CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
UNIDADE DE PÓS-GRADUAÇÃO, EXTENSÃO E PESQUISA
MESTRADO PROFISSIONAL EM GESTÃO E TECNOLOGIA EM
SISTEMAS PRODUTIVOS

MARCELO RAMOS

MODELO DE MATURIDADE DA CULTURA DE SEGURANÇA CIBERNÉTICA PARA UMA ORGANIZAÇÃO PÚBLICA

São Paulo
Março/2025

MARCELO RAMOS

MODELO DE MATURIDADE DA CULTURA DE SEGURANÇA CIBERNÉTICA PARA UMA ORGANIZAÇÃO PÚBLICA

Dissertação apresentada como exigência parcial para a obtenção do título de Mestre em Gestão e Tecnologia em Sistemas Produtivos do Centro Estadual de Educação Tecnológica Paula Souza, no Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos, sob a orientação do Prof. Dr. Carlos Hideo Arima.

Área de Concentração: Sistemas Produtivos
Linha de Pesquisa: Sistemas de Informação e Tecnologias Digitais
Projeto de Pesquisa: Gestão da Tecnologia da Informação

São Paulo
Março/2025

Ramos, Marcelo

R175m Modelo de maturidade da cultura de segurança cibernética para uma organização pública / Marcelo Ramos. – São Paulo: CPS, 2025.

103 f. : il.

Orientador: Prof. Dr. Carlos Hideo Arima

Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos) – Centro Estadual de Educação Tecnológica Paula Souza, 2025.

1. Maturidade. 2. Cultura. 3. Cibersegurança. 4. Sistemas produtivos. I. Arima, Carlos Hideo. II. Centro Estadual de Educação Tecnológica Paula Souza. III. Título.

MARCELO RAMOS

MODELO DE MATURIDADE DA CULTURA DE SEGURANÇA CIBERNÉTICA PARA UMA ORGANIZAÇÃO PÚBLICA

Prof. Dr. Carlos Hideo Arima
Orientador - CEETEPS

Documento assinado digitalmente
gov.br
JOSHUA ONOME IMONIANA
Data: 26/04/2025 12:15:43-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Joshua Onome Imoniana
Examinador Externo - UNIVERSIDADE DE SÃO PAULO - USP

Prof. Dr. Napoleão Verardi Galegale
Examinador Interno - CEETEPS

São Paulo, 27 de março de 2025

Dedico esta obra aos meus pais,
especialmente à memória do meu pai
Waldomiro que me ensinou os valores do
trabalho e da honestidade e de minha mãe
Maria José que sempre orou por mim.

AGRADECIMENTOS

Primeiramente a Deus que me permitiu chegar até aqui, ele me sustentou com o seu amor gracioso e em vários momentos tive a certeza de que não era eu que caminhava e sim ele me carregando em seus braços.

A minha esposa Elaine e meus filhos Jonathan e Ana Sofia, a despeito de minhas rabugices e reclamações, foram pacientes e compreensivos me apoiando integralmente. A eles todo o meu amor!

Ao querido amigo e mestre Abinel Santiago que me colocou nesta digna jornada acadêmica. Sua paciência e apoio ao longo de todo o processo foram fundamentais.

Ao meu orientador professor doutor Carlos Hideo Arima. Aprendi muito mais do que ciência com ele, seu exemplo e sua dedicação foram inspiradores.

Aos demais professores doutores do programa de mestrado em especial ao professor Napoleão por sua empatia, interesse e conhecimento, ao professor Marcelo Duduchi pelas lições de vida e exemplos inspiradores e a professora Márcia Ito pela excelência e dedicação com que conduz o seu trabalho.

Aos meus colegas da turma T11, Cintia, Alan, Claudio, Cristian, Isabel e a todos os demais que compartilharam conhecimentos, alegrias, angústias e risadas durante este ciclo acadêmico. Desejo a vocês um futuro cheio de conquistas e realizações.

Aos colegas da empresa onde atuo por contribuir e apoiar a realização desta pesquisa.

Aos amigos e irmãos da igreja por sua compreensão, intercessão e encorajamento.

A todos que contribuíram direta ou indiretamente para a realização deste trabalho.

Então, do meio de um redemoinho, o Senhor respondeu a Jó: *"Onde você estava quando eu lancei os alicerces do mundo? Diga-me, já que sabe tanto"*

Jó 38:1,4

RESUMO

RAMOS, M. **Modelo de maturidade da cultura de segurança cibernética para uma organização pública.** 103 f. Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2025.

O presente trabalho tem por objetivo avaliar o nível de maturidade da cultura de segurança cibernética no contexto organizacional. A metodologia de pesquisa adotada foi o *design science research*, com a coleta de dados realizada por meio de entrevistas semiestruturadas e *survey*. A pesquisa propôs a elaboração de um modelo de maturidade de cinco níveis e cinco dimensões que abordam aspectos sobre o conhecimento que os indivíduos têm sobre a segurança cibernética, quais as suas percepções sobre os protocolos e questões de segurança, como é o seu comportamento diante de ameaças e o uso que fazem dos recursos tecnológicos, quais as ações de conscientização são realizadas e como se dá o apoio e envolvimento da alta direção na promoção da cultura de segurança cibernética. Os resultados obtidos com a elaboração e aplicação do modelo de maturidade proposto apresentaram que a organização possui uma estrutura e processos estabelecidos para desenvolver a cultura de segurança, mas que existem lacunas no comportamento seguro dos funcionários, o envolvimento da alta direção na promoção da cultura de segurança precisa ser substancialmente aprimorado, são necessárias melhorias nas normas de segurança internas da organização e o programa de conscientização está estagnado. Acredita-se que o modelo de maturidade elaborado nesta pesquisa se constitui numa ferramenta para o aprimoramento da cultura de segurança cibernética nas organizações.

Palavras-chave: Maturidade. Cultura. Cibersegurança. Sistemas Produtivos.

ABSTRACT

RAMOS, M. ***Cybersecurity culture maturity model for a public organization.*** 103 f. Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2025.

This study aims to analyze the level of maturity of cybersecurity culture in the organizational context. The research methodology adopted was design science research, with data collected through semi-structured interviews and surveys. The research proposed the development of a five-level maturity model with five dimensions that address aspects such as individuals' knowledge of cybersecurity, their perceptions of security protocols and issues, their behavior in the face of threats, their use of technological resources, the awareness actions being carried out, and the support and involvement of senior management in promoting a cybersecurity culture. The results obtained from the development and application of the proposed maturity model revealed that the organization has an established structure and processes to develop a security culture, but there are gaps in employees' secure behavior, the involvement of senior management in promoting the security culture needs substantial improvement, internal security policies require enhancements, and the awareness program is stagnant. It is believed that the maturity model developed in this research serves as a tool for improving the cybersecurity culture in organizations.

Keywords: Maturity. Culture. Cybersecurity. Production Systems.

LISTA DE QUADROS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SIGLAS

AHP	Analytic Hierarchy Process
AHP-OS	AHP Online System
C2M2	Cybersecurity Capability Maturity Model
CMI	Culture Maturity Indicators
CMM	Cybersecurity Capacity Maturity Model for Nations
CMMI	Capability Maturity Model Integration
CSC	Cultura de Segurança Cibernética
DS	Design Science
DSRM	Design Science Research Methodology
E-Ciber	Estratégia Nacional de Segurança Cibernética
GSI	Gabinete de Segurança Institucional da Presidência da República
HGMM	Modelo de Maturidade de Conscientização em Segurança da Informação da Comunidade Húngara
KB4MM	KnowBe4 Research Security Culture Maturity Model
MGI	Ministério da Gestão e da Inovação em Serviços Públicos
MIT	Massachusetts Institute of Technology
MITMM	Massachusetts Institute of Technology Sloan Cybersecurity Culture Maturity Model
MM	Modelos de Maturidade
MMCSC	Modelo de Maturidade da Cultura de Segurança Cibernética
NIST	National Institute of Standards and Technology
PNSI	Política Nacional de Segurança da Informação
SANS	System Administration Networking and Security Institute
SANSMM	SANS Security Awareness Maturity Model
SGD	Secretaria de Governo Digital
TCU	Tribunal de Contas da União

SUMÁRIO

INTRODUÇÃO

A transformação digital revolucionou as organizações ao trazer benefícios como maior eficiência, redução de custos, aumento da competitividade e otimização de processos. No setor público, desde os anos 2000, várias iniciativas de governo digital vêm sendo promovidas para desburocratizar e modernizar o Estado brasileiro, aprimorando o atendimento à população e ampliando o acesso aos serviços públicos. No entanto, além dessas vantagens, surgiram novos desafios, especialmente no que tange à segurança da informação (Brasil, 2018; Johansson *et al.*, 2022).

As organizações estão cada vez mais expostas a vários tipos de ataques cibernéticos. Movidos pelo ganho financeiro, criminosos virtuais empregam métodos sofisticados para obter acesso não autorizado a dados sensíveis, praticar extorsão e causar prejuízos operacionais e econômicos às empresas (Alshaikh *et al.*, 2018).

Uma estratégia muito empregada pelos criminosos virtuais é direcionar seus ataques às pessoas dentro das organizações. De acordo com o relatório da Verizon (2024), 68% das violações de dados têm o fator humano como principal componente, evidenciando que o comportamento dos funcionários é uma das principais portas de entrada para os ataques.

Para mitigar esses riscos, muitas empresas têm implementado programas de conscientização que visam educar os funcionários sobre as melhores práticas de segurança e promover comportamentos mais cautelosos diante de ameaças cibernéticas (ENISA, 2017).

No entanto, apenas realizar treinamentos e campanhas educativas não garante que os funcionários desenvolverão uma postura proativa e consistente no longo prazo, pois, a conscientização é apenas uma das facetas na construção de uma cultura de segurança cibernética robusta (Alshaikh; Adamson, 2021).

Al-Darwish e Choe (2019) afirmam que há fatores humanos diretos e indiretos que influenciam a segurança cibernética. Os fatores diretos são aqueles que têm um impacto no sistema geral de segurança da informação, como erros intencionais, imperícia e desvios para facilitar a usabilidade em detrimento da segurança. Os fatores indiretos são aqueles oriundos da percepção de segurança dos funcionários e tem uma forte ligação com a cultura de segurança cibernética, por isso, compreender e abordar estes fatores humanos indiretos é necessário para gerir eficazmente a segurança da informação dentro de uma organização.

Da Veiga e Martins (2015) declaram que analisar a cultura de segurança cibernética significa identificar se o nível de cultura de segurança é apropriado para assegurar a confidencialidade, integridade e disponibilidade da informação na perspectiva do funcionário.

Nesse sentido, a adoção de modelos de maturidade pode se constituir numa ferramenta eficaz para identificar o estágio em que uma organização se encontra em relação a determinado processo, permitindo uma análise estruturada de suas práticas e políticas, além de fornecer uma orientação clara para a melhoria contínua, ajudando as organizações a identificarem lacunas e definir ações específicas para avançar em direção a uma maturidade mais elevada (Muronga *et al.*, 2019).

A aplicação de um modelo de maturidade para analisar a cultura de segurança cibernética pode fornecer indicadores valiosos para a governança e gestão estratégica, além de estabelecer um processo contínuo de análise e melhoria (Becker; Knackstedt; Pöppelbuß, 2009).

No entanto, há uma escassez de estudos que abordem de maneira eficaz a avaliação da maturidade dos programas de conscientização e da cultura de segurança em diferentes setores. Entende-se que o desenvolvimento e a aplicação de um modelo desta natureza pode preencher essa lacuna, oferecendo às organizações, ferramentas concretas para a análise e aprimoramento da segurança cibernética (Ramos; Arima, 2023).

Diante desta necessidade e do contexto apresentado, este estudo propõe a seguinte questão de pesquisa: Como avaliar a cultura de segurança cibernética em uma organização pública utilizando um modelo de maturidade?

Nesta perspectiva, o objetivo geral se constitui em avaliar a cultura de segurança cibernética numa organização pública com base em um modelo de maturidade. E os objetivos específicos abaixo enumerados são:

1. Revisar a literatura sobre modelos de maturidade da cultura de segurança cibernética;

2. Identificar as dimensões e os níveis que compõem um modelo de maturidade para cultura de segurança cibernética;

3. Definir os requisitos do modelo de maturidade da cultura de segurança cibernética;

4. Aplicar o modelo de maturidade para avaliar o nível da cultura de segurança cibernética na organização pública.

1 FUNDAMENTAÇÃO TEÓRICA

A segurança da informação consiste na proteção das informações e dos sistemas contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição indevidos, assegurando a disponibilidade, confidencialidade, integridade, autenticidade, o não-repúdio, a proteção da privacidade pessoal e das informações proprietárias (NIST, 2013; Solms; Niekerk, 2013).

No entanto, os recursos que lidam com a informação possuem vulnerabilidades inerentes e as ameaças virtuais estão cada vez mais sofisticadas, assim, a proteção das informações e dos sistemas é necessária para a organização se prevenir contra incidentes, reduzir o risco de ataques cibernéticos, minimizar os impactos financeiros, regulatórios, operacionais e assegurar a continuidade das operações do negócio, garantindo a conformidade legal e preservando a imagem da empresa (Von Solms, 1998; Solms; Niekerk, 2013).

Com o aumento dos ataques virtuais, a segurança cibernética começou a atrair mais atenção nos últimos anos e expandiu o escopo da segurança da informação, ao proteger não somente as informações, ou os sistemas de uma organização, mas a considerar a proteção de quaisquer ativos vulneráveis no ambiente cibernético, sejam indivíduos, organizações ou a sociedade em geral (Solms; Niekerk, 2013; Aksoy, 2024).

Para avaliar se um espaço cibernético é seguro e qual o nível desta segurança, Le e Hoang (2016) afirmam que não é suficiente apenas identificar as vulnerabilidades corrigidas, ou considerar as soluções de proteção como *firewalls* e sistemas de detecção de intrusos, pois estes, são apenas alguns aspectos da segurança cibernética. Para eles, é necessário analisar a segurança cibernética de forma abrangente, de cima para baixo, avaliando as fraquezas e definindo estratégias de melhoria.

Georgiadou *et al.* (2022) alegam que a maior ameaça de uma organização à privacidade e segurança, ainda que ela não possa reconhecer, são as pessoas que a compõem, Reegård *et al.* (2019) afirmam que é fundamental compreender o comportamento humano e porque os funcionários agem de determinada maneira em relação à segurança cibernética.

Por isso, a segurança cibernética de uma organização depende também da compreensão, do comportamento e da ação das pessoas para gerenciar o risco e implementar medidas de segurança (Kruger; Kearney, 2006).

Wilson *et al.* (1998) asseveram que um incidente de segurança pode ter consequências adversas para todos na empresa, por isso, promover a segurança é uma responsabilidade da coletividade e envolve uma mudança de cultura. Esta mudança, segundo Aksoy (2024), é a essência da transformação nas organizações.

Cada organização possui a sua cultura, que é complexa, dinâmica e compreende os pressupostos relacionados ao grupo, as percepções e adaptações em relação aos problemas e a transmissão de conhecimento entre os seus membros e exerce uma influência significativa na formação das atitudes e comportamentos dos funcionários em relação à segurança da informação (Schein, 1990; Al-Darwish; Choe, 2019).

Quando os atributos comportamentais são utilizados para interagir com os sistemas da organização, tem-se a manifestação da cultura de segurança cibernética (Da Veiga; Martins; Eloff, 2007).

Desta forma, para proteger a organização contra ameaças crescentes e sofisticadas, são necessárias medidas adicionais aos recursos técnicos, como *firewalls* e sistemas de detecção de intrusos. A atuação das pessoas é fundamental, seja no comportamento seguro, seja na implementação de medidas de proteção e no desenvolvimento da cultura de segurança cibernética.

1.1 Cultura de segurança cibernética (CSC)

A cultura de segurança cibernética surge como uma subcultura da cultura organizacional. Ela se refere ao conhecimento, crenças, percepções, atitudes, suposições, normas e valores das pessoas em relação à segurança cibernética e como eles se manifestam no uso das tecnologias da informação (Da Veiga *et al.*, 2020; ENISA, 2017).

A cultura de segurança cibernética decorre das iniciativas regulares de comunicação, sensibilização, formação e educação e está associada à conformidade dos indivíduos com as diretrizes da política de segurança (Da Veiga *et al.*, 2020).

Anilkumar *et al.* (2023) afirmam que a cultura de segurança cibernética abrange os hábitos compartilhados, a mentalidade e a atitude coletiva em relação à segurança e como ela é integrada aos processos diários da empresa.

A recomendação ITU-T X.1054 do *International Telecommunication Union*, uma agência para tecnologias digitais das Nações Unidas, afirma que a cultura da organização é a base para construir a governança da segurança da informação (ITU, 2021).

As características que ilustram a CSC e como ela está inserida na cultura organizacional estão representadas na Figura 1.

Figura 1 – Cultura de segurança cibernética (CSC)

Fonte: Elaborado com base em Da Veiga (2020); Anilkumar *et al.* (2023); ENISA (2017).

De acordo com a Figura 1, a CSC é uma subcultura da cultura organizacional e compreende, dentre outros aspectos, elementos característicos da segurança da informação como as percepções de segurança dos indivíduos, as ações de conscientização que aprimoram a própria CSC, a conformidade com as diretrizes da política de SI e o comportamento seguro dos funcionários.

1.1.1 Conscientização

A conscientização é um subconjunto da CSC, seu objetivo é promover mudanças comportamentais através de um processo contínuo de aprendizagem (ENISA, 2017).

Diesch *et al.* (2020) afirmam que os assuntos que não são abordados com tecnologia e relacionam-se com as preocupações de segurança, referem-se à conscientização.

O *National Institute of Standards and Technology* – NIST – (2013) afirma que as regras de comportamento seguro, que o uso adequado dos sistemas e das informações são mandatórios na organização e que o objetivo do treinamento em segurança é ensinar estas habilidades e criar as competências necessárias para o desempenho das atividades laborais, ao passo que as ações de conscientização se destinam a chamar a atenção das pessoas para os problemas relacionados com a segurança.

A conscientização é essencial para a organização, pois além promover um comportamento seguro, contribui para a correta aplicação dos procedimentos de segurança, evitando interpretações erradas ou omissões que comprometam sua eficácia (Siponen, 2000; Kruger; Kearney, 2006).

Shaw *et al.* (2009) afirmam que a conscientização enfatiza o discernimento dos indivíduos sobre a relevância da segurança da informação, suas responsabilidades e os requisitos necessários para proteger os ativos da organização.

Embora as pessoas sejam consideradas por alguns especialistas o elo mais fraco da cibersegurança, elas são, ao mesmo tempo, as responsáveis por usar e proteger os recursos de TI. Por isso, o programa corporativo de conscientização desempenha um papel fundamental ao proporcionar a formação do indivíduo, promover a mudança de atitude, estimular a mudança de comportamento e contribuir para a cultura organizacional (Wilson *et al.*, 1998; Wilson; Hash, 2003; Muronga *et al.*, 2019).

Portanto, a conscientização é a principal engrenagem no desenvolvimento da cultura de segurança cibernética em uma organização.

1.1.2 Comportamento

O comportamento em relação à segurança cibernética consiste em como são executadas as atividades diárias ou a maneira como as coisas são feitas pelos indivíduos e reflete o desenvolvimento da cultura ao longo do tempo (Da Veiga *et al.*, 2020).

No âmbito da segurança das organizações o comportamento demonstra as ações que os funcionários adotam ao enfrentar riscos de segurança da informação (Zhen *et al.*, 2022).

O comportamento pode ser uma ameaça e ter um impacto negativo na organização quando é descuidado, quando resulta da falta de compreensão das diretrizes de segurança, quando há falta de atenção, treinamento, comunicação, falta de sistemas apropriados, falta de suporte da gerência e falta de consequências e responsabilização. O objetivo é afirmar o comportamento de segurança que proteja os ativos de informação e esteja em conformidade com as políticas de segurança, que aja com cautela, meticulosidade, vigilância, consciência e atenção (Da Veiga *et al.*, 2020).

A mudança de comportamento é evolutiva e compreende três etapas: a) conformidade: quando os indivíduos adotam um comportamento porque esperam receber uma recompensa ou evitar uma punição, mas não acreditam no conteúdo ou no benefício de adotar este comportamento; b) identificação: os indivíduos aceitam um agente influenciador porque desejam manter um relacionamento com a pessoa ou grupo com o qual se identificam, neste caso, a equipe de segurança e c) internalização: os funcionários cumprem as políticas de segurança porque têm a mesma crença e sistema de valores da equipe de segurança (Ramos; Arima, 2023 *apud* Alshaikh e Adamson, 2021).

O comportamento seguro pode ser reforçado com abordagens que usam a punição ou recompensas e bônus (Ramos; Arima, 2023 *apud* Gundu, 2019).

A responsabilização, a prestação de contas e o monitoramento também contribuem para a mudança de comportamento, pois ao saber que sua identidade é revelada e suas atividades estão sendo monitoradas, o funcionário teria menor propensão a uma conduta insegura (Ramos; Arima, 2023 *apud* Yaokumah *et al.* 2019).

A correção de comportamentos indesejáveis, como não clicar em *links* suspeitos de *phishing*, não deve ser a única inciativa, deve-se investir em atitudes proativas na construção de hábitos de segurança positivos, como relatar suspeitas de incidentes, incentivar o uso de gerenciadores de senhas e muito mais (Carpenter, 2022).

O comportamento seguro dos indivíduos e como ele é desenvolvido, praticado e disseminado na organização é um indicador da maturidade da cultura de segurança cibernética.

1.1.3 Atitude

A atitude consiste na visão, sentimentos e crenças que as pessoas têm em relação aos protocolos e questões de segurança (Georgiadou *et al.*, 2022; Zhen *et al.*, 2022).

A organização pode ter tecnologia e processos adequados, no entanto, os funcionários podem contornar os controles de segurança, devido à sua percepção ou atitude em relação aos requisitos de segurança da informação (Da Veiga; Martins, 2015).

Por isso, Al-Darwish e Choe (2019) afirmam as organizações não devem se concentrar apenas em aspectos técnicos da segurança, pois os fatores oriundos da percepção de segurança dos funcionários tem uma forte ligação com a cultura de segurança cibernética e precisam ser desenvolvidos de forma abrangente.

Da Veiga e Martins (2015) declaram que avaliar a cultura de segurança cibernética significa identificar se o nível de cultura de segurança é apropriado para assegurar a confidencialidade, integridade e disponibilidade da informação na perspectiva do funcionário. Esta avaliação é feita através da obtenção das opiniões dos funcionários em relação à segurança da informação. Com isso, os gestores podem medir a percepção dos funcionários sobre a segurança da informação e identificar aspectos que requerem atenção, de modo a melhorar a CSC para um nível aceitável e, dessa forma, proteger a informação.

Kruger e Kearney (2006) sugerem que a consciência de segurança dos funcionários pode ser avaliada por métodos baseados na psicologia social que enfatizam as crenças ou os sentimentos.

Al-Darwish e Choe (2019) e Parsons *et al.* (2010) abordam o conceito do clima de segurança que pode ser observado segundo oito dimensões da percepção dos funcionários sobre o seu ambiente de trabalho: 1) a importância da segurança e do treinamento, 2) os efeitos da conduta segura na promoção, 3) os efeitos da segurança exigida no local de trabalho, 4) os efeitos da conduta segura nas questões sociais, 5) as atitudes da gestão em relação à segurança, 6) o nível de risco no local de trabalho, 7) o status do responsável pela segurança e o 8) status do comitê de segurança.

Kesseler et al. (2020) afirmam que o clima de segurança cibernética consiste nas percepções compartilhadas das políticas de segurança e suas manifestações na organização e pode ser categorizado como são percebidas: a obediência às políticas e procedimentos de

segurança, a importância sobre a segurança da informação e a tolerância da organização para comportamentos de segurança inadequados.

Em suma, a segurança cibernética de uma organização não depende apenas de tecnologias e processos definidos, mas também da atitude dos funcionários. A avaliação da cultura e do clima de segurança cibernética, com foco na percepção dos colaboradores, é necessária para identificar áreas de melhoria e garantir que as práticas de segurança sejam realmente eficazes. Incorporar uma abordagem que considere tanto os aspectos técnicos quanto os humanos da segurança fortalece a proteção da informação e contribui para uma cultura organizacional resiliente e consciente em relação à segurança.

1.1.4 Conhecimento

O conhecimento sobre tecnologia e segurança da informação é um influenciador positivo na cultura de segurança cibernética. Quanto mais conhecimento os funcionários tiverem sobre segurança e sobre as tecnologias envolvidas em sua atividade laboral, mais conscientes eles estarão sobre as ameaças virtuais e mais prevenidos eles estarão de maus comportamentos não intencionais (Khando *et al.*, 2021).

De acordo com Da Veiga *et al.* (2020), o conhecimento sobre segurança é obtido pelos funcionários ao longo do tempo, em decorrência dos programas de conscientização, treinamento e educação.

O treinamento é um processo ativo que capacita para a resolução de problemas operacionais, ao passo que a educação visa a formação de habilidades numa estrutura teórica, para lidar com situações futuras ou desconhecidas e ambos são componentes chave na formação do conhecimento em segurança (Corradini, 2020).

Para Anilkumar *et al.* (2023), o conhecimento é a base para distinguir as ameaças de segurança como *phishing*, *malware*, crimes cibernéticos e as medidas de proteção correspondentes.

Corradini (2020) afirma que o conhecimento não se resume apenas em ter informações, mas sim em ter sensibilidade para discernir questões relevantes de segurança e agir em conformidade com elas.

