JOÃO PAULO FIÚZA DA SILVA

O DESENVOLVIMENTO DE COMPETÊNCIAS-CHAVE EM CIBERNÉTICA POR PROFISSIONAIS QUE NÃO SÃO DE TI:

uma análise dos possíveis impactos sobre a resiliência cibernética das organizações

Trabalho de Conclusão de Curso – Ensaio Científico - apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso Superior de Segurança e Defesa Cibernética (CSSDC).

Orientador: Cel R/1 João de Azevedo.

Rio de Janeiro

2023

C2023 ESG

Documento assinado digitalmente
gov.br
JOAO PAULO FIUZA DA SILVA
Data: 17/03/2024 17:05:08-0300
Verifique em https://validar.iti.gov.br

_____

JOÃO PAULO FIÚZA DA SILVA

RESUMO

O presente ensaio foi elaborado com o objetivo de analisar os impactos da aquisição ou desenvolvimento de competências em cibernética para profissionais que não são da área de Tecnologia da Informação (TI) para a resiliência cibernética desta mesma organização. Para tanto, foi realizada uma pesquisa de base bibliográfica para a revisão de literatura a respeito do tema proposto, seguida de uma análise teórica sobre a relação entre resiliência e competências. A tese estipulada é de que a aquisição de competências em ciber contribui para a resiliência cibernética das organizações. Ao final, restou demonstrado que o desenvolvimento de competências em ciber para profissionais que não são de TI contribuem apenas parcialmente para a resiliência cibernética, de forma complementar às demais ações encetadas com este propósito.

Palavras-chave: resiliência cibernética; competências; segurança da informação; segurança cibernética.

ABSTRACT

This essay was prepared with the objective of analyzing the impacts of the acquisition or development of cybernetic skills for professionals who are not from the Information Technology (IT) area on the cybernetic resilience of this same organization. To this end, bibliographical research was carried out to review the literature on the proposed topic, followed by a theoretical analysis on the relationship between resilience and skills. The stipulated thesis is that the acquisition of cyber skills contributes to the cyber resilience of organizations. In the end, it was demonstrated that the development of cyber skills for non-IT professionals only partially contributes to cyber resilience, in a complementary way to other actions undertaken for this purpose.

Keywords*: cyber resilience; competencies; information security; cybersecurity.*

SUMÁRIO

1 INTRODUÇÃO

O termo cibernética teria sido utilizado pela primeira vez, no sentido que atualmente é tão naturalizado na sociedade atual, pelo matemático americano Nobert Viener, na década de 1940, ao publicar a obra *Cybernetics: or the Control and Communication in the Animal and the Machine*[1]. A proposta de Viener, seria a criação da ciência Cibernética, determinada a estudar e criar possibilidades que mudariam o paradigma da relação entre homem, máquina e sociedade, partindo da premissa de que seria possível aumentar o controle daquela sobre a maquinaria e a própria sociedade, por meio da criação de computadores e outros autômatos (KIM, 2004).

Embora haja uma variedade de compreensão e definições do que venha a ser a cibernética, ou o espaço cibernético ou até mesmo o domínio cibernético, após passados mais de 80 anos da publicação da obra seminal de Viener, é certo que o termo cibernética e todas as derivações decorrentes de combinações com outras palavras e expressões estão mais comuns e cotidianas, totalmente incorporadas às práticas, processos e relações sociais e profissionais.

Cibernética ou simplesmente Ciber, hodiernamente é objeto de interesse difuso da sociedade, das organizações, dos Estados e das forças militares e de defesa, vez que passou a representar uma miríade de tecnologias combinadas representadas por itens como computadores, softwares, redes, sistemas de telecomunicações, criptografia, dados, pessoas e tantas outras que formam as camadas física, lógica e humana do denominado espaço cibernético (VASQUEZ, 2020).

O fato é que há uma crescente exponencial da dependência das organizações do espaço cibernético, especialmente com a incorporação de novas tecnologias como a computação em nuvem, *blockchain*, Inteligência Artificial (IA), Internet das Coisas (IoT), dentre outros, que estão cada vez mais presentes nos seus processos de negócio. Tais mudanças, por via de consequência, as expõe a riscos e ataques até então não enfrentados, criando um ambiente incerto, volátil,

[1] Cibernética: ou o Controle e a Comunicação no Animal e na Máquina (tradução livre do autor).

complexo e ambíguo (BODEAU; GRAUBART; LADERMAN, 2014; GALLARDO, 2021).

Tal ambiência faz com que haja um aumento do número de ciberataques e de uma maior busca e exploração de vulnerabilidades por parte de agentes mal-intencionados. É o que demonstra os dados do site especializado *Security,* publicados em reportagem de janeiro de 2023, dando conta de que número de ataques cibernéticos em âmbito global aumentou 38% em 2022, quando comparado com o ano de 2021 (ANDERSON, 2023).

Muitos destes ataques ou incidentes cibernéticos têm como vetor o fator humano das organizações, ou seja, são profissionais que nelas trabalham e acabam contribuindo de forma involuntária, por falta de conhecimento, como afirma Malagutti (2022) ou de forma maliciosa. Segundo dados divulgados por RISCO AUMENTA (2023), mais de 60% dos ataques cibernéticos registrados no ano de 2022 foram provocados pelos denominados *insiders*[2] negligentes.

Dado todo este contexto, o presente ensaio tem por objetivo responder a seguinte pergunta de pesquisa: “Quais os impactos do investimento no desenvolvimento de competências-chave em cibersegurança, nos profissionais que não são da área de Tecnologia da Informação (TI), para a resiliência cibernética de uma organização?”.

A tese proposta para este ensaio é de que a aquisição ou desenvolvimento de competências em ciber pelos profissionais citados contribuem sim para a resiliência cibernética da organização afetada.

Para alcançar o desígnio proposto, este ensaio terá objetivo exploratório, pois pretende-se inaugurar a discussão sobre competências em ciber para profissionais que não da área de TI e sua contribuição para a resiliência cibernética de uma organização.

