UNIVERSIDADE ESTADUAL DO RIO GRANDE DO SUL
UNIDADE UNIVERSITÁRIA EM PORTO ALEGRE
ESPECIALIZAÇÃO EM GESTÃO PÚBLICA

BRUNA GONÇALVES AGUIAR

Segurança da Informação:
Práticas no Setor Público entre 2018 e 2023

Porto Alegre
2023

BRUNA GONÇALVES AGUIAR

Segurança da Informação:
Práticas no Setor Público entre 2018 e 2023

Trabalho de Conclusão de Curso submetido à Pró-Reitoria de Pesquisa e Pós-Graduação curso de Universidade Estadual do Rio Grande do Sul, como requisito básico para a obtenção do título de Especialista em Gestão Pública.

Orientadora: Prof.ª Dra. Paola Carmen Valenzuela Cánepa

Porto Alegre

2023

Catalogação de Publicação na Fonte

A283g Aguiar, Bruna Gonçalves.
Segurança da Informação: Práticas no Setor Público entre 2018 e 2023 / Bruna Gonçalves Aguiar. – Porto Alegre, 2023.
60 f.

Orientadora: Paola Carmen Valenzuela Cánepa.

Monografia (Especialização) – Universidade Estadual do Rio Grande do Sul, Curso de Especialização em Gestão Pública, unidade em Porto Alegre, 2023.

1. Segurança da informação. 2. Segurança digital. 3. Práticas de segurança. 4.Conscientização. 5. Cultura. I. Valenzuela Cánepa, Paola Carmen. II. Título.

Ficha catalográfica elaborada por Laís Nunes da Silva CRB10/2176.

BRUNA GONÇALVES AGUIAR

Segurança da Informação:

Práticas no Setor Público entre 2018 e 2023

Trabalho de Conclusão de Curso submetido ao curso de Especialização em Gestão Pública, como requisito básico para a obtenção do título de Especialista em Gestão Pública

BANCA EXAMINADORA:

_____

Orientadora Prof.ª Dra. Paola Cánepa

_____

Prof.

_____

Prof.

Dedicado à minha falecida amiga Olga Vieira. Sua sede por conhecimento foram uma grande inspiração, onde apesar de ter quase 80 anos de idade, nossa fascinação por cultura nos uniu.

Agradecimentos

Agradeço principalmente a meu marido pelo apoio desde a matrícula ao ambiente de estudo. Agradeço a compreensão de minha família pela ausência devido à dedicação que precisei ter. Sou eternamente agradecida à UERGS por ser uma instituição acolhedora e séria, aos professores por serem acessíveis e dedicados e a meus colegas por também passarem seu conhecimento e compartilharem suas experiências. Agradeço ao Instituto de Tecnologia e Sociedade pelo incentivo ao assunto tão importante, através da disponibilização de cursos, textos e vídeos.

RESUMO

O objetivo deste trabalho foi realizar um levantamento atualizado de práticas de segurança da informação, de 2018 até agosto de 2023 e realizar uma comparação entre os artigos de âmbito geral com o setor público. A conscientização e a cultura da defesa digital tornam-se cada vez mais importantes para organizações protegerem informações pessoais e confidenciais, a partir do momento que o cibercrime costuma atacá-la. Através de uma pesquisa de abordagem qualitativa e um levantamento bibliográfico sistemático integrativo, as práticas foram classificadas e categorizadas. Posteriormente, as comparações de artigos entre setor público e de nível geral, demonstraram que há poucos estudos direcionados ao setor público. As principais práticas encontradas foram: confidencialidade, integridade, disponibilidade e autenticidade.

Palavras-chave: segurança da informação; segurança digital; práticas de segurança; conscientização; cultura.

ABSTRACT

The objective of this final work was to present a survey about security information practices, between the year of 2018 until the mouth of august of 2023 and will compare between the articles of security inside a general propose with articles of public sector. The awareness and the culture of digital defense becomes increasingly important for companies have some possibility to protect your personal or confidential information, mainly from the moment when the cybercrime can prejudice organizations and users. Beyond this qualitative research and a systematic integrative biographic survey, the practices of security information were classified and categorized. Subsequently, the comparisons of articles between the public sector and general scope, demonstrates just a few studies aimed at the public sector and the mainly practices founded was confidentiality, integrity, availability and authenticity.

Keywords: security information; digital information; security practices; awareness; culture.

SUMÁRIO

1 INTRODUÇÃO

A tecnologia é uma ótima aliada para a comunicação das pessoas do planeta inteiro. No entanto ela necessita de cuidados para que seja utilizada para o bem. Este trabalho visa explorar problemas relacionados à segurança da informação e práticas que podem amenizar situações negativas durante seu uso. É habitual pensar que se está bem mais seguro dentro de casa do que fora. No entanto, cibercriminosos podem esvaziar uma conta bancária de uma pessoa em qualquer momento do dia.

Ao registrar informações pessoais em sites de compras, baixar aplicativos desnecessários, ou salvar senhas no celular, por exemplo, um usuário está facilitando com que seus dados sejam roubados por pessoas com más intenções. Até mesmo uma pessoa de baixo poder aquisitivo pode ser vítima: o criminoso consegue aumentar o limite de uma conta bancária criada e fazer dívidas exorbitantes, ou aplicar outras fraudes, como lavagem de dinheiro através destas contas.

Os dados pessoais precisam ser considerados algo sagrado diante da quantidade de locais em que eles são registrados obrigatoriamente: no Brasil, o Sistema Único de Saúde (SUS) registra informações de todos os cidadãos que se vacinam, o INSS registra as informações de todos que contribuem para a previdência, o SERASA Experian registra informações de Cadastros de Pessoas Físicas (CPFs). Quando um criminoso consegue um simples e-mail verdadeiro, ele já pode disparar diversas tentativas de *phishing*[1], e entrando na conta em algum site, conseguir mais informações pessoais, inclusive números de cartão de crédito salvos, ou fotos íntimas para subornar a vítima. Os principais alvos dos hackers são grandes bancos de dados, como de instituições bancárias e de setor público. É necessário apenas um funcionário sem o devido treinamento para comprometer informações de pacientes e/ou funcionários de um complexo hospitalar, simplesmente por abrir um link de e-mail falso.

Os problemas envolvendo a internet afetam também organizações, que podem ter prejuízos catastróficos: no Brasil, golpes envolvendo nomes de redes de varejo populares geraram prejuízo de dois bilhões de reais desde o início da pandemia de Covid-19 (Axur, 2020). Esta vulnerabilidade justifica a importância deste trabalho,

[1] E-mail falso que induz a ceder alguma senha em um site falso, mas convincente.

que levantou diversos problemas que afetam a segurança e quais práticas viáveis de conscientização e cultura podem auxiliar as organizações a atenuar seus prejuízos.

Ameaças cibernéticas vêm pondo a risco todas as informações disponíveis na internet, abrindo possibilidades para guerras digitais. A Rússia, por exemplo, hackea informações de setores nucleares, água e aviação e o Iran também obteve ilegalmente a propriedade intelectual de professores universitários de outros países (OTTONICAR et al., 2020). A nível mundial, governos vêm sofrendo um aumento exponencial de ciberataques, conforme *Global Threat Landscape Report* (CLOUDSEK, 2022), o que compromete pesquisas e a segurança de países e de cidadãos.

Portanto, diante do cenário, pretendeu-se responder quais as perspectivas em práticas de segurança da informação, de 2018 a 2022 e até agosto de 2023. Esta foi uma pesquisa com metodologia de revisão bibliográfica sistemática integrativa, de caráter descritivo e com abordagem qualitativa. Como um grande alvo dos cibercriminosos costuma ser organizações (Kaspersky, 2023) para roubar grandes quantidades de dados, as práticas levantadas terão utilidade principal durante um expediente de trabalho.

Dentro do universo da segurança da informação, existem as políticas e leis para que elas ocorram e as partes técnicas que se restringem ao setor de tecnologia da informação. Mas a conscientização e capacitação dos colaboradores de uma organização é fundamental para garantir a segurança dela. Pensar que tecnologia é apenas um setor da organização é ultrapassado, por isso é importante se concentrar na forma cultural de envolver os funcionários e aumentar a resiliência cibernética. (GEORG et al., 2023)

Consoante entrevista para o jornal “O Estado de São Paulo”, Marco De Mello - presidente executivo da organização brasileira de segurança digital *Psafe* - afirmou que houve o maior vazamento de dados da história do Brasil: mais de 230 milhões de CPFs vazados em 2021(LEMOS, 2021). Ou seja, como o Brasil possui 214 milhões de cidadãos, há dados vazados de pessoas já falecidas, o que significa que a *deep web* virou um paraíso para criminosos.

O objetivo principal deste trabalho foi identificar práticas de segurança da informação que estejam relacionados à conscientização e à cultura dos últimos anos, e verificar quais são direcionados ao setor público, já que a suma maioria é voltada a instituições em geral. Este trabalho está dividido em seis capítulos. O primeiro

introduz os motivos do tema e os problemas que a sociedade enfrenta ao ignorar medidas de segurança no âmbito digital, como por exemplo a falta de soberania. O segundo capítulo, além de abordar conceitos básicos, apresenta as práticas em três vertentes: Tecnologia, Políticas e Legislação e Conscientização e Cultura. Também, em sua parte quatro, aborda como é a segurança da informação na gestão pública e em outros países.

A metodologia utilizada foi abordada no terceiro capítulo, explicando detalhadamente sobre os recortes e tipo de pesquisa. O quarto capítulo realizou a análise dos artigos coletados, a pesquisa principal deste trabalho, onde as práticas nacionais dos últimos seis anos são categorizadas e comparadas entre forma geral e setor público. O quinto capítulo discute as práticas encontradas e o sexto serão as considerações finais, ou seja, conclusões ao realizar este trabalho.

1.1 Justificativa

O levantamento de práticas, ou seja, as medidas que serão identificadas, poderão ser aproveitadas por qualquer organização, entidade ou órgão que vise iniciar medidas de segurança - inclusive aprimorar as atuais. Afinal, este assunto definitivamente sempre necessitará de atualização, pois a tecnologia acaba sendo modificada conforme os anos: como podemos observar, conforme Relatório da *Flexera*[2] (FLEXERA, 2020), onde foi constatada uma aceleração significativa no processo de uso de nuvem no ambiente corporativo com a vinda da pandemia em 2020.

Em 2022, durante a disciplina de Direito Administrativo desta Especialização, foi feito um trabalho sobre desinformação, o que inspirou a posteriormente criar um Projeto de Lei Estadual sobre cibersegurança[3], em âmbito estadual, pela Assembleia Legislativa do Rio Grande do Sul. Também a realização desta pesquisa está possibilitando levar conteúdo sobre este tema através de vídeos curtos na rede social Instagram, na conta @brunaaguiar05. Desta forma, cria-se uma ponte entre o meio acadêmico e usuários do meio digital. O primeiro vídeo teve milhares de visualizações, o que pode contribuir para o entendimento da relevância do assunto e de medidas pessoais que o cidadão pode tomar, como por exemplo, como criar uma senha segura.

[2]Organização Global de Soluções em TI
[3] PL 200 2022.

Este assunto precisa ser explorado pela academia, pois é nítido o quanto a internet precisa ser um ambiente seguro, onde ela é que deve servir ao ser humano, jamais o oposto. A academia possui um papel importante para a sociedade, visto que ela foge totalmente do chamado senso comum, quando é necessário explorar algum assunto. A UERGS possui um projeto estratégico que propõe um arranjo institucional, o chamado “Uergs 20+: composto por 70 projetos, agrupados em três áreas estratégicas identificadas como portadoras de futuro: energia e mobilidade; recursos naturais e sistemas alimentares; espaços digitais e sistemas produtivos.” (UERGS, 2020, documento não paginado)[4] Portanto, este trabalho está alinhado com a atual filosofia acadêmica.

Mesmo havendo trabalhos na área da segurança cibernética e segurança da informação, conforme as tecnologias mudam ou ficam obsoletas, será sempre necessário aprender a se proteger. Assim como o vírus da gripe que precisa de uma vacina atualizada anualmente, as formas de fraudes e ataques virtuais possuem uma criatividade persistente.

Os dados de qualquer cidadão precisam estar sendo administrados de forma ética, correta e segura. Apesar da Lei Geral de Proteção de Dados (LGPD) estar em vigor desde setembro de 2020, o papel da segurança da informação é de todos. Ademais, todo o cidadão, conforme a Constituição Federal de 1988(BRASIL, 1988 art. 5º, tem direito à privacidade e à segurança:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade; [...]
> **X** - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

De forma geral, as demandas costumam ser criadas pela sociedade civil e devem influenciar a agenda de quem ocupa o poder, ou seja, a agenda estatal de políticas públicas consiste em abordar as pautas relevantes para a sociedade (TEIXEIRA, 2002). Como este assunto é importante a todos, o Estado não pode se abster em atenuar crimes virtuais e outros problemas que causam danos a todos: indivíduos, organizações e Estado.

---

[4] https://uergs.edu.br/projeto-uergs-20-mais

1.2 Objetivo

Este trabalho de conclusão teve como objetivo principal identificar práticas de segurança da informação que são voltadas ao setor público. Os objetivos específicos foram os seguintes:

1. Levantamento pela plataforma *Scholar* sobre práticas de segurança da informação entre 2018 a 2022 e até agosto de 2023;
2. Definição de práticas para influenciar a cultura e conscientização;
3. Comparação entre artigos voltados a instituições em geral ou a setor público.

2 REVISÃO DE LITERATURA

Esta sessão apresentará a definição de conceitos básicos sobre informação, segurança da informação e práticas. Estas serão relacionadas por três partes: tecnologia, legislação e conscientização.

2.1 Informação

Informação pode ser definida como “o produto de um processamento exercido sobre os dados”, sendo uma soma de algo maior do que simplesmente uma junção de partes (MAGNO, 2022). Para uma organização, a informação pode ser considerada como um dos recursos primordiais para a contribuição de uma melhor gestão: “As informações servem como base para a construção do conhecimento”, segundo Lemos II (2011, pág. 18).

Outros conceitos atuais definem informação como um bem, um ativo de uma organização e tendo muito valor, possui fundamental relevância para os negócios (GALVÃO,2023). De forma geral, informação é um telefone ou endereço, todavia, no âmbito computacional, dados e informações são diferentes, onde o primeiro é apenas um elemento que não foi processado ou analisado, já o segundo é o refinamento dos dados (GALVÃO, 2023). Informação também é considerada uma *commodity*, ou seja, uma mercadoria que foi produzida, manipulada e distribuída, onde desde os anos 60, atividades informacionais já eram um desafio para economistas mensurarem. (GALVÃO, 1999)

Uma empresa pública, por mais que não tenha clientes, mas sim, usuários dos serviços prestados, para funcionar precisa de muitas informações que costumam envolver alta complexidade para serem geridas. O Departamento de Informática do Sistema Único de Saúde (DATASUS), por exemplo, disponibiliza diversas informações sobre os usuários do serviço, como localização e estado civil. Porém é óbvio que informações sensíveis, como CPF, nome completo e telefone devem ser sempre sigilosos por questões de segurança do usuário, que tendo suas informações comprometidas, pode sofrer prejuízos - afinal, ninguém gostaria de ter seu nome usado sem autorização.

