispositivos físicos, redes e sistemas de informação existentes na organização devem ser inventariados
		ID.GA-5	Os ativos necessários para a prestação de bens e serviços devem ser classificados
	ID.AO - Ambiente da organização	ID.AO-4	Os ativos críticos devem ser identificados e registados
	ID.GV - Governação	ID.GV-2	Os requisitos legais e regulamentares para a cibersegurança devem ser cumpridos
	ID.AR - Avaliação do risco	ID.AR-1	As vulnerabilidades dos ativos devem ser identificadas e documentadas
	ID.GL - Gestão de risco da cadeia lógica	ID.GL-3	Os contratos com fornecedores devem respeitar o plano de gestão do risco para a cadeia logística
		ID.GL-4	Os fornecedores devem ser periodicamente avaliados
PROTEGER	PR.GA - Gestão de identidade, autenticação e controlo de acessos	PR.GA-1	O Ciclo de vida de gestão de identidades deve ser definido
		PR.GA-2	Devem existir controlos de acesso físico às redes e sistemas de informação
		PR.GA-5	A organização deve proteger a integridade das redes de comunicações
		PR.GA-6	A organização deve verificar a identidade dos colaboradores e vinculá-los às respetivas credenciais
		PR.GA-7	Devem ser definidos mecanismos de autenticação de utilizadores, dispositivos e outros ativos de sistemas de informação
	PR.SD - Segurança de dados	PR.SD-1	A organização deve proteger os dados armazenados
		PR.SD-2	A organização deve proteger os dados de circulação
		PR.SD-3	A organização deve gerir formalmente os ativos durante os procedimentos de remoção, transferência e aprovisionamento dos mesmos
		PR.SD-4	A organização deve providenciar a capacidade adequada para garantir a disponibilidade das rede e dos sistemas de informação
		PR.SD-6	A organização deve utilizar mecanismos de verificação para confirmar a integridade de software, firmware e dados
		PR.SD-7	A organização deve utilizar mecanismos de verificação para confirmar a integridade de software, firmware e dados
		PR.SD-8	A organização deve implementar mecanismos de validação e verificação de integridade do hardware
	PR.PI - Procedimento e processos de proteção da informação	PR.PI-1	Deve ser criada e mantida uma configuração base de redes e sistemas de informação que incorpore os princípios de segurança
		PR.PI-6	Os dados devem ser destruídos de acordo com a política definida
	PR.TP -Tecnologia de proteção	PR.TP-1	Os registos de auditoria e de histórico devem ser documentados, implementados e revistos de acordo com as políticas
		PR.TP-2	Os suportes de dados amovíveis devem ser protegidos e a sua utilização deve ser restrita, de acordo com a política definida
		PR.TP-4	As redes de comunicações e de controlo devem ser protegidas
DETETAR	DE.AE - Anomalias e eventos	DE.EA-3	Os eventos devem ser coletados e correlacionados a partir de várias fontes e sensores
	DE.MC - Monitorização Contínua de Segurança	DE.MC-5	A utilização de aplicações não autorizadas em dispositivos móveis deve ser detetada
		DE.MC-7	Deve ser efetuada a monitorização de acessos não autorizados de colaboradores, conexões, dispositivos e software

Tabela construída a partir do Anexo 1 do QNRCS

b. Quadros práticos – computação, impressão e mobilidade

Este Guia procura proporcionar a todos quantos têm responsabilidades de acautelar a **cibersegurança** na aquisição de *endpoint devices* para utilização nas respetivas organizações, em especial na Administração Pública, um conjunto detalhado de elementos de natureza prática que os habilite a tomar uma decisão informada nesta matéria.

A informação apresentada não é exaustiva quanto a todos os aspectos normativos da segurança dos *endpoint devices*, nem pretende apresentar o estado da arte neste domínio.