O método de raciocínio utilizado foi o indutivo, pois pretendeu-se estabelecer uma relação entre a aquisição de competências em ciber por profissionais que não são de TI e os efeitos gerados sobre a resiliência cibernética de uma organização, não de forma particularizada, mas em sentido geral.

[2] Expressão usada para designar pessoas que trabalham em uma organização e são vetores de ataques cibernéticos (Nota do autor).

A análise proposta foi realizada em duas etapas. A primeira consistiu em revisar a literatura a respeito do tema e delinear os contornos da segunda etapa. Vencida a primeira etapa, definiu-se pela adoção do modelo denominado *Cybersecurity Capability Maturity Model* (C2M2) para definir as categorias analíticas a serem consideradas como parâmetros de verificação, em nível teórico e abstrato, sobre quais competências deveriam ser desenvolvidas e como elas de fato contribuiriam para a resiliência mensurada pelo citado modelo.

Na segunda etapa de análise, as competências mapeadas na literatura foram relacionadas com as categorias do modelo C2M2, de modo a analisar em que nível elas impactariam a resiliência cibernética.

Para cumprir a proposta, além desta introdução, este trabalho está estruturado em mais quatro seções. A seção 2 abordará a temática da resiliência cibernética, trazendo seus conceitos e fundamentos. A seção 3 cuidará de abordar a temáticas das competências em cibernética e a relação destas com resiliência cibernética. A seção 4 contém a análise e discussão proposta, seguida da seção 5 com as considerações finais.

2 RESILIÊNCIA CIBERNÉTICA: DEFINIÇÕES E FUNDAMENTOS PARA A SUA CONSTRUÇÃO

Para a discussão proposta neste ensaio, faz-se necessário introduzir algumas definições e fundamentos relacionados à resiliência cibernética. É o que se pretende fazer nesta seção, que cuidará de apresentar a definição do termo em análise. Além disso, tratará sobre quais são os pressupostos para que uma organização seja considerada detentora deste atributo.

2.1 Afinal, o que é resiliência cibernética?

O termo resiliência tem se popularizado no senso comum e é utilizado em diversas áreas do conhecimento humano, como a Psicologia, a gestão organizacional, a Física e mais recentemente, a cibernética, sempre como um

atributo desejável ao indivíduo ou organização analisada, ao representar a capacidade de resistir e se recuperar diante de agravos oriundos dos contextos em que o ente analisado está inserido.

Em recente publicação sobre o tema da resiliência cibernética, Ramirez (2021) discorre que o termo resiliência teria sua origem em uma tática do exército romano denominada *resilio*, que consistia em recuar diante de ataque do inimigo e logo depois avançar em contra-ataque, mas mudando de posição. Ainda segundo o autor, o termo foi mais tarde incorporado pela Física, para denominar "a propriedade de alguns materiais de retornar à sua forma original após tela perdido por alguma razão, ou ainda a capacidade de deformar-se sem romper-se", sendo depois apropriado por outras áreas do conhecimento humano (RAMIREZ, 2021, p. 97).

No contexto da segurança cibernética, o atributo da resiliência possui múltiplas definições, a depender do autor ou da entidade a abordar o tema, contudo, é possível perceber que há um núcleo comum em todas elas que é a capacidade da organização em manter suas operações e alcançar seus objetivos, a despeito dos riscos e ataques cibernéticos. É o que se depreende que das definições que serão apresentadas a seguir.

Para Carrasco (2015, p. 3) a resiliência cibernética ou ciber-resiliência são definidos da seguinte forma:

> [...] Resiliencia se define como una cualidad intrínseca, una característica propia de uma organización que le permite enfrentarse de forma exitosa a los cambios y a los eventos tanto internos como externos. La resiliencia forma parte de la naturaleza de dicho organismo y está implícita en su estructura.
>
> Ciber-resiliencia se ha definido partiendo de la definición de resiliencia y restringiendo las posibles fuentes de crisis a eventos tecnológicos y procedentes del ciberespacio, o también se ha definido limitando la dimensión afectada de la empresa a lo que son sus sistemas de proceso de datos y sus comunicaciones.[3]

[3] A resiliência é definida como uma qualidade intrínseca, uma característica de uma organização que lhe permite enfrentar com sucesso mudanças e acontecimentos, tanto internos como externos. A resiliência faz parte da natureza desse organismo e está implícita em sua estrutura.
A resiliência cibernética foi definida a partir da definição de resiliência e restringindo as possíveis fontes de crise a eventos tecnológicos e eventos do ciberespaço, ou também foi definida limitando a dimensão afetada da empresa a quais são os seus sistemas de processamento de dados e suas comunicações (Tradução livre do autor).

Björck *et al.* (2015, p. 312), de forma sintética e objetiva, definem a resiliência cibernética como a capacidade de continuar entregando as saídas pretendidas, a despeito de eventos adversos de fonte cibernética.

Para Gallardo (2021), por sua vez, a resiliência cibernética ou digital é a capacidade das organizações de aceitar, sobrepor-se, recuperar-se e superar-se (evoluir) diante dos riscos e ataques cibernéticos, exigindo, portanto, que elas sejam capazes de manter suas operações, mudarem e recuperarem-se rapidamente ante a qualquer adversidade que atente contra suas operações e as respectivas tecnologias da informação que as suportam.

Na mesma esteira está a compreensão do Decreto nº 10.222, de 2020, que aprovou a Estratégia Nacional de Segurança Cibernética (E-Ciber) que apresenta como um dos seus objetivos estratégicos aumentar a resiliência do país à ameaças cibernéticas e, embora não traga uma definição explícita do conceito do termo, sempre que faz referência a ele o emprega no sentido de manter a continuidade das operações e serviços considerados essenciais, como de infraestruturas críticas, por exemplo, a despeito dos riscos ou ataques cibernéticos.

Ser resiliente em termos cibernéticos pode ser definido, portanto, com a capacidade organizacional de identificar e gerenciar os riscos e eventos adversos de origem cibernética. Esta capacidade é resultante da combinação de processos, práticas, mentalidades e tecnologias que envolvem toda a organização de forma integrada e tem por objetivo garantir que esta previna, responda e se recupere de ataques cibernéticos, com foco no menor comprometimento possível em termos operacionais, financeiros, de relacionamento, de reputação, de direitos de terceiros, dentre outros. É neste sentido que o construto será considerado neste ensaio.

