UNIVERSIDADE FEDERAL DE SERGIPE
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO
MESTRADO PROFISSIONAL EM GESTÃO DA INFORMAÇÃO E DO CONHECIMENTO

ANA PAULA MONTEIRO ALMEIDA CHAGAS

GESTÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO ELETRÔNICA:

INTERFACE USUÁRIO, TECNOLOGIA E SISTEMA

SÃO CRISTOVÃO/SE

2023

ANA PAULA MONTEIRO ALMEIDA CHAGAS

GESTÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO ELETRÔNICA:

INTERFACE USUÁRIO, TECNOLOGIA E SISTEMA

Dissertação apresentada à Universidade Federal de Sergipe, como parte das exigências do Programa de Pós-Graduação em Ciência da Informação para obtenção do título de Mestre em Gestão da Informação e do Conhecimento.

Orientadora: Profa. Dra. Telma de Carvalho.

SÃO CRISTOVÃO/SE

2023

DADOS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)

Chagas, Ana Paula Monteiro Almeida
C426g Gestão de segurança dos sistemas de informação eletrônica: interface usuário, tecnologia e sistema / Ana Paula Monteiro Almeida Chagas. - São Cristóvão, SE, 2023.
191 f.: il. ; color.

Orientadora: Dra. Telma de Carvalho.
Dissertação (mestrado profissional em Gestão da Informação e do Conhecimento) – Universidade Federal de Sergipe, Programa de Pós-graduação em Ciência da Informação, 2023.

1. Gestão de Segurança da Informação. 2. Usuários dos Sistemas.3. Sistemas de Informação Eletrônica I. Carvalho, Telma de, orient. II. Título.

CDU 741.5:027.022
CDD 741.5.07.026

Ficha elaborada pela bibliotecária Shirley dos Santos Ferreira (CRB-5/001862/0)

GESTÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO ELETRÔNICA:
INTERFACE USUÁRIO, TECNOLOGIA E SISTEMA

Dissertação apresentada à Universidade Federal de Sergipe, como parte das exigências do Programa de Pós-Graduação em Ciência da Informação para obtenção do título de Mestre em Gestão da Informação e do Conhecimento.

Avaliação: Aprovado

Data da defesa: 01/11/2023

BANCA EXAMINADORA

gov.br Documento assinado digitalmente
TELMA DE CARVALHO
Data: 17/11/2023 08:24:05-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Telma de Carvalho
(Orientadora – PPGCI/UFS)

gov.br Documento assinado digitalmente
BARBARA COELHO NEVES
Data: 21/11/2023 23:31:12-0300
Verifique em https://validar.iti.gov.br

Prof. Dra. Barbara Coelho Neves
(Membro Externo – PPGCI/UFBA)

gov.br Documento assinado digitalmente
ALESSANDRA DOS SANTOS ARAUJO
Data: 22/11/2023 18:38:36-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Alessandra dos Santos Araújo
(Membro Interno - PPGCI/UFS)

Dedico esta dissertação aos meus pais, cujo amor, apoio e cuidado ao longo da minha jornada acadêmica foram inestimáveis. Aos meus irmãos, que sempre me inspiraram com toda dedicação. Ao meu amado marido, Leonel Rodrigues, cujo incentivo e compreensão foram a luz nos momentos mais desafiadores. E à minha querida filha, que trouxe alegria e motivação para cada dia dessa jornada. A Deus, agradeço por sua orientação, força e graça que me sustentaram durante todo esse processo. Que esta dissertação possa refletir a dedicação e o amor que recebi de todos vocês. Com gratidão eterna.

AGRADECIMENTOS

Não há palavras suficientes para expressar a minha gratidão a todas as pessoas que estiveram ao meu lado nessa jornada. Ao listar nomes, há sempre o risco de deixar alguém de fora, o que não é minha intenção, pois cada um de vocês é igualmente importante para mim. Quero apenas transmitir o quanto sou profundamente grata por todo o apoio e encorajamento que recebi ao longo dessa caminhada. Obrigada a todos do fundo do meu coração.

Começo expressando minha profunda gratidão à minha orientadora**, Professora Dra. Telma de Carvalho**. Sua sabedoria, paciência e altruísmo foram verdadeiramente inspiradores. Como sua orientanda, sinto-me honrada por tudo que aprendi com seus ensinamentos e ainda mais orgulhosa por ter tido a oportunidade de ser sua aluna. Serei eternamente grata pelo tempo que compartilhamos e pela generosidade em dividir seu conhecimento comigo.

Sou grata à minha família, o alicerce mais fundamental da minha vida. A minha gratidão aos meus pais, Seu Raimundo e Dona Martha, que não só me deram a vida, mas também me guiaram a cada passo do caminho, permitindo-me disseminar seus ensinamentos onde quer que eu vá. Eles estiveram ao meu lado, tanto nos momentos felizes quanto nos desafios, fornecendo-me uma fonte contínua de força e apoio.

Quero expressar minha profunda gratidão aos meus seis irmãos, cujo companheirismo único e especial é um presente divino. Não há palavras suficientes para agradecer por tudo o que fizeram por mim. Amo vocês imensamente.

Minha profunda gratidão ao meu marido, Leonel Rodrigues, que tem sido uma presença tão especial ao meu lado nesta jornada a dois. Além disso, ele me concedeu o maior presente que já conheci: a dádiva de ser mãe. Agradeço do fundo do meu coração por todo o companheirismo. Esta vitória é nossa e estou imensamente grata por tê-lo ao meu lado.

A minha filha, Gabriela Almeida, quero dizer o quanto sua doçura é como um favo de mel que adoça minha vida e me faz sorrir com as coisas mais simples. Você é meu maior tesouro e nossa ligação é eterna. Saiba que sou profundamente grata por você, minha querida Gabriela, e que te amo mais do que as palavras podem expressar. Sempre estaremos juntas, e sua mãe te ama incondicionalmente.

Aos amigos da Procuradoria da União em Sergipe (PU/SE), com destaque especial para Dr. Ticiano Marcel, Dra. Andrea Carla, Adilson, Cleide e Vanderléa, quero expressar minha sincera gratidão. O apoio de vocês foi fundamental ao longo desta jornada, e sou imensamente grata por isso. Também gostaria de agradecer à organização por ter concedido sua anuência e por acreditar no valor da minha pesquisa. Esse apoio foi fundamental para o sucesso desse trabalho.

RESUMO

Destacando as complexidades inerentes aos fenômenos relacionados à segurança da informação no contexto atual, caracterizadas por ambientes virtual e híbrido em que as informações são acessadas de forma simultânea por diversos setores, através de fluxos contínuos mediados por sistemas de informação e recursos informacionais acessados por servidores, identifica-se uma preocupação substancial relacionada às potenciais vulnerabilidades no uso de sistemas e às ameaças cibernéticas. Essa problemática está diretamente ligada à interação entre o usuário, tecnologia e sistema. A tríade composta pelos elementos de investigação de interesse da Ciência da Informação (CI) - usuários, tecnologia e sistemas - fomenta pesquisas cruciais voltadas para a segurança da informação. Nesse contexto e enfrentando essa problemática, o presente estudo propôs como objetivo geral identificar o comportamento dos servidores da Procuradoria da União em Sergipe (PU/SE) em relação a interface usuário, tecnologia e sistema, com ênfase na segurança da informação visando criar um Manual de Boas Práticas de Segurança da Informação para os usuários dos sistemas. A pesquisa foi conduzida sob os fundamentos teóricos de autores que exploram a temática de maneira interdisciplinar, sendo classificada como bibliográfica, pesquisa de campo e pesquisa-ação de natureza aplicada e quali-quantitativa. Durante a investigação, a informação foi explorada como um recurso de grande valor, inserido no contexto de sistemas de informação informatizados, incluindo a Gestão da Informação, os Sistemas Informatizados de Gestão Arquivística de Documentos (SIGAD), com especial atenção ao comportamento dos usuários, à segurança da informação e às melhores práticas, bem como ao controle de ameaças cibernéticas. Após realizar o diagnóstico e a análise SWOT como ferramenta estratégica para orientar intervenções na PU/SE, a pesquisa alcançou seus objetivos, concluindo que, por meio da exploração das impressões dos usuários, as principais ameaças percebidas por eles puderam ser claramente identificadas. Isso permitiu que a pesquisa não apenas fornecesse uma visão mais abrangente sobre a percepção de segurança da informação na organização, mas também estabelecesse as bases para a proposição de medidas de aprimoramento e a identificação precisa dos incidentes de risco existentes. Ao mesmo tempo, revelou um conjunto de boas práticas que, em alguns casos, poderiam não ter sido devidamente consideradas pela organização anteriormente. Obteve-se, por meio do mapeamento dos principais elementos identificados na análise quali-quantitativa, representando categorias de ameaças e falhas na segurança da informação, uma visão completa do fenômeno da segurança da informação, abordado de maneira científica e holística pelos usuários. Finalmente, constatou-se que essa análise teve um caráter intervencionista, possibilitando o alinhamento e validação dos objetivos da pesquisa por meio da elaboração do produto educacional, o "Manual de Boas Práticas de Segurança da Informação", consolidando assim os resultados obtidos. A pesquisa destaca a importância contínua da educação e preparo dos usuários para enfrentar as ameaças emergentes à segurança da informação no ambiente digital.

Palavras-chave: ameaças cibernéticas; gestão de segurança da informação; segurança da informação; Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD); usuários da informação.

ABSTRACT

Highlighting the complexities inherent to phenomena related to information security in the current context, characterized by virtual and hybrid environments in which information is accessed simultaneously by different sectors, through continuous flows mediated by information systems and information resources accessed by servers, a substantial concern is identified related to potential vulnerabilities in the use of systems and cyber threats. This problem is directly linked to the interaction between the user, technology and system. The triad composed of research elements of interest to Information Science (IC) - users, technology and systems - fosters crucial research aimed at information security. In this context and facing this problem, the present study proposed as a general objective to identify the behavior of employees of the Federal Prosecutor's Office in Sergipe (PU/SE) in relation to the user interface, technology and system, with an emphasis on information security, aiming to create a Manual of Good Information Security Practices for system users. The research was conducted under the theoretical foundations of authors who explore the theme in an interdisciplinary way, being classified as bibliographic, field research and action research of an applied and qualitative-quantitative nature. During the investigation, information was explored as a resource of great value, inserted in the context of computerized information systems, including Information Management, Computerized Document Archival Management Systems (SIGAD), with special attention to user behavior, information security and best practices, as well as the control of cyber threats. After carrying out the diagnosis and SWOT analysis as a strategic tool to guide interventions in PU/SE, the research achieved its objectives, concluding that, through the exploration of users' impressions, the main threats perceived by them could be clearly identified. This allowed the research to not only provide a more comprehensive view of the perception of information security in the organization, but also lay the foundation for proposing improvement measures and accurately identifying existing risk incidents. At the same time, it revealed a set of good practices that, in some cases, might not have been properly considered by the organization previously. By mapping the main elements identified in the qualitative-quantitative analysis, representing categories of threats and failures in information security, a complete view of the information security phenomenon was obtained, approached in a scientific and holistic manner by users. Finally, it was found that this analysis had an interventionist character, enabling the alignment and validation of the research objectives through the development of the educational product, the "Manual of Good Information Security Practices", thus consolidating the results obtained. The research highlights the continued importance of educating and preparing users to face emerging threats to information security in the digital environment.

Keywords: cyber threats; information security; Computerized Document Archival Management System (SIGAD); information users.

LISTA DE FIGURAS

Figura 1	Principais critérios mais frequentes nas etapas da GI.....	39
Figura 2	Principais características essenciais sobre o conceito de GI.....	41
Figura 3	Novas definições de documentos arquivísticos.....	45
Figura 4	Requisitos arquivísticos que caracterizam um SIGAD.....	47
Figura 5	Mapeamento de segurança da informação.....	53
Figura 6	Caracterização da pesquisa.....	76
Figura 7	Justificativas para o uso da abordagem quali-quantitativa.....	78
Figura 8	Etapas da pesquisa bibliográfica.....	82
Figura 9	Principais características da pesquisa-ação.....	86
Figura 10	Etapas do processo de tramitação de protocolos de pesquisa no CEP.....	95
Figura 11	Panorama do ambiente da PU/SE.....	101
Figura 12	Mapa estratégico AGU: planejamento 2020-2023.....	104
Figura 13	Definições dos quadrantes do SWOT.....	114
Figura 14	Diagrama clássico da Matriz SWOT.....	115
Figura 15	Nuvem de palavras na categorização do termo “ameaças”	126
Figura 16	Nuvem de palavras na categorização do termo “boas práticas”	128
Figura 17	Sumário do manual.....	150

LISTA DE GRÁFICOS

Gráfico 1 Modalidade de trabalho..... 131

Gráfico 2 Faixa etária dos participantes da pesquisa..... 132

Gráfico 3 Nível de entendimento sobre segurança da informação..... 133

Gráfico 4 Conhecimentos sobe as normas de segurança da informação estabelecidas pela AGU..... 134

Gráfico 5 Promoção de treinamento ou capacitação sobre segurança da informação..... 135

Gráfico 6 Percepção da segurança da informação e competências da DTI..... 136

Gráfico 7 Percepção dos usuários sobre segurança da informação..... 137

Gráfico 8 Sistemas de informação internos e externos ao órgão utilizados para executar as tarefas..... 137

Gráfico 9 Percentual sobre comportamento de alteração periódica de senhas da rede AGU..... 139

Gráfico 10 Uso de aplicativos ou site de acesso livre e gratuito na internet..... 140

Gráfico 11 Propriedade dos equipamentos tecnológicos utilizados em teletrabalho..... 142

Gráfico 12 Acesso aos sistemas de informação corporativos em dispositivos particulares..... 143

Gráfico 13 Principais canais de comunicação com a DTI usados como suporte..... 144

Gráfico 14 Importância da adesão ao cadastro da MFA..... 145

LISTA DE QUADROS

Quadro 1	Valores da informação.....	26
Quadro 2	Principais sistemas eletrônicos de GI utilizados pelo Poder Executivo Federal e Judiciário no Brasil.....	49
Quadro 3	Principais conceitos sobre segurança da informação.....	55
Quadro 4	Diretrizes específicas de controle de segurança da informação da organização.....	59
Quadro 5	Pontos gerais que podem afetar o comportamento de busca do usuário individualmente.....	63
Quadro 6	Principais significados dos termos que compõem o conceito de GSI.....	67
Quadro 7	Mecanismos de defesa para boas práticas de segurança da informação.....	69
Quadro 8	Principais Normas de segurança da informação da família ISO/IEC 27000.....	71
Quadro 9	Esquema simplificado de funcionamento dos operadores booleanos.....	83
Quadro 10	Caracterização da amostra potencial da pesquisa.....	91
Quadro 11	Diretrizes gerais do processo de análise de conteúdo.....	94
Quadro 12	Atribuições institucionais do planejamento dos macroprocessos estabelecidos pelo PDTIC.....	105
Quadro 13	Principais funcionalidades do SAPIENS por área de atuação organizacional.....	107
Quadro 14	Diagnóstico por análise SWOT da PU/SE.....	118
Quadro 15	Amostra real dos participantes de pesquisa.....	121
Quadro 16	Classificação da variável “ameaça” no questionário.....	122
Quadro 17	Frequência de palavras na categorização do termo “ameaças”	123
Quadro 18	Classificação da variável “boas práticas” no questionário.....	127
Quadro 19	Frequência de palavras na categorização do termo “boas práticas”	127
Quadro 20	Descrição das variáveis das perguntas fechadas do questionário.....	130
Quadro 21	Mapeamento das ameaças X boas práticas em segurança da informação	148

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AGU	Advocacia-Geral da União
AGUDOC	Sistema de Controle de Documentos da Advocacia-Geral da União
AGUOUVIDORIA	Sistema de Ouvidoria da Advocacia-Geral da União
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ASCOM	Assessoria Especial de Comunicação Social
BDTD	Biblioteca Digital Brasileira de Teses e Dissertações
CEP	Comitê de Ética em Pesquisa
CETIC.BR	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CGDI	Coordenação-Geral de Gestão da Documentação e Informação
CI	Ciência da Informação
CNS	Conselho Nacional de Saúde
CONARQ	Conselho Nacional de Arquivos
CONATEC	Coordenação Nacional de Soluções Tecnológicas
CONEP	Comissão Nacional de Ética em Pesquisa
COVID-19	*Coronavirus Disease 2019*
CTDE	Câmara Técnica de Documentos Eletrônicos
CTI	Comitê de Tecnologia da Informação
DATAPREV	Empresa de Processamento de Dados da Previdência Social
DCP	Departamento de Cálculos e Perícias
DGE	Departamento de Gestão Estratégica
DTI	Departamento de Tecnologia da Informação
e-ARQ BRASIL	Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos
EBC	Empresa Brasil de Comunicação
ESAGU	Escola Superior da AGU
EUA	Estados Unidos da América
EVA	Escola Virtual da AGU
GC	Gestão do Conhecimento

GD	Gestão Documental
GED	Gerenciamento Eletrônico de Documentos
GI	Gestão da Informação
GPWEB	Sistema de Gerenciamento de Projetos
GRU	Guia de Recolhimento da União
GSI	Gestão de Segurança da Informação
GSIPR	Gabinete de Segurança Institucional da Presidência da República
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileiras
IHC	Interação Homem-Computador
ISO	International Organization for Standardization
ITI	Instituto Nacional de Tecnologia da Informação
ME	Ministério da Economia
MFA	Autenticação Multifator
MOREQ	Modelo de Requisitos para a Gestão de Arquivos Eletrônicos
NECAP	Núcleo de Cálculos e Perícias
NOTAPAR	Consulta a Cadastro de Notas e Pareceres
NUP	Número Único de Protocolo
OTRS	Open-source Ticket Request System
PAGJUDICIAIS	Consulta Pagamentos Judiciais - Precatórios e RPV
PDF	Portable Document Format
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PGD	Programa de Gestão e Desempenho
PGSI	Política de Gestão e Segurança da Informação
PGU	Procuradoria-Geral da União
PJE	Processo Judicial Eletrônico
PNI	Plano Nacional de Imunização
PPGCI	Programa de Pós-Graduação em Gestão da Informação e do Conhecimento
PRA	Paperwork Reducion Act
PRU5	Procuradoria-Regional da União da 5ª Região
PSI	Política de Segurança Institucional
PU/SE	Procuradoria da União em Sergipe
SAPIENS	Sistema AGU de Inteligência Jurídica

SCDP	Sistema de Concessão de Diárias e Passagens
SEI	Sistema Eletrônico de Informações
SEJUD	Secretaria Judiciária
SGA	Secretaria-Geral de Administração
SGSI	Sistema de Gestão de Segurança da Informação
SICAP	Sistema de Cálculos e Perícias da AGU
SIG	Sistemas de Informação Gerencial
SIGAA	Sistema Integrado de Gestão de Atividades Acadêmicas
SIGAC	Sistema de Gestão de Acesso
SIGAD	Sistemas Informatizados de Gestão Arquivística de Documentos
SIORG	Sistema de Organização e Inovação Institucional do Governo Federal
SISCON	Sistema de Gestão de Convênios
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
SWOT	Strenghts, Weaknesses, Opportunities and Threats
TCLE	Termo de Consentimento Livre e Esclarecido
TCU	Tribunal de Contas da União
TGS	Teoria Geral dos Sistemas
TI	Tecnologia da Informação
TIC	Tecnologias da Informação e Comunicação
TRF4	Tribunal Regional Federal da 4ª Região
UFRN	Universidade Federal do Rio Grande do Norte
UFS	Universidade Federal de Sergipe
UNISIST	Sistema Mundial de Informação Científica e Tecnológica
VPN	Virtual Private Network

SUMÁRIO

1 INTRODUÃO..... 15
1.1 Tema, motivação e problema de pesquisa..... 17
1.2 Objetivos..... 19
1.2.1 Objetivo Geral..... 20
1.2.2 Objetivos Específicos..... 20
1.3 Justificativa..... 20
1.4 Estrutura da dissertação..... 22
2 INFORMAÇÃO COMO VALOR NA PERSPECTIVA DA SOCIEDADE DA INFORMAÇÃO E DO CONHECIMENTO..... 24
2.1 Era da Informação: características e desafios..... 29
2.2 Gestão da informação em sistemas informatizados..... 36
2.3 Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD).... 42
3 SEGURANÇA DA INFORMAÇÃO..... 50
3.1 Comportamento dos usuários dos sistemas informatizados na perspectiva da segurança da informação..... 56
3.2 Boas práticas em segurança da informação..... 64
4 METODOLOGIA..... 73
4.1 Caracterização da pesquisa..... 75
4.1.1 Perspectiva teórica da pesquisa: pesquisa bibliográfica..... 79
4.1.2 Perspectiva prática da pesquisa: pesquisa de campo e pesquisa-ação..... 84
4.2 Ambiente social de intervenção..... 87
4.3 População e amostra..... 89
4.4 Procedimentos de coleta de dados..... 91
4.5 Método de análise de dados..... 93
4.6 Considerações éticas..... 94
5 DIAGNÓSTICO ORGANIZACIONAL POR ANÁLISE SWOT DA PU/SE – AGU..... 100
5.1. Caracterização do ambiente interno..... 102
5.2 Caracterização do ambiente externo..... 108
5.3 Considerações sobre a análise SWOT como ferramenta estratégica..... 112
5.4 Descrição da análise SWOT da TI na PU/SE..... 116
6 RESULTADO DA INTERVENÇÃO E DISCUSSÃO..... 121

6.1 Resultado da análise qualitativa..... 122
6.2 Resultados da análise quantitativa..... 129
6.3 Validando os objetivos da pesquisa..... 146
7 PRODUTO DA INTERVENÇÃO..... 150
8 CONSIDERAÇÕES FINAIS..... 153
REFERÊNCIAS..... 156
APÊNDICE A – Termo de Consentimento livre e Esclarecido – TCLE..... 175
APÊNDICE B – Questionário..... 179
ANEXO A – Comprovante do envio do projeto junto ao Comitê de Ética em Pesquisa Envolvendo Seres Humanos (CEP) da Universidade Federal de Sergipe/UFS..... 183
ANEXO B – Parecer consubstanciado do CEP..... 184
ANEXO C – Termo de anuência e existência de infraestrutura..... 192

1 INTRODUÇÃO

Novas diretrizes têm fundamentado o uso da informação como valor para as organizações, especialmente com a globalização e a internet. Essas transformações têm conduzido a informação no cerne dos processos informacionais, desempenhando um papel fundamental nas transformações sociais, econômicas, científicas, tecnológicas e culturais. Em termos gerais, compreende-se que essas são as novas concepções da informação na Sociedade da Informação e do Conhecimento.

Em termos organizacionais, a informação passou a ser o principal ativo das instituições públicas e privadas, disponibilizada em sistemas integrados de redes virtuais, através de interfaces variadas que intermediam os processos de produção, fluxo e recuperação da informação.

Não obstante, as Tecnologias da Informação e Comunicação (TIC) permitiram otimizar a recuperação da informação dando suporte para a implementação da Gestão da Informação (GI) e a Gestão do Conhecimento (GC), principalmente com o desenvolvimento de Sistemas Informatizados de Gerenciamento Eletrônico de Documentos (GED).

Destacam-se os Sistemas Informatizados de Gestão Arquivística de Documentos (SIGAD), Sistemas de Informação Gerencial (SIG) e Sistema de Gestão de Acesso (SIGAC). Esses sistemas trabalham com plataformas híbridas de documentos digitais e eletrônicos. Soma-se a esse rol os portais corporativos, Fóruns, *E-learning*, e-mails, lista de discussão, Workflow, e redes sociais.