O entendimento das diretrizes, controles de segurança e informações da empresa é individual de cada funcionário e pode ser deficiente na medida em que é incapaz de identificar os riscos de segurança associados ao trabalho (Da Veiga *et al.*, 2020; Zhen *et al.*, 2022).

O conhecimento permite que os funcionários atuem de maneira segura, enquanto a desinformação pode trazer sérios riscos à organização. Por isso, o trabalho precisa ser feito por profissionais preparados e conscientes das ameaças (Kő; *et al.,* 2023; Corradini, 2020; Khando *et al.*, 2021).

Os conceitos de desaprender e reaprender são essenciais para acompanhar a evolução do cenário de segurança cibernética. Desaprender envolve abandonar práticas e hábitos desatualizados que podem representar riscos, enquanto reaprender exige a constante aquisição de novos conhecimentos para lidar com ameaças e tecnologias emergentes. A organizações devem não apenas ensinar o básico, mas também incentivar a revisão de práticas antigas e a adoção de abordagens mais eficazes. Casos reais de violações de segurança podem ser úteis para demonstrar a importância de desaprender e reaprender em um ambiente em constante mudança (Gundu, 2024).

1.1.5 Organizacional

A dimensão organizacional reflete a relação entre a alta direção e a cultura de segurança cibernética dentro de uma organização. Essa dimensão abrange o nível de envolvimento dos líderes organizacionais na promoção e patrocínio das ações de segurança, bem como o apoio e os recursos destinados a essas iniciativas (Ruighaver; Maynard; Chang, 2007).

O compromisso da alta direção se manifesta de diversas formas. Ao demonstrar que a segurança é uma prioridade estratégica, a alta gerência influencia a percepção dos colaboradores sobre a importância da temática. Isso se traduz em maior engajamento e adesão às políticas e procedimentos de segurança. Além disso, o investimento em recursos adequados, como ferramentas, treinamento e pessoal especializado, demonstra o compromisso da organização com a segurança cibernética (Khando *et al.*, 2021).

Para que a cultura de segurança seja efetiva, é crucial que a alta gerência não apenas se envolva ativamente, mas também lidere pelo exemplo pois os funcionários tendem a imitar o

comportamento de seus líderes. Estudos indicam que a participação direta dos gestores no programa de conscientização de segurança, seja liderando sessões de treinamento ou comunicando a relevância das políticas de segurança, tem um impacto significativo na postura dos funcionários em relação à segurança (Carpenter, 2022; Uchendu *et al.*, 2021).

Além disso, é fundamental que os objetivos de negócio da organização estejam alinhados com as diretrizes de segurança. Contradições entre metas gerenciais e práticas de segurança podem prejudicar a implementação de uma cultura de segurança eficiente. Por exemplo, indicadores de desempenho que recompensam comportamentos contrários às metas de segurança podem minar a percepção da segurança como um valor organizacional (Ruighaver; Maynard; Chang, 2007; Anilkumar; Filip Dimitrov; Anup Narayanan, 2023).

Portanto, a dimensão organizacional é um dos alicerces sobre o qual se constrói uma cultura de segurança cibernética positiva. O apoio, o envolvimento e a liderança da alta gerência são elementos indispensáveis para criar um ambiente onde a segurança seja uma prioridade para todos os membros da organização.

1.1.6 Cultura positiva de segurança cibernética

Uma CSC positiva compreende a proteção dos dados, dos sistemas e o gerenciamento dos riscos humanos na salvaguarda da informação (Uchendu *et al.*, 2021; Spitzner, 2019).

Anilkumar *et al.* (2023) afirmam que a organização se torna segura quando a segurança cibernética é tratada como um aspecto fundamental em todas as operações, e não somente uma preocupação do departamento de TI, mas uma responsabilidade compartilhada por todos na empresa. Para alcançá-la, são necessárias ações consistentes que apoiem e promovam a segurança como um dever coletivo, o envolvimento da liderança, políticas eficazes, participação ativa dos funcionários e incentivos para práticas seguras.

A CSC segundo Da Veiga e Martins (2015), pode ser negativa ou fraca quando os funcionários não interagem com as informações de maneira segura. Por exemplo, os funcionários podem não encontrar nada de errado em compartilhar senhas ou podem valorizar o atendimento às expectativas dos clientes acima do cumprimento das políticas.

O desenvolvimento de uma CSC positiva é fundamental, porque não apenas os processos e a tecnologia tornam a organização segura, mas principalmente as pessoas, pois são elas que identificam, comunicam os problemas, sugerem melhorias e aplicam as orientações de segurança em seu trabalho diário (NCSC, 2023).

O envolvimento da alta gestão é preponderante no desenvolvimento da CSC positiva ao dar apoio, promover a coordenação entre as partes interessadas e criar mecanismos para as iniciativas em capacitação, conscientização e integração junto às equipes da organização (ITU, 2021).

Para Ruighaver *et al.* (2007), o que determina uma CSC positiva é a disposição que a organização tem de desafiar a crença de segurança, confrontar a visão que a camada decisória da organização tem sobre a qualidade da segurança e a qualidade dos processos de gerenciamento de segurança, isso, segundo eles, é mais importante do que a crença que o usuário final tem sobre a segurança cibernética.

Outro fator crítico em direção a CSC positiva é a gestão de mudanças, muitas organizações não definem concretamente os passos sobre como fazer mudanças se a cultura de segurança não estiver no nível positivo necessário para proteger a informação e os sistemas (Uchendu *et al.*, 2021).

Uma das características da CSC positiva é quando os indivíduos avaliam constantemente o seu comportamento e refletem sobre a influência de suas ações na segurança e como ela pode ser melhorada (Ruighaver; Maynard; Chang, 2007).

Anilkumar *et al.* (2024b) afirmam que a cultura de segurança pode ser mensurada por indicadores como o conhecimento que os funcionários tem sobre ameaças virtuais (*phishing* e *malware*, por exemplo), o nível de aderência à política e procedimentos de segurança pelos funcionários, a eficácia do processo de gerenciamento de riscos de segurança, a prontidão na resposta a incidentes e o engajamento da alta gestão nas ações de segurança cibernética.

O estudo de Uchendu *et al.* (2021) destacou que o apoio da alta gestão da organização foi o fator mais influente na manutenção de uma cultura de segurança cibernética positiva.

A definição de métricas, o estabelecimento e o monitoramento de indicadores contribuem para o aprimoramento da CSC. Destacam-se as taxas de conclusão de treinamento em segurança, os resultados das simulações de *phishing,* a pontuação das avaliações de conhecimento sobre segurança, o percentual de funcionários envolvidos nas campanhas de conscientização, a eficácia do treinamento e a taxa de conformidade, violações e percepção

sobre a qualidade da política de segurança (Anilkumar; Filip Dimitrov; Anup Narayanan, 2024a).

Para uma organização avaliar a maturidade da cultura de segurança cibernética, Carpenter (2022) afirma que devem ser considerados o treinamento de conscientização, as simulações de *phishing*, o comportamento seguro, o envolvimento organizacional e a aplicação de questionários para obter dados sobre a maturidade de segurança dos funcionários.

Segundo Spitzner (2019) ter uma equipe dedicada em tempo integral para o programa de conscientização é fundamental para gerenciar o risco humano. Segundo ele, as organizações com mais de mil pessoas devem dispor de, pelo menos, três a cinco funcionários dedicados exclusivamente para o programa.

A comunicação e o treinamento contínuo dos funcionários contribuem para que o risco humano de incidentes de segurança seja gerenciado de forma eficaz (Spitzner, 2019).

O treinamento promove a conscientização sobre a importância da segurança cibernética, capacita os funcionários para exercerem suas funções de forma segura, várias organizações tornam o treinamento obrigatório e o incluem como uma etapa no processo de integração de novos empregados. Ele deve ser atualizado periodicamente, pelo menos uma vez por ano (Lie; Utomo; Winarno, 2021).

A pesquisa de Muronga *et al.* (2019) identificou cinco estudos que avaliavam a eficácia dos programas de conscientização e treinamento dos usuários em segurança cibernética. O escopo de análise considerou o comportamento dos indivíduos antes e depois da aplicação de treinamentos com técnicas de gamificação e simulações de *phishing,* a conformidade com a política de senhas e a aplicação de grupos de discussão com especialistas sobre o programa de conscientização.

O monitoramento também desempenha um papel essencial no fortalecimento da CSC, pois a conscientização é um processo cumulativo, dependente de uma compreensão do progresso de suas iniciativas para auxiliar os gestores no planejamento de ações futuras. Por isso, a avaliação contínua da organização ao longo do tempo, com dados empíricos retroalimentados, obtidos por meio de pesquisas periódicas como *surveys,* por exemplo, identifica os avanços e verifica se as ações do programa de conscientização tiveram um impacto positivo na cultura de segurança (Da Veiga; Martins, 2015; Alshammari; Demetis, 2023).

Portanto, a segurança cibernética da organização precisa ser observada sob uma perspectiva abrangente que permita identificar as fraquezas, definir estratégias de abordagem e

medidas de proteção. O processo de avaliação da CSC identifica se houve melhora na proteção dos ativos de informação, nessa perspectiva, os modelos de maturidade se constituem numa ferramenta valiosa, pois permitem aferir o nível da segurança atual e indicam ações para fortalecer e prevenir a exploração de vulnerabilidades (Le; Hoang, 2016; Da Veiga; Eloff, 2010). O Quadro 1 resume as principais características do que representa uma cultura de segurança cibernética positiva nas organizações.

Quadro 1 – Características da CSC positiva

Proteção e Gerenciamento de Riscos	Proteção dos dados e sistemas e gerenciamento de riscos humanos na segurança da informação
Segurança como Dever Coletivo	A segurança cibernética integrada em todas as operações e tratada como uma responsabilidade compartilhada por todos na organização.
Envolvimento da Liderança e Funcionários	Necessidade de políticas eficazes, participação ativa dos funcionários e suporte da liderança para promover a segurança.
Papel Central das Pessoas	As pessoas são essenciais para identificar problemas, sugerir melhorias e aplicar práticas de segurança diariamente.
Disposição para Questionar e Melhorar	Disposição para desafiar e melhorar continuamente a qualidade dos processos de segurança e a percepção da segurança.
Gestão de Mudanças Eficaz	Definição de etapas concretas para gerenciar mudanças culturais em direção a uma segurança mais robusta.
Autoavaliação e Aperfeiçoamento	Encorajamento à reflexão individual sobre como as ações pessoais afetam a segurança e como podem ser melhoradas.
Adoção de Estratégias Comportamentais	Implementação de métodos comportamentais para fortalecer práticas de segurança além da conscientização básica.
Medição da Eficácia da Segurança	Avaliação da cultura de segurança por meio de indicadores como adesão a políticas e conhecimento sobre ameaças.
Métricas de Desempenho em Segurança	Estabelecimento e monitoramento de métricas como taxas de treinamento, conformidade e resultados de simulações.
Avaliação Baseada em Dados	Uso de métricas e dados concretos, em vez de relatos informais, para avaliar a eficácia dos processos de segurança
Perspectiva Abrangente de Segurança	Observação da segurança cibernética de forma holística, identificando fraquezas e estratégias de proteção, com apoio de modelos de maturidade.

Fonte: Elaborado com base em Uchendu *et al*.(2021); Spitzner (2019); Da Veiga e Martins (2015); Ruighaver *et al.* (2007); Le e Hoang (2016).

As características positivas contribuem para o estabelecimento de metas, melhoria contínua dos processos de segurança e servem de parâmetro para o amadurecimento da organização na cultura de segurança cibernética.

1.1.7 Setor público

O setor público foi influenciado pela revolução digital ocorrida na sociedade principalmente nos últimos 20 anos. A oferta de uma gama de serviços públicos digitais como o portal Gov.br, do Governo Federal, a Declaração de Imposto de Renda, a solicitação de Seguro Desemprego e a emissão da nova carteira de identidade, são alguns exemplos de serviços essenciais que dependem dos recursos tecnológicos (BRASIL, 2020; TCU, 2024).

Nesse sentido, o ecossistema tecnológico que suporta estes serviços deve assegurar que os princípios fundamentais de segurança da informação como a disponibilidade, a autenticidade, a integridade dos dados, e a proteção das informações coletadas sejam garantidos, conforme disposto na Política Nacional de Segurança da Informação – PNSI – Decreto nº 9.637, de 26 de dezembro de 2018 (BRASIL, 2021).

O aumento da presença digital pelo governo e o maior acesso às tecnologias pela população também colocou o Brasil em destaque na lista de países que mais sofrem ataques cibernéticos, acrescente-se a isso a baixa maturidade e a inexistência de uma cultura de segurança, fatores estes, que deixam evidente o despreparo da sociedade brasileira (BRASIL, 2020).

O Tribunal de Contas da União fez uma avaliação de vinte e nove áreas críticas da administração pública, dentre elas, a segurança cibernética indicou riscos à soberania digital do país com potencial de comprometer a capacidade econômica, tecnológica e dos dados pessoais e críticos. O órgão de controle afirmou que não há organização oficial no Brasil capaz de zelar pelo nível de maturidade da segurança cibernética e orientar a atividade no país (TCU, 2024).

Para tentar suprir a falta de convergência entre as estratégias de segurança, o desalinhamento das normas e os diversos níveis de maturidade em segurança cibernética na sociedade, foi elaborada, sob coordenação do Gabinete de Segurança Institucional da Presidência da República – GSI –, a Estratégia Nacional de Segurança Cibernética –E-Ciber–. O documento prevê que os entes de governo devem estimular capacitação contínua de seus colaboradores em segurança cibernética e promover campanhas de conscientização para desenvolver o comportamento seguro. Em seus objetivos, destacam-se a necessidade de aumentar a resiliência contra ameaças e elevar o nível de maturidade em segurança cibernética (BRASIL, 2020).

A pedido do governo brasileiro, em 2023, o escritório de assuntos exteriores do Reino Unido, a Organização dos Estados Americanos e o Centro Global de Capacidade de Segurança Cibernética elaboraram o relatório de Revisão do *Cybersecurity Capacity Maturity Model for Nations* – CMM – Brasil, cujo objetivo era indicar investimentos estratégicos para o aprimoramento da segurança cibernética nacional. O relatório apontou que existem iniciativas de conscientização nas entidades governamentais, porém, foi detectado que as práticas de segurança não foram implementadas adequadamente e que há uma discrepância entre as ações de conscientização e a percepção dos riscos de segurança cibernética (BRASIL, 2023).

Gerorg *et al.* (2023) mapearam os principais desafios de segurança cibernética na administração pública federal sob a ótica dos gestores de tecnologia da informação. A pesquisa identificou um baixo investimento em capacitação de segurança cibernética, pouco engajamento em relação à segurança cibernética por parte dos servidores e que em linhas gerais há uma escassez de recursos voltados para a área de segurança cibernética. A percepção é que a segurança não é tratada como prioridade, o que afeta os investimentos estratégicos e o engajamento do corpo funcional.

Almeida *et al.* (2024) conduziram um estudo sobre a percepção dos trabalhadores de uma organização pública federal sobre a conscientização em segurança cibernética. Os resultados apontaram que 67,89% dos participantes disseram que raramente ou ocasionalmente a organização reforça as práticas de segurança online, 82,41% dos respondentes afirmaram que não são comunicados sobre *phishing*, 73,15% não recebem alertas sobre *ransomware* e que 61,11% dos usuários não são comunicados sobre os riscos de programas maliciosos. Em relação aos treinamentos de segurança, 80,73% disseram que raramente a organização efetua treinamentos e 61,47% afirmaram desconhecer o documento da política de segurança cibernética da organização.

Azambuja e Neto (2020) propuseram um modelo de maturidade para auxiliar as organizações públicas federais a avaliaram a situação da segurança cibernética em seus ambientes. O modelo é composto por quatro níveis e nove domínios. O objetivo de desenvolver a força de trabalho em segurança cibernética e o objetivo de aumentar a conscientização estão no domínio de capacitação, conscientização e cultura. O modelo foi aplicado em trinta e cinco órgãos da administração pública federal e indicou que 56,25% das entidades públicas não desenvolvem a força de trabalho em segurança cibernética e que 43% das organizações estão no nível mais baixo de maturidade em relação à capacitação, conscientização e cultura.

A Secretaria de Governo Digital – SGD – do Ministério da Gestão e da Inovação em Serviços Públicos – MGI – elaborou o Framework de Privacidade e Segurança da Informação. O documento auxilia na implementação de controles de privacidade e cibersegurança e é composto por trinta e dois controles organizados em três categorias: uma para estrutura básica de gestão em privacidade e segurança da informação, dezoito voltados para cibersegurança e treze controles para privacidade. Cada controle possui medidas a serem avaliadas e implementadas pela instituição pública. Os controles de conscientização e cultura de segurança abordam o programa de conscientização, ataques de engenharia social, cuidados no tratamento de dados e identificação de incidentes e ameaças (BRASIL, 2024).

O setor público é cada vez mais dependente dos recursos tecnológicos para implementar as políticas públicas em prol da sociedade, no entanto, os desafios para a segurança da informação são cada vez maiores no espaço cibernético. Embora tenham ocorrido iniciativas importantes como o estabelecimento da PNSI, da Estratégia Nacional de Segurança Cibernética e do Framework de Privacidade e Segurança da Informação, ainda assim, as pesquisas mostram que o Estado brasileiro tem um longo caminho a percorrer com necessidade de mais investimentos, alinhamento estratégico em segurança e engajamento dos servidores públicos para elevar a maturidade da cultura de segurança cibernética de forma a proteger os dados e tornar o setor público resiliente às ameaças cibernéticas.

1.2 Modelos de maturidade (MM)

Ruighaver *et al.* (2007) constataram que embora várias organizações acreditem na eficácia de seus processos de segurança cibernética, a maioria delas não realiza qualquer tentativa de avaliá-los ou tampouco medir a sua eficácia, baseiam-se apenas em relatos informais ou em experiências pontuais, ao invés de dados concretos ou métricas quantificáveis.

Diante da necessidade contínua de aperfeiçoamento, as empresas devem avaliar sua posição atual com precisão e analisar detalhadamente seus processos. É fundamental determinar o que medir e como realizar essas medições, identificar critérios de comparação, avaliar a qualidade atual, definir medidas de melhoria e estabelecer métodos eficazes para monitorar o progresso da implementação. O MM é a ferramenta que permite alcançar estes objetivos, pois possui uma sequência de níveis que traça o caminho evolutivo em um domínio específico. Ele funciona como uma escala de avaliação, onde o estágio inicial indica poucas capacidades e o

estágio mais alto representa a maturidade total. Para avançar de nível, é necessária uma progressão contínua das capacidades ou do desempenho. O modelo também define critérios e características que devem ser atendidos para alcançar cada nível (Becker; Knackstedt; Pöppelbuß, 2009).

Os MM oferecem diretrizes formais para as organizações identificarem e melhorarem seus processos e atividades. No contexto da segurança cibernética, esses modelos ajudam a estruturar os processos que protegem os recursos do espaço cibernético (Muronga *et al.*, 2019; Le; Hoang, 2016).

Becker *et al.* (2009) afirmam que os MM podem ser entendidos como artefatos que determinam o status da organização e auxiliam na resolução de problemas.

A aplicação de MM amplia o entendimento sobre o estado e complexidade dos processos e serve de guia para a avaliação de capacidades. A maioria dos modelos é multidimensional, com uma estrutura de níveis sequenciais e critérios de medição, fornecendo um caminho para o aprimoramento da organização (Wendler, 2012).

A elaboração ou melhoria de MM deve ser interativa e requer a comparação com modelos existentes e a observância de certos princípios como utilidade, qualidade, eficácia e rigor metodológico. O Quadro 2, apresenta uma sequência de atividades a serem aplicadas na elaboração de modelos de maturidade (Becker; Knackstedt; Pöppelbuß, 2009).

Quadro 2 – Etapas na elaboração de modelos de maturidade

#	Etapas
1	**Definição do problema** (propósito, domínio alvo, grupo alvo e relevância do problema)
2	**Comparação com modelos existentes** (verificar deficiências e necessidades)
3	**Definição da estratégia de *design*** (modelo totalmente novo, aprimoramento de algum modelo existente, combinação de modelos em um novo, transferência de estruturas ou conteúdos)
4	**Desenvolvimento interativo** (objetivos, estrutura, arquitetura, dimensões, atributos, documentação de abordagem, seções, abrangência, consistência e adequação do problema)
5	**Concepção de transferência de estrutura** (*checklist*, manuais, *software*, formulários)
6	**Implementação e transferia de mídia** (relatórios, questionário de autoavaliação)
7	**Avaliação** (estudo de caso e disponibilização em *site*)

Fonte: Adaptado de Becker *et al.* (2009).

As etapas na elaboração de MM conforme Becker *et al.* (2009), descritas no Quadro 2, iniciam-se com a definição do problema e especificam o propósito, a relevância, o domínio e grupo alvo. Em seguida, realiza-se a comparação com outros MM existentes e a verificação de deficiências e necessidades. Na sequência ocorre a definição de estratégia *design* que define se haverá um modelo novo, aprimoramento a partir de um modelo existente, a transferência de estruturas e conteúdo ou a combinação destas abordagens. Segue-se para o desenvolvimento propriamente dito que envolve a definição da arquitetura e caracterização das dimensões dos demais atributos. A quinta etapa é concepção dos artefatos de transferência seguido pela implementação e avaliação do modelo proposto.

1.2.1 Modelos de maturidade da cultura de segurança cibernética

Os modelos de maturidade proporcionam uma abordagem estruturada para a melhoria contínua da CSC de uma organização. Eles permitem a identificação e o aprimoramento sistemático de práticas e processos, garantindo o alinhamento com os objetivos estratégicos e requisitos de conformidade, além de fortalecer as defesas. À medida que a organização avança nos níveis de maturidade, desenvolve-se uma cultura de segurança abrangente e proativa, essencial para enfrentar as ameaças cibernéticas (Wood, 2024).

Dentre os principais modelos de maturidade de TI, o *Capability Maturity Model Integration* – CMMI – em seu domínio *Security* descreve práticas para integração da segurança aos produtos, serviços e processos da organização (ISACA, 2023).

Lee e Hoang (2016) defendem que os modelos de maturidade devem ser adaptáveis e mensuráveis por meio de métricas para permitir a avaliação por parte da gestão e dos especialistas em segurança em diferentes contextos na organização.

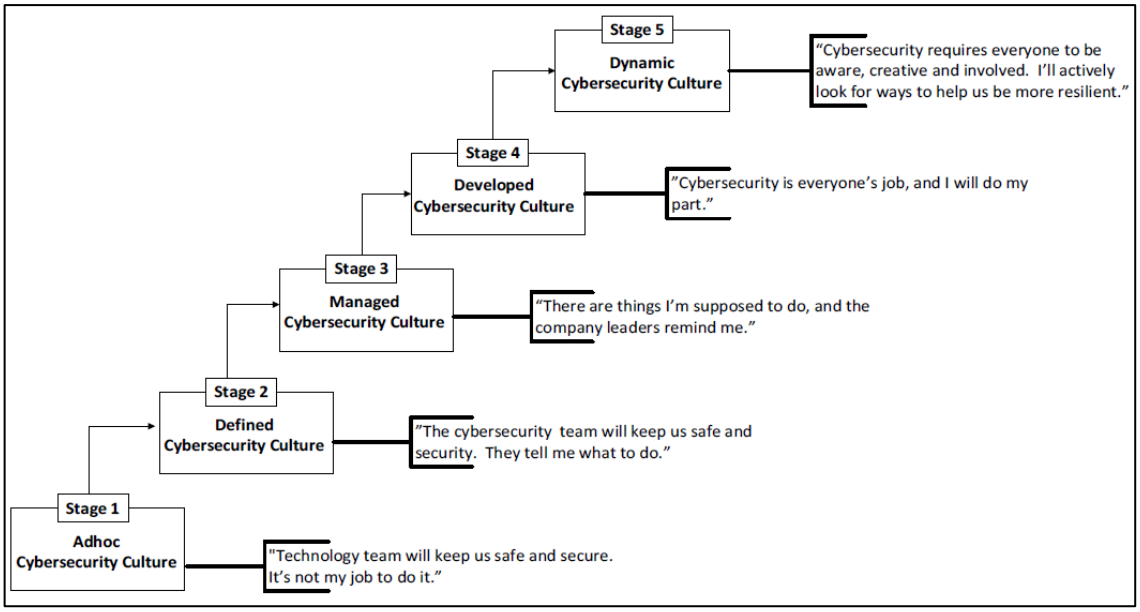
O modelo de maturidade *Cybersecurity Capability Maturity Model* – C2M2 – do *U.S. Department of Energy* dos Estados Unidos, no domínio *Workforce Management* define os objetivos para atribuir as responsabilidades, desenvolver a força de trabalho, implementar controles e aumentar a conscientização em segurança cibernética (U.S. DOE, 2022).

A literatura e a indústria dispõem de vários modelos de maturidade para a segurança da informação e modelos de maturidade para TI. O escopo desta pesquisa se concentrou nos modelos específicos para a conscientização e cultura de segurança cibernética. Os modelos de maturidade que apresentaram maior aderência a este trabalho estão descritos na próxima seção.

1.2.1.1 *Cybersecurity Culture Maturity Model - MIT Sloan (MITMM)*

O MITMM é um modelo criado pelos pesquisadores de cibersegurança da escola de negócios do *Massachusetts Institute of Technology – MIT–* é um modelo de cinco níveis e cinco dimensões que se propõe a avaliar a CSC baseado na crença de que à medida que as ameaças cibernéticas mudam, a cultura de segurança da organização também deve mudar, evoluir e amadurecer. Para sua construção, foram considerados outros modelos existentes, estudos realizados por empresas do setor de segurança e a visão que os líderes de várias organizações têm sobre o que é uma CSC eficaz. A Figura 2, descreve os estágios evolutivos de maturidade do MITMM.