2.2 Construindo a resiliência cibernética de uma organização

Uma vez dada a definição da expressão resiliência cibernética, é necessário compreender como de fato ela se manifesta na realidade, isto é, afinal, quais são os atributos que permitem dizer uma organização é dotada de tal valência? E ainda,

como uma organização pode mensurar sua maturidade a respeito de suas capacidades neste aspecto em particular?

Para responder tais questionamento, é relevante, antes de tudo compreender que a resiliência em cibersegurança parte do pressuposto de que não é possível, especialmente diante do crescimento das capacidades, expertise e volição dos atacantes, manter a infraestrutura de Tecnologia da Informação (TI) imune aos ataques cibernéticos. Portanto, um conjunto de medidas devem ser adotadas para se evitar que esta infraestrutura seja comprometida e, ainda que haja algum nível de comprometimento, exista uma persistência das capacidades em manter as operações neste contexto (BODEAU; GRAUBART; LADERMAN, 2014; DICKSON; GOODWIN, 2020).

Destarte, não obstante a unidade do termo resiliência, sua aplicação prática guarda uma estreita relação com a necessidade de entendimento adequado do contexto de sua aplicação. Tal entendimento deve ser fundamentado na compreensão de qual é o negócio da organização e, portanto, quais variáveis e riscos serão relevantes de serem consideradas para o diagnóstico, planejamento e execução de estratégias que contribuirão para a aquisição de capacidades organizacionais no sentido da resiliência (BODEAU; GRAUBART; LADERMAN, 2014; CARRASCO, 2015; RAMIREZ, 2021).

Essas nuances decorrentes da variabilidade de negócios, organizações e respectivos contextos em que estão inseridos, fazem com que a compreensão dos parâmetros e medidas que evidenciam a resiliência cibernética de uma organização seja igualmente variada. Como relatam de Estay *et al.* (2020) em recente estudo, na mesma proporção em que há um evidente crescimento pela temática da resiliência, há uma proliferação de *framerworks* (modelos) para a avaliação da resiliência cibernética de organizações e entidades, os denominados *Cyber-resilience assessment Frameworks* ou CRF.

A menção a estes modelos no contexto deste ensaio é fundamental, na medida em que eles possuem dupla função. A primeira é avaliativa e informativa, ao apresentar o estado atual da organização ou entidade avaliada a partir de critérios padronizados e objetivos, devidamente reconhecidos por especialistas. A segunda é orientativa, pois antes mesmo de qualquer diagnóstico ou avaliação, é possível

saber quais aspectos deverão ser observados para que se construa a resiliência organizacional em cibernética. Esta função orientativa servirá de referencial para que se possa acoplar posteriormente os construtos da resiliência e da competência em cibernética, que é a proposta deste trabalho.

Dada a variedade de *frameworks* para a avaliação da resiliência cibernética de uma organização ou entidade e considerando a limitação de tempo e espaço deste ensaio, optou-se por desdobrar para fins de análise apenas uma das diversas possibilidades. Destarte, foram utilizadas como referência as recentes publicações de Azambuja e Souza Neto (2020), Ramirez (2021) e Malagutti (2022) que apresentam os diversos modelos, inclusive de forma comparativa, conforme será resumido no quadro 1 a seguir:

Quadro 1 – Modelos de avaliação de maturidade[4] em segurança cibernética
(continua)

Modelo	**Criador(a)**	**Enfoque**
Capability Maturity Model (CMM)	Universidade de Carnegie Melon (EUA)	Processos de implantação de software
Capability Maturity Model Integration (CMMI)	Universidade de Carnegie Melon (EUA)	Todos os processos de negócio de uma organização, divididos em metas genéricas (suporte) e específicas (negócio)
Cybersecurity Capability Maturity Model (C2M2)	Agência de Cibersegurança, Segurança Energética e Resposta a Emergência dos EUA	Implementação de práticas de gestão de segurança tanto para os ativos e e ambientes de Tecnologia da Informação, quanto para os de Tecnologia de Operação (TO)
NIST Cybersecurity Framework	*National Institute os Standards and Technology* (NIST) dos EUA	Proteção de infraestruturas críticas, a partir da adoção de princípios, melhores práticas e gestão de riscos.

[4] Embora os modelos façam referência a termos como maturidade em cibersegurança ou segurança cibernética, deve se ter em mente que a resiliência cibernética não é termo diverso, mas sim resultante desta maturidade ou conformidade em cibersegurança. (Nota do autor)

Quadro 1 – Modelos de avaliação de maturidade[5] em segurança cibernética (fim)

Modelo	Criador(a)	Enfoque
The Community Cyber Security Maturity Model (CCSMM)	Gregory B. White	Enfrentar as ameaças; definir métricas; compartilhar informações.
Melhoria dos Processos de Software Brasileiro (MPS-BR)	Associação para a Promoção da Excelência do Software Brasileiro (Softex)	Processos de desenvolvimento e implantação de software

Fonte: O Autor, 2023 (adaptado de AZAMBUJA; SOUZA NETO, 2020; RAMIREZ, 2021; MALAGUTTI, 2022).

Analisadas as características de cada um dos modelos apresentados, foi escolhido o modelo denominado C2M2 como base para de verificação dos componentes e atributos de uma organização resiliente em cibersegurança. A escolha se justificou pela abrangência e característica prescritiva do modelo, que está estruturado em domínios, objetivos e práticas. Considerando o objetivo deste ensaio, esta tríade facilita estabelecer uma relação com as competências em ciber, vez que esta última é meio para alcance daquela.

