CYBERLAW

by CIJIC

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente.***

CYBERLAW by CIJIC

EDIÇÃO N.º XI – MARÇO DE 2021

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW
by CIJIC

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

CYBERLAW by CIJIC

NOTAS DO EDITOR:

Finda Março do ano de 2021.

Passou um ano desde que o mundo se confinou, massivamente. Fechados, em casa, nunca como a partir disto o acesso à *Internet* se nos desvelou como um direito humano fundamental.

O sonho de uma *internet* livre, neutral, aberta, inclusiva, universal será possível?

Provavelmente muitos de nós, que navegam por ela, num ou noutro canto de conversação e/ou *stop by* possível a partir de um dos nossos hodiernos cárceres físicos, já nos deparámos com um curioso grafo. Nele consta uma espécie de sondagem onde à pergunta: *"Quem fez mais pela digitalização da sua organização no último ano?"*, a percentagem do vencedor surpreende.

Não, não foi o CEO da organização. Também não, não foi o CISO (quando as organizações os têm). Sim, também não foi nenhum diretor de nenhum departamento da organização.

O principal responsável, sim, foi ela: a pandemia de covid-19.

É inegável. A pandemia acelerou o processo de digitalização de grande parte das interações humanas, sejam elas de qualquer natureza, escola, comércio, socialização.

Não obstante, por mais benefícios que este *input*, à *força bruta*, tenha trazido, a humanidade tem ainda um caminho muito longo para percorrer.

Num plano macro, que convoca a humanidade, combater ferozmente a exclusão digital, com particular enfoque nos reversos, *i.e.*, mais novos e mais velhos; sociedades desenvolvidas/mais pobres.

E se o acesso não é universal (sê-lo-á algum dia?), plural, em condições idênticas, inclusivo…também não deixará de ser preocupante, dentro daqueles que podem aceder, o número de indivíduos com falta de formação, com falta de um mínimo de educação/formação para usufruir da Rede.

Atente-se, porém, num plano micro, por exemplo, no caso português.

Entregue, neste último dia de Março de 2021, o RASI2020[1], nele despontam algumas evidências sobre a temática da falta de educação para o *ciber*. Os crimes praticados na e pela *Internet*, nomeadamente, *phishing*, *vishing*, *ransomware* e extorsão[2], em passo crescente, decorrem de variadas falhas ao nível do utilizador. Sobressai, da leitura crua dos números, uma inexistente cultura de ciberhigiene. A facilidade de promoção de engenharias sociais avulsas. É esta omissão de cibereducação responsável pela inabilidade em detetar o logro e burlões, em actividade fervorosa. No compasso da oferta/procura de produtos através do digital, se as trocas aumentam exponencialmente, paralela e em acompanhamento, as situações de fraude, burla, roubo, *Money mules*, etc., *idem*.

As múltiplas deficiências ao nível do utilizador – o famoso factor humano é implacável - e a violência de uma *digitalização à força bruta* de uma grande maioria das organizações, combinadas… dão razão de ser à *tame joke* informática de que, *na prática, em termos de ataques e crimes informáticos, só há dois tipos de organizações: as que*

1 Disponível para consulta em: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDQ1NAUABR26oAUAAAA%3d (último acesso 31MAR21)
2 *Vide* páginas 67 e ss do RASI2020.

sabem que já foram atacadas e as que ainda não o sabem (a premissa irónica é, infelizmente, igualmente válida para as pessoas singulares).

Torna-se inadiável que, paralelamente ao percurso do Direito no séquito da acelerada digitalização, as organizações, as pessoas, o Estado, entendam, decisiva e finalmente, a importância da segurança da informação[3].

Apaticamente, e em crise, as omissões perduram. Sedimentam.

Os alertas não chegam a bom porto. Provenham eles de serviços mais ou menos capacitados do Estado, sejam serviços secretos nacionais, sistema de segurança interna, observatórios…jaz, apenas, a constatação impotente de que "(…) *observa-se um aumento da espionagem através de ameaças persistentes, tecnologicamente avançadas, de origem estatal, direcionadas a importantes centros de informação do Estado. Uma das consequências da sofisticação enunciada, prende-se com a crescente dificuldade em destrinçar ataques informáticos para efeitos de crime económico ou de crimes de sabotagem, dirigidos a empresas e grupos de empresas com relevância no tecido empresarial nacional*."

No presente, de crescente digitalização, de cascata informacional, já todos sabemos que não é a quantidade de informação que serve à melhor tomada de decisão; é a qualidade. Mostra-se-nos angustiante o sublinhado de "*ameaças persistentes, tecnologicamente avançadas, de origem estatal, direcionadas a importantes centros de informação do Estado"*.

O Estado, como nunca, até como condição de promoção e prossecução geracional, tem o dever de defender um desígnio de soberania consubstanciado, precisamente, na superioridade informacional.

Conhecerá o Estado a capital importância da superioridade informacional?

Estará capacitado, humana e tecnologicamente, para proteger, o mais eficazmente possível, os seus mais valiosos *assets*, as suas infraestruturas mais críticas?

---

3 Ainda, no RASI2020 agora dado a conhecer, «(…) *No universo da ciberespionagem, registaram-se novos ciberataques contra infraestruturas críticas nacionais, com a finalidade de aceder a informação classificada, com valor político e económico."*», página 102.

Severa, a frieza dos parágrafos, no contexto pandémico Covid-19: "*No que concerne a outra das ameaças, i.e., as operações cibernéticas ofensivas, foram identificados agentes estatais e não estatais, visando entidades públicas e privadas, em particular no que respeitou à exploração de oportunidades…Verificaram-se inúmeros ciberataques registados contra instituições do setor da saúde, bem como operações de ciberespionagem contra entidades de investigação cientifica, particularmente envolvidas na pesquisa de terapêuticas e de vacinas contra a doença em apreço.*"

A segurança da informação, e a superioridade informacional que daí possa erigir, são, no contexto, de suma importância.

Infelizmente, as ameaças são múltiplas. Se, como veremos nesta nova edição, a Segurança da informação nas organizações(SiO) é tema fulcral, a erosão, de direitos fundamentais humanos, não descola de uma objetificação pronunciada da pessoa, do ser individual. Discreta, mas de forma expedita, as *oportunidades geradas pelo contexto pandémico*, têm servido para que o Estado arroje sistemas de videovigilância por múltiplas localidades nacionais[4]. A febre dos sistemas *CCTV* públicos segue a passo acelerado.