No contexto jurídico, esses sistemas viabilizam o acesso remoto, virtual ou online à documentação jurídica, incluindo doutrinas, legislações e jurisprudências que representam fontes formais de informações essenciais para os profissionais do Direito. Além disso, permitem a gestão dos fluxos de documentos institucionais que desempenham um papel fundamental como subsídios nos processos administrativos e judiciais.

O Conselho Nacional de Justiça (CNJ) destaca em seu relatório de 2022 que a digitalização e a implementação do Processo Judicial Eletrônico (PJE) proporcionou novas perspectiva metodológica abrangente na gestão do sistema judiciário, com um enfoque particular na Gestão Documental (GD) dos documentos arquivísticos digitais e na GC. Esse enfoque compreende a extração de dados de relatórios gerenciais que se baseiam no fluxo processual, bem como em indicadores relacionados à produtividade, ao desempenho e aos índices de resultados consolidados pelos tribunais e diversos segmentos do Poder Judiciário.

Entende-se que o processo eletrônico não modificou somente uma estrutura de suporte, também acrescentou uma nova teoria geral de processo porque “o processo eletrônico não se materializa, vive no fluxo da rede” (Souza; Resende, 2019, p. 190). Pode-se compreender que o impacto das novas tecnologias nas práticas de GD apresentou inúmeras vantagens e grandes desafios para os usuários dos sistemas.

Flores (2023) discute como a gestão de documentos arquivísticos digitais enfrenta desafios complexos devido à transformação digital e aos sistemas informatizados, resultando em um novo paradigma que exige novos modelos científicos e empresariais. Enquanto paradigmas antigos ainda influenciam ações, a adaptação das práticas de GD é fundamental. O autor enfatiza o desafio central de implementar sistemas que assegurem a custódia digital ao longo do ciclo de vida dos documentos, seja por meio de inovação ou disrupção, como parte integrante da transformação digital efetiva.

No cenário atual, caracterizado por ambientes virtual e híbrido, em que as informações são acessadas simultaneamente por diversos setores em fluxos contínuos, mediados por sistemas de informação e recursos informacionais acessados por servidores, emerge uma interdependência complexa entre seres humanos e equipamentos tecnológicos. Essa interação destaca de forma crescente a necessidade premente de salvaguardar esse ativo de significativa relevância social e econômica, cada vez mais vulnerável a diversos riscos de segurança.

No Brasil, a Gestão de Segurança da Informação (GSI) segue as diretrizes estabelecidas pelo conjunto de certificações estabelecidos pela família das normas ISO 27000, padronizadas internacionalmente pela *International Organization for Standardization* (ISO), organização internacional não-governamental para padronização e certificações, representada no Brasil pela Associação Brasileira de Normas Técnicas (ABNT).

As normas da família ISO 27000 servem como base para criar, implementar e revisar o Sistema de Gestão de Segurança da Informação (SGSI). Elas fornecem um conjunto de ações para proteger e preservar os ativos de informação, garantindo sua disponibilidade, integridade, confidencialidade e autenticidade. Isso inclui um glossário com termos e definições usados nos padrões dos sistemas, aplicáveis a organizações de diferentes tipos e tamanhos (Baldissera, 2021).

O termo Interação Homem-Computador (IHC) corresponde a ação exercida de interação mútua caracterizada “por estudos de pessoas por um lado e sistemas baseados em computadores por outro, incluindo as maneiras como um exerce influência sobre o outro”

(Rocha; Baranauskas, 2000, p. 28). É importante ressaltar que essas dimensões estão intrinsecamente interligadas, refletindo uma lógica fundamental.

Entende-se que essa relação mútua amplia a compreensão da segurança da informação para além do âmbito tecnológico, direcionando a formulação da Política de Gestão e Segurança da Informação (PGSI). Isso se diferencia dos modelos atuais, que muitas vezes se concentram excessivamente em aspectos tecnológicos e colocam em menor evidência o comportamento informacional.

A vulnerabilidade mencionada pode decorrer da falta de validação adequada dos campos de entrada nos sistemas e nas aplicações web, permitindo que os usuários enviem dados arbitrários, incluindo códigos maliciosos. Isso ocorre devido à falta de maturidade ou conhecimento em segurança da informação por parte dos usuários e à ausência de uma cultura organizacional focada na segurança da informação, com ênfase no comportamento do usuário.

É de extrema importância verificar se os usuários estão adequadamente sensibilizados e adotam práticas corretas e seguras ao desempenhar suas tarefas nos sistemas de informação. Isso ocorre porque eles podem ser causadores de potenciais problemas por estarem suscetíveis a possíveis danos, tornando-se essencial a promoção de uma cultura de segurança em informática.

Esta pesquisa, parte do Mestrado Profissional em Gestão da Informação e do Conhecimento na Universidade Federal de Sergipe (UFS), abordou a segurança dos sistemas de informação e o comportamento dos usuários, com foco na interface usuário, tecnologia e sistema. Explorou questões interdisciplinares relacionadas à forma como as pessoas utilizam a Tecnologia da Informação (TI) nas organizações.

Frente à importância dessa temática e às frequentes mudanças nos sistemas de informação que são implantados de maneira dinâmica e podem ser facilmente substituídos, a segurança da informação assume um amplo e importante campo de pesquisa. Nesse contexto, existem diversos fenômenos que requerem uma abordagem científica para contribuir e esclarecer lacunas que necessitam de um estudo mais direcionado aos usuários dos sistemas. Os fenômenos informacionais e tecnológicos dos quais a segurança da informação se origina tornaram essencial o desenvolvimento dessa pesquisa.

1.1 Tema, motivação e problema de pesquisa

Em termos organizacionais, as atividades e a cultura informacional estão fundamentadas por usuários, sistemas e as TIC como valor para tomada de decisão. Essa tríade

envolve questões de confidencialidade e integridade da informação, as quais são processadas, armazenadas e distribuídas pelos usuários dos sistemas em rede e em diferentes ambientes ou setores de uma organização integrados a sistemas de órgãos externos.

Na maioria das vezes, o primeiro passo para o acesso a um sistema eletrônico é tão simples que ao realizar o *login* o usuário possui o poder da informação privilegiada em suas mãos. Nessa relação direta do usuário, tecnologia e sistema, se não for observado um conjunto de práticas e regras na utilização desses sistemas corre-se o risco de vulnerabilizar o sistema a ataques cibernéticos, diminuindo o nível da segurança e da integridade da informação. Com a assinatura digital os riscos são ainda maiores porque esta assinatura permite validar atos e documentos decisivos para a organização.

Outro ponto relevante na segurança da informação é a relação entre os sistemas de informação e o comportamento do usuário, que vai além dos investimentos tecnológicos onerosos e necessários para a organização. Essa problemática instigou a pesquisa porque os usuários representam risco de vulnerabilidade e eventuais danos ao SI, e precisam ter um comportamento alinhado à política de segurança da informação da organização.

A organização em que será realizada a intervenção é a Procuradoria da União em Sergipe (PU/SE), que está contextualizada em um ambiente com sistemas de tramitação de processos eletrônicos vinculados ao Poder Judiciário nos âmbitos estadual e federal, por meio de atuação no gerenciamento eletrônico de documentos, por meio do Sistema AGU de Inteligência Jurídica (SAPIENS), o qual promove a orquestração dos vários sistemas informatizados da administração pública de forma transparente para o usuário. Diante dos argumentos considera-se a relevância do tema dessa pesquisa, que é segurança da informação com ênfase nos usuários, fundamentada no problema da interface usuário, tecnologia e sistema.

A motivação para essa pesquisa originou-se pela observação direta da autora durante suas atividades laborais na Advocacia-Geral da União (AGU). Ela percebeu que, semelhante a outros usuários, estava trabalhando com sistemas de informação integrados a sistemas externos, porém sem uma compreensão plena do grau de vulnerabilidade e do potencial risco de causar danos aos sistemas de informação. A identificação dessa lacuna foi o ponto de partida que impulsionou a realização dessa pesquisa. O estudo visou avaliar a percepção dos usuários em relação à vulnerabilidade e aos riscos nos sistemas de informação, considerando as normas de segurança da AGU.

Outro fator crucial que impulsionou essa pesquisa foi a implementação do teletrabalho em todas as unidades regionais e estaduais da AGU como parte da Política de Segurança Institucional (PSI) em resposta à pandemia da COVID-19. Isso foi estabelecido por

meio do Comunicado n. 16/SGA, de 16 de março de 2020, e da desterritorialização determinada pela Portaria nº 26, de 14 de outubro de 2020. Embora essas normativas sejam abordadas em detalhes na análise do ambiente interno, para fins de clareza, o parágrafo único da Portaria nº 26/2020 descreve:

> A desterritorialização constitui instrumento de equalização permanente do volume de trabalho, não promovendo a alteração da lotação ou do exercício de Advogados da União ou servidores administrativos, que permanecem responsáveis pelas atividades presenciais locais (AGU, 2020).

Na prática, os servidores da PU/SE, foco dessa intervenção, mantiveram suas lotações, mas suas atividades passaram a ser integradas às coordenações jurídicas da Procuradoria-Regional da União da 5ª Região (PRU5) em Pernambuco. Alguns estão vinculados à Secretaria-Geral de Administração (SGA), especificamente nos Núcleos de Cálculos e Perícias (NECAP) do Departamento de Cálculos e Perícias (DCP), subordinados à Procuradoria-Geral da União (PGU) em Brasília, onde a pesquisadora está vinculada. A grande mudança é que todas as operações e comunicações da AGU agora são realizadas por meio do SAPIENS e sistemas integrados em rede.

Conforme as informações disponibilizadas no site institucional da AGU (Brasil, 2022), o SAPIENS é um sistema de GED híbrido, equipado com recursos avançados para a produção de conteúdo jurídico e o controle de fluxos administrativos.

Todas as tarefas jurídicas da AGU são controladas pelo sistema SAPIENS AGU, o que facilitou a transição para o trabalho remoto, com cerca de 50% dos servidores atuando nesse formato. No entanto, essa mudança também pode aumentar a vulnerabilidade dos usuários dos sistemas, exigindo maior atenção à segurança da informação.

Entende-se que é fundamental para a organização promover uma cultura de segurança a partir das boas práticas. Portanto, o problema de pesquisa é: Qual é a percepção dos usuários dos sistemas de informação da PU/SE em relação às práticas de segurança da informação e como eles se comportam e agem quando ocorrem falhas de segurança que envolvem a influência do elemento humano em sua interface com a tecnologia e o sistema?

1.2 Objetivos

A fim de responder à questão de pesquisa formulada inicialmente, para que ao final da pesquisa se possa atingir os seus propósitos, traçaram-se os objetivos geral e específicos formulados a seguir.

1.2.1 Objetivo Geral

- Identificar o comportamento dos servidores da Procuradoria da União em Sergipe em relação a interface usuário, tecnologia e sistema, com ênfase na segurança da informação visando criar um Manual de Boas Práticas de Segurança da Informação para os usuários dos sistemas.

1.2.2 Objetivos específicos

- Investigar elementos indicadores de falhas de segurança a partir da percepção dos participantes da pesquisa propondo estratégias alternativas de gestão de segurança da informação que envolva a interface usuário, tecnologia e sistema.
- Analisar o comportamento e as atitudes dos usuários dos sistemas em relação as normas de segurança da informação preestabelecidas pela organização com o objetivo de identificar as principais circunstâncias em que ocorrem as falhas de segurança e como prevenir os incidentes.
- Mapear os principais incidentes de risco para a segurança da informação identificados através de levantamento do trabalho de campo para propor boas práticas de segurança da informação não vislumbradas pela organização.

1.3 Justificativa

Em primeira instância, a pesquisa foi motivada pela observação empírica dessa pesquisadora, que tendo iniciado sua carreira profissional como funcionária pública federal na Universidade Federal de Sergipe, instituição vinculada ao Ministério da Educação (MEC), em janeiro de 1995, foi requisitada no ano de 2004 pela PU/SE, órgão da AGU, onde permanece até os dias atuais, desenvolvendo suas atividades no NECAP.

Tendo vivenciado nesses 27 anos de experiência profissional, as transformações e evolução das TlC e seus impactos no fazer profissional, foi possível sentir na prática esse processo que tem sido um grande desafio.

No campo jurídico, as transformações tecnológicas tornaram-se mais complexas e decisivas. Isso exige que membros e servidores possuam um alto nível de conhecimento e habilidades técnicas, capacitando-os a lidar de forma ágil e inteligente com os desafios de um ambiente judicial incerto e de uma administração pública que demanda altos padrões de

eficiência e segurança jurídica. A informação jurídica hoje é produzida, organizada e compartilhada por meio de Sistemas de Gerenciamento Eletrônico de Documentos e processos integrados entre os Poderes Executivo e Judiciário.

Essa pesquisa se justificou pela importância da temática face a incidência de uma série de ataques cibernéticos a organizações mundiais, o que levanta a discussão sobre a relevância de não somente implantar investimentos na área de segurança da informação como forma de proteger os sistemas de informação, mas também de se debruçar de forma mais científica sobre o comportamento do usuário em relação a interface usuário, tecnologia e sistema. Convém salientar que no Brasil esse fato também vem ganhando importância após uma série de intrusões e ataques cibernéticos a instituições financeiras e a sistemas de órgãos do Governo Federal, revelando a existência de ameaças que têm o potencial de comprometer o pleno funcionamento de infraestruturas críticas e principalmente de dados sigilosos.

Atualmente a questão do usuário dos sistemas ficou mais evidente com as ações desenvolvidas para o distanciamento social em proteção contra a COVID-19, em que a maioria das organizações do poder executivo, legislativo e judiciário adotaram o teletrabalho ou home office por uma questão de extrema necessidade e, com o fim da pandemia, foi estabelecido como nova forma de trabalho em muitas organizações.

Validando essa afirmativa acima, o Decreto nº 11.072, de 17 de maio de 2022, em seu Art. 6º, reconhece e autoriza a adoção das modalidades de trabalho presencial ou teletrabalho na Administração Pública Federal direta, autárquica e fundacional, nos termos do seu Programa de Gestão e Desempenho (PGD).

Com a implementação do teletrabalho, a vulnerabilidade dos sistemas aumentou, uma vez que os usuários não contam com o acesso aos recursos de segurança da informação fornecidos pelo Departamento de Tecnologia da Informação (DTI) no ambiente físico. Essa mudança ocorreu em várias organizações, especialmente em atividades sistematizadas que não demandam atendimento direto ao público.

Nota-se que por parte das organizações existe uma grande preocupação com a renovação de seu parque computacional e a modernização de equipamentos de rede, adotando investimentos com políticas de GI voltadas para a criação de uma cultura de segurança da informação, enquanto ainda existe um espaço a ser preenchido quanto ao comportamento do usuário e os possíveis riscos à segurança da informação.

Nesse contexto, acredita-se que a pesquisa, devido ao seu caráter exploratório e de intervenção, possui o potencial de catalisar transformações na cultura organizacional da PU/SE. Ela se destaca por sua proposta em identificar e compreender o comportamento dos usuários

em relação à gestão de segurança dos sistemas de informação eletrônica, com ênfase na interface usuário, tecnologia e sistema.

1.4 Estrutura da dissertação

Essa dissertação apresentou uma estrutura organizada em oito seções. A introdução estabeleceu o contexto, objetivos e a estrutura do trabalho. Na segunda seção, o referencial teórico explorou a importância da informação e sua gestão, especialmente na era da informação e nos sistemas informatizados. Iniciou-se com uma revisão de literatura acerca dos conceitos da “INFORMAÇÃO COMO VALOR NA PERSPECTIVA DA NA PERSPECTIVA DA SOCIEDADE DA INFORMAÇÃO E DO CONHECIMENTO”, subdividindo-se na subseção 2.1 "Era da informação", com suas principais características e desafios; 2.2 "Gestão da informação em sistemas informatizados" e 2.3 "Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD)". O objetivo da respectiva seção foi abordar a importância da informação como um ativo valioso na sociedade contemporânea, enfatizando a relevância da GI, especialmente em sistemas informatizados.

Na seção 3, intitulada "SEGURANÇA DA INFORMAÇÃO", concentrou-se a atenção na segurança dos dados e no comportamento dos usuários (3.1), bem como na descrição abrangente das “Boas práticas em segurança da informação” (3.2). Examinou-se como as ações dos usuários podem influenciar diretamente a segurança, detalhando políticas de segurança, criptografia, controle de acesso e outros protocolos cruciais para assegurar a proteção dos sistemas e dos dados.

Na seção 4, intitulada "Metodologia," foram descritos os principais aspectos da pesquisa, incluindo sua caracterização, abordagem, procedimentos metodológicos, local de intervenção, população e amostra, técnicas e procedimentos de coleta de dados, bem como as considerações éticas.

Na seção 5, conduziu-se o diagnóstico do ambiente por meio de uma análise crítica, que abrangeu tanto o ambiente interno quanto o externo. O objetivo foi orientar a elaboração de um produto técnico-científico e educacional como resultado da intervenção, com o propósito de resolver o problema identificado após a análise dos dados. Isso englobou a “Caracterização do ambiente interno” (5.1) e “Caracterização do ambiente externo” (5.2), juntamente com “Considerações sobre a análise SWOT como ferramenta estratégica” (5.3) e a “Descrição da análise SWOT da TI na PU/SE (5.4).

Na seção 6, foram apresentados os resultados da intervenção, abordando três áreas principais: análise qualitativa (6.1) e análise quantitativa (6.2) dos resultados da pesquisa, além da validação dos objetivos (6.3). Na análise qualitativa, foram apresentadas descobertas detalhadas e contextualizadas. A análise quantitativa forneceu uma visão numérica dos dados. Na subseção 6.3, os objetivos foram validados relacionando resultados qualitativos e quantitativos, demonstrando sua contribuição para a compreensão do tema e o alcance dos objetivos iniciais.

A estrutura da seção 7, intitulada "Produto da intervenção," enfatizou a aplicação prática e as contribuições concretas da pesquisa para a área de estudo, apresentando e descrevendo o produto final da pesquisa, o produto acadêmico intitulado “Manual de Boas Práticas de Segurança da Informação” o qual apresentou informações concisas sobre a aplicação das práticas essenciais de segurança da informação.

Na Seção 8, intitulada "Considerações Finais," foram destacadas as principais conclusões e as implicações práticas decorrentes da pesquisa. Enfatizou-se a relevância da segurança da informação na sociedade contemporânea, incentivando a adoção de boas práticas para proteger ativos de informação valiosos. Além disso, ressaltou-se a necessidade contínua de conscientização e a implementação de medidas de segurança sólidas em um ambiente digital em permanente transformação. A dissertação foi concluída com a seção de referências. A dissertação foi finalizada com a seção de referências. A dissertação foi finalizada com a seção de referências.

2 INFORMAÇÃO COMO VALOR NA PERSPECTIVA DA SOCIEDADE DA INFORMAÇÃO E DO CONHECIMENTO

Ao longo dos séculos a informação tem evoluído e constituído a base disciplinar da CI alicerçada sob diferentes enfoques, instigando campos de estudos interdisciplinares que se fundamentam em explorar o gerenciamento da informação, quanto a sua organização, acesso uso e compartilhamento disseminado para a sociedade.

Amparada pelos avanços tecnológicos, econômicos e sociais ao longo dos séculos, a informação passou a ocupar um lugar de protagonismo como objeto e fenômeno de estudo e partícipe do fazer profissional em qualquer segmento social no contexto da sociedade da informação e do conhecimento. Nessa conjuntura, o dilema em identificar a informação relevante tem sido um desafio enfrentado pelos usuários de sistemas informacionais, principalmente em função da quantidade de informação produzida e recebida pelas unidades de informação inseridas em um cenário de explosão informacional.

Seguindo a linha dos questionamentos supracitados, Valentim e Ançanello (2018) inferem uma certa dificuldade em se estabelecer o que é uma informação de valor e principalmente como ocorre esse processo. As autoras explicam que em sua grande maioria, os múltiplos conceitos sobre a informação estão associados a questionamentos de redução de incertezas, na busca pelos usuários ou a elementos que compõem o processo comunicacional e participativo entre um emissor e um receptor.

Conforme as mesmas autoras, o valor à informação deve ser pertinente às necessidades informacionais dos indivíduos, nelas estão inerentes ao valor da própria informação e também ao seu uso, que é precedido de uma avaliação do usuário infundindo na qualidade da informação e no seu valor real em determinado contexto (Valentim; Ançanello, 2018).

Corroborando com as autoras, Moraes e Fadel (2009), entendem que ao ser contextualizada, a informação coloca o indivíduo como prioridade porque o processo de internalização da informação leva a construção de conhecimento a partir de novos significados que refletem na sociedade e nas organizações. Sob esse mesmo enfoque e pelo caráter subjetivo da informação, Woida (2008, p. 108) explica que, no contexto organizacional, o usuário deve ser visto como elemento vital, de forma que: “Informações e significados são mecanismos sociais inerentes aos agrupamentos de pessoas e, por isso, deve constar na cultura informacional com uma das ações mais incentivadas”.

Evidencia-se que dimensões complexas entre as organizações e a sociedade tramam diálogos que enveredam por questões econômicas, políticas e sociais. Sob esse prisma, Valentim (2008) compreende que a informação, o conhecimento e as TIC seriam o insumo básico dos processos que alicerçam economicamente a Sociedade da Informação. Para a autora:

> A informação é a matéria-prima, o insumo básico do processo; as tecnologias de informação e comunicação são as estruturas que possibilitam o acesso, a armazenagem, o processamento e a mediação/disseminação; o conhecimento é o resultado do processo (Valentim, 2008, p. 11).

Seguindo a mesma lógica de que a informação perpassa por quase todos os processos de uma organização dispersa nos conhecimentos e experiências dos indivíduos e das suas competências e conhecimento especializado, Choo (2003) apresenta em sua visão clássica de três arenas formas distintas do uso da informação para o seu uso estratégico, que seriam: criar significado, construir conhecimento e tomar decisões.

Para o autor, essas três arenas possuem correlação direta para criar uma organização do conhecimento, levando-o a ter uma visão mais holística do uso da informação, afirmando que: "Sem uma clara compreensão dos processos organizacionais e humanos pelos quais a informação se transforma em percepção, conhecimento e ação, as empresas não são capazes de perceber a importância de suas fontes e tecnologias de informação" (Choo, 2003, p. 27).

Sobre a relevância da informação no cenário organizacional, Moresi (2000) analisa que o valor da informação está relacionado como o sistema de informação, que incide em ações voltadas para tomada de decisão e geração de conhecimento. Para o autor, a informação é um recurso chave de competitividade e instrumento de gestão, afirmando que: "o valor da informação é uma função do contexto da organização, da finalidade de utilização, do processo decisório e dos resultados das decisões" (Moresi, 2000, p. 24).

Santos e Valentim (2020) acreditam que a informação, conhecimento e valor da informação compõem recurso de valor estratégico para o uso da informação como negócio. Ao atribuírem o valor da informação nessa perspectiva, essas autoras entendem que o processo decisório está estruturado em minimizar incertezas a partir da aprendizagem organizacional percebida por seus ativos a partir das experiências adquiridas com erros e acertos. Da mesma forma, o seu valor estratégico perpassa pelos processos, produtos e serviços que buscam ampliar a inovação e o potencial competitivo de uma organização, conforme destacam as autoras:

> Reconhecer o valor da informação como negócio com foco na competitividade é pré-requisito para o desenvolvimento organizacional nesse ambiente mutável e complexo, cuja competição se reflete na busca de vantagem, visando estabelecer um diferencial competitivo no mercado (Santos; Valentim, 2020, p. 593).

