LIZA MARTINS DE AQUINO

CIBERATAQUES A INFRA-ESTRUTURAS CRÍTICAS, ENQUANTO FONTE DE STRESS OCUPACIONAL:

ESTUDO QUALITATIVO SOBRE OS RECURSOS E EXIGÊNCIAS REPORTADAS POR PROFISSIONAIS DE TICS

UNIVERSIDADE DO ALGARVE

FACULDADE DE CIÊNCIAS HUMANAS E SOCIAIS

2020

LIZA MARTINS DE AQUINO

CIBERATAQUES A INFRA-ESTRUTURAS CRÍTICAS, ENQUANTO FONTE DE STRESS OCUPACIONAL:

ESTUDO QUALITATIVO SOBRE OS RECURSOS E EXIGÊNCIAS REPORTADAS POR PROFISSIONAIS DE TICS

Mestrado em Psicologia Social, do Trabalho e das Organizações

Trabalho efetuado sob a orientação de:

Professor Doutor Jean-Christophe Henri François Antoine Giger

Co-orientador:

Professor Doutor Rui Filipe Gaspar de Carvalho

UNIVERSIDADE DO ALGARVE

FACULDADE DE CIÊNCIAS HUMANAS E SOCIAIS

2020

CIBERATAQUES A INFRA-ESTRUTURAS CRÍTICAS, ENQUANTO FONTE DE STRESS OCUPACIONAL:

ESTUDO QUALITATIVO SOBRE OS RECURSOS E EXIGÊNCIAS REPORTADAS POR PROFISSIONAIS DE TICS

Declaração de autoria de trabalho

Declaro ser o(a) autor(a) deste trabalho, que é original e inédito. Autores e trabalhos consultados estão devidamente citados no texto e constam da listagem de referências incluída.

_____

Liza Martins de Aquino

Agradecimentos

Desde o começo dessa trajetória como mestranda, me deparei com desafios, incertezas e encruzilhadas. O primeiro deles foi deixar a minha zona de conforto, o meu país e ir em busca dos meus sonhos. Mas meu co(ração sempre esteve tranquilo por saber que nunca estive sozinha nessa jornada, e que carrego comigo um pouquinho de cada um daqueles que amo.

Trilhar esse caminho não foi fácil, e hoje tenho a certeza de que só foi possível com o apoio e a força de algumas pessoas, às quais deixo meus sinceros agradecimentos e carinho.

Aos meus pais e irmãos, que acreditaram em mim desde que me lembro, me apoiaram em cada uma das minhas decisões e me ensinaram a sempre seguir em frente. Obrigada por serem o meu apoio constante e por vibrarem comigo a cada conquista.

Ao meu marido, que nunca me deixou desistir e sempre me inspira a ser uma pessoa melhor. Obrigada por todo o companheirismo, partilha, carinho e compreensão. A vida é muito melhor ao seu lado.

Aos meus amigos – aqueles que estão do outro lado do oceano e aqueles que encontrei aqui – obrigada por torcerem por mim e por estarem sempre ao meu lado (independente da distância entre nós). Vocês são força, serenidade e cumplicidade.

Ao meu orientador professor doutor Jean Giger, não só por ter aceite esse desafio, mas obrigada também por todo o conhecimento transmitido.

Ao meu co-orientador professor doutor Rui Gaspar, que idealizou e iniciou comigo esse projeto. Obrigada por sempre estar disponível e pronto a me motivar e ajudar.

Por fim, agradeço a todos os participantes que se disponibilizaram a participar desse estudo, e todos os demais que contribuíram para a concretização desta dissertação.

"Solidão foi a única coisa que eu não senti, depois de partir. Nunca. Em momento algum. Estava, sim, atacado de uma voraz saudade. De tudo e de todos. De coisas e pessoas que há muito tempo não via. Mas a saudade às vezes faz bem ao coração. Valoriza os sentimentos, acende as esperanças e apaga as distâncias. Quem tem um amigo, mesmo que um só, não importa onde se encontre, jamais sofrerá de solidão; poderá morrer de saudades, mas não estará só."

— *Amyr Klink, Cem Dias Entre Céu e Mar*

Resumo

Apesar de todos os benefícios da informatização à sociedade, atualmente observam-se cada vez mais desafios e medos relacionados à vulnerabilidade dos sistemas informáticos e de armazenamento de dados. Os crimes informáticos e ataques a esses sistemas (ciberataques) têm sido cada vez mais registados pelas autoridades. A presente dissertação é um estudo qualitativo, em que foram feitas entrevistas com 20 profissionais que trabalham diretamente com as Tecnologias da Informação e Comunicação (TICs). Os dados coletados nas entrevistas foram analisados utilizando o método de Análise Temática. O principal objetivo da investigação foi estudar os efeitos de um ciberataque enquanto fator estressor para os trabalhadores de TICs. Como objetivos específicos, buscámos identificar os recursos e exigências relatados pelos participantes numa situação de ciberataque, além de perceber quais as estratégias usadas por eles para enfrentar o *stress* ocupacional que vão para além do recurso ao capital psicológico e considerando igualmente o capital social. Os resultados mostram que, apesar de cada participante descrever a experiência de um ciberataque de forma distinta, eles relatam essa ocorrência como uma situação de *distress*, que têm consequências negativas para si. Por outro lado, os participantes conseguem reconhecer os recursos disponíveis para lidar com as exigências impostas durante essa ocorrência, enfatizando a importância do capital psicológico e, principalmente, do capital social. Assim, eles reportaram adotar estratégias de *coping* adaptativas e funcionais para responder ao ciberataque enquanto fator estressor.

Palavras-chave: Ciberataque, Capital Psicológico, Capital Social, Estratégias de C*oping*; Recursos, Exigências, Tecnologias de Informação e Comunicação.

Abstract

Despite all the benefits of computerization to society, today there are more and more challenges and fears related to the vulnerability of computer systems and data storage. Cybercrimes and attacks on these systems (cyberattacks) have been increasingly reported by the authorities. This dissertation is a qualitative study, in which were conduced interviews with 20 professionals who work directly with Information and Communication Technologies (ICTs). The data collected in the interviews were analyzed using the Thematic Analysis method. The main goal of the investigation was to study the effects of a cyberattack as a stressor for ICT workers. As specific goals, we seek to identify the resources and demands reported by the participants in a situation of cyberattack, in addition to observe which strategies they use to face occupational stress that go beyond the use of psychological capital and considering social capital as well. The results show that, although each participant describes the experience of a cyberattack differently, they report this occurrence as a distress situation, which has negative consequences for themselves. On the other hand, participants can to recognize the resources available to deal with the demands imposed during this occurrence, emphasizing the importance of psychological capital and, mainly, social capital. This way, they reported adopting adaptive and functional coping strategies to respond to the cyberattack as a stressor.

Keywords: Cyberattack, Psychological Capital, Social Capital, Coping Strategies, Resources, Demands, Information and Communication Technologies.

ÍNDICE GERAL

ÍNDICE DE TABELAS

1. INTRODUÇÃO

Apesar de todos os benefícios que a informatização proporciona à sociedade atualmente, surgem cada vez mais desafios e medos relacionados à vulnerabilidade dos sistemas informáticos e de armazenamento de dados. Têm se verificado um grande crescimento dos crimes informáticos registados pelas autoridades portuguesas ao longo dos últimos anos com ataques a esses sistemas – ciberataques –, e por isso a preocupação com a falta de segurança e privacidade dos gestores e usuários destes, torna-se cada vez mais evidente (Correia & Jesus, 2016).

Recentemente, os ciberataques ganharam grande destaque nos médias internacionais, devido a tentativas e a ataques bem sucedidos, a bases nucleares no Irão e à companhias americanas. Assim, nota-se que os adversários têm se tornado cada vez mais sofisticados em suas ações, tomando medidas cibernéticas para atacar e potencialmente destruir grandes infraestruturas (Finomore et al., 2013).

Segundo dados oficiais das autoridades portuguesas, dentro de poucos anos a criminalidade informática virá a assumir um peso substancial face aos crimes em Portugal, por isso é fundamental que o Estado atue de forma a garantir a ciberdefesa e a cibersegurança para os cidadãos e o território. Nesse sentido, a ciberdefesa é um conceito que pode ser definido como as medidas tomadas para proteger o estado de possíveis ataques; enquanto a cibersegurança diz respeito à segurança interna, ou seja, visa preservar a segurança e tranquilidade pública ao proteger bens e pessoas (Correia, Santos & Correia, 2017).

A constante busca por aumentar a eficácia ao lidar com ciberataques deve ser ainda mais enfática nas infraestruturas críticas, definidas segundo a alínea a) do Artigo 2.º do Decreto-Lei n.º 62/2011 de 9 de Maio como "componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções".

Muitos esforços têm sido feitos para aumentar a cibersegurança nas empresas, e para isso, estas frequentemente tomam medidas relacionadas a regras operacionais, treinamento com relação aos sistemas, monitorização dos trabalhadores, dentre outras ações. No entanto, muito pouca atenção é dispendida para o elemento humano na cibersegurança (Finomore et al., 2013).

Tomando em consideração o papel dos sistemas de informação dentro de uma organização e os custos relacionados com um ciberataque, melhorar a cibersegurança deve ser

uma prioridade da própria organização. No entanto, seria importante trabalhar não só a melhoria dos sistemas informáticos, mas também do elemento humano dessa relação, tomando em conta as competências, habilidades e capacidades como forma de evitar erros e contribuir para a efetividade da cibersegurança (Zaccaro, Dalal, Tetrick, & Steinke, 2016).

Sendo assim, o presente estudo pretende contribuir para o problema colocado acima e busca perceber como os trabalhadores lidam com o potencial *stress* ocupacional gerado por uma situação de ciberataque, e quais as estratégias que usam para enfrentá-lo, indo para além do recurso ao capital psicológico (i.e. caraterísticas/recursos pessoais para lidar com o stress; e.g. resiliência; esperança) e considerando igualmente o capital social (i.e. caraterísticas/recursos sociais para lidar com o stress; e.g. suporte social; conhecimento/formação disponíveis)..

Para isso, faremos uma contextualização teórica, passando por conceitos fundamentais para o desenvolvimento desta pesquisa, tais como o *stress* ocupacional, o capital psicológico e capital social, a perceção dos trabalhadores das exigências colocadas por ciberataques bem como os recursos para lidar com estas, dentre outros. Da mesma forma, ficará aqui explicitado as bases teóricas que serão guias neste trabalho.

2. REVISÃO DE LITERATURA

2.1. O *stress* ocupacional

O *stress* relacionado ao trabalho é um dos maiores problemas e fonte de doenças ocupacionais, gerando custos notórios aos sistemas de saúde. Além disso, pesquisas recentes mostram que 14% dos empregados que sofrem de *stress* vão acabar desenvolvendo também uma depressão (Corradini, Marano & Nardelli, 2016).

Segundo a definição da Comissão Europeia (1999), o *stress* é um padrão de reações que acontecem desde a idade da pedra, em resposta a um estressor para preparar o organismo humano para lidar com uma determinada situação, lutar ou fugir. Com relação ao *stress* no trabalho, este pode ser definido como padrões emocionais, cognitivos, comportamentais e respostas fisiológicas, que acontecem como reação à aspectos nocivos do trabalho, como o seu conteúdo, organização e ambiente.

No entanto, Robbins (2005), alerta que embora altos níveis de *stress* possam ter efeitos negativos, o *stress* em determinadas circunstâncias pode oferecer um potencial de ganho. Nesse sentido, o *stress* pode ter um efeito positivo caso o sujeito tenha o sentimento de controle sobre a situação (Comissão Europeia, 1999).

Como explicam Romero, Oliveira, e Nunes (2007), o *stress* pode ser potencialmente positivo, neste caso é chamado de *eustress*, quando há um equilíbrio entre o esforço dispendido, tempo, realização e os resultados atingidos. Quando existe esse equilíbrio, o *stress* pode ser um aspecto positivo para lidar com as pressões e vencer desafios. No entanto, quando a tensão mobilizada pela pessoa é muito grande e há um rompimento do equilíbrio por excesso ou falta de esforço, por ser incompatível com o tempo disponível, realização e resultados, os efeitos são conhecidos como *distress* e trazem consequências patológicas para o sujeito.

Assim, o *stress* é frequentemente associado a limites e exigências, ou seja, representa um confronto para o indivíduo gerando uma dúvida ou incerteza a respeito de oportunidades, limitações que precisam ser superadas e perdas que precisam ser evitadas (Robbins, 2005).

O *stress* ocupacional torna-se um tema relevante pela forma como a saúde e bem estar podem estar intimamente ligados ao trabalho. Quando o ambiente de trabalho oferece as condições ideais (suporte social, identificação, auto reconhecimento, recursos, autonomia etc.), o trabalho pode se tornar um objetivo e dar sentido à vida do sujeito. No entanto, quando essas condições não são favoráveis, a vida laboral pode gerar *stress* e outras reações emocionais negativas, como ansiedade, depressão, fadiga, dentre outros. (Comissão Europeia, 1999).

Além disso, a Comissão Europeia (1999), assinala que o *stress* laboral pode influenciar também o comportamento dos indivíduos, por exemplo iniciando ou aumentando o comportamento de consumo de tabaco, álcool e outras drogas. Da mesma forma, o *stress* causa alterações fisiológicas, a nível do organismo do indivíduo, como por exemplo alteração da pressão arterial, tensão muscular e até mesmo alterações cardíacas.

Segundo Robbins (2005), podemos identificar ao menos 3 fontes potenciais de *stress* para o trabalhador:

- Fatores ambientais: por exemplo incertezas econômicas, mudanças ou ameaças políticas, incertezas tecnológicas e o terrorismo
- Fatores organizacionais: exigências de tarefas e papéis, demandas interpessoais, a estrutura organizacional, o tipo de liderança, dentre outros
- Fatores individuais: questões familiares, problemas econômicos enfrentados pelo indivíduo, e características de sua própria personalidade.

Diante de todas as consequências negativas do *stress* para o trabalhador, organização e até mesmo para o Estado, a Comissão Europeia (1999), alerta para a necessidade de se conhecer e agir sobre os possíveis estressores organizacionais, tomando medidas preventivas e de promoção de saúde no ambiente de trabalho. Tais medidas preventivas podem ser à nível primário (modificando e agindo diretamente sobre os estressores percebidos no ambiente de trabalho), secundário (visando a mudança das respostas individuais à exposição aos estressores) e terciário (minimizando o *distress* individual e organizacional que resultam da exposição aos estressores).

Sabe-se, ainda, que a forma como os sujeitos lidam com o *stress* pode acabar por potencializar ou diminuir seus efeitos sobre o trabalho, a vida pessoal, aspetos físicos e mentais. Neste sentido, diversos estudiosos sobre o tema ressaltam que o estudo das chamadas Estratégias de *Coping* (Estratégias de Enfrentamento) é fundamental para melhor entender como o *stress* ocupacional afeta a vida das pessoas (Skinner, Edge, Altman, & Sherwood, 2003).

2.2 Estratégias de *Coping*

Dentre os muitos estudiosos sobre as estratégias de *coping*, podemos perceber um grande desacordo no que diz respeito às categorias relacionadas a este conceito. Isso porque este construto não é exatamente um comportamento que pode ser observado garantidamente

livre de equívocos, mas trata-se de uma forma de organização do indivíduo que embasa suas ações para lidar com situações de *stress* (Skinner et al., 2003).

O *coping* incorpora diferentes níveis de processos e reflete a evolução humana. Ou seja, as estratégias de *coping* estão embasadas por integrantes fisiológicas, psicológicas e sociais; neste sentido, muitas componentes do funcionamento psicológico (como por exemplo, emoções, atenção, motivação, etc.), bem como muitas componentes sociais e relacionais (relações de segurança, etc.) acabam por influenciar nas estratégias de *coping* usadas por cada indivíduo em situações de *stress* (Skinner & Zimmer-Gembeck, 2015).

Em um extenso trabalho abordando as diversas propostas de categorização das estratégias de *coping* por inúmeros autores, Skinner e colegas (2003) sugerem uma nova forma de separar as estratégias de enfrentamento segundo 12 Famílias de *Coping* e seus respectivos Processos Adaptativos. A seguir, encontra-se reproduzida e adaptada a Tabela 1, com as proposições destes autores, que será utilizada como base para a interpretação das estratégias de *coping* neste trabalho.