Em simultâneo, embora a aplicação *stayawaycovid* não tenha vingado, ainda, é certo que o controlo à distância da pessoa irá figurar, brevemente, em alguma medida legislativa. Notemos, ainda no contexto da pandemia, por exemplo, e em pleno estado de emergência, os níveis de mobilidade do cidadão. Com a proibição de circulação fora-do-concelho e a aproximação do tema festivo pascal, na semana de 25/26 de Março, acordámos com a notícia: "*Portugueses fogem para longe das restrições: um em cada dez dormiu a mais de 100 quilómetros de casa esta quinta-feira.*"[5].

4 Ainda no RASI2020, dentre renovações e novas autorizações, surgem destacadas 8 despachos de autorização de instalação de múltiplas cameras de videovigilância para localidades. Consultáveis a partir dos Anexos do relatório, Medidas legislativas, página 15 e ss.
Nota: entretanto, no início do mês de março 2021, foi-nos dada a conhecer a autorização para instalação de mais 216 cameras de videovigilância na cidade de Lisboa, para juntar às já existentes (o Bairro Alto já dispõe de sistema, por exemplo).

5 https://expresso.pt/sociedade/2021-03-26-Portugueses-fogem-para-longe-das-restricoes-um-em-cada-dez-dormiu-a-mais-de-100-quilometros-de-casa-esta-quinta-feira-b98a7df0 (último acesso 31MAR21).

A observação - próxima da realidade? - feita por uma consultora privada[6], revelando que mais de *um milhão de portugueses dormiu fora de casa*, curiosamente, não promoveu nenhum sobressalto jurídico. Nem social. A ordem continua serena. *Curiosamente*. Mas, não houve tratamento de dados pessoais para a revelação de tais estatísticas em mobilidade? Que finalidade jurídica prosseguiu a captura de tais dados? Que dados foram recolhidos? Foram coligidos de forma lícita? Que tratamento tiveram? Quais as garantias de anonimização e/ou minimização do tratamento?

Alguém questionou?

Alguém se indignou?

Não sendo a primeira vez que uma entidade privada analisa dados dos portugueses, em massa, sem qualquer tipo de reacção/oposição por parte destes, presumivelmente, como solução eficiente a tomar por parte do Estado, no futuro deveremos promover toda uma actividade concursal de fundos públicos para *investigação* - geral e abstrata - de *tendências*, *mobilidade*, *gostos e desejos* dos portugueses. Não que haja uma qualquer necessidade de uma finalidade concreta, lícita de sopeso. Afinal, o problema, de fundo, do sobressalto cívico e jurídico, da ordem, reside numa mera formalidade de *marketing*, o "publico não pode" vs. "privado tudo pode".

Acabemos prontamente com a folia[7].

O acesso a metadados são um problema para a acção das nossas secretas?

Do titular da acção penal, *tout court*, português?

---

6 Vejamos, por exemplo, o detalhe dos grafos sobre a evolução do confinamento e mobilidade em: https://www.pse.pt/evolucao-confinamento-mobilidade/ (último acesso 31MAR21).

7 Reparem na notícia: https://www.jornaldenegocios.pt/economia/impostos/amp/fisco-vai-ter-assistente-virtual-no-facebook-para-responder-as-duvidas-de-irs (último acesso 31MAR21).
Ora, a Autoridade Tributária portuguesa entende que a plataforma do Facebook é a melhor disponível *para tirar dúvidas a contribuintes nacionais.* Como todos sabemos, e somos *surpreendidos semanalmente*, o Facebook, provavelmente, já é conhecedor da informação fundamental e necessária dos seus utilizadores. Com este *passo de modernidade* da nossa AT, na prática, ao Facebook bastar-lhe-á agrupar a informação detida à contributiva, com os rendimentos declarados, das finanças portuguesas e... *Et voila*, vitracidade completa do cidadão. (quanto será o preço de cada miríade informacional de um contribuinte concreto que a AT poderá desembolsar? Haverá já um acordo bilateral entre a entidade privada e a AT?)
É, pois, tempo de assumirmos já a cedência gratuita dos nossos dados pessoais às entidades privadas e, a partir daí, o Estado seja profícuo no controlo de todas as nossas actividades sem qualquer tipo de sobressalto jurídico ou social.

Renunciemos à recolha de torrentes de dados pessoais às entidades privadas, assumamos a bonomia do *surveillance capitalism*, encapotando o próprio "*estado de vigilância*", e vivamos felizes.

E ordeiros. Sem sobressaltos.

A justificação, para esta aceitação social passiva e dócil, por parte de uma maioria de cidadãos, refletindo, denota muito do seu analfabetismo. Analfabetismo digital. Mas também social. A ordem das coisas apenas sobrepuja o ponto de partida. A liberdade individual é gratuitamente cedida a entidades privadas. Nunca ao Estado. A compressão de direitos fundamentais apenas terá de partir deste porto privado.

Aquiesçamos, afinal, mais de duzentos anos depois, a sociedade não compreende o ditame de que "*uma sociedade que troca um pouco de liberdade por um pouco de ordem acabará por perder ambas, e não merece qualquer delas*"[8].

Nesta nova edição da Cyberlaw by CIJIC, em consonância com os docentes do Mestrado em segurança da informação e direito do ciberespaço[9], tivemos o ensejo de provocar alguns discentes a reflexões sobre a realidade pungente que convoca a sociedade. No presente e para o futuro. Entre a segurança da informação nas organizações (SiO), a consciencialização dos funcionários das organizações para a temática, o factor humano na SiO; dados pessoais em *Schrems II* e acesso a metadados por parte do MP sem um suspeito determinado ou determinável, *not/net neutrality*, os discentes procuraram reunir algumas interjeições que, como já demos conta oportunamente, ajudem a mitigar a desigual compreensão, a despertar a consciencialização individual para promoção de um combate ao analfabetismo digital.

Trazemos, também, a participação de proeminentes juristas brasileiros que acederam ao nosso convite para dissertarem sobre a lei geral de proteção de dados brasileira assim como sobre o fenómeno do *stalking* em contexto laboral inclusive em ambiente digital.