Silva (2017b) promoveu uma análise mais profunda sobre os valores da informação na pragmática gerencial e estratégica, presente nos processos gerenciais e organizacionais no âmbito da CI. O autor argumenta que a informação ganhou na sociedade contemporânea uma característica por ele denominada vital, devido a sua condição estratégica para os processos organizacionais.

O mesmo autor considera que a informação possui dois grandes tipos de valores que possuem relação intrínseca entre o uso da informação e as questões qualitativas da interação, entre as causas e as consequências de produzir informação, a saber: valores causais, que se referem ao caráter moral e humano da informação e os valores consequências, que se referem ao caráter processual da informação. Optou-se por sintetizar em um quadro adaptado, as principais compreensões desses valores, apresentadas por Silva (2017b), face a sua relevância e dimensão apresentada (Quadro 1).

Quadro 1 – Valores da informação

VALORES CAUSAIS	
Refere-se ao caráter moral e humano da informação, envolvendo o valor humano, social, econômico, cultural, político, religioso e ético.	
Tipologias de valores causais	**Aspectos valorativos da informação**
Valor humano	Valores cruciais da informação que indicam comportamento humano dos sujeitos da informação voltado para sua visão de vida.
Valor social	Valor coletivo atribuindo significados culturais, educacionais e políticas com melhoria de construção de sentidos para a população.
Valor econômico	Valor de competitividade, possessividade e materialidade (consumo de produtos informacionais).
Valor histórico-cultural	Compor o repertório de valores culturais dos sujeitos contribuindo tanto para construção individual quanto para construção coletiva
Valor político	Capacidade dos sujeitos, em nível individual ou coletivo, público ou privado, de analisar situações da realidade e tomar decisões, visando benefícios a determinados grupos.
Valor educativo	Reflete o caráter pragmático (age no cotidiano dos sujeitos) e institucional (agregado a instituições como família, escola, universidade, igreja, etc.) sobre como os sujeitos aprendem e produzem conhecimentos a partir das informações que são apropriadas.
Valor religioso	Preconiza os sentidos que os sujeitos produzem para fundamentação espiritual, incluindo a fé e o amor a um ser superior. O valor da informação é baseado em um fundamentalismo que tem a finalidade de persuadir outros sujeitos do que é verdadeiro em termos espirituais.
Valor científico	Valor de produção de novos conhecimentos que sirvam para embasar a opinião de comunidades acadêmico-científicas e profissionais.
Valor ético	Concernente ao comportamento informacional dos sujeitos condizentes com a conduta moral.
VALORES CONSEQUÊNCIAS	
Refere-se ao caráter processual da informação, envolvendo as formas de organização, uso, venda compra, troca, compartilhamento e socialização.	
Tipos de valores consequências	**Aspectos valorativos da informação**
Valor de produtividade	Desenvolvimento de atividade gerencial de qualidade e oferta de serviços dos sujeitos institucionais que visem à satisfação das necessidades de informação dos usuários/clientes.

(Conclusão do quadro 1)

Tipos de valores consequências	Aspectos valorativos da informação
Valor de serviço	Consequência do valor de produtividade que reside em serviços de atendimento, rapidez, qualidade do produto ou processo oferecido.
Valor de organização	Relativa ao valor estruturador da informação no sentido de disponibilizá-la da forma mais adequada possível para os sujeitos da informação.
Valor de uso	O valor de uso da informação engloba perspectivas de busca, recuperação e apropriação da informação, atreladas ao desenvolvimento de competências, planejamento e manejo com as fontes e tecnologias de informação que sejam salutares para a construção do conhecimento.
Valor de troca	Valor de troca da informação se dá a partir do compartilhamento de alguma informação pelo sujeito, visando receber nova informação de outro sujeito que lhe permita conceber novas práticas informacionais.
Valor de compra e venda	O valor de compra e venda envolve a prática de vantagens competitivas, em um mercado que exige atualizações no consumo de suportes da informação.
Valor de compartilhamento	O valor de compartilhamento da informação caracteriza-se por: partilha e troca entre sujeitos, o que ajuda na construção do conhecimento organizacional e pessoal.
Valor sociativo	Esse valor tem dois momentos complementares: o primeiro é inerente à apropriação dos sujeitos a partir da realidade concreta, permitindo a produção de informação; o segundo dá-se quando essa informação apropriada e eivada de sentidos se torna premente de ser aplicada à realidade social, como espécie de retorno daquilo que foi apropriado pelo sujeito.

Fonte: Adaptado de Silva (2017b).

De acordo com as indagações de Silva (2017b) no quadro 1, examina-se que a informação é constituída de um núcleo maior e que se subdivide em diferentes fenômenos que a ela agregam valor formando um todo. Para o autor, torna-se essencial entender e descobrir esses valores com uma visão tanto holística quanto gerencial, visto que esse fenômeno acontece a partir das práticas de interações entre os sujeitos, seu contexto e amplitude social (Silva, 2017b).

Conforme os valores da informação apresentados acima, Silva (2017b) faz uma junção de valores que evidenciam a fundamentação social presente na CI, embora estejam integrados à dimensão humana e tecnológica e esses diálogos se relacionam sempre. Em sua breve síntese da informação na CI, apresentada em outra produção científica, o autor argui:

> Atualmente a CI é um campo de fundamentação social aplicada muito mais preponderante, mas necessita do diálogo com a dimensão humana para norteamento/dimensionamento de teorias, conceitos e métodos, especialmente no âmbito dos sujeitos e com a dimensão tecnológica para aplicação de suas atividades com processos, gestão e fluxos informacionais (Silva, 2017a, p. 240).

Observa-se ainda que no quadro 1, Silva (2017b) aproxima valores ontológicos de caráter individual e coletivo, ou seja, existe uma preocupação direta do usuário da informação, desde o início até o final de uma questão informacional, com os valores humanos, seu contexto

social e a realidade existente. Nessa vertente, pode-se entender porque muito tem se discutido sobre valores éticos, morais, políticos e educativos da informação no panorama contemporâneo e no âmbito da CI, principalmente com os impactos das mídias sociais.

Ao aproximar as reflexões de González de Gómez (2017) ao texto de Silva (2017b), compreende-se, em maior grau, o valor da informação quanto aos valores éticos e morais. González de Gómez (2017) discute que as reflexões de ética da informação estão inseridas em questões complexas e expressivos conflitos de ordem moral, educacional, político, social e profissional relacionados ao valor da informação.

A mesma autora aponta que o uso das TIC e a confiabilidade da informação disponibilizada, entre outras questões de integridade da pesquisa, como a responsabilidade dos que proveem o acesso à informação, plágios, falsificação de documentos, publicidade, desinformação, o papel do testemunho da informação, carece de um olhar mais profundo voltado para a educação e conscientização desses problemas (González de Gómez, 2017).

Na mesma concepção, Pizarro, Poleza e Lopes (2018) entendem que o valor ético da informação se relaciona com os fenômenos informacionais em um contexto científico e social amplo, determinando muitos outros valores. Para as autoras, a ética no campo de ensino e pesquisa se torna essencial e deveria estar instituída nas grades curriculares dos cursos porque a sua prática busca atender a função social da profissão, da pesquisa, da divulgação científica e, principalmente, as questões da responsabilidade social para os profissionais da informação.

Finalizando a análise de Silva (2017b), sobre os valores consequências, descritos no quadro 1, esses são designados a partir da importância e o valor que a informação ocupa em suas variadas funções, elencando o valor da informação para o usuário e para sua produtividade, principalmente no âmbito organizacional, no qual se torna mais evidente a forma de organização, o uso, venda, compra, troca e compartilhamento da informação.

Carvalho e Tavares (2001) analisam o valor da informação através das possiblidades do seu uso e apreensão como fator desencadeante da construção do conhecimento organizacional, ou seja, “Organizações alimentam-se de informações, e ao mesmo tempo são direcionadas por elas, de forma que fornece o sentido de uma organização ser” (Carvalho; Tavares, 2001, p. 3).

Nessa questão, o sinal verde dado pela GC se ilumina e abre espaço para vertentes do processo de inteligência competitiva, vantagem competitiva, aprendizagem organizacional e outros fenômenos informacionais, a partir do contexto em que são produzidos e plausíveis de valores e significados a eles atribuídos (Valentim, 2008).

Nessa linha, pode-se incluir Santos e Valentim (2020), as quais reconhecem na informação o valor estratégico de causa e efeitos aos processos, produtos e serviços no contexto organizacional, estando esses associados aos valores listados por Silva (2017b) como valores consequências. As autoras entendem que a informação e o conhecimento são os principais ativos da informação, indicando que:

> As organizações devem ter visão ampla do valor econômico, social e cultural da informação e do conhecimento, e devem ter noção do seu valor pragmático, pois são cíclicos, desconhecem limites e se revitalizam com o uso, criando potencialidades estratégicas (Santos; Valentim, 2020, p. 591).

Ao analisar os valores compartilhados no quadro 1, pode-se entender que existe uma relação inseparável entre a informação e valor que pode ser atribuído a partir de diferentes contextos na perspectiva do usuário, consumidor ou cliente, dependendo do objetivo e utilidade que seja elaborada.

Considera-se aqui que as discussões elencadas nessa seção abordaram algumas questões pontuais sobre a inter-relação da informação e seu valor no panorama atual, levando a reflexões de que, embora pautada no modelo econômico tradicional, não se restringe à área econômica, mas essencialmente está voltada para suprir satisfação informacional sob diferentes enfoques, estimulando valores existentes e acrescentando novos valores que movem a sociedade em geral.

Outro ponto relevante que vem acrescentar o desenvolvimento dessa pesquisa é o reconhecimento do valor da informação e da relação do seu poder para a geração de conhecimento. A partir desses conceitos e debates, as próximas seções exploraram de maneira mais precisa as questões de segurança da informação e a informação em rede.

2.1 Era da Informação: características e desafios

Vivencia-se atualmente inúmeras transformações quanto ao uso da informação, estando a sua gestão no cerne dos processos informacionais promovidos pelos avanços tecnológicos, os quais compõem a era da informação.

Fatos históricos influenciaram e prepararam a base das mudanças tecnológicas para o desenvolvimento da informação em rede, mas não ocorreram de forma isolada, pois mesmo antes dos avanços tecnológicos a informação já desempenhava papel fundamental na evolução social das civilizações.

A esse respeito, Cardoso (2005), fascinado pelos processos de mudança social da era da informação e da sociedade conectada em rede, explica que a transformação digital passou

por mudanças sociopolíticas, transitando da antiga sociedade industrial para a emergência de uma sociedade informacional, fundamentada por dois aspectos básicos: “a tecnológica, expressa por meio da difusão da Internet, e pela aparição na estrutura e na prática social da sociedade em rede” (Cardoso, 2005, p. 58).

Para Silva (2017a), a era da informação vinha se anunciando desde a revolução científica no século XIX e da crise da cultura econômica capitalista do século XX, institucionalizando-se com a transição da era industrial para a era informacional, a qual ganhou força com a ascensão da revolução tecnológica e os avanços científicos e culturais, culminando em mudanças significativas em todos os setores da sociedade.

Buscando caracterizar a era da informação, Silva (2017a) apresenta reflexão conceitual, por ele elaborada, fundamentada em perspectiva multifacetada quanto ao quadro de renovação, formação e reformulação do intenso processo de desenvolvimento das relações sociais, políticas e econômicas instigadas pela revolução tecnológica e cultural:

> A Era da Informação é mais do que uma prática científica; mais do que uma prática social; mais do que um discurso político; mais do que uma demanda institucional; mais do que uma política econômica; mais do que uma cultura engessada; e mais do que um desenvolvimento tecnológico. A Era da Informação se configura na (re)união, (re)formação, redistribuição, revisão e modificação de todos esses fatores agregados (Silva, 2017a, p. 36).

Inevitavelmente, Silva (2017a), como pesquisador da CI, possui uma visão direcionada para as TIC e seu potencial para reorganizar e ordenar as atividades relacionadas a informação como objeto científico e o seu valor social. Pode-se apreciar na reflexão de Silva (2017a), que o papel da informação nesta nova era incide no seu protagonismo subsidiado pela internet, ou seja, toda revolução tecnológica rompeu as fronteiras de tempo e espaço, atribuindo à informação um valor que se funde às questões científicas, econômicas, políticas e socioculturais.

Como pesquisadoras da área da CI, assim como Silva (2017a), Delbianco e Valentim (2022) exploram a temática situando a informação no núcleo dos processos informacionais, tecnológicos e de transformação social. As autoras destacam como marco histórico para a era da informação, a terceira fase da revolução industrial, quando aconteceu a revolução técnico-científica, conhecida como revolução da informação, período esse em que a informação passou a ter valor econômico devido aos avanços da tecnologia e das telecomunicações. Para as autoras, a era da informação está alicerçada no tripé: “informação, tecnologia da informação e telecomunicação” (Delbianco; Valentim, 2022, p. 1).

Na linha dos impactos promovidos pelos avanços tecnológicos, Paletta, Moreiro-González e Vergueiro (2020) investigam os desafios frente as transformações digitais, principalmente no âmbito da CI. Os autores apoiam que as principais mudanças na atuação dos profissionais da informação estão relacionadas aos processos de produção, gestão e recuperação da informação, demandando o desenvolvimento de novas habilidades e competências.

Paletta, Moreiro-González e Vergueiro (2020), ressaltam ainda que o grande desafio para esses profissionais está em reconhecer e buscar novas oportunidades, com ações proativas, criativas e sustentáveis, desenvolvendo competência digital, *digital literacy*, com a devida atenção aos padrões éticos. Esses autores concordam que a TI exerce papel fundamental na gestão e organização da informação e do conhecimento, permitindo inclusive "a universalização do acesso à informação" (Palletta; Moreiro-González; Vergueiro, 2020, p. 362).

Lévy (2009) apresenta reflexões oportunas para se repensar os caminhos que os homens traçaram frente aos avanços tecnológicos e, em especial, da aprendizagem advinda da emergência do ciberespaço.

O autor acrescenta ainda que, o conhecimento reside na humanidade e dele emana a capacidade de criar, inovar e modificar a cultura de uma sociedade, portanto, em termos gerais, a evolução sociocultural está condicionada aos avanços tecnológicos, contudo, não são por eles determinada. O autor enaltece que toda e qualquer transformação sociocultural deve ser sempre reavaliada com o passar do tempo (Lévy, 2009).

Quanto a emergência de novas técnicas e avanços tecnológicos, Lévy (2009) argumenta que, desde os primórdios da humanidade, condicionaram mudanças socioculturais que aconteceram por meio de uma relação de dependência entre suas causas e efeitos, as quais sozinhas não foram determinantes. O autor cita como exemplo, o revolucionário invento dos tipos móveis de Johann Gutemberg, no Século XV, que abriu possibilidades para o desenvolvimento da moderna ciência europeia, a crise da reforma e o crescimento das ideias iluministas, contudo, não foi o fator determinante. Partindo dessa prerrogativa, Lévy (2009, p. 29) arrazoa:

> As verdadeiras relações, portanto, não são criadas entre "a" tecnologia (que seria da ordem da causa) e "a" cultura (que sofreria os efeitos), mas sim entre um grande número de atores humanos que inventam, produzem, utilizam e interpretam de diferentes formas as técnicas.

Castells (2013) também entende que as redes já eram uma tendência na antiga forma de organização humana, apontando que dados históricos revelam a existência de redes como estrutura fundamental da vida em sociedade. O autor explica que as redes de comunicação eram

a espinha dorsal das sociedades antigas, principalmente para aquelas que detinham o poder, recursos e o sustento além das suas fronteiras geográficas.

Em sua retrospectiva histórica, Castells (2013) descreve que a partir da Revolução Industrial algumas tecnologias, como a rede de energia, o caminho-de-ferro e o telégrafo, constituíram uma infraestrutura de rede quase global.

O mesmo autor explica que, fundamentada na revolução da microeletrônica, nas décadas de 1950 e 1960, aconteceu a transformação das TIC, assentando as bases do paradigma tecnológico consolidado nos anos 70, nos Estados Unidos da América (Castells, 2013).

No que se refere a criação da internet, Castells (2013) relata que inicialmente estava associada as pesquisas militares vinculadas a Agência de Projetos de Pesquisa Avançada ou *Advanced Research Projects Agency* (ARPA) nos Estados Unidos da América (EUA). A ARPA criou a primeira rede de computadores denominada *Advanced Research Projects Agency Network* (ARPANET) no Ano de 1969, que na Década de 80 passou por transformações e foi denominada ARPANET/INTERNET e, posteriormente, INTERNET.

Conforme o autor supracitado, em meados de 1995 a internet passa a ser disponibilizada em escala mundial, produto de um esforço conjunto de interesses militares, científicos, pesquisas tecnológicas e de um movimento contracultural, chegando ao status atual de uma cultura empresarial (Castells, 2013).

Silva, Pereira e Morais (2018) descrevem os inventos do computador programável e o transistor (chip) como revolucionários para esta mudança paradigmática, avançando para o início dos Anos 80 e chegando ao computador manual para o mercado de softwares e microcomputadores. Conforme os autores, esses inventos associados aos avanços na área de telecomunicações, como a transmissão via satélite, micro-ondas e telefonia celular estabeleceram a revolução da TI.

Castells (2013) complementa que, o marco da revolução tecnológica emergiu da crise financeira global no final de 2008, que acompanhou o período de transição da primeira Década do Século XXI, anunciada pela inovação tecnológica. Na sequência desses avanços, o autor detecta uma nova estrutura social, a qual denomina de sociedade em rede, gerada no seio das mudanças radicais no âmbito da comunicação e das tecnologias digitais.

Toda a expansão global da sociedade em rede digital foi moldada a partir da internet, “o mais revolucionário meio tecnológico da Era da Informação” (Castells, 2013, p. 82), que descortinou a revolução da TI com sua principal matéria prima: a informação.

Castells (2013) reforça que amparado no valor da informação, na sua comunicação interativa e através dos seus conteúdos digitais, a sociedade em rede veio remodelar a sociedade,

alicerçada nas transformações técnico-econômicas e sociais. Convém relatar na fala do autor, como essas transformações se revelam:

> O que caracteriza a atual revolução tecnológica não é a centralidade de conhecimentos e informação, mas a aplicação desses conhecimentos e dessa informação para a geração de conhecimentos e de dispositivos de processamento/ comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso (Castells, 2013, p. 69).

Observa-se que no campo da CI, área de interesse desta pesquisa, as principais mudanças permearam a área tecnológica e social, com maior ênfase aos processos informacionais. Sobre esse fato, Roza (2018) concede que os avanços tecnológicos estruturaram um novo relacionamento entre a informação e os seus usuários, ocasionada principalmente pela interoperabilidade.

Roza (2018), aponta a internet como mola mestra para as mudanças nos processos de fluxo da informação e principal mecanismo para a disseminação da informação, contudo, a autora relata alguns problemas informacionais que surgiram nesse meio, citando entre outros: sobrecarga de informação, falta de confiabilidade e a própria segurança da informação.

Desenvolvendo seus estudos no campo da CI, Marteleto (2010) designa a internet como a "rede das redes" porque possui amplitude mundial e suporte de interação, comunicação e sociabilidade entre os atores sociais e as organizações e a sociedade em geral.

A mesma autora destaca dois grandes aspectos sobre a internet na sociedade da informação, a saber: "Primeiro, é um grande acervo de dados e de informações escritas, consultas, leituras, usos e apropriações. Segundo, é uma arena ampliada geograficamente e socialmente para interação, comunicação e sociabilidade" (Marteleto, 2010, p. 32).

Para mensurar o impacto da informação em rede no mundo, Jenkins (2013) arrazoa que o mundo vive uma cultura de convergência, na qual a comunicação acontece a partir de diferentes fenômenos que interligam os indivíduos e as organizações utilizando diferentes meios a partir da internet.

Jenkins (2013) identifica um novo paradigma que apresenta, através da internet, uma nova cultura midiática, a qual está configurada em uma forma ativa de consumir cultura por meio de diferentes mídias possibilitadas pelas tecnologias digitais. O autor defende que a internet oferece uma cultura participativa, em que o uso das mídias deve estar associado também à inteligência competitiva e, nesse sentido explica:

> Meu argumento aqui será contra a ideia de que a convergência deve ser compreendida principalmente como um processo tecnológico que une múltiplas funções dentro dos mesmos aparelhos. Em vez disso, a convergência representa uma transformação cultural, à medida que consumidores são incentivados a procurar novas informações e fazer conexões em meio a conteúdos de mídia dispersos (Jenkins, 2013, p. 29).

Para o autor, existe uma conexão imediata e cortejada por inúmeras plataformas e sistemas de mídias que convergem a partir das transformações tecnológicas, mercadológicas, culturais e sociais. Essa conexão impõe múltiplos desafios que descortinam a revolução do conhecimento (Jenkins, 2013).

Certamente, com novas possibilidades de desenvolvimento e, ao mesmo tempo, novos desafios, a era da informação abriu espaço para profundas discussões que se enlaçam entre questões de desigualdades sociais e digitais, interesses econômicos, políticos e dilemas que provocam a exclusão digital.

Sobre esse questionamento, Castells (2003) explica que a internet está alicerçada em seu potencial de liberdade, produtividade e comunicação, contudo, a realidade denuncia uma "divisão digital", que para o autor é gerada devido a desigualdade já existente e enraizada pela sociedade em classe, educação, gênero e etnia, como uma forma de poder para opressão e exclusão digital, a saber:

> A Internet é de fato uma tecnologia da liberdade - mas pode libertar os poderosos para oprimir os desinformados, pode levar à exclusão dos desvalorizados pelos conquistadores do valor. Nesse sentido geral, a sociedade não mudou muito (Castells, 2003, p. 186).

O autor explica que essa desigualdade se estabelece também por seu uso diferencial no mundo em desenvolvimento, ou seja, envolve fatores econômicos e de poder com relação a disparidade de provedores, infraestrutura de comunicação, os conteúdos de internet e as tímidas estratégias para resolver o problema (Castells, 2003).

Abordar a questão da exclusão digital é como cruzar uma linha invisível, porém real: desencobrir velhos problemas em novos contextos. No bojo dos problemas de inclusão e acesso à informação, o mundo assistiu, com a pandemia de COVID-19, desde março de 2020, o testemunho de um cenário de exclusão e falta de acesso à internet que transitava silenciosamente pelo mundo.

Segundo dados da pesquisa "Democracia e representatividade", publicada sob a organização de Castro (2022) e em parceria com o Instituto Lula (IL), no segundo semestre de 2021, estima-se que entre a população total do planeta, 7,8 bilhões, 4,6 bilhões de usuários da rede são pessoas caracterizadas como incluídas (59%), 2,5 bilhões são caracterizadas como incluídas precariamente (32%) e 3,2 bilhões, cerca de 41 %, são pessoas totalmente excluídas do acesso à internet (Castro, 2022).

Castro (2022) chama a atenção para a situação das comunidades quilombolas, populações ribeirinhas e aldeias indígenas, que em sua maioria não têm acesso próximo a torres de transmissão, uma questão particularmente agravada nas regiões Norte e Centro-Oeste do

Brasil. Analisando esses dados à luz da pandemia de COVID-19, é evidente que muitos estudantes indígenas ou quilombolas enfrentaram dificuldades significativas para acessar a educação remota, o que pode ser um indicativo de exclusão digital (Castro, 2022).

A pesquisa “TIC Domicílios 2021” conduzida pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.BR) apresentou indicadores sobre o acesso e o uso das TIC no país no período de outubro de 2021 a março de 2022.

Enunciou que houve um aumento significativo de acesso à rede no país, passando de 71% em 2019 para 83% em 2020, embora ressalta que desigualdades históricas persistem e atingem as baixas classes sociais, a saber: ausência de computadores, baixa qualidade de conexão à Internet, alto custo de contratação da rede, dificuldades para análise e compartilhamento dos conteúdos, falta de domínio das plataformas, aplicativos, mídias digitais e uso dos aparelhos, somadas ao pouco conhecimento tecnológico e a falta de habilidade e competência digital (CETIC.BR, 2022).