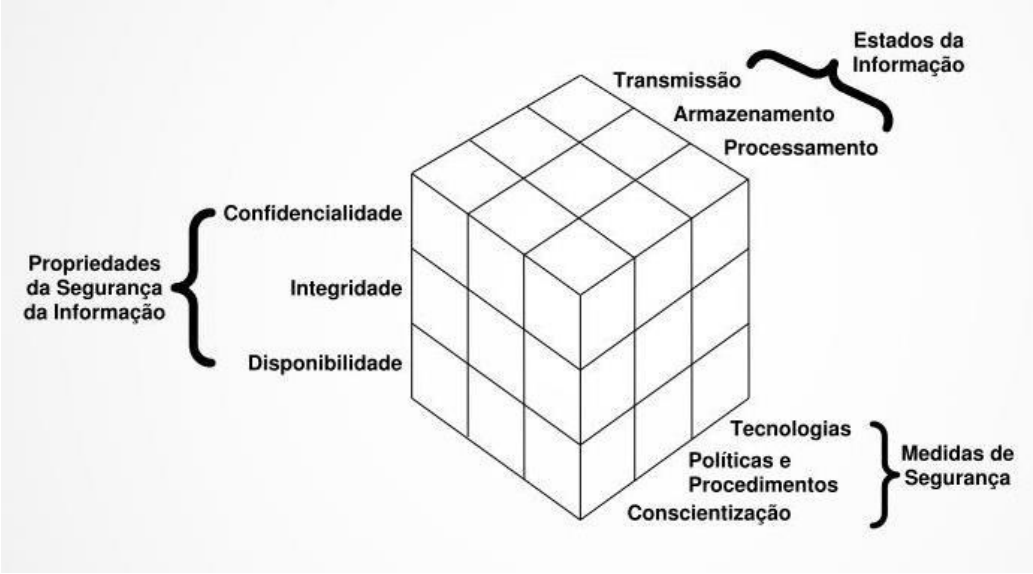
2.2 Segurança da Informação

A complexidade atual faz com que seja cada vez mais difícil organizar e armazenar informações. Na década de 90, por exemplo, as enciclopédias Barsa eram uma importante fonte de informação para consultas em pesquisas e os jornais em papel eram uma tradição muito comum. Ter um *diskman* era um luxo e a revelação de fotografias era cara e demorada. Conforme a digitalização das civilizações do planeta cresce, a complexidade de administrar a vida inteira também: memorizar senhas, baixar aplicativos, aceitas cookies, negar newsletter, fazer backup de imagens, entre muitas outras atividades que eram inimagináveis no passado.

Apesar deste artigo restringir sua pesquisa com o tema destinado ao meio digital, o autor (FONTES, 2012 *apud* ARAÚJO; BASTISTA; ARAÚJO, 2020) define essencialmente a “segurança da informação”, em seu modo mais completo, como sendo mais do que da forma digital. Em outras palavras, desde uma folha de papel com anotações, bem como o conhecimento das pessoas, seja confidencial ou explícito.

É comum que diversos assuntos sejam explicados através de pirâmides (como a dos alimentos, hierarquias empresariais etc.), mas por haver mais de um ponto como base, uma boa definição para o assunto teve origem no ano de 1991, por John McCumber (MUSICH, 2020). Seu modelo revolucionou as formas de enxergar os aspectos fundamentais vistos de diferentes prismas. Abaixo, a Figura 1 apresenta o Cubo, onde a face Medidas de Segurança foi o centro deste trabalho, desenvolvido na parte quatro.

Figura 1 - Cubo de McCumber



Fonte:(Musich, 2020)

Em 2020 a OCDE (Organização para a Cooperação e Desenvolvimento Econômico) concluiu em sua Revisão Bibliográfica que "O Brasil está na fase inicial da promoção da segurança digital na sociedade" e que considerando documentos legais do Brasil, há termos diferentes utilizados neles para abordar "segurança digital, segurança da informação, segurança cibernética, defesa cibernética, proteção de dados, além de termos relacionados, como ativos da informação, infraestruturas críticas, espaço cibernético etc." Além disso, a própria PNSI (Política Nacional de Segurança da Informação) define segurança da informação, como um termo que inclui segurança cibernética, defesa cibernética (OECD, 2020).

Conforme a ABNT (NBR ISO/IEC 27002, 2013), a Segurança da Informação (BARRETO; SUCUPIRA; LIMA, 2022):

a) compreende proteção das informações, sistemas recursos e demais ativos contra desastres ou erros (intencionais ou não) e manipulação não autorizada;
b) redução da probabilidade e do impacto de incidentes de segurança;
c) é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software;
d) "O DTI (Departament of Trade and Industry), localizada no Reino Unido, foi o primeiro órgão internacional a preparar uma norma de Segurança

> da Informação na década de 80, a ISO 17799” (MANOEL, 2014 *apud* OLIVEIRA, 2019, p.6).

2.3 Práticas Utilizadas para a Gestão de Segurança da Informação

Para contextualizar o que são práticas neste trabalho, elas podem ser definidas como procedimentos formais, existindo maneiras tanto diretas quanto indiretas, tradicionais ou inovadoras. “Descobri-las, organizá-las e/ou melhorá-las faz-se necessário tanto em instituições privadas como públicas.” (BURKE, 2016 *apud* ARAÚJO; BASTISTA; ARAÚJO, 2020)

Certas práticas de segurança são restritas ao setor de TI, porém isso pode ser sempre insuficiente e sobrecarregar funcionários que nem sempre resolvem qualquer problema digital. Medidas para fortalecer a segurança de uma organização, apesar de envolverem planejamento e engajamento da alta hierarquia, na verdade dependem bastante de o colaborador receber orientações, ou seja, todos devem estar envolvidos. Abaixo seguem três tópicos que classificam as práticas e sua relevância.

2.3.1 Práticas Relacionadas com Tecnologia

Estas práticas estão diretamente ligadas com o investimento em tecnologia da informação, seja em pessoas capacitadas, seja em modernizar a forma como a informações transitam dentro de uma organização. A inovação sempre existiu na história da humanidade, auxiliando em tarefas e facilitando a vida. Serão citadas algumas tecnologias novas para exemplificar a conexão entre práticas e tecnologia.

O armazenamento em nuvem ganhou sua popularidade através do aumento do trabalho remoto nos últimos anos. Quando os funcionários deixam de centralizar tudo em seu computador (que pode ser danificado, espalhar vírus em pen drives, por exemplo) e passa a usar a nuvem, os seus arquivos e dados estão mais seguros por estarem salvos em mais de uma forma. (TIC Domicílios, 2020) Além disso, ter apenas um servidor que armazena tudo de um local, também não é tão seguro quanto descentralizar as informações e não requer a mesma manutenção, como costuma ser o caso se um servidor central (VIANNA, 2019). A própria Microsoft disponibiliza treinamentos sobre a melhor forma de uso da nuvem, chamada Microsoft Azure, desde 2010 (Microsoft, 2023). Não obstante, é fundamental que haja orientação quanto ao seu uso, pois muitos hackers têm como alvo as nuvens de corporações.

O Blockchain foi criado inicialmente para o uso de bitcoin, mas na verdade é uma tecnologia criptográfica, extremamente segura e transparente, utilizada para registrar transações. Pode-se defini-lo como um “livro contábil digital” grande, onde após ter dados nele, jamais se pode apagá-los. “Dentre os principais benefícios da aplicação da blockchain tem-se o combate a corrupção, a transparência, serviços notariais sem fraudes, aumento de mecanismos de participação social, descentralização de registros civis [...]”(LIMA, 2020, pág. 85). Seu maior obstáculo para implementação pode ser a necessidade de alto investimento financeiro.

2.3.2 Práticas Relacionadas a Legislação, Políticas e Procedimentos

Apesar da internet potencializar diversos novos problemas, ela está longe de ser uma anarquia. Um país costuma possuir leis para que os habitantes convivam de forma civilizada, portanto, elas são inquestionáveis para prover a ordem e a harmonia entre o povo e os Poderes. Em tese, deveriam ser válidas tanto em território quanto dentro da internet, mas cada país também cria as suas legislações e políticas públicas da forma que melhor convém àquela população (que muitas vezes é a responsável por persuadir ou pressionar os tomadores de decisão) (SOUZA, 2007).

O Brasil também possui formulação própria de leis gerais para a internet, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados. Apesar de citarem a inclusão digital, este conceito com o de alfabetização digital são bem diferentes, sendo o segundo inquestionavelmente urgente. É como comparar o direito em obter um veículo com saber dirigir um automóvel. O primeiro “estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil”. Criada no ano de 2014, define a web como um instrumento de democracia e visa defender o direito à internet. Apesar de não abordar políticas de prevenção a fraudes, ela cita a proteção de dados pessoais com algumas exceções de finalidades, como se houver consentimento ou com outra justificativa.

A Lei Geral de Proteção de Dados Pessoais (LGPD), estabelecida em 2018, apesar de ser muito importante, de forma geral dispõe que as organizações privadas cuidem dos dados coletados, sujeitando-se a sanções em caso de descumprimento. Porém, não aborda sobre a responsabilidade de organizações, população em geral, ou do Estado, em promover políticas de instrução, notificação de fraudes, cordialidade

no uso da internet, entre outros assuntos relevantes. Consoante a LGPD, uma informação sensível é definida como “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (BRASIL, 1988, Art 5º, inc. II).

Segundo a Política Nacional de Segurança da Informação (PNSI), o Gabinete de Segurança da Informação da Presidência da República é o órgão governamental mais importante em relação à segurança digital no Brasil desde os anos 2000. (OECD, 2020, pág. 113). Há dois principais escopos de atuação, sendo um deles os “Padrões para implementação da SI”, abordando desde a responsabilidade por normas para a gestão de riscos de segurança da informação nos órgãos e entidades da administração pública federal até a conscientização e a capacitação da administração pública e da sociedade. O segundo escopo são as Políticas Públicas, que precisam formular a adequação à evolução tecnológica e a elaboração da chamada Estratégia Nacional de Segurança da Informação. Ela também apoia a elaboração de planos nacionais e a avaliação da execução da PNSI.

Desde 2005 o Ministério da Defesa é apoiado pela Política Nacional de Defesa (PND), sendo ela uma composição de medidas e ações do Estado com a finalidade de defender o território, a soberania e os interesses da nação contra forças e ameaças externas (VIANNA, 2019). A segurança nacional é determinada como "condição que permite ao país preservar sua soberania e integridade territorial, promover seus interesses nacionais, livre de pressões e ameaças e garantir aos cidadãos o exercício de seus direitos e deveres constitucionais". De forma complementar, o desenvolvimento tecnológico, o engajamento e a gestão da informação são acatados como parte da Capacidade Nacional de Defesa, conjuntamente à proteção, a coordenação e o controle. OLIVEIRA, 2021).

Desde o início de 2020, o Brasil possui o Decreto 10.222 que aprova a Estratégia Nacional de Segurança Cibernética (BRASIL, 2020), uma peça fundamental para a soberania de nosso país. Estrategicamente, houve inclusive consulta pública para adesão e diagnósticos sobre a situação nacional, e posteriormente é que o regimento da lei ocorreu, após 31 reuniões. Considerou-se o chamado “Modelo de maturidade em segurança cibernética”, que ressalta a importância de políticas, estratégias, cultura cibernética, educação, treinamento, entre

outros. A Estratégia também é popularmente atribuída como “E-ciber” e possui efetividade estendida apenas até 2023. (CAETANO, 2023)

Em 2022 o Governo Federal concedeu o Plano Tático de Combate a Crimes Cibernéticos (BRASIL, 2022). Um acordo cooperativo entre a Federação Brasileira de Bancos (Febraban) e a polícia federal para compartilhar informações para identificar a punir criminoso. O Plano também visa o aumento em prevenção de ameaças, criando um programa antifraudes bancárias eletrônicas, onde capacita-se agentes de segurança. (FEBRABAN, 2022)

No Estado do Rio Grande do Sul, a organização de economia mista que cuida de toda a parte de TI do Poder Executivo Estadual chama-se PROCERGS (Companhia de Processamentos do Estado do RS), possuindo normas de uso para todos os servidores públicos seguirem, e desta forma padronizar uma segurança para todos. Por exemplo, existem altas restrições para a instalação de qualquer software ou alterações mínimas de configurações de um computador - até alterar a imagem de fundo da área de trabalho é impossível para o usuário.

A organização em 2016 emitiu uma Política de Segurança da Informação para esclarecer a relação do servidor público como usuário de um computador que pertence à organização. Normas de segurança de senha, por exemplo, são claramente rigorosas, pois elas necessitam de aprovação do próprio sistema, somente a partir da inserção de caracteres diversos, com números e símbolos, além de letras maiúsculas e minúsculas. Também possuem prazo de expiração de senha para obrigar a alteração frequentemente (PROCERGS, 2017)[5].

A nível estadual no Rio Grande do Sul, existem três decretos, uma norma e uma resolução referentes à segurança da informação (PROCERGS, 2017):

1) Decreto Estadual 52.616, publicado em 19/10/2015: Política de Tecnologia da Informação;
2) Decreto Estadual 53.927, publicado em 21/02/2018: Compartilhamento de Dados na Administração Pública Estadual;
3) Decreto Estadual 53.164, publicado em 10/08/2016: Procedimentos para a classificação de informações;

[5] https://www.procergs.rs.gov.br/premiacoes A organização inclusive teve muitas premiações por sua qualidade: entre 2009 e 2022 foram mais de 60 conquistas relevantes, divididas em 3 grandes categorias: Soluções, Gestão e Inovação”.

4) Norma estadual PGOV 03/2016, publicada em 28/11/2016: Padrão de Governança em Segurança da Informação;
5) Resolução Interna: Reestruturação Organizacional, publicada em 05/04/2013: Resolução da Diretoria da PROCERGS que cria a Coordenação de Segurança (CSEG).

É recomendável que toda organização tenha um comitê de segurança[6], onde a diretoria executiva deve ser responsável por criá-lo. Sua política interna pode basear-se na norma internacional ISO 27002 - sendo a mais completa - ou ter como base o modelo chamado COBIT 5[7], uma referência para a governança de SI, pois define estratégia para organizações. Resumidamente, ele possui cinco princípios fundamentais(SOUSA, 2019), sendo eles:

1) Satisfazer a necessidade das partes interessadas[8];
2) envolver a instituição;
3) impor uma estrutura de segurança integrada[9] e excepcional;
4) possibilitar uma visão holística;
5) separar governança do gerenciamento.

Como forma de prevenção, estabelecer uma política de vazamento antes que ele ocorra é fundamental (SUDOSKI, 2017). Se todos os colaboradores estiverem cientes de como proceder, a imagem que a organização costuma precisar zelar, sofrerá menos danos. Também chamado de plano de contingência, precisa ser revisado periodicamente e fazer parte da política de segurança, que envolve além de desastres cibernéticos, como ter portas corta-fogo para um acidente como um incêndio ou tragédia da natureza, como uma enchente, por exemplo (FURTADO NETO; MISAGUI, 2021). Uma organização neste âmbito, evitaria grandes desastres que poderiam arruinar completamente a organização.

Conforme a Associação Brasileira de Normas e Técnicas (ABNT), os Processos de Gestão de Riscos são a forma primordial para a segurança da

[6] Também chamado de ISSC – *Information Security Steering Committee*
[7] Também chamado de *Control Objectives for Information and Related Technology*
[8] Também popularmente chamado de *stakeholder*
[9] Também chamado de *framework*

informação (NETO; ARAÚJO, 2019). Quanto mais informações uma instituição precisa gerir, mais complexa fica sua gestão, porém esta prática ajuda na tentativa de analisar as informações de um outro ângulo. A ABNT adota uma norma de gestão de riscos composta por seis fases:

a) definição do contexto;
b) processo de avaliação de riscos;
c) tratamento do risco;
d) aceitação do risco;
e) comunicação e consulta do risco;
f) monitoramento e análise crítica de riscos.

2.3.3 Práticas Relacionadas à Conscientização/Cultura

De forma geral, pode-se dizer que valores individuais compartilhados são a cultura de um povo. A cultura digital é como qualquer outra, em constante modificação, envolto de ideias e atitudes. “Assim, a cultura digital estaria no mesmo patamar de outras culturas, como a cultura escolar, cultura organizacional, cultura da paz, entre outras” (SANTOS; ALMEIDA, 2020). A conscientização e orientação é inegável para absolutamente todos os colaboradores de uma organização ou instituição precisam promovê-la, como por exemplo, através de atenção ao programa de antivírus ou observando sites suspeitos. Não adianta apenas o setor de T.I engajar-se sozinho (LEITE, 2021). O alto escalão também precisa de engajamento, afinal, por poderem ter mais acessos restritos, podem correr maior risco de armadilhas que poderiam ter sido evitadas.