8 Thomas Jefferson (1743-1826), carta a James Madison.
9 https://fenix.tecnico.ulisboa.pt/cursos/msidc

Resta-me, assim e por fim, agradecer a todos quantos contribuíram para mais esta nova edição da Revista, pelo esforço, pela disponibilidade, pela obra, endereçando a todos, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um merecidíssimo: - Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 31 de Março de 2021

Nuno Teixeira Castro

A SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES NO *NOVO NORMAL* (COVID-19)

RUI FILIPE BARATA PEREIRA*

e

GONÇALO NUNO BAPTISTA DE SOUSA†

* Mestrando em segurança da informação e direito ciberespaço.
† Professor e investigador na Escola Naval.
Contacto: goncalobsousa@gmail.com

RESUMO

A Segurança da Informação em geral e nas Organizações em particular é um tema de importância crescente, contínua e consistentemente, nestas últimas décadas. É um elemento e uma preocupação presente no dia a dia das mais variadas atividades, seja na esfera da área pessoal, individual e social, seja nos serviços e organizações públicas como saúde, justiça, segurança e governação em geral, seja nos serviços e organizações privadas tanto nos sectores primário como secundário e terciário. Por isto tudo é também afetado por uma grande diversidade de eventos e transformações que vão surgindo nas sociedades modernas. Assim eventos como esta mais recente realidade provocada pela Pandemia do Covid-19 têm um impacto muito significativo na abordagem do tema da Segurança da Informação e em especial no que se refere ao tema de estudo deste trabalho, a segurança da informação nas organizações no novo normal (Covid-19).

Palavras-Chave: Segurança da Informação; Segurança da Informação nas Organizações; Pandemia e COVID-19; Cibersegurança.

ABSTRACT

Information Security in general and in Organizations is a topic of increasing and continuous importance in these last decades. Be it in the sphere of personal, individual and social areas, or in public services and organizations such as health, justice, security and government in general, or in services and private organizations either in the primary, secondary and/or tertiary sectors, is a factor as well as a concern supported in the day to day of these varied activities. In addition to all this, it is still affected by a great diversity of events and transformations that are emerging in modern societies. Thus, events like this most recent reality caused by the Covid-19 Pandemic have a very significant impact in addressing the topic of Information Security and regarding this work, namely, information security in organizations in the *new normal* (Covid-19).

Keywords: Information security; Information Security in Organizations; Pandemic and COVID-19; Cybersecurity.

1. Introdução

Este trabalho foca-se no caso das organizações em que a sua área de negócio permite o trabalho remoto, nomeadamente a Indústria de serviços.

O impacto da Pandemia Covid-19, no que concerne a este tema de estudo, levou a que as Organizações fossem obrigadas a uma drástica mudança para um ambiente de trabalho remoto.

Esta alteração dos modos de trabalho forçou uma acelerada Transformação Digital nas Organizações. Transformação essa materializada em processos, sistemas e tecnologias para permitir uma massificação do trabalho remoto em toda a organização. Esta transformação, além de processos e tecnologias, deve envolver também pessoas.

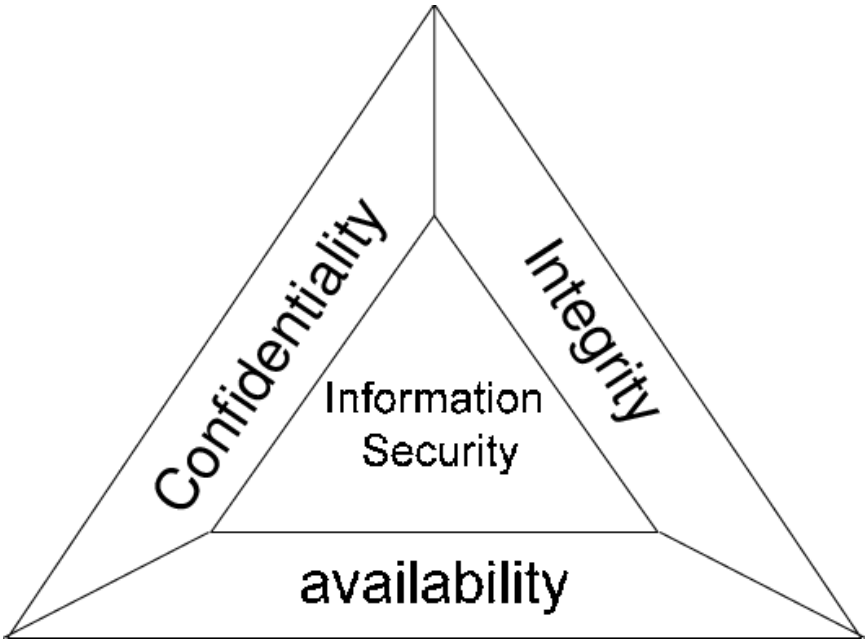
O contexto desta transformação, com a sua rápida mudança para um ambiente de trabalho remoto, criou uma pressão extra nas áreas de Segurança de Informação.

2. O Significado e a Significância da Segurança da Informação

Comecemos primeiro, servindo-nos do trabalho de Joseph Boyce[1], por referir a definição e importância da Segurança da Informação.

Segurança da Informação é todo o processo para a proteção e defesa da informação assegurando a sua Confidencialidade, Integridade e Disponibilidade[2] (DIC) ou na sigla em inglês CIA.

Figura 1



Na sua base a Segurança da Informação (SI) envolve a proteção dos direitos de pessoas e organizações. A SI permite às organizações a proteção dos seus direitos num meio concorrencial em que a informação sendo um ativo importante é também um elemento omnipresente no dia a dia das organizações desde a gestão às operações. A SI

1 Boyce, Joseph. *Information Assurance: Managing organizational IT Security Risks.* s.d.
2 Estas são as três propriedades que de modo mais generalizado são reconhecidas. No entanto existem outras abordagens em que são referidas também as propriedades de **Não Repúdio** e **Autenticação**.

permite também às organizações a capacidade de proteger os direitos de outras entidades com quem interagem. Estas entidades incluem colaboradores, clientes (consumidores dos seus produtos) atuais e potenciais futuros clientes, fornecedores e outras organizações com quem se associem em resultado de parcerias ou *joint ventures*.