O modelo C2M2 está estruturado em 10 domínios[6]. Estes domínios, por sua vez, se desdobram em objetivos que derivam um total de 356 práticas em cibersegurança, sendo estas divididas por nível de maturidade (*OFFICE OF CIBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE*, 2022). O quadro 2 a seguir apresenta uma compilação dos domínios e respectivos objetivos do referido modelo, permitindo uma visão em alto nível do seu conteúdo:

Quadro 2 - Domínios e objetivos do modelo C2M2 (compilação)

[5] Embora os modelos façam referência a termos como maturidade em cibersegurança ou segurança cibernética, deve se ter em mente que a resiliência cibernética não é termo diverso, mas sim resultante desta maturidade ou conformidade em cibersegurança. (Nota do autor)

[6] Um domínio é um conjunto estruturado de práticas de cibersegurança com foco em uma área específica (OFFICE OF CIBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE, 2022, p. 21)

Domínio	Objetivos
Gestão de risco	Estabelecer a estratégia da gestão risco; Gerenciar o risco cibernético; Gestão das atividades.
Gestão de ativos, mudanças e configurações	Gerenciar o inventário de ativos; Gerenciar a configuração de ativos; Gerenciar as alterações de ativos; Atividades de gestão.
Gestão de identidade e acesso	Estabelecer e manter identidades; Controlar o acesso; Atividades de gestão.
Gestão de ameaças e vulnerabilidades	Identificar e responder às ameaças; Reduzir as vulnerabilidades; Atividades de gestão.
Consciência situacional	Realizar registro de *log's;* Realizar monitoramento; Estabelecer e manter uma estrutura operacional; Atividades de gestão.
Compartilhamento de informações e comunicações	Compartilhar informações; Atividades de gestão.
Resposta a eventos, incidentes e continuidade de operações	Detectar eventos; Escalar eventos e declarar incidentes; Responder a incidentes e eventos escalados; Plano de continuidade; Atividades de gestão.
Cadeia de suprimentos e gerenciamento de dependências externas	Identificar dependências; Gerenciar o risco da dependência; Atividades de gestão.
Gerenciamento da força de trabalho	Atribuir responsabilidades; Controlar o ciclo de vida da força de trabalho; Desenvolver a força de trabalho; Aumentar a conscientização em SegCiber; Atividades de gestão.
Gestão do programa de SegCiber	Estabelecer a estratégia do programa; Patrocinar o programa; Estabelecer e manter a arquitetura de SegCiber; Desenvolver *software* seguro; Atividades de gestão.

Fonte: AZAMBUJA; SOUZA NETO, 2020.

Como mencionado alhures, cada um dos domínios apresentados no quadro anterior é avaliado conforme os quatro níveis de maturidade seguintes, conforme o conjunto de práticas evidenciadas na análise:

- Nível 0: as práticas não existem;
- Nível 1: práticas iniciais são implementadas, mas podem ser incidentais;

- Nível 2: práticas são documentadas; recursos adequados são alocados para apoiar o processo; as práticas são mais completas em relação ao nível 1;

- Nível 3: as atividades são guiadas por políticas e diretrizes organizacionais; responsabilidade, accountability e autoridades sobre o desempenho; existem práticas de avaliação; práticas são mais completas que o nível 2 (OFFICE OF CIBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE, 2022, p. 25).

Importante, ressaltar, por fim, que não é objetivo deste ensaio aplicar o modelo C2M2 para alguma avaliação de caráter empírico, de modo que a apresentação de suas características constitutivas nesta seção se presta a fornecer as bases para a elaboração das categorias que subsidiarão a análise proposta como cerne deste trabalho.

3 COMPETÊNCIAS EM SEGURANÇA CIBERNÉTICA PARA PROFISSIONAIS QUE NÃO DE SÃO DE TI

Considerando o objetivo deste ensaio, que é de analisar em perspectiva teórica os possíveis impactos da aquisição de competências em segurança cibernética por profissionais que não são de TI para uma organização, necessário se faz compreender, primeiramente, o conceito de competência no contexto deste trabalho, para posteriormente adentrar-se na apresentação das competências em si, que são consideradas essenciais sob o enfoque proposto para este trabalho.

3.1 Breves definições sobre competências no contexto organizacional

O signo competência pode assumir múltiplos significados conforme o respectivo referente em que for utilizado. Para o contexto deste trabalho, o referencial é a Gestão por Competências, área do conhecimento que integra disciplinas como a Administração, a Psicologia, a Sociologia Organizacional, a Gestão do Conhecimento e da Informação, dentre outras, para promover o

recrutamento, a seleção, o desenvolvimento e avaliação de indivíduos e equipes com foco no alcance dos objetivos organizacionais (CARVALHO, 2015).

Como é possível perceber nestas considerações iniciais, embora possa haver diversidade na definição do conceito de competência, resta evidente que este construto, sob a perspectiva da Gestão por Competências, possui duas dimensões componentes: a existência de uma capacidade individual ou coletiva e a orientação desta capacidade para a missão da organização, seja ela pública ou privada (PRAHALAD; HAMEL, 1990; BRANDÃO; GUIMARÃES, 2001).

Neste sentido, Brandão *et al*. (2008, p. 877) definem competência humana ou profissional como “combinações sinérgicas de conhecimentos, habilidades e atitudes, expressas pelo desempenho profissional dentro de determinado contexto organizacional, que agregam valor a pessoas e organizações”. Fleury e Fleury (2001, p. 188), por sua vez, compreendem a competência como “[...] um saber agir responsável e reconhecido, que implica mobilizar, integrar, transferir conhecimentos, recursos e habilidades, que agreguem valor econômico à organização e valor social ao indivíduo”.

Denota-se, portanto, que a concepção de competência ultrapassa o mero domínio cognitivo, isto é, o saber algo ou possuir determinado conhecimento. É preciso que este conhecimento se converta em uma prática no ambiente organizacional e seja capaz de entregar algum resultado que seja de interesse da organização. Para tanto, exigirá do indivíduo ou de uma equipe a capacidade de combinar saberes, experiências, habilidades técnicas, gerenciais e emocionais, para a produção daquele resultado.

É neste sentido que a noção de competência será abordada neste trabalho, embora se reconheça que a adoção de metodologia exclusivamente teórico-analítica imponha limitações para a verificação teórico-empírica, mas estas poderão compor futura agenda de pesquisa.

