LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO

GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

DISSERTAÇÃO

O FATOR HUMANO DA CIBERSEGURANÇA NAS ORGANIZAÇÕES

RITA SANTOS GONÇALVES

OUTUBRO – 2019

LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO EM
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
DISSERTAÇÃO

O FATOR HUMANO DA CIBERSEGURANÇA NAS ORGANIZAÇÕES

RITA SANTOS GONÇALVES

ORIENTAÇÃO:

PROFESSOR DOUTOR SÉRGIO NUNES

OUTUBRO - 2019

"Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain."

Kevin Mitnick

AGRADECIMENTOS

Foram muitas as pessoas que, direta ou indiretamente, tornaram este trabalho possível. A todos eles, o meu muito obrigada.

A todos os Professores que fizeram parte do meu percurso académico, em especial aos que me acompanharam nestes últimos dois anos, pelo conhecimento, rigor e excelência que transmitiram e exigiram diariamente.

Ao Professor Nuno Reis, deixo o meu muito obrigado pelos sinceros conselhos e por me incentivar a prosseguir os meus estudos.

Ao meu orientador, Professor Sérgio Nunes, por estar sempre disponível a colaborar neste trabalho e pelos sábios conselhos.

A todos os entrevistados, que trabalham diariamente para o sucesso da cibersegurança, o meu muito obrigada por toda a disponibilidade, simpatia e interesse em colaborar.

Aos meus pais, por me darem esta possibilidade de poder continuar a estudar, por me transmitirem todos os valores essenciais para poder ser uma pessoa melhor e melhor profissional, pelo seu esforço, dedicação, apoio e por acreditaram sempre em mim.

Ao Micael, por todo o carinho, apoio, compreensão e motivação.

À Ana, à Cátia, ao Hugo, à Mariana, ao Patrick, ao Pedro, ao Rui, à Sandra e à Sofia, pela vossa amizade, por todos os trabalhos de grupo e por tudo o que pude aprender com cada um de vocês.

À Joana e à Mariana, pela sua amizade e por estarem sempre presentes, ainda que longe.

RESUMO

Numa realidade onde a evolução tecnológica é exponencial e a sociedade demonstra estar cada vez mais dependente da tecnologia, as pessoas revelam que não estão suficientemente preparadas para toda esta evolução, pelo que não se sabem proteger da realidade associada ao crescente número de ciberataques e da sua sofisticação. Desta forma, as pessoas representam uma das maiores vulnerabilidades da cibersegurança das organizações, pelo que são o principal alvo dos ciberataques. Nesse sentido, as organizações devem estar cada vez mais atentas à sua importância na cibersegurança, assegurando que os seus colaboradores estão suficientemente sensibilizados e que têm o conhecimento necessário nesta área. Assim, de forma a tornarem-se mais resilientes, as organizações devem procurar construir uma cultura de cibersegurança sólida, onde as preocupações com a cibersegurança passam a ser parte integrante do quotidiano de todos as pessoas.

Deste modo, esta dissertação estuda a influência que o fator humano tem na cibersegurança das organizações, através da identificação das características e comportamentos humanos que influenciam a cibersegurança, do seu impacto nos níveis de cibersegurança alcançados e das respetivas soluções para estes comportamentos. Para isso, foram realizadas entrevistas individuais a peritos e investigadores em cibersegurança, que permitiram concluir que as pessoas têm realmente uma grande influência e, consequentemente, importância, na cibersegurança das organizações.

Palavras-chave: Cibersegurança, Fator Humano, Organizações, Cultura de Cibersegurança, Consciencialização em Cibersegurança

ABSTRACT

In a reality where technological evolution is exponential and society is increasingly dependent on technology, people reveal that they are not sufficiently prepared for this constant evolution, so they can't protect themselves from the increasing number of cyber attacks and their sophistication. Therefore, people represents one of the biggest vulnerabilities of organizations, making it the main target of cyber attacks. In this way, organizations must be increasingly aware of the importance of people in cybersecurity, ensuring that their employees are sufficiently aware and have the necessary knowledge in this area. Thus, organizations should seek to build a solid cybersecurity culture where concerns with the subject become an integral part of everyone's daily lives and, as a result, organizations will become more resilient.

Having this in mind, this dissertation studies the influence that the human factor have on the cybersecurity's organizations, by identifying the human behaviors and characteristics that influence cybersecurity, its impact on the cybersecurity levels achieved and the respective solutions for these behaviors. To achieve this, individual interviews were conducted with cybersecurity experts and researchers, which led to the conclusion that people really have a major influence and, consequently, importance on the cybersecurity's organizations.

Keywords: Cybersecurity, Human Factor, Organizations, Cybersecurity Culture, Cybersecurity Awareness

ÍNDICE

LISTA DE SIGLAS E ACRÓNIMOS

AP2SI – Associação Portuguesa para a Promoção da Segurança da Informação

CERT – *Computer Emergency Response Team*

CNCS – Centro Nacional de Cibersegurança

ENISA – *European Network and Information Security Agency*

IT – Tecnologia da Informação

PME – Pequenas e Médias Empresas

1. INTRODUÇÃO

Neste capítulo, é apresentado um brevemente enquadramento do tema em estudo. Para além disso, o objetivo principal desta dissertação é identificado, assim como a sua respetiva relevância.

1.1.Enquadramento

Se recuarmos na história da humanidade, sempre existiram pessoas bem e mal-intencionadas. No passado, um castelo era construído para proteger o reino dos ataques oriundos de outros povos, que tentavam alargar o seu território. O objetivo dos soldados atacantes era conseguir passar as muralhas do castelo. Atualmente, as barreiras deixaram de ser físicas para passarem a ser virtuais. *Hackers* denominados de *black hats*[1], tentam, com frequência, aceder a dados de terceiros que, por sua vez, estão protegidos por barreiras não físicas, como as *firewalls*[2] (Gaspar, 2018). Estas barreiras não físicas acabam por trazer novas vulnerabilidades[3] e, consequentemente, novos desafios à humanidade (Leite, 2016).

Fazendo mais um paralelismo, é, aos olhos da sociedade, injustificável sair de casa sem trancar a porta. Com este gesto, as pessoas asseguram, de certa forma, que ninguém entrará dentro da sua casa, nem terá acesso aos seus bens pessoais. Por outro lado, a sociedade não tem a mesma preocupação relativamente aos seus dados, quando relacionados com o ciberespaço[4]. São vários os que reconhecem a necessidade de cibersegurança, mas são poucos aqueles que tomam efetivamente as medidas corretas. Ou seja, muitos reconhecem que se deve trancar a porta, mas a maioria deixa-a aberta. Ora, um *hacker* é um indivíduo que, de forma figurada, vai de porta em porta ver qual

[1] *Black hat*- pessoa que explora as falhas de segurança de um sistema de forma ilegal e com intenção maliciosa (CNCS, s.d.; Rouse, 2017).

[2] *Firewall*- recurso de hardware ou software que limita o acesso entre redes e/ou sistemas de modo a protegê-los do acesso de utilizadores não autorizados (CNCS, s.d.; CNSS, 2015).

[3] Vulnerabilidade- fraqueza que é passível de ser explorada por uma ou mais ameaças (CNCS, s.d.).

[4] Ciberespaço- espaço não físico constituído por uma rede interdependente de infraestruturas de tecnologias da informação, onde se inclui a *internet*, que permite diferentes modos de comunicação entre as pessoas (CNCS, s.d.; CNSS, 2015).

tem uma pequena abertura que o permita entrar. Seguindo o mesmo raciocínio, se não trancarmos a porta, torna-se inútil comprar a melhor fechadura do mercado, assim como não adianta ter a melhor tecnologia para a cibersegurança se as pessoas não tiverem a consciência de que devem "trancar a porta" aos *black hats* (Strawser & Joy, 2015).

Associado a essa ideia, em muitos casos, a cibersegurança é desvalorizada da mesma forma que são desvalorizadas questões de saúde. Ou seja, nada é feito enquanto nada der errado. Nesse sentido, apenas quando surgir um alerta de que existe um problema, a preocupação aumenta exponencialmente. Este tipo de abordagem representa ausência de prevenção, o que exige um esforço muito maior no processo de recuperação das consequências do ciberataque (Siponen, 2001).

1.2. Objetivo principal de estudo e questões de investigação

A cibersegurança não deve ser vista de forma individualizada, mas sim como um conjunto de sinergias entre os três fatores estruturais da organização: pessoas, processos e tecnologia (Raposo (2016) baseado em McCumber (2004)). Nesse sentido, a tecnologia só consegue proteger eficazmente uma organização se as pessoas tiverem conhecimento, competências, compreensão e aceitação necessários relativamente à tecnologia e à cibersegurança. Deste modo, uma organização pode ter à sua disposição os melhores recursos tecnológicos para se defender de ciberataques, mas basta uma das pessoas dessa mesma organização não seguir as diretrizes e os processos estabelecidos para que exista uma falha de cibersegurança, comprometendo toda a organização. (ENISA, 2017)

Desta forma, o fator humano é uma das maiores preocupações das organizações pois é indicado como o elo mais fraco no contexto da cibersegurança organizacional, por ser um alvo fácil de atingir pelos cibercriminosos e, por isso, a vítima mais comum dos ciberataques (Hadlington, 2017; Henshel et al., 2015; Mitnick & Simon, 2003; Ponemon Institute, 2016). Numa primeira análise, esta afirmação pode ser justificada com a negligência das pessoas em relação à cibersegurança, decorrente da sua falta de conhecimento e de algumas características intrínsecas ao ser humano (Hadlington, 2017; Ponemon Institute, 2012a).

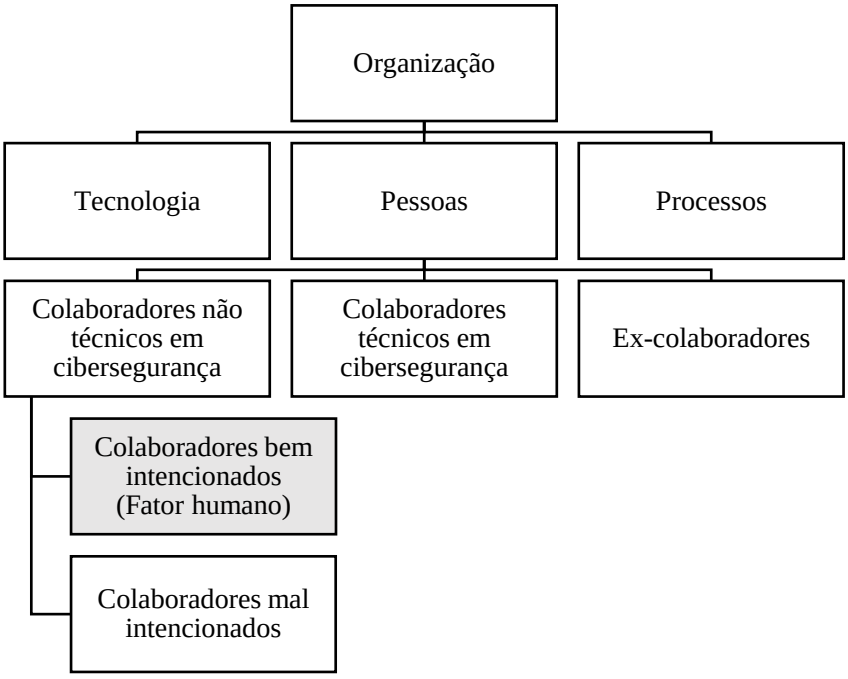

Figura 1- O fator humano na organização

Fonte: elaboração própria com base em CA Technologies (2018), CERT, (2013), Hadlington (2018), Ponemon Institute (2012a) e Raposo (2016) baseado em McCumber (2004).

Dos três fatores estruturais da organização mencionados, o foco deste trabalho é direcionado para o fator "pessoas", mais concretamente para o "fator humano", ou seja, as atenções são incididas nos colaboradores que não são especializados em cibersegurança e que, simultaneamente, agem com boas intenções. Para além disso, este trabalho foca-se no estudo do fator humano no contexto organizacional, sendo que não são feitas distinções entre tipos de organizações. Deste modo são consideradas organizações públicas e privadas, com e sem fins lucrativos e de grandes e pequenas dimensões. Esta escolha deve-se ao facto de todas elas terem pessoas inerentes à sua constituição e de todas serem consideradas potenciais alvos de ataque dos cibercriminosos (Proofprint, 2019).

Assim, o termo fator humano representa todos os colaboradores que não têm intenção maliciosa de prejudicar a organização e a sua cibersegurança, contudo acabam

por colocá-la em risco[5], ainda que de forma acidental. As consequências com origem no fator humano podem ser igualmente prejudiciais para a organização, quando comparadas com as consequências provocadas pelos colaboradores que prejudicam a organização de forma deliberada e planeada. O termo fator humano é muitas vezes associado à falta de conhecimento, planeamento deficiente, falta de atenção, distração e ignorância das pessoas (Hadlington, 2018). Em suma, associa-se o termo fator humano aos colaboradores que, por ação ou inação, causam danos (ou aumenta a sua probabilidade) na confidencialidade[6], integridade[7] ou disponibilidade[8] dos sistemas de informação da organização, de forma não intencional (CERT, 2013).

Desta forma, o objetivo principal deste trabalho é compreender qual a influência e importância do fator humano na cibersegurança das organizações, através da identificação dos comportamentos e características humanos que influenciam a cibersegurança, do seu impacto nos níveis de cibersegurança alcançados e das soluções que permitem corrigir estas situações. De modo a atingir este objetivo principal definido, três questões de investigação foram estabelecidas:

- Q1: Quais os comportamentos e características humanos que influenciam a cibersegurança nas organizações?
- Q2: Quais as consequências dos comportamentos humanos nos níveis de cibersegurança alcançados nas organizações?
- Q3: Quais as soluções para corrigir os comportamentos humanos que influenciam a cibersegurança nas organizações?