3. A Sociedade da Informação

A terceira Revolução Industrial ou Revolução Digital permite nos fins do século 20 a evolução para uma Sociedade da Informação. A chamada quarta Revolução Industrial ou Indústria 4.0 veio na última década dar uma importância acrescida às várias questões e desafios da Sociedade da Informação.

Dos vários desafios identificados a nível político, económico, social e organizacional destaca-se o desafio a nível social da vigilância, questões de confiança e preocupação da privacidade.

A nível organizacional destacam-se os desafios associados a: Problemas de segurança nas Tecnologias de Informação (TI) agravados pela necessidade ade abertura e conectividade de sistemas de produção anteriormente em ambiente fechado. Confiabilidade e estabilidade indispensáveis para todos os sistemas dependentes das TI, mas crítico em sistemas como por exemplo em M2M (*machine-to-machine communication*). Manutenção da Integridade da informação e dos processos de produção. Proteção da confidencialidade da informação. Neste último desafio destaca-se que a nível organizacional há a necessidade não só da proteção da propriedade intelectual, mas também da proteção dos dados pessoais de todos os envolvidos na organização, funcionários, clientes e outros envolvidos em parcerias[3].

A Sociedade da Informação está em todos os setores do quotidiano!

A atual Sociedade da Informação assente na crescente importância da informação e dos processos e meios que aceleram a disponibilidade da mesma tem vindo a potenciar

3 Wikipédia Indústria 4.0

um vasto com junto de melhorias, entre as quais se realçam os contributos para as organizações e sua gestão e também para as infraestruturas e a cidadania.

Temos presenciado, devido à valorização da informação, uma grande evolução nos processos de gestão e de governança.

As infraestruturas tecnológicas e os Sistemas de Informação (SI) permitem às organizações gerar vantagem competitiva sobre potenciais competidores. Assim a economia já não dispensa estes sistemas e infraestruturas que aumentam diretamente a sua cadeia de valor.

Também as chamadas infraestruturas críticas, privadas ou públicas, como telecomunicações, banca e finanças, transportes, energia, água, serviços de emergência, assentam cada vez mais em SI e Tecnologias de Informação e Comunicação (TIC), tornando-se deles dependentes. Aliás, as infraestruturas complexas são mais fáceis de gerir com computadores e sistemas operativos, aplicações e protocolos de redes comuns.

Paralelamente, a Sociedade de Informação traz novos desafios no que respeita à segurança[4].

Paradoxalmente, a conectividade que é uma vantagem é também o maior problema da segurança. O seu funcionamento em rede aberta, sem delimitação de fronteiras físicas, as relações de dependência e interdependência entre infraestruturas críticas, as vulnerabilidades de cariz tecnológico e a exposição a ações malévolas ou mesmo de menores cuidados de utilização, torna o ciberespaço muito exposto a novas vulnerabilidades e ameaças, algumas de natureza disruptiva.

Figura 2

4 Cibersegurança: das preocupações à ação - IDN Instituto da Defesa Nacional

As questões e soluções inerentes à Segurança da Informação baseiam-se em tecnologia, processos e pessoas e devem resultar duma análise, com identificação e avaliação, do valor da informação a proteger. Como é comum designar deve identificar-se quais são as "joias da coroa" da organização, fazer a respetiva avaliação e decorrente desse valor desenvolver e implementar as respetivas soluções.

4. Segurança da Informação e Cibersegurança

Os desafios inerentes à Segurança da Informação são também abordados na área da Cibersegurança.

Na definição do CNCS[5]:

"Cibersegurança - *Conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem*."

"Segurança da Informação - *Proteção dos sistemas de informação contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento,*

5 https://www.cncs.gov.pt/recursos/glossario/

processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não autorizados, incluindo as medidas necessárias para detetar, documentar e contrariar tais ameaças."

Conforme as normas e padrões de referência internacional utilizados assim também se utiliza mais uma definição ou outra.

As normas ISO 2700x são o padrão e a referência internacional para a gestão da Segurança da informação, e definem os requisitos e orientações para o desenho e implementação nas organizações de um Sistema de Gestão de Segurança da Informação (SGSI) ou ISMS (Information Security Management System)[6].

Além do ISO 2700x temos desde 2014 do NIST dos Estados Unidos a publicação da Estrutura de Segurança Cibernética NIST CSF (NIST Cyber Security Framework), que fornece uma estrutura de política de orientação sobre segurança de computadores, mais orientada para a proteção das organizações privadas americanas em relação a ciber ataques[7].

Não obstante a tendência recente que apresenta uma utilização crescente do termo Cibersegurança em detrimento de Segurança da Informação, da análise das definições de segurança da informação e ciber segurança produzidas pelos organismos europeu ENISA[8], americano CNSS[9] e organismos de certificação como o ISACA[10] entende-se a definição de Segurança da Informação como mais abrangente em relação à definição de Ciber Segurança.

6 https://www.27001.pt/
7 https://www.nist.gov/cyberframework
8 https://www.enisa.europa.eu/
9 https://www.cnss.gov/
10 https://www.isaca.org/

5. Impacto da Pandemia Covid-19

O dia 18 de março de 2020 fica marcado para sempre na história da democracia portuguesa. Foi a primeira vez que um Estado de Emergência foi decretado[11]. O anúncio deste estado de exceção indica que a situação "que se vive e a proliferação de casos registados de contágio de COVID-19 exige a aplicação de medidas extraordinárias e de caráter urgente". Uma das medidas indica, de forma sucinta, que todos as ocupações que possam ser feitas em trabalho remoto, ou teletrabalho, o devem ser feitos.

Nas duas semanas que antecederam o decreto do Estado de Emergência, várias empresas começaram a colocar os seus colaboradores em casa. Alguns colocaram todos os seus colaboradores a trabalhar a partir de casa; outros apenas uma parte para diminuir o risco de contágio na empresa. Certo é que, a partir de 18 de março, a larga maioria dos colaboradores passou a fazer o seu trabalho a partir de sua casa.

Passando de uma situação em que a força de trabalho estava localizada, na sua maioria, no perímetro restrito das instalações da organização para a situação oposta em que a maioria se encontra num ambiente de trabalho remoto.

