O FATOR HUMANO DA CIBERSEGURANÇA NAS ORGANIZAÇÕES

Rita Santos Gonçalves e Sérgio Nunes
Advance, ISEG - Lisbon School of Economics & Management
Rua do Quelhas 6, 1200-781 Lisboa, Portugal

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, o fator humano representa uma das maiores vulnerabilidades das organizações, pelo que é um dos principais alvos dos ciberataques. Nesse sentido, as organizações devem estar cada vez mais atentas à importância do fator humano 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 todo o fator humano. Deste modo, torna-se imperativo compreender a forma como o fator humano se relaciona com a cibersegurança das organizações.

PALAVRAS-CHAVE

Cibersegurança, Fator Humano, Organizações, Cultura de Cibersegurança, Consciencialização em Cibersegurança

1. INTRODUÇÃO

Com a tecnologia cada vez mais presente no quotidiano das pessoas, a cibersegurança torna-se uma premissa indispensável nos dias de hoje (Morgan, 2017). A cibersegurança define-se como "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). Esta 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. Desta forma, o fator humano deverá ser uma das maiores preocupações das organizações, até porque 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).

Assim, 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 artigo 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).

Desta forma, o objetivo principal deste trabalho é compreender qual a influência e importância que o fator humano tem na cibersegurança das organizações, através da identificação dos comportamentos e características do fator humano que influenciam a cibersegurança, do seu impacto nos níveis de cibersegurança alcançados e das soluções que permitem corrigir estas situações.

Por fim, o presente artigo encontra-se dividido em seis secções. A presente secção visa introduzir o tema em estudo. Na próxima secção é apresentada a revisão da literatura relativa ao fator humano da cibersegurança

das organizações. Na terceira secção é explicada a metodologia da investigação adotada. Esta é seguida por uma quarta secção, onde são apresentados os resultados da investigação feita. Na quinta secção, a revisão da literatura é contrastada com os resultados obtidos na investigação. Por fim, na sexta secção, são apresentadas as principais conclusões deste artigo.

2. FATOR HUMANO DA CIBERSEGURANÇA

Em primeiro lugar, importa definir o conceito de fator humano. Deste modo, considera-se fator humano um colaborador que não tem intenção maliciosa de prejudicar a organização e a sua cibersegurança, contudo acaba por colocar a organização em risco, 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.

2.1 Comportamentos e Características do Fator Humano

2.1.1 Comportamentos do Fator Humano

No que toca à cibersegurança, é fundamental ter em conta os comportamentos do fator humano (Baptista, 2017). Segundo o CERT (2013), existem quatro tipos principais de incidentes com origem no fator humano.

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

Em segundo lugar, o código malicioso é também identificado como um incidente relacionado com o fator humano. Neste caso, hackers (black hats) acedem a dados confidenciais da organização através de software malicioso (CERT, 2013). Algumas ações do fator humano 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, 2012).

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

Adicionalmente, as passwords representam ainda outro grande problema, onde o fator humano nem sempre segue 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, 2012).

2.1.2 Características do Fator Humano

Importa ainda compreender quais as características intrínsecas do fator humano que levam a muitos dos comportamentos que comprometem a cibersegurança das organizações, acima apresentados. Esta compreensão é fundamental para todos os processos de elaboração e aplicação de políticas de cibersegurança. (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 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 do fator humano, tais como: mau ambiente de trabalho, existência de pressão durante períodos de tempo prolongados e elevadas cargas de trabalho. Assim sendo, colaboradores que se encontrem mais expostos 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 do fator humano, 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 do fator humano, maior a probabilidade de a organização sofrer um ciberataque (CERT, 2014).

2.2 Consequências dos Comportamentos do Fator Humano

Os comportamentos e características do fator humano apresentados 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. Nestes casos, sendo que se trata de consequências dos comportamentos e características do fator humano, a origem dos ataques é, muitas das vezes, a engenharia social. (CERT, 2014)

2.3 Soluções para Corrigir os Comportamentos do Fator Humano

É importante salientar que não existe uma solução única para corrigir os comportamentos do fator humano, mas sim um conjunto de soluções, complementares entre si, que visam aumentar a segurança das organizações (AP2SI, 2016; Leocádio, 2017). Idealmente, cada colaborador deverá agir 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). Contudo, 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).