A prevenção dos problemas virtuais pode ocorrer de diversas formas, visto que “na grande maioria dos casos a fraude ocorre por alguma falha da vítima”. Por exemplo, um e-mail pode instalar um *banker* – analogicamente falando, um vírus - que rouba informações bancárias. (GUIMARÃES, 2010 *apud* MACHADO, 2018). Ou seja, o melhor antivírus é o usuário. Se um funcionário souber identificar a diferença entre um e-mail falso muito bem elaborado de um verdadeiro, ele já preservará a organização, pelo menos desta forma. Abaixo, seguem exemplos de cultura e conscientização:

a) atualização de software: o sistema operacional deve ser recente, de licença original ou *open source* confiável, de modo que o computador possa receber atualizações de segurança sobre vulnerabilidades identificadas em seu sistema operacional. A não correção de vulnerabilidades pode abrir espaço para ataques mal-intencionados (RODRIGUES, 2020);
b) disponibilidade da informação sempre que necessário o seu uso.(FRANCISCO; TOMAZ, 2021) O Backup é uma cópia de dados importantes em uma organização. (SUBA, 2020)Visam garantir que não se percam as informações salvas apenas no computador, através de uma memória externa ou servidor da organização, que fique preferencialmente afastado do local de trabalho;
c) manter as senhas seguras é cria-las somente com a maior complexidade possível. Teoricamente, é proibido utilizar nomes próprios ou datas de qualquer aniversário. Softwares atuais possuem dicionários internos onde senhas simples são instantaneamente reveladas. Boas senhas possuem, ao menos, números e caracteres especiais como “S#nh2SEgur2” (LEITE, 2018). O tempo médio para um hacker descobrir a senha de um usuário comum encontra-se como Anexo A, ao final deste trabalho;
d) desde o ano de 2023, Microsoft disponibiliza gratuitamente às corporações, treinamentos online para tomadores de decisão ficarem totalmente atualizados quanto a medidas de segurança, através do Cybersecurity *Tabletop Exercise* (Microsoft Security, 2023). Uma simulação de problema com ataques a sistema de uma organização fictícia, onde como exercício interativo, deve-se pensar no que fazer de forma rápida e responder o que se deveria fazer naquela situação bem complicada. A cena possui explicações bem definidas, com dados dos relatórios do cibercrime e conta com líderes da organização. O exercício está disponível em diversas línguas após cadastro da organização. Manuais de instruções criados e personalizados pela própria organização devem ser esclarecedores para todos os usuários finais (SUBA, 2020);
e) cautela durante download e instalação de qualquer aplicativo software novo, que sempre seja de fontes confiáveis: normalmente torrentes e pirataria em geral são gratuitos, mas não costumam ser desenvolvidos pela boa vontade

de alguém, podendo ser uma pessoa mal-intencionada querendo espalhar algum vírus (PINHEIRO; SILVA, 2018);

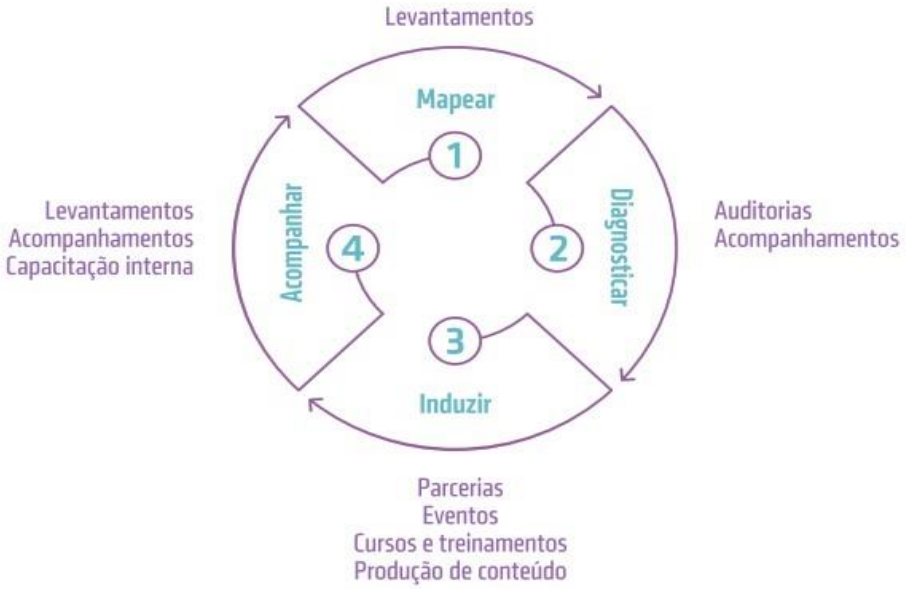
f) *capture the Flag*: similar à brincadeira “Pic-bandeirinha”, torneios competitivos foram implementados sobre o assunto em uma universidade de Novo Hamburgo/RS. Os alunos formavam times e eram desafiados por provas diversificadas sobre cibersegurança. Afinal, combater os problemas online não deixa de ser uma batalha. E a cibersegurança está dentro da segurança da informação (MORAES; HAMBURGO, 2020). Esta prática aparenta estar relacionada à gamificação, uma forma de incrementar as atividades para o aprendizado das práticas de conscientização (MARINHO, 2022);
g) confidencialidade: Muitos arquivos dentro de uma organização podem ser considerados confidenciais: dados de clientes, fornecedores e dos próprios colaboradores. É indispensável que o armazenamento seja no mínimo, protegido por senha, dificultando o acesso (RODRIGUES, 2020) e que somente pessoas pré-determinadas possam ter acesso, restringindo-o conforme a real necessidade (FRANCISCO; TOMAZ, 2021);
h) mais especificamente do setor público, o Serviço Federal de Processamento de Dados (SERPRO)[10], para implementar a cultura de gestão e governança de dados, utiliza o *Data Management Body of Knowledge.* Também *c*onhecido como *DMbok*, desenvolvido pela *Data Management Association*. Ele é um guia tradicional em diversos países e sua estrutura para gestão e governança de dados abrange 11 áreas de conhecimentos de dados, como design, armazenamento, ética, qualidade, entre outros(BARRETO; SUCUPIRA; LIMA, 2022). Alguns princípios fundamentais da SERPRO são: a colaboração, a integridade e a transformação cultural disseminada por toda organização, onde os dados são tratados como ativos patrimoniais. (BARRETO; SUCUPIRA; LIMA, 2022);
i) o Plano de Recuperação de Desastres é uma estratégia para minimizar danos que um ataque possa trazer. Quanto mais a estratégia estiver espalhada pelos colaboradores, melhor de ser implementada, caso necessário (FURTADO NETO; MISAGUI, 2021). Além de cibercriminosos, a

[10] o Serviço Federal de Processamento de Dados (SERPRO) possui 50 anos e é a maior organização pública de TI do mundo.

organização pode sofrer danos por espionagem ou sabotagem de funcionários.

Um ótimo exemplo de prática em uma instituição parte do Tribunal de Contas da União (TCU): em 2021 o órgão publicou suas Estratégias de Fiscalização em Segurança da Informação e Segurança Cibernética. A Secretaria de Fiscalização de Tecnologia da Informação é responsável por examinar a gestão e uso dos recursos da Tecnologia da Informação em todo o âmbito da administração pública a nível federal. A implementação é representada por quatro eixos: mapeamento, diagnóstico, indução à adoção de boas práticas e acompanhamento, conforme figura 2:

Figura 2 – Eixos de Implementação de Segurança



Fonte: (TCU, 2021)

O primeiro eixo de mapeamento realiza levantamentos de riscos em sistemas informacionais, infraestruturas críticas e benchmarking internacional[11], enquanto o eixo de diagnóstico é quem realiza as auditorias sobre a LGPD, em sistemas críticos, em backups, entre outros. O terceiro eixo de boas práticas visa a formalização de parcerias com outras entidades, capacitações para tribunais estaduais e ainda disponibiliza conteúdos de orientação a gestores, enquanto último eixo elabora matrizes de risco, revisa índices de capacidade em Gestão de Segurança da

[11] Isto é, uma comparação com práticas e valores adotados por outras nações.

Informação[12] e aplica questionários para monitoramento de evolução no cenário. Os auditores também recebem treinamento exclusivo.

Por conseguinte, a cultura e conscientização da segurança da informação está em “pequenos” gestos, como ter cautela durante download e instalação de qualquer aplicativo ou software novo, que sempre seja de fontes confiáveis: normalmente *torrents* e pirataria em geral são gratuitos não costumam ser desenvolvidos pela boa vontade de alguém, mas sim uma pessoa mal-intencionada querendo instalar algum vírus no computador da vítima (PINHEIRO; SILVA, 2018).

2.4 Práticas Internacionais

Conforme a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a maioria dos países faz quase que um malabarismo para tentar garantir a segurança nacional, pois há sempre dificuldades em encontrar um equilíbrio saudável entre aspectos econômicos e sociais. Praticamente não existe um modelo universal, fora a ISO 27000. É interessante comparar o que os outros países estão resolvendo (ou apenas atenuando) seus problemas, mas o objetivo desta comparação jamais foi menosprezar o que já existe nacionalmente.

Porém, uma boa prática deve possuir uma abordagem integral: assim como o Brasil, por exemplo Austrália, Japão e Reino Unido também possuem uma equipe que atua em seu Gabinete de Governo. A França criou uma agência centralizada de coordenação nacional, no âmbito de um órgão de coordenação pré-existente que é subordinado ao Primeiro Ministro (ANSSI). Importante lembrar que, conforme o tamanho da população for maior, mais complexo fica de administrar qualquer política pública. Logo, se o país é pequeno, uma política pública tem possibilidade de lidar com menos obstáculos.

Os Estados Unidos estabeleceram uma agência de segurança cibernética e de infraestrutura (CISA) no Departamento de Segurança Interna (Home Security). Por coincidência, três países incrementaram a segurança digital a um ministério já existente: Canadá, Alemanha e Holanda. Em todos os casos citados, há diferentes disposições no que diz respeito a qual ou quais órgãos são responsáveis por questões operacionais e de políticas. (OECD, 2020)

---

[12] Em parceria com a Secretaria Extraordinária de Administração.

Na Estônia, país com menos de dois milhões de habitantes, conforme o canal de televisão Futura, existe a Identidade Digital. Ela pode ser usada internacionalmente e, sua parte física seria um token para garantir que seus dados fiquem apenas onde o cidadão escolher. Esta identidade conseguiu unificar acesso a todos os serviços públicos do país, facilitando a abertura de organização, pagamento de impostos e a segurança dos dados de cada cidadão cadastrado. O Brasil possui algo similar chamado E-digital, porém, é um serviço de assinatura paga.

3.0 METODOLOGIA

Este trabalho é uma revisão bibliográfica sistemática, a respeito do tema Práticas de Segurança da Informação, através de uma pesquisa qualitativa. Foram necessários alguns critérios de exclusão de certos assuntos para poder alinhar o tema.

3.1 Recorte de Pesquisa

a) após busca no Scholar, Scielo, Lume e Gnuteca, não foi encontrado um levantamento de práticas em artigos científico;
b) dentro das três dimensões da Revisão de Literatura, a terceira apresentada como Práticas Relacionadas à Conscientização e Cultura foi desenvolvida neste Trabalho de Conclusão, em 4.1. O recorte final de palavras-chave feito através da ferramenta da pesquisa *Scholar* foi “"segurança da informação" digital práticas proteção conscientização cultura alfabetização”;
c) o recorte inicial seria dos últimos cinco anos, de 2018 a 2022, mas para um trabalho bem atualizado, resolveu-se usar as publicações até agosto de 2023 e apenas a *Scholar*, pois acabou sendo a melhor fonte, com 140 resultados na busca e 29 artigos aproveitados;
d) para melhor alinhamento da pesquisa, certos artigos precisaram ser rejeitados, pois fugiam da proposta principal. A LGPD, por exemplo, abrange outro prisma que é a parte legislativa, então não é exatamente uma prática por si. O Portal da Transparência também fica contido, pois pela lei é o que é obrigado a ser publicado pelo Estado, portanto é o oposto do que precisa ser protegido, sigiloso, como CPFs e telefones, por exemplo (tanto de funcionários de uma organização, como de clientes). Gestão de documentos físicos também foi descartado, pois neste artigo o foco é a parte de dados digitais. Outros detalhes estão no Quadro 2, na página 32, onde foram pontuados critérios de exclusão e inclusão;
e) restrição de pesquisa já esperada: supõe-se que há medidas sigilosas que não devem jamais ser divulgadas. Portanto, muitas organizações e órgãos governamentais não contariam certos segredos de segurança para afastar possíveis problemas.

3.2 Revisão Bibliográfica Sistemática Integrativa

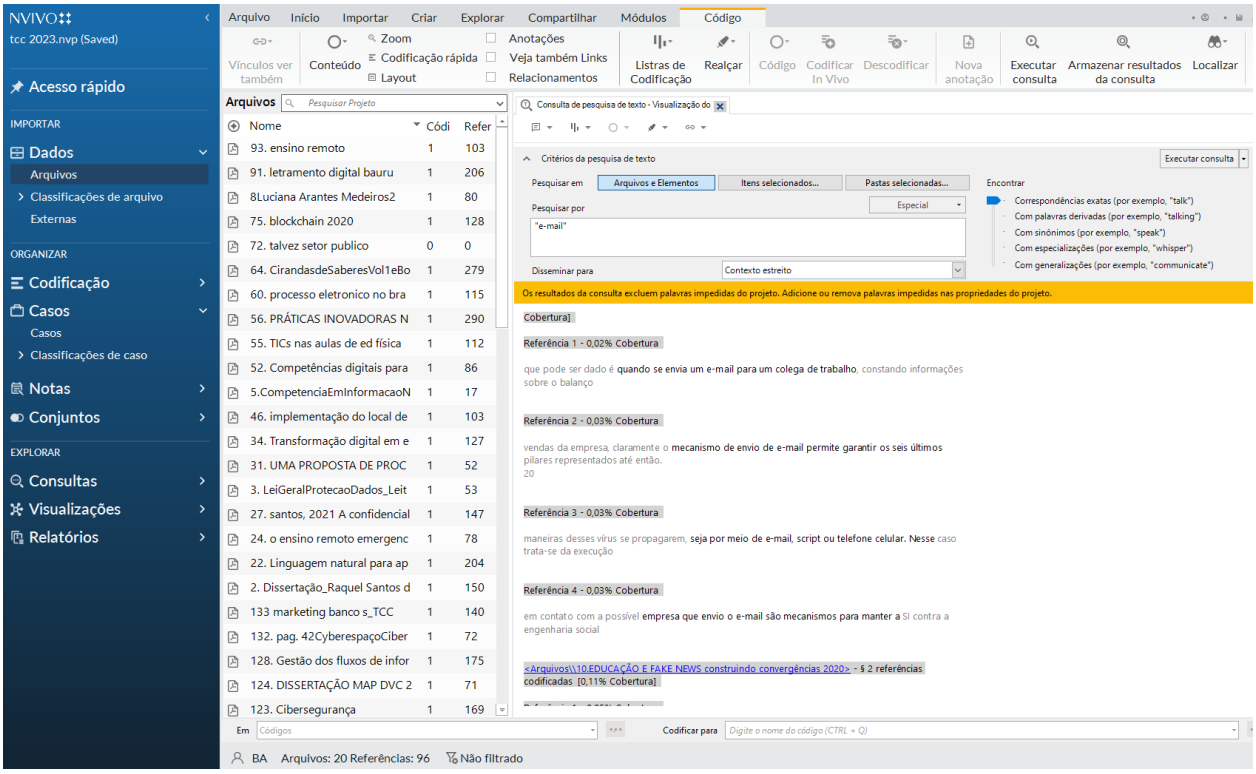
Para ser levado a sério, todo o estudo científico necessita ser rigoroso a ponto de abandonar qualquer tipo de dedução. Consoante o autor Greenhalgh (1997, p. 672, *apud* BOTELHO; CUNHA; MACEDO, 2011), o tipo de revisão bibliográfica sistemática pode ser definido como um resumo contendo “objetivos, materiais e métodos claramente explicitados”, necessitando ser conduzido de forma metodológica com clareza. Outro estudo importante abordando a revisão bibliográfica sistemática, sugere que ela seja cumprida através de sete etapas (ROTHER, 2007):

a) Pergunta principal bem construída;
b) Levantamento de estudos sobre o assunto;
c) Discernimento lógico dos estudos;
d) Levantamento de dados;
e) Análise crítica de dados;
f) Interpretação de dados;
g) Aperfeiçoamento e “upgrade” da revisão.