3.2 Competências em segurança cibernética para profissionais que não são de TI

Como mencionado alhures, a resiliência cibernética, não obstante as variações de *frameworks*, é construída a partir da capacidade de identificar, prevenir, identificar, responder e se recuperar de riscos ou ataques cibernéticos e suas consequências (CARLTON; LEVY, 2017; BODEAU; GRAUBART; LADERMAN, 2014; DICKSON; GOODWIN, 2020).

Para tanto, as organizações precisam adotar um conjunto de estratégias e ações capazes de atuar nas três camadas da cibernética, a física, a lógica e a humana, observando-se para cada uma delas as suas peculiaridades e necessidades. Pela necessidade de domínio tecnológico, é fato que as camadas física e lógica dependem de alto nível de especialização técnica, sustentado por pessoal interno ou externo à organização, que em regra são representados pelos profissionais de TI[7].

De outro lado, a camada humana irá representar sempre o maior contingente de profissionais de qualquer organização, pois abarca, além dos próprios profissionais de TI, aqueles que atuam em todos os demais processos finalísticos, de suporte e gerenciais do negócio. Neste último caso, estão englobados os profissionais que não são de TI, mas que irão utilizar toda a infraestrutura de TI existente para realizar suas atividades profissionais e algumas pessoais.

Dada a relevância do fator humano para a resiliência cibernética, tal aspecto ocupa centralidade nas preocupações, planejamentos e estratégias de Estados e organizações públicas e privadas, buscando-se construir uma cultura de segurança no meio cibernético, inclusive extrapolando os limites da firma.

Tal preocupação está evidente, por exemplo, na Política Nacional de Segurança da Informação (PNSI) do Brasil, que estabelece como um dos seus princípios a “educação como alicerce fundamental para o fomento da cultura em

[7] Um profissional de TI é qualquer um que seja especializado nas subáreas da tecnologia da informação, ou seja, instalação, gerenciamento e manutenção de redes de computadores; análise e desenvolvimento de softwares e sistemas; gerenciamento e manutenção de hardware; administradores de bancos de dados; segurança da informação e cibernética etc. (MORENO; CAVAZOTTE, 2009).

segurança da informação” (BRASIL, 2018). O PNSI é sucedido pela E-Ciber, que estabelece como estratégia de número 2.3.10 “Elevar o nível de maturidade em segurança cibernética da sociedade, com o fim de ensejar a compreensão das ameaças e dos riscos no espaço cibernético, e possibilitar às pessoas o uso adequado e oportuno de procedimentos e de ferramentas em prol da utilização segura do ambiente digital [...]” (BRASIL, 2020).

O foco nas pessoas se justifica na medida em que há um consenso na literatura e nas publicações especializadas de que o fator humano é um dos principais de vulnerabilidades e ataques cibernéticos a dispositivos pessoais e infraestruturas de organizações e governos, decorrentes, principalmente da falta de conhecimento e de percepção de risco das pessoas diante de ameaças e estratégias dos atacantes. Investir em educação e aquisição de competências cibernética, portanto, torna-se um fator de fundamental relevância para a resiliência (CARLTON, 2016; MALAGUTTI, 2022).

Descendo para o nível estritamente organizacional, lócus da análise proposta para o trabalho, isto não é diferente. Conforme publicação recente do site especializado em cibersegurança CISO Advisor aponta que mais de 60% dos ataques a empresas tiveram como vetor o *insider*, ou seja, uma pessoa que compõe os quadros da organização, chamando a atenção para o fato de que o principal comportamento concorrente é a negligência, embora exista também os mal-intencionados (RISCO INTERNO AUMENTA, 2023).

Dado este cenário, investir no desenvolvimento de competências em ciber para o pessoal que não é de TI na organização, mostra-se como uma questão crucial para que ela se torne resiliente em termos cibernéticos. Fazer isto, inclusive, constitui um aspecto distintivo, como já defendia Mata (1995) em seu estudo sobre a TI como elemento de vantagem competitiva, quando ainda se vivia os primórdios da proliferação do domínio ciber.

Mas afinal, quais competências desenvolver? Para tentar responder esta pergunta em termos teóricos, procurou-se ao longo do trabalho encontrar estudos e publicações especializadas que abordassem o recorte escolhido, ou seja, abordar competências desejáveis para os profissionais que não são os especialistas em TI.

Foi possível constar que este é um tema ainda pouco estudado, ou pelo menos com poucas publicações a respeito, destacando-se os estudos dos autores americanos Melissa Carlton e Yair Levi, que em 2015 apresentaram uma proposta de uma plataforma de avaliação de habilidades em ciber para profissionais que não são de TI (CARLTON; LEVI, 2015). Posteriormente publicaram estudo sobre habilidades em ciber para para mitigar ameaças avançadas persistentes[8] (CARLTON; LEVI, 2017) e mais recentemente uma pesquisa sobre como mitigar ciber-ataques através da mensuração de habilidades em ciber dos profissionais que não são de TI (CARLTON; LEVI; 2019), baseado na tese de doutorado de Carlton publicada em 2016. Os autores são referência e, conforme informações do *Google Scholar*, os estudos mencionados foram citados por 253 publicações científicas até a data de elaboração deste ensaio.

Foi encontrado ainda o trabalho elaborado por Gracia-Granados e Bahsi (2020), que analisou as competências em cibersegurança nas organizações, mas apenas para cargos de gestão ou de tomada de decisão, utilizando o *framework* NIST. Contudo, considerado o objetivo deste ensaio, o escopo da pesquisa dos autores é muito restrito e aquém da abrangência ora pretendida.