Este contexto criou uma pressão extra nas áreas de cibersegurança.

O conceito de vírus informático surgiu pela primeira vez referido em 1984 num artigo de Fred Cohen[12]. O isolamento ou a menor conectividade possível dos sistemas informáticos ao mundo era a medida mais adequada para combater essa nova ameaça de infeção de vírus informático. Coincidentemente aquilo que resultava em 1984, e de certa forma ainda hoje, para segurança informática é também a medida recomendada, e imposta, no combate à pandemia do Covid19.

Aqui surge o desafio, no combate às ameaças biológica e informática, enquanto para uma boa proteção de ciber ataques a melhor forma é trabalhar a partir de infraestruturas com arquiteturas de segurança robustas, para uma boa proteção em relação ao Covid-19 o melhor é ficar em casa utilizando os equipamentos informáticos e as redes de comunicação pessoais para uso profissional. O Covid-19 fez com que milhões de

11 https://www.presidencia.pt/?idc=22&idi=176060
12 Herb Lin, 2020. Cybersecurity Lessons from the Pandemic

pessoas passassem a aceder às redes e servidores das suas empresas e organizações a partir de casa e através de redes com níveis de segurança inferiores.

Como publicado no boletim de maio de 2020 do Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS), entre fevereiro e março de 2020, o número de incidentes registados pelo CERT.PT – serviço que coordena a resposta a incidentes de cibersegurança no ciberespaço de interesse nacional – aumentou 84% e, em comparação com o número de incidentes registados em março de 2019, o aumento foi de 176%[13].

Citando Dorit Dor, Vice Presidente da *Products at Check Point Software Technologies*:

> "*A pandemia COVID-19 descarrilou a atividade normal de praticamente todas as organizações, obrigando-as a pôr de lado os planos estratégicos de negócio que tinham já delineado e a adotar rapidamente medidas que garantam a conectividade remota em larga escala para a sua força de trabalho*."

> "*Uma das poucas coisas previsíveis sobre a cibersegurança é que os agentes maliciosos procurarão sempre tirar proveito próprio de grandes eventos ou mudanças – como a COVID-19 ou a introdução do 5G*."

Um dos grandes desafios que as organizações atualmente enfrentam passa por encontrar formas de conciliar o trabalho remoto dos seus colaboradores com a segurança dos dados críticos, mais expostos a riscos online devido à dispersão geográfica de quem está em modo de teletrabalho.

Com a movimentação de centenas de milhar de trabalhadores para as suas casas moveu-se também o perímetro de segurança da respetiva empresa. E se tivermos em conta que estas alterações serão o novo normal, podemos inferir que os dados críticos das organizações estão significativamente mais expostos a ciberataques.

13 https://www.cncs.gov.pt/content/files/boletim_observatorio_maio2020.pdf

A solução passa, claro, pela adoção de soluções de segurança que protejam as infraestruturas, o software e a informação. Mas é hoje necessário olhar para estes riscos de uma forma transversal, através de sistemas de monitorização fiáveis, sistemáticos e que forneçam recomendações para uma atuação proativa de mitigação desses mesmos riscos.

Além disso, é essencial não limitar os utilizadores naquilo que é a sua ação normal de trabalho, disponibilizando em paralelo as ferramentas adequadas para o acesso aos sistemas e aos dados e assegurando sempre a proteção devida – sejam propriedade intelectual ou dados ao abrigo do RGPD.

6. Mudança do Perímetro de Defesa

Segundo Joseph Boyce, numa perspetiva de Segurança da Informação os serviços e mecanismos de segurança devem abranger um vasto campo de equipamentos de TI da organização. A diversidade é a base duma estratégia de Defesa em Profundidade. Essa diversidade pode ser alcançada com a implementação de serviços e mecanismos de segurança em estações de trabalho, as chamadas workstations, desktops, laptops, como em servidores, routers, firewalls, como apenas alguns exemplos.

"*Organizational computing environment boundary protection*"[14]. Estações de trabalho e servidores localizados nas instalações da organização têm de ser protegidos tanto de ameaças internas como externas à organização e suas instalações. Assim os referidos equipamentos deverão ter implementados serviços e mecanismos de segurança tais como autenticação e controlo de acessos.

14 Boyce, Joseph. *Information Assurance: Managing organizational IT Security Risks.* s.d.

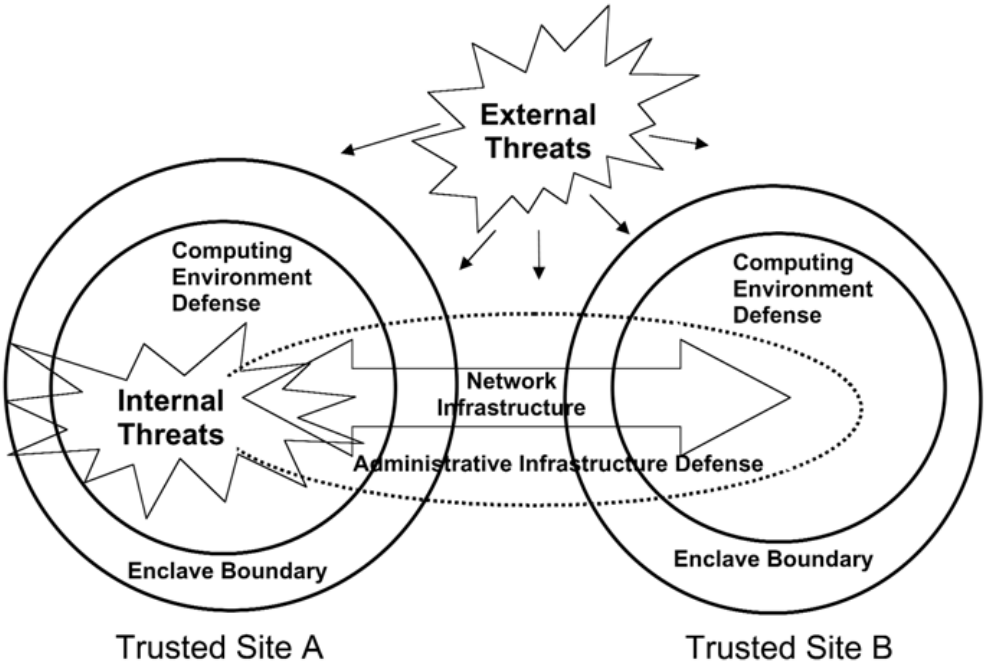


Figura 3[15]

Embora aqui neste ponto Joseph Boyce refira apenas equipamentos localizados nas instalações da organização, já no capítulo 3 refere as fronteiras físicas e virtuais numa organização.