A pesquisa teve abordagem qualitativa, que conforme a autora Maria Oliveira, enobrece uma visão sistêmica do objeto de estudo. Se visa explicar uma totalidade da realidade através do estudo da complexidade de questões, que podem ser, por exemplo, econômicos, éticos, culturais, educacionais, entre outros (OLIVEIRA, 2012). Os artigos filtrados ficam salvos no *Mendeley Reference Manager*, onde registra-se título, autor, data, instituição, links para acesso e o PDF baixado. Este gerenciador possibilita citar as referências bibliográficas durante a escrita do trabalho, e ao final, inseri-las de uma só vez, nas Referências Bibliográficas.

Conforme a pesquisa prosseguia durante a leitura dos artigos, percebeu-se que as práticas às vezes iam se repetindo. Portanto, usou-se o software para dados qualitativos Nvivo®, permitindo a busca por palavras em diversos arquivos no formato PDF ao mesmo tempo. Abaixo, a Figura 3 apresenta uma das formas de pesquisa do Nvivo, onde à esquerda fica seu painel principal, seguido pela lista de artigos, e em boa parte da tela, o painel de buscas com os resultados abaixo. Ao clicar no link em azul no artigo, é possível abri-lo e ver onde estão os resultados de busca, caso necessite ir além da frase para conferir se o contexto faz sentido onde a prática está inserida.

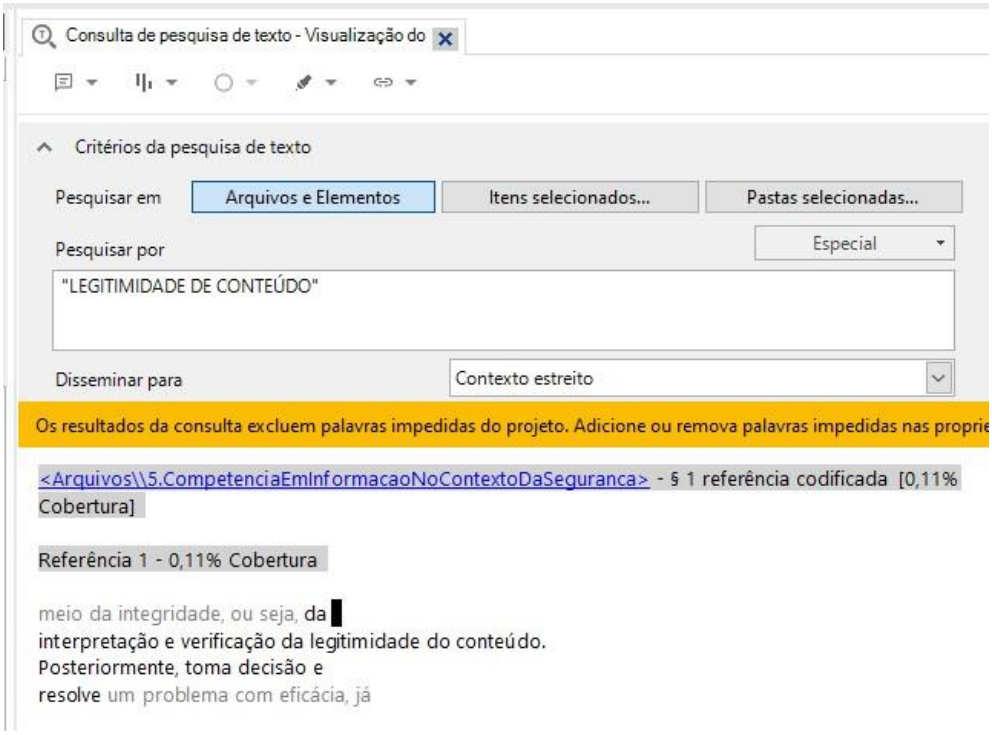
Figura 3 – Busca de práticas



Fonte: produzido pela autora (2023)

A Figura 4 a seguir demonstra como a busca por palavras-chave consegue alcançar sinônimos, sendo ideal para encontrar termos de uma só vez. Abaixo, a pesquisa alcançou termos similares, no caso, com o artigo “do”, como o termo buscado está apresentado no meio do seu próprio texto, facilita interpretar o contexto do seu uso no artigo listado, dispensando abrir o arquivo em uma parte considerável de vezes. Depois, o quadro 1 demonstra pontualmente as diferenças entre utilizar a busca simples pelo Windows e através do Nvivo.

FIGURA 4 – Busca por palavra



Fonte: produzido pela autora (2023)

Quadro 1 – Com e sem o uso do Nvivo

NVivo®	**Ferramenta de Pesquisa Windows**
Lista a palavra inserida nas frases	Lista arquivos contendo a palavra
Busca palavras similares	Apenas a palavra bruta e seu plural
Produz Nuvem de palavras	Não produz
Até mil palavras por busca	Uma palavra por busca

Fonte: produzido pela autora (2023)

Quanto mais rigor na exclusão e inclusão dos artigos do recorte, mais confiável fica o levantamento das práticas. Esta categorização criteriosa é chamada de técnica de bibliometria (AISENBERG; ROBERTO; FERNANDES, 2014), tendo seu uso especificado no Quadro 2 a seguir. Algumas imagens da planilha em Excel estão disponíveis no apêndice deste trabalho. Ao total, 17

práticas foram classificadas através de uma planilha Excel®, contendo seu ano de publicação, se eram voltadas ao setor público ou não e em quais categorias de práticas elas se inseriam.

Quadro 2 – Critérios de Seleção

Critérios de Exclusão	**Critérios de Inclusão**
Livro ou artigo pagos	Site público/livre
Problematização	Solução
Palavra citada fora de contexto[13]	Prática de Cultura ou Conscientização
Outros países[14]	Brasil
Área técnica de TI	Área da educação
Links desativados	Links existentes com PDF
Abordagem grande demais[15]	Objetividade

Elaborado pela autora (2023)

[13] Termo ou palavra apenas citados na parte bibliográfica, ou um edital estatal.
[14] Estes artigos serão aproveitados em 2.4.
[15] Soluções vagas, sem estratégias.

4.0 ANÁLISE DOS ARTIGOS COLETADOS

Este capítulo abordará o levantamento de práticas relacionadas à cultura e à conscientização de segurança da informação, de 2018 a 2022 e até agosto de 2023. Os tópicos abordarão medidas para atenuar os diversos riscos principalmente durante um expediente de trabalho, mas diversas também podem ser usufruídas para uso pessoal. À luz das análises realizadas (Apêndice), identificam-se 17 práticas em ordem alfabética.

4.1 Práticas Relacionadas à Cultura e Conscientização

- **Prática 1 - Atualização**: o Sistema Operacional, softwares e aplicativos de celular devem sempre ter a sua última versão, pois frequentemente há alguma versão com correções de seu desenvolvimento, principalmente os que servem para proteção, como antivírus, ou *anti-spyware*. “São práticas que podem dificultar ações maliciosas e evitar que o usuário vivencie danos muitas vezes irreparáveis, ocasionando não só o prejuízo pessoal como também, perda emocional” (BÉLANGER; CROSSLER, 2019 *apud* DE SOUZA, 2021, pág. 66);
- **Prática 2 - Autenticação Multifator**: também chamado de Autenticação em/por/de dois fatores ou MFA (Multifactor Autentication), costuma ser basicamente um login através de duas senhas(DE SOUZA, 2021). Mecanismos de autenticação de identidade atualmente deveriam ser indispensáveis. Existem alguns tipos que podem compor a segunda etapa, como a biométrica, com o uso de impressões digitais para acessar certos sistemas, contas em banco, etc. (BELLI et al., 2023) A autenticação por voz e facial, apesar de parecerem modernas, não são mais tão seguras devido à inteligência artificial;
- **Prática 3 - Capacitação**[16]: atualizar o usuário que já conhecimento prévio. Catorze artigos citaram como uma prática. Em Lino (2016, *apud* Silva, 2021), é ressaltada a grande importância das pessoas para lidarem com informação. A capacitação desenvolveria a conscientização, fazendo com que as práticas sejam exercidas naturalmente. Unanimemente ela é uma condição essencial

[16] A capacitação é diferente de um treinamento, pois serve para aperfeiçoar o que já se sabe, enquanto um treinamento pode ser mais completo, pois consiste em iniciar um novo assunto. A prática Treinamento é abordada em breve.

para a construção e fortalecimento da soberania digital (BELLI et al., 2023) e para buscar a independência nacional (CAETANO, 2023);

- **Prática 4 - Confidencialidade**: manter sigilo de dados. O usuário competente conhece a cultura de confidencialidade da fonte de informação e avalia seu conteúdo de maneira crítica. (OTTONICAR et al., 2020). Um bom exemplo a ressaltar é o quanto esta prática tem relação com a ética, por exemplo em hospitais onde há diversas informações de pacientes, que devem ter sua privacidade em sigilo garantidos. Há diversas situações altamente sensíveis para lidar, como procedimentos evasivos ou evolução diária de um internado, por exemplo (SANTOS, 2020). O compartilhamento de informações pessoais pode ser arriscado dependendo do ambiente, portanto, deve-se cuidar se o usuário do outro lado da tela é mesmo o funcionário que está pedindo alguma informação. Por exemplo, se o setor de Recursos Humanos entra em contato por telefone, não há como ter certeza de que é ele pedindo atualização de dados pessoais. Ou o setor de pagamentos de fornecedores está pedindo alguma relação que envolva dados pessoais, mas o e-mail não é o oficial da organização. Rigorosas restrições com relação a dados pessoais aumentar sua segurança nesses ambientes, evitando que pessoas mal-intencionadas possam fazer outro uso dessas informações em aplicações de golpes, por exemplo (DE SOUZA, 2021);
- **Prática 5 - Cookies e dados de navegação**: apenas dois artigos foram encontrados, sendo ambos de âmbito geral. São rastreadores que devem ser limpos frequentemente do navegador, e quando possível, pode ser rejeitado no momento de precisar entrar em algum site. A opção de rejeição é o ideal sempre que possível, já que nem todos os sites ainda a possuem (DE SOUZA, 2021). Usuários da internet deixam rastros, seja um histórico de likes, cadastros, visitas a sites, responder a formulários, o histórico de locais visitados salvos pelo GPS - *Global Positioning System* ou, no português, Sistema de Posicionamento Global, aceitar os cookies dos sites, dentre outros tipos de ações ao navegar no ambiente web. Esses rastros formam um corpo virtual, ou seja, a junção de características físicas do usuário, porém, do ambiente web, tornando ele um indivíduo no ciberespaço em que está sujeito a influências, por expor muito de sua vida, fazendo com que as pessoas que estão por trás esses

sites e redes sociais tenham influência sobre suas escolhas, conhecendo muitas características de sua personalidade, monitorando nossos passos por 24 horas. Um exemplo é o excesso de marketing e publicidade conforme o gosto do usuário, capturando informações de itens que podem ser atrativos para aquele usuário (LEITE, 2021);

- **Prática 6 - Disponibilidade**: “é o atributo que garante que os usuários autorizados tenham acesso à informação quando for necessária.” (SILVA, 2021) Um bom exemplo é o backup, que consiste em salvar as informações importantes do computador em outro lugar, como se fosse uma reserva caso precise. De certa forma quando os arquivos estão salvos em apenas um lugar, é como se não estivesse salvo em nenhum, pois não existe garantia de segurança de arquivos salvos somente no computador. Esta vulnerabilidade ocorre devido a possíveis defeitos que o equipamento possa apresentar (PEREIRA et al., 2020), entre outros fatores que corrompem os arquivos. (SOUZA, 2021b), (ALVES, 2021), (OTTONICAR et al., 2020). O Backup pode ser feito também quando a organização possui um centro de processamento de dados, ou seja, uma infraestrutura que armazena as informações da organização (SILVA, 2018). A disponibilidade está totalmente ligada à acessibilidade sem interferência ou obstrução, e pode depender totalmente do setor de TI. (ARANTES, 2019). Outros autores que citam o assunto: BELLI et al., (2023), CAETANO, (2023);
- **Prática 7 - DPO (Data Protect Officer)**: é um novo papel de liderança em uma companhia, o profissional encarregado pelo tratamento de dados pessoais. É responsável por encaminhar comunicações formais, fomentar a cultura, a disseminação e o conhecimento do programa ou processo de segurança de informação(ALVES, 2021). Por ser um profissional relativamente novo, pode ter formação diversa, como em direito, políticas públicas, gestão de TI. O pré-requisito, de forma geral, é ter feito algum curso na área, que pode ser desde alguma especialização a curso de média duração. Apenas dois artigos do recorte citaram a existência deste profissional. Também existe o cargo de CDO (Chief Data Officer), citado apenas por (MUNHOZ, 2022), um papel de liderança também fundamental que além de entender de LGPD, precisa ter formação na área de TI, ou ciência de dados;

- **Prática 8 - E-mail**: Cinco autores citaram alguma forma de cautela ao abrir e-mails. Mensagens com links falsos são chamados de *phishing*, que se caracteriza por motivar sem querer o fornecimento de informações confidenciais, como por exemplo confirmação de identidade, porém, no momento de fazer o login no site, ele é falso, mas aparentemente idêntico ao site original e a vítima digita sua senha inocentemente. Ou o pedido por atualizações, em geral, justificados por razões de segurança. Por fim as informações prestadas podem resultar em roubos de identidade (OLIVEIRA, 2019). Mensagens de e-mail precisam de atenção ao remetente: o serviço foi mesmo solicitado? O remetente é confiável? A informação faz sentido? Tendo qualquer suspeita, jamais deve-se clicar em links ou baixar anexos. (PALADINO, 2019) Se a informação trouxe alguma emoção, pode ser golpe;
- **Prática 9 - Gamificação**: Cinco artigos abordaram o tema, a partir de 2020. Equivocadamente o termo aparenta fazer com que uma atividade a ser ensinada seja transformada em jogo, não obstante, ela quer dizer usar técnicas e métodos de jogos dentro do processo de aprendizagem, ou seja, algo mais pontual (CILLI, 2022) como uma dinâmica que envolva cooperação ou enfrentamento de um problema(LOPES et al., 2022. Afinal, antes da “brincadeira”, ou competição, está o objetivo da aprendizagem, portanto, é muito importante deixar claro o propósito do conteúdo e da atividade (PEREIRA et al., 2020);
- **Prática 10 - Integridade**: um usuário competente sabe como usar a informação por meio da integridade, ou seja, da **interpretação e verificação da legitimidade** do conteúdo. Posteriormente, toma boas decisões e resolve um problema com eficácia, já que se baseia em fontes de informação e conteúdo de qualidade (OTTONICAR et al., 2020). Certos autores explicaram que a integridade é usar a informação com exatidão (SILVA, 2021), ou é a garantia de que uma mensagem enviada seja totalmente recebida de forma completa, ou seja, garantir a informação bem recebida. Atualmente pode-se usar o exemplo da comunicação por *whatsapp* no trabalho, onde às vezes, ocorre de a informação ter sido passada com pressa e incompleta, podendo resultar em graves problemas para a companhia;