Figura 2 – Estágios evolutivos de maturidade do MITMM



Fonte: Prakash e Pearlson (2024).

Conforme ilustrado na Figura 2, no primeiro estágio, a CSC é incipiente e não está estabelecida na organização. Nesta fase, os indivíduos afirmam que a responsabilidade por manter a empresa segura é da equipe de tecnologia. As iniciativas em segurança restringem-se aos investimentos em tecnologia e as ações de conscientização são focadas em dar treinamento e orientações sobre comportamento seguro. No próximo estágio, chamado de definido, há uma equipe de segurança cibernética estabelecida, existem algumas iniciativas para desenvolver a CSC e os funcionários limitam-se a seguir as orientações de segurança.

No terceiro estágio, a CSC é gerenciada por um responsável em toda a organização e os funcionários assumem certas responsabilidades para com a segurança cibernética, porém

necessitam ser lembrados pela liderança da organização acerca de suas responsabilidades. No quarto estágio, a CSC encontra-se desenvolvida, ela é uma prioridade para a gestão da empresa, existem programas para aprimorá-la e os funcionários entendem que a responsabilidade pela segurança compete a todos na organização. O último estágio representa uma CSC dinâmica, capaz de se adaptar a novas ameaças, os funcionários desempenham um papel ativo na segurança buscando maneiras de deixar a organização mais resiliente. O Quadro 3, fornece mais detalhes acerca dos estágios do modelo e quais as percepções e comportamentos dos funcionários em cada fase de maturidade (Prakash; Pearlson, 2024).

Quadro 3 – Atitudes dos funcionários no MITMM

Níveis de Maturidade	**Descrição**	**Valores, atitudes e crenças**
Cultura ***Ad-hoc*** de Segurança Cibernética	A segurança cibernética foca apenas em sistemas de TI e gerenciamento, investimentos em soluções tecnológicas para a proteção. Existem atividades como programas de orientação, treinamento e conscientização para dizer aos funcionários o que fazer e o que não fazer.	Os funcionários acreditam que "a equipe de tecnologia nos manterá seguros" e têm pouca ou nenhuma responsabilidade pessoal sobre segurança.
Cultura de Segurança Cibernética **Definida**	Pode-se identificar alguns comportamentos seguros dos funcionários. Existem alguns mecanismos em vigor para criar valores, atitudes e crenças que impulsionam a CSC.	Um líder/equipe de cultura cibernética impulsiona a cultura, usando mecanismos para criar valores, atitudes e crenças para impulsionar comportamentos cibernéticos.
Cultura de Segurança Cibernética **Gerenciada**	A empresa possui um líder de CSC com a responsabilidade de criar, gerenciar e desenvolver a cultura de segurança cibernética.	Os funcionários compartilham valores, atitudes e crenças sobre a importância da segurança cibernética e fazem o que são instruídos a fazer para manter a organização segura.
Cultura de Segurança Cibernética **Desenvolvida**	A segurança cibernética é uma das principais prioridades da gestão, a atitude predominante é que "a segurança cibernética é parte do trabalho de todos". Existem programas e mecanismos projetados para propagar essa atitude.	Os funcionários são capacitados para fazer o que é necessário para se protegerem e todos pensam que a segurança cibernética é seu trabalho.
Cultura **Dinâmica** de Segurança Cibernética	Os processos que impulsionam a CSC incorporam o ambiente e o cenário de ameaças em constante mudança, e se adaptam naturalmente para construir novos mecanismos de proteção.	Os funcionários estão regularmente envolvidos e criando ações que mantêm a organização mais resiliente.

Fonte: Adaptado de Prakash e Pearlson (2024).

A avaliação da maturidade da organização é realizada sob a ótica de cinco dimensões: treinamento e conscientização, envolvimento da liderança, desempenho e avaliação, expectativas dos funcionários e resposta a novas ameaças. O Quadro 4, descreve os parâmetros de cada dimensão por nível de maturidade.

Quadro 4 – Modelo de maturidade MITMM

Níveis de maturidade	Conscientização e treinamento	Envolvimento da liderança	Avaliação e performance do comportamento	Expectativas dos empregados	Resposta a novas ameaças
Ad-hoc	Pouco ou nenhum	Os líderes de conduzem programas, processos e atividades de segurança.	Nenhuma conexão entre comportamento e desempenho de segurança.	Nenhuma expectativa dos funcionários foi definida.	Tecnologia responsável por lidar com novas ameaças.
Definido	Treinamento anual e campanhas regulares.	Os líderes de tecnologia impulsionam atividades e tentam envolver parceiros.	Recompensas ou incentivos para bons comportamentos de segurança.	Espera-se que os funcionários sigam as políticas e procedi-mentos definidos.	A equipe de segurança responde conforme necessário.
Gerenciado	Programas regulares de treinamento e conscientização oferecidos aos funcionários.	A liderança assume a segurança e impulsiona cultura em suas equipes.	Há consequências para comportamentos inseguros repetidos.	Espera-se que os funcionários sigam as orientações dos supervisores.	Liderança sob orientação da equipe de segurança responde a novas ameaças.
Desenvolvido	Treinamento contínuo sob demanda disponível a qualquer momento. Conscientização constante e envolvente.	Executivos têm compromisso com a segurança, comunica, priorizam e investem.	Comportamento de segurança faz parte da sua avaliação anual de desempenho.	Espera-se que o funcionário tome medidas sem ser avisado ou lembrado.	Liderança identifica novas ameaças e informa a equipe segurança.
Dinâmico	À medida que surgem novas ameaças, os funcionários criam os seus próprios programas de formação e sensibilização.	Todos os líderes estão regularmente envolvidos, sem qualquer estímulo adicional dos seus superiores.	Automotivado. Não são necessárias recompensas adicionais para encorajar o comportamento seguro.	Os funcionários são motivados para ajudar a organização a encontrar maneiras de ser mais segura.	Todos na organização capacitados para responder a novas ameaças de maneira adequada à função.

Fonte: Adaptado de Prakash e Pearlson (2024).

1.2.1.2 *Maturity Model for Information Security Awareness (HGMM)*

O modelo de maturidade de conscientização em segurança da informação HGMM foi elaborado com base no modelo de maturidade do *System Administration Networking and Security Institute* – SANS – e na experiência de especialistas da comunidade húngara de segurança da Informação. O modelo tem como premissa os mecanismos de gerenciamento de risco, a estrutura organizacional e a conscientização em segurança da informação e está distribuído em cinco níveis de maturidade, que variam de "inexistente" a "estrutura de métricas robusta" conforme apresentado no Quadro 5.

Quadro 5 – Estrutura do modelo de maturidade HGMM

Nível de maturidade	**Descrição**	**Conhecimento**	**Atitude**	**Evidência de auditoria**
1 - Inexistente	A conscientização praticamente não existe	Nenhum controle de suporte	Nenhum controle de suporte	Nenhum
2 - Foco na conformidade	O programa de conscientização existe para atender a requisitos específicos de conformidade ou auditoria	Eventos e materiais anuais de treinamento disponíveis. Auditorias internas anuais. Funcionários recebem treinamento inicial com conteúdo genérico de segurança da informação.	Processo disciplinar documentado	Materiais e registros de treinamento; Acordos de confidencialidade assinados; certificados de conformidade emitidos e relatórios de avaliação de risco
3 - Promover a conscientização e a mudança de comportamento	A conscientização é baseada em uma avaliação de risco detalhada, que identifica os tópicos que têm o maior impacto no suporte à missão da organização	Materiais específicos de treinamento com base na avaliação de risco.	Existe um sistema de incentivos definido e documentado.	*Checklist* de avaliação de risco detalhada; comunicações regulares da gestão sobre riscos emergentes, ações, contramedidas e resultados via *e-mail* etc.
4 - Sustentação a longo prazo e mudança cultural	Programa de conscientização com suporte da liderança para um ciclo de vida de longo prazo, revisão e atualização anual.	Procedimentos para a revisão regular dos conteúdos e comunicados, definição dos objetivos de aprendizagem para os grupos-alvo. Avaliações regulares de conhecimento por meio de testes	A avaliação pessoal inclui os objetivos de segurança nas avaliações de desempenho	Documentação relacionada ao programa, orçamento detalhado para um período mais longo (ou seja, três anos)
5 - Estrutura de métricas robusta	O programa de conscientização rastreia o progresso e mede o impacto. Melhora continuamente e demonstra o retorno sobre o investimento.	Procedimentos documentados e implementados para medir a conscientização.	Objetivos são personalizados, específicos, mensuráveis, atingíveis, realistas e oportunos.	Cálculos documentados e rastreáveis de indicadores-chave e de retorno sobre o investimento em segurança.

Fonte: Adaptado Kő *et al.* (2023).

Conforme apresentado no Quadro 5, o HGMM define cinco níveis de maturidade que avaliam o conhecimento e a atitude dos funcionários em relação à segurança da informação. O modelo também fornece indicativos de evidências que podem ser usadas no processo de auditoria.

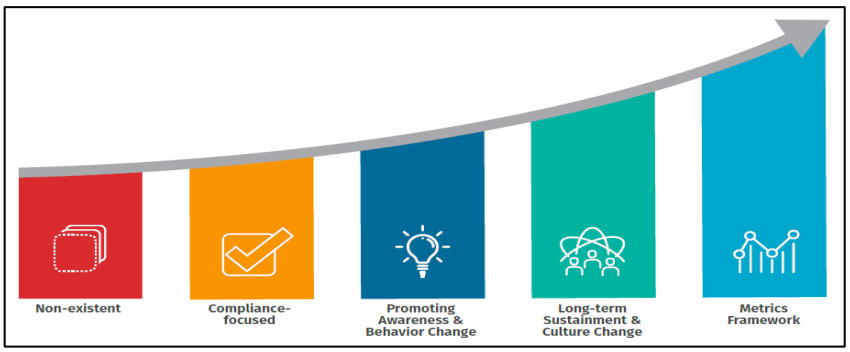
No primeiro nível, chamado de inexistente, não há controles que suportem o desenvolvimento do conhecimento e das atitudes em segurança. No segundo nível, o foco é em conformidade e verifica-se a existência de um programa de conscientização inicial com atividades de treinamento e documentação disciplinar estabelecidos. No terceiro nível, a ênfase é no desenvolvimento da conscientização e na mudança de comportamento, existem mecanismos de avaliação e um sistema de incentivos. No quarto nível, presume-se um desenvolvimento sustentável de longo prazo da conscientização, com avaliação regular dos indivíduos ligada ao desempenho funcional. No último nível é possível identificar um sistema de métricas, melhoria contínua, documentação, medição e indicadores estabelecidos de forma robusta (Kő; Tarján; Mitev, 2023).

1.2.1.3 *Security Awareness Maturity Model - SANS (SANSMM)*

O SANSMM é um modelo de maturidade voltado para programas de conscientização em segurança da informação. Ele foi concebido em 2011, pelo SANS Institute, uma instituição norte-americana que atua em treinamento e certificação em segurança da informação.

O modelo possui cinco níveis de maturidade com a descrição, a percepção de valor, os indicadores, as métricas e as etapas para alcançar o próximo nível que, em alguns casos, podem ser detalhadas em treinamentos específicos comercializadas aos clientes pelo SANS Institute. A Figura 3, descreve os níveis do SANSMM.

Figura 3 – Níveis do SANSMM



Fonte: Spitzner (2019)

Os níveis do modelo SANSMM, conforme ilustrado na Figura 3, indicam que no primeiro nível não há um programa de conscientização estabelecido e os funcionários desconhecem seu papel na segurança da organização.

O nível seguinte é focado em conformidade e o programa existe apenas para atender a requisitos de auditoria, com treinamento anual ou eventual, e os funcionários têm pouca clareza sobre as políticas de segurança. No terceiro nível, o programa identifica grupos-alvo e fornece treinamento contínuo e envolvente, resultando em uma melhor compreensão e adesão às políticas de segurança pelos funcionários.

O quarto nível descreve um programa bem estabelecido, integrado na cultura organizacional, com processos de revisão e atualização regulares e reflexos na mudança de comportamento, atitudes e percepções sobre segurança. O último nível do programa possui uma estrutura de métricas robusta, permite rastrear o progresso, medir o impacto, promove a melhoria contínua e demonstra o retorno sobre o investimento (Spitzner, 2019).

1.2.1.4 *Security Culture Maturity Model (KB4MM)*

O KB4MM é um modelo comercial e foi desenvolvido pela empresa KnowBe4 *Research*. Ele possui cinco níveis de maturidade baseado em um amplo conjunto de dados das plataformas de conscientização e treinamento utilizadas pelos clientes. O Quadro 6, descreve os níveis do modelo.

Quadro 6 – Níveis do modelo de maturidade KB4MM

Nível	Descrição	Características
1	Conformidade básica	• Treinamento mínimo • Métricas limitadas
2	Fundacional da conscientização sobre segurança	• Pelo menos treinamento anual e de integração • Simulações ocasionais de *phishing* • Foco na variedade de conteúdo
3	Conscientização e comportamento de segurança programática	• Programa de conscientização com ferramentas integradas • Treinamento trimestral com simulação de *phishing* • Foco em comportamentos conscientes de segurança

Nível	Descrição	Características
4	Gerenciamento de comportamento de segurança	• Treinamento contínuo em diversos métodos de entrega e públicos • Programa focado em mudança real de comportamento
5	Cultura de Segurança Sustentável	• Programa que mede, molda e reforça intencionalmente a cultura de segurança • Vários métodos de incentivo baseados em comportamento • Valores de segurança entrelaçados em toda a estrutura da organização

Fonte: Adaptado de KnowBe4 (2022).

Conforme apresentado no Quadro 6, o primeiro nível do KB4MM retrata um cenário de conformidade básica com as diretrizes de segurança, no nível seguinte, os fundamentos da conscientização podem ser observados com treinamento anual e simulações esporádicas de *phishing*. No terceiro nível, ocorrem treinamentos e o comportamento consciente é destacado. No quarto nível, o treinamento é contínuo e diverso e a mudança de comportamento é o grande enfoque do programa de conscientização.

No quinto e último nível, pode perceber uma CSC sustentável com diversas métricas definidas, treinamento focado em comportamento e os valores de segurança presentes em toda estrutura organizacional. O KB4MM é alimentado por diversos pontos de coleta de dados individuais chamados de *Culture Maturity Indicators* – CMI – os dados compreendem informações sobre treinamento, respostas das simulações de *phishing*, dados demográficos, organizacionais entre outros. O Quadro 7, apresenta alguns destes indicadores.

Quadro 7 – Indicadores de maturidade CMI

Categoria	Indicadores de maturidade
Treinamento de conscientização de segurança	• Frequência das campanhas de treinamento • Tipos de treinamento (presencial, online, por dispositivo móvel etc.) • Tipos de conteúdo usados • Módulos de aprendizagem realizados • Áreas medidas de força ou fraqueza • Customização/personalização para a organização e seus riscos • Personalização para o indivíduo com base na função/departamento

Categoria	Indicadores de maturidade
Phishing e testes simulados	• Email: aberto, clicado, anexo aberto, respondido, reportado como *phishing* • Explorado: o usuário clicou em um teste habilitado para exploração • Macro habilitada: a macro em um anexo foi habilitada • Padrões organizacionais de uso para simulações de *phishing* (por exemplo, personalização de modelos, gamificação etc.)
Conscientização sobre dados comportamentais	• Rastreamento e relatórios de alertas de comportamento de usuários • Políticas documentadas para falhas de comportamento do usuário • Gamificação
Atividades e envolvimento organizacional	• Comunicações em toda a empresa sobre políticas de segurança • Discussão liderada pelos executivos sobre políticas de segurança • Presença/ausência do Programa *Security Champions* • Recompensas em relação ao comportamento de segurança • Eventos especiais centrados na segurança
Questionário de pesquisa	• Dados de questionário (atitudes, comportamento, conhecimento, comunicação, conformidade, normas, responsabilidade) • Dados de avaliação de proficiência (senha e autenticação, segurança de e-mail, uso da Internet, mídia social, dispositivos móveis, consciência de segurança)

Fonte: Adaptado de KnowBe4 (2022).

Os modelos de maturidade apresentam um panorama geral da cultura de segurança em diversas organizações. Eles permitem a identificação de níveis onde há pouco desenvolvimento das práticas de conscientização, a mentalidade dos funcionários em termos cibersegurança é reativa, pouco engajada e seu comportamento mostra que a segurança não faz parte do seu trabalho diário.

Da mesma forma, os modelos de maturidade também fornecem um indicativo e um roteiro que as organizações podem evoluir até atingir um nível avançado de maturidade. Neste cenário almejado, a cultura de segurança está estabelecida em todas as áreas da empresa, é evolutiva, monitorada e sustentável.

O Quadro 8, apresenta um resumo das principais características dos modelos de maturidade da cultura de segurança cibernética.

Quadro 8 – Características principais dos modelos de maturidade da CSC

Código	Título	Características	Referência
MITMM	Cybersecurity Culture Maturity Model	Enfoque na necessidade de adaptabilidade em função de novas ameaças. Aborda várias dimensões como as atitudes, crenças e valores dos funcionários.	(Prakash; Pearlson, 2024)
HGMM	Information security awareness maturity: conceptual and practical aspects in Hungarian organizations.	Modelo que aborda a influência da gestão de risco, da estrutura organizacional e da conscientização na maturidade de segurança. Apresenta uma lista de controles e evidências de auditoria para os níveis de maturidade.	(Kő; Tarján; Mitev, 2023)
SANSMM	SANS - Security Awareness Maturity Model	Modelo comercial e conceitual com cinco níveis (inexistente, foco em conformidade, desenvolvendo a conscientização e mudança de comportamento, sustentação a longo prazo e mudança cultural, framework de métricas)	(Spitzner, 2019)
KB4MM	Security Culture Maturity Model	Modelo comercial baseado em um conjunto de dados dos clientes sobre conscientização, comportamento e cultura de segurança. É composto por indicadores de treinamento dos clientes, respostas das simulações de phishing, dados demográficos, organizacionais entre outros.	(KnowBe4, 2022)

Fonte: Resultado da pesquisa (2024).

2 METODOLOGIA

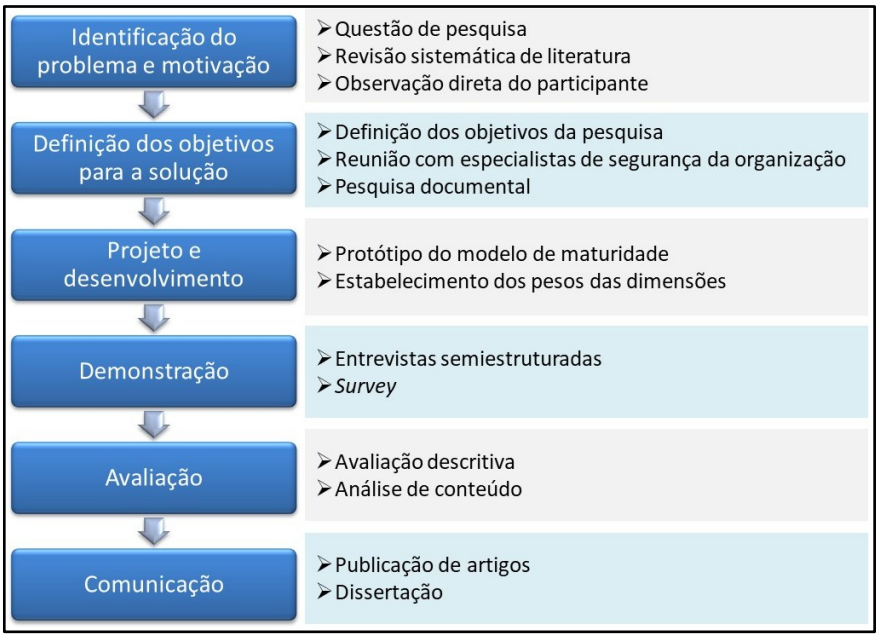
A metodologia empregada nesta pesquisa é baseada no *Design Science* – DS – e instrumentalizada pelo *Design Science Research Methodology* – DSRM – (Peffers *et al.*, 2007).

O DSRM se fundamenta na teoria do conhecimento do DS que consiste numa abordagem de pesquisa concentrada na criação de artefatos novos, como *softwares*, modelos e métodos para resolver problemas específicos e melhorar processos. Em atividades de *design*, modelos representam situações como problema e solução, cuja preocupação é a captura da realidade e sua utilidade (Hevner *et al.*, 2004).

Ao invés de apenas estudar e explicar fenômenos, o DS busca construir soluções concretas e oferecer um arcabouço metodológico que se alinha com o processo de criação de modelos de maturidade, visto que ambos, visam resolver problemas práticos e gerar contribuições científicas. O DS tem como foco a criação de artefatos inovadores, o que, no contexto de modelos de maturidade, significa desenvolver um *framework* estruturado que permita avaliar e aprimorar a maturidade de um determinado domínio (Lacerda *et al.*, 2013).

O método DSRM, conforme a Figura 4, está definido em seis etapas: identificação e motivação do problema, definição dos objetivos para uma solução, projeto e desenvolvimento, demonstração, avaliação e comunicação.

Figura 4 – Etapas do método Design Science Research



Fonte: Adaptado de Peffers *et al.* (2007).

2.1 Identificação do problema e motivação

A etapa de identificação do problema e motivação da pesquisa iniciou com a técnica de observação direta do participante pois, segundo Villaverde *et al.* (2021), esta técnica permite a inserção ativa do pesquisador no ambiente estudado, propiciando uma compreensão profunda dos comportamentos, interações dos sujeitos em seu contexto natural, acesso direto a dados detalhados, informações cotidianas do grupo e a percepção de aspectos que poderiam passar despercebidos por outras técnicas.

A partir da observação direta do participante e da necessidade de estabelecer as bases teóricas iniciais deste estudo, uma revisão sistemática de literatura foi conduzida sob o tema da conscientização em segurança da informação (Ramos; Arima, 2023).

Posteriormente, definiu-se a questão de pesquisa e buscou-se aprofundar a fundamentação teórica com uma nova revisão sistemática da literatura, cujo foco foi a identificação de estudos que descrevessem métodos, ferramentas ou modelos de avaliação da cultura de segurança cibernética. A estratégia, os resultados das buscas e o protocolo de pesquisa adotados são apresentados no Quadro 9.

Quadro 9 – Estratégia de pesquisa da revisão sistemática de literatura

Bases de dados	*Scopus, Web of Science, IEEE Xplore e ACM*
Data de realização das buscas	setembro de 2023
Período de publicação	2019 a 2023
Palavras-chave	*information security awareness; cybersecurity culture; evaluation; assess; appraise; weigh; check; determine; estimate; judge; classify; measure;*
***String* de busca**	*((evaluat OR assess OR appraise OR weigh OR check OR determine OR estimate OR judge OR classify OR measure) AND ("information security awareness" OR "information security culture" OR "cybersecurity culture" OR "cyber awareness" OR "cyber security culture" OR "cyber-security culture" OR "security behavior")) NOT (covid OR student OR education)*
Tipos de publicações incluídas	artigos e publicações de conferência

Fonte: Resultado da pesquisa (2023).

Após a realização das buscas foram encontrados 298 registros conforme ilustrado na Tabela 1.

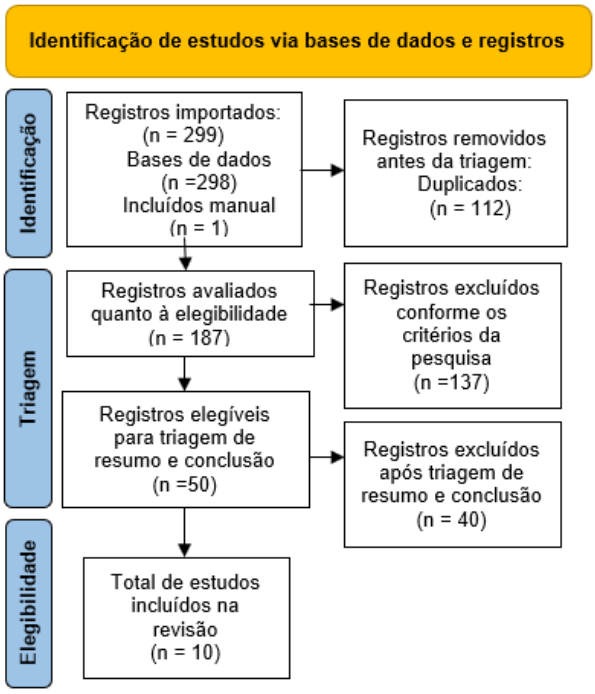
Tabela 1 – Resultados das buscas de publicações

Base de dados	Resultados obtidos
Scopus	148
Web of Science	78
IEEE Xplore	27
ACM	45
Total	**298**

Fonte: Resultado da pesquisa (2023).

O tratamento dos dados seguiu as diretrizes da declaração PRISMA 2020 (Page *et al.*, 2021) cuja as etapas estão identificadas na Figura 5.

Figura 5 – Etapas do protocolo de pesquisa



Fonte: Adaptado de PRISMA 2020 (2021).

Algumas publicações foram incluídas na fundamentação teórica desta pesquisa pela técnica de análise de citação, que consiste no exame das referências de artigos acadêmicos para identificar quais obras são frequentemente citadas e que podem ter uma influência significativa no objeto de estudo (Garfield, 1955).