Tabela 1

Famílias de Coping e Processos Adaptativos

Processo adaptativo	Famílias de *Coping*	Funções no processo adaptativo	Implicações
Coordena ações e contingências no ambiente	Resolução de problema (estratetizar, ação instrumental, planejamento)	Ajusta ações para ser efetivo	Ver, aprender, maestria, eficácia.
	Procura por informação (leitura, observação, perguntar aos outros)	Encontrar contingências adicionais	Curiosidade, Interesse
	Desamparo (confusão, interferência cognitiva, exaustão cognitiva)	Delimita limites das ações	Culpa, desamparo
	Escape (evitamento cognitivo e comportamental, negação, pensamento desejoso)	Escape do ambiente	Largar e deixar rolar, medo, voar

	Autoconfiança (regulação emocional e comportamental, expressão e abordagem emocional)	Proteger os recursos sociais disponíveis	Tendência a fazer amigos, orgulho
	Procura por suporte (busca por contato/conforto, ajuda instrumental, suporte espiritual	Usar os recursos sociais disponíveis	Busca por proximidade, anseio, alianças
	Delegação (procura por ajuda desadaptativa, lastimar-se, auto-piedade)	Encontrar limites dos recursos	Auto-piedade, vergonha
Coordena a confiança e recursos sociais disponíveis	Isolamento (retração social, dissimulação, evitação aos outros)	Retração ao contexto sem apoio	Paralisar, tristeza, fingimento
	Acomodação (distração, reestruturação cognitiva, minimizar o problema, aceitação)	Flexibilização e ajustamento de preferências a opções	Escolha, controle secundário
	Negociação (barganha, persuasão, estabelecer prioridades)	Encontrar novas opções	Compromisso
	Submissão (ruminação, perseverança rígida, pensamentos intrusivos)	Desistir das preferencias	Perseverança rígida, desgosto
Coordena preferências e opções disponíveis	Oposição (culpar os outros, projeção, agressão)	Remover constrangimentos	Luta, raiva, desfiar

Tais categorias serão posteriormente retomadas.

As estratégias de *coping* podem, ainda, ser consideradas como estratégias de aproximação, sendo mais adaptativas e funcionais, ou estratégias de evitação, que são associadas a resultados de *coping* menos adaptativos (Antoniazzi, Souza & Hutz, 2009).

Além das 12 categorias acima propostas, este estudo tem como base a afirmação de que as estratégias de *coping* são parte de processos adaptativos, e dessa forma segue um ciclo. Primeiro, há a detecção e interpretação da informação interna e externa (detecção e avaliação da ameaça); em seguida, os indivíduos preparam uma resposta com base nas suas capacidades internas e guias externos; temos então a execução dessa resposta, coordenando a ação com os recursos e exigências internas e externas (regulação da ação). Por fim, há a recuperação e aprendizagem a partir da situação de *stress*. Sendo assim, a aprendizagem pode vir a alterar e influenciar as partes anteriores desse ciclo, em futuras exposições à fatores estressores (Skinner & Zimmer-Gembeck, 2015).

Através do estudo das estratégias de *coping* adotadas em uma situação de *stress* ocupacional, por exemplo, é possível perceber melhor como este fenómeno afeta a vida das pessoas. No entanto, no campo da Tecnologia da Informação e Comunicação, pouco enfoque se dá aos aspectos psíquicos e mentais dos trabalhadores e, neste sentido, as ações que têm vindo a ser implementadas ao nível da cibersegurança nas organizações, tem tido foco maioritariamente na componente técnica e tecnológica dos sistemas.

2.3 Cibersegurança e ciberataques: Abordagens psicossociais e resiliência de sistemas sócio-técnicos

Quase sempre visando a eficiência e eficácia no campo da tecnologia, existe um grande vazio na literatura científica ao nível das abordagens psicossociais com foco na componente humana do sistema, mesmo que esses sistemas sejam socio-técnicos e dependam da interação de indivíduos/equipas com tecnologia.

Mesmo as raras abordagens psicossociais à cibersegurança, de que é exemplo o trabalho de Zaccaro, Dalal, Tetrick, e Steinke (2016), apenas consideram aquilo que deve ser feito para aumentar a eficácia do sistema sócio-técnico aquando da ocorrência de um ciberataque, mas não consideram uma abordagem com foco na resposta a esses ataques ou no processo de *stress* que emerge e pode colocar em causa essa mesma eficácia.

Neste âmbito, emerge a necessidade de promoção da resiliência do sistema socio-técnico face ao potencial estressor dos ciberataques, no sentido de proporcionar aos indivíduos, equipas e organização como um todo, estratégias adequadas para lidar com o *stress*. Torna-se

então, igualmente relevante a identificação das exigências psicológicas e sociais que este tipo de evento coloca, bem como a perceção dos recursos pessoais e sociais que estão disponíveis para enfrentá-las/lidar com estas (Blascovich & Mendes, 2000).

Neste sentido, ao reduzir exigências e incrementar recursos, este tipo de evento poderá ser interpretado não como uma ameaça, mas como um desafio que o sistema sócio-técnico e os seus vários componentes, terão de enfrentar (Gaspar, Barnett, & Seibt, 2015).

Além do trabalho de Zaccaro e colegas (2016), podemos destacar outros poucos trabalhos com o tema dos ciberataques com foco nos indivíduos e seus recursos. O estudo de Helkala, Knox, Jøsok, Lugo, e Sütterlin (2016) é um destes poucos que investiga as estratégias de *coping* em cadetes do exército cujo trabalho envolvia sistemas informáticos. Neste estudo, foi feito um experimento com os cadetes que deveriam realizar 5 tarefas pré-determinadas, e depois os participantes fizeram uma auto avaliação de seu desempenho e das estratégias utilizadas para melhorar sua performance.

Ainda que existam alguns estudos sobre o elemento humano e suas estratégias relacionadas às tarefas informáticas, estes são ainda muito escassos. Além disso, podemos destacar alguns pontos fracos em seu método e resultados. Por exemplo, o trabalho de Helkala e colegas (2016) conta com uma amostra pequena (35 cadetes) para um método quantitativo que utiliza uma escala para exibir os resultados. Apesar de apresentar resultados plausíveis, em que o desempenho dos cadetes era melhor quando utilizavam estratégias de *coping* relacionadas ao controlo da situação e auto confiança em seu trabalho, pode ser difícil generalizar os resultados para toda a população, uma vez que este pode representar apenas um retrato da amostra em questão.

Neste sentido, torna-se necessário que novas e mais investigações sejam feitas sob a perspectiva de abordagens psicossociais, visando promover o bem-estar dos trabalhadores e combater os efeitos negativos do *stress* laboral. Para isso, um tema que entra em destaque é o aumento da resistência e resiliência dos trabalhadores face aos fatores estressores, com base no incremento de recursos pessoais e sociais que permitam ao trabalhador enfrentar o *stress* (Çelik, 2018).

2.4 Ciberataques enquanto catalizadores de um processo de *stress*

2.4.1 O papel do capital psicológico e do capital social

Segundo Ugale e Ghatule (2011), as pessoas reagem ao *stress* de diferentes formas, de acordo com suas características individuais e intrínsecas, e também de acordo com as

características da sua função e do seu trabalho (como por exemplo, determinados prazos para apresentar resultados, horas de trabalho, possibilidade de gozar de seu bom salário com sua família e em horas de lazer, etc). Ainda segundo os mesmos autores, notam-se diferenças inter-individuais, nomeadamente que algumas pessoas têm melhores estratégias de *coping*, enquanto outras demonstram sofrer mais com o *stress*.

Para Çelik (2018), o capital psicológico pode ser um aliado no combate ao *stress* e na promoção de saúde do trabalhador. Assim Luthans e Youssef (2004) afirmam que este conceito pode ser definido em 4 dimensões de competências pessoais que podem ser trabalhadas e desenvolvidas:

- Auto-eficácia: confiança de que se pode ultrapassar os desafios;
- Otimismo: atitudes e expectativas positivas com relação ao presente ou futuro;
- Esperança: perseverança em busca do sucesso e capacidade para reconsiderar as opções; e
- Resiliência: capacidade para lidar com os problemas e seguir em frente.

A cibersegurança das empresas pode depender consideravelmente dos trabalhadores e suas ações com relação à avaliação, confidencialidade e integridade dos sistemas informáticos. Assim, o capital psicológico pode ajudar também nestes comportamentos (Burns, Posey, Roberts, & Lowry, 2017).

Ainda segundo Burns e colegas (2017), apesar de o capital psicológico ser considerado um conceito relativamente novo, tem sido fortemente aceite no campo da psicologia. Sua aceitação pode ser explicada em parte por considerar as suas dimensões como *state-like* em vez de *trait-like*, ou seja, em vez de considerá-las características individuais estáveis e imutáveis, considera-se que as dimensões supracitadas podem sofrer mudanças com o tempo, dependendo do contexto, situações e exigências. Essa visão sobre o capital psicológico facilita a intervenção e ação no trabalho do psicólogo.

Para Frangopoulos, Eloff, e Venter (2013), os riscos psicossociais, definidos como tensões humanas geradas pelas estratégias empresariais, podem ter um direto efeito adverso nos aspectos físicos e psicológicos dos trabalhadores. Nesse sentido, os indivíduos podem estar sujeitos à diversos riscos psicossociais no trabalho e, para aqueles cujas tarefas envolvem as tecnologias da informação, isso pode afetar diretamente a segurança dos sistemas.

Nesse sentido, torna-se claro que inúmeros aspectos psicológicos e organizacionais interferem na díade "homem-máquina", o que pode levar à erros e falhas humanas que comprometem a segurança dos sistemas de informação. Sendo assim, não basta que as empresas

busquem alternativas para melhorar apenas o sistema, mas torna-se fundamental focar também no sujeito e na mitigação dos riscos psicossociais (Frangopoulos, Eloff, & Venter, 2013).

O campo da tecnologia está em constante mudança e desenvolvimento. Dessa forma, os recursos pessoais como a criatividade e inovação, tornam-se fundamentais para que os trabalhadores envolvidos com a cibersegurança possam acompanhar essas alterações e serem proativos ao criar ferramentas inovadoras a fim de manter o sistema fora do alcance dos *hackers* (Steinke, Fletcher, Niu, & Tetrick, 2016).

Steinke, Fletcher, Niu, e Tetrick (2016) salientam que muitos trabalhadores se beneficiariam caso buscassem o desenvolvimento de suas habilidades de criatividade e resolução de problemas, pois muitas vezes cibersegurança vem em um ciclo: os hackers têm de ser criativos e inovadores para invadir o sistema, e os trabalhadores têm de ter uma resposta à altura, buscando ser inovadores e criativos com ferramentas aliadas às suas competências de resolução de problemas, para proteger o sistema.

Os profissionais em geral desenvolvem estratégias de enfrentamento (estratégias de *coping*) ao *stress* laboral, que fazem parte de um repertório comportamental que busca evitar e/ou controlar as situações estressoras. Esses comportamentos são aprendidos ao longo da vida, em experiências pessoais e às vezes durante a formação académica; e são manifestados dependendo de fatores intrínsecos, exigências situacionais e também dos recursos disponíveis. A escolha, mesmo que inconsciente, de um indivíduo a um determinado tipo de estratégia de enfrentamento é influenciada por diversos aspectos, por exemplo suas crenças, habilidades sociais e de solução de problema, auto-regras, recursos disponíveis e suporte social (Maturana & Valle, 2014).

O capital social pode ser definido como as relações entre os indivíduos, que é de certa forma institucionalizada e reconhecida, criando valores como confiança, normas e relações, podendo até aumentar a eficiência e facilitar a ação coordenada (Babcicky & Seebauer, 2017).

Nesse sentido, o capital social pode ser também um recurso social para lidar com o *stress*, uma vez que o conceito pode ser relacionado como uma componente fundamental no processo de adaptação e ação coletiva. Diversos estudos comprovam que o capital social influencia positivamente a ação das pessoas durante e depois de grandes desastres, aquando da recuperação. Além disso, o capital social atua como catalisador da perceção de auto-eficácia e representa um grande suporte entre os sujeitos (Babcicky & Seebauer, 2017).

Além dos aspectos do capital psicológico e do capital social, existem ainda outros fatores podem influenciar no comportamento das pessoas diante de uma situação de *stress* e na

forma como lidam com essa situação, como por exemplo a perceção de risco que o indivíduo tem. Este conceito também já foi largamente abordado por diversas teorias e mostra-se aqui relevante no âmbito do tema da cibersegurança.

2.4.2 A perceção de risco

Para Schaik e colegas (2017), a perceção de risco inegavelmente exerce um papel no comportamento das pessoas, que julgam o quanto gostariam de se submeter ao risco comparando custos e benefícios que resultarão daquele comportamento, e adaptando seu comportamento a partir de então. Segundo os autores, existe uma variação na forma como as pessoas percebem os riscos relacionados à cibersegurança, e às medidas de precaução tomadas por eles com relação ao risco percebido.

Pode-se dizer que o ambiente político e social, bem como os fatores cognitivos de diferentes níveis podem influenciar na perceção de risco. Dessa forma, para além de como o risco é comunicado, fatores intrínsecos dos sujeitos exercem também influência na perceção de risco (Anderson, Brossard, Scheufele, Xenos, & Ladwig, 2014).

Muitas vezes um ambiente conflitivo, a vulnerabilidade e a perceção de riscos no trabalho podem ser fatores estressores para o trabalhador, e sabe-se que o *stress* tem consequências tanto para a atividade laboral quanto para a vida pessoal e saúde do indivíduo (Coleta & Coleta, 2008). Neste sentido, Maturana e Valle (2014) salientam que a perceção de um estímulo como fonte estressora depende da avaliação do próprio indivíduo e fatores intrínsecos, mas também da sua relação com o ambiente.

Por outro lado, o design do trabalho e decisões que precisam ser tomadas também refletem diretamente na perceção dos indivíduos, sua saúde e bem-estar, assim como para o bom funcionamento das organizações. Nesse sentido, o design de trabalho pode ser entendido como o conteúdo e organização de tarefas, atividades, relacionamentos, e responsabilidades de um indivíduo. Sendo assim, o design de trabalho para aqueles que que lidam com a cibersegurança precisa ser motivador, para incitar a proatividade e persistência dos mesmos (Parker, Winslow, & Tetrick, 2016).

Segundo Julisch (2013), a cibersegurança deve ser tratada como um tema interdisciplinar, sendo seu sucesso influenciado por inúmeros fatores. Assim, para se atingir uma melhor cibersegurança, aspectos psicológicos, técnicos e organizacionais devem ser tomados em consideração, e devem ser ajustados juntos com o foco em uma segurança dos sistemas mais objetiva e eficiente.

Considerando todos estes aspectos, percebemos ainda que a perceção de exigências que um Ciberataque impõe para os indivíduos, bem como dos recursos (pessoais e sociais) disponíveis para lidar com estas, são fatores fundamentais neste estudo. Isso porque estes fenómenos também podem exercer influência no comportamento adotado e na forma com que os indivíduos lidam com o *stress*.

2.4.3 O papel dos recursos e exigências

Segundo Blascovich e Mendes (2000), exigências podem ser definidas como a perceção e avaliação do perigo, esforço do indivíduo na situação e incerteza. Enquanto isso, os mesmos autores definem como recursos a perceção das habilidades e conhecimento relevantes para o desempenho do indivíduo em determinada situação.

Nesse sentido, Domingos, Gaspar, Fonseca, e Marôco (2020) destacam que as estratégias de *coping* dos indivíduos são moldadas pelas suas crenças, e também pela avaliação da situação de *stress* com relação aos recursos disponíveis e as exigências envolvidas. Assim, entender as estratégias de *coping* dos trabalhadores pode ajudar a entender e prever seu comportamento em situações de ciberataque, possibilitando então desenvolver intervenções voltadas para a adaptação e resiliência num futuro.

Com relação aos recursos e exigências, quando um indivíduo avalia que os recursos que tem disponíveis (intrínsecos e sociais) são superiores às exigências em determinada situação, pode-se dizer que ele encara a situação como um desafio. Já quando a avaliação se dá de forma oposta, ou seja, os recursos são inferiores às exigências, a situação passa a ser encarada como uma ameaça (Anderson et al., 2014).

Segundo Domingos e colegas (2020), a avaliação da situação como desafio leva a estratégias de *coping* baseadas na aproximação, como por exemplo a resolução de problemas. Já quando se trata de uma situação avaliada como uma ameaça, as estratégias de *coping* usadas são geralmente baseadas na evitação, como por exemplo o evitamento da informação e afastamento social.

Numa adaptação do trabalho de Domingos e colegas (2020), podemos sistematizar os recursos e exigências numa situação de ciberataque em diferentes níveis. Assim, temos em categorias de primeira ordem, as Exigências e os Recursos; elas dão origem a categorias de segunda ordem, que podem ser classificadas da seguinte forma:

- Exigências: perigo (e.g. por causa do ciberataque, o indivíduo pode perder o emprego); esforço (e.g. mais esforço mental e mais tarefas a desempenhar para mitigar um

ciberataque) e incerteza (e.g. sentimento de incerteza das causas, consequências e implicações do ciberataque).

- Recursos: conhecimentos, habilidades e competências (e.g. conhecimentos técnicos sobre os sistemas de segurança e habilidade para manuseá-los corretamente); disposições (e.g. atitude positiva, resiliência) e suporte externo (e.g. conforto ou ajuda de um colega numa situação de ciberataque).