Trata-se tão só de uma ferramenta prática de referenciação dos aspetos essenciais da **cibersegurança** destes dispositivos, que remete sempre que possível para normas internacionais, ou reconhecidas internacionalmente, por forma a garantir a sua neutralidade tecnológica e, em conformidade com o Código de Conduta da AGEFE, também a sua neutralidade concorrencial.

Assim, partindo das conclusões do estudo do *IDC Government Procurement Device Security Index 2018: Public Sector PC & Printer RfPs Lack Basic Security Consideration,* e tendo em conta o disposto nas normas internacionais, como as da *International Organization for Standardization* (ISO) ou do *National Institute of Standards and Technology* (NIST), o ***Grupo de trabalho*** "**Cibersegurança" da AGEFE** definiu como prioritárias três das categorias mais relevantes destes dispositivos — computação, impressão e mobilidade (computadores, impressoras e *smartphones*) — enquadrando-os nas seguintes tipologias de requisitos do QNRCS:

- PR.GA-7: definição de mecanismos de autenticação de utilizadores, dispositivos e outros ativos de sistemas de informação;
- PR.PI-6: os dados devem ser destruídos de acordo com a política definida;
- PR.SD-6: a organização deve utilizar mecanismos de verificação para confirmar a integridade de *software, firmware e dados*;
- DE.MC-4: a atividade dos colaboradores deve ser monitorizada para se detetarem potenciais incidentes.

A partir de quatro eixos estratégicos (Autenticação, Eliminação segura de dados, Integridade e Deteção e proteção) a estrutura dos quadros práticos que em seguida se apresentam baseia-se na identificação de objetivos, em como dar resposta aos mesmos através de soluções tecnológicas e comprovar a eficácia da solução, apresentando normas e/ou certificações de referência para cada um deles.

Assim, os quadros pretendem constituir-se como uma ferramenta de análise e de desenvolvimento, adaptável à realidade, às preocupações e às necessidades de cada instituição, no momento de preparação de procedimentos pré-contratuais relativos a *endpoint devices*.

Nota introdutória ao quadro de computação

Os dispositivos de computação, pelo seu uso generalizado, são um dos elementos de risco em termos de cibersegurança. O perfil de utilização destes dispositivos, numa adaptação constante à transformação dos modelos de trabalho, obriga a uma particular atenção e salvaguarda em termos de cibersegurança.

O incremento da mobilidade e também o novo perfil dos dispositivos de computação fixos, com as necessidades de verificação de identidade do utilizador, de proteção dos dados, de resiliência perante ataques e capacidade de autorrecuperação com vista a não comprometer a sua disponibilidade para o utilizador, são elementos fundamentais para a eficiência das organizações.

O elemento de acesso do utilizador aos sistemas de informação corporativos é, cada vez mais e por evolução dos perfis de utilização, o mesmo elemento de acesso aos conteúdos pessoais, onde quer que o utilizador utilize o dispositivo de computação e se conecte remotamente. Assim, é fundamental a proteção do dispositivo, na medida em que a sua utilização tende a ser mais flexível e multifacetada, comportando maiores riscos.