Outras obras também foram agregadas ao conjunto da fundamentação teórica pela técnica de seleção por pertinência, que envolve a inclusão de estudos com base em sua relevância, *insights* valiosos, contribuição para a compreensão do tema e profundidade do conteúdo (Patton, 2014).

2.2 Definição dos objetivos para a solução

Os objetivos para a solução foram definidos considerando a questão de pesquisa estabelecida na etapa de identificação do problema, com as informações obtidas junto aos especialistas em segurança da informação e pela análise de documentos relativos à cultura de segurança cibernética disponíveis na *intranet* da organização.

2.3 Projeto e desenvolvimento

Na fase de projeto e desenvolvimento, o protótipo do modelo de maturidade foi elaborado com base no arcabouço teórico conforme explanado no capítulo 3. Os pesos das dimensões do modelo de maturidade foram obtidos com base em elementos do método *Analytic Hierarchy Process* – AHP –, aplicado de forma parcial. Para isso, foram selecionados decisores dentre os especialistas em segurança cibernética e conscientização da organização.

O AHP proposto por Saaty (1990), utiliza comparações pareadas para calcular prioridades e consistência. Ele permite tanto medições objetivas quanto opiniões subjetivas, ajudando a estruturar problemas complexos e facilitando a seleção de critérios relevantes. O método implica no estabelecimento de uma hierarquia, com objetivo, critérios e alternativas, que são avaliadas por uma série de comparações par a par baseadas numa escala de prioridade de importância. Cada comparação entre os critérios gera uma matriz de decisão, cujos valores são normalizados para obter os pesos relativos de cada critério.

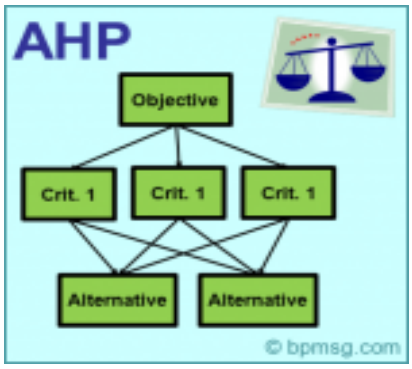
Este método, é uma ferramenta valiosa, pois o processo de tomada de decisão é fundamental em todas as atividades organizacionais e os métodos de análise multicritérios são usados para resolver problemas e escolher a melhor opção considerando as alternativas e preferências do decisor (Silva *et al.*, 2024) *apud* (Chakraborty *et al.*, 2023).

Vários estudos, como a revisão sistemática de Silva *et al.* (2024) indicam que o método AHP é dos mais utilizados no processo de tomada de decisão.

Embora o método AHP permita a comparação em diversos níveis, neste estudo, ele foi utilizado de forma adaptada, apenas para determinar a influência de cada dimensão na cultura de segurança e ao primeiro nível de comparação para definir os pesos das dimensões do modelo de maturidade. Isto permitiu alinhar o método às necessidades da pesquisa, sem a necessidade de explorar todos os níveis hierárquicos e comparações previstos no AHP completo.

Para apoio na utilização do método, adotou-se a aplicação *web* AHP *Online System* – AHP-OS – (Goepel, 2018), disponível em: https://bpmsg.com/ahp/. A Figura 6, ilustra uma representação simplificada do método AHP.

Figura 6 – Método AHP



Fonte: Goepel (2018).

Conforme apresentado na Figura 6, o objetivo está no topo da hierarquia, seguido por vários critérios, Crit.1, Crit.2 e assim sucessivamente. Estes, por sua vez, são usados para avaliar as alternativas disponíveis, que refletem as opções ou escolhas que estão sendo consideradas para atingir o objetivo. As avaliações são feitas em pares, com base numa escala, para determinar a importância relativa de cada critério e a preferência entre as alternativas, a partir dessas comparações são calculados os pesos usados para priorizar as opções e para a tomada de decisão.

2.4 Demonstração

A fase de demonstração, conforme Peffers *et al.* (2007), refere-se a aplicação do artefato por meio de um experimento, simulação, estudo de caso, prova ou atividade pertinente.

O artefato foi aplicado em uma entidade da administração pública federal que atua na esfera social do estado brasileiro. Por questões de confidencialidade, o nome e as demais características que identificam a entidade não serão divulgadas.

Uma entrevista semiestruturada foi aplicada com perguntas relacionadas às dimensões do modelo de maturidade para especialistas em segurança cibernética e conscientização indicados pelos gestores de segurança da organização. As perguntas da entrevista estão relacionadas no Apêndice C.

Uma pesquisa *survey* também foi aplicada aos funcionários da organização para obter a percepção dos participantes sobre a cultura de segurança. A técnica de pesquisa *survey* é indicada pois permite coletar a opinião dos respondentes sobre determinado assunto e obter uma maior compreensão do que é comumente entendido (Pinsonneault; Kraemer, 1993).

A pesquisa elaborada em conjunto com Miranda *et al.* (2024) sobre a conformidade de empresas à Lei Geral de Proteção de Dados Pessoais na perspectiva dos profissionais de TI, serviu de insumo para a elaboração da *survey* neste trabalho.

O questionário tem 33 questões divididas em 2 blocos. O primeiro bloco com 8 questões sobre dados demográficos do respondente e o segundo bloco com 25 questões elaboradas a partir do referencial teórico e a partir das dimensões do modelo de maturidade proposto. As questões da *survey* estão relacionadas no Apêndice B.

Adotou-se uma escala Likert invertida de 5 pontos, sendo: 4 - Totalmente de acordo, 3 - parcialmente de acordo, 2 - neutro, 1 - parcialmente em desacordo e 0 - totalmente em desacordo (Nemoto; Beglar, 2014).

O Apêndice D apresenta as etapas para a aplicação do artefato.

2.5 Avaliação

A etapa de avaliação, segundo Lacerda *et al* (2013), consiste na verificação do comportamento de um artefato para confirmar as soluções propostas. Os principais resultados da avaliação são as descrições e métricas alcançadas. Nesta fase, os dados obtidos através da *survey* e das entrevistas com especialistas são analisados para validar o modelo de maturidade e obter *insights* sobre o nível da cultura de segurança cibernética da organização.

Foi adotada a estratégia de análise descritiva dos dados da *survey,* pois permite descrever os dados de forma manejável, expondo as variáveis e as associações entre elas com o uso de procedimentos estatísticos como médias e proporções (Babbie, 1999; Fowler, 2014).

2.6 Comunicação

A comunicação dos resultados da pesquisa é realizada com a elaboração da dissertação e com a publicação de artigos científicos em revistas, periódicos ou congressos.

3 RESULTADOS

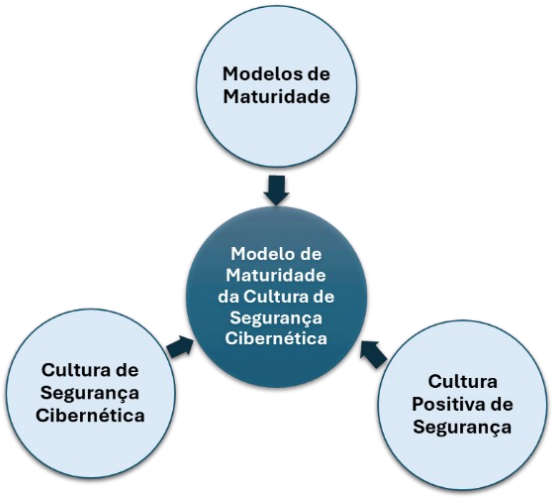
Os resultados da pesquisa foram divididos em cinco partes: 1. elaboração do modelo de maturidade da cultura de segurança cibernética, 2. definição dos pesos das dimensões do modelo de maturidade, 3. resultados das entrevistas com especialistas em segurança e conscientização, 4. resultados da pesquisa *survey* e 5. cálculo do nível de maturidade da organização.

3.1 Elaboração do modelo de maturidade da cultura de segurança cibernética (MMCSC)

Com base no arcabouço teórico exposto previamente nesta pesquisa, este capítulo apresenta uma proposta de modelo de maturidade para avaliar a cultura de segurança cibernética nas organizações.

O MMCSC proposto estabelece cinco níveis de maturidade e cinco dimensões que estão detalhadas nas próximas seções. O modelo foi elaborado a partir de outros modelos de maturidade de referência e incorpora as principais características, boas práticas e recomendações da cultura de segurança cibernética. A Figura 7, ilustra os insumos considerados na elaboração do modelo de maturidade proposto.

Figura 7 – Insumos para o MMCSC



Fonte: Resultado da pesquisa (2024).

Conforme ilustrado na Figura 7, a CSC positiva é um insumo para o MMCSC pois retrata o cenário ideal em termos da cultura de segurança, assim como os princípios, valores, conceitos e melhores práticas da cultura de segurança cibernética são base para o estabelecimento do modelo proposto, e, por fim, os modelos de maturidade de referência indicam os níveis, as métricas e as trilhas de melhoria que foram adaptadas para o novo modelo.

3.1.1 Níveis do MMCSC

A classificação dos níveis e os índices de maturidade do MMCSC foram definidos com base no modelo de gestão de riscos do Tribunal de Contas da União – TCU –.

O modelo apoia os auditores públicos na avaliação da maturidade da gestão de riscos e possui cinco níveis e quatro dimensões. São avaliados aspectos de liderança, políticas e estratégias, pessoas, processos, parcerias e resultados da organização de acordo com a eficiência e eficácia, transparência, *accountability* e conformidade com leis e regulamentos (TCU, 2018).

Os níveis do MMCSC com base no modelo do TCU são apresentados no Quadro 10.

Quadro 10 – Níveis do MMCSC

#	**Níveis de maturidade**	**Índice de maturidade**	**Descrição**
1	Inicial	0% <= 20%	Pouca maturidade, atividades de segurança informais ou inexistentes.
2	Básico	> 20% <= 40%	Processos iniciais em desenvolvimento com esforço mínimo.
3	Intermediário	> 40% <= 60%	Estrutura mais definida, com maior consistência nas práticas.
4	Aprimorado	> 60% <= 80%	Implementação avançada com envolvimento contínuo e melhorias constantes.
5	Avançado	> 80% <= 100%	Cultura madura com processos sustentáveis, integrados e monitorados.

Fonte: Resultado da pesquisa (2024).

Conforme informado no Quadro 10, os níveis do MMCSC descrevem os estágios da cultura de segurança cibernética. O estágio inicial denota um nível de cultura de segurança incipiente e com baixíssima maturidade. Os demais estágios do modelo expressam os avanços graduais na CSC até o patamar avançado que denota uma cultura madura e amplamente desenvolvida na organização.

3.1.2 Dimensões do MMCSC

O MMCSC está estruturado em cinco dimensões: conhecimento, atitude, comportamento, conscientização e organizacional. Cada dimensão aborda um pilar para o fortalecimento da segurança na organização, desde o entendimento sobre ameaças e medidas de proteção, até a postura das pessoas, as ações tomadas diante de ameaças e o apoio estratégico da alta direção. As dimensões oferecem uma visão integrada e detalhada para uma avaliação do nível de maturidade e os caminhos para aprimoramento contínuo da cultura de segurança.

3.1.2.1 Dimensão do conhecimento do MMCSC

A dimensão do conhecimento refere-se ao que as pessoas da organização sabem sobre segurança cibernética. As descrições dos níveis estão indicadas no Quadro 11.

Quadro 11 – Dimensão do conhecimento do MMCSC

Nível	Descrição da dimensão conhecimento
Inicial	Conhecimento superficial ou incipiente sobre ameaças, ataques cibernéticos, medidas de proteção, diretrizes, normas e processos de segurança cibernética da organização.
Básico	Conhecimento básico ou parcial sobre ameaças e ataques cibernéticos; noções elementares sobre medidas de proteção e familiaridade com algumas diretrizes, normas e processos de segurança cibernética da organização
Intermediário	Conhecimento moderado sobre ameaças e ataques cibernéticos; entendimento das principais medidas de proteção e ciente das diretrizes, normas e processos de segurança cibernética da organização.
Aprimorado	Conhecimento abrangente sobre ameaças, ataques cibernéticos, medidas de proteção e entendimento detalhado sobre as diretrizes, normas e processos de segurança cibernética da organização.
Avançado	Conhecimento avançado sobre ameaças recentes, vulnerabilidades emergentes e tendências de ataques globais. As diretrizes, normas e processos de segurança são de pleno conhecimento e recebem contribuições de melhoria.

Fonte: Resultado da pesquisa (2024).

3.1.2.2 Dimensão da atitude do MMCSC

A dimensão da atitude representa o que as pessoas pensam e sentem sobre os protocolos e questões de segurança. Os detalhes desta dimensão estão descritos no Quadro 12.

Quadro 12 – Dimensão da atitude do MMCSC

Nível	Descrição da dimensão atitude
Inicial	As pessoas demonstram pouca ou nenhuma preocupação com questões de segurança. A maioria dos indivíduos não vê a segurança como relevante para suas funções e acreditam que a responsabilidade pela segurança é da equipe de TI ou equipe de segurança.
Básico	Os indivíduos começam a reconhecer a importância da segurança, mas a veem como secundária ou relacionada apenas a certos departamentos. Admitem que a segurança é necessária, mas acreditam que os controles existentes são limitados e insuficientes para proteger a organização.
Intermediário	A maioria dos indivíduos vê a importância da segurança para suas atividades e passam a integrá-la no seu trabalho diário, contudo, alegam que os controles de segurança poderiam ser mais robustos e adaptados às suas funções. A segurança ainda não é considerada uma prioridade absoluta em todas as situações.
Aprimorado	As pessoas estão amplamente conscientes sobre a importância da segurança para suas funções e acreditam que a organização tem controles de segurança eficazes. A segurança é vista como uma prioridade em várias áreas, mas entendem que há oportunidades de melhorias em certos processos.
Avançado	A segurança é vista como essencial em todas as atividades diárias e cada indivíduo entende que é responsável por mantê-la e aprimorá-la. As pessoas creem que a organização possui infraestrutura e controles de segurança robustos e adequados para lidar com ameaças cibernéticas e que ela é uma prioridade em todas as decisões estratégicas.

Fonte: Resultado da pesquisa (2024).

3.1.2.3 Dimensão do comportamento do MMCSC

A dimensão do comportamento retrata como as pessoas agem diante das ameaças de segurança e o uso que fazem dos recursos de tecnologia da informação em relação à segurança cibernética. As características da dimensão do comportamento são apresentadas no Quadro 13.

Quadro 13 – Dimensão do comportamento do MMCSC

Nível	Descrição da dimensão comportamento
Inicial	As pessoas frequentemente adotam comportamentos inseguros, poucos seguem as boas práticas de segurança e não há iniciativas proativas para proteger a organização contra ameaças cibernéticas.
Básico	As pessoas começam a seguir algumas práticas básicas de segurança, como o uso de senhas fortes ou o bloqueio de dispositivos quando não estão em uso. No entanto, essas ações ainda não são consistentes. O comportamento seguro é geralmente reativo, e a maioria só adere às diretrizes quando solicitada ou em resposta a incidentes.
Intermediário	As pessoas demonstram um comportamento mais consciente, regular e seguem as diretrizes de segurança. O comportamento seguro é baseado no risco iminente e o reporte de incidentes é esporádico e limitado.
Aprimorado	O comportamento seguro é parte do cotidiano das pessoas, procuram antecipar e mitigar os riscos proativamente. O reporte de incidentes e possíveis vulnerabilidades é mais frequente. Sugestões de melhorias para os processos de segurança começam a ser compartilhadas.
Avançado	As pessoas são engajadas nas questões de segurança. Agem com cautela e atenção diante de ameaças, antecipam os riscos, incorporam as diretrizes e melhores práticas de segurança em suas rotinas e colaboram com a equipe de segurança. Propõem melhorias para os processos de segurança e trabalham em conjunto com a organização para fortalecer a cultura de segurança.

Fonte: Resultado da pesquisa (2024).

3.1.2.4 Dimensão da conscientização do MMCSC

A dimensão da conscientização abrange as ações que organização executa para desenvolver a cultura de segurança. Envolve o programa de conscientização, os treinamentos, as campanhas, as simulações entre outros. O detalhamento da dimensão da conscientização está descrito no Quadro 14.

Quadro 14 – Dimensão da conscientização do MMCSC

Nível	Descrição da dimensão conscientização
Inicial	Não há um programa de conscientização formalizado. Os comunicados de segurança são esporádicos. Os treinamentos e campanhas de conscientização são inexistentes ou limitados.
Básico	Treinamentos básicos voltados para a conformidade regulamentar ou para a política de SI. Campanhas de conscientização esporádicas. Comunicados de segurança enviados após incidentes, mas sem frequência regular.
Intermediário	Programa de conscientização estruturado com treinamentos regulares e obrigatórios para todos na organização. Comunicados abordam diretrizes de segurança, ameaças e melhores práticas. As campanhas de conscientização são esporádicas com temas gerais de segurança.
Aprimorado	Programa de conscientização estruturado. Treinamento obrigatório, com avaliação para todos na organização, disponível a qualquer momento. As campanhas de conscientização são envolventes e criativas, porém esporádicas. Comunicados de segurança são enviados de forma periódica, cobrem temas atuais e importantes para a organização. Testes eventuais sobre conteúdo de segurança. Equipe com dedicação parcial de tempo para o programa de conscientização. Simulações de phishing são eventuais.

Nível	Descrição da dimensão conscientização
Avançado	Programa de conscientização estabelecido e atualizado anualmente. Treinamento contínuo, personalizado para funções e áreas conforme necessidades específicas, conteúdo atualizado anualmente no mínimo, obrigatório e com avaliação para todos na organização. Campanhas frequentes, criativas e envolventes. Comunicados de segurança periódicos abordando temas recorrentes importantes, novas ameaças, diretrizes de segurança e medidas de proteção. Simulações de phishing e testes sobre temas de segurança. Equipe dedicada exclusivamente para o programa de conscientização. Programa de recompensas para reforçar o comportamento seguro. Agentes promotores da segurança na organização (*security champions*)

Fonte: Resultado da pesquisa (2024).

3.1.2.5 Dimensão organizacional do MMCSC

A dimensão organizacional expressa o apoio, liderança e envolvimento da alta direção na cultura de segurança cibernética. Os atributos da dimensão organizacional estão indicados no Quadro 15.

Quadro 15 – Dimensão organizacional do MMCSC

Nível	Descrição da dimensão organizacional
Inicial	A alta direção tem pouco ou nenhum envolvimento nas questões de segurança cibernética. A segura é vista como responsabilidade de uma área específica. Não há discussões regulares sobre o tema entre os líderes organizacionais. O apoio financeiro para a segurança cibernética é mínimo e restrito a iniciativas corretivas após incidentes.

Nível	Descrição da dimensão organizacional
Básico	Suporte mínimo da alta direção; discussões sobre segurança são raras. Apoio da alta direção em eventos pontuais. Segurança como parte da estratégia da organização. A alta direção começa a demonstrar um interesse crescente pela cultura de segurança, mas com envolvimento ainda limitado. Existem discussões ocasionais sobre a necessidade de políticas de segurança motivadas por exigências regulatórias ou auditorias. O apoio financeiro é esporádico e voltado para a compra de ferramentas de segurança. A segurança começa a ser reconhecida como um tópico importante, mas ainda não é vista como parte essencial da estratégia organizacional.
Intermediário	A alta direção tem envolvimento mais ativo nas discussões de segurança. As políticas são discutidas em nível estratégico, comunicados internos sobre importância da segurança começam a ser divulgados. Há alocação de recursos financeiros para o programa de conscientização. A segurança começa a ser mencionada nas estratégias organizacionais, mas ainda não é plenamente integrada.
Aprimorado	A alta direção lidera a cultura de segurança cibernética, participando em discussões estratégicas e comunicando aos funcionários a importância da segurança. Há um aumento no investimento financeiro e orçamento dedicado à cultura de segurança. A segurança é vista como uma prioridade organizacional. A alta direção participa de eventos públicos promovendo a segurança cibernética organizacional.
Avançado	A alta direção avalia e orienta os processos de gerenciamento da segurança considerando o cenário de ameaças e metas estratégicas da organização. Os líderes executivos participam de fóruns internos e externos sobre segurança. Os comunicados da alta direção reforçam a importância e estimulam a inovação em segurança com o uso de novas tecnologias e abordagens. O investimento financeiro é estratégico, contínuo e de longo prazo. A segurança é essencial nas decisões estratégicas de todas as áreas, operações, produtos e serviços da organização.

Fonte: Resultado da pesquisa (2024).

As dimensões de maturidade representam aspectos fundamentais da cultura de segurança, sua avaliação pode indicar o estágio de maturidade identificando as áreas que necessitam de melhorias. O MMCSC consolidado está descrito no Apêndice A.

3.2 Definição dos pesos das dimensões do MMCSC

A avaliação da cultura de segurança cibernética da organização é influenciada pelas dimensões que compõem o modelo de maturidade. Para identificar quais dimensões exercem maior influência no aprimoramento da cultura de segurança e calcular o nível de maturidade foram estabelecidos pesos com base em elementos do método AHP, conforme descrito no item 2.3, projeto e desenvolvimento.

Foram selecionados dez especialistas em segurança cibernética e conscientização que acessaram de forma individual, durante a etapa das entrevistas, a ferramenta AHP *Online System* – AHP-OS – (Goepel, 2018), disponível em: https://bpmsg.com/ahp/.

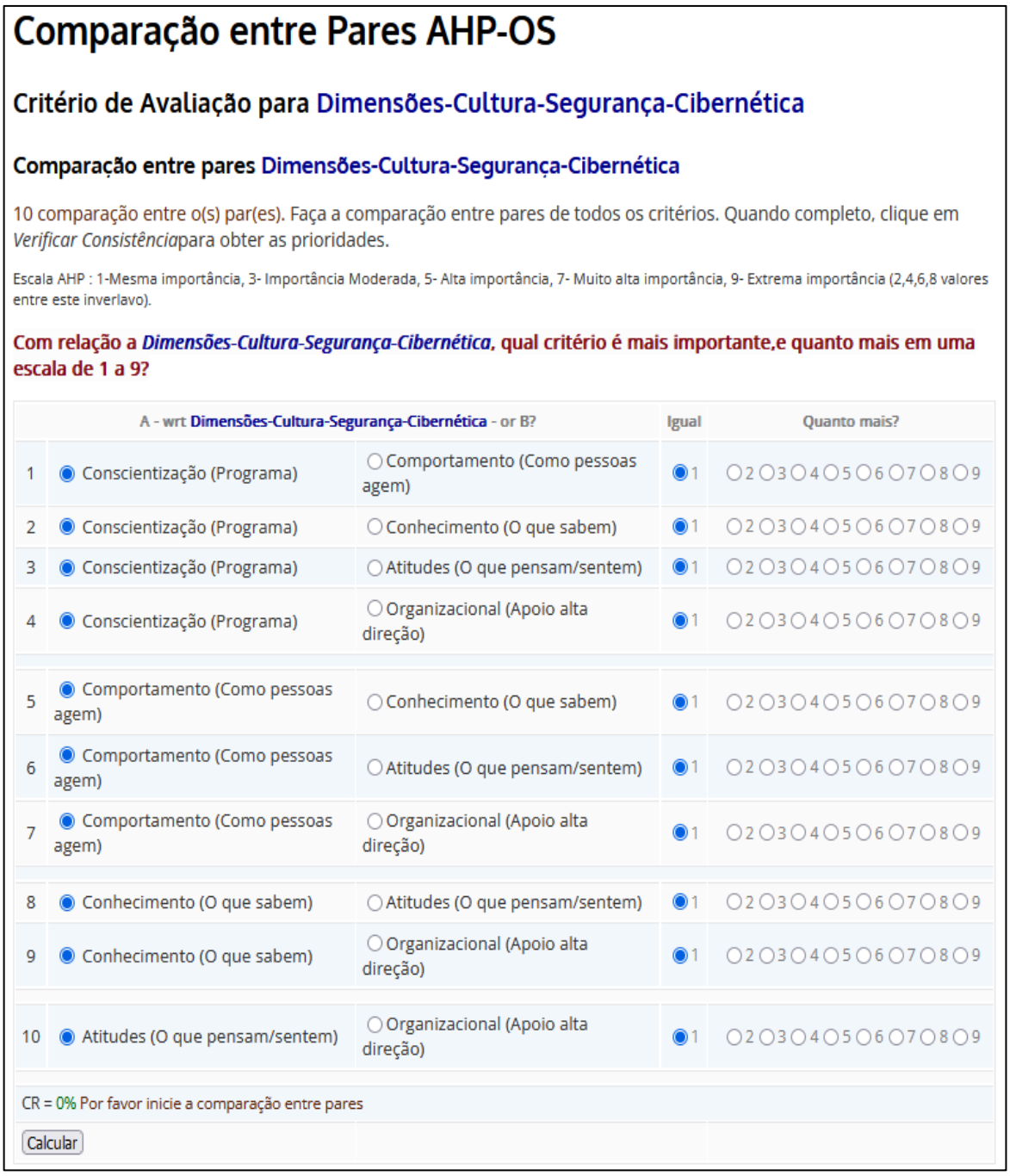
As dimensões foram apresentadas em pares e os especialistas avaliaram a importância relativa de cada uma em relação à cultura de segurança da organização. Adotou-se a escala linear padrão de Saaty (1990), que estabelece valores de 1 a 9 para definir o critério de importância entre as comparações.