Pretende-se ainda que o presente trabalho tenha um contributo prático. Deste modo, espera-se que esta dissertação sensibilize as pessoas, de forma a compreenderem a importância da cibersegurança, e que as leve a substituir comportamentos errados por

[5] Risco- resulta da combinação entre a probabilidade de uma determinada ameaça explorar as vulnerabilidades de uma organização e o respetivo impacto nessa mesma organização (CNCS, s.d.).

[6] Confidencialidade- propriedade da informação de não ser divulgada a entidades não autorizadas ou através de processos não autorizados (CNCS, 2019).

[7] Integridade- propriedade de salvaguardar o carácter exato e completo da informação (CNCS, 2019).

[8] Disponibilidade- propriedade de estar acessível e de poder ser utilizada por uma autoridade autorizada (CNCS, 2019).

boas práticas, contribuindo para a cibersegurança da sociedade no geral. Neste sentido, esta dissertação destina-se a todas as pessoas, independentemente do seu nível de conhecimento relativamente a este tema, procurando utilizar terminologias acessíveis a todos, acompanhadas de definições e explicações associadas a esta temática ao longo de todo o corpo do trabalho.

1.3.Relevância do estudo

A relevância teórica e empresarial deste estudo será justificada por algumas tendências verificadas a nível mundial. Estas demonstram a importância da cibersegurança e do fator humano nas organizações.

Em primeiro lugar, os ciberataques têm aumentado tanto em número como em sofisticação ao longo dos últimos anos, pelo que já não podem ser vistos como uma exceção, mas sim como uma realidade. Desde universidades, a entidades governamentais, passando por empresas com diversas outras áreas de atuação e de diversos setores de atividade, são várias as organizações de dimensão mundial que foram vítimas do cibercrime nos últimos anos. Tanto o WannaCry como o NotPetya, são dois exemplos de grandes ciberataques dos últimos anos, tanto em escala como em complexidade. (Morgan, 2017). Deste modo, a atenção deve ser redobrada pois os ciberataques podem ter diversas origens, desde organizações criminosas, *hackers* que atuam por conta própria ou até mesmo organizações concorrentes, pelo que todas as hipóteses devem ser consideradas (Winnefeld et al., 2015).

Segundo um relatório da Cybersecurity Ventures, o cibercrime é um dos maiores desafios que a humanidade enfrentará nas próximas duas décadas. Está previsto que irá custar, a nível mundial, 6 triliões de dólares por ano até 2021. Importa salientar ainda que o cibercrime representa um conceito complexo e que, por isso mesmo, não se refere apenas ao roubo de dados, mas também contabiliza a destruição dos mesmos, roubo de propriedade intelectual, roubos financeiros, perdas de produtividade, investigação forense, danos reputacionais, restauração de dados e restauração de sistemas invadidos. (Morgan, 2017)

Ainda no mesmo relatório, pode-se concluir que o número de utilizadores da *internet* tem vindo a aumentar ao longo dos anos. Atualmente, representa mais de metade

da população mundial e, em 2022, espera-se que represente 75% da população. Prevê-se ainda que em 2030 os utilizadores da *internet* correspondam a 90% da população mundial. Com este crescimento tão acentuado, as preocupações relativamente à cibersegurança aumentam pois aumenta o número de atacantes e de vítimas do cibercrime. (Morgan, 2017)

Para além disso, a tecnologia está cada vez mais presente no quotidiano das pessoas, e cada vez mais desenvolvida (Morgan, 2017). Ganhos de produtividade, comodidade e novas formas de comunicação e prestação de serviços, são alguns dos benefícios associados à tecnologia (Prodemge, 2017). A utilização de dispositivos móveis como ferramentas de trabalho, o acesso a redes sociais através da rede interna das organizações e a utilização de recursos *cloud*[9], são realidades que já fazem parte da atualidade no contexto organizacional e que devem ser tidas em consideração (Ponemon Institute, 2012a). Para além disso, a disseminação da tecnologia resulta ainda num aumento do volume de dados em circulação no ciberespaço, associado a conceitos como *big data*[10] e *internet of things*[11] (EY, 2018; Morgan, 2017). Esta grande dependência da sociedade pela tecnologia representa uma grande vulnerabilidade, pelo que já é uma das grandes prioridades das organizações (Winnefeld et al., 2015).

2. REVISÃO DA LITERATURA

No presente capítulo, são apresentadas as respostas da literatura às questões de investigação definidas. Desta forma, são identificados os comportamentos e características humanos que influenciam a cibersegurança nas organizações, o seu

[9] *Cloud*- rede vasta de servidores remotos conectados que funcionam como um ecossistema, em que a sua função é armazenar e gerir dados, executar aplicações e fornecer conteúdos ou serviços. Devido a estas características, permitem aceder a conteúdos *online* a partir de qualquer dispositivo, estando as informações disponíveis em qualquer lugar e momento (Microsoft, s.d.).

[10] *Big data*- grande volume de dados, de variadas tipologias, que são coletados a uma elevada velocidade (Hoffer et al., 2016).

[11] *Internet of things*- redes de objetos físicos que incorporam tecnologia que os permite comunicar, serem detetados e interagirem entre eles e com o ambiente externo (Gartner, s.d.).

respetivo impacto nos níveis de cibersegurança alcançados e as correspondentes soluções que visam corrigir os comportamentos apresentados.

2.1.Cibersegurança

Em primeiro lugar, importa perceber o que é a cibersegurança. Ao fragmentar a esta palavra, pode-se obter duas outras: "ciber[12]", associado ao conceito de ciberespaço, e segurança (Craigen et al., 2014).

O conceito de ciberespaço pode ser explicado como sendo uma "rede global de infraestruturas de tecnologias de informação interligadas entre si" (Fernandes, 2012), onde existe uma troca constante de dados e informações, pelo que é extremamente dinâmico (Craigen et al., 2014). De forma mais informal e generalizada, o termo ciberespaço faz referência a algo que está ligado à *internet* direta ou indiretamente (Fernandes, 2012). Para Santos (2018), baseado em Riek, et al. (2016), o ciberespaço apresenta características intrínsecas como o anonimato, a escalabilidade e a inexistência de fronteiras. Estas fazem com que seja um espaço mais propício ao crime, quando comparado com os ambientes tradicionais, o que faz com que a criminalidade *online* registe um crescimento ao longo dos anos. Para além disso, por ser de fácil acesso e mais lucrativo, os cibercriminosos conseguem atingir elevados ganhos e baixas penalizações (Santos, 2018).

Por outro lado, segurança é um termo muito abrangente e pode ser aplicado a diversas áreas. De forma generalizada, segurança é um conceito que refere a ausência de perigo ou ameaças[13] (Craigen et al., 2014).

Em suma, são várias as definições para cibersegurança pelo que, de forma muito generalizada, caracteriza-se por ser a capacidade de proteger ou defender a utilização do ciberespaço dos ciberataques[14] (CNSS, 2015). Aprofundando um pouco mais o conceito,

[12] Ciber- relativo às tecnologias da informação (CNCS, s.d.).

[13] Ameaça- circunstância ou evento com potencial para causar um ou mais incidentes indesejáveis, que pode resultar em danos para a organização (CNCS, s.d.; CNSS, 2015).

[14] Ciberataque- ataque realizado no ciberespaço através das tecnologias da informação. Este dirige-se a um ou vários sistemas e tem como objetivo prejudicar a segurança das tecnologias de informação e da comunicação de forma parcial ou total (CNCS, s.d.).

conclui-se que a cibersegurança é "um conjunto de ferramentas, políticas, diretrizes, abordagens de gestão de risco, formação, boas práticas e tecnologias que podem ser utilizadas para proteger o ciberespaço" (ITU, 2008).

2.2. Comportamentos e características humanos

Mais de 99% dos ataques exploram as características e comportamentos humanos, em vez de explorarem as vulnerabilidades dos sistemas informáticos, ou seja, a maioria dos cibercriminosos foca-se no fator humano da cibersegurança para definir as suas ações e motivações de ataque. Mesmo nos casos em que utilizam ferramentas automatizadas, estas são desenvolvidas de forma a aproveitarem-se das vulnerabilidades das pessoas. (Proofprint, 2019).

Deste modo, importa compreender quais são os principais comportamentos humanos que comprometem a cibersegurança das organizações e quais as suas características intrínsecas. Depois disso, poderão ser identificadas as consequências resultantes dos mesmos e procuradas soluções de modo a corrigir esses comportamentos que influenciam os níveis de cibersegurança alcançados.

2.2.1. Comportamentos humanos

No que toca à cibersegurança, é fundamental ter em conta os comportamentos humanos (Baptista, 2017). Segundo o CERT (2013), existem quatro tipos principais de incidentes[15] com origem nos comportamentos das pessoas:

Primeiramente, a divulgação acidental é identificada como um dos principais incidentes. Esta acontece quando os colaboradores publicam ou partilham informações confidenciais com os destinatários errados, sem intenção de cometer esse erro (CERT, 2013). Alguns comportamentos que podem levar a este tipo de incidente são: o facto de os colaboradores não eliminarem informações dos seus dispositivos, mesmo quando estas não serão necessárias no futuro; o acesso a redes sociais para fins pessoais no trabalho; e,

[15] Incidente- acontecimento com um efeito adverso na segurança das redes e dos sistemas de informação e nas respetivas informações neles armazenadas (CNCS, s.d.)

ainda associado ao último fator apresentado, a divulgação de problemas do trabalho nas redes socias (Ponemon Institute, 2012b).

Em segundo lugar, o código malicioso[16] é também identificado como um incidente relacionado com o comportamento humano. Neste caso, *hackers* (*black hats*) acedem a dados confidenciais da organização através de *software* malicioso (CERT, 2013). Algumas ações dos colaboradores que aumentam substancialmente a probabilidade deste tipo de incidentes vir a acontecer são: ligação a redes Wi-Fi inseguras; utilização de dispositivos próprios para fins laborais; conexão de dispositivos próprios à rede da organização; não atualização dos *softwares* antivírus e *anti-malware*; utilização de serviços *cloud* sem permissão da organização; acesso a *websites* considerados inseguros; *download* de aplicações não aprovadas pela organização; alteração das configurações de segurança dos sistemas; e abertura de anexos ou *links* de e-mails de *spam* e de fontes não fidedignas (Ponemon Institute, 2012b).

O descarte de registos físicos é também apontado como algo que é feito pelos colaboradores de forma acidental. Desde documentos perdidos, deitados fora ou roubados, são vários os exemplos deste tipo de incidente, resultante do comportamento humano. (CERT, 2013)

Por fim, a perda, roubo e descarte de dispositivos como computadores, *smartphones*, *tablets* e alguns componentes de armazenamento como *pens* USB e discos rígidos, colocam em causa a segurança das organizações (CERT, 2013). São vários os comportamentos errados associados a este incidente, tais como: utilização de componentes de armazenamento não protegidos e inseguros; dispositivos são deixados sem supervisão na ausência do proprietário e, em alguns dos casos, desbloqueados; perda de componentes de armazenamento com dados confidenciais e ausência de reporte imediato do desaparecimento à organização; transporte de dispositivos com informações

[16] Código malicioso- *software* ou *firmware* que executa processos não autorizados com vista a impactar negativamente a confidencialidade, integridade ou disponibilidade de um sistema de informação. Vírus e *spyware* são alguns exemplos de código malicioso (CNSS, 2015).

confidenciais desnecessárias em viagem; e não realização de *backups*[17] com regularidade, o que ajudaria em caso de perda ou roubo (Ponemon Institute, 2012b).

Adicionalmente, as *passwords* representam ainda outro grande problema, onde as pessoas nem sempre seguem as melhores práticas. Exemplo disso é o facto de partilharem *passwords* com terceiros, de reutilizarem a mesma *password* em diferentes contas, de não alterarem as *passwords* com regularidade e de não utilizarem *passwords* complexas (Ponemon Institute, 2012b).

2.2.2. Características do humanas

Importa ainda compreender quais as características intrínsecas humanas que, em muitos casos, levam a comportamentos que comprometem a cibersegurança das organizações. Esta compreensão é fundamental para todos os processos de elaboração e aplicação de políticas de cibersegurança. É de salientar ainda que estas características são também exploradas pelos praticantes de engenharia social, de modo a conseguirem atingir os seus objetivos, pelo que a importância da sua compreensão se torna ainda maior (CERT, 2014).