- **Prática 11 - ISO 2700**: a norma padrão é a referência internacional para a gestão da SI, criada em 1992 na Inglaterra. Porém, no Brasil, apenas 279 organizações possuíam o certificado de garantia até 2022(ISO, 2022). Além da norma não ser obrigatória, são 114 pontos de controles de segurança que passam por uma análise rigorosa de auditoria, que pode demorar até 16 meses. Por exigir inclusive criptografia de uma organização, somente por este ponto já se pode considerar algo de alto custo de investimento, onde nem sempre uma organização possui esta possibilidade, ou prioridade. No entanto, este selo garante melhor competitividade entre organizações, pois aumentaria o seu grau de confiança tanto entre os clientes, quanto em bolsa de investimentos, etc. Apenas quatro artigos citaram a importância dele: ARANTES, (2019) OLIVEIRA, (2019), SILVA, (2021), BELLI et al., (2023);
- **Prática 12 - Letramento Digital**: assim como os seres humanos se alfabetizam pela combinação de letras, pela escrita de palavras e frases e pela interpretação de textos, conforme Cilli e Domiciano (2021 *apud* CILLI, 2022), pode-se sim comparar o letramento digital com a alfabetização, a fluência com que é feito o uso de computador ou *smartphone*. Afinal, um indivíduo que tem um bom nível de letramento digital consegue interpretar as informações digitais, prezar pela segurança da informação, identificar e aplicar padrões de comunicação, entre outras habilidades. Sem esse tipo de letramento, utilizar algo tecnológico vira uma execução, de certa forma, mecânica”(CILLI, 2022) e aumenta a vulnerabilidade do usuário;
- **Prática 13 - Normas/Códigos de condutas setorizados**: estabelecer algumas medidas para cada setor, abordando formas, maneiras de comunicações seguras, como voz, vídeo e texto(BELLI et al., 2023). Assim como Conselhos de profissionais da área de saúde, por exemplo, possuem seus códigos de ética, pode-se criar códigos de ética setorizados (SANTOS, 2020). Por exemplo: “verificar domínios de e-mail ao abri-los para saber da origem.”; “não baixar arquivos com final exe.”. Apenas cinco artigos citaram: SANTOS, (2020), SILVA, (2021), BELLI, (2023), ANDRADE, (2023), PAPPIS, (2019);
- **Prática 14 - Plano de Contingência**: também é chamado de Plano de Recuperação, tratamento de incidentes ou ERP (Enterprise Resource Planning). Mesmo se uma organização seguir todas as práticas, não é

totalmente garantido que ela não possa sofrer algum tipo de espionagem. Portanto, deve haver sempre um plano de resposta emergencial pós-desastre, e desta forma haja continuidade das atividades conforme se consiga amenizar os possíveis danos (ARANTES, 2019). Sem esta prática, o pânico pode se instaurar e acabar prejudicando toda a instituição;

- **Prática 15 - Questionário**: com perguntas abertas (LOPES et al., 2022), é importante para conhecer o grupo, uma noção do que necessitam e o que já conseguem considerar útil para a rotina de trabalho. Por exemplo, se os funcionários já sofreram ataques de hackers, ou passaram por algum constrangimento online, provavelmente valorizarão mais ainda a importância do assunto. Ou seja, se já viveram alguma forte emoção, a chance de interesse será grande. “Identificar o problema e as necessidades dos usuários antes de propor a solução”(SILVA, 2018). Quatro artigos a partir de 2020 ressaltaram a relevância de, antes de sair dizendo regras, é fundamental conhecer melhor os seus funcionários para saber qual a melhor didática, quais as práticas que são óbvias e quais que são novidade. Todos estes artigos tinham como alvo o setor público;
- **Prática 16 - Senhas fortes e seu armazenamento**: apesar de controverso, práticas identificadas em outros artigos sugerem não as armazená-las em dispositivos ou navegadores. Se, em último caso for necessário anotá-las, que seja em um local extremamente seguro (DE SOUZA, 2021). Memorização de senhas: Como já demonstrado anteriormente no capítulo 1.4, possuir senhas fracas para realizar logins em sites pode ser extremamente prejudicial para uma instituição. Portanto, é fundamental que haja a exploração de criação de senhas de qualidade, ou seja, com números, letras, *Caps Lock* ativado e símbolos etc., ou seja, diversificadas. Justamente por uma certa dificuldade geral das pessoas em memorizar senhas muito complexas, é que existe um equilíbrio. O ideal é evitar o “óbvio”, como datas de nascimento, números de telefone ou CPF e explorar associações restritamente pessoais com significados, evitando uma senha dedutivamente fácil. Portanto, pode ser importante também evitar aqueles “geradores de senha” que tentam nos ajudar, mas criam senhas bem difíceis de evitar (OLIVEIRA, 2019);

- **Prática 17 - Treinamentos**: apresentando condutas que podem ser adotadas na rotina para defesa, evitando acidentes como por exemplo, o vazamento de dados. Dentre as boas práticas podem ser citadas: informar aos colaboradores que chaves de uso ou senhas são extremamente pessoais, portanto, jamais deve-se expor senhas ou informações pessoais em papéis, murais ou “post it”. (LEITE, 2021) O treinamento visa desenvolver habilidades e competências para identificar as vulnerabilidades. Abaixo são apontados alguns tópicos específicos a serem desenvolvidos nos treinamentos (DE MELO, 2022) como:

> *“a. importância do controle de acesso;*
> *b. a importância da mesa limpa (livre de potenciais informações que possam ser usadas por pessoas mal-intencionadas);*
> *c. proteção contra pragas virtuais e códigos maliciosos;*
> *d. proteção e privacidade da informação de identificação pessoal;*
> *e. backups de rotina”.*

Treinamentos ou aulas, são fundamentais para que o ensino possa ser proveitoso ao transferir o conteúdo a se aprender, algo que não é exclusivo de estudantes. O método de Paulo Freire, por exemplo, estabelece que antes de passar qualquer conteúdo, há uma discussão com experiências prévias. Estes poderão ser utilizadas para aumentar o engajamento, motivação e aprendizagem, trazendo maior conexão com o objetivo final: aprender (PEREIRA et al., 2020).

Como forma alternativa de visualização, as 17 práticas, esmiuçadas acima, estão pontualmente resumidas no Quadro 3 abaixo:

Quadro 3 – Práticas Resumidas

Nº	**Prática**	**Resumo**
1	Atualização	Sistemas com última versão em dia
2	Autenticação Multifator	Login com duas senhas ou mais
3	Capacitação	Atualizar conhecimento do usuário
4	Confidencialidade	Sigilo forte de informações
5	Cookies	Limitar dados de navegação
6	Disponibilidade	Backup e acessibilidade
7	DPO	Líder em segurança
8	E-mail	Cautela com *phishings*
9	Gamificação	Competição e/ou cooperação

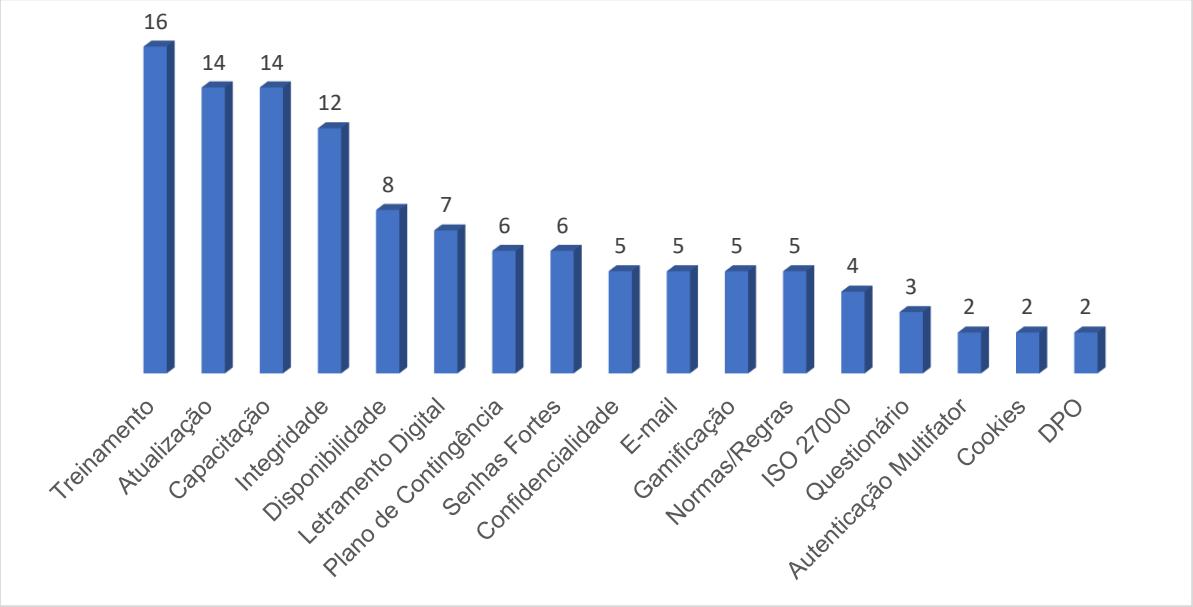
10	Integridade	Interpretar conteúdo verídico
11	ISO 2700	Implementação de norma internacional
12	Letramento Digital	Alfabetização de usuários vulneráveis
13	Normas	Regras pontuais e setorizadas
14	Plano de Contingência	Tratamento de vazamento
15	Questionário	Conhecer o público-alvo, usuário
16	Senhas	Criação complexa e memorizada
17	Treinamento	Cursos, aulas

Fonte: produzido pela autora (2023)

4.2 Comparações entre práticas de abordagem geral e setor público

A nível mundial, os governos costumam ser os principais alvos de cibercriminosos, pois há uma grande quantidade de dados que podem ser usados e vendidos. No Brasil, a União administra altos sistemas de usuários de previdência social e de registro civil, por exemplo. Desta forma, se faz necessário ter alta gestão dos dados dos cidadãos e sempre haver atualização de estudos que possam contribuir para amenizar a questão e orientar servidores, líderes e tomadores de decisão em geral. A seguir, o Gráfico 1 faz o levantamento de todas as práticas citadas anteriormente em 4.1.

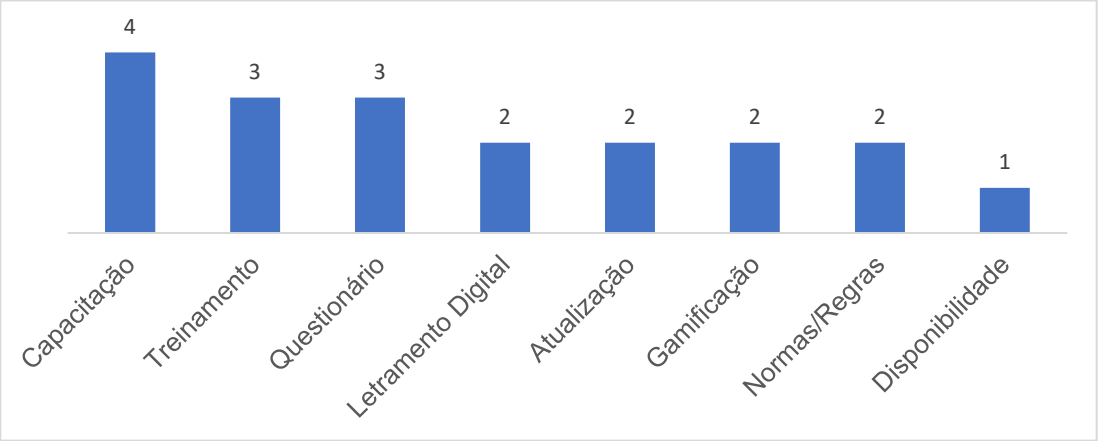
Gráfico 1 - Frequência Total das Práticas em Artigos



Fonte: Produzido pela autora (2023)

De 140 resultados do google *scholar*, foram aproveitados apenas 29. Pode-se observar que a maioria dos artigos do levantamento são de âmbito geral e que dentre as 17 práticas, apenas oito práticas das 17 foram abordadas pelo setor público, com destaque para Capacitação. Houve apenas uma prática abordada exclusivamente pelo setor público, sendo ela a aplicação de questionário, presente em três artigos, como também demonstra o Gráfico 2 abaixo:

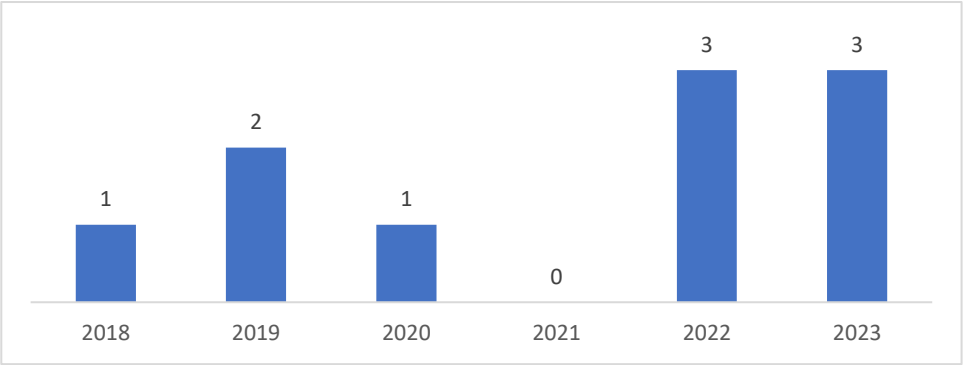
Gráfico 2: Frequência de Práticas em Setor Público



Fonte: Produzido pela autora (2023)

Em contrapartida, a maioria dos artigos foi desenvolvida por alunos de universidades públicas, principalmente as federais (a Universidade Federal do Rio Grande do Norte e a Universidade Federal de Santa Catarina continham cada uma três artigos, portanto são as de maior volume de trabalhos). Ao separar os artigos contendo práticas para o setor público por ano, conforme Gráfico 3 a seguir, percebe-se que em 2021 não há nenhuma, mas a partir de 2022, houve um aumento delas. Como 2023 está apenas em parte, é possível que este número cresça.

Gráfico 3 – Práticas por ano no setor público



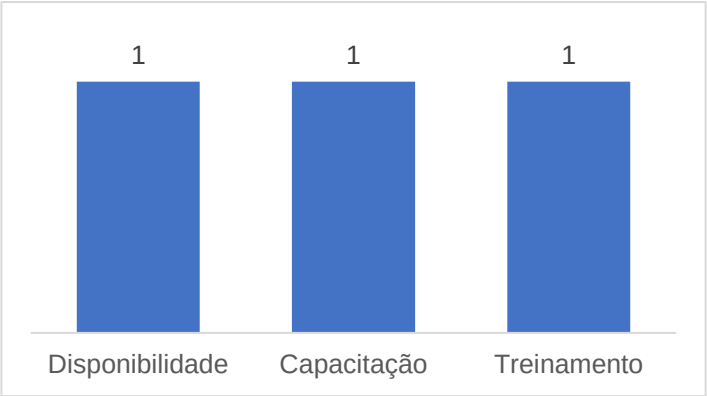
Fonte: Produzido pela autora (2023)

É importante lembrar de ataques cibernéticos que empresas públicas brasileiras sofreram nos últimos anos: a partir de 2020, por exemplo, o STJ, O Ministério da Saúde e o TSE foram vítimas. No ano de 2021 foi a vez da Copel (Companhia Estatal de Energia Elétrica do Paraná), Eletronuclear (uma subsidiária da Eletrobrás), o Tesouro Nacional e novamente o Ministério da Saúde (Folha de São Paulo, 2021). Em 2022 as vítimas divulgadas foram o Governo do Ceará e o Governo do Rio Grande do Sul. E estes foram os vazamentos divulgados que chegaram até a imprensa, porém, pode haver mais ataques que foram mantidos em sigilo.

4.3 Levantamento de Práticas por Ano

Este capítulo separa as 17 práticas encontradas em ordem decrescente nos 29 artigos pelos últimos cinco anos completos, mais parte de 2023. Abaixo, o Gráfico 4 foi o mais simples de todos, onde apenas um artigo foi encontrado, contendo ao total, três práticas direcionadas ao setor público. O autor Rodrigo da Silva da Universidade Federal do Rio Grande, realizou uma pesquisa de metodologia exploratória qualitativa sobre o uso de Processo Eletrônico (PE) na Administração Pública.