A ferramenta AHP-OS permitiu calcular a taxa de consistência das decisões de cada especialista. Segundo Saaty (1990), este é um indicador que avalia a coerência das comparações em pares, indicando que valores abaixo de 10% possuem julgamentos consistentes, enquanto valores superiores sugerem a necessidade de revisão das comparações.

Os julgamentos de cada especialista foram submetidos ao cálculo de consistência pela ferramenta AHP-OS, quando a taxa ficava acima de 10%, o especialista reavaliava sua decisão e procedia os ajustes para que a consistência das decisões ficasse abaixo dos 10%.

A Figura 8 apresenta a escala AHP linear padrão e as dimensões dispostas em pares antes dos julgamentos.

Figura 8 - Comparação das dimensões no AHP



Comparação entre Pares AHP-OS

Critério de Avaliação para Dimensões-Cultura-Segurança-Cibernética

Comparação entre pares Dimensões-Cultura-Segurança-Cibernética

10 comparação entre o(s) par(es). Faça a comparação entre pares de todos os critérios. Quando completo, clique em *Verificar Consistência*para obter as prioridades.

Escala AHP : 1-Mesma importância, 3- Importância Moderada, 5- Alta importância, 7- Muito alta importância, 9- Extrema importância (2,4,6,8 valores entre este inverlavo).

Com relação a *Dimensões-Cultura-Segurança-Cibernética*, qual critério é mais importante,e quanto mais em uma escala de 1 a 9?

	A - wrt Dimensões-Cultura-Segurança-Cibernética - or B?		Igual	Quanto mais?
1	◉ Conscientização (Programa)	○ Comportamento (Como pessoas agem)	◉ 1	○2 ○3 ○4 ○5 ○6 ○7 ○8 ○9
2	◉ Conscientização (Programa)	○ Conhecimento (O que sabem)	◉ 1	○2 ○3 ○4 ○5 ○6 ○7 ○8 ○9
3	◉ Conscientização (Programa)	○ Atitudes (O que pensam/sentem)	◉ 1	○2 ○3 ○4 ○5 ○6 ○7 ○8 ○9
4	◉ Conscientização (Programa)	○ Organizacional (Apoio alta direção)	◉ 1	○2 ○3 ○4 ○5 ○6 ○7 ○8 ○9
5	◉ Comportamento (Como pessoas agem)	○ Conhecimento (O que sabem)	◉ 1	○2 ○3 ○4 ○5 ○6 ○7 ○8 ○9
6	◉ Comportamento (Como pessoas agem)	○ Atitudes (O que pensam/sentem)	◉ 1	○2 ○3 ○4 ○5 ○6 ○7 ○8 ○9
7	◉ Comportamento (Como pessoas agem)	○ Organizacional (Apoio alta direção)	◉ 1	○2 ○3 ○4 ○5 ○6 ○7 ○8 ○9
8	◉ Conhecimento (O que sabem)	○ Atitudes (O que pensam/sentem)	◉ 1	○2 ○3 ○4 ○5 ○6 ○7 ○8 ○9
9	◉ Conhecimento (O que sabem)	○ Organizacional (Apoio alta direção)	◉ 1	○2 ○3 ○4 ○5 ○6 ○7 ○8 ○9
10	◉ Atitudes (O que pensam/sentem)	○ Organizacional (Apoio alta direção)	◉ 1	○2 ○3 ○4 ○5 ○6 ○7 ○8 ○9

CR = 0% Por favor inicie a comparação entre pares

Calcular

Fonte: Resultado da pesquisa (2024).

Após o julgamento de todos os especialistas a ferramenta AHP-OS calculou as prioridades globais e os percentuais das decisões de cada respondente para as dimensões do modelo de maturidade.

A Figura 9, apresenta o resumo das prioridades globais definida pelo grupo de decisores.

Figura 9 - Prioridades globais do grupo de decisores

Participante	Conscientização (Programa)	Comportamento (Como pessoas agem)	Conhecimento (O que sabem)	Atitudes (O que pensam/ sentem)	Organizacional (Apoio alta direção)	CR_{max}
Resultado do Grupo	**16.3%**	**31.2%**	**17.9%**	**18.9%**	**15.7%**	**0.5%**
Respondente 10	6.9%	50.4%	24.7%	14.9%	3.1%	7.2%
Respondente 9	11.9%	51.1%	5.9%	23.8%	7.4%	7.1%
Respondente 8	3.2%	14.4%	52.1%	23.9%	6.3%	7.0%
Respondente 7	45.2%	14.3%	5.8%	31.4%	3.4%	5.0%
Respondente 6	17.2%	4.8%	7.5%	3.6%	67.0%	9.8%
Respondente 5	16.5%	33.0%	17.4%	27.0%	6.1%	10.0%
Respondente4	26.5%	3.5%	17.5%	6.2%	46.3%	8.4%
Respondente 3	8.2%	51.6%	10.1%	23.7%	6.4%	10.0%
Respondente 2	7.0%	53.8%	3.8%	8.7%	26.8%	9.0%
Respondente 1	7.7%	36.3%	30.6%	7.1%	18.3%	7.8%

Fonte: Resultado da pesquisa (2024).

O resultado obtido pelo cálculo da ferramenta AHP-OS com a hierarquia final das decisões é apresentado na Figura 10.

Figura 10 - Pesos das dimensões do MMCSC

Hierarquia com as prioridades consolidadas

Participantes Selecionados: All

Hierarquia de decisão		
Nível 0	Nível 1	Glb Prio.
Dimensões-Cultura-Segurança-Cibernética	Conscientização (Programa) 0.163	16.3%
	Comportamento (Como pessoas agem) 0.312	31.2%
	Conhecimento (O que sabem) 0.179	17.9%
	Atitudes (O que pensam/sentem) 0.189	18.9%
	Organizacional (Apoio alta direção) 0.157	15.7%
		1.0

Fonte: Resultado da pesquisa (2024).

De acordo com a Figura 10, mediante a opinião consolidada dos decisores, a dimensão do comportamento é a mais influente e tem uma importância de 31,2% na determinação do nível de maturidade da cultura de segurança cibernética, a dimensão das atitudes aparece em segundo lugar com 18,9%, seguido pela dimensão do conhecimento com 17,9%, conscientização com 16,3% e organizacional com 15,7%.

3.3 Resultados das entrevistas com especialistas em segurança e conscientização

As entrevistas semiestruturadas foram realizadas com dez especialistas internos em segurança cibernética e conscientização e procuraram obter uma visão qualificada e detalhada sobre a maturidade da cultura de segurança cibernética da organização. As questões das entrevistas estão relacionadas no Apêndice C e foram elaboradas a partir do MMCSC proposto estando diretamente relacionadas à questão e aos objetivos da pesquisa que se propõem a avaliar o nível de maturidade da cultura de segurança cibernética utilizando um modelo de maturidade.

As entrevistas foram conduzidas no período de 24 de outubro a 05 de novembro de 2024, de forma *online,* pelo aplicativo *Microsoft Teams,* Microsoft (2024), com transcrição gerada automaticamente pelo aplicativo. A seleção dos especialistas internos da organização se deu pelo seu conhecimento e experiência na área de segurança cibernética, pela indicação dos gestores de segurança e por sua atuação relacionada ao tema da pesquisa. Para atender aos requisitos de privacidade exigidos pela organização, a identificação e anonimização dos especialistas seguiu o disposto no Quadro 16.

Quadro 16 – Especialistas internos da organização

Identificação	Área	Escolaridade	Tempo de empresa	Código
Especialista 1	Segurança gestão	Pós-graduação (*lato sensu*)	Mais de 10 anos	Esp01
Especialista 2	Segurança gestão	Pós-graduação (*lato sensu*)	Mais de 10 anos	Esp02
Especialista 3	Segurança operacional	Pós-graduação (*lato sensu*)	Mais de 15 anos	Esp03
Especialista 4	Segurança gestão	Pós-graduação (*lato sensu*)	Mais de 20 anos	Esp04
Especialista 5	Segurança gestão	Pós-graduação (*lato sensu*)	Mais de 10 anos	Esp05
Especialista 6	Segurança normativos	Pós-graduação (*lato sensu*)	Até 5 anos	Esp06
Especialista 7	Segurança operacional	Mestrado	Até 10 anos	Esp07
Especialista 8	Segurança de aplicações	Pós-graduação (*lato sensu*)	Até 10 anos	Esp08
Especialista 9	Conscientização gestão	Doutorado	Até 10 anos	Esp09
Especialista 10	Segurança operacional	Pós-graduação (*lato sensu*)	Mais de 10 anos	Esp10

Fonte: Resultado da pesquisa (2024).

Após obter o consentimento de cada especialista interno para a realização da entrevista o roteiro seguiu a seguinte ordem: 1) breve contextualização sobre o cenário de segurança cibernética; 2) explicação sobre os objetivos e características da pesquisa; 3) definição dos pesos das dimensões do modelo de maturidade (conforme item 3.2); 4) questões para avaliar a cultura de segurança cibernética da organização; 5) agradecimentos.

As transcrições das entrevistas foram consolidadas, codificadas e agrupadas em categorias, pois, de acordo com Bardin (1977), a análise de conteúdo é uma técnica que permite a descrição sistemática e objetiva de pesquisas qualitativas, sendo útil na análise de entrevistas semiestruturadas ao permitir a categorização e interpretação das falas dos sujeitos, identificando padrões, temas e significados que emergem dos dados.

Os resultados das entrevistas com os especialistas internos da organização são apresentados a seguir.

3.3.1 Nível de conhecimento dos funcionários sobre ameaças recentes, vulnerabilidades e ataques globais (Q1)

Os especialistas relataram dois aspectos catalisadores para o aumento do conhecimento sobre ameaças recentes, vulnerabilidades e ataques globais. A exposição do tema na mídia foi o fator mais indicado: *"[...] a informação sobre ameaças que tem causado ataques globais ela tem se tornado mais frequente e acaba, de certa forma, fazendo parte do dia a dia do funcionário"* [Esp07]. Outro especialista corroborou: *"[...] eles leem sobre alguns ataques, sobre os golpes que saem na praça, que são compartilhados e tal"* [Esp02]

A plataforma de treinamento adotada nos últimos pela empresa também se destacou como outra influência positiva no conhecimento dos funcionários: *"[...] a gente tem elevado esse nível de conhecimento dos empregados e pelo caráter também dos treinamentos estarem mais atrativos, ele prende mais a atenção e o interesse aumentam em relação ao tema"* [Esp09], assim como: *"[...] eles fazem o treinamento e pedem para desbloquear a outra temporada da série de vídeos"* [Esp03].

Os especialistas também identificaram pontos negativos para o conhecimento dos funcionários sobre o tema abordado na Q1. A afinidade que funcionários de áreas técnicas e de

segurança tem em relação aos de outras áreas foi um dos principais destaques: *"acredito que as áreas operacionais de tecnologia elas acabam tendo um conhecimento maior do que o usuário que não trabalha diretamente com tecnologia"* [Esp07], *"no perfil das pessoas que trabalham aqui, nem todas têm as mesmas experiências e nem todas têm as mesmas mesmos conhecimentos para lidar com ameaças"* [Esp08], e por fim: *"Aqui na área de segurança a gente vê o assunto o tempo todo, mas quando a gente está falando de outras áreas, o entendimento e o conhecimento não são tão grandes"* [Esp06].

Outro tema relevante informado como obstáculo para o conhecimento foi a falta de interesse: *"[...] não é um tema de interesse da maioria das pessoas"* [Esp02], outro reiterou: *"[...] aqui pouco se consome sobre segurança"* [Esp05], bem como: *"[...] Algumas pessoas por gostar do assunto ou por trabalhar na área de segurança podem ter mais conhecimento"* [Esp10].

Os especialistas também apontaram a dificuldade de o funcionário estar atualizado sobre o tema: *"[...] a velocidade dos ataques é bem evoluída, é muito rápido. Até para os analistas de segurança é difícil acompanhar"* [Esp04] e *"[...] é difícil ficar atualizado se você não tem um hábito de estudo periódico sobre este assunto"* [Esp10].

3.3.2 Nível de conhecimento dos funcionários sobre as diretrizes, normas e processos de segurança (Q2)

Sobre o tema da Q2 os especialistas destacaram vários aspectos que dificultam o conhecimento das normas e diretrizes de segurança da organização. A complexidade das normas, as questões envolvendo a sua divulgação e o baixo engajamento dos funcionários foram os temas mais relevantes: *"[...] as pessoas tendem a ver as normas como extensas, muito técnicas, então são pouco atrativas"* [Esp09], *"[...] as normas são documentos mais extensos com uma linguagem mais formal"* [Esp10].

Outro destacou: *"[...] O problema são as nossas normas. A pessoa não se identifica com o que está escrito lá"* [Esp03].

Sobre a divulgação: *"[...] Existe um problema de comunicação na empresa, por exemplo, mesmo que você decida por atitude própria, pesquisar uma informação [...] você vai*

ter trabalho" [Esp08], bem como: *"[...] eu acho que a gente tem um pouco de dificuldade do corpo funcional de ter total conhecimento das normas"* [Esp09].

Em relação ao engajamento dos funcionários: *"[...] só leem quando é obrigatório"* [Esp06] e *"[...] não vejo muito interesse em conhecê-las"* [Esp10].

3.3.3 Percepção dos funcionários sobre a importância da segurança cibernética (Q3)

Na opinião dos especialistas, a maioria entendeu que é positiva a percepção que os funcionários têm sobre a importância da segurança cibernética. Os fatores que contribuíram para isso foram a quantidade de informação disponível na mídia sobre ataques e ameaças cibernéticas e a estrutura da área de segurança existente na organização: *"[...] Devido à quantidade de incidentes que existem e tipos de ataques que existe hoje no fora da empresa. Isso deixa a pessoa muito alerta mais do que pelo próprio processo de conscientização da empresa"* [Esp04] e *"[...] importante principalmente pelos ataques que sempre são veiculados na mídia"* [Esp10].

Sobre a estrutura da segurança na empresa: *"[...] se a pessoa sabe que você é da segurança, você percebe que o comportamento deles muda. Então, minimamente é uma percepção que eles têm"* [Esp05], assim como: *"[...] entendem que é importante pelo fato de a gente ter algumas áreas de segurança na empresa, não apenas uma"* [Esp08].

3.3.4 Visão dos funcionários sobre a segurança da empresa (Q4)

A visão que os funcionários têm sobre a segurança da empresa, na opinião de parte dos especialistas, foi negativa. Para eles, a segurança é vista como um obstáculo. O [Esp04] destacou: *"[...] a segurança é muito mais vista como um obstáculo [...] o acesso a banco de dados, por exemplo, tem uma burocracia, é uma série de regras para conseguir. Eles dizem: Pô, então às vezes é difícil entender por que eu passo por todo esse processo"*.

Há também, segundo eles, uma visão distorcida da segurança da empresa ou ainda distante da realidade: *"[...]as pessoas relaxam por conta disso, pela crença de que nada vai me acontecer"* [Esp03], *"[...] historicamente quando tem um incidente [...] aí as pessoas mudam essa visão."* [Esp04], também: *"[...] o corpo funcional tem essa visão de que tem áreas de segurança e que eles zelam por um comportamento seguro, ou seja, para mitigar os riscos aí existentes."* [Esp05].

Outros especialistas identificaram uma percepção positiva dos funcionários em relação à segurança da empresa: *"[...] é falado o tempo todo que é seguro [...] então eles têm uma visão do que é passado para eles."* [Esp06], assim como: *"[...] Creio que são muito bem comunicadas a todos e que isso fortalece a visão que os funcionários têm sobre a segurança da empresa como um todo"* [Esp07].

3.3.5 Percepção sobre o comportamento seguro dos funcionários (Q5)

Sobre o comportamento dos funcionários relativo à segurança cibernética, os especialistas destacaram que há comportamentos que são considerados imprudentes e que é necessário investir em medidas para aprimorar o comportamento do corpo funcional.

O principal destaque nos comportamentos imprudentes foi deixar a estação de trabalho desbloqueada: *"[...] o comportamento de pessoas que deixam a estação de trabalho aberta é ainda um número considerável de pessoas que comete esta falha regularmente"* [Esp08].

Outro aspecto levantado foi descaso com as diretrizes de segurança por acreditar que nada vai lhes acontecer: *"[...] existe essa confiança estabelecida, as pessoas então acabam baixando a guarda e aí você tem um comportamento não seguro por conta disso"* [Esp03].

Alguns especialistas apontaram a necessidade de aprimorar o comportamento: *"[...] creio que há pontos a serem ajustados no que diz respeito ao comportamento"* [Esp07], *"[...] no comportamento temos muito que trabalhar e conscientizar"* [Esp06], assim como: *"[...] tem muito espaço para melhorar"* [Esp05].

3.3.6 Percepção sobre a eficácia do programa de conscientização (Q6)

Sobre o programa de conscientização a opinião dos especialistas foi divergente em alguns pontos. Alguns deles ressaltaram os benefícios que a plataforma de treinamento contratada pela empresa trouxe para a cultura de segurança e apontaram as simulações de *phishing* como um fator contributivo. Por outro lado, uma boa parte dos especialistas destacaram fragilidades e deficiências no programa atual de conscientização.

Sobre os aspectos positivos o [Esp02] destacou: *"[...] houve uma contratação de um fornecedor externo especializado em treinamentos em formas de vídeo. Ajudou bastante, gerou um impacto muito positivo"*, ainda: *"[...] outro destaque que eu vejo são as simulações de phishing nos e-mails enviados pela própria área de segurança para testar o funcionário"*, outro ressaltou: *"[...] atualmente tem uma plataforma boa de treinamento"* [Esp10].

Sobre as lacunas no programa de conscientização: *"[...] nosso programa de conscientização estagnou [...] a plataforma de treinamento é muito generalizada e repetível [...] ela não ensina as nossas regras, ela não fala sobre a empresa, não tem aquele conteúdo customizado [...] as pessoas estão ficando mais ignorantes com relação à segurança, estão desaprendendo, estão piorando o comportamento"* [Esp03].

Outros ainda destacaram: *"[...] o programa não exercita realmente as pessoas. Ele é por demais simples"* [Esp08], *"[...] eu acho que ele carece de mais ações"* [Esp01].

Alguns especialistas apontaram fatores externos ao programa, mas que, segundo eles, tem influência no seu desempenho. Mencionaram a necessidade de a alta direção dar o exemplo em comportamento seguro e oferecer mais apoio nos projetos e inciativas de conscientização.

3.3.7 Visão sobre o apoio e envolvimento da alta direção na cultura de segurança (Q7)

A opinião dos especialistas sobre a relação que alta administração tem com a cultura de segurança cibernética na organização destacou basicamente dois pontos: o apoio e a comunicação, entendida como a manifestação explícita sobre segurança por parte da direção da empresa.

Sobre o apoio, três especialistas entendem que há apoio consistente porque a área de segurança está diretamente ligada à presidência da empresa, porque as ações de segurança estão previstas no plano de ação da companhia e que a contratação da plataforma de treinamento demonstra esse apoio da direção da empresa.

Outros especialistas reforçaram que o apoio mínimo que se tem se deve à necessidade de a organização cumprir exigências regulamentares dos órgãos de controle e evitar questionamentos de auditorias externas.

A comunicação é outro ponto destacado como negativo pelos especialistas. Eles disseram que não há demonstrações públicas sobre as ações ou sobre a importância da segurança, nem para o corpo funcional, nem em eventos internos ou externos. Alguns ainda acrescentaram que o apoio que a segurança recebe é sazonal, que no passado ele já foi melhor e que a segurança atualmente não uma prioridade.

As entrevistas com os especialistas revelaram uma visão variada sobre a cultura de segurança cibernética na organização. Eles apontaram algumas características que promovem o conhecimento dos funcionários sobre segurança, mas ainda existem barreiras significativas, como a complexidade das normas e a falta de interesse em alguns perfis profissionais. A percepção sobre a segurança cibernética é, para alguns, positiva, mas para outros, a segurança é vista como um obstáculo ou algo distante do cotidiano. O comportamento seguro dos funcionários é um ponto a ser trabalhado continuamente, as limitações do programa de conscientização atual foram apontadas como desafios que demandam envolvimento estratégico. Por fim, o apoio e a comunicação da alta direção surgem como elementos vitais para transformar a segurança cibernética em uma prioridade permanente e visível.

3.4 Resultados da pesquisa *survey*

A *survey* foi aplicada através de formulário *online* com a utilização da ferramenta *Google Forms* (Google, 2024). O questionário foi validado por um pré-teste com quatro respondentes da área de tecnologia da informação, com o intuito de corrigir eventuais falhas no entendimento dos enunciados e promover ajustes na ordem de apresentação das questões (Malhotra, 2010).

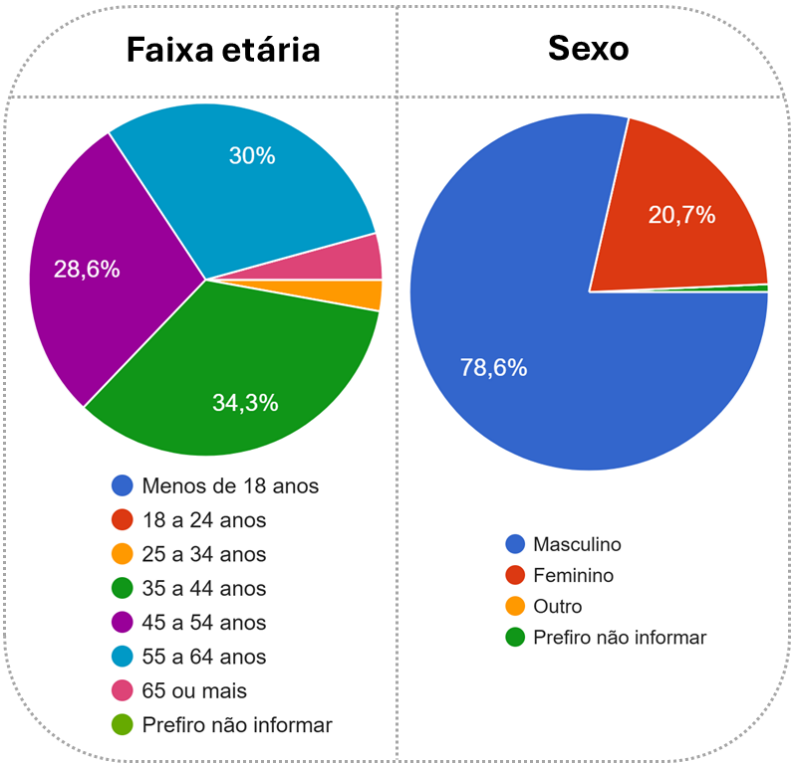
O universo dos respondentes se constituiu por funcionários de uma entidade da administração pública federal. Foi adotada para a pesquisa a *survey* não probabilística por conveniência, devido aos critérios de seleção não aleatórios e pela disponibilidade e facilidade de acesso aos participantes (Baxter, 2004; Cooper, 2016)

Foram enviados 258 convites individuais com o *link* do questionário pelo aplicativo *Microsoft Teams* (Microsoft, 2024). O questionário esteve aberto aceitando respostas no período de 23 de outubro a 05 de novembro de 2024 e obteve 140 respostas preenchidas integralmente.

3.4.1 Perfil dos respondentes

O perfil dos respondentes é composto em sua maioria de pessoas do sexo masculino 78,57%, seguido pelas mulheres com 20,71%. A faixa etária está distribuída entre 35 e 44 anos com 34,29%, de 55 a 64 anos com 30% e de 45 a 54 anos com 28,57%.

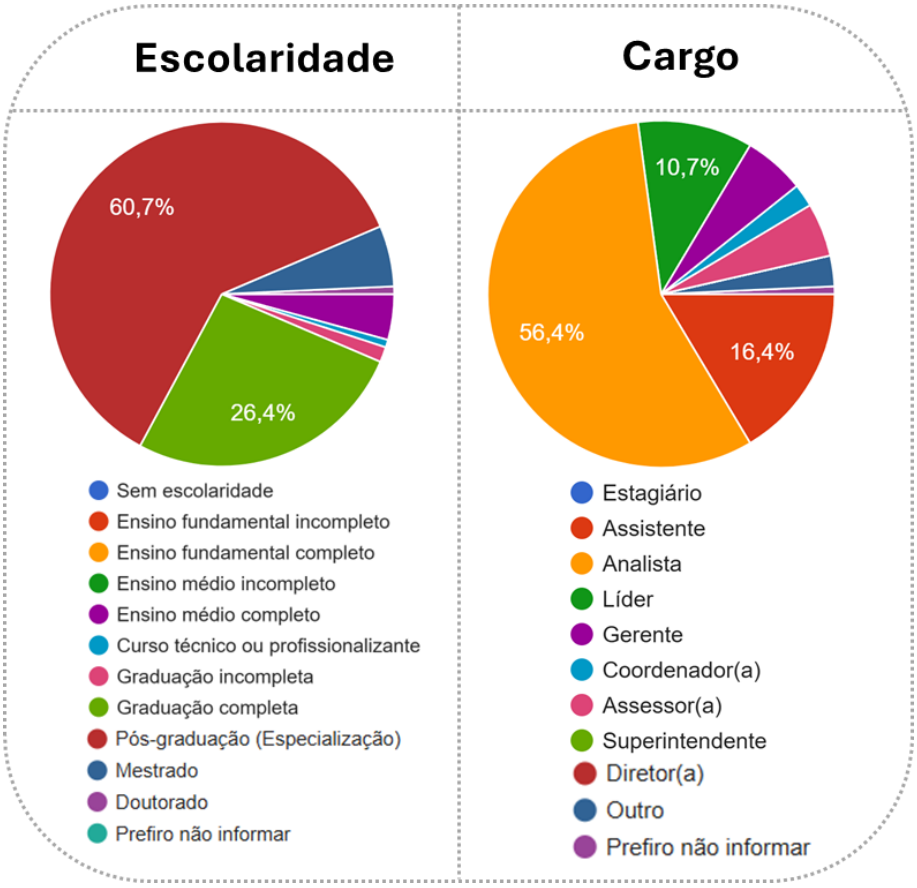
Gráfico 1 - Idade e sexo dos respondentes



Fonte: Resultado da pesquisa (2024).