As pesquisas revelam, por meio dos dados, que a exclusão digital ainda persiste entre as classes menos privilegiadas. Em outras palavras, simplesmente fornecer acesso a um dispositivo com internet não garante uma inclusão digital adequada, muitas vezes resultando em uma inclusão precária. Nesse contexto, diversos fatores têm um impacto direto, incluindo o desenvolvimento multidimensional do território brasileiro e a complexidade de seu sistema socioeconômico (Castro, 2022; CETIC.BR, 2022).

Corroborando as análises, Popova (2020) explica que para avaliar e abordar a desigualdade digital de forma eficaz, é essencial considerar tanto as características micro quanto macro dos problemas, em uma perspectiva que abranja toda a área territorial. Isso envolve a combinação de características objetivas e subjetivas, como eles ponderam:

> Assim, para formar um quadro completo da situação socioeconômica atual e conclusões sobre o grau de impacto no desenvolvimento da desigualdade digital não basta avaliar as características objetivas do sistema territorial, registadas em estatísticas, também é necessário determinar e fixar a atitude perante a situação dos indivíduos e grupos sociais (Popova, 2020, p. 7, tradução nossa).

Com base nas discussões apresentadas pelos autores nesta subseção, as mudanças tecnológicas e seu impacto global foram contextualizados. A era da informação trouxe uma transformação constante e irreversível em todos os aspectos da sociedade, proporcionando inúmeras vantagens no que diz respeito ao acesso e uso da informação em rede. No entanto, é igualmente essencial considerar as contradições presentes na realidade da sociedade da informação, o que pode levar a reflexão sobre os desafios e as oportunidades desse cenário em constante evolução.

2.2 Gestão da informação em sistemas informatizados

O desafio estratégico no contexto organizacional atual reside no eficaz gerenciamento e nas práticas relacionadas à GI. Predominantemente, as informações são administradas em ambientes digitais, tornando fundamental que os profissionais da área de informação demonstrem competência no manejo das novas abordagens para gestão de informações, contribuindo para a agregação de valor no contexto organizacional, conforme destacado por Valentim (2008).

Em termos retrospectivos, o gerenciamento da informação teve em sua gênese a influência da obra *Traité de Documentation: le livre sur le livre: théorie et pratique*, publicada por Paul Otlet em 1934, com proposta de organização do conhecimento em uma Rede Universal de Documentação (Ortega, 2009; Vieira, 2021), da explosão bibliográfica promovida pela invenção da imprensa de Gutemberg (1448) e pelos investimentos em pesquisa pelos governos no período pós-segunda guerra mundial, o qual Weitzel (2002, p. 61) chama de "florescimento técnico-científico". Somando-se a esses fatos, pode-se incluir os avanços das TIC, na Década de 80, os quais impulsionaram os serviços de informação, organização e recuperação da informação (Weitzel, 2002).

Embora não seja o propósito dessa pesquisa discutir exaustivamente a GI e sua interação com a GD, torna-se essencial entender suas peculiaridades. A Câmara Técnica de Documentos Eletrônicos (CTDE), do Conselho Nacional de Arquivos (CONARQ), prevê que o sucesso dos SIGAD necessita previamente da implantação de uma política de GD objetivando apoiar e subsidiar a GI (CONARQ, 2022).

Posto isto, Santos (2015) argumenta que o foco da GC está no fundo arquivístico dos documentos e a GI tem seu foco na informação como suporte à eficácia administrativa por meio dos seus processos informacionais. Para o autor, a informação arquivística contempla todos dos dados e informações de um SI ocupando um conceito amplo no viés digital:

> Aquela acumulada (produzida e recebida) pela instituição no exercício de suas funções e atividades, ou por pessoa física no decurso de sua existência, atendendo ou não aos requisitos de fixidez de forma e conteúdo (documento), servindo para registrar, contextualizar e permitir compreensão de ações envolvendo a instituição [ou pessoa] (Santos, 2015, p.114).

Viana e Valls (2016) complementam que a GD, por se concentrar na proveniência dos seus fundos, em seu registro, tratamento e conservação nas bases da diplomática e tipologia documental, pode ser considerada como auxiliar nos processos da GI. Os autores entendem que o foco da GD está na "criação, avaliação, classificação, descrição e acessos das informações

registradas em documentos" (Viana; Valls, 2016, p. 22), enquanto a GI tem seu foco na "aquisição, organização, controle, monitoramento, disseminação e uso da informação" (Viana; Valls, 2016, p. 22).

Para Santos (2021), a GD se relaciona diretamente com a informação orgânica e as práticas arquivísticas, desde a criação dos documentos úteis até a sua guarda, objetivando assim a otimização do uso e acesso à informação em seus variados suportes. Para a autora, ambas estão estruturadas no valor da informação e ocupam papel preponderante porque "o potencial para apoiar decisões, antecipar demandas e replicar boas práticas é real" (Santos, 2021, p. 106).

Corroborando com a mesma linha de pensamento, Santos e Valentim (2021) apontam que "muitas vezes a GI se traduz no conhecimento dos sujeitos organizacionais, cujo uso e/ou aplicação pode gerar nova informação estratégica para a organização" (Santos; Valentim, 2021, p. 15). Essas autoras entendem em termos consensuais, que os processos de GD e de GI potencializam o valor da informação como fator de competitividade.

Para Monteiro e Duarte (2019), o progresso conceitual do termo GI teve o seu marco com a proposta apresentada pela Lei *Paperwork Reducion Act* (P.R.A) promulgada em 1978, à qual tinha por objetivo o controle da documentação produzida pela população e empresas por parte do governo dos EUA. Os autores apoiam que a GI se consolidou na Década de 90, que quando apoiada pelas TIC passou a ser utilizada como gestão estratégica junto as empresas, tornando-se "ferramenta fundamental no processo de gestão das organizações, no intuito de oferecer a qualidade e eficácia dos sistemas dessas" (Monteiro; Duarte, 2019, p. 94).

Estando a informação registrada, as empresas devem organizar, usar e compartilhar a informação como um bem econômico, visto que para que possam alcançar os resultados esperados é preciso usar a informação como fator estratégico e a GI apoia estas ações por possuir características com "finalidade concreta, tangível e visível" (Almeida; Biaggi; Vitoriano, 2021, p. 8).

Barboza e Fadel (2017) atentam para a multiplicidade de informações inseridas no fluxo informacional, as quais de forma dinâmica e contínua, são compostas por fluxos formais, que estão formalizados em sistemas e se relacionam com a GI, enquanto os fluxos informais estão intrínsecos no conhecimento tácito das pessoas e se relacionam com a GC. Para as autoras, os fluxos formais e informais em dado momento se relacionam e a informação formal é posteriormente utilizada na GC. Na perspectiva dos diferentes processos da GI e da GC, Valentim (2004) complementa que ambas estão diretamente relacionadas com a GI, devendo a organização sistematizar tanto os fluxos formais quanto os informais, ou seja, "desenvolver

sistemas corporativos de diferentes naturezas, visando o compartilhamento e uso da informação" (Valentim, 2004, p. 31).

A GI, conforme a definição de Moraes e Fadel (2009), abrange o processo complexo de gerenciamento dos fluxos de informações formais e do ciclo de vida dessas informações dentro de uma organização. O objetivo fundamental da GI é a consecução de metas estratégicas, o que requer a consideração cuidadosa de diversos fatores, incluindo aspectos tecnológicos, questões humanas e a dinâmica da comunicação organizacional. Essa abordagem integrada busca assegurar que a informação seja adequadamente coletada, organizada, armazenada, disseminada e utilizada para melhorar a tomada de decisões e, consequentemente, o desempenho da organização como um todo.

Conforme enfatizado por Tarapanoff (2001, p. 44), a essência da GI reside em "Identificar e potencializar os recursos informacionais de uma organização e sua capacidade de informação, ensiná-la a adaptar-se às mudanças ambientais". Esses recursos são considerados um alicerce fundamental para impulsionar a inovação e promover a construção do conhecimento dentro da organização, como ressaltado por Barboza (2019).

Assis (2008) concorda que a GI tem um impacto direto nos resultados dos negócios e, portanto, deve estar perfeitamente alinhada com a missão e os objetivos estratégicos da organização, além de contar com o suporte dos recursos das TIC. Essa perspectiva estratégica da GI pode ser complementada pela definição clássica de Davenport e Prusak (1998, p. 173):

> [...] um conjunto estruturado de atividades que incluem o modo como as empresas obtém, distribuem e usam a informação e o conhecimento [...] identificar todos os passos de um processo informacional – todas as fontes envolvidas, todas as pessoas que afetam cada passo, todos os problemas que surgem – pode indicar o caminho para mudanças que realmente fazem diferença.

A incorporação da tecnologia nas organizações trouxe consigo a automação da informação, o que resultou em melhorias nas atividades e processos relacionados à informação. Isso teve um impacto significativo no fluxo de trabalho e nos resultados obtidos. Essa mudança nas práticas exigiu uma reavaliação das abordagens profissionais em relação à organização e ao gerenciamento da informação e do conhecimento, introduzindo uma perspectiva renovada nessa área.

Dutra e Barbosa (2020) realizaram uma análise minuciosa dos modelos e das fases de GI que são reconhecidos tanto na literatura nacional quanto internacional. Para isso, eles examinaram os modelos propostos por diversos autores renomados, tais como Beal (2005), Choo (2003), Davenport, Marchand e Dickson (2004), Sordi (2015), McGee e Prusak (1994), Ponjuán Dante (1998), Probst, Raub e Romhardt (2002), bem como Reginato e Gracioli (2012).

Essa análise contribuiu para um entendimento mais aprofundado das diferentes perspectivas e abordagens no campo da GI, conforme ilustrado na Figura 1

Figura 1 – Principais critérios mais frequentes nas etapas da GI

Fonte: Adaptado de Dutra e Barbosa (2020, p. 125).

Com relação aos critérios acima, os autores identificaram que existe um elevado grau de subjetividade na tradução dos termos, contudo, as contribuições da área tiveram ascensão marcante a partir dos anos 2000. De posse de uma visão baseada nas práticas profissionais pode-se supor que a virada do milênio aproximou os computadores e a internet para uma realidade tangível nas práticas organizacionais, motivo de muitas transformações que instigaram a sociedade em geral e as pesquisas no campo científico.

Dutra e Barbosa (2020) depreendem ainda que as etapas de mediação e acompanhamento de resultados, juntamente com as etapas que envolvem a supervisão, avaliação, manutenção e retroalimentação foram muito pouco mencionadas nos artigos analisados. Para os autores não existe um consenso sobre um modelo ideal para a GI.

Molina (2008) compreende que os sistemas informatizados potencializaram a dinâmica do fluxo documental melhorando a busca, controle e uso da informação para o

desenvolvimento da atividade fim das instituições. Para a autora, a automação possibilitou maior rapidez no acesso e recuperação da informação, gerando economia de tempo, custo e, principalmente, confiabilidade para o uso da informação na tomada de decisão, apontando esses fatores como indicadores para o desenvolvimento dos sistemas informacionais (Molina, 2008).

A nova realidade digital impulsionou a informação em rede, conectada e interativa, de forma que transformou a realidade e qualidade de gestão nas organizações. Para Jucá (2019), essas mudanças ultrapassaram as barreiras geográficas, e com as novas tecnologias os sistemas informatizados evoluíram e ampliaram os limites da competitividade e da inovação no universo organizacional, de tal forma que:

> O que já se tinha como conhecido e controlável dentro das organizações, hoje passam por mutações intensas de ordens diversas, tais como, econômicas, sociais, culturais, políticas, ideológicas e tecnológicas que impulsionam a metamorfose destes ambientes. A informação assume um papel fundamental na busca pela competitividade e sobrevivência das organizações, e sua gestão tornou-se a engrenagem estratégica que auxiliam os administradores, gestores e executivos no processo decisório (Jucá, 2019, p. 6).

Santos e Valentim (2021) atribuem o mesmo lugar de protagonismo da GI para recuperação da informação em SI, contribuindo com os processos decisórios. As autoras justificam que a GI apoia todas as ações voltadas para o planejamento e desenvolvimento organizacional por meio da sistematização dos fluxos formais da informação. Complementam ainda, que outro fator importante é a cultura organizacional positiva, a qual proporciona "uma comunicação informacional eficiente, por meio do uso da TIC, com o objetivo de prospectar e monitorar as fontes de informação" (Santos, Valentim, 2021, p. 13).

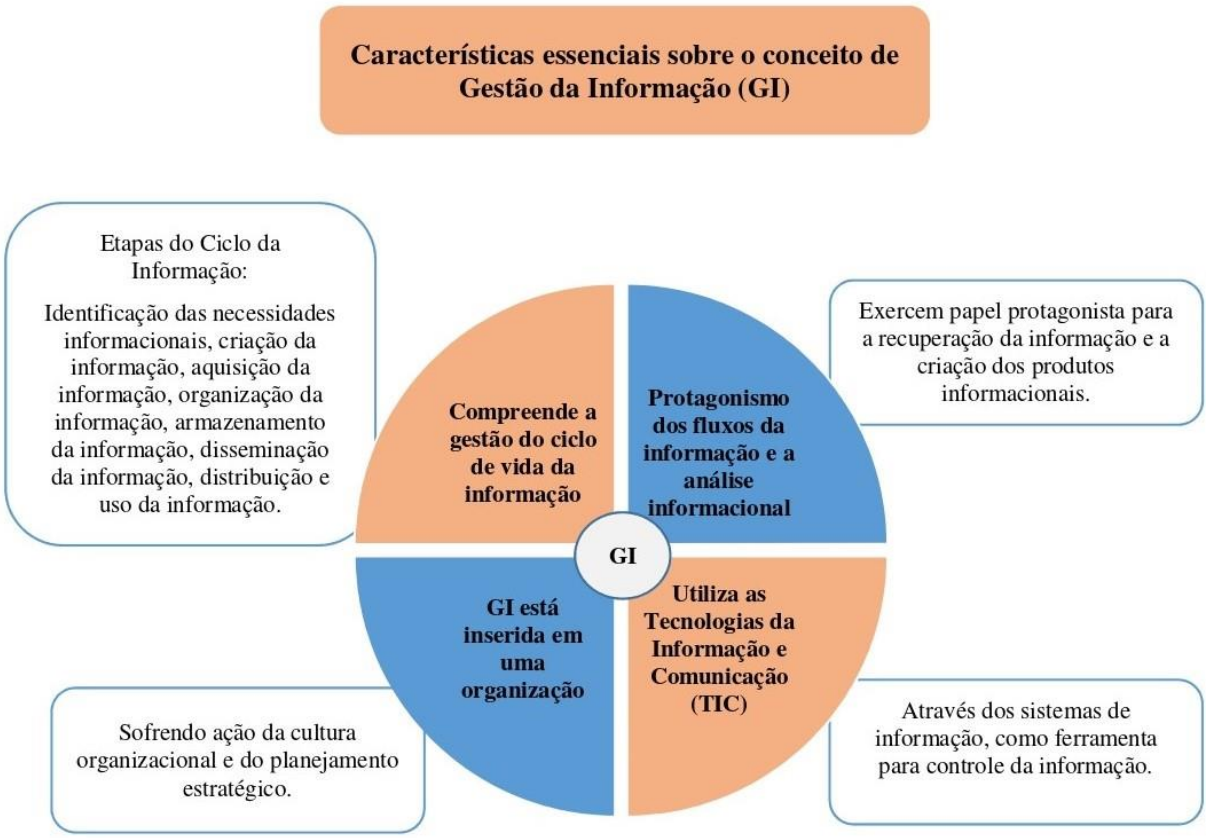
Nesse cenário, os sistemas de informação potencializam os recursos informacionais apoiando o conjunto de atividades administrativas e processuais, principalmente a gestão estratégica. Levando em consideração que o gerenciamento do fluxo informacional é essencial e gera valor à organização, o crescimento exponencial do universo digital desenvolveu a produção de recursos informacionais e otimizou as atividades e processos de trabalho (Santos; Valentim, 2021).

Nonato e Aganette (2022) salientam que a transformação digital redesenhou as práticas tradicionais de GI, demandando novas competências dos profissionais para uma abordagem mais sistemática da informação. Eles propõem uma revisão do conceito de GI à luz dos desafios da era digital, ressaltando a falta de uma definição consensual e contextualizada para GI no cenário atual.

É evidente que os princípios teóricos e conceituais da GI têm suas bases na CI e disciplinas correlatas. No entanto, é importante destacar que a constante evolução tecnológica exige uma revisão contínua desses conceitos e abordagens.

Nessa perspectiva, Nonato e Aganette (2022) conduziram uma revisão bibliográfica com o intuito de estabelecer uma definição contemporânea e amplamente aceita de GI. Com base nos princípios de indexação do Sistema Mundial de Informação Científica Tecnológica (UNISIST), eles propuseram quatro categorias fundamentais, visando contribuir para a formulação de uma definição abrangente e consensual de GI (Figura 2).

Figura 2 – Principais características essenciais sobre o conceito de GI



Fonte: Adaptado de Nonato e Aganette (2022).

Com base nas quatro características apresentadas pelos autores, fica evidente que a GI é uma disciplina que se apoia em diversos pilares fundamentais. Primeiramente, o ciclo de vida da informação desempenha um papel crucial na GI, pois envolve a coleta, a organização, o armazenamento, a disseminação e a utilização adequada das informações ao longo do tempo. Além disso, a GI está intrinsecamente ligada à gestão organizacional, pois visa aprimorar os processos de tomada de decisões e melhorar o desempenho da organização como um todo.

Nonato e Aganette (2022) destacam que as etapas do ciclo de vida da informação devem ser aplicadas de forma a atender às necessidades informacionais existentes e também

para dar suporte a outras atividades que possam surgir, contribuindo assim para a tomada de decisões eficazes. Santos (2021) reforça a importância da identificação das necessidades informacionais como um elemento fundamental para orientar as fases de mapeamento e monitoramento da gestão do ciclo da informação. Isso pode promover uma cultura informacional visionária e até mesmo antecipar a obtenção de resultados mais eficazes nos processos e produtos de uma organização.

Ainda de acordo com Nonato e Aganette (2022), outra característica relevante que deve ser considerada na definição atual e consensual de GI é o papel central que os fluxos informacionais desempenham. Eles destacam que a recuperação da informação e a geração de produtos informacionais ocorrem de forma integrada e holística na organização, alinhando-se com metas, objetivos e processos decisórios. Isso enfatiza a importância da GI como um elemento estratégico no contexto organizacional.

Nos modelos clássicos de GI, como proposto por Choo (2003) e Davenport (1998), as necessidades informacionais são amplamente evidenciadas, sugerindo-se que cada organização deve elaborar e estabelecer as etapas de GI de acordo com sua estratégia de gestão e as necessidades informacionais. Essas necessidades emergem em resposta às exigências e objetivos estabelecidos pela organização. A identificação e solução de problemas desencadeiam a busca por informações, integradas às práticas e rotinas cotidianas da organização.

A literatura consolidada aponta para importantes modelos elaborados com as principais etapas da GI nas organizações. Esses modelos caracterizam alguns requisitos que norteiam as principais características de um SIGAD. Consequentemente, a comunicação e a GI nas organizações ocorrem, na atualidade, predominantemente por meio de sistemas informatizados. Nesse contexto, as próximas discussões se concentrarão na análise do SIGAD.

2.3 Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD)

Os sistemas informatizados desempenham um papel fundamental no dia a dia das organizações, desempenhando um papel essencial na facilitação da produção e controle do fluxo de informações. Eles representam uma abordagem inovadora que contribui significativamente para a gestão estratégica das organizações.

A base conceitual de Bertalanffy (2010), um renomado teórico da Teoria Geral dos Sistemas (TGS), oferece uma abordagem sistêmica para os sistemas de informação, enfocando uma visão complexa da organização e destacando a interconexão entre seus diversos setores em busca de um objetivo compartilhado. A interdependência entre os sistemas e seus constituintes

é para o autor "uma transformação nas categorias básicas de pensamento da qual as complexidades da moderna tecnologia são apenas uma – e possivelmente não a mais importante – manifestação" (Bertalanffy, 2010, p. 22).

Conforme as ideias apresentadas por Bertalanffy (2010), tornou-se essencial, em todos os campos do conhecimento e atuação, lidar com as mudanças provocadas pelos sistemas e sua complexidade. Da mesma forma, é imperativo reavaliar a abordagem na resolução de problemas e na criação de soluções de maneira integrada e otimizada, considerando essa complexidade.

Laudon e Laudon (2010) destacam que as TIC, incluindo computadores e sistemas operacionais, tiveram um impacto significativo na evolução das práticas de GI e na comunicação da informação através dos sistemas de informação, principalmente com a crescente adoção do formato digital. Isso resultou em mudanças nos métodos de registro da informação, abrangendo suportes convencionais, híbridos e digitais, o que ampliou os conceitos tradicionais de práticas arquivísticas. A definição de sistema de informação apresentada pelos autores está relacionada intrinsicamente com as práticas da GI e da GC, a saber:

> Um Sistema de Informação (SI) pode ser definido tecnicamente como um conjunto de componentes inter-relacionados que coletam (ou recuperam), processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização. [...] esses sistemas também auxiliam os gerentes e trabalhadores a analisar problemas, visualizar assuntos complexos e criar novos produtos (Laudon; Laudon, 2010, p.12).

Para Marcial, Gomes e Marques (2015), dentro de um conceito dinâmico e complexo, um sistema de informação é composto por vários subsistemas centrados no valor operativo da informação alinhado ao domínio da GI, objeto de interesse da CI. As autoras entendem que a multiplicidade de sentidos da base conceitual do sistema de informação se dá pela própria complexidade das organizações, as quais integram um macrossistema social que é representado por diferentes realidades, ou seja:

> Todos os SI estão, pois, e desde sempre, dinamicamente dependentes do universo orgânico que lhes dá origem, com a complexidade que naturalmente se vai gerando, e é esta realidade que deve ser reconhecida, numa evolução dinâmica diacrônica, como aquela que serviu e serve de contexto sistêmico envolvente (Marcial, Gomes; Marques, 2015, p. 7).

Para Rosini e Palmisano (2012), o sistema de informação está fundamentado nos princípios de processamento da informação para apoiar as decisões administrativas e operacionais da organização, projetados para atender as necessidades informacionais existentes de uma maneira geral, coordenando todos os seus subsistemas, assim definidos: "conjuntos de

elementos interdependentes que interagem para atingir um objetivo comum, que ajudará o sistema a atingir seu objetivo maior" (Rosini; Palmisano, 2012, p. 3).

Klettenberg (2016) aponta o imediatismo como uma das principais características da relação entre o usuário e o sistema de informação, acredita que quanto mais se estreita essa relação, maior a sua interação e atribui esses resultados à recuperação da informação e a própria segurança do sistema que resguarda o valor da informação.

A década de 90 foi marcada pelos avanços das TIC, que promoveram mudanças decisivas na forma de GI, destacando-se a informatização dos sistemas que vieram apoiar a gestão de ciclo de vida dos documentos em formato digital. Dentro de um universo tecnológico, diversos sistemas surgiram para o gerenciamento das informações em meio eletrônico. Apresenta-se o SIGAD, caracterizando os requisitos básicos para sua implementação, sua função, objetivos e bases conceituais. Esse tipo de sistema é o mais utilizado para gerenciar informação e processos na Administração Pública Federal (CONARQ, 2022).