	COMPUTAÇÃO			
REQUISITOS	**OBJETIVO / FINALIDADE (CONCEITO)**	**COMO? (TECNOLOGIA / SOLUÇÃO)**	**FORMAS DE COMPROVAR**	**OBSERVAÇÕES E REFERÊNCIAS**
AUTENTICAÇÃO	Verificação eficiente da identidade em autenticação física	Leitor de cartões de identificação, que podem incluir gravação em relevo e / ou tarja magnética e / ou marca de identificação táctil	Leitor de cartões chip, banda magnética, RFID, NFC. Leitor de impressão digital. Reconhecimento facial IR.	ISO7816 Class A, B, and C (5V/3V/1.8V)
	Verificação eficiente da identidade em autenticação on-line	Segurança da identidade digital como representação exclusiva de um sujeito envolvido numa acção online, por gestão, modificação e reposição de palavra-passe.	Autenticação multi-fator. Chips criptográficos no dispositivo.	NIST 800-63B
	Verificação eficiente da identidade reivindicada de indivíduos que procuram acesso lógico a sistemas de informações governamentais	Garantia de segurança, com verificação da identidade através de sistemas criptográficos e smartcards	Leitores de smartcard e contactless incorporados no dispositivo suportando algoritmos encriptados.	FIPS 201, PC/SC 2.0
ELIMINAÇÃO SEGURA DE DADOS	Potencial inviabilização de recuperação de dados eliminados	Processo de eliminação segura de dados em suportes Solid State Drive	Funcionalidade, activada a partir da BIOS do dispositivo que tenda a assegurar a impossibilidade de recuperação/reconstrução dos dados num dispositivo de armazenamento, através de Block Erase ou de Crypto Erase.	NIST SP 800-88r1
INTEGRIDADE (SOFTWARE, FIRMWARE E DADOS)	Proteção do sistema de arranque do dispositivo	Mecanismo para impedir a modificação não autorizada do firmware da BIOS (Basic Input / Output System)	Funcionalidade embebida no dispositivo que assegure, no seu arranque, a detecção e alerta de alterações da BIOS.	ISO/IEC 19678:2015
	Identificação e recuperação de ataques ao sistema de arranque do dispositivo	Mecanismo para detetar a modificação não autorizada do firmware do BIOS (Basic Input / Output System) e recuperar para uma versão funcional.	Funcionalidade embebida no dispositivo que assegure, no seu arranque, a deteção e alerta de alterações da BIOS e a sua recuperação automática permitindo o normal e seguro funcionamento do dispositivo.	NIST SP 800-147
	Proteção de dados armazenados, através de sistemas criptográficos	Unidades de criptografia automática e Programas de Validação de Módulo Criptográfico.	Discos encriptados e chips de segurança para armazenamento criptográfico de elementos de segurança.	TCG Opal 2, FIPS 140-2 (encriptação de dados)
DETEÇÃO E PROTEÇÃO	Salvaguarda dos componentes necessários para inicializar o sistema	Plataforma de proteção, deteção e recuperação dos componentes (BIOS e Firmware) e fornecer serviços implementados pelos componentes de hardware	Funcionalidade embebida no dispositivo que assegure, no seu arranque, a deteção de alterações da BIOS e no Firmware recuperando automaticamente todos os componentes e agentes necessários ao funcionamento seguro do dispositivo.	NIST SP 800-193

Nota introdutória ao quadro de impressão

Relativamente aos dispositivos de impressão, é muito importante considerar que a cibersegurança (possível intromissão ou ataque a uma infraestrutura informática, tendo como ponto de entrada um dispositivo de impressão ligado à mesma), é apenas um dos aspetos da segurança a ter em conta.

Considerando a segurança a 360º, as maiores vulnerabilidades de acesso à informação produzida por este tipo de dispositivos estão relacionadas com documentos e utilizadores. Um documento "esquecido" com informação crítica ou confidencial (informação de produtos em fase de desenvolvimento, custos internos, salários, entre outros) bem como a utilização maliciosa por pessoas das organizações para envio ou extração de informação, representam a quase totalidade destes problemas de segurança, de acordo com alguns estudos produzidos por entidades internacionais especializadas nesta matéria.

Atualmente, e no que à cibersegurança diz respeito, procura-se manter o controlo através de medidas que os fabricantes do equipamento têm tomado para impedir diversos tipos de ataques. As capacidades tecnológicas de quem pretende pôr em prática atividades maliciosas são cada vez mais sofisticadas, e como tal, os fabricantes continuam a antecipar tais riscos com soluções preventivas, como são as diferentes soluções tecnológicas referenciadas no quadro seguinte.