Neste mesmo capítulo define também o conceito de ambiente de computação como tudo o que trabalha com qualquer ou todos os ativos do sistema de informação do enclave, enclave que define como uma área fisicamente protegida dentro da organização, no entanto adiciona que neste enclave pode incluir-se também um laptop com uma sessão remota a partir dum hotel por parte dum funcionário em viagem. Nesta altura ainda não existia esta realidade de trabalho remoto massivo.

Mudando para um trabalho remoto, em casa, mudou-se assim também o perímetro de defesa ou perímetro de segurança da respetiva empresa.

Esta mudança do perímetro de defesa coloca os seguintes desafios nas áreas de cibersegurança:

15 Boyce, Joseph. *Information Assurance: Managing organizational IT Security Risks.* s.d.

• Explosão "BYOD – *Bring your own device*" – Muitos colaboradores não tinham dispositivos (ex.: *laptops* ou *smartphones*) atribuídos pela empresa para uso *off-site* no momento do confinamento.

• Ambiente de computação remoto – As organizações não têm controlo sobre o ambiente de computação remoto dos seus colaboradores.

• Acesso remoto seguro – A maioria das empresas simplesmente não estava pronta para um mundo onde a maioria dos colaboradores não tem acesso remoto seguro às aplicações corporativas.

• A ameaça interna – Os ambientes de competitividade económica continuarão a contribuir para um aumento no volume de ameaças internas.

• Processos "*ad hoc*" inseguros – Foram executados processos de desenvolvimento rápidos para suportar esta nova realidade, ou mesmo para aumentar o volume de negócios em canais digitais, que infelizmente num número significativo de organizações, eventualmente devido à urgência, não passaram por nenhuma validação da área de cibersegurança.

Todos estes desafios têm implícitos uma panóplia de riscos que não sendo novos na sua maioria, são, no entanto, exacerbados pela procura crescente de soluções de trabalho remoto e pela necessidade das organizações em concretizar uma rápida transformação digital de modo a fazer face a esta nova realidade de trabalho remoto massivo.

7. Como será o novo normal?

Em resultado da análise duma plêiade de estudos constata-se que todos convergem para uma conclusão: O trabalho remoto vai manter-se e vai intensificar-se[16][17][18].

No entender dos investigadores da *Check Point*, os efeitos causados pelas mudanças introduzidas pela pandemia COVID-19 continuarão a ser o foco das equipas de TI e de segurança das organizações. Um estudo recente da Gartner estima que 81% das empresas adotaram massivamente o trabalho remoto, sendo que 74% pondera esta opção permanentemente[19].

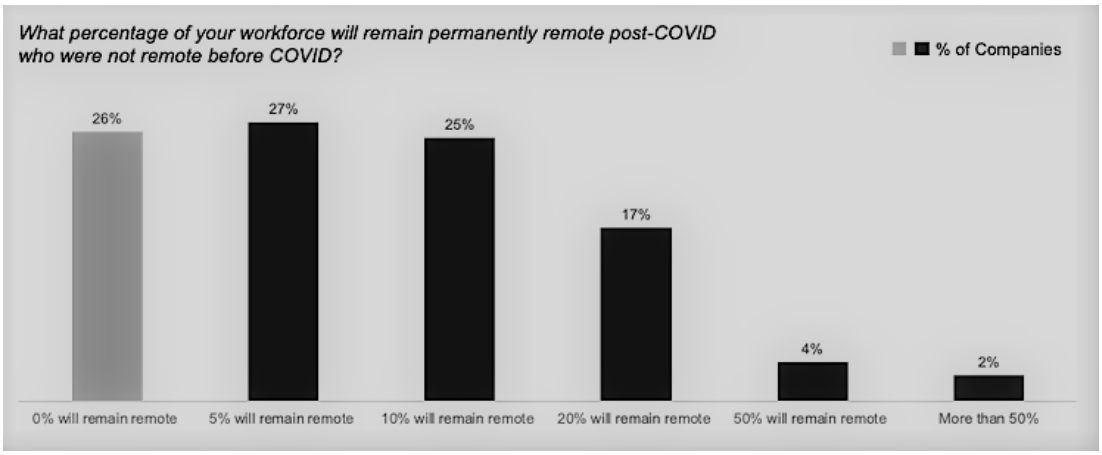


Figura 4 [20]

A *Check Point* alerta ainda para as repercussões que a emergência de ataques ransomware e de botnets terá no que respeita a capacidade das empresas de proteger as redes 5G e a crescente conetividade entre dispositivos.

Como foi apresentado anteriormente, tanto a explosão de BYOD como o desconhecido ambiente de computação remoto dos seus colaboradores são dos principais

16 EU Science Hub JRC: jrc120945_policy_brief_-_covid_and_telework_final.pdf
17 https://blog.sage.hr/post-covid-future-of-work-trends/
18 https://businessfacilities.com/2020/06/even-after-covid-19-execs-expect-remote-work-trend-to-continue/
19 https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2
20 https://emtemp.gcom.cloud/ngw/globalassets/en/newsroom/images/graphs/cohotrm.png

desafios das áreas de cibersegurança para este novo normal de permanência de trabalho remoto.

Assim identificam-se como fundamentais os seguintes 3 processos para assegurar a adequação das organizações ao novo cenário de trabalho remoto massificado:

- Garantir que as equipas de Tecnologias de Informação implementam as políticas e diretrizes de segurança corporativa para os "BYOD – *Bring your own device"*.
- Rever e adequar as regras de firewalls corporativas para acesso remoto, monitorizar e analisar os Comportamentos de Utilizadores e Entidades (UEBA- *User and Entity Behavior Analytics*).
- Restringir o acesso à rede corporativa apenas a equipamentos pessoais aprovados.