Com relação ao nível de escolaridade, o grupo maior são de pessoas com pós-graduação (especialização) com 60,71%, seguido pela graduação completa com 26,43% e demais níveis de formação. Os cargos predominantes são de analista com 56,43%, assistente com 16,43% e líder com 10,71%.

Gráfico 2 - Escolaridade e cargo dos respondentes



Fonte: Resultado da pesquisa (2024).

No que se ao tempo de trabalho na empresa, o maior grupo foi o de pessoas com mais de 10 anos de serviço, com 79,29%, seguido por indivíduos de 6 a 10 anos, representando 10% dos respondentes.

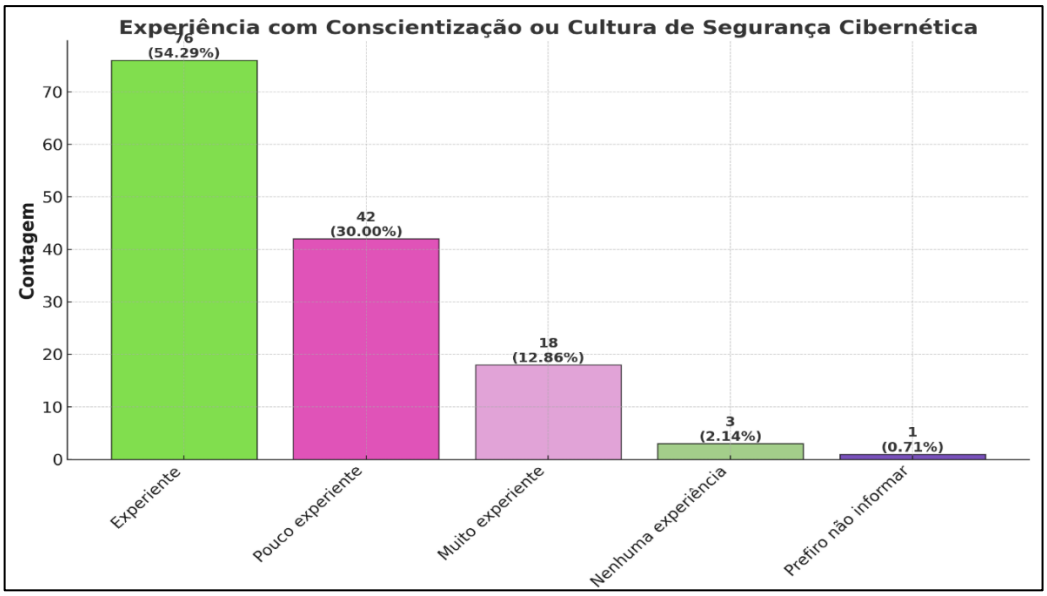
As áreas em que os respondentes atuam está bem distribuída, sendo a área de segurança da informação a maior com 24,29% e a área técnica de infraestrutura com 20,71%.

Gráfico 3 - Experiência e área profissional

Fonte: Resultado da pesquisa (2024).

Em relação à experiência com conscientização ou cultura de segurança cibernética a maioria dos participantes se declarou experiente representando 54,29%, em contrapartida, os que disseram serem pouco experientes nesse tema foi de 30%.

Gráfico 4 - Experiência com conscientização ou CSC

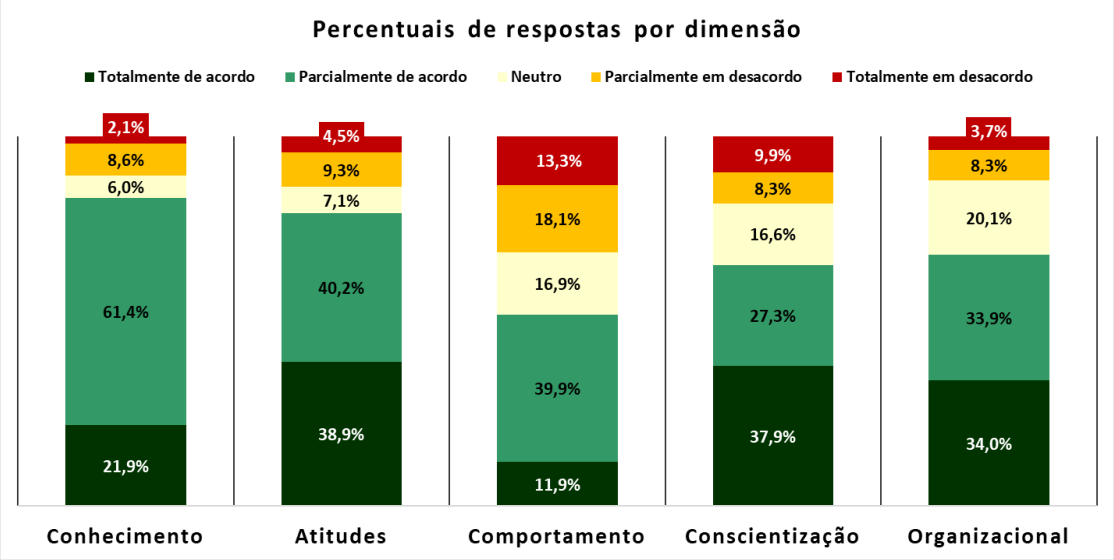


Fonte: Resultado da pesquisa (2024).

3.4.2 Resultados das perguntas sobre a CSC

Os resultados das perguntas sobre a cultura de segurança cibernética estão agrupados por dimensão. O Gráfico 5, apresenta os percentuais das respostas.

Gráfico 5 - Percentuais de respostas por dimensão

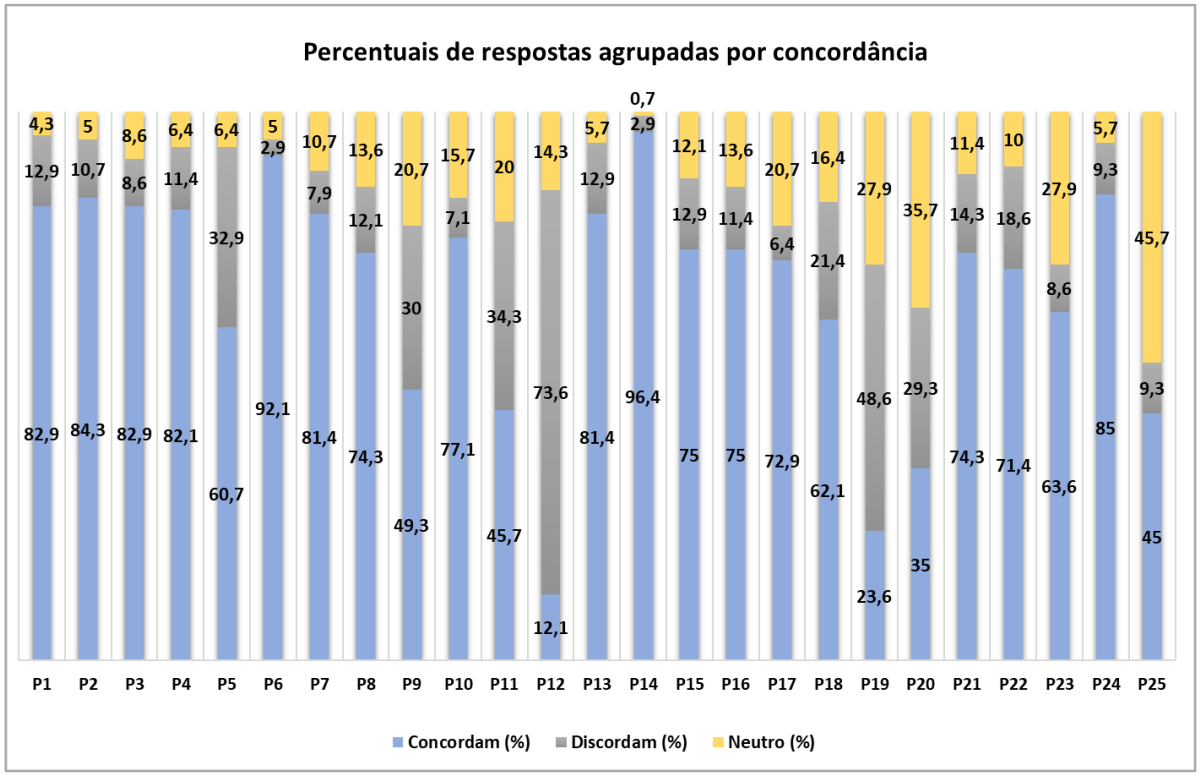


Fonte: Resultado da pesquisa (2024).

Conforme apresentado no Gráfico 5, os respondentes concordam totalmente (21,9%) e concordam parcialmente (61,4%), que os funcionários possuem conhecimento sobre ameaças, vulnerabilidades, ataques, diretrizes de segurança e possuem habilidade para executar o trabalho de forma segura. Em relação à dimensão das atitudes, há uma concordância total de 38,9% e concordância parcial de 40,2%, dos funcionários sobre importância e a priorização estratégica da segurança na empresa. No que se refere ao comportamento, pouco mais da metade dos respondentes (51,8%) concordam que os funcionários têm uma conduta segura em suas atividades diárias. Referente ao programa de conscientização e aos processos para desenvolver a cultura de segurança na organização o entendimento foi de que as iniciativas são efetivas e consistentes para 65,2% dos respondentes. No que tange ao apoio e ao envolvimento da alta direção, as opiniões mostram que 12% discordam, 20,1% declaram neutralidade para avaliar e os demais 33,9% e 34% entendem que a liderança oferece apoio efetivo para aprimorar a cultura de segurança na organização.

As respostas individuais agrupadas por concordância e discordância das afirmações podem ser observadas no Gráfico 6.

Gráfico 6 - Percentuais agrupados por concordância

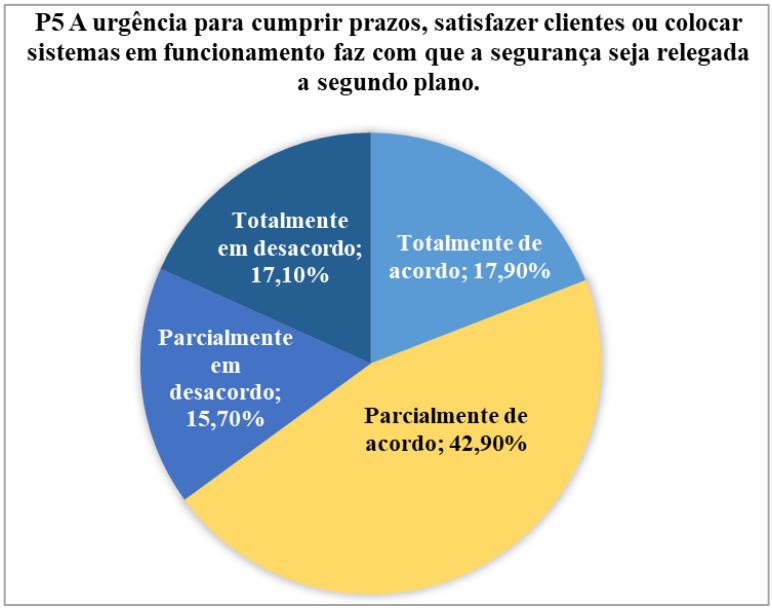


Fonte: Resultado da pesquisa (2024).

De acordo com o Gráfico 6, percebe-se uma alta concordância de mais de 80% para as três primeiras perguntas da dimensão do conhecimento, isso também ocorre na P6 com 92,1%, referente à infraestrutura e controles de segurança da empresa, na P14 sobre os treinamentos de segurança, com 96,4% e na P24 com 85% relativo à segurança estar presente nas decisões estratégicas da empresa. A P25 referente à participação dos líderes executivos em fóruns de segurança apresenta o maior grau de neutralidade na opinião dos respondentes com 45,7% e a P12 sobre a maioria das condutas serem inseguras teve a maior discordância com 73,6%.

As perguntas P5, P11 e P12 tiveram por objetivo estimular o pensamento crítico do respondente em relação à segurança na empresa, as respostas assinaladas como de acordo, demonstram aspectos negativos ou incipientes da cultura de segurança na organização. O Gráfico 7 retrata a percepção referente a P5.

Gráfico 7 - Concordâncias e discordâncias pergunta 5

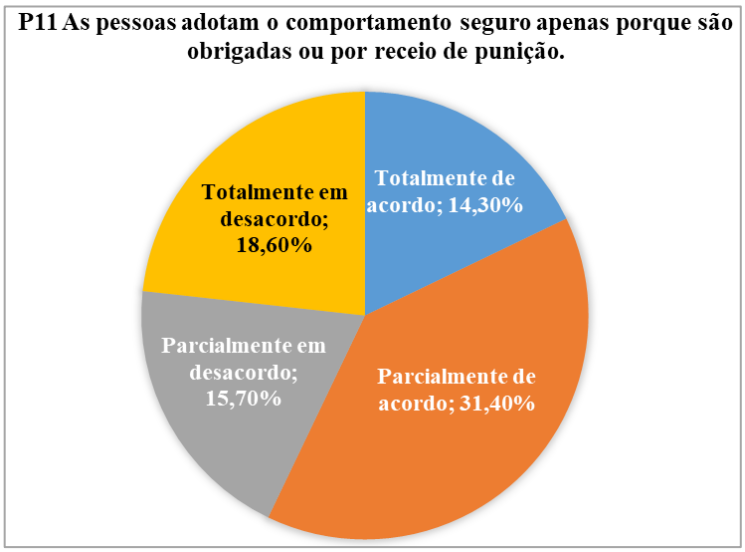


Fonte: Resultado da pesquisa (2024).

A opinião dos respondentes na P5, conforme indicado no Gráfico 7, mostrou que mais da metade 60,8%, concordam que a segurança fica relegada a segundo plano devido à urgência para cumprir prazos, satisfazer clientes ou colocar sistemas em funcionamento.

O Gráfico 8, apresenta a percepção dos respondentes sobre a obrigatoriedade do comportamento seguro.

Gráfico 8 - Concordâncias e discordâncias pergunta 11

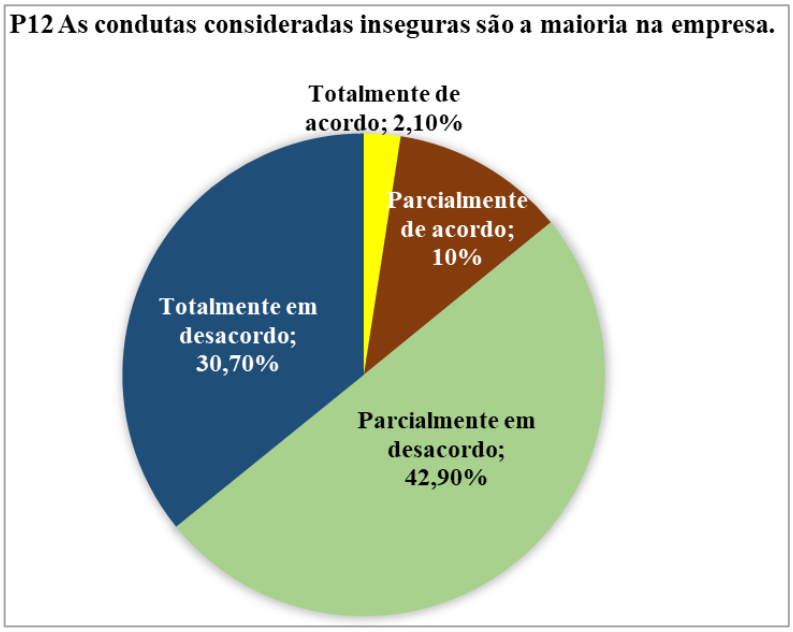


Fonte: Resultado da pesquisa (2024).

Segundo o Gráfico 8, a parcela de 45,7% dos respondentes entende que os funcionários seguem as diretrizes de segurança apenas porque são obrigados ou por receio de serem punidos.

O Gráfico 9, ilustra a percepção sobre a conduta insegura dos funcionários na organização.

Gráfico 9 - Concordâncias e discordâncias pergunta 12



Fonte: Resultado da pesquisa (2024).

Conforme o Gráfico 9, a percepção sobre a conduta dos funcionários ser predominantemente insegura na empresa não é a maioria conforme indicaram 73,6% dos respondentes, apenas 12,1% concordaram que o comportamento inseguro é o mais comum.

3.5 Cálculo do nível de maturidade da organização

O nível de maturidade da cultura de segurança cibernética da organização, de acordo com os dados obtidos, foi mensurado a partir de duas fontes de informação. A primeira obtida através das entrevistas com os especialistas internos da organização e a segunda a partir das respostas da *survey*.

3.5.1 Nível de maturidade segundo a percepção dos especialistas

Para obter o nível de maturidade a partir das entrevistas com os especialistas foi necessário realizar a conversão numérica dos dados, de forma que, as respostas que indicavam vales como “baixo” “frágil”, “boa”, “pouco” e assim sucessivamente, foram codificadas numericamente para corresponder aos valores dos níveis do modelo de maturidade, conforme o Quadro 10, do item 3.1.1, níveis do MMCSC. Adotou-se novamente a Likert de 5 pontos, sendo: 1 - Inicial, 2 - Básico, 3 - Intermediário, 4 - Aprimorado e 5 - Avançado (Nemoto; Beglar, 2014). A Tabela 2, apresenta os valores tabulados e consolidados de cada questão por entrevistado.

Tabela 2 - Percepções de maturidade dos especialistas

Questão	Esp01	Esp02	Esp03	Esp04	Esp05	Esp06	Esp07	Esp08	Esp09	Esp10
Ameaças (Q1)	2	2	3	3	3	3	4	2	3	2
Diretrizes SI da empresa (Q2)	2	2	3	3	3	3	2	2	3	1
Importância segurança (Q3)	5	3	5	4	4	2	3	4	5	5
Visão SI empresa (Q4)	3	4	4	2	3	4	5	2	4	4
Comportamento (Q5)	2	4	2	3	3	2	3	2	2	2
Eficácia conscientização (Q6)	2	5	2	3	3	4	3	2	4	4
Apoio alta direção (Q7)	3	3	2	2	3	2	3	2	4	3

Fonte: Resultado da pesquisa (2024).

Conforme apresentado na Tabela 2, a visão dos especialistas sobre o nível, a importância e a gradação das dimensões de maturidade foram codificadas numericamente. O especialista 06, por exemplo, entende que a percepção que os funcionários têm sobre a segurança cibernética na organização é básica, o que corresponde ao valor 2, de acordo com a escala apresentada acima. Para calcular o nível de maturidade foi apurada a média aritmética das questões para cada dimensão. As questões Q1 e Q2, Q3 e Q4, referem-se às dimensões do conhecimento e atitudes respectivamente, conforme o Apêndice C, elas foram somadas para apurar a média da dimensão. O Quadro 17, apresenta os valores do nível de maturidade segundo os especialistas internos da organização.

Quadro 17 – Maturidade segundo os especialistas

Dimensões	Conhecimento			Atitudes			Comporta-mento		Conscien-tização		Organiza-cional		Maturidade
Questões	Ameaças (Q1)	Diretrizes SI da empresa (Q2)	2,55	Impor-tância segurança (Q3)	Visão SI empresa (Q4)	3,75	Comporta-mento (Q5)		Eficácia conscienti-zação (Q6)		Apoio alta direção (Q7)		3,00
Maturidade dimensão	2,70	2,40	Básico	4,00	3,50	Interme-diário	2,50	Básico	3,20	Interme-diário	2,70	Básico	Interme-diário

Fonte: Resultado da pesquisa (2024).

Conforme apresentado no Quadro 17, o nível de maturidade da cultura de segurança cibernética, segundo a visão dos especialistas, é intermediário. De acordo com o MMCSC, esta classificação indica que há consistência nas práticas de conscientização e que existe uma estrutura definida para o aprimoramento da cultura de segurança.

Contudo, os respondentes demonstraram que a dimensão do conhecimento, comportamento e organizacional ainda estão no nível básico de maturidade, indicando que os processos relacionados a estas dimensões estão em estágios iniciais e que apenas o mínimo em relação à cultura de segurança está sendo executado na organização.

3.5.2 Nível de maturidade com base na survey

O nível de maturidade da cultura de segurança cibernética com base nas respostas da *survey* é calculado em etapas. O primeiro passo é a soma de todos os valores das perguntas de cada dimensão.

Em seguida, obtêm-se o valor máximo possível para cada dimensão. Na sequência, com a soma de todas as perguntas e o valor máximo da dimensão, calcula-se o percentual de maturidade da dimensão.

Posteriormente, aplicam-se os pesos das dimensões aos percentuais resultando no valor ponderado de maturidade para a dimensão.

Finalmente, somam-se os valores ponderados das dimensões para obter o nível de maturidade. As equações abaixo detalham as etapas de cálculo do nível de maturidade da organização.

3.5.2.1 Somatória das respostas de cada dimensão

O valor total das respostas da dimensão é soma de todos os valores das perguntas, até o valor 4, segundo a escala, de acordo com a quantidade de perguntas daquela dimensão. Por exemplo, a dimensão do conhecimento possui 3 perguntas, os valores obtidos com o questionário somaram 402 para a P1, 418 para a P2 e 408 para a P3. Desta forma, a soma das respostas da dimensão do conhecimento é de 1228. O cálculo da somatória da dimensão é definido na Equação (1).

$$S_{D_i} = \sum_{j=1}^{n_i} R_{ij} \tag{1}$$

Onde:

S_{D_i} é a soma das respostas para a dimensão;

R_{ij} é o valor da resposta da j-ésima pergunta na dimensão;

n_i é o número de perguntas na dimensão.

3.5.2.2 Cálculo do valor máximo possível para a dimensão

O cálculo do valor máximo para cada dimensão é necessário para se obter o percentual de maturidade da dimensão. Ele é calculado pela multiplicação do número total de perguntas da dimensão, pela pontuação máxima possível na pergunta e pela quantidade total de respostas obtidas no questionário.

Por exemplo, a quantidade de perguntas da dimensão do conhecimento é de 3, multiplicado pela pontuação máxima que é 4, pelo total de respostas obtidas que é 140, resulta no total de 1680. O cálculo do valor máximo possível para a dimensão é definido na Equação (2).

$$M_{D_i} = n_i \times P_{\text{máx}} \times N \tag{2}$$

Onde:

n_i é o número de perguntas na dimensão;

$P_{\text{máx}}$ é a pontuação máxima de cada pergunta;

N é o número total de respostas;

M_{D_i} é o valor máximo possível para a dimensão.

3.5.2.3 Cálculo do percentual de maturidade de cada dimensão

O cálculo do percentual de maturidade de cada dimensão é obtido pela divisão da somatória das respostas de cada dimensão, pelo valor máximo possível para a dimensão, multiplicado por 100. Por exemplo, o valor da somatória da dimensão do conhecimento é de 1228, dividido pelo máximo possível desta dimensão que é de 1680, multiplicado por 100, resulta no valor de 73,10%. O cálculo do percentual de maturidade de cada dimensão é definido na Equação (3).

$$P_{D_i} = \left(\frac{S_{D_i}}{M_{D_i}} \right) \times 100 \tag{3}$$

Onde:

S_{D_i} é a soma das respostas para a dimensão;

M_{D_i} é o valor máximo possível para a dimensão;

P_{D_i} é o percentual de maturidade da dimensão.

3.5.2.4 Valor ponderado das dimensões

O valor ponderado das dimensões é calculado com base na aplicação dos pesos das dimensões, apresentado na Figura 10, do item 3.2., definição dos pesos das dimensões do MMCSC, sobre o percentual de maturidade da dimensão. Por exemplo, o percentual de maturidade da dimensão do conhecimento é de 73,10%, multiplicado pelo peso da dimensão que é 0,179, resulta no valor de 13,08. O cálculo do valor ponderado das dimensões é definido na Equação (4).

$$W_{P_{D_i}} = P_{D_i} \times W_{D_i} \tag{4}$$

Onde:

P_{D_i} é o percentual de maturidade da dimensão;

W_{D_i} é o peso associado para cada dimensão;

$W_{P_{D_i}}$ é o valor ponderado de maturidade para a dimensão.

3.5.2.5 Cálculo do nível de maturidade da organização

O nível de maturidade da organização é o resultado da soma dos valores ponderados das dimensões e está definido na Equação (5).

$$\text{NMO} = \sum_{i=1}^{k} W_{P_{D_i}} \tag{5}$$

Onde:

k é o número total de dimensões;

$W_{P_{D_i}}$ é o valor ponderado de maturidade para a dimensão.

NMO é o nível de maturidade da organização.

Os valores calculados resultantes da aplicação das equações acima são apresentados na Tabela 3.