A falta de atenção é apresentada como uma característica humana que está na origem de diversos incidentes. Esta pode ser mais evidente em situações de preocupação, que leva as pessoas a terem um défice de atenção nas tarefas que estão a desempenhar. Para além disso, devido à falta de atenção, as pessoas podem não conseguir identificar os sinais de mudança e, por isso, nem conseguir detetar sinais associados a acontecimentos suspeitos. Associado a isso, as pessoas acabam por não ter consciência da situação atual em que se encontram. Deste modo, pessoas que se encontrem mais desatentas e preocupadas com outros assuntos, incorrem num maior risco de despoletar novos incidentes de cibersegurança. (CERT, 2014)

Deve-se salientar ainda que nem todas as pessoas reagem de igual forma ao risco. Nesse sentido, pessoas com elevada aceitação ao risco, acabam por apresentar comportamentos mais arriscados para a organização. Por outro lado, pessoas mais avessas

[17] *Backup*- cópia de segurança de ficheiros e programas que visa facilitar a sua recuperação em caso de necessidade (CNSS, 2015).

ao risco representam uma menor probabilidade de colocar em prática ações de risco, pelo que são consideradas mais cautelosas e menos propícias a estarem na origem de incidentes de cibersegurança. (CERT, 2014)

Importa ainda destacar que o *stress* e ansiedade podem estar correlacionados com a prática de erros que comprometem a cibersegurança. São vários os fatores que podem estar na origem do *stress* das pessoas, tais como: mau ambiente de trabalho, existência de pressão durante períodos de tempo prolongados e elevadas cargas de trabalho. Assim sendo, pessoas que se encontrem mais expostas a situações de *stress* têm também mais propensão a comprometer a cibersegurança da organização onde se inserem. (CERT, 2014)

Ainda que noutro âmbito, as condições de saúde física também têm bastante impacto no desempenho humano. Aspetos cognitivos como a atenção, memória e raciocínio podem ser afetados por condições como fadiga, doença ou lesão. Nesse sentido, um colaborador que não se encontre bem a nível físico, poderá representar um maior risco de cibersegurança para a organização. (CERT, 2014)

Deve-se ter ainda em consideração que valores, crenças e hábitos de um colaborador podem influenciar o cumprimento das diretrizes de cibersegurança. Por um lado, estas podem estar de acordo com as diretrizes da organização, o que facilita o seu cumprimento. Por outro, os valores, crenças e hábitos podem sobrepor-se às diretrizes de cibersegurança, se não forem compatíveis, o que poderá representar um risco para a organização. (CERT, 2014)

Por fim, apesar de a falta de conhecimento não ser considerada diretamente como uma característica intrínseca humana, esta está na origem de muitos incidentes de cibersegurança, pelo que é uma das principais preocupações das organizações em relação aos seus colaboradores. A falta de conhecimento pode levar ao incumprimento das diretrizes de cibersegurança devido a incompreensão parcial ou total das mesmas. Nesse sentido, quanto menor for o conhecimento dos colaboradores, maior a probabilidade de a organização sofrer um ciberataque (CERT, 2014).

2.3. Consequências dos comportamentos humanos

2.3.1. Principais consequências

Deste modo, os comportamentos e características humanos apresentados anteriormente poderão ter diversas consequências na cibersegurança das organizações que, por conseguinte, trazem diversos prejuízos para as mesmas. Nesse sentido, as organizações preocupam-se essencialmente com os danos causados na qualidade dos produtos e serviços, a perda de confiança por parte dos clientes, os danos causados à reputação da marca, a perda de informação confidencial, a perda de oportunidades de negócio, os danos causados em equipamentos e o custo de mitigação e resposta ao ataque. Assim, sendo que se trata de consequências resultantes do comportamento humano, a origem dos ataques é, em muitos casos, a engenharia social. (CERT, 2014)

2.3.2. Engenharia Social

A engenharia social pode ser definida como um processo utilizado pelos cibercriminosos para manipular pessoas, de modo a que estas realizem involuntariamente ações do interesse do manipulador, explorando a falta de consciencialização e conhecimento das pessoas. Geralmente, estas ações causam danos, ou aumentam a probabilidade de causar danos futuros, à confidencialidade, integridade e disponibilidade dos recursos ou ativos da organização. Por outras palavras, a engenharia social tem como objetivo coletar informações, cometer fraudes e obter o acesso a sistemas. Assim sendo, os praticantes desta atividade baseiam-se na psicologia humana e nas suas características e limitações cognitivas de modo a explorá-las, conseguindo assim enganar as pessoas. (CERT, 2014; Mitnick & Simon, 2003) Atualmente, a engenharia social encontra-se cada vez mais eficaz e difundida, pelo que deve ser uma das grandes preocupações das organizações (Proofprint, 2019).

Na maioria das vezes a engenharia social não é composta por um único ataque, mas sim por uma sequência complexa de ações, o que leva a ataques de maior escala. No caso de existir uma única fase de ataque de engenharia social, acontece um único incidente. Neste caso, o invasor obtém as informações e usa-as para causar danos à organização, sendo que estas informações não serão utilizadas para novos casos de

engenharia social. No caso de acontecer uma sequência de múltiplos ataques de engenharia social, o atacante aproveita-se das informações obtidas num ataque inicial para executar ataques posteriores de engenharia social. Estes múltiplos ataques poderão acontecer com um intervalo de minutos, horas, semanas ou até meses. (CERT, 2014)

É ainda de salientar que qualquer pessoa dentro de uma organização pode ser alvo de engenharia social, independentemente da sua posição na hierarquia da organização. Isto porque as pessoas acabam por serem facilmente identificadas através dos mídia, em *websites* e até em redes sociais. Deste modo, muitos dos *e-mails* de colaboradores e diretores são descobertos através de uma simples pesquisa no Google. (Proofprint, 2019)

2.3.3. *Phishing*

Uma das práticas mais comuns de engenharia social é o *phishing*. Este é composto por um *phisher*, que normalmente envia um ou vários *e-mails* que parecem ter origem numa entidade fidedigna. Estes *e-mails* contêm um *link* direto para um *website* fraudulento que, em muitos casos, é visualmente semelhante à página *web* verdadeira da organização. Geralmente, é através deste *link* fraudulento que o *phisher* obtém dados e informações confidenciais como *passwords*. Ainda dentro da mesma área, o *spear phishing* é uma forma de *phishing* direcionado onde o *phisher*, antes do ataque, se dedica a estudar a vítima e, com base nessas informações, direciona o seu ataque, aumentando bastante a sua probabilidade de sucesso. (CERT, 2014; O'Brien, 2005)

2.4.Soluções para corrigir os comportamentos humanos

A engenharia social continua a ter sucesso nos dias de hoje, pelo que as "as pessoas continuam a ser o principal alvo dos atacantes e a última linha de defesa das organizações" (CERT, 2014; Proofprint, 2019). Nesse sentido, a necessidade de estudar os aspetos psicológicos das pessoas, que são também estudados pela engenharia social, é cada vez maior. Com esse estudo, diversas práticas, sistemas e abordagens de consciencialização e formação são desenvolvidas e implementadas para combater o cibercrime (CERT, 2014). Contudo, é importante salientar que não existe uma solução única para corrigir os comportamentos humanos, mas sim um conjunto de soluções,

complementares entre si, que visam aumentar a segurança das organizações (AP2SI, 2016; Leocádio, 2017).

Adicionalmente, pretende-se que cada colaborador aja como um "sensor" da organização, prevenindo, detetando e reagindo a eventuais ataques, protegendo a organização a que pertence (Martins et al., 2016). Nesse sentido, espera-se que exista uma compreensão integral de todos os fenómenos e não apenas uma análise isolada dos mesmos, para que não existam "elos mais fracos" dentro das organizações. Esta abordagem holística representa um esforço coletivo, onde cada colaborador contribui no combate ao cibercrime. Neste sentido, a cibersegurança está dependente de cada membro da organização individualmente e coletivamente (ENISA, 2017).

Ainda que a cibersegurança deva fazer parte das tarefas diárias de todos os colaboradores, esta não deve ser excessivamente complexa de modo a não dificultar o desempenho das suas funções normais associadas ao *core business* (ENISA, 2017). Nesse sentido, deve existir um equilíbrio entre os níveis de segurança que são exigidos, a usabilidade e a funcionalidade dos sistemas. Ou seja, se os níveis de segurança forem extremamente elevados, os colaboradores terão muitas dificuldades em utilizar os sistemas pois estes tornam-se menos funcionais e, consequentemente, mais difíceis de utilizar, fazendo com que os colaboradores desistam do processo. Por outro lado, se um sistema for extremamente fácil de utilizar, a sua segurança acaba por ficar comprometida, representando uma vulnerabilidade adicional para a organização. (Bada et al., 2015; Nurse et al., 2011)

Por fim, é de extrema relevância que todas as organizações se preocupem com a cibersegurança pois "os incidentes não discriminam organizações", ou seja, as vulnerabilidades são exploradas em organizações de grandes e pequenas dimensões, independentemente da indústria onde se inserem (Baptista, 2017; Proofprint, 2019). Nesse sentido, apesar de as organizações de maior dimensão parecerem mais atraentes para os cibercriminosos, as organizações de menores dimensões acabam por ser mais lucrativas devido à falta de preparação que apresentam (Matos, 2018; Proofprint, 2019). Deste modo, nos últimos anos registou-se um aumento constante de ataques contra organizações de pequenas dimensões (Symantec, 2016).

2.4.1. Cultura de cibersegurança

Uma cultura de cibersegurança sólida é uma das principais soluções para mitigar os problemas de cibersegurança com origem no comportamento humano. Segundo a ENISA (2017), a cultura de cibersegurança das organizações pode ser definida como o conjunto de "conhecimentos, crenças, perceções, atitudes, suposições, normas e valores das pessoas relativamente à cibersegurança e a forma como estes se manifestam nos seus comportamentos com as tecnologias da informação". Deste modo, por se tratar de uma cultura, quer dizer que as preocupações com a cibersegurança serão parte integrante do trabalho, hábitos e conduta das pessoas, integrando o seu quotidiano e moldando o pensamento de toda a equipa. Assim, o principal objetivo da cultura de cibersegurança é tornar as organizações mais resilientes, sem impor medidas onerosas, para que não sejam um obstáculo ao bom funcionamento das organizações. Desta forma, espera-se que os colaboradores olhem para as políticas de cibersegurança como diretrizes e não como obrigações. Para além disso, e uma vez que a fronteira entre "casa" e "local de trabalho" é cada vez menos visível, espera-se que a mudança de mentalidade dos colaboradores em relação à cibersegurança também se reflita na sua vida privada. (ENISA, 2017)

Assim sendo, consciencializar, formar e educar os colaboradores para comportamentos adequados para a cultura de cibersegurança é a base para tornar as organizações mais resilientes (Baptista, 2017). Importa salientar ainda que, mesmo que os termos consciencialização, treino e educação sejam frequentemente utilizados de forma indiferenciada, estes têm diferentes significados e contribuem para diferentes fases e necessidades no estabelecimento de uma cultura de cibersegurança numa organização (Furnell, 2017).

2.4.2. Consciencialização em cibersegurança

A consciencialização em segurança da informação[18], mais concretamente em cibersegurança, é parte integrante da cultura de cibersegurança (ENISA, 2017). Nesse sentido, a consciencialização tem como objetivo fazer com que as pessoas estejam cientes e, idealmente, comprometidas com os objetivos de segurança da organização (Siponen,

[18] Segurança da informação- proteção da informação e dos sistemas de informação contra acesso, uso, divulgação, modificação ou destruição não autorizados (CNSS, 2015).

2000). Pode ser considerada, essencialmente, como uma medida preventiva que tem como objetivo estabelecer os princípios e procedimentos de cibersegurança na mente de todos os colaboradores, alertando-os para os problemas de segurança existentes e as suas possíveis consequências (Kajava & Siponen, 2002, Woerner, 2012). Em suma, pretende-se concentrar a atenção dos colaboradores na segurança da informação e cibersegurança e aumentar a sua preocupação e sensibilização com estes temas (Furnell, 2017; Wilson & Hash, 2003).

O aumento da consciência relativamente à cibersegurança e à segurança da informação irá fazer com que os colaboradores reduzam a prática de comportamentos que colocam a cibersegurança em causa, isto se for bem utilizada, aplicada e interpretada. Para isso, importa identificar, quantificar e compreender os erros cometidos anteriormente pelos colaboradores da organização, tendo sempre em conta que se trata de um processo contínuo que requer repetição (Siponen, 2000, Woerner, 2012).

2.4.3. Formação em cibersegurança

A formação em cibersegurança é um processo de ensino de competências e de utilização de ferramentas que tem como principal objetivo criar competências de segurança relevantes e necessárias em todos os colaboradores (Peltier, 2005; Zafra et al., 1998). Assim sendo, a formação procura ensinar competências mais específicas e, por isso, exige um papel mais ativo por parte dos colaboradores, quando comparado com a consciencialização (Wilson & Hash, 2003). Relativamente à sua duração, a formação caracteriza-se por ser geralmente de curto prazo, tendo uma duração habitual de dias ou semanas (Woerner, 2012).