	IMPRESSÃO			
REQUISITOS	**OBJETIVO / FINALIDADE (CONCEITO)**	**COMO? (TECNOLOGIA / SOLUÇÃO)**	**FORMAS DE COMPROVAR**	**OBSERVAÇÕES E REFERÊNCIAS**
AUTENTICAÇÃO	Identificação inequívoca de um determinado indivíduo/utilizador ou dispositivo para acesso a um ou vários sistemas	Interoperabilidade com sistemas de gestão de ciclo de vida de entidades/utilizadores	Assegurar a integração com sistemas de gestão de utilizadores	LDAP
		Implementação de RBAC (Role Based Access Control)	Disponibilizar acesso a função, configurações e documentos do equipamento de acordo com perfil do utilizador	
		Autenticação por múltiplos dispositivos/tecnologias	Assegurar a integração com leitor de cartão de identificação, username e password de domínio, NFC, etc.	ISO14443A/B ISO15693 ISO18092
ELIMINAÇÃO SEGURA DE DADOS	Eliminação de dados sensiveis contidos nos suportes de armazenamento ou outros, presentes nos equipamentos	Sobreposição de escrita de dados	Disponibilizar mecanismos que garantam a sobreposição de escrita nos dados contidos nos suportes de armazenamento	
		Eliminação automática de dados	Disponibilizar mecanismos que garantam a eliminação automática de dados nos suportes de armazenamento	
		Eliminação de dados temporários	Disponibilizar mecanismos que garantam a eliminação de dados temporários dos suportes de armazenamento	
		Destruição e eliminação segura de dados	Disponibilizar mecanismos que garantam a destruição e eliminação segura de dados contidos em suportes de armazenamento	
		Processo de eliminação de dados que inviabilize potencialmente a sua recuperação	Disponibilizar processos que garantam a potencial eliminação definitiva dos dados	NIST 800-88
INTEGRIDADE (SOFTWARE, FIRMWARE E DADOS)	Manutenção e consistência dos dados durante o ciclo de vida dos mesmos	Consistência/validade dos dados ao longo do seu ciclo de vida	Garantir encriptação de dados	FIPS 140-2
			Garantir atualização das últimas versões certificadas de firmware e software	ISO/IEC 15408
		Verificação de firmware no arranque do equipamento	Disponibilizar ferramentas que assegurem a protecção e detecção de todas as alterações que se vierem a verificar ao nível do firmware (ex: monitorização e prevenção automática de software malicioso)	FIPS 140-2
		Integridade das aplicações instaladas	Assegurar processos de validação de segurança no desenvolvimento aplicacional	ISO 15408s
		Rastreamento e auditoria	Assegurar o controlo e registo dos acessos ao dispositivo e transmissão de logs para um sistema de auditoria	Integração com ferramentas SIEM
DETEÇÃO E PROTEÇÃO	Identificar, detetar e proteger os dispositivos contra actividades intrusivas e/ou software maligno	Mecanismos preventivos e/ou sistemas de monitorização e deteção de potenciais ataques	Permitir a criação de regras para filtragem de tráfego de dados com base em combinações de endereços IP (origem/destino)	ISO/IEC 27033-4
			Disponibilizar software residente nos equipamentos para uma constante verificação de potenciais ameaças	
		Encriptação de dados	Assegurar a encriptação dos dados nos suportes de armazenamento	FIPS 140-2 - Encriptação
		Encriptação das comunicações	Garantir a impressão e digitalização encriptadas	FIPS 140-2 - Encriptação IPsec IEEE 802.1x SSL/TLS
		Validação de equipamentos na rede	Disponibilizar mecanismos para autenticação de dispositivos nas redes LAN ou WLAN	IEEE 802.1x

Nota introdutória ao quadro de mobilidade

Segundo um estudo disponibilizado pela Insight, 93% dos colaboradores que tem *smartphone* usa-o diariamente para trabalho. Diz o mesmo estudo que estes colaboradores utilizam o *smartphone* em 33% do seu tempo de trabalho. Esta mesma fonte refere ainda que 58% dos inquiridos considera provável que os dispositivos móveis possam substituir os computadores tradicionais num espaço temporal de 5 anos.