2.3.1 Cultura de Cibersegurança

Uma cultura de cibersegurança sólida é uma das principais soluções para mitigar os problemas de cibersegurança com origem no fator 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 dos colaboradores, 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 (ENISA, 2017).

2.3.2 Consciencialização em Cibersegurança

A consciencialização em segurança da informação, 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, 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 cibersegurança e aumentar a sua preocupação e sensibilização com estes temas (Furnell, 2017; Wilson & Hash, 2003).

2.3.3 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).

2.3.4 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).

3. METODOLOGIA DE INVESTIGAÇÃO

Tendo em conta o objetivo principal deste artigo, optou-se por se seguir uma abordagem de investigação qualitativa, de modo investigar em profundidade o objeto em estudo, alcançando uma maior compreensão do tema (Gil, 2008). Nesse sentido, foram realizadas entrevistas individuais para que se pudesse 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).

Para além disso, todos os entrevistados são peritos e/ou investigadores em cibersegurança, pois foi este o critério de seleção definido. Esta escolha foi baseada no facto de estas pessoas lidarem diariamente com o tema abordado, estando por isso sensibilizados e familiarizados com a matéria em estudo numa ótica profissional, pelo que as suas respostas foram baseadas no seu conhecimento teórico e experiência profissional.

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.

Na tabela 1 é apresentada uma listagem com os detalhes de todas as entrevistas realizadas para recolha de dados para o presente trabalho. Todas elas 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.

Tabela 1. Detalhes das entrevistas realizadas. Fonte: elaboração própria com base em (Monzelo, 2018)

Ordem	Código	Duração (aprox.)	Tipo
1	E1	60 minutos	Presencial
2	E2	45 minutos	Presencial
3	E3	60 minutos	Presencial
4	E4	30 minutos	Remota
5	E5	30 minutos	Presencial
6	E6	15 minutos	Escrita + Remota
7	E7	45 minutos	Remota

4. APRESENTAÇÃO DE RESULTADOS

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. Muitas não estão cientes de que a cibersegurança implica uma sinergia entre pessoas, processos e tecnologia, pelo que se concentram apenas na tecnologia, negligenciando a importância do fator humano na cibersegurança (E1, E2, E4, 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).

4.1 Comportamentos e Características do Fator Humano

O fator humano desempenha um papel fundamental dentro das organizações, contudo é considerado 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 do fator humano pois é ele quem os decide, utiliza, desenvolve e implementa. Este elevado nível de importância traduz-se num maior nível de vulnerabilidade (E6).

O desconhecimento do fator humano relativamente à cibersegurança é algo alarmante e que deve ser corrigido. Este desconhecimento leva a que o fator humano pratique diversos comportamentos que colocam em causa a cibersegurança das organizações. Alguns destes comportamentos são a partilha indevida de passwords (E1 e E3), a partilha de informações privadas (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 do fator humano, 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 ao fator humano que o 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 facilidade em julgar negativamente quem questiona ou coloca dúvidas (E6).

4.2 Consequências dos Comportamentos do Fator Humano

Para além dos comportamentos acima apresentados, os ataques de engenharia social encontram-se cada vez mais aperfeiçoados, traduzindo-se 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 do fator humano 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 da segurança (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).

4.3 Soluções para Corrigir os Comportamentos do Fator Humano

"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) Neste sentido, é de extrema importância para as organizações ter uma cultura de cibersegurança sólida (E3, E4 e E7) pois esta "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 o fator humano e transmitir-lhe 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 do fator humano 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, o fator humano olhará 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).

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, revelando a existência de uma grande dependência pela mesma. 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).

Apesar de a literatura afirmar que o fator humano é o elo mais fraco da cadeia de cibersegurança (Hadlington, 2017; Henshel et al., 2015; 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 do fator humano 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 o fator humano deverá ser uma das maiores preocupações das organizações no que toca à cibersegurança, representando uma grande vulnerabilidade das mesmas.