Ainda em relação à formação, idealmente é fornecido um nível básico a todos os colaboradores e uma formação específica a determinados grupos-alvo. Estes grupos são constituídos por colaboradores que, devido às funções que desempenham, enfrentam desafios específicos dentro da organização e, por isso, estão mais sujeitas ao risco. (ENISA, 2017)

2.4.4. Educação em cibersegurança

A educação, neste contexto, procura aliar todas as competências de cibersegurança num estudo multidisciplinar desta área (Wilson & Hash, 2003). Assim sendo, para além dos conceitos fundamentais que são transmitidos, permite ainda a compreensão de ferramentas, técnicas e tecnologias relacionadas com a cibersegurança. Desta forma, a educação em cibersegurança caracteriza-se por ser um estudo formal de longo prazo, que compreende uma duração de meses ou anos. (Woerner, 2012)

2.4.5. Métodos de Comunicação

Importa salientar que são vários os métodos de comunicação e as atividades que podem ser utilizados para implementar e fomentar a cultura de cibersegurança. Idealmente, deverão ser selecionados vários métodos para que o alcance da comunicação seja o maior possível. (ENISA, 2017)

Assim sendo, existem três métodos possíveis para a implementação de uma boa cultura de cibersegurança: *online*, híbridos e *offline*. O método *online* sugere diversas atividades como o envio de *e-mails*, o recurso a jogos, a elaboração de *webinars*, a disponibilização de cursos *online*, a existência de uma *intranet* e até a comunicação através das redes sociais. Por outro lado, o método *offline* é sugerido para a elaboração de sessões de treino em grupo, a distribuição de *flyers*, a disponibilização de *workshops*, a presença em eventos de cibersegurança e palestras com especialistas da área e a afixação de *posters*. Por fim, o método híbrido, que resulta de uma combinação dos dois métodos anteriores, sugere atividades como simulações de ataques em contexto laboral, criação de diferentes cenários e *sandboxes*, o relato de histórias relacionadas com boas práticas e a oferta de incentivos. (ENISA, 2017)

2.4.6. Adaptação da consciencialização, formação e educação

Para elaborar ações de consciencialização e de formação bem sucedidas, deve-se identificar as competências individuais e coletivas que devem ser desenvolvidas nos colaboradores, assim como se deve escolher o tipo de exercício que se adequa mais à organização em causa e aos seus respetivos recursos humanos. (Martins et al., 2016)

Nesse sentido, e de forma a deixar os colaboradores mais recetivos, as mensagens de consciencialização, formação e educação idealmente devem ser direcionadas e adaptadas a cada colaborador, consoante as suas necessidades, preferências e perceções. Deste modo, consideram-se diferentes aspetos como: a função desempenhada pelo colaborador dentro da organização, tendo em conta as suas responsabilidades e os sistemas que utiliza; o conhecimento prévio do colaborador em segurança, políticas da organização e tecnologia; barreiras à aplicação do conhecimento transmitido, como valores pessoais e culturais do colaborador; o estilo de aprendizagem ideal para cada colaborador; e a perceção de segurança de cada colaborador, que reflete a sua relação com a segurança. (Furnell, 2017)

Atualmente, este nível de detalhe na adaptação de ações de consciencialização e formação não se verifica em muitos casos, pelo que a maioria das mensagens transmitidas são genéricas para todos os colaboradores. Nos casos em que é feito algum tipo de adaptação, esta é elaborada com base no tipo de organização a que se destina. (Furnell, 2017)

2.6.6.1. Características humanas a considerar

Adicionalmente, o ser humano apresenta características intrínsecas que devem ser tidas em conta no desenvolvimento de planos de consciencialização e formação de modo a serem atingidos melhores resultados (ENISA, 2017). Estas características humanas, em muitos dos casos, são o que distingue cada um dos colaboradores e o que os leva a serem mais ou menos propensos a cumprir as políticas de cibersegurança (Hadlington, 2018).

Contudo, deve-se ter em conta que não se consegue predeterminar o comportamento humano na sua totalidade. Assim sendo, os planos de consciencialização e formação acabam por ser limitados por estarem dependentes da situação em que o ciberataque ocorre, do *hacker* e do alvo escolhido pelo mesmo (Siponen, 2000).

A primeira característica destacada está associada ao facto de as pessoas seguirem as ações praticadas pelos restantes membros do grupo onde estão inseridas, acabando por ser influenciadas, ainda que de forma involuntária. Deste modo, a adesão a políticas de cibersegurança pode ser influenciada se os restantes membros da equipa decidirem aderir também, beneficiando toda a organização. Nesse sentido, espera-se que exista uma taxa

crescente de adesão onde, numa fase mais avançada são poucos aqueles que não seguirão as diretrizes de cibersegurança, caso a maior parte dos membros da organização as siga. Por outro lado, se a maioria decidir não adotar as diretrizes de cibersegurança, o mais provável é que muitos colaboradores também não o façam, ainda que estivessem predispostos a adotar as diretrizes apresentadas pela organização. (Hadlington, 2018)

Adicionalmente, se um colaborador não tem conhecimento ou consciência da importância da cibersegurança na organização e de todas as práticas que com ela se relacionam, acaba por não se alinhar às suas diretrizes e, consequentemente, não as colocará em prática por desconhecimento ou falta de compreensão. Deste modo, pode-se concluir que a consciencialização, a formação e a educação são processos fundamentais para levar os colaboradores a seguirem as diretrizes de cibersegurança estabelecidas, aumentando o seu conhecimento e consciência sobre este tema (Hadlington, 2018). Em suma, para atingir uma mudança duradoura, é fundamental que os colaboradores compreendam as ameaças que enfrentam, as diretrizes de segurança que devem cumprir e a responsabilidade que lhes é atribuída (ENISA, 2017).

Por um lado, sabe-se que as pessoas que são consideradas mais racionais e ponderadas têm tendência a estar mais atentas a e seguir as diretrizes de cibersegurança com mais rigor. Por outro lado, pessoas que são mais impulsivas acabam por ser mais propensas a não cumprir as diretrizes e, consequentemente, a serem vítimas de um ciberataque. Isto deve-se aos reduzidos níveis de ponderação, fruto da rapidez na tomada de decisão. Para além disso, ainda que associado à racionalidade, sabe-se que o facto de uma pessoa ter em consideração as consequências futuras das suas ações faz com que esta seja mais ponderada e, nesse sentido, agirá de acordo com as diretrizes estabelecidas. Adicionalmente, pessoas mais questionadoras também representam um ponto positivo para a cibersegurança. Estas, ao invés de ignorar ou aceitar de imediato as circunstâncias, preferem investigar para poderem agir ou retirar conclusões. (Hadlington, 2018)

Por fim, sabe-se que a persuasão é uma peça chave para levar as pessoas a seguir as diretrizes de cibersegurança da organização. Nesse sentido, são várias as abordagens de persuasão que podem ser utilizadas de modo a garantir que os colaboradores seguem as diretrizes estabelecidas. Primeiramente, é importante garantir que todas as ações demonstradas são lógicas e não contraditórias, para que seja transmitida coerência e

credibilidade. Para além disso, é sabido que as emoções são parte integrante do pensamento e tomada de decisão das pessoas. Nesse sentido, quando uma pessoa é obrigada a fazer uma escolha ou a tomar uma decisão, a aprendizagem emocional, resultante das experiências passadas, ajudará na tomada de decisão. Sabe-se ainda que a moral e a ética orientam fortemente o comportamento das pessoas. Assim, se os colaboradores compreenderem as dimensões éticas da negligência em cibersegurança, estarão mais propensos a seguir as diretrizes definidas. Ainda dentro do tema da persuasão, sabe-se que, para garantir o seu bem-estar, os colaboradores são menos negligentes e cometem menos erros que comprometem a segurança. Nesse sentido, a perceção do risco associado às suas ações é muito importante. Para além disso, as pessoas têm o instinto de procurar sentir-se seguras e protegidas. Pelo que importa explicar-lhes que, quanto mais sólida for a cibersegurança de uma organização, maior será a segurança e proteção dos mesmos. Por fim, a racionalidade é um fator que também deve ser tido em conta, pelo que deve existir sempre uma explicação racional e factual das diretrizes para que todos as possam compreendê-las e segui-las. (Siponen, 2000)

2.4.7. Importância da gestão de topo

A gestão de topo representa um papel muito importante na cultura de cibersegurança de uma organização pois é o elemento responsável por traçar a estratégia da organização e por definir o orçamento financeiro destinado à cibersegurança. Deste modo, a alta gestão deve alinhar a estratégia organizacional com as políticas de cibersegurança da organização e garantir que são alocados os recursos necessários para o estabelecimento de uma cultura de cibersegurança sólida. Para isso, é fundamental sensibilizar a gestão de topo para a importância da cibersegurança, deixando-a ciente de todos os riscos e consequências a que a organização está exposta. Deste modo, espera-se que a gestão de topo compreenda que a cibersegurança não se trata de mais uma despesa, mas sim de uma forma de prevenção e redução de risco (ENISA, 2017).

Contudo, ainda que a existência de políticas de cibersegurança possa evidenciar o comprometimento da gestão de topo com a cibersegurança, deve-se ter em conta que é apenas uma das partes necessárias para garantir uma cultura de cibersegurança sólida. Nesse sentido, não basta criar-se um conjunto de políticas, mas também garantir que existe um compromisso da gestão de topo com a cibersegurança (AP2SI, 2016). Desta

forma, espera-se que a alta gestão dê a conhecer todas as políticas de cibersegurança aos colaboradores da organização e que seja um exemplo para todos eles, cumprindo-as no seu quotidiano (ENISA, 2017). Porém, nem sempre é o que se verifica na realidade. Ainda que a cibersegurança possa ser uma preocupação da gestão de topo, nem todos os colaboradores têm conhecimento das políticas de cibersegurança existentes, pelo que se deve trabalhar nesse sentido (AP2SI, 2016).

Atualmente, a gestão de topo está extremamente focada no *core business* da organização. Em muitos casos, esta considera que os riscos a que a organização está exposta não justificam a contratação de pessoal especializado ou a criação de um departamento específico na organização. Estas situações podem ser justificadas pelo facto de a alta gestão não ter um nível de conhecimento em cibersegurança suficiente para poder compreender a sua importância (AP2SI, 2016; EY, 2018). Desta forma, pode-se verificar que, nos casos em foi estabelecido um orçamento destinado à cibersegurança, este representou menos de 1% do orçamento total da organização. Para além disso, a maioria não considera aumentar esse valor no ano seguinte. Deste modo, pode-se concluir que a falta de recursos atribuídos à cibersegurança é um problema nas organizações portuguesas, decorrente da falta de conhecimento e consciencialização da gestão de topo. (AP2SI, 2016)

2.4.8. Avaliação dos planos

A avaliação dos resultados dos programas de consciencialização e formação e educação é uma peça fundamental para que se possa averiguar se foram alcançados os resultados pretendidos e para identificar as mudanças a efetuar no futuro. Neste sentido, para avaliar a eficácia destes programas deve-se verificar os pontos seguintes.

Em primeiro lugar, importa saber se os colaboradores gostaram dos programas de consciencialização, formação e educação efetuados, pois são eles a peça chave de todo este processo. Assim sendo, é fundamental que o seu feedback seja positivo, mostrando o seu interesse em seguir as diretrizes do programa (Kajava & Siponen, 2002).

Em segundo lugar, é muito importante garantir que os colaboradores adquirem efetivamente o conhecimento. Caso contrário, não conseguirão colocar em prática as

diretrizes de cibersegurança definidas, mesmo que tenham gostado dos programas de cibersegurança (Kajava & Siponen, 2002).

De seguida, deve-se averiguar se os colaboradores aplicam corretamente os conhecimentos adquiridos no decorrer do seu trabalho. Deste modo, mesmo que os colaboradores tenham compreendido as diretrizes de cibersegurança, não é garantido que as coloquem em prática (Kajava & Siponen, 2002).

Para além disso, importa perceber se os programas de consciencialização, formação e educação sortiram efetivamente efeitos na cibersegurança da organização (Kajava & Siponen, 2002). Nesse sentido, a utilização de métricas é muito importante pois permite avaliar a eficácia dos programas implementados. Desta forma, podem ser retiradas conclusões relativas à evolução registada, fazendo comparações com valores passados e com valores esperados. (ENISA, 2017)

Adicionalmente, numa perspetiva de avaliar a cibersegurança de uma organização, existem vários modelos de maturidade de cibersegurança que podem servir como referência. Estes permitem identificar o nível de maturidade atual da organização e o caminho que esta deve percorrer, de modo a tornar-se mais segura. Desta forma, espera-se que a organização evolua progressivamente, desde uma fase muito inicial, onde o conhecimento em cibersegurança é limitado, até chegar a um nível de cibersegurança bastante elevado. Por fim, importa salientar que as organizações devem garantir que se atualizam constantemente face à atualidade, pelo que devem estar em constante evolução. (Barclay, 2014; Christopher, 2018; IEEE, s.d.)

3. METODOLOGIA DE INVESTIGAÇÃO

O presente capítulo encontra-se dividido em duas partes. Em primeiro lugar, é explicada a abordagem de investigação seguida nesta dissertação. Por fim, a amostra e o processo de recolha de dados são apresentados.

3.1. Tipo de estudo

Tendo em conta o objetivo principal deste estudo, optou-se por seguir uma abordagem de investigação qualitativa. O método qualitativo caracteriza-se por estudar uma situação ou fenómeno com base em representações, crenças, perceções e opiniões, resultantes das interpretações dos seres humanos, procurando obter uma compreensão de uma realidade particular a partir das opiniões e perceções dos entrevistados (Batista et al. (2017) com base em Minayo (2010)). Desta forma, esta abordagem permite investigar em profundidade o objeto em estudo, procurando uma maior compreensão do tema (Gil, 2008).

Nesse sentido, a recolha de dados foi feita através de entrevistas individuais. Deste modo, pode-se compreender a forma como os entrevistados observam, vivenciam e analisam o tema em estudo no seu contexto social e temporal, com base no seu conhecimento valores e crenças (Duarte, 2004). Assim, procurou-se obter o ponto de vista de peritos e investigadores em cibersegurança que lidam diariamente com este tema, estando por isso sensibilizados e familiarizados com o tema em estudo numa ótica profissional, pelo que as suas respostas foram baseadas no seu conhecimento teórico e experiência profissional.

Importa salientar que, para além de todas as vantagens inerentes às entrevistas como método de recolha de dados, a opção de fazer questionários foi excluída devido ao tema em estudo. Acredita-se que, devido à sensibilidade associada à matéria da cibersegurança, a taxa de resposta a questionários nesta área seja reduzida e, para além disso, que as respostas obtidas nem sempre correspondam à verdade por se tratar de uma área tão crítica das organizações. Adicionalmente, para este trabalho julgou-se ser muito mais proveitoso recolher dados através de questões de resposta aberta e não de resposta fechada pois são alcançados níveis de detalhe mais profundos e não apenas respostas standardizadas, o que permite uma compreensão mais aprofundada do tema.