Em face de todo o exposto, serão consideradas como referencial teórico de base os achados da pesquisa de Carlton (2016), segundo a qual seriam 9 as competências essenciais desejáveis para os profissionais que não são de TI de uma organização, para contribuir para a resiliência cibernética daquela. O estudo foi realizado com uma amostra de 188 profissionais, com a utilização de técnicas de autoavaliação, observação e avaliação de desempenho via plataforma eletrônica. As competências essenciais são as descritas no quadro 3 a seguir:

Quadro 3 – Competências principais em cibernética para profissionais que não são de TI em uma organização (continua)

Competência	**Descrição**
Prevenir o vazamento de informações para pessoas não autorizadas	Conhecer as ameaças e táticas de potenciais atacantes e aplicar medidas para prevenir a obtenção de dados e informações confidenciais em meio digital, por pessoas não autorizadas

[8] Tradução livre para o termo *Advanced Persistent Threat (APT)* que usa técnicas de invasão contínuas, clandestinas e sofisticadas para obter acesso a um sistema e permanecer dentro dele por um período prolongado, com consequências potencialmente destrutivas.

Quadro 3 – Competências principais em cibernética para profissionais que não são de TI em uma organização (fim)

Competência	Descrição
Prevenir *malware*[9] via sites inseguros	Conhecer e adotar práticas que evitem a infecção da infraestrutura (computadores, sistemas, dados, rede etc.) de TI da organização por *malware*, através de acesso a sites inseguros na internet
Prevenir a subtração de dados pessoais pela utilização de redes inseguras	Conhecer e adotar práticas que evitem a subtração de dados pessoais de identificação (nome, endereço, local de trabalho, informações familiares etc.) através da utilização de redes inseguras (públicas, sem criptografia etc.), pois elas podem facilitar procedimentos de exploração de senhas e credenciais de acesso
Prevenir *malware* via e-mail	Conhecer e adotar práticas que evitem a infecção da infraestrutura (computadores, sistemas, dados, rede etc.) de TI da organização por *malware*, enviados via e-mail, normalmente usando a técnica de *phishing*[10]
Prevenir a subtração de dados relativos a cartão de crédito, via sites inseguros	Conhecer e adotar práticas que evitem a subtração de dados de cartão de crédito (número, códigos de segurança, senhas etc.) através de sites inseguros
Prevenir o comprometimento de sistemas de informação pelo uso de dispositivos USB ou similares	Conhecer e adotar práticas que evitem a infecção de sistemas informatizados e infraestrutura de TI da organização pela utilização de dispositivos USB (pen drive, HD externo, cabos etc.)
Prevenir acessos indevidos a sistemas de informação através de exploração de senhas	Conhecer e adotar práticas que evitem a obtenção de credenciais de acesso a sistemas por pessoas não autorizadas, como guarda adequada de senhas, uso de senhas fortes, evitar acesso a sites inseguros etc.
Prevenir obtenção de dados pessoais de identificação via redes sociais	Conhecer e adotar práticas que evitem a obtenção indevida de dados pessoais de identificação por terceiros através de redes sociais (Whats App, Telegram, Facebook, Instagram, Tik Tok etc.)

Fonte: O Autor, 2023 (adaptado de CARLTON, 2016, p. 90; CARLTON; LEVI, 2019, p. 109).

Estas serão as competências consideradas para a seção de análise deste ensaio, vez que foram consideradas aquelas comuns a todos os profissionais de

[9] Malware é qualquer software intencionalmente feito para causar danos a um computador, servidor, cliente, ou a uma rede de computadores. Em regra, se aproveita de comportamentos negligentes do usuário para se instalar no dispositivo e agir. (Nota do autor)

[10] Técnica de ataque cibernética que consiste em atrair a vítima (pescar) usando uma informação que lhe possa chamar a atenção (isca), mas que contém links ou arquivos maliciosos. (Nota do autor)

uma organização que não são de TI. Como é possível perceber, são muito próximas do que se exigiria de qualquer pessoa em sua vida cotidiana, o que demonstra o quanto a dimensão cibernética encontra-se inserida em todos os contextos da sociedade contemporânea.

4 ANÁLISE E DISCUSSÃO

A revisão de literatura realizada neste ensaio deixa estreme de dúvidas que a construção da resiliência cibernética de uma organização decorre de um conjunto complexo de diagnósticos, planos, estratégias e ações direcionadas ao aperfeiçoamento dos componentes que compõem as camadas física (infraestrutura de telecomunicações, redes, computadores etc.), lógica (softwares, dados e sistemas) e humana (pessoas, processos e cultura).

Neste sentido, o desenvolvimento de competências em cibernética pertence naturalmente à dimensão humana. Ao considerar esta dimensão no âmbito organizacional, denota-se que ela pode ser dividida em dois grandes grupos: os profissionais que são de TI, inclusive os gestores desta área, e os que não de TI. Dada a conceituação apresentada por Moreno Jr. e Cavazotte (2009) anteriormente, por exclusão, não são de TI todos os demais profissionais de uma organização que não atuam diretamente com o gerenciamento e operação da infraestrutura de TI, isto é, com a instalação ou desenvolvimento, operação e manutenção de itens de rede, hardware, softwares e sistemas, bancos de dados, segurança da informação e cibernética.

Remarcadas tais diferenciações, passa-se analisar como a aquisição de competências consideradas essenciais em ciber pode contribuir para a construção da resiliência cibernética de uma organização ou ente.

Para este fim, foi estabelecida uma relação baseada em raciocínio lógico indutivo entre os domínios e objetivos do *framework* C2M2, apresentado na subseção 2.2 deste ensaio, e as competências consideradas essenciais em ciber descritas na subseção 3.3.

Como estabelecido nos aspectos metodológicos da introdução, para cada domínio e seu conjunto de objetivos foi analisado em que nível o conjunto de competências descritas por Carlton (2016) pode contribuir para que aqueles sejam plenamente implementados na organização e, consequentemente, a tornem mais resiliente. Esta análise foi realizada como base na avaliação do próprio autor, visto que uma das características do ensaio é ser opinativo e expositivo das suas ideias, sem a necessidade da realização de pesquisas extensivas ou intensivas no empírico.