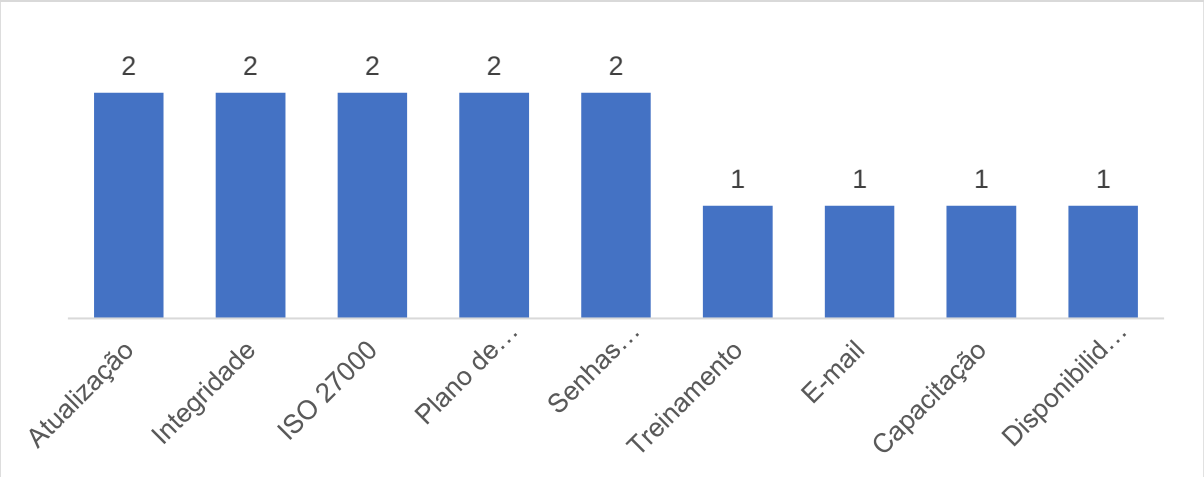
Gráfico 4 - Práticas em 2018



Fonte: Produzido pela autora (2023)

O artigo mais completo de 2019 citava oito práticas das 17. Apenas um dentre os três artigos do ano eram voltados ao setor público, sendo da autora Lisiane Pappis. O tema aborda o Plano de Desenvolvimento Institucional (PDI) na gestão universitária, da Universidade Federal de Santa Maria (UFSM), através de uma abordagem metodológica qualitativa narrativa, entrevistando os chefes de departamento. A seguir, o Gráfico 5 apresenta as nove práticas encontradas nos três artigos:

Gráfico 5 – Práticas em 2019

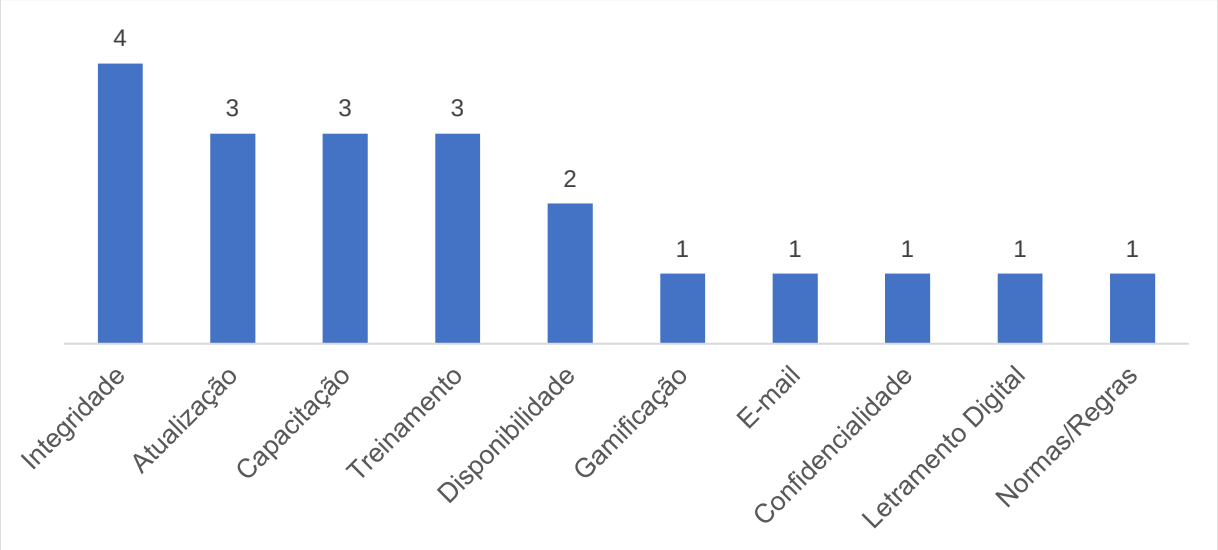


Fonte: Produzido pela autora (2023)

No ano de 2020, seis artigos foram identificados como de âmbito geral e zero voltados ao setor público. O artigo “A Confidencialidade e o Sigilo da Informação Sensível em Saúde”, por Évelin dos Santos, da Universidade Federal Da Bahia

(UFBA) foi o mais completo com seis práticas e utiliza de metodologia descritiva exploratória. A seguir, o Gráfico seis demonstra as dez práticas citadas pelo ano de 2020:

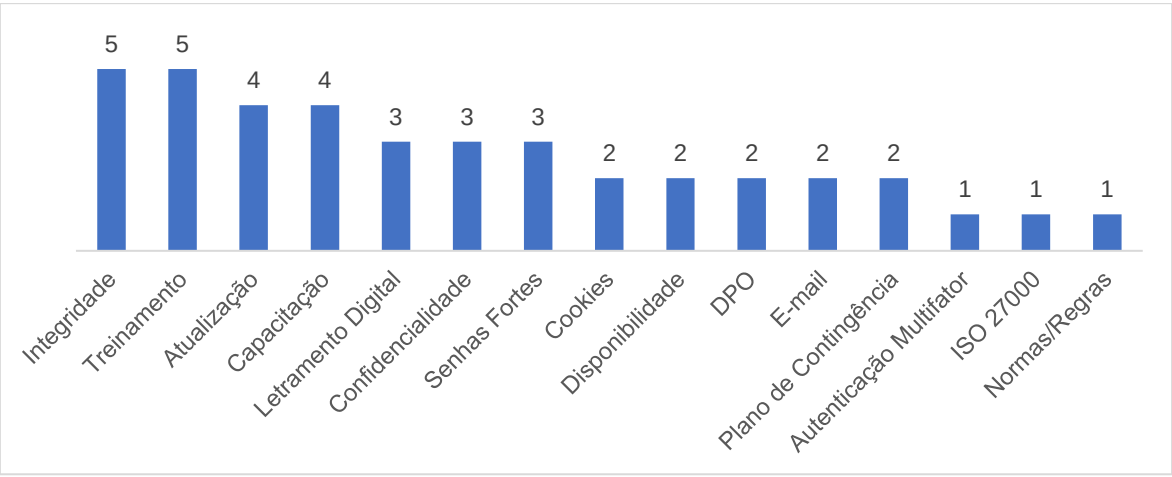
Gráfico 6 – Práticas em 2020



Fonte: Produzido pela autora (2023)

O ano de 2021 ficou entre os mais produtivos em práticas, sendo 15 das 17, com ênfase para Integridade e Treinamento, que apareceram cinco vezes cada. Todavia, nenhum dos artigos era restrito ao setor público, como demonstrado anteriormente no Gráfico 3. Abaixo, o Gráfico 7 apresenta as 15 práticas:

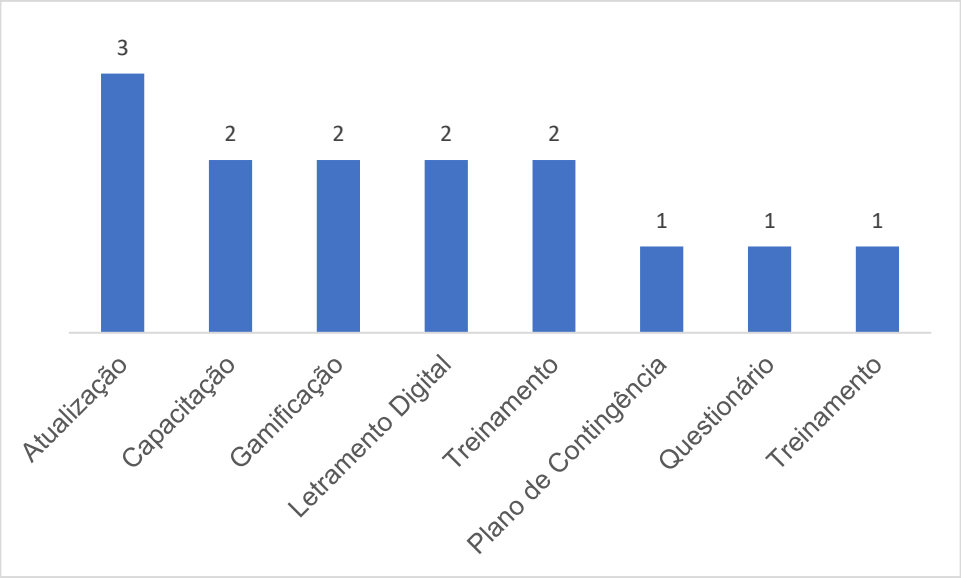
Gráfico 7 – Práticas em 2021



Fonte: Produzido pela autora (2023)

Oito práticas no total foram identificadas em 2022, sendo Atualização a de destaque, por ser a única a aparecer três vezes. Apenas um trabalho é voltado para o setor público: “O Ensino Remoto Emergencial e o Desenvolvimento de Competências Digitais na Perspectiva dos Estudantes de Administração da Universidade Federal do Rio Grande do Sul”. A autora Patrícia Joner utiliza metodologia de pesquisa exploratória de abordagem qualitativa e quantitativa.

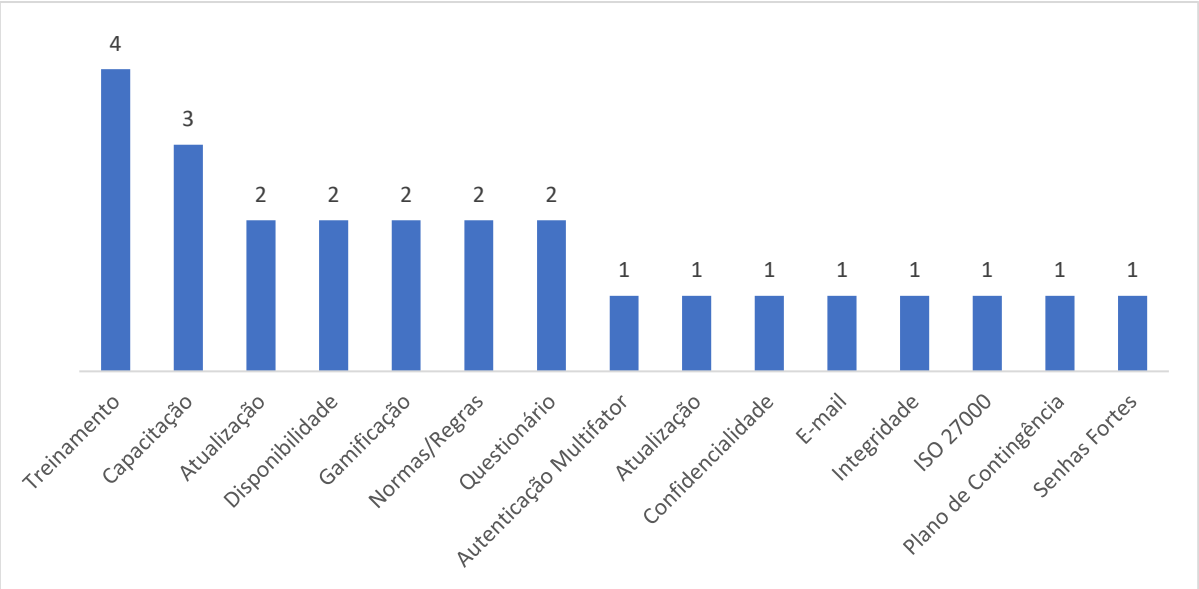
Gráfico 8 – Práticas em 2022



Fonte: Produzido pela autora (2023)

Assim como o de 2021, o ano de 2023 também conseguiu apresentar 15 práticas de âmbito geral, com apenas três artigos voltados ao setor público. Pode-se concluir que 2023 foi o ano com pesquisas direcionadas ao setor público desde 2018. A seguir, o Gráfico 9 com relevância à prática de Treinamento.

Gráfico 9 – Práticas em 2023



Fonte: Produzido pela autora (2023)

5 DISCUSSÃO DOS RESULTADOS

Percebe-se que a prática mais citada de forma geral foi treinamento, seguida de atualização e capacitação. Destaque para o artigo de Santiago (2022) sob título “Implementação do Local de Trabalho Digital”, onde a tese de doutorado foi a descrição da própria implementação de SI ocorrendo dentro de uma instituição. O estudo de caso foi caracterizado por abordar uma metodologia descritiva e interpretativa.

A autora cita que cultura desejada é responsabilidade a ser moldada pelos líderes, então eles também precisam ser preparados e ressaltou que este assunto pode trazer de forma exemplar, a real transformação cultural dentro de uma empresa de grande porte privada[17], onde ressaltou-se que a importância da confiança entre funcionários, a rigorosa responsabilidade e quais foram os resultados. A mudança cultural foi sendo incorporada até que todos os funcionários seguissem os mesmos padrões, inclusive os que trabalhassem fora da sede. “Aspectos importantes da cultura foram reforçados: confiança, ética, colaboração e o comprometimento” (SANTIAGO, 2022, pág. 84)

A Figura 5 a seguir representa um levantamento das palavras mais citadas neste recorte de cultura e conscientização, de 2018 a 2023. Pode-se concluir que estes os artigos coletados estão inclinados à área de ensino e boa parte foi elaborada por uma universidade federal:

[17] A autora não citou o nome da organização.

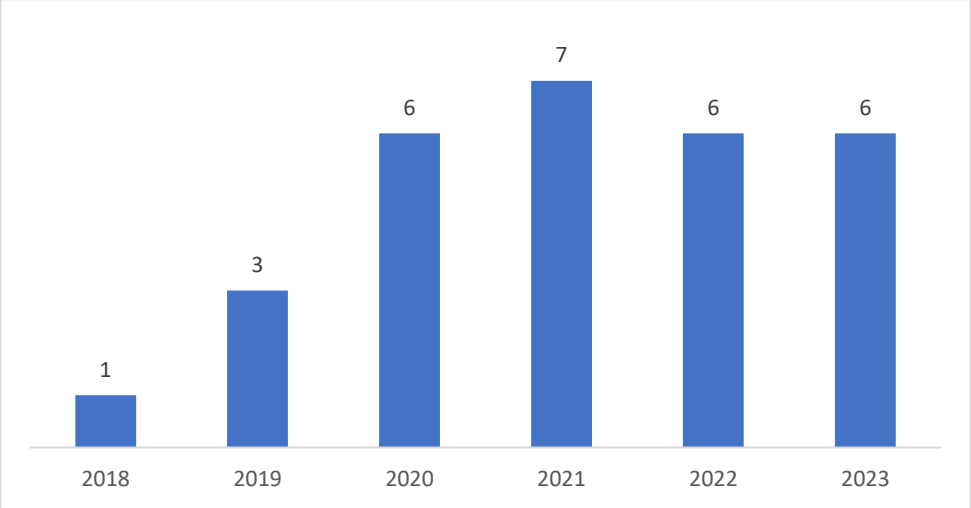
FIGURA 5 – Nuvem de Palavras

Fonte: Produzido pela autora (2023)

Comparando a Revisão de Literatura com a Análise dos Artigos Coletados, encontrou-se praticamente as mesmas ações de segurança. Vezes seguidas, citadas algumas características básicas de segurança, sendo elas: Confidencialidade, Integridade, Disponibilidade e Autenticidade.