Em Portugal os *smartphones* são responsáveis por 92,1% do total dos acessos à internet, recaindo apenas 7,9% para *tablets* e computadores. Com a crescente passagem de processos de negócio para ambientes móveis verifica-se por um lado uma cada vez maior dependência dos *smartphones* e *tablets* para a realização de tarefas por parte dos colaboradores e por outro um aumento de risco de ciberataques através destes *endpoints* pois é ainda residual o número de organizações públicas ou privadas que implementou mecanismos de segurança para proteção destes dispositivos.

É evidente assim que cada vez mais é imperativa, para qualquer organização, definir uma estratégia sólida de segurança para a mobilidade, implementando ou reforçando mecanismos que visem a mitigação de riscos de ciberataques através dos smartphones ou *tablets*.

Pretendemos de seguida e através do quadro "Mobilidade" apresentar um conjunto de medidas e ações que visam ajudar os decisores a avaliar os riscos que enfrentam e as medidas que poderão implementar visando o incremento dos níveis de cibersegurança nos processos de autenticação, na eliminação segura de dados, na integridade dos dispositivos móveis ou na deteção e proteção de vulnerabilidades.

MOBILIDADE

REQUISITOS	OBJETIVO / FINALIDADE (CONCEITO)	COMO? (TECNOLOGIA / SOLUÇÃO)	FORMAS DE COMPROVAR	OBSERVAÇÕES E REFERÊNCIAS
AUTENTICAÇÃO	Identificação inequívoca de um determinado indivíduo/utilizador ou dispositivo para acesso a um ou vários sistemas	Credenciais fornecidas pela entidade	Utilização de certificados digitais	ISO/IEC 9594-8 NIST SP 800-63B
		Autenticação biométrica	Utilização de dados biométricos para autenticação (impressão digital)	SO/IEC 19795 ISO/IEC 30107
		Autenticação biométrica	Utilização de dados biométricos para autenticação (impressão digital)	NIST SP 800-53 ISO/IEC 2700; 15408
ELIMINAÇÃO SEGURA DE DADOS	Eliminação de dados sensíveis contidos nos suportes de armazenamento ou outros, presentes nos equipamentos	Encriptação dos dados	Através do SO é possível proteger os dados com encriptação utilizando AES256, não só da memória interna mas também externa, como um cartão de memória	FIPS 140-2 NIST SP 800-111
		Utilização de container/work profile para separação dos dados	Através de uma plataforma de EMM é possível criar e gerir esta área segura e isolada do restante dispositivo	NIST SP 800-124; SP 800-164 ISO/IEC 27001
		Remote wipe/local wipe	Pode ser definida uma política para que um dispositivo seja apagado quando deixar de comunicar com a plataforma de EMM por um período de tempo, ou quando uma palavra-passe incorrecta é submetida vezes demais	NIST SP 800-53 ISSO/IEC 27001; 15408
INTEGRIDADE (SOFTWARE, FIRMWARE E DADOS)	Manutenção e consistência dos dados durante o ciclo de vida dos mesmos	Arranque seguro	No arranque, todos os componentes são verificados para garantir que não existe corrupção do OS	NIST SP 800-193 ISO/IEC 11889
		Attestation	O processo de attestation passa por comparar duas imagens do SO para perceber se são idênticas ou se existem alterações suspeitas	ISO/IEC 15408 NIST SP800-53
		Assinatura de atualizações	Todas as actualizações de aplicações e firmware devem ser assinadas de forma a garantir a sua integridade e desta forma mitigar a instalação de software malicioso	ISO/IEC 9594-8 NIST SP800- -63B
DETEÇÃO E PROTEÇÃO	Identificar, detetar e proteger os dispositivos contra actividades intrusivas e/ou software malignos	Updates de segurança regulares	Todos os meses são lançados patches de segurança para várias vulnerabilidades identficadas e reportadas aos fabricantes forma de mitigar a instalação de software malicioso	NIST SP 800-53 ISO/IEC 27001
		Permissões necessárias	As aplicações apenas têm permissões a certos componentes do SO necessários à sua operação e não podem aceder a operações mais sensíveis, nem obter privilégios de root	ISO/IEC 15408 NIST SP 800-53
		Monitorização em tempo real	Monitorização e proteção em tempo real do Kernel, prevenindo a modificação do seu código, mapeamento dos dados em mémoria ou o fluxo de controlo	NIST SP 800-53
		Canais de comunicação seguros	Utilização de VPN para comunicação segura e encriptação dos dados in- transit	FIPS 140-2 NIST SP 800-77; SP 800-113