Conforme será apresentado no quadro 4 a seguir, a classificação do grau de contribuição foi dada em três níveis: nada, parcialmente e contundentemente. Senão vejamos:

Quadro 4 – Análise da contribuição das competências tidas como essenciais por Carlton (2016) para o alcance dos domínios e objetivos do *framework C2M2 (continua)*

Domínio	**Objetivos**	**Competências essenciais contribuem?**
Gestão de risco	Estabelecer a estratégia da gestão risco; Gerenciar o risco cibernético; Gestão das atividades.	Nada
Gestão de ativos, mudanças e configurações	Gerenciar o inventário de ativos; Gerenciar a configuração de ativos; Gerenciar as alterações de ativos; Atividades de gestão.	Nada
Gestão de identidade e acesso	Estabelecer e manter identidades; Controlar o acesso; Atividades de gestão.	Parcialmente, apenas para o objetivo de “Controlar o acesso”
Gestão de ameaças e vulnerabilidades	Identificar e responder às ameaças; Reduzir as vulnerabilidades; Atividades de gestão.	Parcialmente, apenas para o objetivo “Reduzir as vulnerabilidades”
Consciência situacional	Realizar registro de *log’s;* Realizar monitoramento; Estabelecer e manter uma	Nada

	estrutura operacional; Atividades de gestão.	

Quadro 4 – Análise da contribuição das competências consideras essenciais por Carlton (2016) para o alcance dos domínios e objetivos do *framework C2M2* (fim)

Domínio	**Objetivos**	**Competências essenciais contribuem?**
Compartilhamento de informações e comunicações	Compartilhar informações; Atividades de gestão.	Nada
Resposta a eventos, incidentes e continuidade de operações	Detectar eventos; Escalar eventos e declarar incidentes; Responder a incidentes e eventos escalados; Plano de continuidade; Atividades de gestão.	Parcialmente, apenas em relação ao objetivo “Detectar eventos”
Cadeia de suprimentos e gerenciamento de dependências externas	Identificar dependências; Gerenciar o risco da dependência; Atividades de gestão.	Nada
Gerenciamento da força de trabalho	Atribuir responsabilidades; Controlar o ciclo de vida da força de trabalho; Desenvolver a força de trabalho; Aumentar a conscientização em SegCiber; Atividades de gestão.	Parcialmente, apenas em relação ao objetivo “Aumentar conscientização em SegCiber”
Gestão do programa de SegCiber	Estabelecer a estratégia do programa; Patrocinar o programa; Estabelecer e manter a arquitetura de SegCiber; Desenvolver *software* seguro; Atividades de gestão.	Nada

Fonte: O AUTOR, 2023.

Como demonstrado no quadro, o desenvolvimento das competências essenciais em ciber para profissionais que não são de TI não contribui contundentemente para nenhum dos 10 domínios e respectivos conjuntos de objetivos. Isto se explica pelo fato de todos eles possuírem um conteúdo intensivo em conhecimentos técnicos da área de TI, especialmente em segurança da

informação e cibernética. Quando se analisam os objetivos de cada um dos domínios é possível observar que alcançá-los depende de diagnósticos, planos e emprego de técnicas específicas, como a implantação e gerenciamento de soluções em prevenção e detecção de intrusões, por exemplo.

Por outro lado, é possível dizer que a aquisição das mesmas competências contribui parcialmente para 4 dos 10 domínios do modelo C2M2, sendo 1 objetivo para cada domínio.

Quanto ao domínio Gestão de Identidade e Acesso, a contribuição ocorre para o objetivo “Controlar o acesso”, na medida em que o fato de o profissional não TI prevenir ataques de *phishing* ou a exposição de seus pessoais em redes sociais, por exemplo, irá contribuir para as políticas e processos de controle de acesso estabelecidas pela área de TI da organização.

O mesmo ocorre com o domínio Gestão de Ameaças e Vulnerabilidades, que encontra contribuição para o objetivo “Reduzir vulnerabilidades”, posto que se os profissionais não TI previnem as infecções por malware, ransonware ou a utilização de dispositivos inseguros na infraestrutura de TI da organização, irão evitar a instalação de APT, por exemplo, e o risco de comprometimento de sistemas, dados e informações da organização e seus clientes ou usuários.

De igual modo, o domínio Resposta a Eventos, Incidentes e Continuidade de Operações, teria a contribuição das competências essenciais quanto ao objetivo “Detectar eventos”, posto que uma vez conhecedores das técnicas e tipos de ataques dos perpetradores, os profissionais não TI podem percebê-los mais facilmente e comunicar aos responsáveis pela gestão de incidentes da organização.

Por fim, quanto ao domínio Gerenciamento da Força de Trabalho, o desenvolvimento das competências-chave em ciber representaria o cumprimento do objetivo “Aumentar a conscientização em SegCiber”. Todas as competências descritas por Carlton (2016) e Carlton e Levi (2019) possuem um conteúdo de conscientização intrínseco na fase de recebimento dos elementos cognitivos a respeito das posturas preventivas que devem adotar. Agindo assim, irão evitar o comprometimento de dados, os ataques por agentes maliciosos e a exposição de

dados que possam servir de subsídio para elaboração de táticas por potenciais atacantes, como ocorre nos ataques de força-bruta[11], por exemplo.

Quanto aos domínios, não se verifica contribuição das competências essenciais para que sejam alcançados seus objetivos, posto que estes exigem outras que são típicas dos profissionais de TI, dado o nível de especialização exigido.

5 CONSIDERAÇÕES FINAIS

Considerando que o objetivo deste ensaio era analisar se o desenvolvimento de competências em cibernética em profissionais que não são de TI geraria algum impacto na resiliência cibernética de uma organização, constata-se que ele foi atingido integralmente, e que a tese inicial estabelecida, qual seja de que a aquisição de tais provocaria impactos positivos, foi confirmada.

Como restou evidenciado, embora o impacto seja limitado, a considerar todos os domínios e objetivos do modelo C2M2, ao menos 4 objetivos de 4 domínios são impactados positivamente, na medida em que diminui os riscos e vulnerabilidades para a ocorrência de incidentes cibernéticos que possam acometer a infraestrutura de TI da organização considerada. Há de se destacar que este mesmo raciocínio pode ser ampliado para outros contextos, como na prestação de serviços públicos digitais, por exemplo, protegendo o cidadão usuário e próprio ente estatal.