O CONARQ (2022), considerando que o sistema de informação está associado ao controle da gestão do ciclo de vida dos documentos, conceitua o SIGAD como:

> Solução informatizada que visa o controle do ciclo de vida dos documentos, desde a produção até a destinação final, seguindo os princípios da gestão arquivística de documentos. Pode compreender um software particular ou um determinado número de softwares integrados, adquiridos ou desenvolvidos por encomenda (CONARQ, 2022, p. 20).

Segundo a CTDE do CONARQ, o SIGAD tem a funcionalidade de gerenciar a elevada produção de documentos produzidos de forma eletrônica, digital e híbrida de forma confiável.

Partindo da concepção de que as informações que são formalizadas e registradas nos sistemas de informação passam pelo processo de digitalização, com a pretensão de progressivamente se eliminar os trâmites físicos dos documentos, muitos conceitos foram apresentados para identificar as novas nomenclaturas de termos relacionados aos documentos e seus processos.

Cada dia as mudanças nos sistemas informacionais acontecem de forma tão acelerada que, antes que seus usuários dominem o seu uso, novas mudanças acontecem. Essas mudanças influenciaram também as práticas de tratamento da informação quanto a sua recuperação, ou seja, na conversão dos documentos convencionais em dados binários, precisa-se dominar a indexação dos assuntos e preencher os metadados com todas as informações necessárias para a sua recuperação.

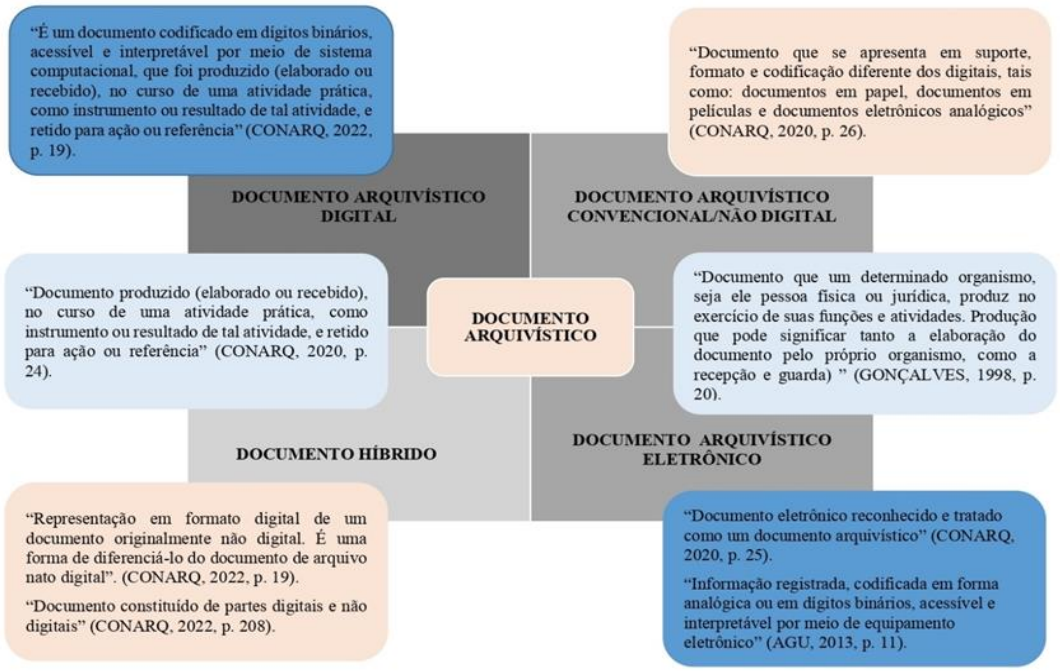
Santos (2012) discute que muitas são as dificuldades das instituições em controlar as práticas de uso e preservação de documentos em sistema de informação, quiçá as práticas de preservação. Para o autor, entender e definir os requisitos dos sistemas informatizados que garantam uma cadeia de custódia ininterrupta de criação, recepção, transmissão, manutenção e descarte dos documentos é fundamental para adoção de uma política de gestão de documentos arquivísticos digitais.

Nesse sentido, a Lei nº 12.682 de 9 de julho de 2012, que trata da elaboração e o arquivamento de documentos em meios eletromagnéticos, dispõe em seu Art. 4º, a seguinte recomendação:

> As empresas privadas ou os órgãos da Administração Pública direta ou indireta que utilizarem procedimentos de armazenamento de documentos em meio eletrônico, óptico ou equivalente deverão adotar sistema de indexação que possibilite a sua precisa localização, permitindo a posterior conferência da regularidade das etapas do processo adotado (Brasil, 2012).

Baseado nos conceitos da CTDE (CONARQ, 2020; 2022), pela Coordenação-Geral de Gestão da Documentação e Informação (CGDI) da AGU (2013) e por Gonçalves (1998), a figura 3 apresenta as nomenclaturas atribuídas aos documentos arquivísticos presentes nos SIGAD.

Figura 3 – Novas definições de documentos arquivísticos



Fonte: Adaptado de CONARQ (2020; 2022), CGDI/AGU (2013) e Gonçalves (1998).

Outro conceito importante que faz referência aos documentos arquivísticos digitais e eletrônicos é a assinatura eletrônica. Essa modalidade foi prevista pelo Art. 3º, da Lei nº 12.682/2012, que trata da assinatura eletrônica: "O processo de digitalização deverá ser realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento digital, com o emprego de assinatura eletrônica" (Brasil, 2012).

Segundo o Instituto Nacional de Tecnologia da Informação (ITI), autarquia vinculada à Presidência da República, antes que se proceda uma assinatura digital é preciso obter uma certificação digital através da Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil), ou identidade virtual, que é um produto ou software personalizado. De posse dessa certificação, a assinatura digital ganha validade jurídica, permitindo o dinamismo dos processos de validação para os documentos (Brasil, 2017). O ITI explica que a assinatura digitalizada difere da assinatura digital, ou seja, a primeira reproduz a assinatura manuscrita como imagem, não garantindo a autoria e integridade do documento eletrônico (Brasil, 2017).

Segundo glossário dos termos arquivísticos digitais (CONARQ, 2020, p. 11), entende-se por assinatura digital "Modalidade de assinatura eletrônica, resultado de uma operação matemática, que utiliza algoritmos de criptografia e permite aferir, com segurança, a origem e a integridade".

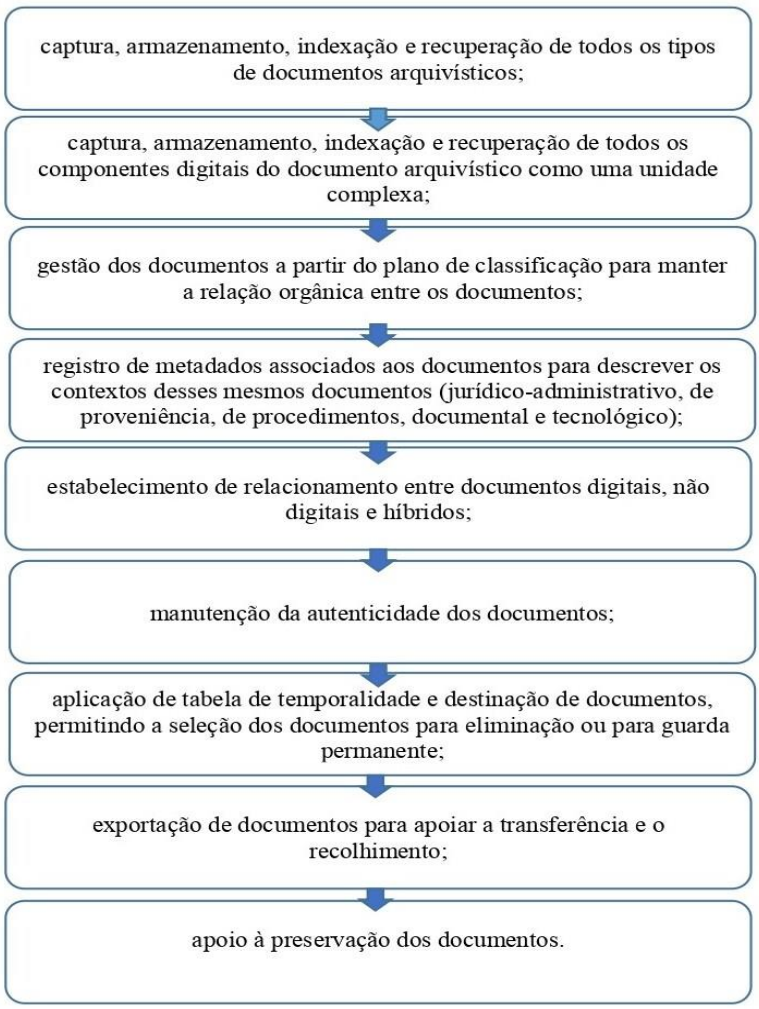
Ainda com relação aos documentos arquivísticos, segundo declara a CTDE (CONARQ, 2022), um SIGAD gerencia diferentes documentos que podem ser digitais, não digitais e híbridos. Quanto aos documentos convencionais, o sistema inclui em seus registros apensas as informações pertinentes ao seu número de protocolo, código de classificação e data. Deve-se preencher os metadados exaustivamente para que as informações possibilitem a recuperação da informação, visto que, somente os documentos digitais podem ser incluídos. Para os documentos imagéticos, audiovisuais e sonoros, entre outros, o SIGAD requer a adoção de metadados específicos pelo sistema de informação (CONARQ, 2022).

A CTDE elaborou os requisitos funcionais para a implantação de um SIGAD, publicados no Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil). Em sua versão inicial, o documento tinha sido baseado no Modelo de Requisitos para a Gestão de Arquivos Eletrônicos (MOREQ, 2001), publicada no início do ano 2000, estando hoje na sua versão 2, produzido pelo CONARQ em junho de 2021. A principal função do e-ARQ é "uniformizar o desenvolvimento e aquisição de sistemas que visem produzir e manter documentos arquivísticos em formato digital" (CONARQ, 2022, p. 11).

De acordo as orientações para contratação de SIGAD e serviços correlatos previstos na Orientação Técnica nº 1, de abril de 2011, o SIGAD abrange todas as fases do ciclo documental, e implantado em conformidade com as funcionalidades do e-ARQ Brasil apresenta benefícios que, além de aperfeiçoar e padronizar o ciclo de vida da informação, a interoperabilidade entre os sistemas e a integração das áreas da TIC com o arquivo e a administração, possibilita "confiabilidade, a autenticidade e o acesso aos documentos arquivísticos em todo o seu ciclo de vida" (CONARQ, 2011, p. 4)

Segundo preconiza o modelo de requisitos para o SIGAD adotado pelo e-ARQ Brasil (CONARQ, 2022), os principais requisitos arquivísticos que o caracterizam estão descritos na figura 4.

Figura 4 – Requisitos arquivísticos que caracterizam um SIGAD



Fonte: Adaptado do CONARQ (2022, p. 21).

A CTDE procura acompanhar a implementação dos requisitos do e-ARQ na avaliação dos sistemas, a exemplo destaca a participação de seus integrantes na implantação dos sistemas da Unicamp, Câmara dos Deputados, Tribunal Regional Federal da 2ª Região e da

Empresa de Processamento de Dados da Previdência Social (DATAPREV), incluindo nesse rol a implantação do sistema SAPIENS AGU (CONARQ, 2022). Para a CTDE, a participação de seus integrantes na estruturação e implementação desses sistemas proporciona uma visão prática em diferentes contextos organizacionais, o que reverte em ações e reflexões que podem trazer revisão e possíveis mudanças no esquema de metadados.

Uma outra questão que se evidencia quando o tema é sistema de informação são as diferenças consideráveis que existem entre o SIGAD e o sistema de GED. Embora se apresentem como solução tecnológica para o gerenciamento dos documentos por meio de sistemas informatizados, o CONARQ (2022) explica que o GED realiza um tratamento compartimentado da informação, enquanto o SIGAD possui uma abordagem orgânica e arquivística, com uma política de GI definida e voltada para as atividades da instituição a qual se insere.

Segundo o CONARQ (2020, p.31), o GED pode ser definido como:

> Conjunto de tecnologias utilizadas para organização da informação não estruturada de um órgão ou entidade, que pode ser dividido nas seguintes funcionalidades: captura, gerenciamento, armazenamento e distribuição. Entende-se por informação não estruturada aquela que não está armazenada em banco de dados, como mensagens de correio eletrônico, arquivo de texto, imagem ou som, planilhas etc.

Ainda na linha de uma definição clássica de GED, Avedon (2002, p. 11) assim o define:

> O Gerenciamento Eletrônico de Documentos (GED) é uma configuração de equipamento, software e, normalmente, de recursos de telecomunicações baseada em computador e automatizada que armazena e gerencia imagens de documentos – e seus índices codificados – que podem ser lidas por máquinas e processadas por computador para recuperação sob solicitação.

O CONARQ (2020) aponta que as principais diferenças entre o SIGAD e o GED estão nos seus objetivos, enquanto o SIGAD objetiva o documento arquivístico e o seu gerenciamento em todo o ciclo de vida, o GED tem por objeto o documento sem gerenciar a sua destinação final e toda a cadeia de custódia. O GED possui em sua funcionalidade: digitalização, automação dos fluxos de trabalho (*workflow*), promove ainda indexação e gestão de documentos, serve de repositórios entre outras.

Diversos sistemas são utilizados no âmbito do Poder Executivo Federal buscando otimizar a GI e a GD, que em sua maioria são utilizados como requisitos para atender as necessidades informacionais fundamentadas nas políticas de GD e de GI. A título de esclarecimento, com base nas pesquisas dos sites da AGU, Ministério da Economia (ME), Tribunal Regional Federal da 4ª Região (TRF4) e da Universidade Federal do Rio Grande do

Norte (UFRN), selecionou-se alguns sistemas utilizados no âmbito do Poder Executivo e Judiciário do Governo Federal, estando esses ocupando o status de ativos na presente data (Quadro 2).

Quadro 2 – Principais sistemas eletrônicos de GI utilizados pelo Poder Executivo Federal e Judiciário no Brasil

SAPIENS	Sistema AGU de Inteligência Jurídica
Criação	AGU
Funcionalidades Específicas	Inclui operações como: captura de documentos, aplicação do plano de classificação, controle de versões, controle sobre os prazos de guarda e destinação, armazenamento seguro e procedimentos que garantam o acesso e a preservação a médio e longo prazo de documentos arquivísticos digitais e não digitais confiáveis e autênticos.
Órgãos que utilizam	AGU
SEI	**Sistema Eletrônico de Informações**
Criação	Tribunal Regional Federal da 4ª Região (TRF4)
Funcionalidades Específicas	Controle de prazos, ouvidoria, estatísticas da unidade, tempo do processo, base de conhecimento, pesquisa em todo teor, acompanhamento especial, modelos de documentos, textos padrão, sobrestamento de processos, assinatura em bloco, organização de processos em bloco, acesso externo, entre outros.
Órgãos que utilizam	Receita Federal, Justiça Federal da 3ª Região, Anatel, Embrapa, Justiça Federal da 4ª Região, Policia Rodoviária Federal, Ministério da Saúde, Comissão de Valores Mobiliários, entre outros.
SIGAA	**Sistema Integrado de Gestão de Atividades Acadêmicas**
Criação 2005	Universidade Federal do Rio Grande do Norte
Funcionalidades Específicas	Disponibiliza as funcionalidades dos processos de Graduação, Pós-graduação (Stricto Sensu e Lato Sensu), gestão dos projetos e bolsistas de pesquisa, submissão e controle de ações de extensão, monitorias, registro e relatórios da produção acadêmica dos docentes, atividades de ensino à distância, além de um ambiente virtual de aprendizado denominado Turma Virtual.
Órgãos que utilizam	Universidades Federais
SIORG	Sistema de Organização e Inovação Institucional do Governo Federal
Criação	Ministério da Economia (ME)
Funcionalidades Específicas	Constituir rede colaborativa destinada à melhoria da gestão pública, proporcionar os meios para melhorar o desempenho institucional e otimizar a utilização dos recursos disponíveis, geração, adaptação e difusão de tecnologias de inovação.
Órgãos que utilizam	Unidades administrativas responsáveis pela organização e inovação institucional.
Super.GOV.BR 1.0	Sistema Único de Processo Eletrônico em Rede
Criação	AGU
Funcionalidades	Assinatura avançada, a identificação dos processos concluídos e não arquivados, arquivamento e o desarquivamento de processos; cálculo automático dos prazos de guarda, geração automática de listagens de eliminação e de recolhimento de documentos.
Órgãos que utilizam	Órgãos do Poder Executivo Federal

Fonte: Elaborado pela autora baseada nos dados dos sites institucionais da AGU (Brasil, 2022), TRF4 (Brasil, 2014), Ministério da Economia (Brasil, 2022) e UFRN (2016).

Acredita-se que os sistemas evoluem e se aperfeiçoam, moldados em atender as necessidades dos seus usuários e nos resultados do desempenho organizacional alinhado ao seu planejamento estratégico e, nessa perspectiva, pode-se citar que a evolução histórica dos sistemas de informação foram evoluindo em paralelo as TIC, de forma dinâmica e rápida nos últimos vinte anos.

3 SEGURANÇA DA INFORMAÇÃO

Na condição da sociedade em rede e composta por diferentes sistemas informacionais, os ativos informacionais são subsídios para as atividades sócio-organizacionais, centralizadas no seu valor para o desenvolvimento e o sucesso das instituições.

Diniz e Silva (2021) esclarecem que quando a organização identifica a informação como valor estratégico, ela passa a ocupar o centro dos processos de trabalho, direcionando a tomada de decisão e potencializando o desenvolvimento, a competitividade e a inteligência organizacional. Conforme os autores, essa junção de fatores eleva o papel da informação como principal ativo informacional e, ao mesmo tempo, destaca também o papel da Segurança da Informação que abrange em seu ciclo sistemas, aplicativos, equipamentos, serviços e pessoas (Diniz; Silva, 2021).

A informação disponibilizada em sistemas informatizados, acessados por diferentes pessoas, nos mais diferentes pontos da empresa, ou mesmo por meio remoto, ao mesmo tempo em que fortalece a gestão, aumenta o nível de risco para a segurança da informação. Para Alcoforado (2014) as organizações ainda precisam desenvolver ações integradas que reduzam ou tornem administráveis os riscos de segurança da informação. Em sua indagação, o autor questiona o quanto estamos dependentes da informação, o que nos torna vulneráveis e onde estão concentrados os riscos à segurança da informação? Estaria presente no meio externo ou dentro dos quadros funcionais por ações de imperícias ou negligências?

Em nível organizacional, geralmente a segurança da informação está voltada para investimentos na tecnologia, não considerando o fator humano. Nesse sentido, Dhillon (2004, tradução nossa) argumenta que a definição de segurança da informação se constitui de seis elementos essencialmente ligados as pessoas ou usuários de sistemas em uma organização, como: a confidencialidade, a integridade, a responsabilidade, a honestidade das pessoas, a confiança e a ética. O autor complementa que a segurança da informação compreende uma construção heterogênea, que envolve questões mais subjetivas e complexas que extrapolam o campo técnico, considerando questões estruturais, comportamentais e aspectos sociais.

A segurança da informação está voltada também para a usabilidade do sistema, que acontece entre o usuário, o sistema e a tecnologia. Oleto (2006, p. 18) pontua os principais atributos da qualidade da informação que a literatura associa ao usuário: “adequação da indexação e classificação (atributo do sistema); eficácia, eficiência da recuperação (atributo do sistema); impacto, relevância, utilidade, valor esperado, valor percebido e valor de uso”.

A abordagem sobre segurança da informação pode estar relacionada tanto com a TI quanto com as pessoas na figura de usuários dos sistemas. Para Furnell e Thomson (2009) um dos maiores obstáculos a ser superado pelas organizações é a inter-relação dos usuários dos sistemas e a segurança da informação que pode ser afetada pelo comportamento dos usuários finais, apontando como problemas mais recorrentes a apatia, negligência, ignorância, indiferença, entre outros comportamentos.

Os autores argumentam ainda que, para proteger os ativos informacionais é preciso desenvolver uma cultura organizacional pautada no compromisso dos seus integrantes com a segurança da informação, fortalecida pelo desenvolvimento de estratégias e política de conscientização e percepção dos riscos que alguns comportamentos dos usuários podem causar para a segurança da informação, no que tange ao mau uso dos sistemas de informação, favorecendo assim uma mudança cultural por meio das boas práticas comportamentais (Furnell;Thomson, 2009).

Pimenta e Quaresma (2016) entendem que estabelecer o nível de segurança é fundamental para constituir uma proteção para os sistemas de informação nas organizações, porque as vulnerabilidades e eventuais danos na segurança da informação partem dos usuários. Esses autores explicam que é fundamental verificar se os usuários estão sensibilizados quanto as práticas corretas e seguras do uso dos sistemas de informação quanto à segurança da informação no desempenho das suas tarefas.

Alcoforado (2014) argumenta que não existe uma solução única e objetiva que responda isoladamente as questões da segurança da informação, vai muito além, é preciso que a organização adote um conjunto de ações integradas e conjugadas em verbos que indiquem ações de: “conhecer, planejar, agir, auditar, educar, monitorar, aprender e gerenciar” (Alcoforado, 2014, p. 9).

Em um contexto da administração pública brasileira, Lima, Ferreira e Peixoto (2022) reconhecem que a defesa da informação, por eles qualificadas como ativo valioso, deve ser realizada por meio de políticas e o desenvolvimento de áreas especializadas que visam fundamentalmente garantir a segurança da informação sob três pilares: confidencialidade, integridade e disponibilidade (CID). Para Fraga (2019) esses pilares constituem os principais atributos para orientar, planejar e implementar um programa de GSI, embora outros fatores possam afetar o seu estabelecimento:

> A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem a utiliza, pelo ambiente ou infraestrutura que a cerca, ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação (Fraga, 2019, p. 14).

Machado Júnior (2018) explica que o princípio da confidencialidade se relaciona à garantia de que uma informação só seja liberada com autorização prévia, seja por senha, conta de e-mail, banco de dados etc. Na mesma ideia, Gaivéo (2008) considera a chave mestra da proteção de um sistema, o campo da identificação e do login, efetuados pelos usuários, embora alerta que no mundo corporativo, eventualmente existem usos e costumes de permissão do acesso entre usuários. Pode-se identificar que essas ações podem trazer ameaças, vulnerabilidades, ataques e riscos para a segurança da organização.

Para Fraga (2019), o princípio da integridade corresponde à propriedade que garante que a informação ao ser manipulada não sofra alterações na inteireza do seu teor, o que Mascarenhas Neto e Araújo (2019) chamam de manter a fidedignidade das informações, e essa preocupação repercute em ações para evitar a manipulação dos seus conteúdos, a exemplo dos citados por Lima, Ferreira e Peixoto (2022): conversão de documentos em formatos que não permitam modificação, assinatura digital, entre outras. Corroborando com os autores, Sêmola (2014, p. 28) torna claro que para garantir a integridade da informação ela deve "ser mantida na mesma condição em que foi disponibilizada por seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais".

Beal (2012) acrescenta aos pilares da segurança da informação acima citados, dois princípios, a saber: o princípio da autenticidade, o qual permite a "garantia de que a informação seja proveniente da fonte à qual ela é atribuída" (Beal, 2012, p. 54) e o princípio da irretratabilidade da comunicação (não repúdio), ou seja, a "proteção contra a alegação por parte de um dos participantes de uma comunicação de que não ocorreu" (Beal, 2012, p. 54).