c. Normas, certificações, fontes e boas práticas

O enquadramento normativo apresentado neste Guia tem por base normas internacionais ISO (*International Organization for Standardization*) e/ou IEC (*International Electrotechnical Commission*). Tratando-se de organismos internacionais de normalização as suas normas são acessíveis ao público em geral, e constituem *standards* internacionais, conforme o Regulamento 1025/2012 da UE.

Pela especificidade técnica no âmbito da cibersegurança são ainda utilizadas referências a regras e padrões de conformidade produzidos pelo NIST (*National Institute of Standards and Technology*), com particular relevo para o desenvolvimento de *standards* FIPS (*Federal Information Processing Standards*) relativos à especificação de padrões de segurança em sistemas de criptografia.

Por último é também referido o padrão TCG Opal, desenvolvido pelo *Trusted Computing Group*, uma organização internacional sem fins lucrativos que desenvolve especificações de segurança usadas para aplicar a criptografia baseada em *hardware* para dispositivos de armazenamento

O conjunto de referências utilizado, pela amplitude de cada uma delas e embora estando diretamente relacionado com os *endpoint devices*, é em muitos casos extensivo a outros dispositivos ou componentes de uma infra-estrutura tecnológica.

Existem ainda normas, que não estando diretamente ligadas aos *endpoint devices* enquanto dispositivos, são relevantes no que respeita ao seu fabrico, instalação e gestão. A título de exemplo a certificação ISO 27001, que assegura que o fabricante dos dispositivos e/ou o prestador de serviços tem implementado um modelo para estabelecer, implementar, operar, monitorizar, analisar, manter e melhorar um Sistema de Gestão de Segurança da Informação.

Também a compatibilidade dos *endpoint devices* com ferramentas de gestão centralizada que garantam a conformidade com as políticas de segurança implementadas, bem como a atualização automática dos controladores, *firmware* e BIOS dos dispositivos, pode reforçar a resiliência perante ciberataques.

Pela atual amplitude e pela constante evolução tecnológica e normativa o grande desafio é a aposta constante, numa perspetiva de prevenção, deteção e resposta, no incremento de camadas de segurança no *endpoint device*, bem como a montante e a jusante do mesmo. O Quadro Nacional de Referência para a Cibersegurança, pela sua abordagem holística, e o Quadro de Avaliação de Capacidades de Cibersegurança, como ferramenta de classificação das organizações na sua capacitação em cibersegurança, ambos produzidos pelo Centro Nacional de Cibersegurança, constituem-se como boas referências transversais. Também a ENISA nas suas várias publicações, com destaque para *Standards Supporting Certification - February 04, 2020*, fornece várias indicações com o objetivo de apoiar a definição de uma estratégia de cibersegurança.

V. CONCLUSÃO

V. Conclusão

A segurança do ciberespaço é seguramente um dos maiores desafios que hoje se colocam à segurança (e ao bem-estar) dos cidadãos, das organizações, e mormente, dos próprios Estados.