Os artigos que mais se destacaram citando práticas foram o da Fundação Getúlio Vargas (FGV), por Belli *et al*., publicado em agosto de 2023 e o da autora Souza, de 2021. O primeiro é um robusto levantamento de práticas de cibersegurança, porém não aborda aplicação de questionário, não cita a importância de administrar os cookies e não levanta a prática de se ter um DPO ou CDO. O segundo artigo de grande qualidade, inclui levantamento de práticas a nível internacional, mas razoavelmente desatualizado (de 2021). Consoante o Gráfico 9, percebe-se que o tema explorado neste trabalho provavelmente recebeu mais atenção devido a pandemia iniciada em 2020.

Gráfico 9 –Divisão dos 29 artigos ao decorrer dos anos pesquisados



Fonte: Produzido pela autora (2023)

A prática autenticação multifator costuma envolver mais de uma senha, podendo também ser usado um token para gerar a secundária. Em 2023, a Microsoft começou a citar a “tokenização”, que quer dizer a substituição de senhas para logins. Porém, o problema de usar esta prática será quando uma pessoa tiver seu token furtado, ou perdê-lo. Então ela talvez seja uma prática sempre questionável.

Certos artigos trouxeram ótimos modelos como o levantamento bibliográfico de implementação de sistemas de gestão de segurança da informação em diferentes hospitais. O sucesso consegue se concretizar quando todos os envolvidos percebem a importância de se protegerem de ameaças reais (CIPRIANO, 2020) e o aperfeiçoamento é constante.

6 CONSIDERAÇÕES FINAIS

Uma prática nova, mas que não foi encontrada nos artigos, foi a chamada Higiene Digital. Conforme o programa de atualização corporativa *Microsoft Tabletop Exercise*[18], episódio 2, em 19 de abril de 2023, a palavra prática de segurança pode ou não ser adotada, portanto, precisa-se usar o termo “higiene digital”, ou seja, algo que é de rotina obrigatória. Se aconselha apagar arquivos inúteis da memória e atualizar aplicativos frequentemente. Porém, ao tentar usar esta palavra na ferramenta de busca, a palavra higiene digital é caracterizada no contexto de afastar-se temporariamente da internet. Também foi afirmado o seguinte lema sobre segurança: “preparar é melhor do que remediar” (Informação Verbal).

Por conseguinte, já se pode perceber que há alta complexidade de formas para lidar com a gestão da segurança da informação. A revisão sistemática integrativa foi bem estruturada conforme a proposta em 3.2. Não existe uma única solução para os problemas e a cultura e a conscientização precisam estar em todos os espaços de uma organização:

> “Das três camadas de segurança existentes: física, lógica e humana, a camada humana é a mais difícil de se avaliar. os riscos e gerenciar a segurança, pois envolve o fator humano, com características psicológicas, socioculturais e emocionais, que variam de forma individual” (Schneier, 2001 *apud* Paulo Aramuni; Maia, 2018).

O Cubo de McCumber não foi encontrado em qualquer momento da fundamentação teórica (Explicado na Figura 1, página 15), o que leva a concluir que aparenta ser mais utilizado pela área da TI. Acontece que dentre suas faces, havia uma separação de alguns conceitos. No entanto, durante a fundamentação, esta separação não ocorreu de forma tão rigorosa, trazendo a proximidade com que a disponibilidade, integridade e confidencialidade façam totalmente parte da cultura da segurança da informação, não sendo uma parte separada apenas para o setor de Tecnologia da Informação.

O Planejamento voltado à segurança da informação deve ser constante para instituições:

> “Desenvolver, documentar, atualizar periodicamente e implementar planos de segurança para sistemas de informação organizacionais que descrevam os controles de segurança instalados ou planejados

[18] Os exercícios eram disponibilizados apenas para e-mails corporativos no Brasil.

> para os sistemas de informação e as regras de comportamento para indivíduos que acessam os sistemas de informação”(ARANTES, 2019, pág. 23).

É evidente que a reputação das instituições e organizações é alterada com este novo crime organizado (como foi explicado na página 17), porém este Trabalho de Conclusão não teve o objetivo de problematizar e trazer medo quanto ao assunto, mas sim trazer soluções viáveis para colaboradores se protegerem. A cultura organizacional tornou-se um requisito estratégico importantíssimo que deve ser estimulado de forma permanente (SILVA; SILVA, 2020), pois isso além de proteger a própria organização, preserva as informações dos clientes, ou usuários.

Este trabalho conseguiu acatar as sete etapas da revisão bibliográfica sistemática apontados por Rother (2007), pois há pergunta uma principal, o levantamento de estudos sobre o assunto encontra-se na parte dois e quatro, o discernimento lógico está em praticamente todo o trabalho, o levantamento de dados e sua análise crítica está em 4.2, 4.3 e 5. A interpretação dos dados está em 5 e 6 e o aperfeiçoamento está a seguir.

Sobre este tema de pesquisa possuir limitações é que se espera de instituições a existência de medidas sigilosas que não devem jamais ser divulgadas em nome da segurança, portanto, impossíveis de abordar. Também infelizmente foi nítida a grande quantidade de artigos no recorte que foram descartados por falta de clareza ao abordar as práticas de forma real. Outra limitação relevante é não ter cursado anteriormente uma graduação na área de tecnologia, o que favoreceria a capacidade no recorte da pesquisa e base no assunto, pois pode ser que alguém vindo da área da Tecnologia da Informação tenha outras referências bibliográficas, apesar do tema ser transversal.(BELLI et al., 2023)

A partir desta pesquisa, sugerem-se outras futuras:

a) levantamento de práticas sugeridas diretamente dos sites de bancos, ou redes sociais dos bancos;
b) mapeamento de medidas sugeridas pelos sites de segurança, como de antivírus;

c) estudos de caso de implementação de práticas pode ter um recorte apenas do setor público;
d) aplicação da Norma Internacional ISO 2700 voltada para o setor público e quem já aderiu (No Scholar há apenas dois resultados de artigo), zero na scielo.

REFERÊNCIAS

AISENBERG, H.; ROBERTO, F.; FERNANDES, F. **Passo-a-passo para construção da Revisão Sistemática e Bibliometria Utilizando a ferramenta Endnote®**. Instituto de Gestão do Conhecimento e Inovação. Santa Catarina. 2014. Disponível em: https://revistaacb.emnuvens.com.br/racb/article/view/1194/pdf Acesso em: 05 set. 2023

ALVES, G. B. **Uma Proposta de Processo de Gerenciamento de Riscos Baseado na LGPD**. Goiânia: PUC Goiás, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/3731/1/TCC%202%20final%20-%20Guilherme%20Barbosa%20Alves.pdf Acesso em 17 jul. 2023

ARAMUNI, J.; CLÁUDIO MAIA, L. **O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa**. Minas Gerais: Universidade FUMEC, 2018. Disponível em: http://revistas.ufpr.br/atoz/about/submissions#copyrightNotice. Acesso em: 19 jul. 2023.

ARANTES, L. **RELAÇÕES À VIOLAÇÃO INDIVIDUAL DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO**. São Bernardo do Campo/SP: Universidade Metodista de São Paulo, 2019. Disponível em: http://tede.metodista.br/jspui/bitstream/tede/1898/2/Luciana%20Arantes%20Medeiros2.pdf Acesso em: 14 jul. 2023

Axur **Atividade criminosa online no Brasil.** Disponível em: https://blog.axur.com/pt/relat%C3%B3rio-da-atividade-criminosa-online-no-brasil-q4-2020 acesso em: 19 nov. 2023

BARRETO, G. G.; SUCUPIRA, A. L.; LIMA, A. G. B. *et al.* **Governança em Privacidade e Proteção de Dados:** Uma Visão Integrada Aos Negócios Empresariais. SERPRO. Curitiba: Editorial Casa, 2022. Disponível em: https://images.serpro.gov.br/Web/ServicoFederalDeProcessamentoDeDadosSerp/%7Bfc9495bc-e309-4515-be23-e808d0dbfca9%7D_Livro_Governan%C3%A7a_em_PPD_-_uma_vis%C3%A3o_integrada_aos_neg%C3%B3cios_empresariais_compressed.pdf?utm_campaign=Livro_Governanca_e_privacidade-%20Link%20p Acesso em 09 nov. 2023

BELLI, L. *et al*. **Cibersegurança:** uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. Rio de Janeiro: Fundação Getúlio Vargas, 2023. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/33784 Acesso em: 12 ago 2023

BOTELHO, L. L. R.; CUNHA, C. C. DE A.; MACEDO, M. **O Método da Revisão Integrativa nos Estudos Organizacionais**. Gestão e Sociedade, v. 5, n. 11, p. 121, 2011.
BRASIL, 1988. Lei Federal nº 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
Acesso em: 07 nov. 2023

BRASIL, 1988. Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm
Acesso em: 09 nov. 2023.

BRASIL, 1988. **DECRETO 10.222.** 05 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 09 nov. 2023.

Brasil. **Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos**.2022. Disponível em: https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos Acesso em: 07 nov. 2023

CAETANO, J. V. F. **Ciberespaço, Cibersegurança e os Desafios da Implantação da Tecnologia 5g no Brasil**. Uberlândia/MG: Universidade Federal de Uberlândia, 2023. Disponível em: https://repositorio.ufu.br/handle/123456789/37481 Acesso em: 16 ago. 2023

CETIC.BR. **TIC Domicílios 2020**. São Paulo: Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, 2021. Disponível em: https://cetic.br/pt/tics/domicilios/2020/domicilios/ Acesso em: 07 nov. 2023

CILLI, T. L. B. Jornada ao Virtual: **O design de um Framework para Desenvolvimento de Objetos de Aprendizagem em Realidade Virtual na Modalidade Fotografia em 360°**. Bauru: Universidade Estadual Paulista, 2022. Disponível em: https://www.bdtd.ibict.br/vufind/Record/UNSP_9905b54476506ea6ef3bcaeaafd12cdd Acesso em: 14 ago. 2013.

CIPRIANO, W. F. **A Segurança da Informação com o Advento da Internet das Coisas em Ambientes Hospitalares**: uma abordagem bibliográfica. Salvador: UNIS-MG, 2020. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/9237/1/CGAEM_2021_1_majcipriano.pdf. Acesso em: 28 jun. 2023.

CloudSEK, 2023. **Global Threat Landscape Report 2021-2022**. Singapura: CloudSEK, 2023. Disponível em: https://uploads-ssl.webflow.com/635e632477408d12d1811a64/63e32e242a73c87f1f973ee9_Global%20Threat%20Landscape%20Report%202021-%202022.pdf Acesso em: 07 nov. 2023

FEBRABAN. **FEBRABAN assina acordo de cooperação com Polícia Federal para repressão a crimes cibernéticos**. 2022. Disponível em: https://portal.febraban.org.br/noticia/3773/pt-br/. Acesso em: 07 nov. 2023

FRANCISCO, D.; TOMAZ, M. 1,RIBEIRO,.**Uso dos Frameworks na Gestão de Riscos de Segurança da Informação.** São Paulo: Fatec Mococa, 2021. Disponível em: https://congresso.fatecmococa.edu.br/index.php/congresso/article/view/325/98. Acesso em: 28 jun. 2023

FURTADO NETO, JOÃO J.; MISAGUI, DR. M. **Plano de Recuperação de Desastres em TI com Foco no ERP.** Santa Catarina: Unisociesc, 2021. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/14677. Acesso em: 2 jul. 2023.

Folha de São Paulo. **Governo Brasileiro e Estatais na Mira dos Hackers.** 2021.Disponível em: https://fotografia.folha.uol.com.br/galerias/1690766956288555-governo-sob-ataque-%20hacker#foto-1690768542638231. Acesso em: 07 nov. 2023

GALVÃO, A. P. **A informação como commodity: mensurando o setor de informações em uma nova economia.** Rio de Janeiro: Universidade Federal do Rio de Janeiro, 1999. Disponível em: https://www.scielo.br/j/ci/a/S6nQWWnxJf8G7FgjHNsdwMd/?lang=pt&format=html#. Acesso em: 5 nov. 2023

GALVÃO, M. C. **Fundamentos em segurança da informação**. São Paulo: Pearson, 2015. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 09 nov. 2023.

GEORG, M. A. C. *et al.* **Os Desafios da Segurança Cibernética no Setor Público Federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação**. Universidade de Brasília. Revista Ibérica de Sistemas e Tecnologia de Informação, p. 602–616, 2023. Disponível em: https://www.researchgate.net/publication/370189315. Acesso em: 09 nov. 2023

Hive Systems. **Are Your Passwords in the Green?** 2023. Disponível em: https://www.hivesystems.io/blog/are-your-passwords-in-the-green?utm_source=footer Acesso em: 07 nov. 2023

ISO Survey. International Organization for Standardization (ISO), The ISO Survey 2022. Disponível em:

https://www.iso.org/committee/54998.html?t=KomURwikWDLiuB1P1c7SjLMLEAgXOA7emZHKGWyn8f3KQUTU3m287NxnpA3DIuxm&view=documents#section-isodocuments-top

LEITE, L. M. **Políticas De Segurança Física E Lógica De Tecnologia Da Informação Em Redes De Computadores E Seus Ativos**. Curitiba: Universidade Tecnológica Federal do Paraná, 2018. Disponível em: https://riut.utfpr.edu.br/jspui/bitstream/1/17306/1/CT_GESER_X_2018_04.pdf . Acesso em: 29 jun. 2023.

LEITE, V. R. **Lei Geral De Proteção De Dados (LGPD): Características e Aplicações na Biblioteconomia e Ciência da Informação**. Natal: UFRN, 2021. Disponível em: https://repositorio.ufrn.br/handle/123456789/41518 Acesso em: 14 jul. 2023.

LEMOS II, D. L. **Tecnologia Da Informação**. Florianópolis: Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina 2011. Disponível em: https://educapes.capes.gov.br/bitstream/capes/206391/2/CST%20GP%20-%20Tecnologia%20da%20informa%C3%A7%C3%A3o%20-%20MIOLO.pdf. Acesso em: 09 nov. 2023

LEMOS, Ronaldo. **O Vazamento do Fim do Mundo.** Folha UOL. 31 de jan 2021. Disponível em: https://www1.folha.uol.com.br/colunas/ronaldolemos/2021/01/o-vazamento-de-dados-do-fim-do-mundo.shtml Acesso em: 10 abr. 2022.

LIMA, T. M. L. **Administração Pública Digital**: estudo sobre a constitucionalidade da implementação da blockchain pelo Instituto Nacional da Propriedade Industrial. Natal/RN: Universidade Federal do Rio Grande do Norte, 2020. Disponível em: https://repositorio.ufrn.br/handle/123456789/31386. Acesso em: 10 ago. 2023.

LOPES, M. *et al*. **Relato de Experiência Docente:** curso remoto sobre metodologias ativas de aprendizagem para formação docente em meio a pandemia. em: Práticas Inovadoras no Ensino das Ciências: experiências e olhares docentes. 1. ed. Chapadinha, MA: Alfa Ciência, 2022. v. 1p. 129–150. Disponível em: https://www.researchgate.net/publication/365476459. Acesso em: 09 nov. 2023

MACHADO, T. **Prevenção de Fraudes em Bancos Comerciais.** Cerro Largo, RS: Universidade Federal da Fronteira Sul, 2018. Disponível em: https://rd.uffs.edu.br/handle/prefix/4880 Acesso em: 09 nov. 2023

MAGNO, P. G. S. **Contrastes Entre a Atual Situação da Segurança da Informação Nacional e as Medidas Governamentais Tomadas**: uma análise dos mais recentes ataques cibernéticos no Brasil. São Luís/MA: Centro Universitário Dom Bosco, 2022. Disponível em: http://repositorio.undb.edu.br/handle/areas/770 Acesso em: 09 nov. 2023

MARINHO, R. A., Bodê, J. **Gamificação Aplicada a Programas e Campanhas de Conscientização de Segurança da Informação**. Fatec Americana - - Congresso de Segurança da Informação 2022. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/50/19 Acesso em: 09 nov. 2023

MELO, A. O. **As Fake News e seu Potencial Risco Para a Segurança de Ativos Informacionais Pessoais**. Natal, RN: Universidade Federal do Rio Grande do Norte, 2022. Disponível em: https://repositorio.ufrn.br/bitstream/123456789/46282/1/FakeNewseSeuPotencialRisco_Melo_2022.pdf. Acesso em: 2 jul. 2023.