Categorias de terceira ordem podem ser acrescentadas, de acordo com a situação específica a que se referem as categorias anteriores.

2.5 O *Tecnostress*

Não é novidade que as Tecnologias da Informação e Comunicação (TIC) têm originado grandes transformações na sociedade, nas mais diversas esferas: desde a economia, política, cultura e até mesmo as relações interpessoais (Carlotto & Câmara, 2010).

Segundo Alevato (2009), a rápida renovação e implementação dos aparatos tecnológicos vêm mudando o cotidiano das famílias, comunidades, escolas e também o ambiente de trabalho. Neste sentido, surgem novas questões que merecem ser exploradas, como por exemplo o conceito de tecnostress.

Neste novo paradigma tecnoeconómico, centrado nas ferramentas tecnológicas, os trabalhadores utilizam cada vez mais destes aparatos no seu dia a dia e novas formas de trabalho surgem em torno das TICs, como por exemplo o teletrabalho, o e-comércio e as reuniões e conferências virtuais (Carlotto, 2010).

Com isso, não só é exigido dos trabalhadores maior capacitação, mas também grande velocidade e dinamismo. Sendo assim, a inserção da tecnologia no ambiente de trabalho e essa urgência por mais e novos conhecimentos, pode gerar uma sobrecarga nos processos mentais e deixar os indivíduos mais sujeitos ao *stress* tecnológico, também conhecido como tecnostress (Carlotto & Câmara, 2010).

Apesar de ser um conceito bastante atual, o tecnostress não é um conceito novo. Já em 1984, Craig Brod publicou o livro intitulado "Tecnostress – o custo humano da revolução do computador". Neste sentido, o tecnostress pode ser definido como um estado psicológico negativo ocasionado pela relação e uso das TICs ou com a ameaça ao seu uso futuro. É uma patologia considerada moderna, na qual os profissionais sofrem para adaptar-se às novas tecnologias, não conseguindo lidar com elas de maneira saudável. Assim, surgem sintomas característicos ao *stress* tanto a nível individual, como problemas com sono, dores de cabeça,

irritabilidade; quanto a nível organizacional, com o aumento do absenteísmo e diminuição do desempenho (Portella, 2019).

O tecnoestresse pode ser avaliado em 4 dimensões: descrença, fadiga, ansiedade e ineficácia. Neste sentido, muitas vezes, os próprios trabalhadores da área das TICs têm a perceção de que o trabalho é estressante e de que a utilização da tecnologia acaba por afetar a sua saúde física e emocional. Isso, muitas vezes, leva-os a cogitar trocar de profissão e eleva o sentimento de insatisfação profissional (Carlotto & Câmara, 2010).

Essas variáveis estão ligadas ao conceito de tecnoestresse, mas podem também se agravar com o *stress* ocupacional induzido por uma situação de ciberataque, por exemplo.

Assim, apesar de o conceito de tecnostress ser fundamental para entender a saúde mental dos trabalhadores, neste estudo não iremos abordar tais dimensões, uma vez que o foco aqui não é observar os efeitos e a relação dos profissionais de TICs com as próprias tecnologias da informação, mas sim identificar os efeitos de um evento de grande magnitude como um ciberataque enquanto um fator estressor e a forma com que os profissionais lidam com essa situação.

3. OBJETIVOS DA INVESTIGAÇÃO

O presente estudo teve como objetivo geral estudar os efeitos de um ciberataque enquanto fator estressor para os trabalhadores de TICs. Mais ainda, traçámos dois objetivos específicos: o primeiro consistiu em identificar duas categorias avaliativas – recursos e exigências – do ponto de vista do elemento humano dos sistemas socio-técnicos, tendo por base uma abordagem de *stress* ocupacional. O segundo objetivo específico consistiu em perceber quais seriam as estratégias dos trabalhadores para enfrentar o *stress* ocupacional que iriam para além do recurso ao capital psicológico e considerando igualmente o capital social.

Estes são temas de grande relevância na sociedade de hoje, que caminha cada vez mais para a informatização e com isso, a cibersegurança passa a ser um assunto emergente no ambiente laboral. Sendo assim, é fundamental focar no bem-estar dos trabalhadores, buscando meios de potenciar o seu capital socio-psicológico e aumentar a sua resiliência diante dos ciberataques. Por essa razão, o presente estudo poderá também beneficiar a atuação profissional dos psicólogos organizacionais ao proporcionar aos trabalhadores, ferramentas para lidar com o dia a dia do seu trabalho, cada vez mais alvo de ciberataques que podem ser particularmente graves, se atingirem infraestruturas críticas (e.g. energia, transportes, hospitais, telecomunicações, etc.).

Uma vez que Christensen, Everitt, Chartrand e Boeke (2014) provaram a eficiência de um Sistema de Treinamento de Resiliência ao *Stress* e o destacaram como uma possível forma de se reforçar as estratégias de *coping* contra o *stress*, o presente estudo pode servir como base teórica para o desenvolvimento de técnicas de formação e treinamento voltadas para a resiliência dos profissionais das TICs. Nesse sentido, um novo Sistema de Treinamento inspirado no sistema supracitado e nos resultados aqui encontrados e descritos, poderá ser desenvolvido a fim de diminuir o *stress* ocupacional neste contexto de comprovada importância emergente.

Com este fim, busca-se aqui dar um contributo teórico, ao permitir uma melhor compreensão do processo de *stress* perante ciberataques enquanto estressor, bem como prático, ao permitir formação e treino de resiliência de trabalhadores, baseada na evidência científica. Busca-se também dar um contributo metodológico, ao realizar uma investigação com uma metodologia qualitativa, ainda não usada por outras pesquisas sobre o assunto. Ou seja, tendo aqui um enfoque qualitativo, com base em entrevistas individuais semi-estruturadas, e sendo assim possível aprofundar mais e obter uma maior heterogeneidade de dados recolhidos junto

de trabalhadores, podemos destacar este como um diferencial da pesquisa, uma vez que os demais estudos já realizados sobre este tema tinham enfoque quantitativo (e.g. Burns et al., 2017).

4. METODOLOGIA

A escolha do método de pesquisa voltado para a abordagem qualitativa resultou da vasta pesquisa bibliográfica sobre o tema, constatando-se uma grande carência na literatura referente às variáveis abordadas no estudo, tendo por base a recolha de dados qualitativos.

A abordagem qualitativa trabalha com valores, crenças, representações, atitudes e "adequa-se a aprofundar a complexidade dos fenómenos, factos e processos particulares e específicos de grupos mais ou menos delimitados em extensão e capazes de serem abrangidos intensamente" (Minayo & Sanches, p. 247, 1993).

Nesse sentido, Godoy (1995) salienta que a pesquisa qualitativa parte de questões amplas, que vão se delimitando ao longo do processo da investigação. Assim, nesse tipo de estudo, a obtenção dos dados é realizada a partir do contato direto do pesquisador com o objeto de estudo, buscando compreender os fenômenos em vez de descrevê-los.

Além disso, a constatação da lacuna de pesquisas neste campo sob uma abordagem qualitativa também influenciou a escolha desde método, uma vez que "a adoção de metodologias diferenciadas que privilegiem o acesso livre à cognição dos sujeitos, além das escalas que normalmente são utilizadas em trabalhos dessa natureza, é útil, sobretudo em face das constantes transformações no ambiente social e no mundo do trabalho em particular. Assim, a adoção de metodologia com tais características consegue captar melhor o impacto das mudanças na cognição dos sujeitos" (Melo, 2006, p.169).

Apesar de todos os benefícios apresentados do método qualitativo, sabe-se que apesar da natureza diferenciada da abordagem qualitativa e da abordagem quantitativa, ambas são importantes para a compreensão da realidade social. Assim, elas podem ser utilizadas de forma a se complementar, abrindo espaço para uma metodologia mista, sempre que o planejamento da investigação estiver em conformidade (Minayo & Sanches, 1993).

Sendo assim, optamos por realizar entrevistas semiestruturadas para a recolha de dados e, para isso, centramos nas questões mais amplas do presente estudo para desenvolver um guião de entrevista, e conforme fomos avançando neste processo, fomos chegando a questões mais específicas.

Para a análise dos dados, adotamos a metodologia de Análise Temática. Esse é um método amplamente usado em pesquisas qualitativas em diversos campos, especialmente dentro da psicologia, no qual busca-se identificar, analisar e relatar padrões ou temas manifestos

nos dados. Para isso, os dados são organizados e descritos em conjuntos de ricos detalhes (Braun & Clarke, 2006).

Segundo Barbosa, Silva e Nunes (2017), a análise temática representa uma ferramenta flexível e útil, que é capaz de fornecer uma análise de dados complexa, rica e bastante detalhada. Ela é bastante utilizada em pesquisas que envolvem um nível de subjetividade alto, uma vez que possibilita uma nova forma de produção de conhecimento sobre determinado assunto, através de novos caminhos de coleta e análise de dados.

Para Braun e Clarke (2006), o método de análise temática traz consigo diversas vantagens: seja por se tratar de um método relativamente fácil e rápido de aprender e aplicar, por ser acessível aos diversos perfis de investigadores, por possibilitar traçar semelhanças e diferenças no conjunto de dados, por permitir interpretações sociais e psicológicas dos dados, ou por outros tantos motivos.

No presente estudo, a análise temática fez-se indicada como método de análise de dados, uma vez que buscávamos aqui entender fenómenos complexos e altamente subjetivos, considerando as particularidades de cada sujeito na forma de lidar com uma situação de ciberataque em seu ambiente de trabalho. Pudemos assim, interpretar os resultados através do olhar psicossocial e traçar padrões de respostas, considerando as semelhanças e diferenças nos dados recolhidos.

Além da análise temática, utilizamos também o software SPSS para análise estatística dos dados quantitativos que também compunham o Guião de Entrevista, conforme explicaremos a seguir.

4.1 O instrumento: guião de entrevista

O instrumento usado teve por base uma adaptação do guião de entrevistas aplicado por Domingos e colegas (2020) em sua investigação acerca dos efeitos das vagas de calor. Pudemos perceber que muitas questões ali colocadas teriam relevância para a nossa pesquisa depois de sofrer algumas alterações e adaptações para o tema aqui estudado, dado que ambos os estudos consideram os processos de psicossociais de avaliação e resposta face ao um stressor. Apesar desse stressor ser diferente, os processos psicológicos base inferem-se ser semelhantes, sendo a abordagem aplicável a vários tipos de stressores (Domingos et al., 2020). Assim, prosseguimos com uma adaptação do guião enquanto instrumento de recolha de dados, eliminando aquelas questões que não se aplicavam aos nossos objetivos, e adequando aquelas que fariam sentido.

O instrumento original usado pelos autores supracitados, continha 35 questões divididas em dois tipos de perguntas: aquelas de resposta oral (para recolha de dados qualitativos) e outras em que o participante respondia apontando com o dedo à uma escala - Escalas Visuais Analógicas. Ao fim era ainda aplicado um questionário para auferir os dados sociodemográficos. Assim, o método de recolha de dados era misto, uma vez que continha dados qualitativos e quantitativos.

No nosso instrumento, mantivemos os dois tipos de perguntas (perguntas abertas - de resposta oral, e perguntas segundo uma Escala Visual Analógica). Depois do processo de adaptação do guião, em que eliminamos as questões que não importavam para o presente estudo e adaptamos aquelas que se encaixavam aos nossos objetivos, chegamos a um total de 25 questões.

Tendo em vista que o presente estudo se trata de uma pesquisa em psicologia, que busca entender os recursos e exigências reportadas pelos profissionais de TICs com relação ao estressor "ciberataque", esse tipo de metodologia e instrumento de recolha de dados tornam-se adequados, pois "colabora na investigação dos aspectos afetivos e valorativos dos informantes que determinam significados pessoais de suas atitudes e comportamentos" (Boni & Quaresma, 2005, p. 75).

Além disso, sabemos que a questão da complementaridade entre os métodos qualitativos e quantitativos traz ainda mais força para a investigação, na compreensão da realidade social. (Minayo & Sanches, 1993).

4.2 Pré-teste

Segundo Boni e Quaresma (2005), nas entrevistas semiestruturadas, o entrevistador segue um roteiro com perguntas previamente elaboradas, mas constrói um clima que se assemelha à uma conversa informal, possibilitando uma abertura e proximidade com o sujeito que está sendo entrevistado. Essa interação entre pesquisador-entrevistado acaba favorecendo respostas mais espontâneas a respeito de assuntos considerados mais delicados. Além disso, a maior liberdade e abertura que esse tipo de entrevista proporciona, pode colaborar para surgirem questões novas e adicionais que ajudam a tornar a fala do sujeito mais clara e completa.

Seguindo esta perspectiva, realizamos uma fase de pré-testes, na qual aplicamos uma versão preliminar do guião de entrevista em uma pequena amostra, buscando construir um clima amigável e favorecendo a abertura do entrevistado para responder livremente as questões propostas e acrescentar novas informações. Essa fase de pré-teste tinha como objetivo perceber

erros de compreensão das questões, coerência das perguntas e perceber se havia necessidade de incluir novas questões complementares ou eliminar alguma que não estava bem colocada.

O pré-teste foi realizado com 6 sujeitos, tendo todos eles Ensino Superior Completo ou em curso. Dessa amostra, 3 sujeitos já trabalhavam na área de Tecnologias da Informação e Comunicação, sendo 2 deles em infraestrutura crítica e 1 em infraestrutura não-crítica. Os outros 3 sujeitos não ainda não atuavam no mercado de trabalho na área de TICs.

A partir das entrevistas realizadas nesta etapa, percebemos necessárias algumas alterações no guião e, dessa forma, optamos por excluir uma questão que antes focava nas dificuldades do indivíduo e seus colegas em uma situação de ciberataque. Alteramos essa questão para o foco apenas no indivíduo, pois o pré-teste mostrou que os participantes tinham dificuldades em enxergar uma separação entre o Eu e o Outro nesse momento de adversidade, respondendo sempre pensando mais sobre si.

Além disso, acrescentamos nas questões sobre Recursos e Exigências, algumas "pistas" sobre o tema, ou seja, na Questão 08 do Guião de Entrevista (vide Anexo 1) quando falávamos de exigências mencionávamos a seguir "perigo, incerteza e esforço, dificuldades e barreiras". Já na Questão 09 do mesmo Guião de Entrevista, quando falávamos de recursos mencionávamos em seguida "conhecimentos, atributos pessoais, etc.". Isso porque os participantes demonstraram no pré-teste grande dificuldade em entender e associar os conceitos na hora de responder as questões.

Depois que acrescentávamos as "pistas", eles tinham notavelmente uma maior facilidade em responder. Salientamos aqui que ao acrescentar essas definições dos termos, buscamos fazê-lo de forma a não influenciar a resposta dos sujeitos, dando apenas grandes categorias. Assim, eles conseguiam fazer uma associação livre com sua própria experiência, sem sofrer viés.

Outro ponto que julgamos necessário alterar no guião foi acrescentar logo ao começo uma definição exata de ciberataque. Isso porque apesar de se tratar de profissionais de TICs a serem entrevistados, alguns podiam não saber exatamente do que se tratava o termo. Assim, logo na introdução do guião, acrescentamos o conceito de ciberataque que embasa nossa investigação.

4.3 População e amostra

O conceito de população pode ser definido como "uma coleção de elementos ou de sujeitos que partilham características comuns, definidas por um conjunto de critérios" (Fortin,

1999, p. 202). A mesma autora refere ainda que a amostra é definida como um sub-conjunto da população alvo, ou seja, uma réplica em miniatura dessa população.

Sendo assim, na presente investigação, define-se como população o universo de trabalhadores da área de Tecnologias da Informação e Comunicação de organizações consideradas infraestruturas críticas de Portugal e do Brasil.

4.3.1 Critérios de inclusão

Como critérios de inclusão na amostra, os participantes deveriam estar contratados na organização há pelo menos 6 meses, pois assim assume-se que os profissionais já conheceriam melhor o dia-a-dia da empresa e saberiam melhor relatar sobre a perceção de risco de ciberataques e comportamentos para lidar com esse tipo de estressor.

Além disso, na natureza das suas funções, deveriam ser responsáveis pela administração de sistemas informáticos ou serem trabalhadores com funções que implicassem a utilização das Tecnologias de Informação e Comunicação.

A seleção da amostra foi feita por amostragem não probabilística, mais especificamente pela amostragem acidental. Esse tipo de amostra é formado por sujeitos que são facilmente acessíveis, presentes em um determinado local num determinado momento. Assim, os sujeitos que cumpram os critérios de inclusão, vão compondo a amostra até que a mesma atinja o tamanho desejado (Fortin, 1999).