Coelho, Araújo e Bezerra (2014) acrescentam dois atributos essenciais para a segurança da informação, os quais objetivam aumentar a segurança da informação, incluindo o princípio da conformidade, que consiste em:

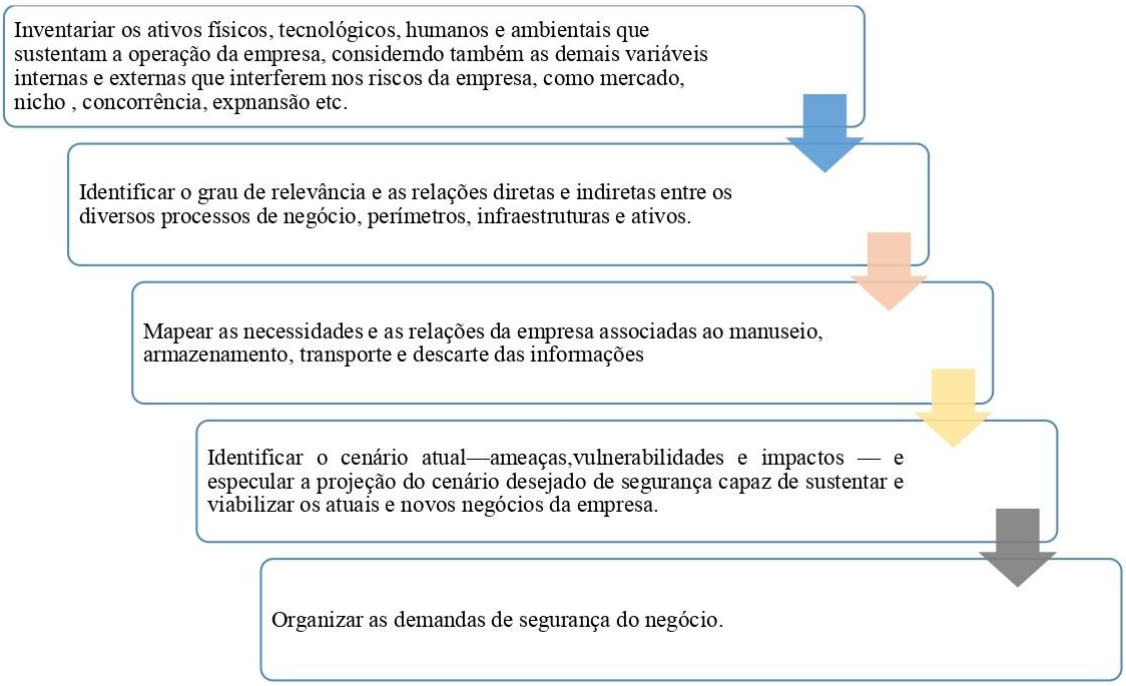
> Dever de cumprir e fazer cumprir regulamentos internos e externos impostos às atividades da organização. Estar em conformidade é estar de acordo, seguindo e fazendo cumprir leis e regulamentos internos e externos (Coelho; Araújo; Bezerra, 2014, p. 26).

O segundo princípio apresentado por Coelho, Araújo e Bezerra (2014, p. 26) é o controle de acesso, assim explicado: "trata de limitar e controlar o acesso lógico/físico aos ativos de uma organização, com o objetivo de proteger os recursos contra acessos não autorizados".

Sêmola (2014) adverte que ao mesmo tempo em que os sistemas informatizados romperam as fronteiras virtuais de acesso, uso e compartilhamento da informação, tornaram-se mais vulneráveis aos riscos de segurança da informação, os quais excedem os limites

tecnológicos e envolvem os aspectos físicos e humanos. Para esse autor, cada organização tem suas particularidades, portanto é preciso aplicar solução personalizada para gestão de riscos, desta forma sugere algumas práticas referentes ao mapeamento da segurança da informação (Figura 5).

Figura 5 – Mapeamento de segurança da informação



Fonte: Adaptado de Sêmola (2014, p. 32).

Conforme a figura, o mapeamento orienta ações de segurança voltadas para um modelo direcionado e específico de segurança da informação para determinada organização. O mapeamento de segurança da informação, de acordo com Sêmola (2014), guia ações específicas para uma organização, identificando riscos e permitindo a criação de um plano de ação. Isso ajuda a adotar medidas corretivas, especialmente em situações de riscos iminentes, como ataques de hackers, vírus, falhas de software, entre outros, que visam comprometer a informação.

À medida que a segurança da informação evolui nas organizações, a compreensão da sua complexidade também cresce. A visão contemporânea da segurança da informação não se limita mais às medidas de controle tecnológico; ela incorpora uma abordagem sistêmica que reconhece a centralidade do fator humano nesse contexto. O conceito apresentado por Marciano (2006, p. 14) ilustra essa perspectiva abrangente ao considerar não apenas os aspectos técnicos, mas também as interações sociais dos usuários:

> Segurança da informação é um fenômeno social no qual os usuários (aí incluídos os gestores) dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso.

Conforme destacado por Marciano (2006), a segurança da informação é uma questão que transcende a mera tecnologia e implica a necessidade de uma abordagem holística, em que a colaboração ativa dos usuários desempenha um papel crucial em todas as fases do ciclo de vida da informação. Isso realça a complexidade inerente à segurança da informação e a importância de equilibrar de maneira eficaz os elementos tecnológicos e humanos nesse contexto.

Segundo o Tribunal de Contas da União (TCU, 2012), a manutenção de um Sistema de Gestão da Informação (SGI) que preserve seus princípios básicos é crucial para a sobrevivência da organização. A integridade do SGI implica na ausência de violações dos dados, seja por acesso não autorizado, alterações acidentais ou intencionais, ou exclusões.

Machado Júnior (2018) destaca a necessidade de preservar o princípio da disponibilidade da informação, mesmo em face dos riscos das interações entre sistemas e pessoas. Isso garante o acesso contínuo à informação, fundamental para atividades organizacionais, mas alerta para os perigos de ataques cibernéticos que podem comprometer a integridade dos dados.

A Norma Complementar nº 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, publicada pelo Gabinete de Segurança Institucional da Presidência da República (GSIPR), apresenta dentre outras orientações, os principais conceitos relativos à segurança da informação e comunicação. Acrescenta aos preceitos de confidencialidade, disponibilidade e integridade, acima citados, o princípio de autenticidade: “propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade” (Brasil, 2012).

De acordo com a norma nº 10/IN01/DSIC/GSIPR, o processo de inventário e mapeamento de ativos de informação envolve três etapas principais: identificação e classificação de ativos informacionais, identificação de potenciais ameaças e vulnerabilidades e avaliação de riscos. A título de definições, o GSIPR considera como valores tangíveis e intangíveis da informação estando nessa seara “Os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram os meios, e também os recursos humanos que a eles têm acesso” (Brasil, 2012).

A fim de proporcionar uma visão mais abrangente e fundamentada sobre o conceito de segurança da informação, relacionaram-se algumas compreensões apresentadas por autores de áreas interdisciplinares (Quadro 3).

Quadro 3 – Principais conceitos sobre segurança da informação

Ano	Autor (es)	Conceitos Perspectiva
2001	Thomas R. Peltier	"A segurança da informação compreende o uso de controles de acesso físicos e lógicos, com o intuito de proteger os dados contra modificações acidentais ou não autorizadas, destruição, quebra de sigilo, perda ou danos aos ativos informacionais" (2001, p. 8).
2001	Wilson Oliveira	"Processo de proteção de informações e ativos digitais armazenados em computadores e redes de processamento de dados" (2001, p. 40).
2002	Luís Rodrigues	"Conjunto de procedimentos, atividades, pessoas e tecnologias envolvidos na coleta de dados relevantes, armazenamento enquanto necessário, processamento dos dados e na disponibilização de informação a quem necessite da mesma" (2002, p. 64).
2005	Associação Brasileira de Normas Técnicas - ABNT NBR ISO/IEC 27002:2022	"A proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (2022).
2012	Brasil Norma Complementar 10/IN01/DSIC/GSIPR/2012	"Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações" (2012, p. 3).
	Luciana Emirena dos Santos Carneiro	"A Segurança da Informação surge como recurso relevante, que busca atrelar ao negócio da empresa às variáveis segurança e proteção dos ativos informacionais como elementos integradores do negócio principal, uma vez que salvaguardar as informações é fundamental para o sucesso, competitividade e sobrevivência no mercado globalizado" (2012, p. 47).
2014	Marcos Sêmola	"A segurança da informação é uma área de conhecimento voltada à proteção da informação e dos ativos associados contra indisponibilidade, alterações indevidas e acessos não autorizados" (2014, p. 41).
2016	Luís Borges Gouveia	"De um modo geral, a segurança da informação é um requisite obrigatório, de forma a minimizar os riscos associados a uma atividade ou negócio e assegurar a conformidade com disposições legais ou de natureza regulatória, como é o caso de regulamentos comunitários ou provenientes da legislação nacional" (2016, p. 8).
2019	Brasil, Portaria nº 93, de 26 set. 2019	"Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações" (2019, s. n.).
Ano	**Autor (es)**	**Conceitos Perspectiva**
2019	Fraga	"A segurança da informação se refere à proteção existente sobre as informações de uma determinada empresa e pessoa; isto é, aplica-se tanto às informações corporativas como às pessoas. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição" (2019, p. 12).
2019	Mário Cesar Jucá	"Entendemos que a gestão da segurança da informação é uma atividade básica para proteger a informação de ameaças a sua integridade, disponibilidade e confidencialidade e responsável por assegurar e controlar o ambiente informacional na organização" (2019, p. 11).

Fonte: Elaborado pela autora com base no corpus da pesquisa (2022).

Considerando os conceitos acima, pode-se especular que a maioria dos autores direcionam os estudos para uma preocupação fundamentada em proteger a informação em relação aos pilares confidencialidade, integridade, disponibilidade, o que fica claro na definição clássica da ABNT (2022). Percebe-se ainda que os conceitos estão em sua maioria fundamentados nos aspectos: tecnológicos, técnicos e sociais.

Fraga (2019) apresenta um conceito intimamente relacionado com a definição da segurança dos computadores, ou seja, apesar de incluir o papel do usuário, a sua apreciação restringe a importância da percepção do usuário e sua inter-relação com o sistema e peca pelo reducionismo tecnológico. Na mesma concepção, Oliveira (2001) apresenta uma visão tecnológica desenvolvida na linha de que a segurança da informação está voltada para proteção dos dados armazenados em sistemas computadorizados. Essa preocupação está intrínseca na maioria das compreensões, o que se justifica devido as ameaças constantes dos ataques cibernéticos, principalmente nos dados de instituições públicas e governamentais.

Na obra de Mascarenhas Neto e Araújo (2019), as definições ultrapassam esses limites, focando no valor da informação para a produtividade e na integração dos ativos com os processos e as pessoas. Esses autores são da área da CI e produziram um livro sobre a temática, na vertente de uma visão sistêmica para ser utilizada nas organizações. Esse tipo de publicação procura contrapor modelos atuais, votados para as questões tecnológicas, o que não está completamente errado, contudo, com a visão no paradigma social da CI, o papel integrado dos aspectos humanos e tecnológicos se integram e apresentam novas perspectivas nas pesquisas.

Considerando que a informação representa na organização o elemento estratégico para tomada de decisão, a segurança da informação deve ser instituída e orientada por políticas, normas e procedimentos de segurança da informação que envolvam também um trabalho de conscientização e participação dos usuários.

3.1 Comportamento dos usuários dos sistemas informatizados na perspectiva da segurança da informação

Comumente, no universo organizacional, as mudanças e as atualizações dos sistemas informatizados acontecem antes mesmo que os usuários dominem as suas funções, o que provoca sentimentos de medo, insegurança, resistência tecnológica, desconhecimento e tantos outros problemas que afetam o seu fazer profissional. Os usuários desses sistemas enfrentaram um novo mundo, de profundas transformações tecnológicas, que iniciou na década de noventa e não mais parou.

Socialmente, o progresso chegou sem aviso prévio, desde o uso da máquina de datilografia manual para a elétrica, das calculadoras, do Telex ao *Fac-símile* até os computadores e celulares, muitos produtos foram esquecidos e se tornaram obsoletos. Foram invenções incríveis utilizadas durante muitos anos por todo o mundo corporativo, no entanto as mudanças continuaram acontecendo ininterruptamente e transformaram as práticas profissionais.

Em termos metafóricos, as TIC evoluem à velocidade da luz, da mesma forma os sistemas de informação se utilizam da TIC e das pessoas para funcionarem e evoluírem, por isso a inovação tecnológica surpreende em todas as esferas sociais. Os sistemas de informação têm a função principal de otimizar cada vez mais os fluxos das informações, condição vital para que possa atender as necessidades informacionais das unidades a que se destinam. Paralelo ao sistema, estão os usuários e suas necessidades.

Alencar e Araújo Júnior (2022) destacam que as organizações têm mantido o foco no desenvolvimento e atualização dos seus sistemas para a gestão estratégica, desconsiderando na maioria das vezes os seus usuários, suas necessidades e as suas próprias particularidades. Os autores acreditam que a maioria dos sistemas informatizados são implementados sem um estudo técnico prévio e sem um estudo dos próprios usuários, o que traz problemas como: dificuldade de uso do sistema, desconfiança e inconsistências.

Muito se discute sobre comportamento informacional, mas antes que se possa explorar essa terminologia, apresenta-se o conceito de usuário no sentido de usuário de sistemas de informação, com ênfase em seu comportamento, frente às boas práticas de segurança da informação.

Segundo o glossário de segurança da informação publicado pelo GSIPR, o conceito de usuário é assim definido:

> Usuário da informação é pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade (Brasil, 2021, n. p.).

O glossário abrange o seu conceito, reconhecendo que nos quadros funcionais da Administração Pública Federal existem os usuários visitantes em condições que diferem da definição acima:

> Usuário visitante com dispositivo móvel são agentes públicos ou não, que utilizem dispositivos móveis, de sua propriedade ou do órgão ou entidade a que pertencem, dentro dos ambientes físicos de órgãos ou entidades da administração pública federal dos quais não fazem parte (Brasil, 2021, n. p.).

Araújo (2012) explica que no campo da CI os estudos dos usuários evoluíram centralizados na informação e em sua apropriação, fator capaz de alterar os estados cognitivos dos sujeitos, colocando-os na linha da ação da construção do conhecimento, ou seja:

> A informação nessa perspectiva deixa de ser entendida enquanto documento ou item informacional usado/acessado pelos usuários e passa a ser definida em termos de sua relação com o conhecimento – ou melhor, com a ausência de conhecimento. Informação passa a ser entendida como algo capaz de alterar os estados cognitivos dos sujeitos, dando-se, a partir daí especial atenção às maneiras como os indivíduos percebem seus estados de lacuna cognitiva e as estratégias utilizadas por eles para buscar e usar as informações de que necessitam (ARAÚJO, 2012, p. 148).

Ainda no campo da CI, Woida (2008) ressalta que o comportamento do usuário é moldado a uma realidade social em que se insere e esse fato acontece no desenvolvimento de uma cultura informacional baseada na interação entre pessoas, informação e TIC. Em um sistema de informação, o uso da informação é motivado pela necessidade informacional do usuário e pela própria organização. Esse estímulo molda um comportamento de "desenvolvimento individual e organizacional, cuja dinâmica alimenta o comportamento informacional" (Woida, 2008, p. 96).

O comportamento do usuário parte da conscientização, do conhecimento e da capacitação para que possa compreender os riscos e a sua responsabilidade em relação à adoção de comportamento seguro do uso da informação. Para Pimenta e Quaresma (2016), o grande desafio é como fazer com que eles compreendam o valor da informação e a tratem de maneira segura a partir das estratégias estabelecidas pela adoção de uma SGI, estabelecida e implementada por uma política de segurança da informação.

A conscientização sobre a política de segurança da informação é crucial para o comportamento dos usuários, sob esse aspecto a Norma NBR ISO/IEC 27001:2022 (ABNT, 2022), relaciona três diferentes elementos que a organização deve tornar ciente as pessoas que trabalham diretamente na organização e sob o seu controle:

> a) a política de segurança da informação;
> b) sua contribuição para a eficácia do sistema de gestão da segurança da informação, incluindo os benefícios de um melhor desempenho da segurança da informação; e
> c) as implicações de não estar em conformidade com os requisitos de gerenciamento de segurança da informação (ABNT, 2022, p. 6).

Segundo a Norma NBR ISO/IEC 27002:2022(ABNT, 2022), a adoção de uma política de informação é promovida visando trazer maior segurança aos gestores e aos usuários dos sistemas de informação. As suas diretrizes devem ser estabelecidas, aprovadas pela direção e comunicadas a todos os funcionários e partes externas.

As diretrizes para implementação da política de informação são estabelecidas envolvendo a organização como um todo, documentadas e validadas pela direção, tendo como enfoque o gerenciamento e a segurança da informação. De acordo com a Norma NBR ISO/IEC 27002:2022 (ABNT, 2022), a política de segurança da informação é abrangente, portanto, adaptável a diferentes contextos organizacionais. Algumas diretrizes sobre as melhores práticas de controle de segurança da informação sugeridas pela respectiva norma podem ser verificadas no quadro 4.

Quadro 4 – Diretrizes específicas de controle de segurança da informação da organização.

CONTROLES ORGANIZACIONAIS	
Diretrizes	**Controle**
Políticas de segurança da informação	Definir, aprovar, publicar, comunicar e revisar políticas de segurança da informação periodicamente.
Funções de segurança da informação e responsabilidades	Adaptar as funções e responsabilidades de segurança da informação às necessidades da organização.
Contato com interesse especial grupos	A organização deve manter contato com grupos de interesse e associações especializados em segurança da informação.
Inteligência sobre ameaças	Coletar e analisar informações de ameaças para produzir inteligência sobre segurança da informação.
Segurança da informação no gerenciamento de projetos	A segurança da informação deve ser integrada ao gerenciamento de projetos.
Inventário de informações e outros ativos associados	Deve ser desenvolvido e mantido um inventário de informações e outros ativos associados, incluindo os proprietários.
Classificação e rotulagem das informações	Classificar informações com base em segurança, considerando confidencialidade, integridade, disponibilidade e requisitos das partes interessadas, e aplicar procedimentos de rotulagem conforme o esquema organizacional.
Transferência de informações	Definir regras, procedimentos ou acordos para transferência de informações em todas as instalações internas e externas da organização.
Controle de acesso	Implementar regras de controle de acesso físico e lógico com base nos requisitos de segurança empresarial e de informações.
Informações de autenticação	Gerenciar informações de autenticação com um processo e orientações adequadas.
Retorno de ativos	Ativos da organização devem ser devolvidos após a saída de funcionários e partes interessadas
Direitos de acesso	Gerenciar direitos de acesso conforme políticas e regras de controle de acesso da organização.
Gerenciamento da segurança da informação na cadeia de suprimentos da TIC	Gerenciar riscos de segurança na cadeia de suprimentos de TIC.
Monitoramento, revisão e gerenciamento de mudanças de serviços de fornecedores	Monitorar e gerenciar regularmente mudanças nas práticas de segurança de fornecedores e na prestação de serviços.
Segurança da informação para uso de serviços em nuvem	Estabelecer processos para serviços em nuvem alinhados com requisitos de segurança da organização.
Planejamento e preparação do gerenciamento de incidentes de segurança da informação	Preparar gestão de incidentes de segurança com processos, funções e responsabilidades definidos e comunicados.

(Continuação do quadro 4).

CONTROLES DE PESSOAS	
Diretrizes	**Controle**
Triagem	Conduzir verificações de antecedentes em candidatos a funcionários conforme a lei, regulamentos, ética e necessidades da organização.
Termos de condições de emprego	Os acordos contratuais de trabalho devem estabelecer as responsabilidades do pessoal e da organização com relação à segurança das informações.
Diretrizes	**Controle**
Conscientização, educação e treinamento em segurança da informação	Fornecer treinamento em segurança da informação e atualizações de políticas aos funcionários e partes interessadas relevantes de acordo com suas funções.
Processo disciplinar	Estabelecer um processo disciplinar para lidar com violações da política de segurança da informação.
Responsabilidade após a rescisão ou mudança de emprego	Comunicar e manter responsabilidades de segurança da informação após rescisão ou mudança de emprego.
Contratos de confiabilidade ou de não divulgação	Obter acordos de confidencialidade que protejam as informações da organização.
Trabalho remoto	Implementar medidas de segurança ao trabalhar remotamente para proteger informações fora das instalações da organização.
Reportagem de eventos de segurança da informação	A organização deve ter um mecanismo para relatórios de segurança da informação por parte dos funcionários.
CONTROLE TECNOLÓGICO	
Diretrizes	**Controle**
Direitos de acesso privilegiado	Restringir e gerenciar a alocação e o uso de direitos de acesso privilegiado.
Restrições de acessos às informações	Restringir o acesso de acordo com a política de controle específica.
Autenticação segura	Implementar autenticação segura com base nas restrições de acesso às informações e na política específica de controle de acesso.
Proteção contra *malware*	Implementar proteção contra *malware* com conscientização adequada do usuário.
Gerenciamento de vulnerabilidades técnicas	Identificar vulnerabilidades em sistemas, avaliar exposição da organização e aplicar medidas de mitigação adequadas.
Gerenciamento de configuração	Configurações de segurança devem ser estabelecidas, documentadas e monitoradas.
Prevenção de vazamento de dados	Implementar medidas de prevenção de vazamento de dados em sistemas, redes e dispositivos que manipulam informações confidenciais.
Backup de informações	Manter e testar regularmente cópias de *backup* de informações, software e sistemas conforme a política de *backup* acordada.
Registro em log	Produzir, armazenar, proteger e analisar logs que registram atividades, exceções, falhas e eventos relevantes.
Atividades de monitoramento	Monitorar e responder a comportamentos anômalos em sistemas e redes para avaliar possíveis incidentes de segurança.
Segurança de serviços de rede	Proteger, gerenciar e controlar redes e dispositivos de rede para garantir a segurança das informações em sistemas e aplicativos.

(Conclusão do quadro 4).

Diretrizes	Controle
Segregação de redes	Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados nas redes da organização.
Filtragem da Web	O acesso a site externos deve ser gerenciado para reduzir a exposição a conteúdo malicioso.
Uso de criptografia	Definir e implementar regras para o uso eficaz da criptografia, incluindo o gerenciamento de chaves criptográficas.
Diretrizes	**Controle**
Gerenciamento de mudanças	Mudanças em instalações e sistemas de informação devem obedecer a procedimentos de gerenciamento de mudanças.
Codificação segura	Aplicar princípios de codificação segura no desenvolvimento de software.
CONTROLE FÍSICO	
Diretrizes	**Controle**
Monitoramento de segurança física	Monitorar instalações para evitar acesso não autorizado com controles adequados.
Proteção contra ameaças físicas e ambientais	Proteger contra ameaças físicas e ambientais, incluindo desastres naturais e intencionais, na infraestrutura.
Limpeza, localização e proteção dos equipamentos	Definir e aplicar regras claras para papéis e mídias de armazenamento removíveis, bem como regras de segurança para instalações e equipamentos.
Localização e proteção de equipamento	Instalar equipamento de forma segura e protegida.
Segurança de ativos fora do local	Os ativos fora do local devem ser protegidos.
Mídia de armazenamento	Gerenciar mídia de armazenamento de acordo com a classificação e requisitos da organização durante todo o seu ciclo de vida.
Segurança do cabeamento e manutenção de equipamentos	Proteger cabos e equipamentos para garantir a segurança das informações.
Descarte seguro ou reutilização de equipamentos	Verificar equipamentos com mídia de armazenamento para garantir a remoção segura de dados confidenciais e software licenciado antes do descarte ou reutilização.

Fonte: Adaptado da ABNT NBR ISO/IEC 27002 (2022).