Ciente desta realidade, o Governo assumiu a cibersegurança como um vetor estratégico para o País, consubstanciado no **Quadro Nacional de Referência para a Cibersegurança** (QNRCS) e, mais recentemente, no **Plano de Ação para a Transição Digital**, em que a "Digitalização do Estado" é um dos três pilares da transição digital em Portugal, e a cibersegurança surge como um dos seus catalisadores transversais.

Este Plano de Ação reconhece a **desadequação do enquadramento legal de contratação pública inerente à prestação de serviços e aquisição de bens no âmbito das TIC, pela Administração Pública, e dá carácter prioritário à sua simplificação.**

Ora, no quadro da anunciada alteração legislativa dos procedimentos de contratação pública na área das TIC, a cibersegurança não pode deixar de ser introduzida como um requisito de base, em especial quanto aos ***endpoint devices*, que são a porta de entrada para a grande maioria dos ciberataques, e a origem de mais de um quarto das quebras de segurança.**

O nível da exigência quanto à cibersegurança dos *endpoint devices* poderá variar em maior ou menor grau, face ao tipo de dispositivo e de utilização que lhe vai ser dada, mas aquela deverá ser sempre um requisito. Quer por razões de coerência na execução do próprio Plano de Ação para a Transição Digital, quer porque, se a cibersegurança for descuidada, o risco de ciberataques com origem naqueles aumentará consideravelmente.

Tendo presente que a generalidade dos dispositivos oferecidos no mercado incorpora funcionalidades de cibersegurança, apesar de poderem existir alguns em que tal não suceda, com este Guia, a AGEFE vem proporcionar uma **ferramenta prática de referenciação dos aspetos essenciais da sua segurança**, com base na normalização, por forma a garantir a sua neutralidade tecnológica e concorrencial.

Os decisores, públicos ou privados, não especialistas em matéria de cibersegurança, poderão encontrar neste documento a informação essencial sobre o enquadramento normativo para os *endpoint devices* neste domínio, que os habilita a tomarem opções informadas na aquisição destes dispositivos, fornecendo-lhes de uma forma operacional os elementos complementares de que necessitam para a execução do QNRCS.

Reconhece-se que o investimento em cibersegurança é direta e predominantemente traduzível pelo preço e/ou esforço de implementação, porém, nunca é demais salientar que o **custo do não investimento nesta área pode ser projetado nas consequências de uma possível indisponibilidade de serviço, no preço e esforço de recuperação de dados ou sistemas, nos danos reputacionais, ou em eventuais consequências indemnizatórias por roubo de dados, entre outros.**

É a conciliação entre o contexto normativo, a tecnologia e a mitigação do risco, que constitui o necessário e permanente desafio dos responsáveis públicos e privados em matéria de cibersegurança.