Na presente investigação, os sujeitos foram contactados através de redes sociais como LinkedIn ou através do e-mail, pelos quais foram enviados convites para a participação em uma entrevista por vídeo-chamada via Skype, uma vez que os procedimentos de recolha de dados coincidiram com o período de isolamento social imposto pelos governos devido à pandemia Covid-19.

Inicialmente, traçámos o objetivo de atingir uma amostra constituída por aproximadamente 30 trabalhadores, que habitualmente se considera como um número de participantes necessário para alcançar a saturação teórica. Este conceito pode ser explicado como a suspensão da inclusão de novos sujeitos à amostra quando os dados recolhidos passam a apresentar, pela avaliação do investigador, muita repetição ou redundância. Diferentemente das investigações quantitativas, nas quais o tamanho da amostra é definido por cálculos estatísticos, aqui o fechamento amostral acontece quando as informações obtidas através das entrevistas com os novos sujeitos, atingem uma saturação e passam a não contribuir ou não acrescentar aos dados já obtidos (Fontanella, Ricas, & Turato, 2008).

Para o presente estudo, detetou-se que a saturação teórica foi atingida aos 18 sujeitos, dado que as últimas entrevistas até aí realizadas, não permitiram identificar novos temas com interesse teórico. Ainda assim, foram realizadas mais duas entrevistas para garantir que a saturação havia sido atingida. Dessa forma, o fechamento amostral deu-se com um total de 20 sujeitos.

4.3.2 Caracterização da amostra

A amostra total foi constituída por 20 sujeitos, sequencialmente denominados como P.1 a P.20, de acordo com a ordem em que foram entrevistados. A seguir, na Tabela 2, apresentamos a caracterização dos trabalhadores que participaram deste estudo, em termos de idade e tempo que estavam a trabalhar na organização.

Tabela 2

Caracterização da amostra quanto a idade e tempo na organização

	Média	Mediana	Desvio Padrão	Máximo	Mínimo
Idade	30.85	28.5	7.75	58	24
Tempo na organização	4.80	1.91	5.91	20	0.5

Nota. Idade e Tempo na organização medidos em anos.

Como se observa na Tabela 2, a média de idade dos entrevistados encontrava-se entre 30 e 31 anos, sendo que o sujeito mais novo tinha 24 anos e o sujeito mais velho tinha 58 anos. A diferença entre o valor etário mínimo e máximo é bastante elevada, o que explica um alto valor de desvio padrão.

Podemos ainda perceber através da Tabela 2, que a média de tempo que os entrevistados estavam a trabalhar nas suas respetivas organizações é de 4,80 anos. No entanto, o sujeito que trabalhava a menos tempo na organização, estava ali há apenas meio ano, sendo que o sujeito que trabalhava a mais tempo na organização estava ali há 20 anos. Essa grande diferença entre os tempos mínimo e máximo explicam também o alto valor de desvio padrão.

A seguir, na Tabela 3, apresentamos a caracterização dos trabalhadores que participaram deste estudo, em termos do género, escolaridade e função que desempenhavam na organização.

Tabela 3

Caracterização da amostra quanto ao género, escolaridade e função

	Nº de sujeitos	% da amostra
Género		
Masculino	17	85%
Feminino	3	15%
Escolaridade		
12º Ano	2	10%
Ensino Superior Incompleto	2	10%
Ensino Superior Completo	7	35%
Pós Graduação	9	45%
Função		
Analista de Segurança da Informação e Resposta a Incidentes	7	35%
Analista de TI	5	25%
Consultor de TI	3	15%
Gerente de TI	3	15%
Arquiteto de Software	1	5%
Técnico Informático	1	5%

Como podemos observar na Tabela 3, no que concerne ao género, 17 participantes (85%) eram do género masculino, enquanto apenas 3 participantes (15%) eram do género feminino. Estes valores revelam uma amostra maioritariamente formada por homens.

Ao analisarmos o nível de escolaridade dos participantes, pudemos observar que 16 deles (80%) possuíam Ensino Superior Completo ou Pós Graduação. Apenas 4 dos participantes (20%) não haviam terminado o Ensino Superior ou tinham concluído apenas até o 12º ano.

Ainda na Tabela 3, percebemos que, relativamente às suas funções, podemos dividir os participantes em 6 diferentes categorias, sendo que a maior parte deles desempenhava a função de Analista de Segurança da Informação e Resposta a Incidentes (7 participantes – 35%). Como um dos critérios de inclusão na amostra era a natureza das funções, sendo que os sujeitos deveriam ser responsáveis pela administração de sistemas informáticos ou cujas funções implicassem a utilização das Tecnologias da Informação, tivemos também participantes cujas

atividades diárias não estavam ligadas diretamente a respostas a incidentes, como é o caso dos Analistas de TI (5 participantes – 25%), Consultores de TI (3 participantes – 15%), Gerentes de TI (3 participantes – 15%), Arquitetos de Software (1 participante – 5%) e Técnicos Informáticos (1 participante – 5%). Ainda assim, pouco mais de um terço dos entrevistados lidavam diretamente com cibersegurança e incidentes.

Conclui-se, assim, que apesar das diferenças entre os participantes que constituem a amostra, se trata de uma amostra maioritariamente masculina, jovem, com um nível de escolaridade avançado, e cujas funções dentro da organização estavam diretamente ligadas a cibersegurança e incidentes como ciberataques.

4.4 Procedimento

Após a recolha dos dados através das entrevistas semi-estruturadas, procedeu-se com a análise de dados.

Para explicar os procedimentos de análise de dados através da análise temática, é preciso primeiro abordar o conceito de tema: os temas organizam um grupo de ideias, sendo constituídos por códigos que tem pontos em comuns e uma alta generalidade. Assim, representam um tipo de resposta padrão relacionado com as questões de pesquisa (Barbosa et al., 2017).

Braun e Clarke (2006) propõem 6 fases para a aplicação da análise temática, no entanto salientam que é importante ter consciência de que tais fases não são regras imutáveis, uma vez que a pesquisa qualitativa é marcada por ser flexível e ajustada às especificidades da investigação. Essas fases também não representam um processo linear, mas sim um processo adaptável no qual transita-se para frente e para trás, entre as fases, conforme o necessário e sem pressa em fazê-lo.

Assim, procedemos com as 6 fases propostas por Braun e Clarke (2006):

- Familiarizar-se com os dados: faz-se a transcrição dos dados, leitura e releitura dos mesmos, apontando as ideias que o investigador considera pertinentes.
- Gerar códigos iniciais: codificação das características principais dos dados, de forma sistemática.
- Busca por temas: faz-se o agrupamento dos códigos em potenciais temas. A partir de várias releituras das transcrições, a interpretação vai sendo construída e surgem pistas que ajudam na busca dos temas.

- Revisão dos temas: verifica-se como os temas relacionam-se entre si, e se possuem verdadeiramente uma autonomia de conteúdo que contribui significativamente para a análise. Surge um "mapa" temático tomando o cuidado de não procurar trechos que confirmem suposições do investigador, o que levaria a um viés. Para isso, deve-se ter bastante clareza nos objetivos da pesquisa para não se perder nos relatos dos participantes
- Definição e nomeação de temas: faz-se uma nova análise para refinar os temas, deixando os seus nomes e definições bastante claros. É preciso uma análise bem feita para identificar a história de cada tema, e a história geral contada pela análise.
- Produção do relatório: seleção de exemplos do extrato, num relato conciso e coerente da história contada através dos temas. Produz-se um relatório da análise, com provas suficientes dos temas, apontando a relação entre a análise, a questão da pesquisa e a literatura.

Ao transcrever os dados e dar início à análise temática, fomos transitando entre as fases apresentadas, de forma a extrair dos relatos a maior quantidade de informação possível, levando em consideração a sua complexidade e a subjetividade dos sujeitos. Ao agrupar as falas dos participantes, não nos prendemos à ordem das perguntas do guião, mas sim levamos em consideração os temas levantados e as histórias contadas pelos entrevistados.

5. RESULTADOS

5.1 Ocorrência de Ciberataques

Quando questionados sobre a sua perceção de risco de acontecer um ciberataque na organização para a qual trabalham, todos os 20 sujeitos entrevistados reconheceram que as suas respetivas organizações correm esse risco, revelando uma consciência do risco associado, na amostra.

No entanto, apenas 12 (60%) dos 20 participantes relataram que a organização para a qual trabalham já sofreu algum tipo de ataque, ou ao menos alguma tentativa. Enquanto isso, sete dos entrevistados (35%) disseram que a organização nunca passou por uma situação assim desde que iniciaram suas funções ali, e apenas um (5%) dos participantes referiu que a organização já sofreu um ciberataque, mas a ocorrência foi antes de que ele iniciasse suas funções ali e, portanto não sabia dar informações detalhadas sobre a situação.

É importante ter em consideração que este aspeto poderá ter alguma influência sob os resultados encontrados, uma vez que os temas emergidos nas entrevistas poderão estar ligados ao facto de os participantes terem vivenciado uma situação de ciberataque ou não. Neste sentido, o facto de apenas 60% da amostra já ter vivenciado uma situação de ciberataque poderá ter implicações para os resultados apresentados a seguir.

5.2 Exploração das situações típicas de ciberataque

Relativamente aos tipos de ciberataques, vimos que 12 participantes relataram que a empresa já foi alvo de mais de um tipo de ciberataque ou tentativa. Nesse caso, a situação típica mais relatada pelos entrevistados, foi a tentativa de sobrecarregar o sistema e tornar os recursos do mesmo indisponíveis para os utilizadores. Este tipo de ataque é também conhecido como Ataque de Negação de Serviço, ou DDOS, e foi relatado por sete participantes (35%), a exemplo da fala:

> ***"****Ataques de sobrecarga de pacotes, sobrecarga de serviços e aplicações, para tirar o serviço do ar"* (P.17).

> *"Tivemos um ataque de DDOS, que o atacante ou o hacker tenta deixar o seu sistema indisponível"* (P.9).

O segundo tipo de ciberataque mais relatado pelos entrevistados foi o ataque tipo *Ransomware*, cujo objetivo é o sequestro ou criptografia dos dados. Essa situação típica foi relatada por seis entrevistados (30%), como por exemplo:

> "*Fizeram a tentativa de entrar, para compactar os arquivos, com o objetivo de sequestrar os dados*" (P.18).

> ***"****Eu acho que no nosso meio, os tipos de ataque mais comuns são ataques para sequestro de dados"* (P.20).

A terceira situação mais comentada pelos participantes foi o ataque do tipo *Phishing*. Este tipo de ataque chega aos usuários através de e-mails ou mensagens fraudulentas, disfarçadas muitas vezes sob o nome de entidades confiáveis, com o fim de obter informações confidenciais (senhas, detalhes da conta, etc.) ou obter acesso ao sistema e à rede. Dos 20 entrevistados, cinco (25%) citaram esse tipo de ocorrência, como pode-se observar nas seguintes falas:

> "*Muitas vezes são ataques de Phishing, que é um ataque em que é enviado um e-mail para alguém persuadindo a pessoa a clicar em um link, ou revelar informações sensíveis, senha, etc. E nesse caso a própria pessoa pode enviar essa informação para o atacante e comprometer o sistema*" (P.2).

> *"Nós constantemente temos tentativas de phishing"* (P.14).

Outra situação bastante comentada pelos entrevistados foram ataques para roubo de informação sigilosa ou dados sensíveis. Neste caso, quatro participantes (20%) comentaram sobre esse tipo de ciberataque, como por exemplo:

> "*Mas quando se trata de hospital, você tem dados sensíveis de pacientes, dados sensíveis de funcionários, etc. Então você pode ter ataques que buscam roubar esse tipo de informação, principalmente relacionado a pacientes, como pessoas do governo e pessoas famosas*" (P.15).

> *"Invasão pela rede de computadores para roubar dados"* (P.11).

Outras situações menos comentadas pelos entrevistados foram ataques para divulgação de *Fake News* em nome da empresa (relatado por um entrevistado – 5%); ataques de exploração, para detectar vulnerabilidades do sistema (relatado por um entrevistado - 5%); e ataques do tipo "*Man in the Middle*", cujo objetivo é interceptar e observar informações trocadas entre duas partes, sem que as vítimas percebam (relatado por um entrevistado – 5%).

No entanto, quatro dos participantes não souberam classificar o tipo de ataque ou tentativa frequente, uma vez que nunca haviam passado por uma situação de ciberataque em seu ambiente de trabalho.

5.3 Vulnerabilidade dos sistemas

Apesar de muitos dos entrevistados nunca terem vivenciado uma situação de ciberataque, a maioria deles reconhece que os sistemas informáticos, os computadores e a rede de comunicações das empresas para a qual trabalham, são vulneráveis a ameaças de segurança.

Dos 20 participantes, 16 (80%) reconheceram vulnerabilidade no sistema, enquanto apenas quatro (20%) disseram que não consideram o sistema vulnerável. Neste sentido, muitos deles comentaram que independente de todas as medidas de segurança que são tomadas, sempre existe algum tipo de vulnerabilidade, o que pode ser observado através das seguintes falas:

> "*Eu acho que a gente tem um sistema muito seguro, mas se você for parar para pensar, todo sistema está sujeito a algum tipo de vulnerabilidade. Não tem como existir um sistema perfeito, completamente seguro*" (P.20);

> "*Olha, isso é difícil. Acho que todos os sistemas, por mais caros e modernos que sejam, têm alguma vulnerabilidade*" (P.14).

Dos 16 participantes que reconheceram existir alguma vulnerabilidade nos sistemas, oito deles atribuem essa vulnerabilidade ao fato de a tecnologia estar em constante evolução, e por isso sempre existe a possibilidade de surgirem novas formas ou ferramentas de ciberataque que ainda não se tem conhecimento. Isso pode ser inferido a partir de falas como:

> "*A todo momento nasce uma ameaça nova, que o pessoal costuma chamar de 'zero-data'. É um ataque que ainda não tem nenhum tipo de defesa, é uma ameaça nova*" (P.9).

"Podem ser desenvolvidos novos tipos de ataque a qualquer momento. Estamos lidando com uma área que está em constante evolução. Então até que aconteça a primeira tentativa daquela nova forma, nós não saberemos lidar com ela" (P.5).

Enquanto isso, oito deles atribuem essa vulnerabilidade a falhas humanas, a exemplo das seguintes falas:

"*Primeiro porque o sistema é manipulado por pessoas, e pessoas cometem erros às vezes. Então alguém pode cair em uma tentativa de ataque de phishing, pode clicar em links que vão conceder acessos a pessoas indevidas, ou alguma coisa assim*" (P.10).

"Eu diria que 80% da proteção para um ciberataque, são os próprios usuários. Então a vulnerabilidade não é equipamento, não é servidor. Porque por mais que se tome uma medida para que proteja, sempre tem um usuário que clica num link malicioso, que instala uma aplicação que não está na matriz. Então a gente está vulnerável o tempo todo" (P.15).

5.4 Os efeitos de uma situação de ciberataque: *distress* ou *eustress*?

Quando questionados se uma situação típica de ciberataque interfere de alguma forma na sua vida profissional ou com alguma atividade profissional que faça normalmente no seu dia a dia, 90% dos entrevistados relatou que sim. Apenas dois participantes (10%) disseram que a ocorrência de um ciberataque não afeta ou afeta muito pouco a sua atividade diária ou vida profissional.

Os 18 participantes (90%) que reconheceram que uma situação de ciberataque interfere na sua vida profissional ou atividade diária mencionaram diversas formas com que essa situação tem impacto sobre si. Neste sentido, oito dos entrevistados (40%) relataram que têm de dispender um maior esforço, atenção e trabalho durante a ocorrência de um ataque, o que podemos exemplificar através das seguintes falas:

"*Isso afeta todos da organização, todo mundo tem mais trabalho, desde quem recebe as reclamações dos clientes, até nós que estamos diretamente ligados com o dever de solucionar o problema*" (P.8).

"Com o ciberataque, aumenta as reclamações dos clientes, consequentemente, as ordens de serviço. Com isso, os atendimentos podem atrasar um pouco devido a demanda e preocupação dos clientes" (P.11).

Outro ponto bastante comentado pelos entrevistados foi uma mudança na sua rotina diária, sendo que seis participantes (30%) relataram que a ocorrência de um ciberataque gera uma mudança nas atividades que desempenham diariamente, como podemos perceber através da fala:

"*Muda completamente a minha dinâmica do trabalho. Por mais que seja parte das minhas atividades diárias, um evento de incidente é algo que muda completamente a rotina para qualquer um dos envolvidos. E quando eu digo os envolvidos, é porque um incidente não pode ser tratado somente pela equipe de cibersecurity. Ele envolve o departamento jurídico, envolve até mesmo o marketing e o pessoal que faz a comunicação"* (P.14).

"Com certeza toda a operação da empresa seria alterada até que a situação fosse regularizada, então afeta a atividade daquele dia" (P.3).