As abordagens atrás mencionadas irão impulsionar o interesse renovado em tecnologias que permitam acesso remoto seguro. Das tecnologias disponíveis atualmente algumas já existiam há bastante tempo, mas tiveram, no entanto, fraca adesão no passado devido a questões de complexidade e custo de implementação, agora, devido à crescente evolução para *Cloud* estão assim novamente com grande potencial de utilização no sentido de contribuir para as abordagens referidas anteriormente.

Destacam-se[21]:

• "VDI – *Virtual Desktop Infrastructure*" e "DaaS – *Desktop as a Service*":

• "IAM – *Identity and Access Management*";

• *Cloud computing*.

21 https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-covid-19-cyber-and-the-remote-workforce.pdf

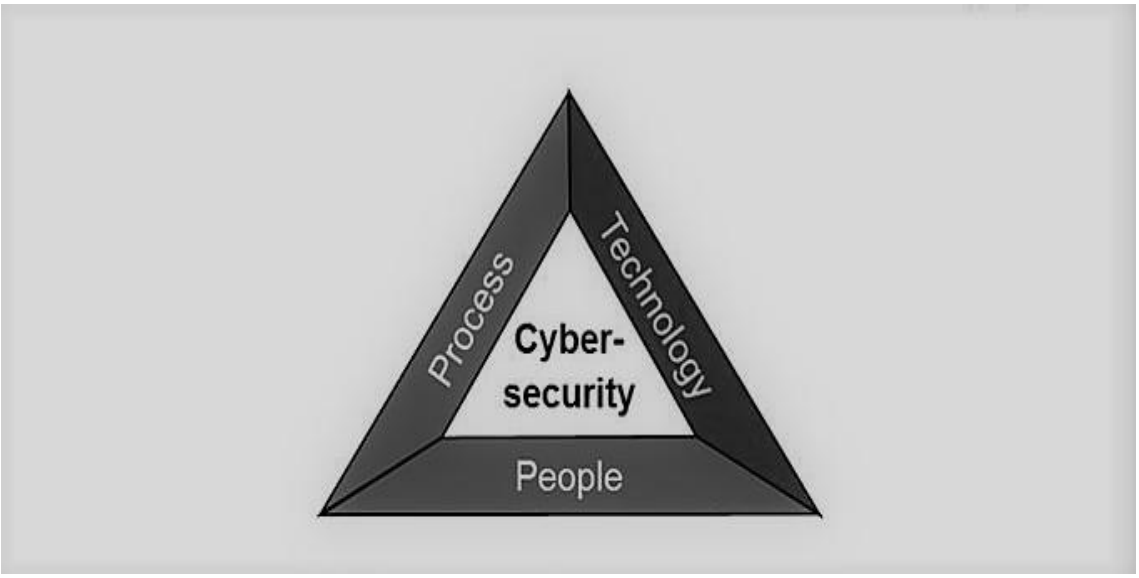
Conclusões

As organizações da área das TI, algumas já referidas como "*cloud-native*", tinham em geral já estabelecidos a maioria dos processos e tecnologias necessários para o trabalho remoto. Neste caso a mudança para um trabalho remoto massificado pode ser encarado como mais um passo ou apenas uma evolução nesse processo. As organizações com mais dificuldades são as que ainda têm de evoluir no seu grau de maturidade na Segurança da Informação.

Segundo um estudo da *EU Science HUB*[22], em vários países da União Europeia mais de metade das pessoas atualmente em trabalho remoto nunca tinham tido essa experiência anteriormente.

O desempenho e sucesso das organizações no geral e também neste tema da Segurança da Informação em particular tem como base a articulação da tríade: Pessoas, Processos, Tecnologias.

Figura 5



22 EU Science Hub JRC: jrc120945_policy_brief_-_covid_and_telework_final.pdf

Então, que devem as organizações, e seus colaboradores, fazer para a proteção da sua informação e dados críticos?

Da análise dos vários estudos[23] [24] [25] [26] e das muitas recomendações analisadas sintetizaram-se as similares e agregaram-se nas 3 vertentes de processos, tecnologias e pessoas.

Portanto muito resumidamente teremos:

Processos

• Assumir que as ameaças vão existir

• Definir uma política para o trabalho remoto

• Encriptar Informação/Dados críticos

Tecnologias

• Especificar a lista de equipamentos de trabalho remoto e implementar as respetivas medidas de segurança

• Usar autenticação, controlos e privilégios de acesso apropriados para cada utilizador

• Usar uma VPN

23 https://www.cmswire.com/information-management/6-ways-to-keep-employer-data-secure-when-working-remotely/
24 https://techbeacon.com/security/pandemic-your-remote-workforce-9-ways-stay-secure
25 https://www.cybereason.com/blog/cyber-security-tips-for-allowing-employees-to-work-from-home
26 https://memory.ai/timely-blog/cyber-security-for-remote-workers

Pessoas

• Fomentar a sensibilização (*awareness*) dos funcionários para o problema da segurança da informação.

• Aumentar também o conhecimento técnico dos funcionários em relação a esta mesma problemática da segurança da informação.