Depois de concluídas as entrevistas, estas foram detalhadamente analisadas. O tratamento de toda a informação recolhida foi feito através da análise de conteúdo, com base nas respostas dadas pelos entrevistados, sendo este o *corpus* da análise. Depois de transcritas as respostas obtidas nas entrevistas, estas foram categorizadas com base em cinco grandes categorias: estado geral do fator humano da cibersegurança nas

organizações; comportamentos e características humanos; consequências dos comportamentos humanos; soluções que visam corrigir os comportamentos humanos; e desafios da cibersegurança associados ao fator humano. Por sua vez, foram geradas várias unidades de registo, ou seja, vários segmentos de conteúdo inseridos nas categorias anteriormente descritas, com base nas unidades de contexto analisadas. (Bardin, 2016; Vala, 1986)

3.2.Amostra e recolha de dados

Como referido no ponto anterior, os entrevistados foram selecionados com base em caraterísticas previamente determinadas e que se consideraram ser as mais pertinentes. Neste sentido, decidiu-se, previamente, que as pessoas a entrevistar seriam apenas peritos e investigadores em cibersegurança. Esta decisão teve por base o objetivo de obter respostas que permitissem retirar conclusões fidedignas. Assim sendo, pode-se afirmar que a amostra deste estudo é não probabilística e baseada no julgamento pois os entrevistados não foram selecionados aleatoriamente, mas sim com base em critérios próprios que se consideraram mais pertinentes para o estudo em causa (Kothari, 2004).

Adicionalmente, foi garantido o anonimato a todos os entrevistados, de forma a garantir o conforto dos mesmos e incentivando-os a responder com mais detalhe e veracidade às questões colocadas, assegurando que, tanto eles como a organização que representam, não serão identificados pelos leitores do presente trabalho.

Relativamente ao número de entrevistados, este foi determinado pela saturação da informação recolhida, ou seja, depois de 7 entrevistas realizadas chegou-se à conclusão de que o leque de respostas dadas não sofria grande variação, pelo que poderiam ser retiradas conclusões fiáveis com base nas respostas obtidas.

Tabela I - Detalhes das entrevistas realizadas

Ordem	**Função**	**Setor**	**Código**	**Duração**	**Tipo**
1	Consultor especialista	Regulador	E1	60 min.	Presencial
2	Consultor especialista	Regulador	E2	45 min.	Presencial
3	Professor catedrático	Educação	E3	60 min.	Presencial
4	*Lead CyberSecurity Architect*	Telecomunicações	E4	30 min.	Remota
5	*Data Protection Officer*	Banca	E5	30 min.	Presencial
6	*Information Security Professional*	Telecomunicações	E6	15 min.	Escrita + Remota
7	*Cyber Security Engineer*	Tecnologia	E7	45 min.	Remota

Fonte: elaboração própria com base em (Monzelo, 2018)

Na tabela I é apresentada uma listagem com os detalhes de todas as entrevistas realizadas. Assim, para cada entrevista, é apresentado: a ordem em que a entrevista foi realizada; a principal função desempenhada atualmente pelo entrevistado na organização; o setor de atividade da organização onde o entrevistado se insere; o código atribuído à entrevista; a duração aproximada da entrevista; e a identificação do tipo de entrevista (presencial, escrita ou remota).

Todas as entrevistas foram realizadas no ano de 2019, mais concretamente entre os meses de agosto e setembro. Algumas destas entrevistas foram realizadas presencialmente (E1, E2, E3 e E5) e as restantes (E4, E6 e E7) foram realizadas remotamente, via telefone ou Skype. No caso da entrevista número 6 (E6) importa ressalvar que algumas perguntas foram respondidas de forma escrita, sendo que posteriormente ocorreu uma breve entrevista via telefone de modo a serem discutidas

algumas das respostas dadas, com a possibilidade de serem colocadas algumas questões adicionais.

O guião das entrevistas, elaborado para o presente trabalho (anexo 1), funcionou como um referencial organizado e é o resultado da preparação prévia de todas as entrevistas realizadas (Amado & Ferreira, 2013). Este contém várias questões orientadoras e um conjunto de questões opcionais, que foram colocadas consoante as necessidades verificadas no decorrer das entrevistas, resultantes das respostas dadas pelos entrevistados. Nesse sentido, considera-se que as entrevistas realizadas podem ser classificadas como semiestruturadas pois o guião e as questões que o constituem não foram vistas como uma imposição rígida para a entrevistadora, mas apenas como um guia de apoio à condução da entrevista de modo a assegurar que todos os objetivos da mesma são alcançados (Batista et al. (2017) com base em Minayo (2010)).

Para além disso, o guião encontra-se dividido em quatro grandes grupos. No primeiro, as questões apresentadas visam compreender a relação entre a cibersegurança e o fator humano no contexto organizacional, de uma forma geral. No segundo grupo, as questões definidas relacionam-se com a primeira questão de investigação deste trabalho, pelo que procuram compreender quais os comportamentos e características humanos que influenciam os níveis de cibersegurança alcançados nas organizações. Em terceiro lugar, consideram-se questões que visam responder à segunda questão de investigação desta dissertação, ou seja, procura-se compreender quais as consequências dos comportamentos humanos na cibersegurança das organizações. Por fim, as questões apresentadas no último grupo do guião, procuram identificar as soluções que permitem corrigir os comportamentos humanos que influenciam a cibersegurança, pelo que estão relacionadas com a terceira questão de investigação.

4. APRESENTAÇÃO DOS RESULTADOS

No presente capítulo, são apresentados os resultados obtidos através das entrevistas, apresentados pela ordem das questões de investigação pré-definidas. Desta forma, são identificados os comportamentos e características humanos que influenciam a cibersegurança nas organizações, o seu respetivo impacto nos níveis de cibersegurança

alcançados e as correspondentes soluções que visam corrigir os comportamentos apresentados, do ponto de vista dos entrevistados.

4.1. Cibersegurança nas organizações

"De acordo com as normas, standards e boas práticas, as organizações deverão realizar uma análise de risco e, a partir dos resultados, identificar as suas estratégias, implementá-las e monitorizá-las continuamente, repetindo o processo quando necessário." (E6)

No que toca à preocupação das organizações com a cibersegurança, importa ressalvar que não se deve generalizar uma resposta para todas as organizações (E3 e E4). Desta forma, aspetos como a dimensão das organizações, setor de atividade e obrigações legais e reguladoras estão, muitas das vezes, na origem de um maior ou menor grau sensibilização das organizações para questões relacionadas com a cibersegurança (E3 e E5). Na prática, organizações de grandes dimensões ou de alguns setores mais críticos tendem a estar mais sensibilizadas para a cibersegurança, ainda que existam exceções. Contudo, mesmo nestes casos, o nível de maturidade de cibersegurança destas organizações encontra-se abaixo do esperado (E5).

Por outro lado, a maioria das organizações, classificadas como microempresas e PMEs, não têm *know-how* suficiente nesta área, nem se preocupam com a cibersegurança tal como deveriam, pelo que o seu nível de maturidade é muito baixo (E1, E2, E3, E4, E5, E6 e E7). Porém, ainda que em alguns casos exista um crescimento da perceção de risco de cibersegurança nos últimos tempos (E1, E5 e E7), este não é acompanhado pela prática, pelo que o nível de preparação destas organizações é muito reduzido (E1, E3, E4 e E7). Este problema tem origem, muitas das vezes, na gestão de topo das organizações, que, para além de estar centrada numa única pessoa, esta desvaloriza a cibersegurança e considera-a como uma despesa e não como um investimento, pois está exclusivamente focada no *core business* da organização e, por isso, não disponibiliza parte do orçamento necessário para satisfazer as necessidades de cibersegurança existentes na organização (E1 e E3). Este tipo de decisões poderá estar associado à má avaliação de risco por parte da gestão de topo, consequente da sua falta de conhecimento e competências nesta área (E1 e E3).

Contudo, estas discrepâncias entre organizações de diferentes dimensões não deveriam existir pois, atualmente, todas elas são igualmente consideradas como potenciais alvos de ataque para os cibercriminosos. Isto porque, do lado do cibercrime, apenas são procuradas vulnerabilidades que possam ser exploradas, pelo que não são feitas distinções entre a dimensão ou setor de atividade das organizações (E7).

Para além disso, em muitas organizações existe uma perceção errada do que é a cibersegurança e do que esta envolve. Isto deve-se ao baixo nível de maturidade de cibersegurança em muitas destas organizações. A maioria das mesmas não está ciente de que a cibersegurança implica uma sinergia entre pessoas, processos e tecnologia, pelo que se concentram apenas na tecnologia, negligenciando a importância das pessoas na cibersegurança das organizações (E1, E2, E4, E5 e E7). Nesse sentido, consideram ser uma responsabilidade exclusiva do departamento de IT, descurando a responsabilidade inerente aos restantes departamentos e a importância de ter um departamento exclusivo para a cibersegurança (E2, E5 e E7). Contudo, não se pode generalizar, existem organizações que evidenciam ter uma visão holística da cibersegurança, ainda que representem uma percentagem muito mais reduzida do total das organizações (E3, E4 e E5).

4.2. Comportamentos e características humanos

As pessoas desempenham um papel fundamental dentro das organizações, contudo são consideradas um dos elos mais vulneráveis ou até mesmo um dos elos mais fracos das mesmas, ainda que a tecnologia também represente algumas vulnerabilidades (E1, E2, E3, E4, E6 e E7). Atualmente, muitos processos e tecnologias estão dependentes das pessoas pois são elas quem os decide, utiliza, desenvolve e implementa. Este elevado nível de importância traduz-se num maior nível de vulnerabilidade (E6).

O desconhecimento das pessoas relativamente à cibersegurança é algo alarmante e que deve ser corrigido. Este desconhecimento leva a que os colboradores pratiquem diversos comportamentos que colocam em causa a cibersegurança das organizações. Alguns destes comportamentos são a partilha de *passwords* indevida (E1 e E3), a partilha de informações privadas e corporativas (E2 e E4), a partilha do *e-mail* profissional para fins pessoais (E2), a utilização *pens* como dispositivos de armazenamento (E3), o acesso

a *websites* não fidedignos (E4), o não cumprimento das políticas e processos instituídos pela organização (E6) e a abertura de *e-mails* de remetentes desconhecidos (E2, E4 e E6), assim como a abertura dos respetivos URL e anexos (E2 e E4).

Associado ainda ao desconhecimento dos colaboradores, muitas pessoas consideram que as realidades onde se inserem estão perfeitamente separadas, ou seja, consideram que, por exemplo, o seu *e-mail* pessoal é completamente alheio às suas redes sociais. Contudo, isto não se verifica atualmente pois todas as realidades estão interligadas, pelo que o ataque a um dos vetores muito rapidamente pode ser escalado para outros. Neste sentido, não adianta ter o máximo de zelo com um dos vetores, se o mesmo não for feito com os restantes. (E7)

Para além do desconhecimento, mencionado acima, são várias as características intrínsecas às pessoas que as levam a cometer erros que acentuam o fator de risco nas organizações e, por serem intrínsecas, acredita-se que não mudem (E1). Estas são algumas das características identificadas pelos entrevistados: curiosidade (E1), distração (E1 e E3), necessidade de protagonismo (E2), disponibilidade para ajudar (E6), obediência a hierarquias (E6), dificuldade em avaliar o risco (E3) e rápida penalização a quem questione ou coloque dúvidas (E6).

4.3. Consequências dos comportamentos humanos

Para além dos comportamentos acima apresentados, os ataques de engenharia social encontram-se cada vez mais aperfeiçoados, o que se traduz em consequências bastante prejudiciais para as organizações (E1, E3 e E4). Estas poderão variar consoante a dimensão, modelo de negócio e mercado onde se insere a organização (E1).

Algumas das consequências resultantes dos comportamentos humanos são: danos reputacionais à organização (E1 e E2), perdas financeiras (E1, E2 e E6), paragem temporária ou definitiva da organização (E1), perda de quota de mercado (E1), perda de informações (E2, E3 e E6) e incumprimentos legais ou normativos (E6). De forma generalizada, todas estas consequências comprometem a integridade, disponibilidade e confidencialidade dos sistemas da informação (E5). Atualmente, as consequências que mais preocupam as organizações são aquelas que estão relacionadas com o

incumprimento da lei como, por exemplo, penalizações financeiras e paragem da organização temporariamente ou definitivamente (E6).

4.4.Soluções para corrigir os comportamentos humanos

"A cultura de cibersegurança aparece naturalmente em organizações que já têm uma cultura de gestão estruturada do risco. (…) Se não existir esta cultura estruturada, qualquer risco será sempre tratado de forma *ad-hoc*, quando é identificado ou se materializa (tipicamente é tratado tardiamente e de forma reativa)." (E6)

É de extrema importância para as organizações ter uma cultura de cibersegurança sólida (E3, E4 e E7) pois "torna a organização mais robusta e menos vulnerável, ainda que não exista cem por cento de segurança e alguns erros sejam sempre cometidos" (E1). Para que funcione corretamente, a cultura de cibersegurança deverá envolver todos os elos da cadeia, desde o *C-level*, passando por todos os departamentos da organização (E1 e E2). Atualmente, verifica-se a inexistência de uma cultura de cibersegurança sólida em muitas organizações em Portugal, associado a baixos níveis de maturidade. Contudo, existem exceções, pelo que algumas organizações já refletem a existência de uma cultura de cibersegurança sólida, aproximando-se da sua maturidade total (E5).

Como mencionado anteriormente, o desconhecimento está na origem de grande parte dos erros cometidos, onde a sensibilização é uma das soluções (E1). Deste modo, a consciencialização dos colaboradores é uma das principais linhas de defesa das organizações (E6). Contudo, tal como na cultura de cibersegurança, o nível de consciencialização dentro das organizações é muito reduzido, ainda que existam exceções (E2, E3 e E6).