Cinco dos participantes (25%) relataram ainda um maior *stress*, preocupação e incerteza durante uma situação de ciberataque e que isso interfere na sua atividade diária, conforme se pode ver nos exemplos seguintes:

"*Em termos de cansaço, stress, para poder fazer a reestruturação e restauração do ambiente, sim, teria um desgaste grande físico e psicológico.*" (P.15);

"*Gera aquele stress, e você leva isso para casa: a preocupação de um ciberataque, uma tentativa de invasão ou propriamente dita a invasão. A gente fica preocupado. Cada uma dessas tentativas de ataque gera pra a gente um pensamento de 'se acontecer mesmo, qual vai ser o impacto? Qual é o risco que eu estou sofrendo?*" (P.12).

Neste sentido, percebemos que participantes que levantam temas como o aumento do esforço, mudança nas suas atividades diárias e inclusive sentimentos de preocupação e incerteza, reportavam também a ocorrência de um ciberataque como uma situação de *distress*.

Ou seja, a maioria dos participantes associa essa situação com limites e exigências que criam um desequilíbrio entre o esforço, tempo e resultados, gerando assim consequências patológicas.

Por outro lado, um entrevistado (5%) relatou que a ocorrência de um ciberataque pode interferir positivamente com a sua vida profissional, permitindo-o aprender com a experiência e evoluir enquanto profissional. Foi o caso do P.9, que disse:

> "*Além da experiência que você adquire nesses momentos críticos, tensos e de uma pressão muito grande, você acaba desenvolvendo o seu lado profissional e o seu psicológico para tratar o assunto. Depois de um ataque grave, muda bastante a perceção do analista, e muda muitas vezes a empresa como um todo. Ele fica mais preparado*".

É notável que o P.9 quando diz que a ocorrência de um ciberataque pode ser uma boa oportunidade de aprender e evoluir com a experiência, encara essa situação através da ótica do *eustress*. Sendo assim, para ele, existe um equilíbrio entre o esforço, tempo e resultados e, portanto, a situação revela um potencial de ganho e passa a ter um aspecto positivo para vencer desafios.

Ainda assim, apesar dos fatores subjetivos e particulares que influenciam a forma com que cada indivíduo lida com situações de *stress*, percebemos que a maioria dos participantes relata a situação de ciberataque como fonte de *distress*, enquanto apenas um deles relata o potencial de ganho pelo *eustress.* Iremos então considerar aqui a prevalência das consequências patológicas na ocorrência de ciberataque nesta amostra.

5.5 Exploração das exigências percebidas na situação típica de ciberataque

No que diz respeito às exigências, 19 dos entrevistados (95%) consideram que situações de ciberataque lhes colocam dificuldades e barreiras para o seu trabalho, que em circunstâncias normais não teriam ou teriam menos. Apenas um sujeito (5%) disse que não sente tais exigências.

Quando questionados sobre o tipo de exigência percebida, a maioria dos participantes referiu um maior esforço físico e mental, sendo ele ocasionado por uma maior carga de trabalho, ou até mesmo pela necessidade de mais dedicação e atenção durante aquela situação. Neste sentido, 10 participantes (50%) relataram esse tipo de exigência como "esforço", o que podemos exemplificar através das seguintes falas:

"*Durante o ciberataque, teríamos que colocar todos os nossos esforços para regularizar a situação. Isso exigiria mais horas de trabalho, mais dedicação*" (P.3).

"As exigências seriam o esforço da equipe durante o tempo necessário para tomar todas as medidas e protocolos, até que tudo volte ao normal" (P.4)

Outros seis entrevistados (30%) relataram que dentre as exigências estão um maior *stress*, ansiedade, pressão e até mesmo desgaste, como podemos observar nas falas a seguir:

"*Caso tenhamos dificuldade em descobrir o problema em si antes de resolvê-lo, a pressão só aumenta. Com isso vem o stress, a ansiedade, e quando você fica exposto a esse tipo de situações e sentimentos, você pode até vir a ter problemas físicos e de saúde decorrentes dessa pressão toda*" (P.11).

"Além de conter aquela vulnerabilidade que fez o ciberataque acontecer, você tem que verificar o seu ambiente, para ver se não tem a mesma vulnerabilidade em outros locais. Então é um trabalho muito desgastante, tem muita pressão" (P.15).

Igualmente podendo ser considerado como "esforço", referem-se o senso de urgência e a perceção de uma necessidade de agir com rapidez diante da situação de ciberataque sendo que cinco (25%) deles relataram esse tipo de sentimento.

"*Geralmente você tem pouco tempo para agir, então em questão de minutos você tem que entender o que está acontecendo e resolver aquele problema*" (P.2).

"Muda toda a rotina do meu trabalho, e isso já coloca um sentimento de dificuldade né. E como a gente tem que tomar ações rápidas para mitigar e solucionar o problema" (P.20).

Outro tipo de exigência bastante comentado pelos entrevistados foi o sentimento de incerteza e insegurança. Esse tema foi levantado por sete participantes (35%), como por exemplo nos seguintes relatos:

"*Acho que até que se resolva o problema, você sente uma incerteza. Incerteza de saber se você vai conseguir resolver aquilo, quais as consequências que aquilo vai ter, que proporção aquela situação vai chegar*" (P.10).

"Acho que a incerteza é de não conseguir re-estabilizar o sistema da forma que deveria ser né. Quando acontece um ataque, nas primeiras horas, é um grande escuro. Até você descobrir o que aconteceu, você sente um medo muito grande. Fica aquela incerteza de "e agora, o que a gente vai fazer se não conseguir estabilizar isso?". E depois que descobre o que efetivamente aconteceu, tem o problema de "como resolver?" (P.9).

Por último, outro tipo de exigência percebida pelos participantes, são os sentimentos de perigo, preocupação e medo. Neste caso, quatro participantes (20%) levantaram essa temática, como por exemplo:

"*A preocupação, o medo... A gente da área de TI sente muito isso em condições normais, imagina sob a condição de um ciberataque. É o medo de não conseguir resolver a situação, de perder dados importantes, e a preocupação de que aquilo tome uma proporção extrema.*" (P.12).

"Acho que quem trabalha com TI sabe o que que um ciberataque pode causar, as consequências que uma situação de um ataque cibernético pode ter. Então, acho que coloca um sentimento de medo até que a situação se resolva. Medo de não saber até que ponto aquilo vai chegar, qual o objetivo dos atacantes." (P.18).

5.6 Recursos percebidos na situação típica de ciberataque: indicadores de capital psicológico e capital social

Quando questionados a respeito dos recursos que podem usar para enfrentar as exigências colocadas pelas situações de ciberataque, todos os entrevistados relataram que têm acesso a diversos tipos de recursos.

A começar pelas ferramentas do sistema e equipamentos da empresa, estes recursos técnicos foram citados por quatro participantes (20%) para enfrentar situações de ciberataque, a exemplo das falas:

"É saber que a empresa tem todas as melhores ferramentas do mercado para lidar com situações como essas" (P.4).

"Os próprios recursos da empresa são fundamentais. Os sistemas, as ferramentas de segurança, eles estão aí para isso" (P.14).

No entanto, percebemos que os relatos mais comuns acerca dos recursos envolvem o capital psicológico e o capital social. Neste sentido, como exemplo do capital psicológico, 16 participantes (80%) citaram como recursos disponíveis para lidar com as exigências o seu conhecimento ou a sua experiência profissional, sendo estes os recursos mais reconhecidos por eles. Podemos observar isso através das seguintes falas:

> *"O tempo inteiro, o conhecimento é a sua maior arma. O conhecimento tanto dado pela organização, em formações e palestras, quanto o conhecimento de self-study. E a experiência, porque por exemplo, uma pessoa que sofre um ataque de phishing pela primeira vez, no próximo phishing que ele sofrer, ele não vai ficar tão preocupado assim. Cada vez mais que você vai sofrendo ataques, vai adquirindo conhecimento com isso*" (P.13).

> *"Eu acho que o conhecimento é o principal. Acima de tudo você tem que estar ciente do que está fazendo, o que está acontecendo. Ter o conhecimento de que tipo de ataque, como ele acontece, porque ele está acontecendo dessa forma"* (P.16).

Outros nove participantes (45%) citaram como recurso alguns atributos pessoais ou traços de personalidade, em falas como:

> "*Eu acredito que o fator pessoal e emocional é muito importante. Eu acredito que eu tenho um forte autocontrole, é uma coisa muito forte que eu tenho e funciona muito bem*" (P.12).

> *"Eu acredito que é da minha personalidade não me abalar muito numa situação caótica. Eu consigo manter bem a calma nesses momentos assim, continuo com meu bom raciocínio lógico. E uma coisa que eu tenho é a persistência. Às vezes, na área de infraestrutura tem um problema que você fica 2 dias tentando resolver, sem dormir direito. Então muita gente desiste, se deixa afetar e fala 'Não dá mais, eu quero ir embora. Não consigo mais pensar'. Nessas situações eu sempre consegui me sair bem, com muita persistência e mantendo o foco nessas situações críticas"* (P.9)

Em outra pergunta na entrevista, dessa vez especificamente sobre os atributos pessoais e capital psicológico, quase todos os participantes reconheceram que possuem características

intrínsecas a si que os ajudam a lidar melhor com as exigências colocadas por situações de ciberataque. Apenas um entrevistado (5%) disse não reconhecer em si algum atributo que o ajuda em situações de ocorrência de ciberataque.

Dentre estes atributos pessoais, os mais citados foram os conhecimentos e a experiência profissional (nove participantes – 45%). Outros atributos pessoais destacados foram a capacidade de manter a calma e paciência (seis participantes – 30%); a dedicação, persistência e resiliência (cinco participantes – 25%); o auto controle, concentração e foco (três participantes – 15%); habilidades sociais e de comunicação (três participantes – 15%); e, por fim, o senso investigativo, pensamento crítico e a capacidade de discernimento (três participantes – 15%).

Para além dos vários exemplos de capital psicológico referidos, exemplos de indicadores de capital social foram igualmente identificados. Neste sentido, um recurso bastante valorizado pelos participantes foi o apoio social, sendo que cinco participantes (25%) comentaram sobre este tema quando questionados acerca dos recursos, como por exemplo:

"*A gente tem uma base muito forte aqui, um grupo muito forte de apoio. A gente tem vários amigos que conversam entre si e um ajuda o outro*" (P.15).

> *"A sua equipe né, que está ali para trabalhar em conjunto e dividir as responsabilidades"* (P.20).

Além disso, 18 participantes (90%) disseram que sentem que podem contar com a ajuda dos colegas de trabalho para enfrentar uma situação típica de um ciberataque, e destacam a importância do trabalho em equipa em falas como:

"*Sim, com certeza. Eu acho que todo mundo aqui trabalha verdadeiramente como uma equipe, e numa situação estressante assim, a ajuda e o apoio dos colegas é fundamental"* (P.10).

> *"Sem dúvida. Eu conto com eles. Se eu não tiver esse apoio, não vai dar certo"* (P.12).

Dessa forma, percebemos que os participantes, em sua maioria, sentem uma boa rede de apoio na sua equipa, e reconhecem a importância do que chamamos aqui de capital social para o enfrentamento de situações de *stress*.

O reconhecimento dessa rede de suporte fica claro quando 16 dos 18 participantes que relataram poder contar com os colegas, referiram que quando ocorreu o ciberataque, a equipe

trabalhou de maneira colaborativa oferecendo apoio e ajuda uns aos outros. Podemos tomar como exemplo a seguinte fala:

"*Os meus colegas são muito bem instruídos e têm bastante conhecimento sobre o sistema, então pudemos trabalhar em uma solução em conjunto e encontrar formas de garantir que o problema não voltasse a acontecer*" (P.11).

"Numa situação de ciberataque na verdade, a gente tem que envolver todos, de diversas áreas. E o apoio e a colaboração de cada um deles é essencial. Eles têm que se apoiar, tem que colaborar, tem que manter a calma e raciocinar. Esse raciocínio, essa calma e essa colaboração é o faz a gente ter sucesso nessas situações" (P.12).

Os dois outros entrevistados que anteriormente relataram poder contar com os colegas, disseram que não sabiam exatamente como a equipe reagiria e trabalharia numa ocorrência de ciberataque, pois nunca haviam sofrido um ataque.

Percebemos assim, que tanto o capital psicológico quanto o capital social são fortemente identificados nas falas dos participantes do presente estudo, onde notamos o capital social enquanto garantia de suporte entre os indivíduos e facilitador da ação coletiva; enquanto o capital psicológico ajuda na perceção de autoeficácia para enfrentar as adversidades.

Nesse sentido, o capital psicológico e igualmente o capital social, poderão ter potencial de influenciar o desempenho diante da situação típica de ciberataque e na avaliação de Recursos *vs.* Exigências.

5.7 Estratégias de *coping* reportadas

Ao longo da entrevista, questionamos aos participantes se eles tinham alguma estratégia para lidar com as exigências colocadas por uma situação de ciberataque, ou o que eles faziam para não deixar que as exigências o afetassem. Neste sentido, todos os participantes conseguiram relatar as suas estratégias e, algumas das vezes, relatavam mais de uma.

De acordo com a Tabela 1, que apresentou anteriormente as 12 famílias de *coping* que guiam teoricamente o nosso trabalho, identificamos nos relatos dos participantes apenas cinco delas: procura por suporte, autoconfiança, resolução de problema, isolamento e procura por informação. As demais categorias não serão abordadas a seguir, uma vez que não foram identificadas na amostra.

5.7.1 Procura de suporte

Nesta família de *coping*, o sujeito busca o contato e o conforto com os outros ou em uma ajuda instrumental. Neste sentido, o processo adaptativo busca coordenar a confiança e usar os recursos sociais disponíveis.

Pudemos perceber que 13 entrevistados (65%) citaram esse tipo de estratégia ao longo da entrevista, a exemplo das seguintes falas:

> "*Acho que a minha estratégia é manter a calma e confiar na equipe. Conversar, trocar conhecimentos entre a equipe. Porque é o que dizem: duas cabeças pensam melhor do que uma. Então eu me apoio bastante na minha equipe*" (P.20).

> *"Eu procuro a ajuda dos meus colegas, da minha equipe. Trocar conhecimento e experiências com eles, ajuda a enfrentar esse tipo de problema"* (P.17).

5.7.2 Autoconfiança

Diante dessa família de *coping*, existe uma regulação emocional e comportamental. Ao longo da entrevista, sete participantes (35%) citaram esse tipo de estratégia, o que pode ser observado, por exemplo, através das falas:

> *"Eu tento manter o autocontrole. Você não pode se deixar levar pelo fator emocional, pelo medo, pelo stress. Então eu me esforço para manter a cabeça fria, para controlar a situação"* (P. 12).

> "*A estratégia que eu tenho, não só pra situações de stress como um ciberataque, mas para lidar com o stress em geral, é tentar ao máximo zelar pela minha qualidade de vida. Além disso, eu tento ter uma estratégia de tentar manter a calma, sem fazer as coisas com correria, participando das reuniões com a direção, e tento transparecer para a equipe que está sob o controle*" (P.16).

5.7.3 Resolução de problema

Uma vez que esta família de *coping* refere-se ao processo adaptativo de coordenar as ações e contingências no ambiente, a pessoa procura estratetizar e planear a sua atuação, ter uma ação instrumental. Neste sentido, pode-se dizer que a pessoa ajusta as suas ações para ser mais efetivo.

Dos 20 participantes, seis deles (30 %) relataram esse tipo de estratégia em algum momento da entrevista. Podemos tomar como exemplo as falas a seguir:

"*Eu tento sempre primeiro entender o que está acontecendo ali, porque entendendo isso, eu já consigo ter na minha cabeça uma linha de como fazer o processo inverso que o atacante fez, para tentar mitigar isso o mais rápido possível. Então eu tento estratetizar, criar na minha cabeça uma lista de prioridades, identificando cada ponto, e assim fica mais fácil para identificar como é que o ataque começou, de onde partiu, e porque isso ocorreu*" (P.13).

"Acho que me ajuda estabelecer um passo a passo das tarefas e procedimentos para identificar o problema e resolver." (P.3).

5.7.4 Isolamento

Na família de *coping* Isolamento, existe uma retração social, dissimulação e evitação aos outros. Ou seja, uma retração ao contexto sem apoio. Dos entrevistados, dois (10%) citaram esse tipo de estratégia em uma situação de ciberataque, como podemos perceber nas seguintes falas:

"*Me isolar em uma sala e tentar trabalhar com foco, sem a interferência de pessoas. Porque o quando você tem um incidente, a grande maioria das pessoas ficam atrás de ti, te pressionando para que você resolva logo. E isso não ajuda, só atrapalha. Então o isolamento é a melhor estratégia, sem pessoas por perto tentando te pressionar*" (P.15).

"Pra enxergar melhor o problema você tem que meio que se isolar, às vezes... Colocar um fone de ouvido, ouvir uma música, e tentar focar pra entender o que está acontecendo e tentar acabar com aquele problema que está acontecendo. Acho que essa é uma estratégia minha para manter a calma e o auto controle" (P.2).