VI. ANEXO

VI. Anexo

EMPRESAS ASSOCIADAS / SETOR DE TIC E ELÉTRONICA - 2022
APPLE PORTUGAL, UNIPESSOAL, LDA.*
ATLANT PHOTO IMAGE, S.L
BEEVC, ELECTRONIC SISTEMS, LDA.
BELTRÃO COELHO - SISTEMAS DE ESCRITÓRIO, LDA.
BROTHER IBÉRIA, S.L. - SUCURAL EM PORTUGAL
CANON MEDICAL SYSTEMS, S.A.
CLOVER PORTUGAL, LDA.
COMERCIALFOTO - IMPORTAÇÃO E COMÉRCIO DE ARTIGOS FOTOGRÁFICOS, LDA.
COMPANHIA I.B.M. PORTUGUESA, S.A.
CONSTRÓNICA - PROJECTOS, MONTAGEM E COMERCIALIZAÇÃO EQUIPAMENTOS ELECTRÓNICOS, LDA.
COVISE - IMPORTAÇÃO E EXPORTAÇÃO, LDA.
CPCDI - COMPANHIA PORTUGUESA DE COMPUTADORES - DISTRIBUIÇÃO DE PRODUTOS INFORMÁTICOS, S.A.
DITRAM - COMPONENTES E ELECTRÓNICA LDA.
E. DIAS SERRAS, S.A.
EPSON IBÉRICA, S.A. - SUCURSAL EM PORTUGAL
ERICSSON TELECOMUNICAÇÕES, LDA.
FUJIFILM EUROPE GMBH - SUCURSAL EM PORTUGAL
FUJITSU TECHNOLOGY SOLUTIONS, LDA.
GENERAL ELECTRIC HEALTHCARE PORTUGAL, SOCIEDADE UNIPESSOAL, LDA.
HPCP - COMPUTING AND PRINTING PORTUGAL, UNIPESSOAL, LDA.
IBERTRADE - EXPORTAÇÃO, IMPORTAÇÃO E IMÓVEIS, S.A.
KONICA MINOLTA BUSINESS SOLUTIONS PORTUGAL, LDA.
KYOCERA DOCUMENT SOLUTIONS PORTUGAL, LDA.
LECTRA PORTUGAL - SOLUÇÕES DE ALTA TECNOLOGIA PARA A INDÚSTRIA, LDA.
LEICA GEOSYSTEMS - SISTEMAS PARA GEODESIA E TOPOGRAFIA, SOCIEDADE UNIPESSOAL, LDA.
LEICA MICROSISTEMAS - INSTRUMENTOS DE PRECISÃO, SOCIEDADE UNIPESSOAL, LDA.
LENOVO (SPAIN) SL - SOCIEDAD UNIPESSOAL SUCURSAL PORTUGAL*
LEXMARK INTERNATIONAL (PORTUGAL) - SERVIÇOS DE ASSISTÊNCIA E MARKETING, SOCIEDADE UNIPESSOAL, LDA.
LG ELECTRONICS PORTUGAL, S.A.
LISCIC - SISTEMAS DE INFORMAÇÃO E COMUNICAÇÃO, LDA
MULTIMAC – MÁQUINAS E EQUIPAMENTOS DE ESCRITÓRIO, S.A.
OKI SYSTEMS (IBERICA), S.A. - SUCURSAL EM PORTUGAL
OLYMPUS IBERIA, S.A.U. - SUCURSAL EM PORTUGAL - SUCURSAL EM PORTUGAL
OLYMPUS SERVICE FACILITY PORTUGAL - TECNOLOGIAS ÓPTICAS E DIGITAIS, LDA.
PANASONIC PORTUGAL, SUCURSAL DE PANASONIC MARKETING EUROPE GMBH
PHILIPS PORTUGUESA, S.A.
PROSONIC - PRODUTOS DE IMAGEM E COMUNICAÇÃO S.A.
RADIO HOLLAND PORTUGAL - RHP, S.A.
RETAIL4PEOPLE, S.A.
RICOH PORTUGAL, UNIPESSOAL, LDA.
ROBERT BOSCH, S.A,
SAMSUNG ELECTRÓNICA PORTUGUESA, SA.
SCHNEIDER ELECTRIC, LDA.
SIMMEDICA - SISTEMAS INTEGRALES DE LA MEDICINA, S.A. - SUCURSAL EM PORTUGAL
SONY EUROPE B.V. SUCURSAL EM PORTUGAL
TD TECH DATA PORTUGAL, LDA.
TOSHIBA EUROPE GMBH - SUCURSAL EM PORTUGAL
XEROX PORTUGAL - EQUIPAMENTOS DE ESCRITÓRIO, LDA.

* Aderiram à AGEFE em 2021

agefe

ASSOCIAÇÃO EMPRESARIAL DOS SETORES ELÉTRICO, ELETRODOMÉSTICO, ELETRÓNICO E DAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

Campo Grande, 28 - 10.º C, 1700-093 Lisboa
Telf. 210 182 127
www.agefe.pt