Para alcançar uma mudança duradoura é necessário sensibilizar os colaboradores e transmitir-lhes conhecimento de modo a que sejam criados bons hábitos, que serão também transferidos para a sua vida pessoal (E1 e E2). É importante que estes conhecimentos sejam "reciclados", ou seja, são necessários *add-ons* à informação que é transmitida ao longo das ações de sensibilização e formação. Estes complementos devem ser feitos à medida que os desafios vão surgindo, de modo a incrementar o conhecimento dos colaboradores dentro das organizações, mantendo as pessoas atualizadas e preparadas para os riscos a que estão sujeitas. Caso contrário, se os colaboradores das várias camadas

da organização não estiverem sensibilizados com o tema e se não tiverem o conhecimento suficiente dos perigos que os rodeiam e das consequências das suas ações ou inações, o nível de maturidade de cibersegurança da organização nunca evoluirá positivamente. (E2, E6 e E7)

Numa fase inicial, os colaboradores olharão para algumas medidas de segurança como uma obrigação, tal como acontece com todos os novos hábitos que são incutidos no seu quotidiano. Contudo, as organizações, têm a obrigação de não impor apenas regras aos seus colaboradores, mas também de explicar as razões das medidas a seguir, de forma a garantir uma mudança duradoura (E5 e E6). É neste aspeto que muitas organizações falham atualmente (E6).

Para além disso, "o nível de literacia em cibersegurança não deveria ser apenas responsabilidade das organizações, mas também do Estado" (E5). Neste sentido, a educação em cibersegurança nas escolas é de extrema importância (E2, E3 e E7). Este será um dos pontos de partida para a criação de uma cultura de cibersegurança sólida (E2). Contudo, atualmente não existe uma valorização da literacia em cibersegurança, principalmente em idades mais jovens (E5), o que deveria estar a acontecer devido à introdução de tecnologias nas atividades das crianças desde muito cedo (E7). Para além disso, quanto mais jovens forem as pessoas, mais recetivas estarão a receber novas informações e conhecimento, o que poderia ser aproveitado para despertar a atenção das mesmas para este tema tão importante na sociedade (E2 e E7).

Importa ainda salientar que, quanto mais protegida estiver uma organização, menor é a probabilidade de esta ser atacada, ainda que essa possibilidade exista sempre. Nesse sentido, se olharmos para o cibercrime como um negócio, os cibercriminosos têm como objetivo maximizar o lucro do seu trabalho. Ou seja, quanto mais protegida estiver uma organização, mais difícil será atacar a mesma e, consequentemente, mais recursos terão de ser imputados para tornar aquele ataque bem-sucedido. Neste sentido, a organização torna-se menos aliciante para os cibercriminosos, que tentarão atacar outras organizações menos protegidas e, por conseguinte, mais rentáveis. Ainda assim, não podem ser esquecidos os ciberataques que têm como objetivo atacar uma determinada organização em concreto. Nesse caso, ainda que a tarefa dos cibercriminosos seja dificultada, eles têm uma motivação superior para causar danos nessa mesma organização

e, por isso, procurarão qualquer falha que exista na cibersegurança dessa organização para conseguirem atacá-la (E6). Neste sentido, é de extrema importância garantir que as pessoas têm conhecimento suficiente em cibersegurança. Assim, as organizações que procuram consciencializar e formar os seus colaboradores estão mais seguras do que aquelas que não transmitem conhecimento suficiente, nem sensibilizam os seus colaboradoes. Em suma, cada organização deve ser suficientemente melhor do que as suas concorrentes no que toca à cibersegurança, de modo a aumentar as possibilidades de serem as organizações concorrentes a serem alvo de ataques e a reduzir a probabilidade de ataque à própria organização por se encontrar mais protegida. (E7)

Ainda que a prevenção seja de extrema importância para a cibersegurança, na maioria dos casos as organizações estão a "correr atrás do prejuízo", no que toca a este tema (E1, E2, E5 e E7). Ou seja, é necessário acontecerem os ataques para surgirem as soluções (E7). Isto deve-se ao facto de se tratar de um modelo permanentemente evolutivo e assimétrico ao nível do risco. Por outras palavras, os cibercriminosos não respeitam qualquer tipo de regras ou legislação para alcançarem os seus fins e vão sempre aperfeiçoando as suas técnicas, enquanto que quem está do lado da cibersegurança respeita os padrões éticos e obrigatórios por lei, agindo em defesa desses mesmo ataques (E5). Contudo, ainda que sempre a "correr atrás do prejuízo", deve-se lutar pela antecipação de cenários, como forma de minimizar os danos em caso de ataque (E7).

4.5.Desafios da cibersegurança nas organizações

Ainda que todos os aspetos da cibersegurança sejam de extrema importância, alguns pontos foram destacados com maior preocupação por parte dos entrevistados. Desta forma, alguns tópicos chave foram identificados como desafios da atualidade que terão de ser tidos em conta e ultrapassados no futuro.

Em primeiro lugar, o facto de diversas questões de cibersegurança continuarem a ser descuradas, assim como alguns processos de gestão de risco, é uma das grandes preocupações da atualidade, o que revela que a sociedade não está suficientemente sensibilizada para este tipo de questões (E1 e E6). Neste sentido, o desafio que se impõem para o futuro é a criação de uma cultura de cibersegurança sólida através da

consciencialização, formação e educação dos colaboradores, permitindo-lhe estar a par dos desafios, em vez assumir um papel reativo (E2, E5 e E7).

Associado a este aspeto, muitas das pessoas consideram que nunca serão atacadas, nem as organizações onde se inserem. Este é um pensamento errado que assume que as organizações de dimensão mais reduzida ou de determinado setor de atividade não são aliciantes para os atacantes. Contudo, atualmente, as ferramentas utilizadas nos ciberataques procuram falhas e exploram-nas assim que as encontram, sendo por isso transversais à pessoa ou organização em causa. Neste sentido, todas as organizações estão sob risco de ataque, independentemente da sua dimensão ou qualquer outra característica. Face a esta realidade, o desafio que se impõem é que todas as organizações têm de estar igualmente bem protegidas. (E7)

Em simultâneo, a tecnologia nos últimos anos tem evoluído a uma velocidade exponencial e espera-se que continue a registar elevadas taxas de crescimento. Neste sentido, as pessoas não se prepararam para acompanhar o ritmo de mudança digital a que são expostas (E3, E4 e E7) e, para além disso, a tecnologia está cada vez mais presente no dia a dia das pessoas, que muitas das vezes menosprezam os riscos em prol dos benefícios aparentes da tecnologia (E5 e E6). Neste sentido, acredita-se que esta atitude perante as tecnologias resulte de uma má avaliação do risco, pois trata-se de uma área que é difícil de avaliar através dos sentidos humanos, pelo que as pessoas não se apercebem da sua complexidade, nem do valor associado às informações nelas armazenadas. Neste caso, o desafio é garantir que as pessoas têm o conhecimento necessário e que se encontram suficientemente sensibilizadas, estando desta forma preparadas para a evolução tecnológica vindoura (E7).

Por fim, com a crescente competitividade dos mercados, a boa gestão dos orçamentos é uma prioridade. Neste sentido, é imperativo que a gestão de topo tenha as informações necessárias e conhecimento para entender os riscos a que a organização está exposta e as consequências a que está sujeita, de modo a investir na cibersegurança de acordo com as necessidades da organização. Por outras palavras, espera-se que a gestão de topo veja a cibersegurança como uma mais valia e não apenas como um custo. Neste sentido, a preocupação é garantir que a gestão de topo se encontra sensibilizada e tem o conhecimento e informação necessários de modo a poder assegurar que o departamento

de cibersegurança da organização tem os recursos necessários à sua disposição para garantir a cibersegurança da mesma. (E4, E5, E6 e E7)

5. DISCUSSÃO

Segundo Raposo (2016), baseado em McCumber (2004), a cibersegurança deve ser vista como um conjunto de sinergias entre os três fatores estruturais das organizações: pessoas, processos e tecnologia. Contudo, muitas organizações não veem a cibersegurança desta forma, mas apenas como uma área relativa à tecnologia, descurando a importância dos restantes fatores, de entre os quais, as pessoas (E1, E2, E4, E5 e E7).

O autor Morgan (2017) afirma que a tecnologia está cada vez mais presente na vida das pessoas. Contudo, os entrevistados afirmam que as pessoas não se prepararam de modo a conseguir acompanhar o ritmo de mudança digital a que são expostas diariamente (E3, E4 e E7). Esta falta de preparação, associada à existente dependência pela tecnologia, representa uma grande vulnerabilidade para as organizações (Winnefeld et al., 2015).

Apesar de a literatura afirmar que o fator humano é o elo mais fraco da cadeia de cibersegurança (Hadlington, 2017; Mitnick & Simon, 2003; Ponemon Institute, 2016), alguns entrevistados mostraram não estar totalmente de acordo com a afirmação pois consideram que a tecnologia também apresenta diversas vulnerabilidades, até porque está dependente das pessoas para ser desenvolvida e implementada. Nesse sentido, afirmaram que o fator humano é um dos elos mais vulneráveis de uma organização, mas não é o único (E1 e E6). Por outro lado, outros entrevistados mostram plena concordância com o facto de o fator humano ser o elo mais fraco de uma organização no que toca à cibersegurança (E2, E3, E4 e E7). Em suma, apesar nem todos estarem de acordo com o tema, todos concordam que os colaboradores deverão ser uma das maiores preocupações das organizações no que toca à cibersegurança, representando uma grande vulnerabilidade das mesmas.

No relatório da Proofprint (2019) é indicado que a engenharia social se encontra cada vez mais eficaz e difundida, pelo que as organizações devem estar cada vez mais atentas a este método de ataque, o que está em total concordância com o ponto de vista

dos entrevistados (E1, E3 e E4). Neste sentido, pode-se concluir que as técnicas que visam explorar as vulnerabilidades humanas se encontram cada vez mais aperfeiçoadas, pelo que, mais uma vez, a preocupação com os colaboradores deve ser uma premissa obrigatória dentro das organizações, pois este é um dos principais alvos dos cibercriminosos.

Apesar de existir uma ideia errada de que apenas as organizações de grandes dimensões são alvo de ataque, a literatura defende que as organizações de pequenas dimensões se tornam mais lucrativas para os cibercriminosos por estarem precariamente preparadas para se defenderem. Neste sentido, todas as organizações são potenciais alvos de ataque para os cibercriminosos, independentemente da sua dimensão ou setor de atividade (Baptista, 2017; Proofprint, 2019; Symantec, 2016). Contudo, o entrevistado E7 revelou que muitas organizações não estão cientes dessa realidade. Estas continuam presas à falácia de que as organizações de pequenas dimensões não são atacadas por não serem suficientemente atrativas para os cibercriminosos. Assim, importa sensibilizar todas as pessoas de modo a que tenham consciência de que todos estão em risco, independentemente das características das organizações onde se inserem.

O CERT (2014) defende que a probabilidade de uma organização sofrer um ciberataque é tanto maior quanto menor for o conhecimento em cibersegurança dos colaboradores. Ora, com base nas respostas dos entrevistados, pode-se concluir que várias organizações em Portugal estão sujeitas a sofrer um ou vários ciberataques, pois os seus colaboradores apresentam elevados níveis de desconhecimento relativamente à cibersegurança. Deste modo, a existência de diversas ações de formação, consciencialização e educação é fundamental para proteger as organizações.

Adicionalmente, a literatura defende que cada colaborador deve agir como um sensor, de modo a prevenir, detetar e reagir a eventuais ataques que possam surgir contra a organização (Martins et al., 2016). Deste modo, espera-se que exista uma cultura de cibersegurança sólida, onde as preocupações com cibersegurança sejam parte integrante do trabalho quotidiano de todos os colaboradores (ENISA, 2017). Para isso, processos de consciencialização, formação e educação dos colaboradores são fundamentais para tornar as organizações mais resilientes (Baptista, 2017). Apesar dos entrevistados estarem em concordância com a literatura, a realidade que estes identificam é que o nível existente de

cultura de cibersegurança de muitas organizações em Portugal continua a ser muito inferior àquele que seria esperado, pelo consideram que estas se encontram muito vulneráveis (E1, E2, E3, E4, E5, E6 e E7). Deste modo, muitas organizações portuguesas acabam por ter um papel reativo no que toca à cibersegurança, enquanto que o ideal seria assumirem um papel preventivo (E1, E2, E5 e E7). Em suma, as organizações ainda têm um longo caminho a percorrer de forma a atingir uma cultura de cibersegurança sólida. Neste percurso, as pessoas serão, mais uma vez, estritamente indispensáveis para o alcance deste objetivo, pelo que é fundamental que estas tenham o conhecimento necessário para poder contribuir para a cibersegurança da organização.

Relativamente à gestão de topo, verifica-se uma plena concordância entre a revisão da literatura e a opinião dos entrevistados (E1, E3, E4, E5, E6 e E7). Segundo a ENISA (2017), a gestão de topo tem um papel fundamental na cibersegurança de uma organização. Isto deve-se ao facto de ser esta entidade que está responsável pela definição da estratégia da organização e dos respetivos orçamentos para cada área. Desta forma, é fundamental sensibilizar a gestão de topo para a importância inerente à cibersegurança, de modo a que seja criado um comprometimento com a mesma. Assim, espera-se que a gestão de topo inclua a cibersegurança na estratégia da organização e que aloque recursos suficientes a este departamento. Contudo, no relatório da AP2SI (2016), verifica-se que, na realidade, isto não acontece. A gestão de topo encontra-se extremamente focada no *core business*, pelo que destina valores residuais do orçamento total da organização para a cibersegurança, o que faz com que exista uma grande escassez de recursos nesta área. Sabendo de antemão que grande parte do tecido empresarial português é constituído por PMEs e por microempresas, os entrevistados E1 e E3 referiram que a gestão de topo se resume, em muitos casos, a uma única pessoa, que muitas das vezes não tem conhecimento, nem competências suficientes em cibersegurança para se sentir minimamente sensibilizada com o assunto. Em suma, a gestão de topo, representa um papel crucial na cibersegurança das organizações, contudo nem sempre tem noção dessa sua responsabilidade, nem dos riscos que a rodeiam.