Tabela 3 - Cálculo do nível de maturidade

Dimensões	Conhecimento			Atitudes				Comportamento					Conscientização								Organizacional				
Perguntas	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25
Soma perg	402	418	408	421	238	479	457	383	308	410	266	423	435	513	438	407	441	358	208	279	414	390	395	456	348
Média perg	2,87	2,99	2,91	3,01	1,70	3,42	3,26	2,74	2,20	2,93	1,90	3,02	3,11	3,66	3,13	2,91	3,15	2,56	1,49	1,99	2,96	2,79	2,82	3,26	2,49
Soma dimen	1228			1595				1790					3079								2003				
Média dimen	409,33			398,75				358,00					384,88								400,60				
Max dimen	1680			2240				2800					4480								2800				
matur perg	71,79	74,64	72,86	75,18	42,50	85,54	81,61	68,39	55,00	73,21	47,50	75,54	77,68	91,61	78,21	72,68	78,75	63,93	37,14	49,82	73,93	69,64	70,54	81,43	62,14
matur dimen	73,10			71,21				63,93					68,73								71,54				
Nivel dimen	Aprimorado			Aprimorado				Aprimorado					Aprimorado								Aprimorado				
Dimen peso	13,08			13,46				19,95					11,20								11,23				

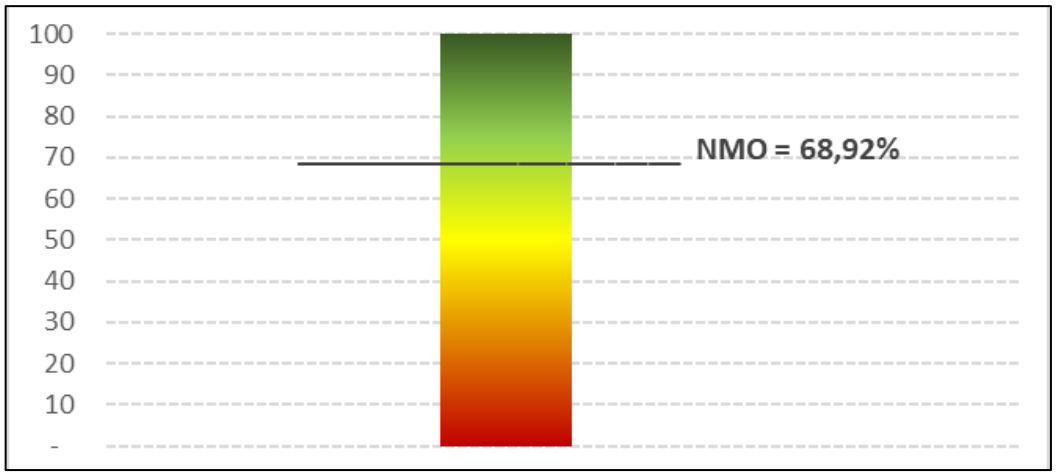
Fonte: Resultado da pesquisa (2024).

A Tabela 3, apresenta o resultado das etapas de cálculo de apuração do nível de maturidade da organização. As colunas indicam os valores calculados para cada dimensão segundo o MMCSC.

As respostas das perguntas foram somadas, agrupadas, calculadas as médias, apurados os valores de maturidade por dimensão, aplicados os pesos conforme indicados pelos especialistas e somados os valores para determinação do nível de maturidade da cultura de segurança cibernética.

O Gráfico 10, apresenta o NMO apurado para a organização com base no MMCSC.

Gráfico 10 - Nível de maturidade da organização



Fonte: Resultado da pesquisa (2024).

Conforme apresentado no Gráfico 10, o percentual apurado de 68,92% indica a classificação aprimorada de maturidade, enquadrando-se na faixa de valores maiores que 60% e menores ou iguais a 80%. Esta classificação, embora esteja no início do nível aprimorado, caracteriza-se por uma cultura de segurança cibernética com ações e processos implementados

e melhorias constantes. Neste nível, identifica-se o conhecimento sobre ameaças, medidas de proteção e diretrizes de segurança pelos funcionários, há uma consciência sobre a importância da segurança para suas funções e uma crença disseminada que a organização tem controles de segurança eficazes.

No que tange ao comportamento seguro, algumas práticas de segurança fazem parte do cotidiano dos indivíduos, há reportes eventuais sobre incidentes e contribuições esporádicas sobre melhorias na segurança.

O programa de conscientização é visto como adequado em termos de treinamentos, o apoio da alta direção é percebido por parte dos funcionários através do plano de ação e de alguns investimentos na cultura de segurança na organização.

4 DISCUSSÃO

A análise dos dados coletados pela *survey* e pelas entrevistas com especialistas permitiu uma radiografia sobre a maturidade da cultura de segurança cibernética na organização avaliada.

De maneira geral, os dados revelam que a visão entre estes dois grupos é divergente, sendo mais conservadora e menos otimista na opinião dos especialistas. Os respondentes da *survey*, entretanto, tem uma percepção bem mais positiva sobre vários aspectos da segurança na organização.

A seguir, são discutidas as principais implicações desses resultados com base nas dimensões do modelo de maturidade proposto.

4.1 Conhecimento

O nível de conhecimento dos funcionários sobre ameaças cibernéticas e diretrizes internas de segurança da organização está no nível básico, segundo os especialistas. Isto indica que os conhecimentos são parciais sobre ataques cibernéticos e há pouca familiaridade com as normas e processos de segurança da organização. As razões, segundo eles, residem na falta de interesse, dificuldade em manter-se atualizado e complexidade das normas de segurança.

A percepção obtida na coleta de dados realizada pela *survey* é mais otimista, pois indica que a organização está no nível aprimorado, o que representa um conhecimento abrangente sobre ameaças e um entendimento detalhado sobre diretrizes e processos de segurança da empresa.

A discrepância entre as duas visões pode residir no fato de os especialistas se depararem com incidentes de segurança, e terem uma noção mais aguçada sobre a complexidade dos ataques, bem como, em certa medida, lidarem com eventos de inobservância das diretrizes por parte de alguns funcionários ao longo do tempo, o que de certa forma influencia a sua percepção sobre o conhecimento do corpo funcional.

4.2 Atitudes

Sobre a dimensão das atitudes os especialistas entenderam que a organização está no nível intermediário indicando que a maioria das pessoas na organização reputa a segurança como importante e aplicam-na em suas atividades laborais. Os controles de segurança, entretanto, poderiam ser melhores e a segurança ainda não é vista como prioridade para toda a organização.

A *survey* apontou novamente uma visão mais positiva, no nível aprimorado, mostrando que os controles de segurança são eficazes, que a segurança é vista como prioridade em várias áreas, mas que existem processos em que ela precisa ser melhorada.

Por outro lado, quando questionados se outras demandas da empresa fazem com que a segurança seja relegada a segundo plano, mais da metade dos respondentes concordou que sim, o que de certa forma corresponde à visão dos especialistas no quesito prioridade da segurança para a organização.

Outros aspectos podem ter influência sobre estas divergências, já que, os desafios enfrentados pela área de segurança para disseminar a cultura e implementar os controles no âmbito corporativo não são percebidos pela maioria dos funcionários.

4.3 Comportamento

Em relação ao comportamento os especialistas entendem que o nível é básico, pois percebe-se comportamentos imprudentes e um certo descaso com as diretrizes de segurança, indicando que as práticas adotadas pelo corpo funcional não são consistentes, neste caso, o comportamento dos funcionários é adequado apenas quando solicitado e reativo diante dos incidentes de segurança.

Os respondentes da *survey* sinalizaram o comportamento no nível aprimorado, segundo o modelo de maturidade, destacando que a segurança integra o cotidiano das pessoas, com condutas proativas e reportes de incidentes. O contraponto nesta dimensão foi o fato de que quase a metade dos respondentes indicou que os funcionários seguem as diretrizes de segurança

apenas porque são obrigados ou por receio de serem punidos, esta percepção corresponde a dos especialistas em que o comportamento seguro é aderente apenas quando solicitado.

A dimensão do comportamento, embora classificada em níveis diferentes pelos especialistas e pelos respondentes da *survey*, é a dimensão com a menor nota em ambas as visões, este é um indicativo importante que a cultura de segurança na organização precisa evoluir, é possível que uma coleta de dados mais ampla entre os demais funcionários leve a uma percepção mais aproximada à visão dos especialistas.

4.4 Conscientização

A dimensão da conscientização foi classificada como intermediária pelos especialistas e ressaltou que os principais destaques positivos são as simulações de phishing e a plataforma de treinamento contratada. Contudo, alguns especialistas foram contundentes na avaliação do programa de conscientização indicando que ele está estagnado, não avalia o conhecimento sobre segurança dos funcionários e mesmo a plataforma de treinamento não atende às necessidades específicas e peculiares da organização.

Os respondentes da *survey* indicaram que a conscientização está no nível aprimorado, com o mesmo destaque positivo dos especialistas para as simulações de phishing e plataforma de treinamento com acréscimo positivo para os comunicados de segurança enviados aos funcionários.

A convergência entre as visões pode ser observada no quesito treinamento em segurança, porém, a percepção dos especialistas quanto aos desafios da conscientização é mais realista visto que, são eles os gestores deste processo na organização.

4.5 Organizacional

Para os especialistas, o envolvimento da alta gestão na dimensão organizacional do MMCSC é classificado no nível básico, com apoio mínimo e foco restrito ao cumprimento de

exigências dos órgãos de controle. Além disso, há pouco envolvimento público em eventos e fóruns de segurança, e as demonstrações de comportamento em segurança não são exemplares.

Os respondentes da *survey*, no entanto, entendem que a atuação da alta direção na promoção da cultura de segurança cibernética está no nível aprimorado, que o apoio existe, pois, a segurança está incluída no planejamento estratégico e que há investimentos em segurança. Contudo, pouco mais de um terço dos respondentes da *survey* discordaram desta opinião ou se mantiveram neutros neste quesito, o que sugere ainda, um obstáculo por parte dos funcionários de perceber tal apoio estratégico.

CONCLUSÃO

Este trabalho teve como premissa avaliar a cultura de segurança cibernética em uma organização pública com base em um modelo de maturidade.

Ao investigar a literatura e as referências da indústria constatou-se que existem poucos modelos de maturidade específicos da cultura de segurança cibernética. Verificou-se que alguns aspectos da cultura de segurança e da conscientização não foram contemplados de forma ampla. Diante destas lacunas, esta pesquisa propôs a elaboração de um novo modelo de maturidade de cinco níveis e cinco dimensões.

A construção deste artefato fundamentou-se na revisão da literatura, baseou-se nos princípios da cultura de segurança cibernética, em modelos de maturidade encontrados e nos elementos positivos da cultura de segurança.

Foram aplicadas técnicas de pesquisa para analisar o nível de maturidade de uma organização pública sob duas óticas, a dos especialistas em segurança com entrevistas semiestruturadas e sob a ótica dos demais funcionários com a *survey*.

Os resultados indicaram que a dimensão do comportamento tem a maior a influência na determinação do nível de maturidade. A dimensão do conhecimento teve como destaque positivo a plataforma de treinamento contratada, mas ressaltou-se a sua falta de adaptabilidade frente às necessidades específicas de segurança da organização.

As normas internas de segurança foram reputadas como complexas, pouco divulgadas e necessitam de adaptações na linguagem para se tornarem mais atrativas aos funcionários. A percepção sobre a importância da segurança entre os funcionários é majoritariamente alta, porém, a visão deles é distorcida, acreditam estar totalmente protegidos quando conectados na rede interna da empresa, levando-os a ter um comportamento displicente, relaxando nas práticas de segurança, imaginando que nada de mal lhes acontecerá. Ainda em relação ao comportamento seguro percebem-se condutas impróprias básicas, como, por exemplo, deixar a estação de trabalho desbloqueada.

Considera-se que o programa de conscientização apresentou avanços, porém atualmente está estagnado e não aborda as necessidades emergentes de segurança da empresa. O envolvimento da alta direção na promoção da cultura de segurança foi avaliado como mínimo e se restringe ao cumprimento de obrigações legais.

Sobre o nível de maturidade, a visão dos especialistas foi mais conservadora e foi classificada como intermediária. Este nível indica que há consistência nas práticas de conscientização e uma estrutura definida na organização para desenvolver a cultura de segurança.

A percepção dos demais funcionários, no entanto, foi mais otimista pois entenderam que o nível de maturidade é aprimorado, indicando que há ações e processos mais desenvolvidos e melhorias constantes.

A divergência entre as visões não se constitui num problema para a organização, pelo contrário, traz ganhos, pois permite observar a cultura de segurança sob dois ângulos diferentes, aproveitando a experiência dos especialistas em segurança que são responsáveis pelos processos de gestão de segurança, e lidam com os desafios diários para aprimorar a conscientização, e a visão dos demais funcionários, que são os clientes destes processos, e podem fornecer *insights* valiosos para detectar as lacunas e possíveis melhorias na cultura de segurança.

Acredita-se que a contribuição desta pesquisa foi substancial pois estabeleceu a metodologia de cálculo do nível de maturidade da organização propiciando um indicador valioso para mensurar o estágio atual de maturidade da cultura de segurança, além de fornecer um roteiro bem definido para melhorias futuras.

O modelo proposto nesta pesquisa é de natureza aberta, flexível e escalável, permitindo ajustes e adaptações conforme as características de cada organização. A pesquisa apresentou os passos de como o modelo foi construído e as bases adotadas para isso. Os instrumentos de coleta para aferir o nível de maturidade da organização estão lastreados nas dimensões e nos requisitos de cada nível do modelo e permitem a identificação clara de qual aspecto da cultura de segurança cibernética está sendo avaliado.

Em termos de abrangência, o modelo proposto é inovador pois, além de considerar os temas tradicionais do conhecimento em segurança, treinamento e programa de conscientização, aborda atributos comportamentais, como as percepções e ações dos funcionários e os aspectos corporativos da gestão e governança relacionados diretamente com a cultura de segurança cibernética.

No que tange ao aprimoramento da maturidade que o modelo propõe para as organizações, as diretivas estão em consonância com o que é sugerido por outros modelos de

maturidade de referência, pelas recomendações e estudos de especialistas na área e pelas melhores práticas aplicadas na indústria.

Os órgãos da administração pública, em sua ampla maioria, são dependentes dos recursos de tecnologia da informação, que são operados por pessoas da entidade. Para que os dados e sistemas sejam protegidos contra as ameaças virtuais e erros não intencionais, a conscientização precisa ser realizada sob diversas formas para que haja o desenvolvimento da cultura de segurança cibernética.

Entretanto, não foi possível encontrar instrumentos normativos, frameworks ou modelos de maturidade no setor público que avaliassem especificamente a cultura de segurança cibernética de forma ampla e que orientassem o seu aprimoramento. Este modelo tem a sua relevância destacada ao suprir esta lacuna e contribuir para o avanço da cibersegurança na esfera governamental.

As limitações desta pesquisa residem na baixa amostragem comparada à quantidade de funcionários da organização e na forma de obtenção dos dados que foi fundamentalmente baseada no autorrelato.

Para estudos futuros, sugere-se investigar a possibilidade de utilizar sensores para a coleta de dados relativos à cultura de segurança cibernética de forma a automatizar e aprimorar os modelos de maturidade.

REFERÊNCIAS

AKSOY, Cenk. **Building a cyber security culture for resilient organizations against cyber attacks**. *Building a cyber security culture for resilient organizations against cyber attacks*, [S. l.], v. 7, n. 1, p. 96–110, 2024.

AL-DARWISH, Ahmed I.; CHOE, Pilsung. **A Framework of Information Security Integrated with Human Factors**. In: MOALLEM, Abbas (org.). *A Framework of Information Security Integrated with Human Factors*. Cham: Springer International Publishing, 2019. (Lecture Notes in Computer Science, v. 11594). p. 217–229. Disponível em: https://link.springer.com/10.1007/978-3-030-22351-9_15. Acesso em: 4 jul. 2024.

ALMEIDA, Daniela et al. **Conscientização em Segurança Cibernética: Estudo baseado na percepção de trabalhadores de uma organização pública federal brasileira**. *Revista Ibérica de Sistemas e Tecnologias de Informação*, [S. l.], n. E65, p. 661–673, 2024.

ALSHAIKH, Moneer et al. **An exploratory study of current information security training and awareness practices in organizations**. *An exploratory study of current information security training and awareness practices in organizations*, [S. l.], 2018. Disponível em: https://aisel.aisnet.org/hicss-51/os/practice-based_research/4/. Acesso em: 17 out. 2024.

ALSHAIKH, Moneer; ADAMSON, Blair. **From awareness to influence: toward a model for improving employees' security behaviour**. *From awareness to influence: toward a model for improving employees' security behaviour*, [S. l.], v. 25, n. 5, p. 829–841, 2021.

ALSHAMMARI, Mohammad Mulayh; DEMETIS, S. D. **House of Card: developing KPIs for monitoring cybersecurity awareness (CSA)**. *Journal of Information Systems Security*, [S. l.], v. 19, n. 2, p. 1–15, 2023.

ANILKUMAR, Anagha; DIMITROV, Filip; NARAYANAN, Anup. **Awareness, Behavior & Cyber Security Culture Differences**. [S. l.: s. n.], 2023. Disponível em: https://securityquotient.io/the-differences-and-relationship-between-awareness-behavior-and-culture-in-cyber-security/. Acesso em: 5 maio 2024.

ANILKUMAR, Anagha; DIMITROV, Filip; NARAYANAN, Anup. **Key Benchmarks for Cyber Security Culture Assessments**. [S. l.: s. n.], 2024a. Disponível em: https://securityquotient.io/assessing-the-state-of-your-cyber-security-culture-key-benchmarks/. Acesso em: 5 maio 2024.

ANILKUMAR, Anagha; DIMITROV, Filip; NARAYANAN, Anup. **Key Metrics and KPIs for Cyber Security Behavior and Culture**. [S. l.: s. n.], 2024b. Disponível em: https://securityquotient.io/key-metrics-and-performance-indicators-kpis-for-cyber-security-behavior-and-culture/. Acesso em: 5 maio 2024.

AZAMBUJA, Antônio João; NETO, João Souza. **Modelo de maturidade de segurança cibernética para os órgãos da administração pública federal**. *Revista do Serviço Público*, [S. l.], v. 71, n. 3, p. 660–712, 2020.

BABBIE, Earl. **Métodos de Pesquisa de Survey**. 1. ed. Belo Horizonte: Editora UFMG,

1999.

BARDIN, Laurence. **Análise de Conteúdo**. Tradução: Luís Antero Reto; Augusto Pinheiro. Lisboa: Edições 70, 1977.

BAXTER, Leslie A.; BABBIE, Earl R. **The basics of communication research**. Boston: Cengage Learning, 2004.

BECKER, Jörg; KNACKSTEDT, Ralf; PÖPPELBUSS, Jens. **Developing Maturity Models for IT Management**. *Business & Information Systems Engineering*, [S. l.], v. 1, n. 3, p. 213–222, 2009.

BRASIL. Presidência da República. **Estratégia Nacional de Segurança Cibernética**. [S. l.], 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 1 mar. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços. **Guia de Implementação do Framework de Política de Segurança da Informação**. [S. l.: s. n.], 2024. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf.

BRASIL. Presidência da República. **Política Nacional de Segurança da Informação**. [S. l.], 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10641.htm. Acesso em: 1 mar. 2025.

BRASIL. Gabinete de Segurança Institucional. **Revisão da Capacidade de Segurança Cibernética: Relatório de Revisão do Cybersecurity Capacity Maturity Model for Nations (CMM) Brasil**. Brasília: GSI/PR, 2023. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber/cmm-report-brazil-2023_final_pt.pdf. Acesso em: 1 mar. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Revisão da Estratégia de Governança Digital 2016-2019**. [S. l.: s. n.], 2018. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/revisaodaestrategiadegovernancadigital20162019.pdf.

CARPENTER, Perry. **5 security culture maturity indicators every organization must know**. [S. l.: s. n.], 2022. Disponível em: https://www.securityinfowatch.com/cybersecurity/article/21262310/5-security-culture-maturity-indicators-every-organization-must-know. Acesso em: 5 maio 2024.

CHAKRABORTY, Santonab et al. **A comprehensive and systematic review of multi-criteria decision-making methods and applications in healthcare**. *Healthcare Analytics*, [S. l.], p. 100232, 2023.

COOPER, Donald R.; SCHINDLER, Pamela S. **Métodos de pesquisa em administração**. 12. ed. [S. l.]: McGraw Hill Brasil, 2016.

CORRADINI, Isabella. **Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology**. Cham: Springer International Publishing, 2020. (Studies in Systems, Decision and Control, v. 284). Disponível em: http://link.springer.com/10.1007/978-3-030-43999-6. Acesso em: 3 out. 2024.

DA VEIGA, Adéle et al. **Defining organisational information security culture—Perspectives from academia and industry**. *Computers & Security*, [S. l.], v. 92, p. 101713, 2020.

DA VEIGA, A.; ELOFF, J. H. P. **A framework and assessment instrument for information security culture**. *Computers & Security*, [S. l.], v. 29, n. 2, p. 196–207, 2010.

DA VEIGA, Adéle; MARTINS, Nico. **Improving the information security culture through monitoring and implementation actions illustrated through a case study**. *Computers & Security*, [S. l.], v. 49, p. 162–176, 2015.

DA VEIGA, Adele; MARTINS, Nico; ELOFF, Jan H. P. **Information security culture-validation of an assessment instrument**. *Southern African Business Review*, [S. l.], v. 11, n. 1, p. 147–166, 2007.

DIESCH, Rainer; PFAFF, Matthias; KRCMAR, Helmut. **A comprehensive model of information security factors for decision-makers**. *Computers & Security*, [S. l.], v. 92, p. 101747, 2020.

ENISA. European Union Agency for Network and Information. **Cyber security culture in organisations**. LU: Publications Office, 2017. Disponível em: https://data.europa.eu/doi/10.2824/10543. Acesso em: 19 maio 2024.

FOWLER, Floyd J. **Survey Research Methods**. 5. ed. Thousand Oaks, CA: SAGE Publications, 2014.

GARFIELD, Eugene. **Citation Indexes for Science: A New Dimension in Documentation through Association of Ideas**. *Science*, [S. l.], v. 122, n. 3159, p. 108–111, 1955.

GEORG, Marcus Aurélio Carvalho et al. **Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação**. [S. l.: s. n.], 2023. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Os-desafios-da-Seguranca-Cibernetica-no-setor-publico-federal-do-Brasil-estudo-sob-a-otica-de-gestores-de-tecnologia-da-informacao.pdf. Acesso em: 1 mar. 2025.

GEORGIADOU, Anna et al. **A Cyber-Security Culture Framework for Assessing Organization Readiness**. *Journal of Computer Information Systems*, [S. l.], v. 62, n. 3, p. 452–462, 2022.

GOEPEL, Klaus D. **Implementation of an Online Software Tool for the Analytic Hierarchy Process (AHP-OS)**. *International Journal of the Analytic Hierarchy Process*, [S. l.], v. 10, n. 3, 2018. Disponível em: https://ijahp.org/index.php/IJAHP/article/view/590. Acesso em: 2 set. 2024.

GOOGLE. **Google Forms**. [S. l.: s. n.], 2024.

GUNDU, Tapiwa. **Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance**. In: ICCWS 2019 14th International Conference on Cyber Warfare and Security. [S. l.: s. n.], 2019. p. 94–102. Disponível em: https://books.google.com/books?hl=pt-BR&lr=&id=UfedDwAAQBAJ&oi=fnd&pg=PA94&dq=GUNDU,+T.+Acknowledging+and+Reducing+the+Knowing+and+Doing+gap+in+Employee+Cybersecurity+Compliance&ots=

C_BFeEsNa9&sig=rByWVaROompgg5HFDQTo516n_iY. Acesso em: 8 set. 2024.

GUNDU, Tapiwa. **Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture Model**. In: International Conference on Cyber Warfare and Security. [S. l.: s. n.], 2024. p. 95–102. Disponível em: https://papers.academic-conferences.org/index.php/iccws/article/view/2177. Acesso em: 3 out. 2024.

HEVNER, Alan R. et al. **Design science in information systems research**. *MIS Quarterly*, [S. l.], p. 75–105, 2004.

ISACA. CMMI Institute. **Capability Maturity Model Integration (CMMI) - Security**. [S. l.]: ISACA, 2023. Disponível em: https://cmmiinstitute.com/cmmi/sec#:~:text=CMMI%20Security%20is%20an%20integrated,and%20retain%20the%20best%20talent. Acesso em: 12 mar. 2025.

ITU. International Telecommunication Union. **X.1054 : Information security, cybersecurity and privacy protection - Governance of information security**. [S. l.], 2021. Disponível em: https://www.itu.int/rec/T-REC-X.1054-202104-I. Acesso em: 11 mar. 2025.

JOHANSSON, Kevin et al. **Improving Cybersecurity Awareness Among SMEs in the Manufacturing Industry**. In: NG, Amos H. C. et al. (org.). *Advances in Transdisciplinary Engineering*. [S. l.]: IOS Press, 2022. Disponível em: https://ebooks.iospress.nl/doi/10.3233/ATDE220140. Acesso em: 17 out. 2024.

KESSLER, Stacey R. et al. **Information security climate and the assessment of information security risk among healthcare employees**. *Health Informatics Journal*, [S. l.], v. 26, n. 1, p. 461–473, 2020.

KHADER, Mohammed; KARAM, Marcel; FARES, Hanna. **Cybersecurity Awareness Framework for Academia**. *Information*, [S. l.], v. 12, n. 10, p. 417, 2021.

KHANDO, Khando et al. **Enhancing employees information security awareness in private and public organisations: A systematic literature review**. *Computers & Security*, [S. l.], v. 106, p. 102267, 2021.

KNOWBE4. **Security Culture Maturity Model | KnowBe4**. [S. l.], 2022. Disponível em: https://www.knowbe4.com/security-culture-maturity-model. Acesso em: 26 maio 2024.