As diretrizes acima elencadas são projetadas para que as organizações possam usar como referências no processo de implementação da PGSI. A NBR ISO/IEC 27002:2022 (ABNT, 2022) orienta que sejam elaboradas o conjunto de políticas de segurança da informação definindo o seu conceito, seus objetivos e princípios com atribuição de responsabilidades e papeis definidos no ambiente corporativo, incluindo os processos para o tratamento das possíveis exceções que venham acontecer.

Dada a forte influência que os usuários dos sistemas de informação exercem sobre a segurança da informação, Pimenta e Quaresma (2016) defendem ainda que, a adoção participativa de um planejamento e controle de políticas de segurança da informação pode estabelecer um padrão de comportamento de usuários confiáveis, competentes e comprometidos com a sua segurança.

A preocupação em integrar o fator humano aos conceitos de segurança da informação perdura por décadas e, a esse respeito, Hitchings (1995) reconhece uma lacuna dada a pouca relevância que o usuário de sistemas de informação ocupa nas pesquisas dessa ordem. Para o autor, falta percepção do papel que ocupam em segurança da informação, o que restringe as contribuições colaborativas na política de segurança da informação e inibe a apropriação dos reais problemas que os envolvem (Hitchings, 1995).

Mascarenhas Neto e Araújo (2019) destacam que ao criar um documento para implementar a política de segurança em uma organização, é essencial conhecer os usuários dos sistemas de informação. Da mesma forma, os usuários devem estar familiarizados com os modelos de sistemas de gestão e suas estratégias. A proteção da informação deve ser o foco, e os autores enfatizam que os usuários desempenham um papel fundamental no controle de acesso. Isso envolve certificações, conscientização e capacitação para lidar com os riscos, conclui os autores.

Segundo Marciano (2006), a dinâmica da interação social no uso intensivo dos sistemas transcende as políticas de informação impostas aos usuários. Ele ressalta que os usuários não devem ser considerados meros consumidores ou produtores de informações, mas sim participantes ativos. A busca contínua por informações e a produção de conhecimento são aspectos cruciais que definem o usuário nessa perspectiva.

De acordo com Dhillon (2004) é fundamental que o usuário adquira plena consciência da importância de seu papel na área da segurança da informação. Isso envolve assumir uma posição que o integre de maneira efetiva no processo multifacetado de construção de uma gestão engajada na segurança da informação. Para o autor, a responsabilidade pela proteção da informação e dos seus também é atribuída aos deveres dos usuários dos sistemas.

Na visão de Chowdhury (2015), a definição do usuário de informações não deve ser limitada apenas pelas suas necessidades, mas deve considerar também a natureza da informação que atende às demandas da organização em que o usuário está inserido. Isso significa que a necessidade informacional do usuário está intrinsecamente ligada às suas demandas e visa resolver problemas, baseando-se em conhecimentos específicos.

A autora supracitada identifica que cada usuário é único e possui diferentes tipos de necessidades informacionais, destacando:

- Necessidade de informação é um conceito relativo; ela depende de diversos fatores e não permanece constante;
- Ela muda sobre um período de tempo;
- Varia de pessoa para pessoa, de profissão para profissão, de área para área, organização para organização, e assim por diante;

> - As necessidades informacionais das pessoas são em grande medida dependentes de seu ambiente; por exemplo, as necessidades daqueles que estão no ambiente acadêmico são diferentes daqueles num ambiente industrial, de negócios, ou administrativo;
> - Mensurar (quantificar) a necessidade de informação é difícil;
> - Frequentemente, essa necessidade permanece inexpressável ou insuficientemente expressa;
> - A necessidade de informação frequentemente muda ao se receber alguma informação (Chowdhury, 2015, p. 7).

De acordo com a citação acima, Chowdhury (2015) explica que as demandas dos usuários de sistemas são diversificadas e passíveis de mudanças contínuas. A autora reforça suas ideias argumentando que, à medida que os usuários identificam suas necessidades de informação, eles têm a tendência de adquirir conhecimento, assimilar informações e compartilhar dados, o que, por sua vez, contribui para o aprimoramento de suas atividades profissionais.

Pode-se inclusive argumentar que busca de informações decorre de problemas em evolução no cotidiano, impulsionando o crescimento contínuo da interação entre usuários e sistemas nas organizações. A complexidade dos fluxos de informação, devido ao alto volume e à necessidade de recuperação eficaz, também amplia essa necessidade por informações.

Com base nos fatores que podem influenciar o comportamento de busca por informações dos usuários, Chowdhury (2015) destaca alguns pontos gerais que podem servir como referência em diversas organizações, conforme apresentados no Quadro 5.

Quadro 5 – Pontos gerais que podem afetar o comportamento de busca do usuário individualmente

	Pontos Gerais
	O contexto educacional e profissional, e, o ambiente no qual o usuário cresceu e/ou está vivendo atualmente;
	Sua percepção e habilidade para acessar fontes de informação
	Seu relacionamento com a unidade de informação concernente;
	Facilidade de acesso à unidade de informação
	Condições de trabalho do usuário;
	O tempo disponível para consultar sistemas de informação;
	Seu prestígio hierárquico e posição socioprofissional;
	O quão desafiador são seus trabalhos;
	O nível de competitividade que há em seus campos de atuação;
	Suas experiências anteriores;
	O quanto eles já sabem;
	Suas atitudes em geral para com as pessoas e organizações;
	O quão amigavelmente, versados e eficientes são os membros da unidade de informação;
	Os vários produtos e serviços da unidade de informação;
	Qual amigável ao usuário é o sistema de informação;
	Quão efetiva é a política de promoção da unidade de informação;
	Quão efetivos são os programas de educação, sensibilização, orientação e assistência ao usuário, da unidade de informação;
	Suas conexões pessoais e profissionais;

Fonte: Adaptado de Chowdhury (2015, p. 16).

Esses fatores mencionados abrangem diferentes contextos que podem afetar o comportamento do usuário. Chowdhury (2015) buscou elencar os mais comuns e, em uma leitura rápida, já se reconhecem fatores internos da organização, relações interpessoais, a interface do sistema, questões cognitivas do conhecimento do usuário e a própria relação que o usuário possui com a sua empresa. Esses pontos afetam comunitariamente toda a organização e, muitas vezes não são percebidos pela gestão, embora influenciem indiretamente a organização.

Para Baptista (2019), entender o comportamento e as necessidades informacionais para os usuários dos sistemas, por ele intitulados como usuários na recuperação de informação, requer certas peculiaridades que os destacam: são proativos e possuem diferentes concepções de necessidade de informação. Para o autor, há uma lacuna significativa que deve ser considerada em relação à interação entre os usuários e os sistemas de informação. Essa lacuna exige uma análise mais aprofundada por parte dos gestores ao implementar um sistema ou buscar melhorias. Isso implica em uma investigação mais detalhada das questões cognitivas dos usuários, suas competências e as oportunidades de mediação da informação no processo de aquisição e compartilhamento de conhecimento.

Com base na CI, Andrade e Andrade (2016) consideram que existem muitas definições e conceitos sobre a identificação dos usuários e suas necessidades, situando-os em um vasto campo de demandas tecnológicas com elementos de intersubjetividade no fator interação usuários e sistema de informação, relacionando necessidades cognitivas de busca pelo conhecimento e ampliando o seu campo de visibilidade: “Deixam, pois, de ser usuários de bibliotecas, arquivos e museus (unidades informacionais), passando a ser usuário em qualquer contexto no qual a informação seja o objeto de estudo” (Andrade; Andrade, 2016, p. 108).

Com base nas discussões apresentadas por diversos autores, é inquestionável que a participação ativa, o comportamento e as atitudes dos usuários dos sistemas de informação desempenham um papel de extrema relevância na determinação do aumento ou da diminuição do risco e da segurança das informações. Esses fatores exercem uma influência substancial sobre a integridade e a proteção dos dados e sistemas.

3.2 Boas práticas em segurança da informação

Ao iniciar essa seção, a palavra de ordem é entender como os sistemas estão contextualizados dentro das organizações, suas mudanças e abordar questionamentos antigos,

velhas discussões frente a novos problemas que as pessoas têm enfrentado como usuários de sistemas no que tange às práticas de segurança da informação na sociedade contemporânea.

Segundo a Secretaria de Fiscalização da TI do TCU, o avanço da computação e da informatização resultou em uma estrutura de segurança da informação mais complexa, requerendo equipes especializadas, equipamentos e métodos para garantir a política de segurança da informação nas organizações. Isso é crucial, uma vez que as informações são armazenadas em Sistemas de Informação (SI), que desempenham um papel fundamental no fluxo de informações para atender às demandas institucionais e garantir a sobrevivência no mercado de trabalho. (Brasil, 2012).

Com relação às boas práticas em segurança da informação, o TCU (Brasil, 2012) manifesta uma preocupação em atribuir a cada servidor de atividade-meio e de atividade-fim o conhecimento das práticas de segurança envolvendo o uso adequado da informação e os recursos informacionais, considerando nesse sentido que a informação "é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico" (Brasil, 2012, p. 10).

Nos últimos dois anos, a pandemia da COVID-19 impulsionou uma grande transformação no uso de sistemas informacionais e nas atividades laborais. Além da disseminação do vírus Sars-Cov-2, a pandemia também transformou os meios de comunicação e as relações interpessoais em todos os setores da sociedade. Isso resultou na conexão das pessoas a uma sociedade em rede informatizada, que já existia, mas nunca havia sido tão explorada. O teletrabalho, inicialmente adotado como medida emergencial, rapidamente se tornou uma realidade, deslocando as atividades profissionais do presencial para o virtual (Teixeira, 2022).

Outro ponto identificado com a imposição governamental do teletrabalho foi a superação do receio dos trabalhadores de serem substituídos por máquinas, fator que Castells (2013) chamava a atenção há anos em sua abordagem da sociedade em rede.

A mudança foi além do esperado, afetando todas as camadas sociais. O Governo Federal, por meio do Decreto nº 11.072, de 17 de maio de 2022, utilizando seu PGD, oficializou a possibilidade da adoção do teletrabalho, sujeito ao interesse da administração, não constituindo um direito do servidor público. Essa regulamentação levou alguns órgãos federais a adotarem o teletrabalho, ampliando as preocupações com a segurança da informação além dos limites físicos das organizações.

Analisando-se o decreto citado acima, que abrange todos os órgãos da Administração Pública Federal, identificou-se que não há nenhuma menção à segurança da

informação em seus artigos. Novamente encontramos uma preocupação maior com a estrutura tecnológica (antivírus, *firewall*, *backup* e outros), ficando pendentes as questões das boas práticas de segurança com relação aos usuários dos sistemas.

Considerando-se ainda as questões acima citadas, pode-se exemplificar outra norma instituída a partir do teletrabalho, a Portaria Normativa PGU/AGU nº 5, de 3 de agosto de 2021, que institui o teletrabalho para os Advogados da União, identificando-se em seu Art. 8º, alínea IV do capítulo III, que trata da autorização do teletrabalho, uma breve menção sobre a segurança da informação, a saber:

> IV - zelar pela segurança das informações e pelo sigilo profissional, não utilizando equipamentos públicos para acesso aos sistemas e redes institucionais, não compartilhando senhas, certificados digitais e outras ferramentas de trabalho e mantendo os sistemas operacionais e softwares antivírus atualizados (Brasil, 2021, n. p.).

Dado que os servidores estão distribuídos em diversas classes hierárquicas, subdivididas entre atividade-meio e atividade-fim, a orientação para a segurança da informação é detalhada na Portaria Normativa nº 17, de 16 de julho de 2021, que instituiu o teletrabalho para os servidores técnico-administrativos da AGU. No capítulo IV, especificamente no Plano de Pactuação Individual, artigo VII, são estabelecidas as diretrizes para a segurança da informação, da seguinte forma:

> VII - cláusula de compromisso com o sigilo dos documentos e informações acessados e manuseados, observados os procedimentos relativos à segurança da informação e àqueles relacionados à salvaguarda de informações de natureza sigilosa, nos termos de normas específicas aplicáveis (Brasil, 2021, n. p.).

A inclusão dessas normas no corpus do referencial teórico foi uma escolha deliberada devido à sua relação direta com o problema de pesquisa em questão. No entanto, é interessante observar que, ao investigar essas normas referenciadas, não se identifica qualquer menção a potenciais problemas ou situações específicas que possam surgir na modalidade de teletrabalho.

Para abordar efetivamente as boas práticas de segurança da informação, Mascarenhas Neto e Araújo (2019) enfatizam a necessidade de ir além dos princípios fundamentais da segurança da informação e conduzir a identificação dos principais ativos de informação. Essa abordagem mais abrangente permite uma compreensão mais profunda das medidas de segurança necessárias para proteger os recursos críticos de informação de uma organização.

Para os autores mencionados, no contexto organizacional, a questão da segurança da informação é muito mais complexa, pois envolve valores, organizações, competitividade e,

em última análise, a sobrevivência em um ambiente altamente competitivo, os seja: “um problema de negócio e demandam esforços abrangentes, como foco em gerenciamento de riscos ligados a objetivos mais amplos, como continuidade dos negócios [...]” (Marcarenhas Neto; Araújo, 2019, p. 27).

A GSI é desenvolvida para proteger a informação de forma integrada, para diminuir e/ou evitar os riscos e danos informacionais. Conforme o glossário do GSIPR, a gestão da segurança da informação pode ser definida como:

> Processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação (BRASI, 2021, s. n.).

O conceito prevê uma integração de ações que podem dirimir os riscos de perda da informação por diversos meios em prol de resguardar o valor estratégico da informação. Para maior esclarecimento, com base no glossário da GSI (Brasil, 2021), os termos que o compõem, estão descritos no quadro 6.

Quadro 6 – Principais significados dos termos que compõem o conceito de GSI

Termos	Significados
Gestão de riscos	Processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;
Gestão de Continuidade de Negócios	Processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;
Tratamento de Incidentes	Consiste nas ações e procedimentos tomados imediatamente após a identificação do incidente, visando garantir a continuidade de operações, preservar evidências e emitir as notificações necessárias;
Tratamento da Informação	Conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
Conformidade	Cumprimento das legislações, normas e procedimentos relacionados à segurança da informação da organização;
Credenciamento	O processo pelo qual o usuário recebe credenciais de segurança para acessar um sistema, envolvendo identificação, autenticação, cadastro de código de identificação e definição de perfil de acesso, com base em autorização prévia e necessidade de conhecimento.
Segurança cibernética	Ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;
Segurança orgânica e organizacional	Conjunto de medidas passivas, com o objetivo de prevenir e, até mesmo, obstruir as ações que visem o comprometimento ou a quebra de segurança de uma organização. Inclui os processos relacionados às áreas: de pessoal, de documentação, das comunicações, da tecnologia da informação, dos materiais e das instalações de uma organização, dentre outros;

Fonte: Adaptado do glossário GSI (Brasil, 2021).

Alguns erros podem ser cometidos na implantação de uma GSI, pois muitas vezes a organização não tem uma cultura organizacional de gerenciamento de riscos ou não pretende investir recursos nessa área. Sêmola (2014, p. 20) entende por equivocadas essas ações e acredita que o motivo seja provocado "pela visão míope do problema e a percepção distorcida da questão", o que pode refletir de forma negativa nos negócios.

Segundo Fraga (2019) existem mecanismos de segurança da informação que nem sempre estão ligados aos aspectos tecnológicos. Em termos de controles físicos, as barreiras são de limites estruturais: portas e trancas; os controles lógicos, que seriam as barreiras de acesso, geralmente eletrônicas, usadas para manter a segurança da informação em ambientes controlados; os mecanismos de criptografia e assinatura digital e mecanismos de certificação protegem os princípios de integridade e confiabilidade da informação; e a aquisição de *Honeypo*t, nome de um software que possui a função de detectar a ação de *cracker*, *spammer* ou qualquer agente estranho ao sistema.

Segundo Furnell e Thomson (2009), os riscos associados à segurança da informação são caracterizados pela interação entre pessoas e tecnologia. Os autores identificam atitudes apáticas, desinteresse, negligência e ações descomprometidas com a proteção dos ativos de informação como riscos predominantes por parte dos usuários do sistema.

A implementação de controles de segurança é uma componente fundamental das boas práticas de segurança da informação, conforme sugerido por Sêmola (2014). Ele apresenta mecanismos que têm como objetivo manter o nível de risco sob controle. Essas ações são projetadas para se adaptar às mudanças tecnológicas e comportamentais, porém, é crucial que os gestores tenham clareza de que, diante de uma ampla variedade de controles disponíveis, devem selecionar aqueles que melhor se adequam aos seus recursos e às situações específicas enfrentadas.

O autor apresenta uma variedade de medidas, tais como a realização de seminários de sensibilização, a oferta de cursos de capacitação, a implementação de campanhas de divulgação da política de segurança, a adoção de crachás de identificação, a aplicação de termos de responsabilidade e confidencialidade, bem como a utilização de softwares de auditoria de acessos, entre outras ações recomendadas para fortalecer a segurança da informação (Sêmola, 2014).

Não obstante a presença de mecanismos de defesa da segurança da informação, Ferreira (2017) reforça a sua importância e ressalta que em algumas vezes são os próprios usuários dos sistemas de informação os principais agentes responsáveis pelos incidentes de

comprometimento desses sistemas. Essa ênfase destaca a necessidade de conscientização e envolvimento ativo dos usuários na manutenção da segurança da informação.

Pimenta e Quaresma (2016) argumentam que a implementação de pequenas ações, o engajamento dos colaboradores e a adoção de programas de capacitação podem atenuar problemas relacionados à segurança da informação. A própria organização, ao manter uma cultura de campanhas de conscientização, alertas sobre condutas adequadas e precaução em relação aos riscos, desempenha um papel significativo nesse processo.

Dessa forma, com base nas orientações fornecidas por Ferreira (2017) e Pimenta e Quaresma (2016), pode-se resumir os principais mecanismos das boas práticas de segurança da informação que devem ser implementados nos ambientes de trabalho, como destacado no Quadro 7 a seguir:

Quadro 7 – Mecanismos de defesa para boas práticas de segurança da informação

Medidas de Segurança
Aplicar as atualizações de segurança recomendadas
Criptografia
Controle de acesso
Utilizar e atualizar com frequência os programas antivírus
Atualização de softwares
Realizar cópias de segurança (*backup*
Registro de eventos (Log)
Política de segurança da informação
Cópias de segurança (*backup*)
Realizar cópias de segurança com regularidade
Adotar controle de acesso nos sistemas sem salvar as senhas e não as transferir a terceiros
Utilizar senhas robustas e diferentes em cada aplicação
Biometria
Não partilhar a informação do seu computador com outros
Não compartilhar ou divulgar as suas senhas com os outros
Ser responsável e cuidadoso na utilização da Internet e do correio eletrônico
Firewall
Registro de eventos (Log)
Biometria
Ser cuidadoso na utilização de equipamentos de armazenamento externos
Informar no caso de incidentes com vírus, roubos ou perdas de informação
Estar ciente que todos os atos praticados têm consequências
Utilizar um firewall
Bloquear o computador quando se ausentar
Não utilizar software ilegal ou de compartilhamento de arquivos.

Fonte: Adaptado de Ferreira (2017) e Pimenta e Quaresma (2016).

Observando os mecanismos relativos à defesa das boas práticas de segurança da informação, conforme apresentados pelos autores Ferreira (2017) e Pimenta e Quaresma (2016), pode-se afirmar que as ações sugeridas desempenham um papel crucial na prevenção de potenciais danos aos sistemas de informação e na redução da vulnerabilidade em seu uso.

Essas estratégias priorizam especialmente a segurança no desenvolvimento de senhas, certificações digitais, Internet, estações de trabalho e na rede institucional.

A segurança da informação é uma área altamente regulamentada, respaldada por padrões internacionais e normas nacionais que definem diretrizes obrigatórias para serem adotadas por organizações. Essas normas desempenham um papel crucial, proporcionando uma estrutura sólida para a proteção de sistemas, dados e informações. Fraga (2019) explica que ao aderir a essas normas, as organizações não apenas asseguram maior segurança, mas também colhem uma série de benefícios relacionados à conformidade, que incluem a mitigação de riscos, a melhoria da confiança do cliente, a proteção da reputação e a promoção de práticas de negócios mais sólidas e eficientes.

Conforme apontado por Santana (2021), é importante esclarecer que os padrões estabelecidos não possuem caráter obrigatório ou sancionatório, mas sim representam diretrizes que servirão de base para a implementação da PGSI. Essas diretrizes são desenvolvidas para facilitar a efetiva e apropriada adoção das melhores práticas e técnicas relevantes, com o objetivo de promover a criação de um ambiente de segurança da informação robusto e confiável.

Outro importante marco para combater os incidentes de segurança da informação no Brasil foi a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), que em seu Art. 1º:

> Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

Ressalta-se também a Lei nº 12.965, de 23 de abril de 2014, que em seu Art. 2º "Disciplina o uso da Internet no Brasil e tem como fundamento o respeito à liberdade de expressão" (Brasil, 2014).

A crescente preocupação com a segurança da informação tem impulsionado a criação de padrões e normas internacionais que se concentram na implementação e aprimoramento dos SGSI. Essas diretrizes têm encontrado uma aplicação significativa das PGSI adotadas nos órgãos da Administração Pública Federal. Isso reflete a importância atribuída à segurança da informação como um elemento essencial para proteger dados sensíveis e garantir o funcionamento eficaz das instituições governamentais em um cenário cada vez mais digital e interconectado.

Nessa pesquisa, foi empregada a fundamentação normativa da série ISO/IEC 27000, com ênfase nas normas de segurança da informação da ABNT listadas no quadro 8, que são relevantes para o estudo.

Quadro 8 – Principais Normas de segurança da informação da família ISO/IEC 27000

Normas	
ABNT NBR ISO/IEC 27000	
Título	Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da Segurança da Informação - Descrições e vocabulário.
Data/Vigor	2016
Objetivo	Proporcionar uma visão geral de sistemas de gestão de segurança da informação, de termos e de definições comumente usados na família ISMS de normas. Essa Norma é aplicável a todos os tipos e tamanhos de organização (por exemplo, empresas comerciais, agências governamentais e organizações não lucrativas)
ABNT NBR ISO/IEC 27001	
Titulo	Segurança da informação, segurança cibernética e proteção de privacidade – Sistemas de gestão da segurança da informação – Requisitos.
Data/Vigor	2022
Objetivo	Fornecer requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gerenciamento de segurança da informação.
ABNT NBR ISO/IEC 27002	
Titulo	Segurança da informação, segurança cibernética e proteção da privacidade — Controles de segurança da informação.
Data/Vigor	2022
Objetivo	Estabelecer diretrizes para as práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, considerando os ambientes de risco da segurança da informação da organização.
ABNT NBR ISO/IEC 27003	
Titulo	Tecnologia da informação - Técnicas de segurança – Sistemas de gestão da segurança da informação – Orientações.
Data/Vigor	2020
Objetivo	Tratar dos aspectos críticos necessários para a implantação de um projeto bem-sucedido de um SGSI, de acordo com a ABNT NBR ISO IEC 27001:2005. A norma descreve o processo de especificação e o projeto do SGSI desde a concepção até a elaboração dos planos de implantação.
ABNT NBR ISO/IEC 27004	
Titulo	Tecnologia da informação - Técnicas de segurança – Sistemas de gestão da segurança da informação – Monitoramento, mediação, análise e avaliação.
Data/Vigor	2017
Objetivo	Auxiliar as organizações a avaliar o desempenho da segurança da informação e a eficácia do sistema de gestão de segurança da informação, a fim de atender aos requisitos da ABNT NEB ISSO/IEC 27001:2013.
ABNT NBR ISO/IEC 27005	
Titulo	Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação
Data/Vigor	2019
Objetivo	Essa Norma dá as diretrizes para o processo de gestão de riscos de segurança da informação.