5.7.5 Procura por informação

Ainda seguindo o processo adaptativo no qual o sujeito procura coordenar as suas ações e contingências do ambiente, apenas um participante (5%) citou a estratégia de *coping* da família Procura por Informação. Neste caso, ele recorre à leitura, observação e até mesmo pergunta aos outros sobre o acontecimento, para encontrar contingências adicionais. O P.10 relata:

"*Eu acho que em uma situação assim eu tento acessar todo o conhecimento que eu tenho, e todas as fontes de conhecimento possíveis, para tentar resolver a situação*".

Dentre as estratégias supracitadas, percebemos que a maioria dos participantes refere adotar estratégias de *coping* de aproximação, cujas funções são mais adaptativas e funcionais (Antoniazzi et al., 2009). Nesse caso, classificamos como estratégias de aproximação a procura por suporte, autoconfiança, resolução de problema e procura por informação. Algumas vezes os participantes fazem ainda referência a mais de uma estratégia de aproximação, em momentos diferentes.

Apenas a estratégia de isolamento, aqui relatada, pode ser classificada como estratégia de evitação, por ser menos adaptativa e levar à retração social. Ainda assim, o número de entrevistados que recorre a essa estratégia é muito pequeno (apenas 10% da amostra).

Neste sentido, apesar das especificidades do contexto de cada participante, podemos dizer que, de modo geral, a amostra lida com a situação de ciberataque de uma forma ajustada e funcional.

5.8 Dados quantitativos

Como foi citado anteriormente, ao longo da entrevista tivemos também questões seguindo uma Escala Visual Analógica, em que o participante apontava na escala o que melhor representava a sua resposta.

Neste sentido, pudemos realizar uma análise estatística acerca dessas respostas, utilizando o Software SPSS. Para isso, medimos em centímetros as distâncias do ponto de partida da escala ao ponto em que os participantes indicavam. O valor mínimo que podiam responder era 0 e o valor máximo da escala era 12,5.

A seguir, a Tabela 4 apresenta os dados relativos à Estatística Descritiva.

Tabela 4

Estatística Descritiva

	Mínimo	Máximo	Média	Desvio Padrão	Assimetria	Curtose
Probabilidade de acontecer um ciberataque	2.00	12.50	8.06	3.70	-0.36	-1.40
A situação interfere nas suas atividades diárias / vida profissional	2.60	12.50	8.65	3.23	-0.73	-0.77
É uma situação ameaçadora para si	0.00	12.50	7.58	3.75	-0.65	-0.69
Está inclinado para receber formação voltada para o *stress*	0.00	12.50	10.46	3.86	-2.26	4.32
Está inclinado para receber formação voltada para a *cibersecurity*	7.00	12.50	11.42	1.82	-1.70	1.86
A situação representa um risco para si	0.00	11.00	6.77	3.54	-0.59	-0.76
Gravidade das consequências para si	0.00	12.50	8.95	3.57	-1.19	0.89

Nota. N = 20

Os resultados da Tabela 4 revelam uma distribuição normal da amostra. Os valores de assimetria e curtose encontram-se abaixo dos índices recomendados (2 para a assimetria e 7 para a curtose; Curran, West, & Finch,1996), à exceção da variável "Está inclinado para receber formação voltada para o *stress*", que tem o valor de assimetria ligeiramente superior a 2.

A Tabela 5 revela as médias das respostas dos participantes para cada uma das perguntas de Escala Visual Analógica.

Tabela 5

Médias das respostas

	Média	Desvio Padrão	Erro padrão da média
Probabilidade de acontecer um ciberataque	8.06*	3.70	0.82
A situação interfere nas suas atividades diárias / vida profissional	8.65*	3.23	0.72
É uma situação ameaçadora para si	7.58	3.75	0.83
Está inclinado para receber formação voltada para o *stress*	10.46*	3.86	0.86
Está inclinado para receber formação voltada para a *cibersecurity*	11.42*	1.82	0.40
A situação representa um risco para si	6.77	3.54	0.79
Gravidade das consequências para si	8.95*	3.57	0.79

Notas. N = 20

**. As médias encontram-se significativamente distantes do valor médio da escala (i.e., 6.25) a p < .05 (teste de uma amostra com método Bootstrap – 1000 amostras – intervalo de confiança a 95%).*

A partir dos dados apresentados na Tabela 5, percebemos que as médias das respostas podem ser consideradas significativas, quando comparadas com o ponto médio da escala (6,25), à exceção das variáveis "É uma situação ameaçadora para si" e "A situação representa um risco para si". O teste foi realizado utilizando do método Bootstrap, a fim de acrescentar confiança nos resultados, tomando em consideração o tamanho relativamente pequeno da amostra.

A seguir, a Tabela 6 apresenta as correlações entre as variáveis das questões de Escala Visual Analógica, utilizando o coeficiente de Spearman, sendo que nem todas elas possuem correlações significativas.

Tabela 6

Correlações entre as variáveis

	Q.1	Q.4.1	Q.5	Q.13.3	Q.13.4	Q.16	Q.18
Q.1							
Correlação de Spearman	1.000	0.652**	0.733**	0.465*	0.402	0.393	0.537*
Sig.		0.00	0.00	0.03	0.07	0.08	0.01
Q.4.1							
Correlação de Spearman	0.652**	1.000	0.537*	0.362	0.406	0.114	0.188
Sig.	0.00		0.01	0.11	0.07	0.63	0.42
Q.5							
Correlação de Spearman	0.733**	0.537*	1.000	0.411	0.351	0.554*	0.466*
Sig.	0.00	0.01		0.07	0.12	0.01	0.03
Q.13.3							
Correlação de Spearman	0.465*	0.362	0.411	1.000	0.756**	-0.011	0.105
Sig.	0.03	0.11	0.07		0.00	0.96	0.66
Q.13.4							
Correlação de Spearman	0.402	0.406	0.351	0.756**	1.000	0.059	0.228
Sig.	0.07	0.07	0.12	0.00		0.80	0.33
Q.16							
Correlação de Spearman	0.393	0.114	0.554*	-0.011	0.059	1.000	0.690**
Sig.	0.08	0.63	0.01	0.96	0.80		0.00
Q.18							
Correlação de Spearman	0.537*	0.188	0.466*	0.105	0.228	0.690**	1.000
Sig.	0.01	0.42	0.03	0.66	0.33	0.00	

Notas. N = 20

***. A correlação é significativa no nível 0,01 (2 extremidades).*

**. A correlação é significativa no nível 0,05 (2 extremidades).*

Q.1 = Probabilidade de acontecer um ciberataque; Q.4.1 = A situação interfere nas atividades diárias / vida profissional; Q.5 = É uma situação ameaçadora para si; Q.13.3 = Está inclinado para receber formação voltada para o stress; Q.13.4 = Está inclinado para receber formação sobre cibersecurity; Q.16 = A situação representa um risco para si; Q.18 = Gravidade das consequências para si.

Sig. = Significância (2 extremidades)

Podemos perceber através dos valores apresentados na Tabela 6 que a variável Q.1 (Probabilidade de acontecer um ciberataque) possui correlação positiva e significativa com as variáveis Q.4.1, Q.5, Q.13.3 e Q.18, sendo que a correlação com as variáveis Q.4.1 e Q.5 é mais forte. Ou seja, quanto mais os participantes julgam provável acontecer um ciberataque na sua organização, mais eles percebem uma grande interferência dessa situação na sua atividade diária ou vida profissional e mais sentem-se ameaçados por esse tipo de situação.

Ainda que a correlação seja um pouco mais fraca, podemos inferir também que quanto mais os participantes consideram provável acontecer um ciberataque, percebem uma maior gravidade das consequências do mesmo para si e estão mais interessados em participar de formações relacionadas ao *stress*.

Também é possível inferir a partir dos dados estatísticos que a variável Q.5 (É uma situação ameaçadora para si) está positivamente correlacionada com o quanto um ciberataque interfere nas atividades diárias e na vida profissional dos participantes, representa um risco para si próprio, e com a gravidade percebida das consequências de uma situação de ciberataque para si mesmo.

Relativamente ao tema das formações, as variáveis "Está inclinado para receber formação sobre *cibersecurity*" e "Está inclinado para receber formação voltada para o *stress*" apresentam uma forte correlação significativa e positiva. Ou seja, quando os participantes relatavam estar inclinados a participar de uma formação relacionada com novas formas de lidar com o *stress* em uma situação de ciberataque, estavam também inclinados a participar de uma formação técnica sobre cibersegurança.

6. DISCUSSÃO

Tendo como objetivo geral estudar os efeitos de um ciberataque enquanto potencial estressor para os trabalhadores de TICs, pudemos perceber que as evidências apontam para a premissa de que os participantes do presente estudo reportam a ocorrência de ciberataque como um estressor.

Neste sentido, a fala dos participantes quanto aos efeitos de uma situação de ciberataque revela que, em sua maioria, os entrevistados encaram essa ocorrência como uma situação de *distress*, onde o *stress* traz consequências patológicas por haver um desequilíbrio entre o esforço, tempo, realização e resultados (Romero, Oliveira & Nunes, 2007).

Segundo Robbins (2005), o *stress* é frequentemente associado a limites e exigências, ou seja, representa um confronto para o indivíduo gerando uma dúvida ou incerteza a respeito de oportunidades, limitações que precisam ser superadas e perdas que precisam ser evitadas. Em congruência com a teoria, a preocupação, dúvida e incerteza foram temas levantados com elevada frequência na fala dos participantes.

No entanto, lembramos ainda que Robbins (2005) ressalta que embora altos níveis de *stress* possam ter efeitos negativos, o *stress* em determinadas circunstâncias pode oferecer um potencial de ganho. Nesse mesmo sentido, Romero, Oliveira, e Nunes (2007) levantam o conceito de *eustress* como uma situação onde há um equilíbrio entre o esforço dispendido, tempo, realização e os resultados atingidos. Nestes casos o *stress* passa a ser um aspecto positivo para lidar com as pressões e vencer desafios.

Sabemos que a perceção de um estímulo como fonte estressora depende não só da relação do indivíduo com o ambiente, mas também da sua própria avaliação e fatores intrínsecos (Maturana & Valle, 2014). Apesar disso, percebemos que a maioria dos participantes retratam o ciberataque como uma situação de *distress*, enquanto apenas um participante enxerga tal ocorrência com o potencial positivo do *eustress*.

Tornou-se ainda evidente que todos os participantes reconhecem a possibilidade de acontecer um ciberataque na infraestrutura para a qual trabalham. Muitos atribuem a vulnerabilidade dos sistemas informáticos ao facto de a tecnologia estar em constante evolução. Neste mesmo sentido, Finomore e colegas (2013) confirmam que os adversários que tentam invadir e destruir as infraestruturas, têm se tornado cada vez mais sofisticados em seus ataques.

Diante disso, como defendem Steinke e colegas (2016), é importante desenvolver nestes trabalhadores recursos pessoais como a criatividade e inovação, para que possam ser eficazes ao manter o sistema fora do alcance dos *hackers*.

Importam aqui não só as ferramentas e softwares para a proteção dos sistemas, mas torna-se fundamental compreender os aspectos psicológicos envolvidos nessa relação homem-máquina para prever comportamentos e assim treinar os profissionais a terem respostas mais eficazes em situações de ciberataque que podem ser geradoras de *stress*.

Segundo Robbins (2005), podemos identificar ao menos 3 fontes potenciais de *stress* para o trabalhador: fatores ambientais (incertezas econômicas, mudanças ou ameaças políticas, incertezas tecnológicas e o terrorismo), fatores organizacionais (exigências de tarefas e papéis, exigências interpessoais, a estrutura organizacional, o tipo de liderança, dentre outros), e fatores individuais (questões familiares, problemas econômicos e características de sua própria personalidade). O trabalho aqui exposto explora os 3 tipos de potenciais estressores.

Podemos perceber que a situação de ciberataque pode ser considerada um fator ambiental gerador de *stress,* já que é um risco a que estão expostos diariamente e não se pode negar e controlar a incerteza tecnológica. Além disso, a análise estatística demonstra que quando percebem uma maior probabilidade de acontecer um ciberataque, os participantes sentem-se mais ameaçados e consideram que a situação tem graves consequências para si.

Os fatores organizacionais podem ser observados através das falas dos participantes, que dizem que a ocorrência de ciberataque gera uma maior demanda de tarefas e papéis no seu trabalho e, assim sentem-se mais “pressionados”.

Já os fatores individuais podem ser explorados nas falas dos participantes que consideram ou não ter em si atributos pessoais que lhes ajudam a lidar com as exigências colocadas por uma situação de ciberataque. Neste sentido, foram levantados temas como calma e paciência, auto controle, concentração e resiliência.

Vimos que cada participante vivenciou o conflito gerado pela ocorrência de ciberataque de uma forma distinta, evidenciando em seus relatos formas particulares de lidar com os problemas e angústias emergentes nessa situação.

Como objetivo específico, buscamos identificar os recursos e exigências associadas à situação de ciberataque que os participantes identificavam, sabendo que quando um indivíduo avalia os recursos disponíveis como superiores às exigências impostas, ele encara a situação como um desafio; mas quando a avaliação dá-se de forma oposta a situação é encarada como ameaça (Anderson et al., 2014).

Segundo Blascovich e Mendes (2000), as exigências referem-se à avaliação de perigo, esforço do indivíduo durante a situação e incerteza. Já os recursos podem ser definidos como a perceção de habilidades e conhecimentos importantes para o desempenho diante de uma determinada situação.

Neste sentido, pudemos perceber que as exigências mais relatadas pelos participantes foram um maior esforço físico e mental gerados por uma maior carga de trabalho; o sentimento de incerteza e insegurança; um maior *stress*, ansiedade e pressão; o senso de urgência para responder e agir para a mitigação do ciberataque; e os sentimentos de medo, perigo e preocupação.

Relativamente aos recursos, os participantes citaram o capital psicológico como recurso para lidar com as exigências. Nessa mesma perspectiva, segundo Çelik (2018) o capital psicológico pode ser um grande aliado contra o *stress*, sendo possível trabalhar e desenvolver as 4 dimensões de competências pessoais que compõem este conceito: auto-eficácia, otimismo, esperança e resiliência.

Nesse sentido, os participantes citaram como recursos, indicadores de capital psicológico como: o seu conhecimento, experiência profissional e atributos pessoais como traços de personalidade.

No entanto, também tivemos indicadores de capital social como recurso identificados pelos participantes. O capital social pode ser definido como as relações institucionalizadas e reconhecidas, que criam valores como confiança, aumentam a eficiência e facilitam a ação coordenada (Babcicky & Seebauner, 2017).

Assim, o apoio social foi um tema bastante frequente na fala dos participantes, enquanto recurso disponível. Diante da fala de vários participantes, percebemos que, para eles, o capital social é fundamental para lidar com o *stress* em situações de ciberataque. Neste sentido, os resultados deste estudo encontram respaldo teórico em autores como Babcicky e Seebauner (2017), que defendem que o capital social ajuda no processo de adaptação, ação coletiva, atua como um catalizador da perceção de auto-eficácia, bem como representa um grande suporte entre os sujeitos.

Tomando em consideração que numa ocorrência de ciberataque a perceção dos recursos disponíveis e as exigências sentidas pelos indivíduos são um fator fundamental para a forma com que lidam com aquela situação, respondemos a mais um objetivo específico: perceber quais são as estratégias dos trabalhadores para enfrentar o *stress* ocupacional que vão para além do recurso ao capital psicológico e considerando igualmente o capital social.

Para isso, apoiamo-nos na literatura de Domingos e colegas (2020), que salientam que a avaliação dos recursos e exigências influenciam ainda nas estratégias de *coping* escolhidas inconscientemente para enfrentar aquela situação (Domingos et al., 2020).

Dentre as 12 estratégias de *coping* utilizadas como base para estre trabalho, apenas 5 foram mencionadas pelos participantes: procura por suporte (65%), autoconfiança (35%), resolução de problema (30%), isolamento (10%) e procura por informação (5%).

Percebemos novamente nas estratégias de *coping* reportadas, que o capital social aparece como um fator de destaque, sendo que 65% dos participantes adotam a estratégia procura por suporte, buscando o contato e o conforto com os outros para enfrentar a situação de ciberataque.

Vimos ainda que a maioria dos participantes mencionaram estratégias de *coping* de aproximação, ou seja, estratégias adaptativas e funcionais (Antoniazzi et al., 2009). São exceção os participantes que mencionaram a estratégia de isolamento, onde há a retração social, dissimulação e evitação aos outros. Esse tipo de estratégia pode ser considerada uma estratégia de evitação, sendo menos adaptativa.