KŐ, Andrea; TARJÁN, Gábor; MITEV, Ariel. **Information security awareness maturity: conceptual and practical aspects in Hungarian organizations**. *Information Technology & People*, [S. l.], v. 36, n. 8, p. 174–195, 2023.

KRUGER, H. A.; KEARNEY, W. D. **A prototype for assessing information security awareness**. *Computers & Security*, [S. l.], v. 25, n. 4, p. 289–296, 2006.

LACERDA, Daniel Pacheco et al. **Design Science Research: A research method to production engineering**. *Gestão & Produção*, [S. l.], v. 20, p. 741–761, 2013.

LE, Ngoc T.; HOANG, Doan B. **Can maturity models support cyber security?**. In: 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC). [S. l.: s. n.], 2016. p. 1–7. Disponível em: https://ieeexplore.ieee.org/abstract/document/7820663. Acesso em: 8 jul. 2024.

LIE, Laksana Budiwiyono; UTOMO, Prio; WINARNO, P. M. **Investigating the Impact of Cybersecurity Culture on Employees' Cybersecurity Protection Behaviours: A Conceptual Paper**. *Conference Series*, [S. l.], v. 3, n. 2, p. 295–305, 2021.

MALHOTRA, Naresh K. **Marketing research: an applied orientation**. Upper Saddle River: Pearson Education, 2010.

MICROSOFT. **Microsoft Teams**. [S. l.: s. n.], 2024.

MIRANDA, Isabell Carolina Zorzi de et al. **Avaliação da Conformidade de Empresas à LGPD: Uma Pesquisa com Profissionais de Tecnologia da Informação**. *Revista H-TEC Humanidades e Tecnologia*, [S. l.], v. 9, n. Especial, p. 68–90, 2024.

MURONGA, Khangwelo et al. **An Analysis of Assessment Approaches and Maturity Scales used for Evaluation of Information Security and Cybersecurity User Awareness and Training Programs: A Scoping Review**. In: 2019 Conference on Next Generation Computing Applications (NextComp). Mauritius: IEEE, 2019. p. 1–6. Disponível em: https://ieeexplore.ieee.org/document/8883535/. Acesso em: 12 maio 2024.

NCSC. UK National Cyber Security Centre. **Developing a positive cyber security culture**. [S. l.: s. n.], 2023. Disponível em: https://www.ncsc.gov.uk/collection/board-toolkit/developing-a-positive-cyber-security-culture. Acesso em: 5 maio 2024.

NEMOTO, Tomoko; BEGLAR, David. **Likert-scale questionnaires**. In: JALT 2013 Conference Proceedings. [S. l.: s. n.], 2014. p. 1–6. Disponível em: https://jalt-publications.org/sites/default/files/pdf-article/jalt2013_001.pdf. Acesso em: 18 out. 2024.

NIST. National Institute of Standards and Technology. **Glossary of Key Information Security Terms**. [S. l.], 2013.

PAGE, Matthew J. et al. **The PRISMA 2020 statement: an updated guideline for reporting systematic reviews**. *Systematic Reviews*, [S. l.], v. 10, n. 1, p. 89, 2021. Disponível em: https://doi.org/10.1186/s13643-021-01626-4.

PARSONS, Kathryn et al. **Human factors and information security: individual, culture and security environment**. [S. l.: s. n.], 2010. Disponível em: https://apps.dtic.mil/sti/citations/ADA535944. Acesso em: 4 set. 2024.

PATTON, Michael Quinn. **Qualitative research & evaluation methods: Integrating theory and practice**. [S. l.]: Sage Publications, 2014. Disponível em: https://books.google.com/books?hl=pt-BR&lr=&id=ovAkBQAAQBAJ&oi=fnd&pg=PP1&dq=Michael+Q.+Patton:+%22Qualitative+Research+%26+Evaluation+Methods&ots=ZSY_6ptAB1&sig=I-LCu29QXUpQU3qsDjmHdO_KxmA. Acesso em: 16 set. 2024.

PEFFERS, Ken et al. **A Design Science Research Methodology for Information Systems Research**. *Journal of Management Information Systems*, [S. l.], v. 24, n. 3, p. 45–77, 2007.

PINSONNEAULT, Alain; KRAEMER, Kenneth. **Survey Research Methodology in Management Information Systems: An Assessment**. *Journal of Management Information Systems*, [S. l.], v. 10, n. 2, p. 75–105, 1993.

PRAKASH, Mridula; PEARLSON, Keri. **Cybersecurity Culture Maturity Model**. [S. l.]: Cybersecurity at MIT Sloan, 2024.

RAMOS, Marcelo; ARIMA, Carlos Hideo. **Conscientização em Segurança da Informação na Indústria 4.0**. In: ENCONTRO NACIONAL DE ENGENHARIA DE PRODUÇÃO (ENEGEP 2023). Fortaleza, CE: Associação Brasileira de Engenharia de Produção, 2023.

REEGÅRD, Kine; BLACKETT, Claire; KATTA, Vikash. **The Concept of Cybersecurity Culture**. In: Proceedings of the 29th European Safety and Reliability Conference (ESREL). [S. l.]: Research Publishing Services, 2019. p. 4036–4043. Disponível em: http://rpsonline.com.sg/proceedings/9789811127243/html/0761.xml. Acesso em: 3 jul. 2024.

RUIGHAVER, A. B.; MAYNARD, S. B.; CHANG, S. **Organisational security culture: Extending the end-user perspective**. *Computers & Security*, [S. l.], v. 26, n. 1, p. 56–62, 2007.

SAATY, Thomas L. **How to make a decision: the analytic hierarchy process**. *European Journal of Operational Research*, [S. l.], v. 48, n. 1, p. 9–26, 1990.

SCHEIN, Edgar H. **Organizational culture**. [S. l.]: American Psychological Association, 1990. v. 45.

SHAW, R. S. et al. **The impact of information richness on information security awareness training effectiveness**. *Computers & Education*, [S. l.], v. 52, n. 1, p. 92–100, 2009.

SILVA, Cíntia Peixoto da et al. **Métodos Multicritérios para Auxiliar no Processo de Tomada de Decisão na Indústria 4.0: Uma Revisão da Literatura**. *Revista H-TEC Humanidades e Tecnologia*, [S. l.], v. 9, n. Especial, p. 119–133, 2024.

SIPONEN, Mikko T. **A conceptual foundation for organizational information security awareness**. *Information Management & Computer Security*, [S. l.], v. 8, n. 1, p. 31–41, 2000.

SOLMS, Rossouw von; NIEKERK, Johan van. **From information security to cyber security**. *Computers & Security*, [S. l.], v. 38, p. 97–102, 2013.

SPITZNER, Lance. **SANS - Security Awareness Maturity Model**. [S. l.], 2019. Disponível em: https://www.sans.org/blog/security-awareness-maturity-model/. Acesso em: 25 maio 2024.

TCU. Tribunal de Contas da União. **Gestão de Riscos–Avaliação de Maturidade**. Brasília: TCU, 2018.

TCU. Tribunal de Contas da União. **Lista de Alto Risco da Administração Pública Federal 2024**. Brasília: Tribunal de Contas da União, 2024. Disponível em: https://portal.tcu.gov.br/data/files/55/C0/B5/DD/2B293910FDB48339E18818A8/Lista%20de%20Alto%20Risco%20da%20Administracao%20Publica%20Federal%202024.pdf. Acesso em: 1 mar. 2025.

UCHENDU, Betsy et al. **Developing a cyber security culture: Current practices and future needs**. *Computers & Security*, [S. l.], v. 109, p. 102387, 2021.

U.S. DOE. **Cybersecurity Capability Maturity Model (C2M2)**. [S. l.], 2022. Disponível em: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2. Acesso em: 9 jul. 2024.

VERIZON. **Data Breach Investigations Report 2024**. [S. l.], 2024. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: 19 maio 2024.

VILLAVERDE, Adão et al. **Fundamentos teóricos e metodológicos da pesquisa em educação em ciências**. [S. l.]: Editora Bagai, 2021. Disponível em: https://books.google.com/books?hl=pt-BR&lr=&id=4dcWEAAAQBAJ&oi=fnd&pg=PA4&ots=fzlzMHGHpM&sig=XKbS8QarodSaz_gJm9K5O9Y4orw. Acesso em: 16 set. 2024.

VON SOLMS, R. **Information security management (3): The Code of Practice for Information Security Management (BS 7799)**. *Information Management and Computer Security*, [S. l.], v. 6, n. 5, p. 224–225, 1998.

WENDLER, Roy. **The maturity of maturity model research: A systematic mapping study**. *Information and Software Technology*, [S. l.], v. 54, n. 12, p. 1317–1339, 2012.

WILSON, Mark et al. **Information technology security training requirements: a role- and performance-based model**. Gaithersburg, MD: National Institute of Standards and Technology, 1998. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf. Acesso em: 29 jun. 2024.

WILSON, M.; HASH, J. **Building an Information Technology Security Awareness and Training Program**. Gaithersburg, MD: National Institute of Standards and Technology, 2003. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf. Acesso em: 29 jun. 2024.

WOOD, Andy. **Developing a Security Culture Maturity Model (SCMM)**. [S. l.], 2024. Disponível em: https://buildasecurityculture.com/wp-content/uploads/2024/06/developing-a-maturity-model-for-security-culture.pdf. Acesso em: 16 ago. 2024.

YAOKUMAH, Winfred; WALKER, Daniel Okyere; KUMAH, Peace. **SETA and security behavior: Mediating role of employee relations, monitoring, and accountability**. *Journal of Global Information Management (JGIM)*, [S. l.], v. 27, n. 2, p. 102–121, 2019.

ZHEN, Jie et al. **Factors Influencing Employees' Information Security Awareness in the Telework Environment**. *Electronics*, [S. l.], v. 11, n. 21, p. 3458, 2022.

APÊNDICE A – MODELO DE MATURIDADE DA CULTURA DE SEGURANÇA CIBERNÉTICA (MMCSC)

Nível	Conhecimento (O que as pessoas da organização sabem sobre segurança)	Atitudes (O que as pessoas pensam e sentem sobre os protocolos e questões de segurança)	Comportamento (Como as pessoas agem diante das ameaças de segurança e como usam os recursos de TI)	Conscientização (O que é feito para desenvolver a cultura de segurança. Treinamento, campanhas etc.)	Organizacional (O apoio, liderança e envolvimento da alta direção na cultura de segurança cibernética)
Inicial Pouca maturidade, atividades de segurança informais ou inexistentes	Conhecimento superficial ou incipiente sobre ameaças, ataques cibernéticos, medidas de proteção, diretrizes, normas e processos de segurança cibernética da organização.	As pessoas demonstram pouca ou nenhuma preocupação com questões de segurança. A maioria não vê a segurança como relevante para suas funções e acreditam que a responsabilidade pela segurança é da equipe de TI ou equipe de segurança.	As pessoas frequentemente adotam comportamentos inseguros, poucos seguem as boas práticas de segurança e não há iniciativas proativas para proteger a organização contra ameaças.	Não há um programa de conscientização formalizado. Os comunicados de segurança são esporádicos. Os treinamentos e campanhas de conscientização são inexistentes ou limitados.	A alta direção tem pouco ou nenhum envolvimento nas questões de segurança cibernética. A segura é vista como responsabilidade de uma área específica. Não há discussões regulares sobre o tema entre os líderes organizacionais. O apoio financeiro para a segurança cibernética é mínimo e restrito a iniciativas corretivas após incidentes.
Básico Processos iniciais em desenvolvimento com esforço mínimo	Conhecimento básico ou parcial sobre ameaças e ataques cibernéticos; noções elementares sobre medidas de proteção e familiaridade com algumas diretrizes, normas e processos de segurança cibernética da organização	Os indivíduos começam a reconhecer a importância da segurança, mas a veem como secundária ou relacionada apenas a certos departamentos. Admitem que a segurança é necessária, mas acreditam que os controles existentes são limitados e insuficientes para proteger a organização adequadamente.	As pessoas seguem algumas práticas básicas de segurança, como o uso de senhas fortes ou o bloqueio de dispositivos quando não estão em uso, mas ainda não são consistentes. O comportamento seguro é reativo, e a maioria só adere às diretrizes quando solicitada ou em resposta a incidentes.	Treinamentos básicos voltados para a conformidade regulamentar ou para a política de SI. Campanhas de conscientização esporádicas. Comunicados de segurança enviados após incidentes, mas sem frequência regular.	Suporte mínimo da alta direção; discussões sobre segurança são raras. Apoio da alta direção em eventos pontuais. Segurança como parte da estratégia da organização. A alta direção começa a demonstrar um interesse pela cultura de segurança, mas com envolvimento ainda limitado. Existem discussões ocasionais sobre a necessidade de políticas de segurança motivadas por exigências regulatórias ou auditorias. O apoio financeiro é esporádico e para a compra de ferramentas de segurança. A segurança começa a ser reconhecida como importante, mas ainda não é parte essencial da estratégia.
Intermediário Estrutura mais definida, com maior consistência nas práticas	Conhecimento moderado sobre ameaças e ataques cibernéticos; entendimento das principais medidas de proteção e ciente das diretrizes, normas e processos de segurança cibernética da organização.	A maioria dos indivíduos vê a importância da segurança para suas atividades e passam a integrá-la no seu trabalho diário, mas alegam que os controles de segurança poderiam ser mais robustos para suas funções. A segurança ainda não é considerada uma prioridade em todas as situações.	As pessoas demonstram um comportamento mais consciente, regular e seguem as diretrizes de segurança. O comportamento seguro é baseado no risco iminente e o reporte de incidentes é esporádico e limitado.	Programa de conscientização estruturado com treinamentos regulares e obrigatórios para todos na organização. Comunicados abordam diretrizes de segurança, ameaças e melhores práticas. As campanhas de conscientização são esporádicas com temas gerais de segurança.	A alta direção tem envolvimento mais ativo nas discussões de segurança. As políticas são discutidas em nível estratégico, comunicados internos sobre importância da segurança começam a ser divulgados. Há alocação de recursos financeiros para o programa de conscientização. A segurança começa a ser mencionada nas estratégias organizacionais, mas ainda não é plenamente integrada.

APÊNDICE A – MODELO DE MATURIDADE DE CULTURA DE SEGURANÇA CIBERNÉTICA (MMCSC) - continuação

Aprimorado Implementação avançada com envolvimento contínuo e melhorias constantes	Conhecimento abrangente sobre ameaças, ataques cibernéticos, medidas de proteção e entendimento detalhado sobre as diretrizes, normas e processos de segurança cibernética da organização.	As pessoas estão amplamente conscientes sobre a importância da segurança para suas funções e acreditam que a organização tem controles de segurança eficazes. A segurança é vista como uma prioridade em várias áreas, mas entendem que há oportunidades de melhorias em certos processos.	O comportamento seguro é parte do cotidiano das pessoas, procuram antecipar e mitigar os riscos proativamente. O reporte de incidentes e possíveis vulnerabilidades é mais frequente. Sugestões de melhorias para os processos de segurança começam a ser compartilhadas.	Programa de conscientização estruturado. Treinamento obrigatório, com avaliação para todos na organização, disponível a qualquer momento. As campanhas de conscientização são envolventes e criativas, porém esporádicas. Comunicados de segurança são enviados de forma periódica, cobrem temas atuais e importantes para a organização. Testes eventuais sobre conteúdo de segurança. Equipe com dedicação parcial de tempo para o programa de conscientização. Simulações de *phishing* são eventuais.	A alta direção lidera a cultura de segurança cibernética, participando em discussões estratégicas e comunicando aos funcionários a importância da segurança. Há um aumento no investimento financeiro e orçamento dedicado à cultura de segurança. A segurança é vista como uma prioridade organizacional. A alta direção participa de eventos públicos promovendo a segurança cibernética como um valor organizacional.
Avançado Cultura madura com processos sustentáveis, integrados e monitorados	Conhecimento avançado sobre ameaças recentes, vulnerabilidades emergentes e tendências de ataques globais. As diretrizes, normas e processos de segurança são de pleno conhecimento e recebem contribuições de melhoria.	A segurança é vista como essencial em todas as atividades diárias e cada indivíduo entende que é responsável por mantê-la e aprimorá-la. As pessoas creem que a organização possui infraestrutura e controles de segurança robustos e adequados para lidar com ameaças cibernéticas e que ela é uma prioridade em todas as decisões estratégicas.	As pessoas são engajadas nas questões de segurança. Agem com cautela e atenção diante de ameaças, antecipam os riscos, incorporam as diretrizes e melhores práticas de segurança em suas rotinas e colaboram com a equipe de segurança. Propõem melhorias para os processos de segurança e trabalham em conjunto com a organização para fortalecer a cultura de segurança.	Programa de conscientização estabelecido e atualizado anualmente. Treinamento contínuo, personalizado para funções e áreas conforme necessidades específicas, conteúdo atualizado anualmente no mínimo, obrigatório e com avaliação para todos na organização. Campanhas frequentes, criativas e envolventes. Comunicados de segurança periódicos abordando temas recorrentes importantes, novas ameaças, diretrizes de segurança e medidas de proteção. Simulações de *phishing* e testes sobre temas de segurança. Equipe dedicada exclusivamente para o programa de conscientização. Programa de recompensas para reforçar o comportamento seguro. Agentes promotores da segurança na organização (*security champions*)	A alta direção avalia e orienta os processos de gerenciamento da segurança considerando o cenário de ameaças e metas estratégicas da organização. Os líderes executivos participam de fóruns internos e externos sobre segurança. Os comunicados da alta direção reforçam a importância e estimulam a inovação em segurança com o uso de novas tecnologias e abordagens. O investimento financeiro é estratégico, contínuo e de longo prazo. A segurança é essencial nas decisões estratégicas de todas as áreas, operações, produtos e serviços da organização.

APÊNDICE B – QUESTIONÁRIO DA SURVEY

Faixa etária	Sexo	Nível de escolaridade	Cargo	Tempo de experiência na área	Área de atuação na empresa	Experiência com conscientização / cultura de segurança cibernética?
• Menos de 18 anos • 18 a 24 anos • 25 a 34 anos • 35 a 44 anos • 45 a 54 anos • 55 a 64 anos • 65 ou mais • Prefiro não informar	• Masculino • Feminino • Outro • Prefiro não informar	• Sem escolaridade • Ensino fundamental incompleto • Ensino fundamental completo • Ensino médio incompleto • Ensino médio completo • Curso técnico ou profissionalizante • Graduação incompleta • Graduação completa • Pós-graduação (Especialização) • Mestrado • Doutorado • Prefiro não informar	• Estagiário • Assistente • Analista • Líder • Gerente • Coordenador(a) • Assessor(a) • Superintendente • Diretor(a) • Outro: • Prefiro não informar	• Menos de 1 ano • 1 a 2 anos • 3 a 5 anos • 6 a 10 anos • Mais de 10 anos • Prefiro não informar	• Segurança da informação • Técnica infraestrutura • Técnica suporte • Técnica desenvolvimento • Recursos humanos • Administrativa • Financeira • Marketing • Jurídica • Negócios/cliente • Gestão/governança • Auditoria/Corregedoria • Outra: • Prefiro não informar	• Muito experiente • Experiente • Pouco experiente • Nenhuma experiência • Prefiro não informar

Dimensão do conhecimento		
ID	**Questão**	**Referência**
P1	As pessoas da empresa têm conhecimento sobre ameaças recentes, vulnerabilidades emergentes e tendências de ataques globais.	(Khando *et al.*, 2021) Anilkumar *et al.* (2024b)
P2	As diretrizes, normas e processos de segurança cibernética são de pleno conhecimento das pessoas na empresa.	(Zhen *et al.*, 2022) (Kő; Tarján; Mitev, 2023)
P3	As pessoas sabem como executar suas atividades de forma segura.	Anilkumar *et al.* (2024a)

APÊNDICE B – QUESTIONÁRIO DA SURVEY - CONTINUAÇÃO

Dimensão das atitudes		
ID	**Questão**	**Referência**
P4	A segurança é vista pelas pessoas como essencial em todas as atividades diárias e cada indivíduo entende que é responsável por mantê-la e aprimorá-la.	(Da Veiga; Martins, 2015) (Georgiadou *et al.*, 2022)
P5	A urgência para cumprir prazos, satisfazer clientes ou colocar sistemas em funcionamento faz com que a segurança seja relegada a segundo plano.	(Zhen *et al.*, 2022) Al-Darwish e Choe (2019) e Parsons *et al.* (2010)
P6	A empresa possui uma infraestrutura e controles de segurança robustos e adequados para lidar com ameaças cibernéticas.	(Georgiadou *et al.*, 2022; Zhen *et al.*, 2022)
P7	A segurança cibernética é uma prioridade nas decisões estratégicas da organização.	Kesseler et al. (2020) Al-Darwish e Choe (2019)

Dimensão do comportamento		
ID	**Questão**	**Referência**
P8	As pessoas se comportam de forma segura, agem com cautela e atenção diante de ameaças, antecipam os riscos, seguem as diretrizes e melhores práticas de segurança em suas rotinas diárias.	(Da Veiga *et al.*, 2020) (Zhen *et al.*, 2022)
P9	As pessoas trabalham em conjunto com a equipe de segurança propondo melhorias para os processos de segurança e fortalecer a cultura de segurança da empresa.	(Gundu, 2019) (Alshaikh; Adamson, 2021)
P10	As pessoas reportam os incidentes de segurança e possíveis vulnerabilidades para a área de segurança.	(Yaokumah; Walker; Kumah, 2019) (Carpenter, 2022)
P11	As pessoas adotam o comportamento seguro apenas porque são obrigadas ou por receio de punição.	(Georgiadou *et al.*, 2022) (Ruighaver; Maynard; Chang, 2007)
P12	As condutas consideradas inseguras são a maioria na empresa.	(Wood, 2024) (Khader; Karam; Fares, 2021)

APÊNDICE B – QUESTIONÁRIO DA SURVEY - CONTINUAÇÃO

Dimensão da conscientização		
ID	**Questão**	**Referência**
P13	São veiculados comunicados de segurança periódicos abordando temas recorrentes importantes, novas ameaças, diretrizes e medidas de proteção.	(Khader; Karam; Fares, 2021)
P14	Os treinamentos em segurança são obrigatórios, contínuos, personalizados e com conteúdo atualizado pelo menos uma vez ao ano.	(Spitzner, 2019) (Lie; Utomo; Winarno, 2021) (Khando *et al.*, 2021)
P15	Todas as pessoas têm suas competências em segurança avaliadas anualmente.	(Wood, 2024)
P16	O programa de conscientização realiza campanhas frequentes, criativas e envolventes.	(Carpenter, 2022)
P17	Há uma equipe dedicada exclusivamente para gerir o programa de conscientização.	(Spitzner, 2019)
P18	Simulações de phishing e testes sobre temas de segurança são frequentes.	(Carpenter, 2022)
P19	Há um programa de recompensas para reforçar o comportamento seguro.	(Carpenter, 2022)
P20	O programa de conscientização conta com agentes promotores da segurança na organização (*security champions*).	(Carpenter, 2022)

Dimensão organizacional		
ID	**Questão**	**Referência**
P21	A alta direção (diretoria e presidência) apoia, avalia e orienta a segurança cibernética na empresa.	Anilkumar *et al.* (2023)
P22	A alta direção promove comunicados que reforçam a importância da segurança e estimulam o seu desenvolvimento.	Ruighaver *et al.* (2007)
P23	O investimento financeiro para desenvolver a cultura de segurança é estratégico, contínuo e de longo prazo.	Khando *et al.* (2021)
P24	A segurança é essencial nas decisões estratégicas de todas as áreas, operações, produtos e serviços da organização.	Uchendu *et al.* (2021)
P25	Os líderes executivos participam de fóruns internos e externos sobre segurança.	Spitzner (2019) Carpenter (2022)

APÊNDICE C – PERGUNTAS DA ENTREVISTA

ID	Pergunta	Dimensão do MMCSC	Referência
Q1	Como você avalia o nível de conhecimento dos funcionários sobre ameaças recentes, vulnerabilidades e ataques globais?	Conhecimento	(Khando *et al.*, 2021) Anilkumar *et al.* (2024b)
Q2	Qual o nível de conhecimento dos funcionários sobre as diretrizes, normas e processos de segurança?	Conhecimento	(Zhen *et al.*, 2022) (Kő; Tarján; Mitev, 2023)
Q3	Qual a percepção que os funcionários têm sobre a importância da segurança cibernética?	Atitudes	(Da Veiga; Martins, 2015) (Georgiadou *et al.*, 2022)
Q4	Qual a visão que os funcionários têm sobre segurança da empresa? (infraestrutura, controles e normas etc.)	Atitudes	(Georgiadou *et al.*, 2022; Zhen *et al.*, 2022)
Q5	Como você descreveria o comportamento dos funcionários em relação à segurança cibernética na empresa?	Comportamento	(Da Veiga *et al.*, 2020) (Zhen *et al.*, 2022)
Q6	Como você avalia a eficácia do programa de conscientização para desenvolver a cultura de segurança dentro da empresa?	Conscientização	(Carpenter, 2022) (Spitzner, 2019) (Lie; Utomo; Winarno, 2021) (Khando *et al.*, 2021)
Q7	De que maneira a alta direção demonstra seu apoio e envolvimento na promoção da cultura de segurança cibernética?	Organizacional	Anilkumar *et al.* (2023) Khando *et al.* (2021) Ruighaver *et al.* (2007)

APÊNDICE D – ETAPAS PARA APLICAÇÃO DO MODELO DE MATURIDADE DA CULTURA DE SEGURANÇA CIBERNÉTICA