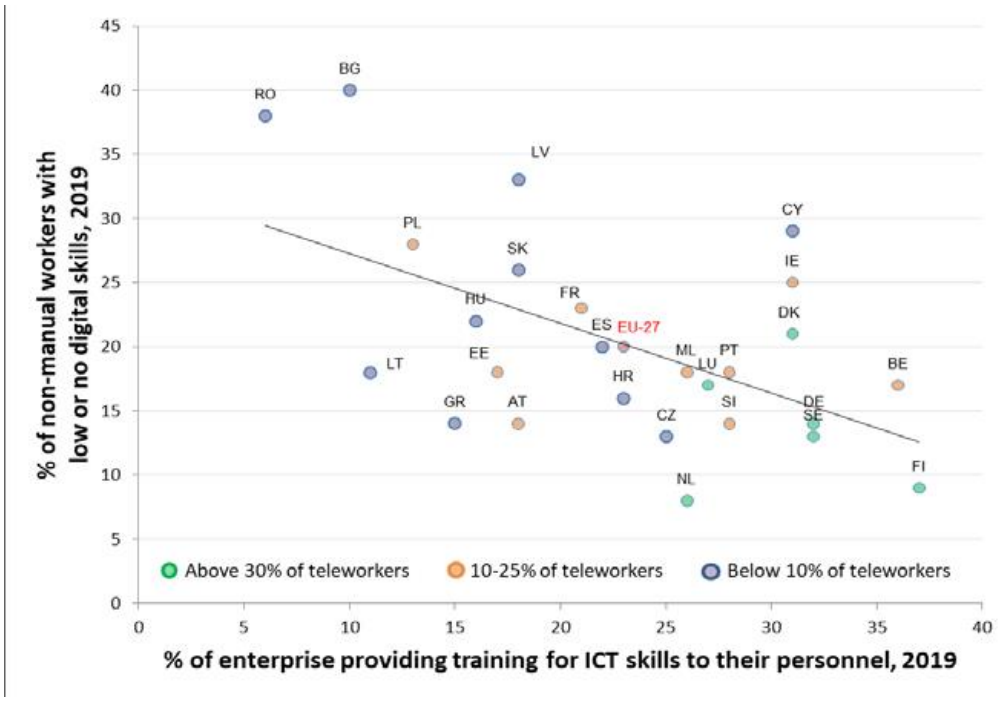
Ou seja: Treinar, treinar, treinar. Sensibilizar, sensibilizar, sensibilizar.

As tecnologias existem, evoluirão muitas das atuais, surgirão novas e desaparecerão algumas. Os processos também já existiam, e evoluirão também tal como as tecnologias.

São as pessoas o elo mais fraco nesta tríade.

Neste gráfico apresentado abaixo, do mesmo estudo da EU Science HUB JRC[27] já referido também anteriormente, constatam-se as diferenças entre competências digitais e formação providenciada pelas empresas nos diferentes estados-membro e consoante as diferentes políticas de trabalho.

Figura 6 [28]



27 EU Science Hub JRC: jrc120945_policy_brief_-_covid_and_telework_final.pdf
28 Figure 11: Digital skills, ICT training and telework: jrc120945_policy_brief_-_covid_and_telework_final.pdf.

Neste gráfico temos como média da EU-27 que 20% dos colaboradores (em trabalho não manual) têm nenhumas ou baixas competências digitais e menos de 25% das empresas providenciam formação em competências digitais.

Nota-se também a influência positiva das empresas com mais de 30% dos colaboradores em trabalho remoto, todas no quadrante inferior direito do gráfico, em contraste com a situação inversa das empresas com menos de 10% dos colaboradores em trabalho remoto, mais no quadrante superior esquerdo do gráfico.

Assim, esta crise provocada pela pandemia do Covid-19 com as consequentes restrições impostas sendo uma delas o trabalho remoto massivo forçado, deve ser aproveitada no sentido da transformação digital que foi forçada também em muitas das empresas e acelerada noutras que já a tinham em curso ser, entretanto, agora com o devido tempo e ponderação, analisada e aperfeiçoada.

Essa análise e aperfeiçoamento deve incidir não só nos processos e tecnologias como também nas pessoas. Será mais difícil ter uma transformação digital bem-sucedida e também uma Segurança da Informação bem implementada sem as respetivas competências nas pessoas.

Parafraseando Winston Churchill: "*Never let a good crisis go to waste*".

Bibliografia

Boyce, Joseph. *Information Assurance: Managing organizational IT Security Risks.* s.d.

Caldas, Alexandre, e Vicente Freire. "Cibersegurança: das preocupações à ação - IDN Instituto da Defesa Nacional." s.d.

check-point-softwares-cyber-security-predictions-for-2021. s.d. https://www.checkpoint.com/press/2020/check-point-softwares-cyber-security-predictions-for-2021-securing-the-next-normal/.

"Ciberseguranca eciberdefesaemtemposdepandemia_IDNBrief_N_32_Julho_2020." s.d.

cmswire. *6-ways-to-keep-employer-data-secure-when-working-remotely.* s.d. https://www.cmswire.com/information-management/6-ways-to-keep-employer-data-secure-when-working-remotely/.

CNCS. *boletim_observatorio_maio2020.* s.d. https://www.cncs.gov.pt/content/files/boletim_observatorio_maio2020.pdf.

—. *Cibersegurança, Glossário.* s.d. https://www.cncs.gov.pt/recursos/glossario/.

CNSS. *CNSS.* s.d. https://www.cnss.gov/.

cybereason. *cyber-security-tips-for-allowing-employees-to-work-from-home.* s.d. https://www.cybereason.com/blog/cyber-security-tips-for-allowing-employees-to-work-from-home.

Deloitte. "gx-covid-19-cyber-and-the-remote-workforce." s.d. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-covid-19-cyber-and-the-remote-workforce.pdf.

ENISA. *ENISA.* s.d. https://www.enisa.europa.eu/.

Facilities, Business. *Business Facilities - Surveys & Research.* s.d. https://businessfacilities.com/2020/06/even-after-covid-19-execs-expect-remote-work-trend-to-continue/.

Gartner. *Gartner press-releases.* s.d. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2.

ISACA. *ISACA.* s.d. https://www.isaca.org/.

ISO. *ISO.* s.d. https://www.iso.org/news/ref2266.html.

—. *ISO 27001 pt.* s.d. https://www.27001.pt/.

JRC, EU Science Hub. "Telework in the EU before and after the COVID-19: where we were, where we head to." *European Commission > EU Science Hub.* s.d. https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf.

Lin, Herb. *Cybersecurity Lessons from the Pandemic.* s.d. https://www.lawfareblog.com/cybersecurity-lessons-pandemic-or-pandemic-lessons-cybersecurity.

memory.ai. *cyber-security-for-remote-workers.* s.d. https://memory.ai/timely-blog/cyber-security-for-remote-workers.

NIST. *NIST CSF.* s.d. https://www.nist.gov/cyberframework.

post-covid-future-of-work-trends. s.d. https://blog.sage.hr/post-covid-future-of-work-trends/.

Presidencia. *Presidencia.* s.d. https://www.presidencia.pt/?idc=22&idi=176060.

techbeacon. *pandemic-your-remote-workforce-9-ways-stay-secure.* s.d. https://techbeacon.com/security/pandemic-your-remote-workforce-9-ways-stay-secure.