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 do fator humano 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). Em suma, as organizações ainda têm um longo caminho a percorrer de forma a atingir uma cultura de cibersegurança sólida. Neste percurso, o fator humano será, mais uma vez, estritamente indispensável para o alcance deste objetivo, pelo que é fundamental que este tenha o conhecimento necessário para poder contribuir para a cibersegurança da organização.

6. CONCLUSÃO

Atualmente, o fator humano não está suficientemente preparado nem é suficientemente incluído na cibersegurança de uma organização, pelo que muitas questões de cibersegurança continuam a ser descuradas, sendo o desconhecimento e a falta de sensibilização os maiores problemas inerentes ao fator humano. 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 o fator humano estiver preparado, mais resiliente será a organização.

Assim, 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 do fator humano.

AGRADECIMENTO

Este trabalho é financiado por Fundos Nacionais através da FCT - Fundação para a Ciência e a Tecnologia no âmbito do projeto de financiamento com a Referência UID/SOC/04521/2019.

REFERÊNCIAS

AP2SI, 2016. *Inquérito à Segurança da Informação nas Instituições em Portugal,* s.l.: s.n.

Baptista, I. M. A. S., 2017. *O fator humano na cibersegurança,* Lisboa: s.n.

CERT, 2013. *Unintentional Insider Threats: A Foundational Study,* Pittsburgh: s.n.

CERT, 2014. *Unintentional Insider Threats: Social Engineering,* Pittsburgh: CERT.

Duarte, R., 2004. Educar em Revista. *Entrevistas em pesquisas qualitativas,* Volume 24, p. 219.

ENISA, 2017. *Cyber Security Culture in organisations,* novembro.

Furnell, S., 2017. *Security education and awareness: just let them burn?,* s.l.: s.n.

Gil, A. C., 2008. *Métodos e técnicas de pesquisa social.* 6ª ed. São Paulo: Atlas.

Hadlington, L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon.*

Henshel, D., Cains, M. G., Hoffman, B. & Kelley, T., 2015. Trust as a human factor in holistic cyber security risk assessment. Volume 3, pp. 1117-1124.

ITU, 2008. Overview of cybersecurity. *Recommendation ITU-T X.1205,* abril.

Kajava, J. & Siponen, M., 2002. IT Security Awareness - Issues for Industry.

Leocádio, A. R. G., 2017. Segurança cibernética, pessoas, empresas e governos. Precisamos muito falar sobre isso. *Cibersegurança: educação digital e proteção de dados,* dezembro, Issue 18, p. 66.

Martins, J. et al., 2016. Sensibilização e Treino em Cibersegurança: Exercício de Recolha de Informação. *Proelium,* 7(10), pp. 141-160.

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

Mitnick, K. D. & Simon, W. L., 2003. *A Arte de Enganar.* s.l.:Pearson Education.

Monzelo, P. M. C. S., 2018. *A função do chief information security officer nas organizações,* s.l.: s.n.

Morgan, S., 2017. *2017 Cybercrime Report,* s.l.: Cybersecurity Ventures.

Peltier, T. R., 2005. Implementing an Information Security Awareness Program. *Information Systems Security,* Volume 14, p. 37.

Ponemon Institute, 2012. *The Human Factor in Data Protection,* s.l.: s.n.

Ponemon Institute, 2016. *Managing Insider Risk through,* s.l.: s.n.

Proofprint, 2019. *Human Factor Report,* s.l.: s.n.

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,* Lisboa: s.n.

Siponen, M., 2000. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security,* março, pp. 31-41.

Wilson, M. & Hash, J., 2003. Building an Information Technology Security Awareness and Training Program. *Special Publication,* outubro.

Woerner, R., 2012. *Cybersecurity education vs. cybersecurity training.* [Online] Available at: https://searchsecurity.techtarget.com/magazineContent/Cybersecurity-education-vs-cybersecurity-training [Acedido em 25 setembro 2019].

Zafra, D. E. d., Pitcher, S. I., Tressier, J. D. & Ippolito, J. B., 1998. Information Technology Security Training Requirements: A Role- and Performance- Based Model. *NIST Special Publication,* abril.