Segundo Domingos e colegas (2020), quando o resultado da avaliação recursos/exigências é encarado como desafio, são adotadas estratégias de *coping* baseadas na aproximação. Neste sentido, podemos inferir que a maioria dos participantes deste estudo consideram seus recursos disponíveis superiores às exigências impostas e, portanto, encaram a situação como um desafio, em vez de uma ameaça.

Tal facto pode ser constatado também através da análise estatística, onde notamos que a média de respostas para a pergunta “É uma situação ameaçadora para si” não é significativamente maior do que o ponto médio da escala.

Neste sentido, ainda que os participantes tenham retratado a ocorrência de um ciberataque como uma situação de *distress*, a maioria deles encontra estratégias eficazes para lidar com aquela situação e se comportam de forma adaptativa em vez de reativa, voltando-se para a resolução do problema.

É importante ainda ressaltar que as estratégias de *coping* são parte de processos adaptativos e por isso formam um ciclo, que passa pela detecção e avaliação da ameaça, preparação da resposta e regulação da ação, e finalmente recuperação e aprendizagem. Sendo assim, a situação de *stress* gera uma aprendizagem e isso pode alterar e influenciar as partes anteriores do ciclo em situações futuras (Skinner & Zimmer-Gembeck, 2015).

Assim, sabe-se que caso o indivíduo tenha uma boa consciência dos recursos disponíveis tanto a nível do capital psicológico e considerando igualmente o capital social, isso leva-o a adotar de estratégias de *coping* positivas para lidar com o *stress* gerado por uma situação de ciberataque. A partir disso, torna-se possível desenvolver intervenções e instrumentos voltados para o desenvolvimento e reconhecimento de tais recursos, que garantam respostas cada mais eficazes diante de situações como as relatadas aqui.

Nesse sentido, apesar de a literatura apontar que pouca atenção é dispendida para o elemento humano na cibersegurança, enquanto a maior preocupação é com os sistemas e ferramentas (Finomore et al., 2013), percebemos, através dos dados estatísticos neste estudo, que os participantes estariam abertos e interessados em receber formações voltadas para o seu desenvolvimento pessoal e focadas na componente psicológica. Na verdade, vimos que os participantes estavam inclinados a receber tanto formações técnicas sobre cibersegurança, quanto formações voltadas para novas formas de lidar com o *stress* gerado por um ciberataque.

Assim, o facto de, muitas vezes, as organizações não adotarem abordagens voltadas para o lado psicológico e subjetivo dos trabalhadores, pode não estar ligado ao desinteresse dos mesmos em participar de ações dessa natureza. Pelo contrário, vimos que a referida amostra demonstrou inclinação para ações voltadas para o *stress*.

Nesse sentido, confirma-se a importância de trabalhar não só os sistemas informáticos, mas incluir a componente humana, levando em consideração as competências, habilidades e capacidades dos indivíduos, a fim de mitigar erros e tornar ainda mais eficaz a cibersegurança das organizações (Zaccaro et al., 2016). Assim, faz-se fundamental que os psicólogos organizacionais sensibilizem os gestores nesse sentido.

Sabemos, no entanto, que apesar de todos os contributos e implicações desta investigação, durante a realização deste trabalho enfrentamos algumas limitações.

Primeiro, é importante destacar que as conclusões e generalizações apresentadas aqui são baseadas nos dados colhidos em uma amostra composta por apenas 20 trabalhadores, maioritariamente jovens, de sexo masculino e com um alto nível de escolaridade. Assim, salientamos que, apesar de na pesquisa qualitativa o tamanho da amostra não estar diretamente ligado com a profundidade e complexidade dos dados recolhidos, a amostra relativamente pequena torna difícil a generalização dos resultados encontrados para a população como um todo. Nesse sentido, é possível que os resultados sejam apenas um retrato da amostra.

Além disso, chegar até os profissionais de TICs foi um processo bastante difícil e trabalhoso porque, em geral, as empresas não demonstravam grande abertura para a realização

das entrevistas com os seus colaboradores. Muitas das vezes, as empresas e os próprios colaboradores demonstravam-se desconfiados e receosos para falar sobre um assunto delicado como a cibersegurança. Devido a isso, a explicação sobre o objetivo da entrevista e explicitação do campo de estudo em psicologia eram sempre muito bem abordados na apresentação, a fim de ultrapassar essa barreira.

Outra limitação encontrada foi que, apesar de a investigadora ter alguma experiência com ferramentas de recolha de dados como as entrevistas, as mesmas foram realizadas por meio virtual, devido à condição de isolamento social imposto pela pandemia Covid-19. Nesse sentido, a separação do entrevistador/entrevistado por uma tela pode tornar um pouco mais difícil a criação do *raport*, e do clima de abertura tão importante na realização das entrevistas. Por esse motivo e pensando nas implicações que este fator poderia ter nos critérios de qualidade dos resultados deste trabalho, houve uma atenção maior e preocupação na preparação das entrevistas e nos primeiros contatos com os participantes.

Além disso, por se tratar de uma amostra bastante homogénea no que diz respeito ao género (trata-se de uma amostra maioritariamente masculina), é possível que este fator tenha influenciado em alguns resultados obtidos. Segundo Matud (2004), o género pode influenciar diversos elementos envolvidos no processo de *stress*, inclusive nas respostas ao elemento estressor e estratégias de *coping* adotadas.

Apesar das limitações supracitadas, futuras investigações podem ser feitas tomando como partida os resultados aqui encontrados. Continua ainda sendo importante que mais investigações sejam feitas sobre este tema, sob o enfoque da metodologia qualitativa, uma vez que a revisão de literatura mostrou escassez de estudos a partir dessa ótica.

Nesse sentido, incentivamos o pensamento crítico e a ousadia para o uso dessa metodologia, que oferece novos caminhos, bem como novas e inexploradas possibilidades de construção de conhecimento nessa área.

Como referido anteriormente, futuras investigações no âmbito do ciberataque enquanto fonte de *stress*, sob a ótica dos recursos e exigências, podem ainda trazer grandes contributos. Por exemplo, uma investigação voltada para a criação e validação de um instrumento que possa ser aplicado nas organizações, como forma de treinamento e sessões de formação, visando desenvolver nos colaboradores a capacidade de reconhecer os recursos disponíveis e aumentar a sua resiliência, incentivando comportamentos de *coping* mais adaptativos.

Além disso, em nosso estudo, vimos que apesar de a procura de informação ter sido uma estratégia identificada, apenas um participante faz referência a esse tipo de estratégia de *coping*.

Era expectável que houvesse uma maior procura de informação, a fim de restabelecer o controlo percebido sobre a situação.

No entanto, percebemos que os participantes estavam inclinados a receber tanto formações técnicas sobre cibersegurança, quanto formações voltadas para novas formas de lidar com o *stress* gerado por um ciberataque. Portanto, podemos inferir que apesar de a procura por informação ter sido uma estratégia pouco relatada, os participantes ainda não consideravam ter informação o suficiente e estavam abertos para receber mais formações. Neste sentido, o motivo da baixa adoção deste tipo de estratégia pode ser alvo para futuras pesquisas, uma vez que este resultado pode ser reflexo de diversos fatores, como por exemplo a perceção individual da relevância da informação como recurso.

Deixamos ainda, como proposta para investigações futuras, explorar a relação de causalidade de como o capital psicológico e o capital social poderão influenciar no desempenho diante de uma situação de ciberataque.

7. CONCLUSÕES

Entendendo os ciberataques como algo que tem recebido bastante destaque na atualidade e que os crimes informáticos tem sido cada vez mais reportados pelas autoridades, percebemos que esses eventos podem trazer consequências não só para a infraestrutura alvo da invasão, mas também pode ter grandes consequências a nível profissional e psicológico para os trabalhadores ligados aos sistemas informáticos.

Para além do tecnoestresse, definido pelos efeitos psicossociais negativos advindos do uso das TIC (Portella, 2019), buscamos aqui entender o ciberataque enquanto um potencial estressor e de que forma os profissionais entrevistados respondiam aos recursos e exigências impostas nessa situação, considerando o capital psicológico e, igualmente, o capital social.

Neste sentido, podemos dizer que os objetivos do presente estudo foram alcançados, sendo que conseguimos responder às questões aqui levantadas.

Alcançamos o objetivo geral ao evidenciar que os trabalhadores de TICs entrevistados reportam uma situação de ciberataque como um fator estressor, identificando essa ocorrência como uma situação de *distress*. E atingimos os objetivos específicos, identificando quais os recursos e exigências percecionados pelos trabalhadores na ocorrência de um ciberataque, e quais as estratégias adotadas por eles para enfrentar o *stress* ocupacional gerado por essa situação.

Os resultados das entrevistas realizadas com 20 trabalhadores de TICs mostraram que, em sua maioria, os participantes encaram a ocorrência de ciberataque como uma situação de *distress*. Apesar disso, eles conseguem percecionar a situação como um desafio em vez de ameaça, através do balanceamento entre recursos disponíveis e exigências, o que os leva a adotarem estratégias de *coping* adaptativas, ou seja, estratégias de aproximação.

De acordo com as 12 categorias de coping (vide Tabela 1) propostas por Skinner e colegas (2003), as estratégias de aproximação observadas neste estudo foram: procura por suporte, autoconfiança, resolução de problema e procura por informação.

Ficou também evidente a importância do capital psicológico, bem como do capital social, como recursos para os trabalhadores durante a ocorrência de um ciberataque.

Sendo assim, a realização desta investigação contribui de diversas formas para a sociedade como um todo: produz conhecimento no universo académico; permite a aplicação desse conhecimento em atividades práticas no universo do trabalho e contribui de forma metodológica nas investigações acerca do *stress*, sob a perspectiva dos recursos e exigências.

Sabendo que a sociedade atualmente é marcada pela informatização e que, por isso, os profissionais de TICs lidam com questões sobre a cibersegurança diariamente, o presente estudo permite entender a relação entre os recursos e exigências percepcionados pelos profissionais em situações de ciberataque e quais estratégias de enfrentamento eles adotam nessas circunstâncias. Nesse sentido, traz implicações práticas ao possibilitar que os psicólogos organizacionais desenvolvam e apliquem ferramentas voltadas para desenvolver o capital socio-psicológico dos trabalhadores, aumentando assim a sua resiliência em situações de ciberataque e promovendo o bem-estar.

Essas ferramentas podem ser, por exemplo, um Sistema de Treinamento de Resiliência ao *Stress* ou mesmo técnicas de formação que visem o aumento e desenvolvimento do bem-estar dos profissionais de TICs, baseados na evidência científica aqui exposta.

Além disso, o contributo e implicação teórica ficam aqui evidentes ao possibilitar uma compreensão mais aprofundada do ciberataque enquanto um fator estressor e o processo que evolve a perceção e reação a ele.

Apontamos também as implicações metodológicas, uma vez que o enfoque qualitativo foi uma condição ímpar, quando comparado às pesquisas que anteriormente foram realizadas sobre este assunto, as quais empregavam a metodologia quantitativa. Assim, reforçamos através de entrevistas semi-estruturadas e da Análise Temática, a força da pesquisa qualitativa enquanto produção de conhecimento.

Os resultados aqui encontrados apontam ainda para a importância de novas e mais investigações a respeito do tema, visando desenvolver ferramentas que corroborem com o trabalho do psicólogo dentro das organizações no sentido de desenvolver a resiliência dos trabalhadores, e treiná-los para a adoção de estratégias de *coping* mais eficazes e adaptativas diante da ocorrência de ciberataques.

REFERÊNCIAS BIBLIOGRÁFICAS

Alevato, H. (2009). Tecnoestresse: entre o fascínio e o sofrimento. *Boletim Técnico do Senac*. *35*(3), 60-75. Recuperado em 17 de julho de 2020 de https://www.bts.senac.br/bts/article/view/238/221

Anderson, A. A. Brossard, D., Scheufele, D. A., Xenos, M. A., & Ladwig, P. (2014). The ‘‘Nasty Effect:’’ Online Incivility and Risk Perceptions of Emerging Technologies. *Journal of Computer-Mediated Communication*. *19*(3), 373-387. doi: 10.1111/jcc4.12009

Antoniazzi, A. S., Souza, L. K., & Hutz, C. S. (2009). Coping em situações específicas, bem-estar subjetivo e autoestima em adolescentes. *Gerais: Revista Interinstitucional de Psicologia*, *2*(1), 34-42. Recuperado em 08 de julho de 2020, de http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1983-82202009000100005&lng=pt&tlng=pt.

Babcicky, P., & Seebauer, S. (2017). The two faces of social capital in private flood mitigation: opposing effects on risk perception, self-efficacy and coping capacity. *Journal of Risk Research*, *20*(8), 1017-1037. doi: 10.1080/13669877.2016.1147489

Barbosa, M. A. S., Silva, M. R., & Nunes, M. S. C. (2017). Pesquisa qualitativa no campo Estudos Organizacionais: explorando a Análise Temática. In Associação Nacional de Pós-Graduação e Pesquisa em Administração (Ed.) *Anais eletrônicos da 41º Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração*, 41º Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração. São Paulo: AnPAD. Recuperado em 21 de julho de 2020, de http://ri.ufs.br/jspui/handle/riufs/7085

Blascovich, J., & Mendes, W. B. (2000). Challenge and threat appraisals: the role of affective cues. In J. Forgas (Ed.), *Studies in emotion and social interaction, second series. Feeling and thinking: the role of affect in social cognition* (pp. 59-82). New York, USA: Cambridge University Press.

Boni, V., & Quaresma, S. J. (2005). Aprendendo a entrevistar: como fazer entrevistas em ciências sociais. *Revista Eletrônica dos Pós Graduandos em Sociologia Política da UFSC*, *2*, 68-80. Recuperado em 10 de setembro de 2018 de https://periodicos.ufsc.br/index.php/emtese/article/view/18027/16976

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3* (2), 77-101. doi: 10.1191/1478088706qp063oa

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior. 68,* 190-209. doi:10.1016/j.chb.2016.11.018

Carlotto, M. S. (2010). Fatores de risco do tecnoestresse em trabalhadores que utilizam tecnologias de informação e comunicação. *Estudos de psicologia (Natal). 15*(3), 319-324. doi: 10.1590/S1413-294X2010000300012

Carlotto, M. S., & Câmara, S. G. (2010). O tecnoestresse em trabalhadores que atuam com tecnologia de informação e comunicação. *Psicologia: Ciência e Profissão, 30*(2), 308-317. doi: 10.1590/S1414-98932010000200007

Çelik, M. (2018). The Effect of Psychological Capital Level of Employees on Workplace Stress and Employee Turnover Intention. *Innovar*, *28*(68), 67-75. doi: 10.15446/innovar.v28n68.70472

Christensen, J. C., Everitt, B. D., Chartrand, D., & Boeke, D. K. (2014). *Evaluation of the Stress Resilience Training System*. Air Force Research Laboratory. doi: 10.21236/ada612432

Coleta, A. S. M. D., & Coleta M. F. D. (2008). Fatores de estresse ocupacional e coping entre policiais civis. *Psico-USF*, *13*(1), 59-68. doi: 10.1590/S1413-82712008000100008

Comissão Europeia (1999). *Guidance on work-related stress: spice of life or kiss to death?*. Luxembourg: European Communities.

Corradini, I., Marano, A., & Nardelli, E. (2014). Work-related stress risk assessment: a critical review based on psychometric principles of an objective tool. *Social Science Open Access Repository*. Recuperado em 14 de outubro de 2018, de https://nbn-resolving.org/urn:nbn:de:0168-ssoar-441923

Correia, P. M. A. R., & Jesus, I. O. A. (2016). Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas. *Revista Direito GV*, *12*(2), 542-563. Recuperado em 23 de setembro de 2018, de http://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/63635

Correia, P. M. A. R., Santos, S. I. S., & Correia, M. C. A. R. F. (2017). Perceções sobre Cibersegurança e Privacidade em Portugal: Evidências Estatísticas de Igualdade e Desigualdade Homem-Mulher. *Revista Latino-Americana de Geografia e Género. 8*(1), 35-50. Recuperado em 23 de setembro de 2018, de https://revistas2.uepg.br/index.php/rlagg/article/view/8062/pdf4

Curran, P. J., West, S. G., & Finch, J. F. (1996). The robustness of test statistics to nonnormality and specification error in confirmatory factor analysis. *Psychological Methods*, *1*(1), 16-29. doi:10.1037/1082-989X.1.1.16

Decreto-Lei n.º 62/2011 de 9 de Maio. Diário da República n.º 89/2011, Série I de 2011-05-09. Lisboa: Ministério da Defesa Nacional. Recuperado em 07 de agosto de 2018, de https://dre.pt/pesquisa/-/search/286758/details/maximized

Dictionary.com (2020). Recuperado em 07 de agosto de 2018, de https://www.dictionary.com/browse/cyberattack

Domingos, S., Gaspar, R., Fonseca, H., & Marôco, J. (2020). DeCodeR framework: data collection and coding for demands and resources appraisal in extreme weather events. *PsyEcology*, *11*(1), 90-103. doi: 10.1080/21711976.2019.1643988.