Ademais, é importante ressaltar que dado o caráter inicial e ainda opinativo que é típico de um ensaio acadêmico, seria interessante aprofundar na pesquisa sobre a relação estabelecida, aplicando-se procedimentos e técnicas que possam testar esta relação no campo empírico, para fins de confirmação ou refutação da tese ora apresentada.

[11] Técnica de intrusão em que o ataque obtém dados diversos da vítima e criar algoritmo para tentar quebrar uma senha, uma criptografia etc., por meio de tentativa e erro, ou seja, tentando diversas combinações. (Nota do autor)

REFERÊNCIAS

AZAMBUJA, Antonio João G.; SOUZA NETO, João. Modelo de maturidade de segurança cibernética para os órgãos da administração pública federal. **Revista do Serviço Público (Civil Service Review)**, v. 71, n. 3, 2020.

ANDERSON, Joy LePree. Global cyberattacks increased 38% in 2022. **Security**, 20 Jan. 2023. Disponível em: https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022. Acesso em: 29 out. 2023.

BJÖRCK, Fredrik et al. Cyber resilience–fundamentals for a definition. *In*: NEW Contributions in Information Systems and Technologies: [*S. l.*]: Springer International Publishing, 2015. v. 1, p. 311-316.

BODEAU, Deborah J.; GRAUBART, Richard D.; LADERMAN, Ellen R. Cyber resiliency engineering overview of the architectural assessment process. **Procedia Computer Science**, v. 28, p. 838-847, 2014.

BRANDÃO, Hugo P.; GUIMARÃES, Tomás A. Gestão de competências e gestão de desempenho: tecnologias distintas ou instrumentos de um mesmo constructo? **Revista de Administração de Empresas**, v. 41, n. 1, p. 8-15, 2001.

BRANDÃO, Hugo Pena et al. Gestão de desempenho por competências: integrando a gestão por competências, o balanced scorecard e a avaliação 360 graus. **Revista de Administração Pública**, v. 42, p. 875-898, 2008.

BRASIL. Decreto n. 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, 27 dez. 2018. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/56970098/do1-2018-12-27-decreto-n-9-637-de-26-de-dezembro-de-2018-56969938. Acesso em: 26 out. 2023.

BRASIL. **Decreto n. 10.222, de 5 de fevereiro de 2022.** Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**: seção 1, Brasília, DF, 06 fev. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 26 out. 2023.

CARLTON, Melissa; LEVY, Yair. Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. *In*: **SoutheastCon 2015**. [New York]: IEEE, 2015. p. 1-6.

CARLTON, Melissa. Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills. 2016. Dissertation (Doctor of Philosophy in Computer Information Systems) - Nova Southeastern University, Florida, 2016

CARLTON, Melissa; LEVY, Yair. Cybersecurity skills: Foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation. **Online Journal of Applied Knowledge Management (OJAKM)**, v. 5, n. 2, p. 16-28, 2017.

CARLTON, Melissa; LEVY, Yair; RAMIM, Michelle. Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. **Information & Computer Security**, v. 27, n. 1, p. 101-121, 2019.

CARRASCO, L. **Ciber-Resiliencia**. Madrid: Instituto Espanhol de Estudos Estratégicos, 2015.

CARVALHO, Ieda Maria Vecchioni. **Recrutamento e seleção por competências**. Rio de Janeiro: Editora FGV, 2015.

DICKSON, Frank; GOODWIN, Phil. **Five key technologies for enabling a Cyber-resilience framework**. [New York]: IBM, 2020. US45455119 White Paper.

ESTAY, Daniel A. Sepulveda et al. A systematic review of cyber-resilience assessment frameworks. **Computers & security**, v. 97, p. 101996, 2020.

FLEURY, Maria Tereza Leme; FLEURY, Afonso. Construindo o conceito de competência. **Revista de administração contemporânea**, v. 5, n. SPE, p. 183-196, 2001.

GALLARDO, Sara. Resiliencia digital. **Revista Sistemas**, n. 159, p. 66-81, 2021.

GARCIA-GRANADOS, F. Bahsi; BAHSI, Hayretdin. Cybersecurity knowledge requirements for strategic level decision makers. In: **International Conference on Cyber Warfare and Security**. Academic Conferences International Limited, 2020. p. 559-XIII.

KIM, Joon Ho. Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural. **Horizontes antropológicos**, v. 10, p. 199-219, 2004.

MALAGUTTI, Marcelo. **Ciberdefesa e cibersegurança**: um olhar brasileiro. Brasília, DF: Instituto Vegetius, 2022.

MATA, Francisco J.; FUERST, William L.; BARNEY, Jay B. Information technology and sustained competitive advantage: a resource-based analysis. **MIS quarterly**, p. 487-505, 1995.

MORENO JR, Valter de Assis; CAVAZOTTE, Flávia de Souza Costa Neves; FARIAS, Eduardo de. Carreira e relações de trabalho na prestação de serviços de tecnologia da informação: a visão dos profissionais de TI e seus gerentes. **JISTEM-Journal of Information Systems and Technology Management**, v. 6, p. 437-462, 2009.

OFFICE OF CIBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE. **Cybersecurity Capability Maturity Model (C2M2).** v. 2.1. Washington,

DC: Office of Cibersecurity, Energy Security, and Emergency Response, 2022. Disponível em: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2. Acesso em: 24 out. 2023.

PRAHALAD, CKy HAMEL; HAMEL, Gary. G. The Core Competence of the Corporation. **Harvard Business Review**, v. 68, n. 3, p. 295-336, 1990.

RAMÍREZ, Norman A. Ciberresiliencia. **Revista Sistemas**, n. 159, p. 96-110, 2021.

RISCO interno aumenta e custo dispara para US$ 16,2 milhões. **Ciso Advisor,** 21 set. 2023. Disponível em: https://www.cisoadvisor.com.br/risco-interno-aumenta-e-custo-sobe-para-us-162-milhoes/. Acesso em: 27 out. 2023.

VASQUEZ, Vinícius Lacerda. O processo de elaboração da lista de alvos cibernéticos no nível tático. **Data & Hertz**, v. 1, n. 1 jan./dez, p. 42-51, 2020.