Por fim, os entrevistados revelaram que as organizações portuguesas apresentam níveis de maturidade de cibersegurança muito baixos, ainda que existam algumas exceções (E3, E4 e E5). No caso das organizações de grandes dimensões, estas encontram-se mais sensibilizadas para o tema, contudo, mesmo nestes casos, o nível de

maturidade de cibersegurança destas organizações encontra-se abaixo do esperado (E5). Já no caso das organizações de pequenas dimensões, ainda que apresentem um aumento da perceção do risco relacionado com cibersegurança, este não é acompanhado pela prática (E1, E2, E3, E4, E5, E6 e E7). Nestes casos, o nível de maturidade em cibersegurança é muito reduzido. Assim, a consciencialização, formação e educação dos colaboradores são fundamentais para que exista um crescimento dos níveis de maturidade de cibersegurança nas organizações (E2, E6 e E7). Desta forma, com base na literatura, espera-se que os níveis de cibersegurança evoluam continuamente, desde uma fase muito inicial, até atingirem um nível bastante elevado, não esquecendo que devem garantir que se atualizam constantemente face à atualidade (Barclay, 2014; Christopher, 2018; IEEE, s.d.).

Em suma, conclui-se que, na maioria dos casos, a opinião dos entrevistados vai de encontro à literatura existente. Contudo estes revelaram que a realidade da cibersegurança das organizações portuguesas se encontra bastante atrasada face àquilo que seria esperado, pelo que existe muito trabalho pela frente na maioria das organizações portuguesas até atingirem uma cultura de cibersegurança sólida.

6. CONCLUSÕES

Neste capítulo são apresentadas as principais conclusões desta dissertação. Para além disso, também são identificados os principais contributos deste trabalho, assim como as suas respetivas limitações e sugestões de investigação futura.

6.1. Principais conclusões

Nos últimos anos, a tecnologia tem registado elevadas taxas de crescimento e espera-se que essa tendência se mantenha nos próximos anos. Contudo, a sociedade não se preparou para as mudanças associadas a este crescimento, ainda que esteja cada vez mais dependente da tecnologia, o que a torna as pessoas ainda mais vulneráveis. Essa vulnerabilidade faz com que o fator humano seja o principal alvo dos ciberataques.

Atualmente, as pessoas não estão suficientemente preparadas nem são suficientemente incluídas nas políticas de cibersegurança das organizações, pelo que

muitas questões de cibersegurança continuam a ser descuradas, sendo o desconhecimento e a falta de sensibilização os maiores problemas inerentes às pessoas. Deste modo, as organizações devem olhar para a cibersegurança como um conjunto de sinergias e não apenas como uma questão tecnológica, pelo que devem incluir as pessoas nas suas políticas de cibersegurança. Desta forma, quanto mais os colaboradores estiverem preparados, mais resiliente será a organização. A par disso, importa informar e sensibilizar a gestão de topo, de modo a existirem políticas direcionadas para a cibersegurança e para que sejam alocados recursos suficientes para garantir a segurança da organização.

Neste momento, as organizações portuguesas apresentam um longo caminho a percorrer de forma a aumentar o seu nível de maturidade em cibersegurança. Neste sentido, espera-se que todas as organizações evoluam continuamente e que garantam que estão constantemente atualizadas face aos desafios da atualidade. Assim, a consciencialização, a formação e a educação surgem como soluções, no sentido de se estabelecer uma cultura de cibersegurança sólida. Desta forma, a prevenção revela-se como uma das principais soluções pois quanto mais protegida estiver uma organização, menor é a probabilidade de esta ser vítima de um ciberataque. Nesse sentido, espera-se que as organizações passem a assumir um papel maioritariamente preventivo, sendo, por isso, cada vez menos reativo.

É ainda de salientar que existem exceções, pelo que existem organizações que se distinguem pelas boas práticas de cibersegurança e pela boa preparação dos seus colaboradores. No entanto, não existem soluções infalíveis, pelo que existe sempre a possibilidade de melhoria.

Em suma, pode-se concluir que o fator humano tem uma grande influência e, consequentemente, importância, na cibersegurança das organizações. Deste modo, tanto as suas ações, como inações, têm um grande impacto nos níveis de cibersegurança alcançados. Assim sendo, a solução que permite obter uma mudança duradoura é a criação de uma cultura de cibersegurança sólida, que pode ser alcançada através da consciencialização, formação e educação dos colaboradores.

6.2.Contributos

Este trabalho foi desenvolvido com o objetivo de ter um contributo tanto numa vertente técnica, como numa ótica prática. A nível técnico, procurou-se aprofundar o estudo do fator humano da cibersegurança nas organizações, apresentando conceitos teóricos e o cenário atual desta área de estudo, com base em referências bibliográficas fidedignas e em entrevistas a peritos e investigadores em cibersegurança. Relativamente à vertente prática deste trabalho, espera-se que este consiga transmitir conhecimento e sensibilizar a sociedade para a importância da cibersegurança, contribuindo para uma mudança de comportamentos e mentalidades em prol de uma cultura de cibersegurança sólida.

6.3.Limitações do estudo

Este trabalho apresenta algumas limitações que importam ser referidas, ainda que se considere que os objetivos do trabalho tenham sido alcançados com sucesso.

Em primeiro lugar, os dados recolhidos nas entrevistas e analisados posteriormente dizem respeito a uma apreciação dos especialistas na atualidade. Ainda que sejam dadas perceções de evoluções, quer positivas, quer negativas, por parte dos mesmos, seria mais conclusivo fazer recolhas de dados em dois momentos temporais suficientemente distantes, de modo a averiguar as diferenças existentes nas respostas dadas às mesmas perguntas.

Em segundo lugar, importa salientar que os dados recolhidos se baseiam em opiniões e perceções de peritos e investigadores em cibersegurança e que apenas é analisado o seu ponto de vista, o que, de certa forma, poderá tornar as respostas mais homogéneas por terem origem num grupo que também ele é homogéneo, devido às suas características. Desta forma, os dados recolhidos transmitem as perceções de um grupo em específico, não incluindo opiniões de grupos que representam um papel diferente na cibersegurança das organizações, como é o caso dos próprios colaboradores. Isto permitiria ter uma visão mais abrangente das diferentes interpretações existentes relativamente à cibersegurança e ao próprio fator humano.

Por fim, o facto de se ter seguido uma abordagem qualitativa, não possibilita a realização de inferência estatística devido ao elevado volume de dados recolhidos nas entrevistas. Para além disso, as perguntas de resposta aberta levaram, ainda que em poucos casos, a respostas inconclusivas.

6.4.Investigação futura

Com base no trabalho desenvolvido, surgiram novas ideias e sugestões para trabalhos futuros. Em muitos dos casos, estes poderão ser complementares ao trabalho atual, permitindo uma comparação posterior.

Em primeiro lugar, sugere-se a elaboração de um estudo semelhante, noutro momento temporal para que possa ser feita uma comparação entre diferentes momentos, podendo-se retirar padrões e perceber evoluções entre diferentes períodos temporais.

Em segundo lugar, considera-se pertinente efetuar o mesmo tipo de estudo noutros países, com diferentes culturas e diferentes graus de desenvolvimento de modo a compreender as discrepâncias entre países e a forma como o fator humano da cibersegurança é considerado a nível mundial.

Em terceiro lugar sugere-se que seja elaborado um estudo com uma linha de raciocínio idêntica, contudo que procure compreender o ponto de vista da gestão de topo e dos colaboradores de diferentes departamentos e com diferentes graus de responsabilidade nas organizações, de modo a obter o ponto de vista das pessoas que constituem as organizações.

Por outro lado, seria interessante seguir a mesma ideia de estudo em organizações de diferentes setores de atuação. Desta forma, seria possível averiguar quais os setores que estão mais cientes da importância do fator humano da cibersegurança, apresentando um maior nível de maturidade de cibersegurança.

Ainda na mesma linha de raciocínio, seria de elevado interesse contrastar grandes empresas com pequenas e microempresas, no sentido de avaliar as diferentes perceções existentes relativamente à importância do fator humano da cibersegurança entre organizações de diferentes dimensões.

Por outro lado, seria interessante estudar isoladamente uma ou várias organizações. Deste modo, era possível identificar e estudar de perto os comportamentos humanos, as suas características intrínsecas, o impacto destes mesmos comportamentos e as respetivas soluções implementadas nas organizações.

Por fim, sugere-se que, em complementaridade ao presente trabalho, se estude a relação das pessoas com a cibersegurança numa perspetiva pessoal e não organizacional. Neste sentido, espera-se que, ao cruzar-se os dois trabalhos, se possa aferir se a cultura de cibersegurança nas organizações se torna algo inerente às pessoas, transpondo-se para a sua vida privada e integrando o seu quotidiano.

REFERÊNCIAS BIBLIOGÁFICAS

Amado, J., & Ferreira, S. (2013). A entrevista na investigação educacional. Manual de Investigação Qualitativa em Educação (pp. 207-232). Coimbra: Imprensa da Universidade de Coimbra.

AP2SI. (2016). *Inquérito à Segurança da Informação nas Instituições em Portugal*, 1ª edição. Disponível em: https://ap2si.org/iniciativas-ap2si/inquerito/resultados-2015/.

Bada, M., Sasse, A. M., & Nurse, J. R. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, (pp.118-131). Disponível em: https://www.researchgate.net/publication/274663655_Cyber_Security_Awareness_Campaigns_Why_do_they_fail_to_change_behaviour

Baptista, I. M. (2017). *O fator humano na cibersegurança* (Dissertação de Mestrado). Instituto Superior Técnico, Lisboa.

Barclay, C. (2014). Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM2). *Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world - Impossible without standards*, 275-282. Disponível em: https://www.semanticscholar.org/paper/Sustainable-security-advantage-in-a-changing-The-Barclay/437691631794fb21f6b2f3bb91f6880854293890.

Bardin, L. (2016). *Análise de Conteúdo* (L. Reto & A. Pinheiro ,Trad). São Paulo: Edições 70 (Obra originalmente publicada em 1977).

Batista, E. C., Matos, L. A., & Nascimento, A. B. (2017). A entrevista como técnica de investigação na pesquisa qualitativa. *Revista Interdisciplinar Científica Aplicada*, 11(3), 23-38. Disponível em: https://www.researchgate.net/publication/331008193_A_ENTREVISTA_COMO_TECNICA_DE_INVESTIGACAO_NA_PESQUISA_QUALITATIVA.

CA Technologies. (2018). *Insider Threat Report*. Disponível em: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-

report.pdf?fbclid=IwAR1QyfYJ74m4lIt-wGTQ0-CpbwQCbF0RP_IrsPLUoa6_elKQXwI6ikZpl-s.

CERT. (2013). *Unintentional Insider Threats: A Foundational Study*. Disponível em: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf

CERT. (2014). *Unintentional Insider Threats: Social Engineering*. Disponível em: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf

Christopher, J. (2018). *The Cybersecurity Maturity Model: A Means To Measure And Improve Your Cybersecurity Program*. Consultado em 25 de setembro de 2019. Disponível em: https://www.forbes.com/sites/forbestechcouncil/2018/11/01/the-cybersecurity-maturity-model-a-means-to-measure-and-improve-your-cybersecurity-program/#732e8bfa680b.

CNCS. (2019). *Quadro Nacional de Referência para a Cibersegurança*. Lisboa: Centro Nacional de Cibersegurança.

CNCS. (s.d.). *Glossário*. Consultado em 31 de agosto de 2019. Disponível em: https://www.cncs.gov.pt/recursos/glossario/

CNSS. (2015). *National Information Assurance Glossary*. Committee on National Security Systems. Disponível em: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, (pp. 13-21). Disponível em: https://www.researchgate.net/publication/267631801_Defining_Cybersecurity

Duarte, R. (2004). Entrevistas em pesquisas qualitativas. *Educar*, 24, 214-225. Disponível em: http://www.ia.ufrrj.br/ppgea/conteudo/T2-5SF/Sandra/Entrevistas%20em%20pesquisas%20qualitativas.pdf

ENISA. (2017). *Cyber Security Culture in Organisations*. Disponível em: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

EY. (2018). Is cybersecurity about more than protection? *EY Global Information Security Survey 2018–19*. Disponível em: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2018-19.pdf

Fernandes, J. P. (2012). Utopia, Liberdade e Soberania no Ciberespaço. *IDN Nação e Defesa*, (133), 11-32. Disponível em: https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf

Furnell, S. (2017). Security education and awareness: just let them burn? *Network Security*, 2017(12), 5-9. Disponível em: https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/10782/Security%20Education%20and%20Awareness%20-%20Just%20let%20them%20burn%3F%20-%20for%20PEARL.pdf?sequence=1&isAllowed=y

Furnell, S., & Clarke, N. (2005). Organisational Security Culture: Embedding Security Awareness, Education and Training. *Proceedings of the IFIP TC11 WG*, 11, 67-74. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.678.9294&rep=rep1&type=pdf

Gartner. (s.d.). *Internet of Things (IoT)*. Consultado em: 08 de setembro de 2019. Disponível em: https://www.gartner.com/it-glossary/internet-of-things/

Gaspar, F. (2018). *Ciber (in)segurança*. Consultado em: 02 de dezembro de 2018. Disponível em: https://www.youtube.com/watch?v=-6EDs5Vkz6w&feature=youtu.be

Gil, A. C. (2008). *Métodos e técnicas de pesquisa social* (6ª ed.). Editora Atlas SA. Disponível em: https://ayanrafael.files.wordpress.com/2011/08/gil-a-c-mc3a9todos-e-tc3a9cnicas-de-pesquisa-social.pdf

Greig, J. (2018). *Why human vulnerabilities are more dangerous to your business than software flaws*. Consultado em: 28 de março de 2019. Disponível em: https://www.techrepublic.com/article/why-human-vulnerabilities-are-more-dangerous-to-your-business-than-software-flaws/?fbclid=IwAR2zPlzFapkpG9k3pogjhRs5E0oYmOoKheERpwxAbPKUVtKCHUK-KkK97Rk

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7). Disponível em: https://www.researchgate.net/publication/318222445_Human_factors_in_cybersecurity_examining_the_link_between_Internet_addiction_impulsivity_attitudes_towards_cybersecurity_and_risky_cybersecurity_behaviours

Hadlington, L. (2018). The "Human Factor" in Cybersecurity: Exploring the Accidental Insider. *Psychological and Behavioral Examinations in Cyber Security* (pp. 46-63). IGI Global. Disponível em: https://www.dora.dmu.ac.uk/bitstream/handle/2086/15621/Hadlington%20-%202018%20-%20The%20%E2%80%9CHuman%20Factor%E2%80%9D%20in%20Cybersecurity.pdf?sequence=1&isAllowed=y&fbclid=IwAR2d0iQn_OOIeM0fCn3jTVsA-MY1pYj5mRcWIJ3ENqagXTgYzKwDTPM9jHo

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*, 3, 1117-1124. Disponível em: https://pdf.sciencedirectassets.com/306234/1-s2.0-S2351978915X00047/1-s2.0-S2351978915001870/main.pdf?X-Amz-Security-Token=AgoJb3JpZ2luX2VjEMX%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJHMEUCIQC5T3ws0Za%2FmkwX5s6SkNE1rWWgEM%2BGvehkiCxptmVEPgIgZMPNUFii

Hoffer, J., Venkataraman, R., & Topi, H. (2016). *Modern Database Management*. Harlow: Pearson.