Finomore, V., Sitz, A., Blair, E., Rahill, K., Champion, M., Funke, G.,…Knott, B. (2013). Effects of Cyber Disruption in a Distributed Team Decision Making Task. *Proccedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1), 394-398. doi: 10.1177/1541931213571085

Fontanella, B. J. B., Ricas, J., & Turato, E. R. (2008). Amostragem por saturação em pesquisas qualitativas em saúde: contribuições teóricas. *Cadernos de Saúde Pública. 24*(1), 17-27. doi: 10.1590/S0102-311X2008000100003

Fortin, M. F. (1999). Métodos de amostragem. In M. F. Fortin (Ed.), *O processo de investigação: da concepção à realização* (pp.201-214). Loures: Lusociência.

Frangopoulos, E. D., Eloff, M. M., & Venter, L. M. (2013). Psychosocial risks: Can their effects on the security of information systems really be ignored?. *Information Management & Computer Security*. *21*(1), 53-65. doi: 10.1108/09685221311314428

Gaspar, R., Barnett, J., & Seibt, B. (2015). Crisis as seen by the individual: the norm deviation approach. *Psyecology, 6*(1), 103-135. doi: 10.1080/21711976.2014.1002205

Godoy, A. S. (1995). Introdução à pesquisa qualitativa e suas possibilidades. *Revista de Administração de Empresas*, *35*(2), 57-63.

Helkala, K., Knox, B., Jøsok, Ø., Lugo, R., Sütterlin, S. (2016). How Coping Strategies Influence Cyber Task Performance in the Hybrid Space. In Stephanidis C. (Eds.) *HCI International 2016 - Posters' Extended Abstracts*, 18ª International Conference on Human-Computer Interaction. Communications in Computer and Information Science (Vol. 617, pp. 192-196). Toronto: Springer. doi: 10.1007/978-3-319-40548-3_32

Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks. 57*(10), 2206–2211. doi: 10.1016/j.comnet.2012.11.023

Luthans, F., Youssef, C. M. (2004). Human, social, and now positive psychological capital management: Investing in people for competitive advantage. *Organizational Dynamics*, *33*(2), 143–160. doi: 10.1016/j.orgdyn.2004.01.003

Matud, M. P. (2004). Gender differences in stress and coping styles. *Personality and Individual Differences*. *37* (7), 1401-1415. doi: 10.1016/j.paid.2004.01.010

Maturana, A. P. P. M., & Valle, T. G. M. (2014). Estratégias de enfrentamento e situações estressoras de profissionais no ambiente hospitalar. *Psicologia Hospitalar*, *12*(2), 02-23. Recuperado em 02 de outubro de 2018, de http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1677-74092014000200002&lng=pt&tlng=pt

Melo, E. A. A. (2006). *Vínculo do trabalhador com a organização: Um estudo de representações sociais.* (Tese de Doutoramento). Programa de Pós-Graduação em Psicologia, Instituto de Psicologia, Universidade de Brasília. Brasília. Brasil. Recuperado em 02 de julho de 2020, de https://repositorio.unb.br/handle/10482/3669

Minayo, M. C., & Sanches, O. (1993). Quantitativo-Qualitativo: Oposição ou Complementaridade? *Cadernos de Saúde Pública*. *9*(3), 239-262. doi: 10.1590/S0102-311X1993000300002

Parker, S. K., Winslow, C. J., & Tetrick, L. E. (2016). Designing meaningful, healthy and effective ciber security work. In: S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A Steinke (Eds.), *Psychosocial Dynamics of Ciber Security*. (pp. 240 -266). New York: Routledge.

Portella, U. A. (2019). *Percepção de Tecnoestresse em profissionais de TI.* (Dissertação de mestrado). Programa de Pós-Graduação Stricto Sensu em Gestão do Conhecimento e Tecnologia da Informação, Universidade Católica de Brasília. Brasília. Brasil. Recuperado em 17 de julho de 2020, de https://bdtd.ucb.br:8443/jspui/handle/tede/2753

Robbins, S. (2005). *Comportamento Organizacional*. (11ª Ed). São Paulo: Pearson Prentice Hall.

Romero, S. M., Oliveira, L. O., & Nunes, S. C. (2007). Estresse no ambiente organizacional: estudo sobre o corpo gerencial. In Associação Educacional Dom Bosco. *Anais do IV Simpósio de Excelência em Gestão e Tecnologia*, IV Simpósio de Excelência em Gestão e Tecnologia. Rio de Janeiro: SEGeT. Recuperado em 08 de julho de 2020, de https://www.aedb.br/seget/arquivos/artigos07/1215_SEGET0701Stress.pdf

Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of ciber-security and precautionary behaviour. *Computers in Human Behavior*. *75*, 547-559. doi: 10.1016/j.chb.2017.05.038

Skinner, E. A., Edge, K., Altman, J., & Sherwood, H. (2003). Searching for the Structure of Coping: A Review and Critique of Category Systems for Classifying Ways of Coping. *Psychological Bulletin*. *129*(2), 216-269. doi: 10.1037/0033-2909.129.2.216

Skinner, E. A., & Zimmer-Gembeck, M. (2015). Coping across the lifespan. In *International Encyclopedia of the Social & Behavioral Sciences* (2ª ed.; pp. 887-894). doi: 10.1016/B978-0-08-097086-8.26015-7

Steinke, J. A., Fletcher, L., Niu, Q., & Tetrick L. E. (2016). In S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.), *Psychosocial Dynamics of Ciber Security*. (pp. 111-134). New York: Routledge.

Ugale, A. R. & Ghatule A.P. (2011). A comparative study of effect of job characteristics on stress of IT-Professionals and IT-Teachers. In International Proceedings of Economics Development and Research (Ed.), *International Proceedings of Economics Development and Research's Archive*, 2011 International Conference on Economics, Trade and Development (Vol. 7, pp. 98-102). Singapura: IACSIT Press. Recuperado em 07 de agosto de 2018, de http://www.ipedr.com/vol7/21-D10006.pdf

Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Steinke, J. A. (2016). The psychosocial Dynamics of Ciber Security. In S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.) P*sychosocial Dynamics of Ciber Security*. (pp. 1-13). New York: Routledge.

ANEXO 1. Guião de Entrevista

Parte 1: Instruções Iniciais

Ao longo deste estudo, vou fazer-lhe algumas perguntas. Por vezes vou pedir-lhe que dê a resposta oralmente, segundo as suas palavras. Noutras vezes, você deverá dar as respostas apontando com o dedo no local indicado. Logo lhe darei um exemplo de como fazer, para que fique mais claro.

Não há respostas certas nem erradas. O importante é que suas respostas sejam sinceras e descrevam o melhor possível aquilo que pensa ou sente no momento.

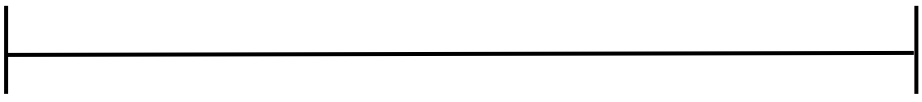
Aqui está um exemplo de cada um dos tipos de perguntas que estarão presentes neste estudo:

1. **Pergunta de resposta oral:** Pense num dia típico no seu dia-a-dia de trabalho. Pode descrever-me em que pensou?

2. **Pergunta de resposta apontando com o dedo:** Qual é a probabilidade de não conseguir cumprir com um prazo de entrega de um trabalho?

   Para responder a essa pergunta, coloque o dedo sobre a linha, no local que pensar que melhor representa sua resposta

Muito pouco provável — Extremamente provável



Quanto mais perto das pontas da linha colocar o dedo, mais forte é o seu sentimento. Ou seja, quando mais perto do extremo esquerdo, maior o seu sentimento de que a situação é muito pouco provável, e quanto mais perto do extremo direito, maior o seu sentimento que a situação é extremamente provável de acontecer.

Alguma dúvida?

Então agora vamos começar.

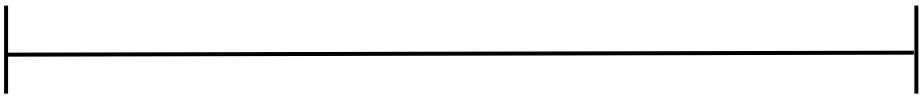
Parte 2: Evocação da situação e exploração da mesma

Os ataques informáticos ou **ciberataques** podem ser definidos como uma tentativa de danificar, provocar disrupção ou ganhar acesso não autorizado a um computador, sistema informático ou rede de comunicações eletrónicas[1]. Os ciberataques podem ter como alvo pessoas, grupos, empresas/organizações e nações, bem como serviços e infra-estruturas críticas – instalações físicas e de tecnologia de informação, redes, serviços e ativos.

Q1. Você acredita que a organização para qual trabalha está sob risco de sofrer um ciberataque?

Q1.1 Para você, qual a probabilidade disso acontecer?

Muito pouco provável Extremamente provável



Q2. A empresa para qual traballha já sofreu algum tipo de ciberataque?

Q2.1 Que tipo de ciberataque?

Q2.2 Descreva o que seria uma situação típica de ocorrência de um ciberataque na sua empresa. *Peço que pense naquilo que é comum neste tipo de situações, nas características típicas destas situações.*

Q3. Nesta situação típica de ocorrência de um ciberataque na sua empresa que referiu, quais seriam seus comportamentos nesta (o que você faria)?

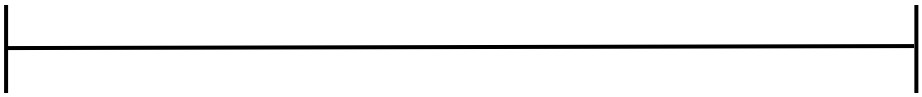
Q4. A situação típica em que pensou anteriormente, interfere de alguma forma com a sua vida profissional ou com alguma atividade profissional que faça normalmente no seu dia a dia? (Se sim) Em que aspeto(s)?

Q4.1. Em que grau é que a situação típica em que pensou anteriormente, interfere ou não interfere com a sua vida profissional ou com alguma atividade profissional que faça normalmente no seu dia a dia?

[1] www.dictionary.com/browse/cyberattack

Não interferiu nada com a minha vida profissional

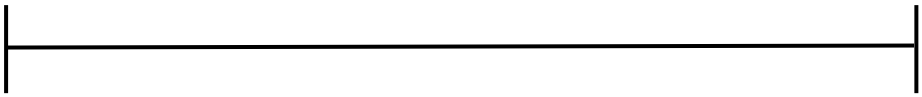
Interferiu extremamente com a minha vida profissional



Q5. Em que medida é que a situação típica em que pensou é uma situação ameaçadora para si?

Nada ameaçadora

Extremamente ameaçadora



Q6. Você considera que os computadores, sistemas informáticos e a rede de comunicações da empresa para qual trabalha são vulneráveis a ameaças de segurança?

Q6.1 (Se sim) A que se deve essa vulnerabilidade?

Q7. Você acha que os órgãos de gestão da organização para qual trabalha demonstram preocupação e apoio à prevenção de situações de Ciberataques como a que descreveu anteriormente?

Q7.1 (Se sim) Quais são as medidas tomadas que o levam a pensar que sim?

Parte 3: Exploração dos recursos e exigências na situação típica

Q8. Considera que situações típicas de um Ciberataque à sua empresa como aquela em que pensou são situações que lhe colocam exigências, ou seja, perigo, incerteza e esforço (dificuldades e barreiras) para o seu trabalho, que em circunstâncias normais não teria ou que teria menos?

Q8.1. (Se sim) Qual ou quais considera serem essas exigências, ou seja, perigo, incerteza e esforço?

Q8.2. (Se sim) Tendo em conta o nível de exigências que as situações típicas de um Ciberataque como aquela em que pensou têm para si, o que você faz para lidar com essas exigências ou impedir que estas o afetem?

Q9. Qual ou quais considera serem os recursos (conhecimentos, atributos pessoais, etc) que você pode usar para enfrentar as exigências colocadas pelas situações típicas de Ciberataque

como aquela em que pensou (o que você pode fazer para lidar com situações de um Ciberataque como aquela em que pensou)?

Q9.1 Tem acesso a todos esses recursos?

Q9.2 Para além desses recursos, existem recursos aos quais você não tem acesso?

Q10 Na situação em que você pensou anteriormente, você podia compartilhar informações sobre o ciberataque com outras pessoas dentro da sua organização ou era exigido que houvesse secretismo (sigilo)? Até que nível você podia falar sobre o acontecimento dentro da empresa?

Q10.1 Você podia falar sobre o acontecimento com pessoas de fora da empresa? Se sim, você escolheu fazê-lo?

Q10.2 Você acha que manter a situação em segredo pode influenciar a forma como você lida com um ciberataque? Quais as consequências disso para a empresa? E para você?

Q11. Tem alguma estratégia ou estratégias para lidar com as exigências colocadas por situações de um Ciberataque como aquela em que pensou?

Q11.1 (Se sim) Qual (quais)?

Q12. Você considera que tem em si algum atributo pessoal que o ajudaria a lidar com as exigências colocadas por situações de um Ciberataque como aquela que pensou? (Se o participante tiver dificuldade, referir como atributos pessoais o seu conhecimento, habilidades, características de personalidade, etc)

Q12.1 (Se sim) Qual (Quais)?

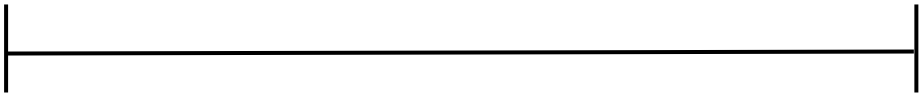
Q13. Você acha que a empresa poderia tomar alguma medida para desenvolver em seus funcionários estratégias para lidar com o risco de ocorrer uma situação de Ciberataque como aquela que você pensou?

Q13.1 (Se sim) Quais medidas seriam essas?

Q13.2 Quais seriam custos e benefícios para a empresa diante da adoção de tais medidas?

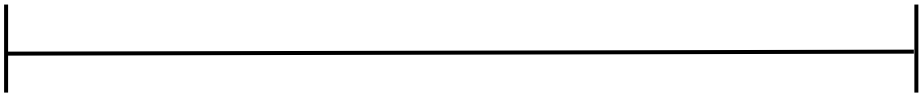
Q13.3 Quão inclinado(a) estaria para receber formação voltada para novas formas de lidar com o estresse gerado por um ciberataque?

Nada inclinado Muito inclinado



Q13.4 Quão inclinado(a) estaria para receber formação adicional em cibersegurança, se a sua organização fizesse essa oferta?

Nada inclinado Muito inclinado



Q14. Diante da situação típica de um Ciberataque que pensou, você sente que pode contar com a ajuda de seus colegas de trabalho para enfrentar esta situação?

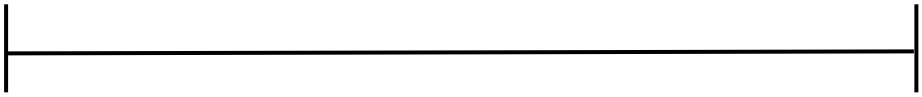
Q14.1 O que seus colegas de trabalho fizeram diante da situação típica que você descreveu anteriormente?

Q15. Com base em vários estudos efetuados acerca dos Ciberataques, sabe-se que existe um risco cada vez maior de no futuro esses ataques se tornarem mais frequentes. O que considera que poderá fazer para evitar estes Ciberataques?

Q15.1 O que considera que poderá fazer para evitar que o medo de que aconteçam Ciberataques no seu ambiente de trabalho afetem a sua atividade laboral diária?

Q16. Em que medida é que situações de Ciberataques como aquela em que pensou representam um risco para si?

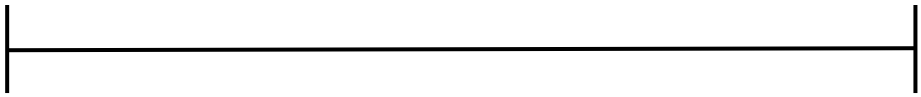
Risco muito mais baixo que o normal Risco muito mais alto que o normal



Q17. Quais as consequências que as situações típicas de Ciberataques como aquela em que pensou podem ter para si?

Q18. Como classifica o grau de gravidade ou severidade que essa(s) consequências podem ter para si?

Nada graves Extremamente graves



Parte 4: Dados socio-demográficos e questões de controlo

Q19. Idade

Q20. Género

Q21. Nível de Escolaridade

Q22. Há quanto tempo trabalha nesta organização?

Q23. Qual a sua função? Há quanto tempo trabalha nesta função?

Q24. Já trabalhou anteriormente em alguma outra organização que considera que também estava sob o risco de sofre um Ciberataque? Que tipo de organização?

Q25. Gostaria de acrescentar alguma informação adicional acerca do tema da pesquisa e as situações descritas anteriormente?