Microsoft Security. **Microsoft Cybersecurity Tabletop Exercise.** 2023. Disponível em: https://info.microsoft.com/LA-DAT-VDEO-FY23-08Aug-27-Microsoft-Cybersecurity-Tabletop-Exercise-SRGCM7646_LP01-Registration---Form-in-Body.html Acesso em: 07 nov. 2023

MORAES, L. DE; HAMBURGO, N. **CTF: um estudo teórico e prático para construção de conhecimento na área de segurança da informação**. Novo Hamburgo: UNIVERSIDADE FEEVALE, 2020. Disponível em: https://tconline.feevale.br/tc/files/0002_5215.pdf. Acesso em: 28 jun. 2023.

MUNHOZ, V. T. **Transformação Digital em Empresas do Agronegócio Brasileiro**: quais são os desafios e o papel da área de TI nesta jornada? São Paulo: Insper, 2022. Disponível em: https://repositorio.insper.edu.br/handle/11224/5722 Acesso em: 22 nov. 2023

MUSICH, P. **Maintaining Data Protection in a Hybrid, Multi-Cloud World**. IBM, 2023. Disponível em: https://www.ibm.com/downloads/cas/ANGVYBQ9 Acesso em: 07 nov. 2023

NETO, P. T. M.; ARAÚJO, W. J. **Segurança da Informação - uma visão sistêmica para implantação em organizações.** João Pessoa, PB: Editora UFPB, 2020. Disponível em: http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/book/209 Acesso em: 07 nov. 2023

OECD. **A Caminho da Era Digital no Brasil: revisões da OCDE sobre a transformação digital.** Paris: OECD Publishing, 2020. Disponível em: https://doi.org/10.1787/45a84b29-pt . Acesso em: 15 out. 2023.

OLIVEIRA, D. **BYOD: práticas de gestão de segurança da informação para smartphones em órgãos públicos**. 2019. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/3673 Acesso em: 09 nov. 2023.

OLIVEIRA, J. **Segurança e defesa cibernética: um estudo do caso brasileiro à luz de países nórdicos e Estôni**a. Brasília: Universidade de Brasília, 2021. Disponível em: http://icts.unb.br/jspui/bitstream/10482/42264/1/2021_RaquelCristinaJorgedeOliveira.pdf. Acesso em: 18 jul. 2023.

OLIVEIRA, M. M. DE. **Como fazer pesquisa qualitativa**. Rio de Janeiro, RJ. Editora Vozes, 2012.

OLIVEIRA, R. S**. Engenharia Social e Segurança da Informação: análise das questões relacionadas ao uso das redes sociais online**. Niterói/RJ: Universidade Federal Fluminense, 2019. Disponível em: https://app.uff.br/riuff/bitstream/handle/1/10890/Disserta%c3%a7%c3%a3o_Raquel%20Santos%20de%20Oliveira.pdf?sequence=1&isAllowed=y Acesso em: 14 jul. 2023

OTTONICAR, S. L. C. *et al.* **Competência em Informação no Contexto da Segurança da Informação**: modelo teórico-conceitual para o uso seguro da informação. Revista ACB, v. 25, n. 3, p. 477–492, São Carlos, Universidade Federal de São Carlos, 2020. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7700561 Acesso em: 14 jul. 2023

PALADINO, T. **Segurança da Informação**: 8 Dicas Práticas Para Usuários., 2019. Disponível em: https://blog.diferencialti.com.br/seguranca-da-informacao-praticas-para-usuarios/. Acesso em: 24 jul 2020.

PEREIRA, C. A. R. *et al*. **Suporte ao Ensino Remoto: Metodologias Ativas de Aprendizagem e Avaliação Formativa.** Disponível em: https://pantheon.ufrj.br/bitstream/11422/12914/3/SUPORTE_AO_ENSINO_REMOTO_2versao.pdf Acesso em: 19 jul. 2023.

PINHEIRO, N.; SILVA, R. **Uso da Tecnologia na solução de crimes virtuais e Boas práticas de segurança de informação**. Revista Tecnologias em Projeção, v. 9, n. 1, p. 9, 2018. PROCERGS. Política de segurança da informação. p. 17, 2017. Disponível em: https://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/view/1358/0 Acesso em: 09 nov. 2023

RODRIGUES, Y. J. M. **Segurança da informação aos jovens: uma cartilha sobre arquivos e dados pessoais.** São Paulo: Faculdade de Tecnologia de São Caetano do Sul, Antônio Russo, 2020. Disponível em: http://ric-cps.eastus2.cloudapp.azure.com/bitstream/123456789/5260/1/07_Baitz_20200630.pdf Acesso em: 09 nov. 2023

ROTHER, E. T. **Revisión Sistemática X Revisión Narrativa**. Acta paulista de enfermagem, 20, v-vi., v. 20, n. 3, p. 360, 2007. Disponível em: https://www.scielo.br/j/ape/a/z7zZ4Z4GwYV6FR7S9FHTByr/?lang=es. Acesso em: 09 nov. 2023

SANTIAGO, C. DE F. **Implementação do Local de Trabalho Digital: um estudo exploratório em uma grande empresa de tecnologia**. São Paulo, SP: FGV, 2022. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/31658 Acesso em 09 nov. 2023

SANTOS, É. C. **A Confidencialidade e o Sigilo da Informação Sensível em Saúde**: importância de normas e procedimentos para o acesso ao prontuário do paciente nas instituições de saúde universitárias. Salvador/BA: Universidade Federal da Bahia, 2020. Disponível em: https://repositorio.ufba.br/handle/ri/33744 Acesso em: 14 ago. 2023.

SANTOS, P. C.; ALMEIDA, M. E. B. T. M. P. DE. **Educação e Fake News: construindo convergências**. Revista Exitus, v. 10, p. e020057, 30 jul. 2020. Disponível em: http://educa.fcc.org.br/scielo.php?script=sci_arttext&pid=S2237-94602020000100114 Acesso em 09 nov. 2023

SILVA, E. F.; SILVA, A. F. **Informação na Sociedade Contemporânea.** Florianópolis, SC: Rocha Gráfica e Editora Ltda., 2020. Disponível em: https://repositorio.ufrn.br/handle/123456789/31021 Acesso em: 17 set. 2023.

SILVA, I. M. P. **Segurança da Informação e o Bibliotecário**: um guia prático. Natal: Universidade Federal do Rio Grande do Norte, 2021. Disponível em: https://repositorio.ufrn.br/bitstream/123456789/44651/1/SegurancaInformacaoBibliotecario_Silva_2021.pdf Acesso em: 14 jul. 2023

SILVA, R. B. **Processo Eletrônico no Brasil:** um estudo sobre facilitadores, inibidores e benefícios da sua adoção. Rio Grande, RS: Universidade Federal do Rio Grande do Norte, 2018. Disponível em: https://repositorio.furg.br/handle/1/7907 Acesso em: 18 jul. 2023

SOUSA, J. S. **Práticas De Segurança Da Informação Em Cooperativas De Crédito Por Meio Do Modelo Cobit5.** 2019.
State of the Cloud de 2020. **Flexera**,2020. Chicago. Acesso em: 07 nov. 2023. Disponível em: https://www.flexera.com/about-us/press-center/flexera-releases-2020-state-of-the-cloud-report

SOUZA, S. T. C. **Linguagem Natural para Apoio ao Reconhecimento de Usuários em Ambientes Virtuais de Ensino e Aprendizagem**. Araranguá: UFSC, 2021. Disponível em: https://app.uff.br/riuff/bitstream/handle/1/10890/Disserta%c3%a7%c3%a3o_Raquel%20Santos%20de%20Oliveira.pdf?sequence=1&isAllowed=y Acesso em: 14 de jul de 2023

SUBA, A. L. S. **Metodologia para institucionalização de Normas.** Curitiba: Universidade Tecnológica Federal do Paraná, 2020. Disponível em: https://repositorio.utfpr.edu.br/jspui/bitstream/1/26450/1/CT_COTEL_2020_1_04.pdf Acesso em: 07 nov. 2023.

TEIXEIRA, E. C. **O Papel das Políticas Públicas no Desenvolvimento Local e na Transformação da Realidade**. Bahia: AATR-BA, p. 1–11, 2002. Disponível em: http://dhnet.org.br/dados/cursos/aatr2/a_pdf/03_aatr_pp_papel.pdf

VIANNA, E. W. **Segurança da informação digital: proposta de modelo para a Ciber Proteção nacional**. Brasília, DF: Universidade de Brasília, 2019. Disponível em: https://repositorio.unb.br/bitstream/10482/35253/1/2019_EduardoWallierVianna.pdf Acesso em: 07 nov. 2023

Tribunal de Contas da União. **Estratégia de Fiscalização do TCU**. 2021. Brasília. Disponível em: https://portal.tcu.gov.br/estrategia-de-fiscalizacao-do-tcu-em-seguranca-da-informacao-e-seguranca-cibernetica-2020-2023.htm Acesso em: 07 nov. 2023

APÊNDICE A - Quadro 4 - Parte do Levantamento em Excel

TÍTULO	AUTOR	ANO	INSTITUIÇÃO/EMPRESA	AMBITO	P1	P2	P3
PROCESSO ELETRÔNICO NO BRASIL: UI	da Silva RB	2018	Universidade Federal do Rio Gr	Setor Público			Capacitaçã
RELAÇÕES À VIOLAÇÃO INDIVIDUAL DE	Arantes L	2019	Universidade Metodista de São	Geral	Atualização		
Engenharia Social e Segurança da Informa	Oliveira RS	2019	Universidade Federal Fluminen	Geral			Capacitaçã
A CONFIDENCIALIDADE E O SIGILO DA IN	dos Santos ÉC	2020	Universidade Federal da Bahia	Geral	Atualização		Capacitaçã
Educação e fake news: construindo conve	Santos PC,de Almeida ME	2020	Revista Exitus	Geral			
SUPORTE AO ENSINO REMOTO: METODO	Pereira CA,Araújo FS,de E	2020	Universidade Federal do Rio de	Geral			
ADMINISTRAÇÃO PÚBLICA DIGITAL: estu	de Lima TM	2020	Universidade Federal do Rio Gr	Geral			
COMPETÊNCIA EM INFORMAÇÃO NO CO	Ottonicar SL,Brito JF,Silva	2020	Revista ACB (Associação Catar	Geral	Atualização		Capacitaçã
Ciberespaço e Segurança Cibernética: as	Rê E	2021	Universidade Federal de Santa (	Geral			Capacitaçã
Competências digitais para a educação: M	Bereta JS	2021	Universidade Federal de Santa (	Geral	Atualização		Capacitaçã
UMA PROPOSTA DE PROCESSO DE GER	Alves GB	2021	PUC Goiás	Geral			
MODELO DE COMPETÊNCIA DOCENTE D	dos Santos Perin E,Freita	2021	Universidade Federal do Paraná	Geral	Atualização		Capacitaçã
LEI GERAL DE PROTEÇÃO DE DADOS (LG	Leite VR	2021	Universidade Federal do Rio Gr	Geral			
SEGURANÇA DA INFORMAÇÃO E O BIBLI	da Silva IM	2021	Universidade Federal do Rio Gr	Geral	Atualização		Capacitaçã
A UTILIZAÇÃO DE TIC'S COMO FERRAME	Fernandes VB	2022	Centro Universitário Vale do Cri	Geral			
RELATO DE EXPERIÊNCIA DOCENTE: CU	Lopes M,Lima F,Pereira R	2022	Editora Alfa Ciência	Geral	Atualização		
Jornada ao Virtual: O design de um framev	Cilli	2022	Universidade Estadual Paulista	Geral	Atualização		
IMPLEMENTAÇÃO DO LOCAL DE TRABAL	de Farias Santiago C	2022	Fundação Getúlio Vargas	Geral			
TRANSFORMAÇÃO DIGITAL EM EMPRES/	Munhoz VT	2022	Insper	Geral	Atualização		Capacitaçã
CIBERESPAÇO, CIBERSEGURANÇA E OS	Caetano JV	2023	Universidade Federal de Uberlâ	Geral			
Cibersegurança: uma visão sistêmica rum	Belli L,Franqueira B,Bako	2023	Fundação Getúlio Vargas	Geral	Atualizaçã	Autenticação Mult	Capacitaçã
MARKETING NA ERA DIGITAL NO SETOR	Santos BS	2023	Universidade Federal de Sergip	Geral			
GESTÃO DOS FLUXOS DE INFORMAÇÃO	Andrade D	2023	Universidade Estadual Paulista	Setor Público			Capacitaçã
Inclusão dos Servidores Públicos do Minis	do Carmo DV	2023	Fundação Getúlio Vargas	Setor Público	Atualização		Capacitaçã
PIBID em Computação: desafios, estratégi	Rodrigues AN,Mário C,Ro	2023	Universidade de Pernambuco	Setor Público			
O ENSINO REMOTO EMERGENCIAL E O D	de Maria Joner P	2022	Universidade Federal do Rio Gr	Setor Público			Capacitaçã
PLANO DE DESENVOLVIMENTO INSTITU	Pappis L	2019	Universidade Federal de Santa I	Setor Público	Atualização		
Linguagem Natural Para Apoio ao Reconh	de Souza, Samara Tomé C	2021	Universidade Federal de Santa (	Geral	Atualizaçã	Autenticação Multifator	
Ciranda de Saberes	Dickmann, Ivanio et all	2020	Editora Diálogo Freiriano	Geral	Atualização		Capacitaçã

Fonte: Produzido pela autora (2023)

APÊNDICE B – Quadro 5 - Todas as Práticas da Mesma Planilha Anterior

		Capacitação			Disponibilidade											Treinament
Atualização					Disponibilidade			Integridad	ISO 27000			Plano de Contingência	Senhas Forte	Treinament		
		Capacitação				E-mail		Integridad	ISO 27000			Plano de Contingência	Senhas Fortes			
Atualização		Capacitaçã	Confidencialidade					Integridade			Normas/Regras				Treinament	
										Letramento	Digital					
					Disponibilidade	E-ma	Gamificaç	Integridade								
								Integridade							Treinament	
Atualização		Capacitação			Disponibilidade			Integridade								
		Capacitaçã	Confidencialidade					Integridade								
Atualização		Capacitação								Letramento	Digital				Treinament	
						DPO		Integridade				Plano de Contingência				
Atualização		Capacitação								Letramento	Digital				Treinament	
				Cookies		DPO		Integridade					Senhas Forte		Treinament	
Atualização		Capacitaçã	Confidencialidade		Disponibilidade	E-mail		Integridad	ISO 2700	Letramento	D	Normas/Regr	Plano de Contingência	Senhas Forte	Treinament	
															Treinament	
Atualização							Gamificação									
Atualização							Gamificação			Letramento	Digital					
															Treinament	
Atualização		Capacitação										Plano de Contingência				
					Disponibilidade										Treinament	
Atualização	Autenticação Mult	Capacitaçã	Confidencialidade		Disponibilidade	E-mail		Integridad	ISO 27000		Normas/Regr	Plano de Contingência	Senhas Forte	Treinament		
		Capacitação									Normas/Regras		Questionário		Treinament	
Atualização		Capacitação					Gamificação						Questionário		Treinament	
							Gamificação									
		Capacitação								Letramento	Digital		Questionário			
Atualização										Letramento	D	Normas/Regras				
Atualizaçã	Autenticação Multifator		Confidenci	Cookie	Disponibilidade	E-mail		Integridade						Senhas Forte	Treinament	
Atualização		Capacitação													Treinament	

Fonte: Produzido pela autora (2023)

ANEXO A - Tempo médio para um hacker descobrir senhas

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

Fonte: Hive Systems (2023)