IBM. (2017). *IBM X-Force Threat Intelligence Index 2017- The year of the mega breach*. IBM. Disponível em: http://branden.biz/wp-content/uploads/2017/06/IBM-X-Force-Threat-Intelligence-Index-20.pdf

IEEE. (s.d.). *What Is a Cyber Security Maturity Model?* Consultado em 29 de setembro de 2019. Disponível em: https://innovationatwork.ieee.org/what-is-a-cyber-security-maturity-model/

ITU. (2008). Recommendation ITU-T X.1205. *Series X: data networks, open system communications and security*. Disponível em: https://www.itu.int/rec/T-REC-X.1205-200804-I

Kajava, J., & Siponen, M. (2002). IT Security Awareness - Issues for Industry. *European Intensive Programme on Information and Communication Technologies Security*. Disponível em: https://www.researchgate.net/publication/267794563_IT_Security_Awareness_-Issues_for_Industry

Kothari, C. R. (2004). *Research Methodology - Methods and Techniques* (2º ed.). New Age International Publishers. Disponível em: http://www.modares.ac.ir/uploads/Agr.Oth.Lib.17.pdf

Leite, A. M. (2016). A problemática da cibersegurança e os seus desafios. *CEDIS Working Papers Direito, Segurança e Democracia*, 49, 1-22. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2017/10/CEDIS-working-paper_DSD_A-problem%C3%A1tica-da-ciberseguran%C3%A7a-e-os-seus-desafios.pdf

Leocádio, A. R. (2017). Segurança cibernética, pessoas, empresas e governos. Precisamos muito falar sobre isso. *Cibersegurança: educação digital e proteção de dados*(18), 66. Disponível em: https://www.prodemge.gov.br/images/com_arismartbook/download/22/revista_18.pdf

Martins, J., Silva, J., Pimentel, C., Galindro, A., & Rocha, J. (2016). Sensibilização e Treino em Cibersegurança: Exercício de Recolha de Informação. *Proelium*, 7(10), 141-160. Disponível em: https://revistas.rcaap.pt/proelium/article/view/8919

Matos, P. C. (2018). *Cibersegurança: Políticas Públicas para uma Cultura de Cibersegurança nas Empresas* (Dissertação de mestrado). ISCTE, Lisboa. Disponível em: https://repositorio.iscte-iul.pt/bitstream/10071/17630/1/Master_Pedro_Abreu_Matos.pdf

McCumber, J. (2004). *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*. Auerbach Publications.

Microsoft. (s.d.). *What is the cloud?* Consultado em 08 de setembro de 2019. Disponível em: https://azure.microsoft.com/en-us/overview/what-is-the-cloud/

Minayo, M. C. (2010). *O Desafio do Conhecimento: pesquisa qualitativa em saúde*. Hucitec.

Mitnick, K. D., & Simon, W. L. (2003). *A Arte de Enganar* (K. Roque, Trad.). São Paulo: Pearson Education. Disponível em: https://www.docdroid.net/Mq0Edkm/kevin-mitnick-a-arte-de-enganar.pdf

Monzelo, P. M. (2018). *A função do chief information security officer nas organizações*. ISEG, Lisboa. Disponível em: https://www.iseg.ulisboa.pt/aquila/getFile.do?fileId=1194717&method=getFile

Morgan, S. (2017). *2017 Cybercrime Report*. Disponível em: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Nobles, C. (2018). *Shifting the Human Factors Paradigm in Cybersecurity*. Disponível em: https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/17.pdf?fbclid=IwAR33Nc2VSx169p9GkvXZjKAXJFwRtTJvFQu1w5xjRjOPjKMzdcsbmhsVyfo

Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Guidelines for Usable Cybersecurity: Past and Present. *Proceedings - Third International Workshop on Cyberspace Safety and Security (CSS)* (pp. 21-26). IEEE. Disponível em: https://www.researchgate.net/publication/224264159_Guidelines_for_usable_cybersecurity_Past_and_present

O'Brien, T. L. (2005). *Gone Spear-Phishin'*. Consultado em 28 de março de 2019. Disponível em: https://www.nytimes.com/2005/12/04/business/yourmoney/gone-spearphishin.html

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*, 14(2), 37-49. Disponível em:

https://pdfs.semanticscholar.org/d4e4/0602cbf1eaaffc69bccf6af1e5f4745624c2.pdf?_ga=2.36561576.988920864.1562013352-465508998.1530045649

Ponemon Institute. (2012a). *Future State of IT Security: a Survey of IT Security Executives*. Disponível em: https://www.ponemon.org/local/upload/file/Future_state_of_IT_Security_FINAL%207.pdf

Ponemon Institute. (2012b). *The Human Factor in Data Protection*. Disponível em: https://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf

Ponemon Institute. (2016). *Managing Insider Risk through*. Disponível em: https://www.experian.com/assets/data-breach/white-papers/experian-2016-ponemon-insider-risk-report.pdf

Prodemge. (2017). Cibersegurança: educação digital e proteção de dados. *Fonte* (18), 3. Disponível em: https://www.prodemge.gov.br/images/com_arismartbook/download/22/revista_18.pdf

Proofprint. (2019). *Human Factor Report*. Disponível em: https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-r-human-factor-2019_0.pdf

Raposo, R. G. (2016). *Gestão do risco e garantia da informação: a influência do fator humano e da ética na segurança da informação e cibersegurança nas organizações* (Dissertação de Mestrado). Universidade de Lisboa, Lisboa. Disponível em: https://fenix.tecnico.ulisboa.pt/downloadFile/563345090415169/19122016%20Rogerio%20Raposo%20-%20Dissertacao.pdf

Riek, M., Bohme, R., & e Moore, T. (2016). Measuring the Influence of Perceived Cybercrime. *IEEE Transactions on Dependable and Secure*, 13(2), 261-273. Disponível em: https://ieeexplore.ieee.org/abstract/document/7056466

Rouse, M. (2017). *Black hat*. Consultado em 05 de janeiro de 2019. Disponível em: https://searchsecurity.techtarget.com/definition/black-hat

Santos, S. I. (2018). *Estudo das Perceções de Cibersegurança e Cibercrime e das Implicações na Formulação de Políticas Públicas* (Dissertação de Mestrado). Universidade de Lisboa, Lisboa. Disponível em: https://www.researchgate.net/publication/328612737_Estudo_das_Percecoes_de_Ciberseguranca_e_Cibercrime_e_das_Implicacoes_na_Formulacao_de_Politicas_Publicas

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security* , 8(1), 31-41. Disponível em: https://www.researchgate.net/publication/220208245_Siponen_M_A_conceptual_foundation_for_organizational_information_security_awareness_Information_Management_Computer_Security_81_31-41

Siponen, M. (2001). Five Dimensions of Information Security Awareness. *SIGCAS Computers and Society*, 31(2), 24-29. Disponível em: https://www.researchgate.net/publication/228702672_Five_dimensions_of_information_security_awareness

Strawser, B. J., & Jr., D. J. (2015). Cyber Security and user responsability: surprising normative differences. *Procedia Manufacturing*, *3, 1101-1108*. Disponível em: https://www.sciencedirect.com/science/article/pii/S2351978915001845

Symantec. (2016). *Attackers Target Both Large and Small Businesses*. Disponível em: https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf

Vala, J. (1986). A análise de conteúdo. Em A. S. Silva, & J. M. Pinto, *Metodologia das Ciências Sociais* (pp. 101-128). Porto: Edições Afrontamento. Disponível em: https://vdocuments.site/a-analise-de-conteudo-jorge-valapdf-577e182d2e307.html

Wilson, M., & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. *NIST Special publication*, 800(50), 1-39. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf?fbclid=IwAR2uKREyf2zVPYr4qJ96aj58U99UJv1cKWtTBFXcRWPhpDkXZK93OFcunGo

Winnefeld, J. A., Kirchhoff, C., & Upton, D. M. (2015). Cybersecurity's Human Factor: Lessons from the Pentagon. *Harvard Business Review*, 86–95. Disponível em: https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon?fbclid=IwAR2zPlzFapkpG9k3pogjhRs5E0oYmOoKheERpwxAbPKUVtKCHUK-KkK97Rk

Woerner, R. (2012). *Cybersecurity education* vs. cybersecurity training. Consultado em 25 de setembro de 2019. Disponível em: https://searchsecurity.techtarget.com/magazineContent/Cybersecurity-education-vs-cybersecurity-training

Zafra, D. E., Pitcher, S. I., Tressier, J. D., & Ippolito, J. B. (1998). Information Technology Security Training Requirements: A Role- and Performance- Based Model. *NIST Special Publication 800-16*. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

ANEXOS

Anexo 1 - Guião da entrevista detalhado

Relacionado com	Objetivo das perguntas	Perguntas orientadoras	Perguntas de recurso	Referências
Tema em geral: cibersegurança e fator humano	Relacionar Cibersegurança com fator humano no contexto organizacional.	Atualmente, considera que as organizações se preocupam com a cibersegurança tal como deveriam?	Considera que as organizações olham para a cibersegurança como uma sinergia entre pessoas, processos e tecnologia?	CA Technologies (2018),CERT (2013), ENISA (2017), Hadlington (2017, 2018), Henshel et al. (2015), Mitnick & Simon (2003), Ponemon Institute (2012a, 2016), Raposo (2016) baseado em McCumber (2004),
			Considera que as pessoas estão conscientes do risco a que estão expostas?	
		De que forma as organizações têm relacionado as suas políticas de cibersegurança com os colaboradores? São considerados como uma das maiores preocupações?	Considera que o fator humano é o elo mais fraco de uma organização no âmbito da cibersegurança?	
Primeira questão de investigação	Compreender quais os comportamentos e características humanos que influenciam os níveis de cibersegurança alcançados nas organizações.	Quais os comportamentos cometidos mais frequentemente pelas pessoas que comprometem a cibersegurança das organizações?	Considera que as pessoas tendem a melhorar ou piorar os seus comportamentos no que toca à cibersegurança?	Baptista (2017), CERT (2013, 2014), Ponemon Institute (2012b), Proofprint (2019)
		Quais as características intrínsecas humanas que tornam as pessoas mais vulneráveis?		

Segunda questão de investigação	Compreender quais as consequências dos comportamentos humanos nos níveis de cibersegurança alcançados nas organizações.	Quais as principais consequências dos comportamentos humanos nas organizações?	Qual o impacto que a engenharia social e o phishing têm nas organizações atualmente?	CERT (2014), Mitnick & Simon (2003), Proofprint (2019)
		Quais das consequências indicadas geram maiores preocupações nas organizações?		
Terceira questão de investigação	Compreender quais as soluções para corrigir os comportamentos humanos que influenciam a cibersegurança nas organizações.	Qual é a sua opinião relativamente à cultura de cibersegurança?	Considera que uma cultura de cibersegurança sólida é uma das principais soluções para mitigar os problemas de cibersegurança relacionados com as pessoas?	AP2SI (2016), CERT (2014), ENISA (2017), Furnell (2017), Kajava & Siponen (2002), Martins et al. (2016), Peltier (2005), Proofprint (2019), Woerner (2012), Zafra et al. (1998)
		Qual é a sua opinião relativamente à consciencialização, formação e educação dos colaboradores em cibersegurança?	Existem outras soluções igualmente importantes para corrigir o comportamento humano?	
		Qual o nível de consciencialização dos colaboradores em cibersegurança considera existir atualmente nas organizações?		
		O que considera fundamental para conseguir uma mudança duradoura na cibersegurança das organizações?	Considera que a prevenção alguma vez estará um passo à frente do cibercrime?	
		Quais são as suas maiores preocupações no que toca ao fator humano da cibersegurança nas organizações?		

Fonte: elaboração própria com base em (Amado & Ferreira, 2013)