Adaptado da ABNT (2022).

As normas são elaboradas para orientar a implantação de SGSI, mas possuem algumas especificidades que as diferenciam umas das outras. A ABNT NBR ISO/IEC 27000 é mais geral e pode ser aplicada em qualquer tamanho de organização (por exemplo: empresas

comerciais, agências governamentais e organizações não lucrativas). A Norma ABNT NBR ISO/IEC 27000 e a Norma ABNT NBR ISO/IEC 27001 apresentam modelo para implementar, manter e/ou melhorar um SGSI, com o intuito de orientar as empresas na implementação de sistemas de segurança da informação com redução dos riscos operacionais e com abordagem de processo.

As normas acima discutidas trazem em sua estrutura os aspectos voltados aos conceitos básicos sobre informação, segurança da informação, ativos da informação, entre outros. Dessa forma, contextualizam a política da segurança da informação e todo o seu entorno, os seus pontos críticos e orientações para implementação com programa de treinamento (ABNT, 2022). Orientam, enfim, como manter a continuidade do negócio.

4 METODOLOGIA

Nesta seção, o roteiro foi elaborado para a condução desta pesquisa, contemplando as etapas e os instrumentos que puderam responder às questões da pesquisa e alcançar seus objetivos.

A compreensão da metodologia científica, de acordo com Mattos (2020), está intrinsecamente ligada à importância da ciência e da geração de conhecimento para o benefício da sociedade. Isso envolve a capacidade de interpretar fenômenos e contribuir para o avanço do conhecimento, motivando o pesquisador a explorar tanto o que já foi estudado quanto o que ainda permanece inexplorado, com foco nas lacunas do conhecimento que inspiram novas pesquisas. Nesse sentido, ela explica: “Cabe ao pesquisador, na busca do novo conhecimento, livrar-se dos pré-conceitos e ater-se àquilo que se apresenta no mundo. É um constante re-fletir, ou seja, dobrar sobre si mesmo e olhar o que está posto” (Mattos, 2020, p. 18).

Koche (2011) afirma que na sociedade contemporânea, as ações voltadas para o desenvolvimento científico têm sido fundamentadas em uma base teórica do conhecimento. Isso, por sua vez, desempenha um papel crucial no processo de tomada de decisão sobre as ações humanas nos diversos setores da sociedade.

Nessa justificativa, destaca-se, como mencionado por Koche (2011), que o conhecimento pode ser efetivamente organizado e aplicado por meio de pesquisas científicas, sendo notável por sua natureza revolucionária e constante evolução. Em consonância com essa visão, conforme Demo (1995, p. 19), a metodologia científica se encarrega de acordo com seus objetivos: “ Das formas de se fazer ciência. Cuida dos procedimentos, das ferramentas, dos caminhos”.

Conforme ressaltado pelos autores mencionados acima, a metodologia científica é fundamental no constante avanço da ciência e na busca pela qualidade científica. Ela direciona de forma dinâmica e sistemática as abordagens e ferramentas empregadas no processo de pesquisa.

Esse estudo, inserido no campo das Ciências Sociais, enfatiza a marcante mutabilidade e dinamismo inerentes à realidade social. Almeida, Perucchi e Freire (2020) observam que essa característica confere uma complexidade multidimensional às pesquisas nesse campo, que se fundamentam em uma ampla variedade de fenômenos sociais em constante transformação.

Além disso, os mesmos autores afirmam que tais pesquisas são fundamentadas em conceitos sólidos, especialmente no núcleo intelectual da CI, onde os domínios da informação,

conhecimento e comunicação se entrelaçam em campos interdisciplinares, situando estas pesquisas entre “Teoria e prática, ciência e sociedade, conhecimento teórico e mercado, informação e intervenção” (Almeida; Perucchi; Freire, 2020, p. 3)

Sobre a configuração social das pesquisas em CI, González de Gómez (2000) entende que os fenômenos informacionais são articulados em zonas interdiscursivas do conhecimento resultando na construção de novos significados das práticas e ações sociais da informação. Para melhor explicar estas indagações:

> Quando são abordadas as práticas e ações de informação, devemos usar estratégias comunicacionais seja para reconstruir a produção de sentido dos atores sociais, seja para construir e interpretar indicadores operacionalizados sobre produtos e resultados observáveis das ações de informação (González de Gómez, 2000, p. 4).

Ainda no prisma das ciências sociais, Coutinho (2011) destaca a necessidade de adotar um espírito científico flexível como um pilar essencial da metodologia científica. Isso significa que, durante o desenvolvimento da pesquisa, diversos fatores podem influenciar a compreensão e a essência do fenômeno social em análise. Portanto, o pesquisador deve estar preparado para ter à sua disposição uma variedade de opções para planejar e, se necessário, ajustar as estratégias de investigação, conforme enfatizado pelo autor.

Braga (2007) aborda a metodologia científica como um percurso que, quando adequadamente planejado e conduzido com rigor científico, produz resultados que validam a pesquisa e enriquecem os estudos de alta qualidade. Na visão do autor, os resultados significativos alcançados nas pesquisas em CI resultam da sua abordagem multidisciplinar, que levanta questões capazes de influenciar várias áreas do conhecimento.

Na mesma linha de pensamento, Sampieri, Collado e Lucio (2013) argumentam que as pesquisas atendam aos critérios que possibilitem avaliar sua importância potencial, conforme enunciam: “Conveniência, relevância social, implicações práticas, valor teórico e utilidade metodológica. Além de analisar a viabilidade da pesquisa, é preciso considerar suas possíveis consequências” (Sampieri; Collado Lucio, 2013, p. 68).

Considerando que a metodologia desempenha um papel fundamental na orientação e organização da pesquisa de maneira estruturada, é relevante incorporar as reflexões de Valentim (2005) sobre a construção do conhecimento científico e a metodologia no campo da CI. A autora defende a construção do conhecimento como o alicerce essencial para o desenvolvimento científico de qualquer área e atribui ao sujeito cognoscente a responsabilidade de formular questões e incertezas que estimulam a busca por soluções e a criação de novos conhecimentos.

De acordo com a mesma autora, por meio do conhecimento cumulativo promovido pela ciência, a pessoa apreende, analisa, reflete e gera novos questionamentos criando um ciclo de geração de conhecimento que retroalimenta as pesquisas no campo científico. Nesse sentido, Valentim (2005, p. 13) enfatiza a relevância da metodologia científica, uma vez que:

> A natureza da ciência é compreensiva e metodológica, isto é, os procedimentos para fazer ciência devem permitir a observação racional do (s) fato (s), a interpretação e a explicação adequada do (s) fenômeno (s), possibilitar a verificação através de técnicas próprias e fundamentar os princípios da generalização (Valentim, 2005, p. 13).

Dadas as discussões elencadas nessa seção e tendo como meta apresentar as principais estratégias a serem adotadas na pesquisa, na sequência dessa introdução metodológica seguirão as seguintes subseções: caracterização da pesquisa, identificando o tipo de pesquisa e a abordagem adotada; o local da intervenção; a população e a amostra; os critérios de inclusão e/ou exclusão da amostra; as técnicas/procedimentos de coleta; o método de análise dos dados coletados e as considerações éticas.

4.1 Caracterização da pesquisa

A classificação de uma pesquisa permite esquematizar os métodos e técnicas que foram aplicados para atingir os seus objetivos, apresentando uma solução para o problema formulado.

De forma geral, existem diferentes maneiras de classificar uma pesquisa, a maioria das quais são critérios adotados de acordo com os objetivos estabelecidos para responder ao problema de pesquisa. Nesse contexto, Gil (2017) enfatiza que a classificação da pesquisa é apoiada pela sua especificidade, considerando a existência de elementos gerais comuns nas investigações científicas, as quais se diferenciam pelas suas tipologias, enfoques e abordagens

Segundo Sampieri, Collado e Lucio (2013), deve-se inicialmente elaborar um desenho ou design da pesquisa adequado a sua classificação, baseando-se principalmente na elaboração de um plano que apresente melhor resultado quanto aos métodos de coleta e análise de dados, validando os seus resultados.

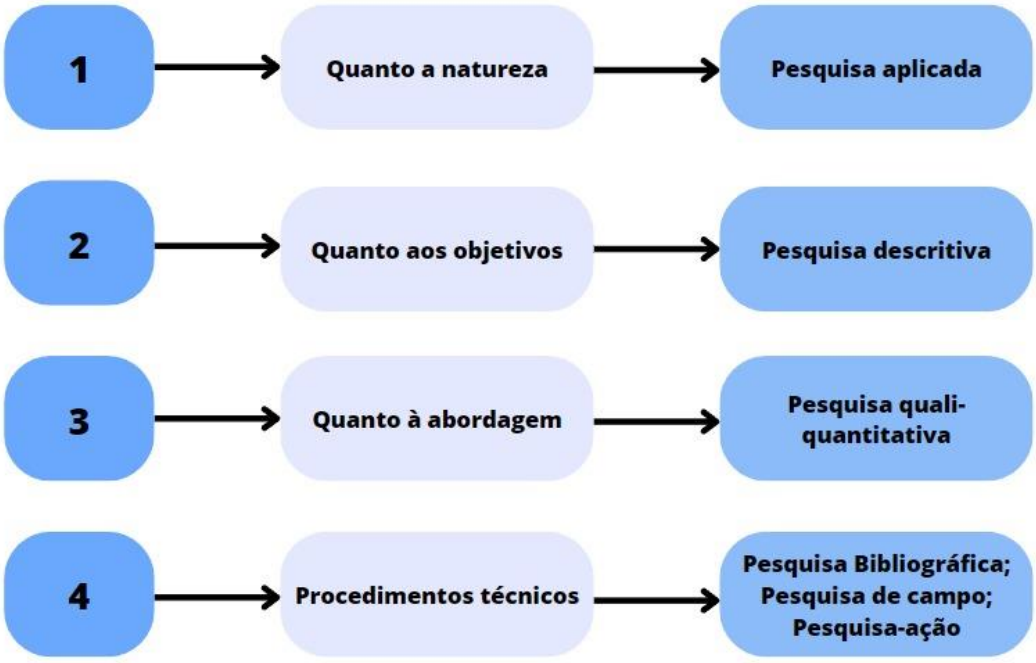
Sobre a classificação da pesquisa, Gil (2017) esclarece que no núcleo das pesquisas existe uma grande diversidade dos fenômenos e ambientes dispersos em que se inserem as pesquisas. Para o autor, a grande variedade de métodos e enfoques que envolvem a análise e interpretação da pesquisa, depende do seu planejamento baseado em uma boa caracterização da pesquisa, principalmente porque “o delineamento da pesquisa expressa tanto a ideia de modelo quanto a de plano” (Gil, 2017, p. 33).

Sob uma perspectiva metodológica, Bortoloti (2015) destaca que a classificação da pesquisa envolve um processo dinâmico que vai além de um mero protocolo. Ela busca explicitar de maneira clara a natureza da pesquisa e os principais métodos que a orientaram durante seu desenvolvimento. De acordo com o autor, o delineamento da pesquisa se concentra na resolução do problema de pesquisa em várias dimensões.

Cervo, Bervian e Silva (2007) esclarecem que a diversidade de tipos de pesquisa e seus distintos aspectos, que englobam os objetivos e problemas de pesquisa, têm como base três elementos essenciais: "dúvida/problema, método científico e resposta/solução" (Cervo, Bervian; Silva, 2007, p. 57). Em outras palavras, a resolução de um problema de pesquisa é alcançada por meio do método científico adotado pelo pesquisador.

Considerando a questão e os objetivos desse estudo, elaborou-se o seu delineamento, adaptado através das bases conceituais discutidas por Gil (2017) e Sampieri, Collado e Lucio (2013), buscando-se classificar e esquematizar a caracterização da pesquisa, como ilustrado na Figura 6.

Figura 6 – Caracterização da pesquisa



Fonte: Elaboração própria, adaptado de Gil (2017) e Sampieri, Collado e Lucio (2013).

Com relação à natureza prática da pesquisa, uma vez que envolve uma intervenção que culmina em um produto técnico-científico, é apropriado classificá-la como pesquisa aplicada. Marques (2016) argumenta que ambas as tipologias de pesquisa, básica e aplicada,

desempenham papéis igualmente significativos no avanço da ciência, embora o impacto econômico das pesquisas aplicadas seja mais prontamente perceptível.

A pesquisa aplicada se destaca por seu compromisso com a geração de produtos e soluções práticas, em oposição à pesquisa básica, que não possui uma aplicação direta imediata. Nesse contexto, a pesquisa aplicada direciona seus objetivos para a promoção de novos produtos, a inovação e o progresso científico, concentrando-se na capacidade de resolver problemas do mundo real. Essa abordagem é fundamental para impulsionar avanços significativos e tangíveis em diversas áreas do conhecimento (Zucatto, Freitas; Marzzoni, 2020).

Com base em seus objetivos, foi possível classificar esta pesquisa com alcance descritivo, a qual “descreve tendências de um grupo ou população” (Sampieri; Collado; Lucio, 2013, p. 102), fornecendo detalhes sobre “dados e fatos colhidos da própria realidade (Cervo; Bervian, 2002, p. 67). Com base nas abordagens dos autores mencionados, os objetivos desta pesquisa foram estabelecidos com a finalidade de descrever uma situação real, conduzindo análises e identificando várias variáveis relevantes.

Conforme Sampieri, Collado e Lucio (2013) destacam, os estudos descritivos são direcionados para a tarefa de fornecer uma visão detalhada e completa de diversos fenômenos. Essa abordagem de pesquisa envolve uma análise minuciosa e meticulosa, com o objetivo de especificar e narrar exaustivamente as características e particularidades de perfis de indivíduos, grupos, comunidades, processos, objetos e uma ampla variedade de fenômenos, oferecendo assim uma compreensão aprofundada desses elementos em estudo.

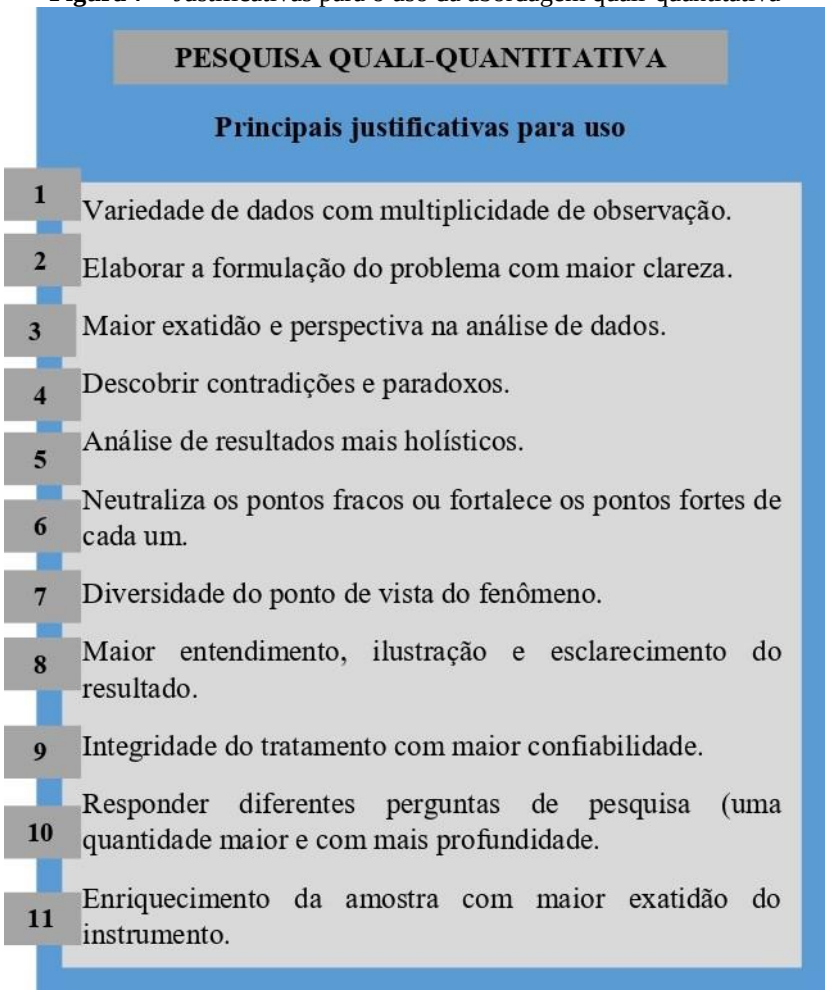
Evêncio *et al*. (2019) defendem que, ao realizar uma pesquisa com objetivo descritivo, é possível investigar e detalhar minuciosamente um grupo específico. Isso envolve a identificação de variáveis que, ao longo da pesquisa, podem fornecer esclarecimentos adicionais e novas perspectivas em relação ao problema de pesquisa.

A abordagem escolhida para esse estudo foi direcionada de acordo com os objetivos estabelecidos, que envolveram a coleta de dados numéricos e análise de texto. Optou-se pela abordagem quali-quantitativa, pois ela amplia a análise dos dados e permite "obter uma perspectiva mais abrangente e profunda do fenômeno" (Sampieri; Collado; Lucio, 2013, p. 552).

Dada a diversidade de abordagens de pesquisa disponíveis, a escolha de adotar uma abordagem quali-quantitativa foi respaldada pela integração de princípios fundamentais dos renomados autores Creswell e Clark (2013), Sampieri, Collado e Lucio (2013) e Sampieri e

Torres (2018). Esse processo de adaptação e fundamentação pode ser visualizado na Figura 7, onde se delineiam as principais justificativas para essa escolha.

Figura 7 – Justificativas para o uso da abordagem quali-quantitativa



Fonte: Adaptado de Creswell e Clark (2013), Sampieri, Collado e Lucio (2013) e Sampieri e Torres (2018).

Em sua reflexão, Creswell e Clark (2013) pontuam que estudos quali-quantitativos são embasados nas questões de pesquisa e na condução da coleta e análise de dados, possibilitando combinar, conectar, integrar e incorporar seus resultados. Para o autor, cabe ao pesquisador verificar se o enfoque misto corresponde racionalmente para o delineamento da abordagem do estudo proposto.

Na perspectiva metodológica, os mesmos autores explicam que, somente a partir da escolha da abordagem da pesquisa o pesquisador poderá determinar o método de coleta e análise de dados, sendo uma etapa fundamental para validação dos dados (Creswell; Clark, 2013).

Para Sampieri, Collado e Lucio (2013), a pesquisa quali-quantitativa ou mista, aproxima fenômenos em uma realidade intersubjetiva, ou seja, transcorre entre a dualidade dos

fenômenos reconhecendo a convergência da explicação dos dados por meio da estatística e pela interpretação da realidade social.

Os autores nessa concepção reconhecem que existe uma abundância de dados que propiciam maior dimensão interpretativa e de conhecimento permitindo obter “uma fotografia mais completa do fenômeno” (Sampieri; Collado; Lucio, 2013, p. 550).

Em consonância com o exposto, Hernández e Torres (2018) reconhecem a abordagem quali-quantitativa como uma terceira via para atender os diferentes fenômenos que emergiram a partir do século XXI, trazendo um novo olhar para diferentes áreas do conhecimento e desenvolvimento profissional e científico.

Para os autores supracitados, a adoção de uma abordagem investigativa que responda e mescle questões de pesquisa objetivas e subjetivas consegue resultados mais precisos e dinâmicos. Nesse entendimento, complementam:

> Os métodos mistos representam um conjunto de processos de pesquisa sistemáticos, empíricos e críticos e envolvem a coleta e análise de dados quantitativos e qualitativos, bem como sua integração e discussão conjunta, para fazer inferências como resultado de todas as informações coletadas (metainferências) e alcançar uma melhor compreensão do fenômeno em estudo (Sampieri; Torres, 2018, p. 612, tradução nossa).

Quanto aos procedimentos técnicos, considera-se como a etapa em que se aplicam as técnicas de pesquisa para sua operacionalização, ou seja, consiste na parte prática da pesquisa que delibera os métodos da coleta de dados (Gil, 2017). Para esse estudo, a pesquisa foi caracterizada como bibliográfica, pesquisa de campo e pesquisa-ação.

Inicialmente é preciso identificar os principais autores que irão embasar e fundamentar teoricamente o estudo, que consiste no desenvolvimento da perspectiva teórica da pesquisa, realizada através de uma pesquisa bibliográfica e, em seguida, identifica-se a perspectiva prática da pesquisa, que consiste na inserção do pesquisador no campo da pesquisa. Esses procedimentos serão apresentados em subtópicos, a seguir.

4.1.1 Perspectiva teórica da pesquisa: pesquisa bibliográfica

De acordo com autores como Gil (2017), Marconi e Lakatos (2017), Severino (2017), a pesquisa bibliográfica é o ponto de partida da pesquisa científica, parte da busca pelo conhecimento de determinado assunto para esclarecer e embasar os fundamentos teóricos da pesquisa, colaborando com a elaboração do problema de pesquisa e identificando como determinado fenômeno tem sido explorado e discutido em âmbito científico.

Garcia (2016) explica que, para a realização de uma pesquisa científica é preciso que ela seja adequadamente classificada, mesmo porque cada pesquisa possui etapas determinantes para o alcance do seu resultado. Não fugindo a regra, a pesquisa bibliográfica não pode se resumir em alguns conceitos escolhidos sem critérios ou propósitos, por isso, atribui a revisão de literatura como uma etapa. Em sua concepção:

> As pesquisas que podem ser classificadas como bibliográficas são na sua maioria, aquelas que buscam discutir sobre ideologias ou ainda as que buscam conhecer e analisar as contribuições culturais ou científicas do passado sobre um determinado assunto, tema ou problema (Garcia, 2016, p. 293).

Em sua afirmação, o autor reforça que a pesquisa bibliográfica embasa teoricamente todo os tipos de pesquisa e vem trazer melhor entendimento teórico sobre o objeto de estudo. Garcia (2016) reforça a importância dessa pesquisa para os possíveis diálogos existentes na comunicação científica e nos diferentes campos de conhecimento (Garcia, 2016).

Corroborando com as alegações supra, Sousa, Oliveira e Alves (2021) apresentam como fundamento da pesquisa bibliográfica uma sistematização do conhecimento amparada por uma sequência de etapas que a validam. Os autores explicam que a pesquisa bibliográfica inicia o processo científico, baseada em trabalhos publicados e validados pela comunidade científica, colabora com a escolha do problema e o método adequado, “uma vez que nos permite conhecer melhor o fenômeno em estudo” (Sousa; Oliveira; Alves, 2021, p. 65)

Sampieri, Collado e Lucio (2013) defendem a perspectiva teórica da pesquisa como um apoio e referência para o esclarecer o objeto de pesquisa e o desenvolvimento do estudo. Implica em uma análise mais profunda sobre as teorias, conceitos, pesquisas prévias e antecedentes em geral que possam referenciar da melhor forma a fundamentação teórica do estudo.

Para os autores, a pesquisa bibliográfica proporciona o estado da arte e orienta o estudo, possibilitando ampliar seus horizontes por meio de ideias úteis, pelo compartilhamento de novas descobertas e através do diálogo entre os principais teóricos para enriquecer de conhecimento da área (Sampieri; Collado; Lucio, 2013).

Gil (2017) entende que ao realizar uma pesquisa bibliográfica o pesquisador deve verificar a veracidade das fontes, incluindo as possíveis incoerências ou contradições que as obras possam apresentar. O autor identifica como principal vantagem desse tipo de pesquisa a gama de diferentes fenômenos que se acessa e a cobertura de posicionamentos de determinado assunto, sem esquecer que pesa sobre a qualidade da pesquisa uma análise criteriosa das fontes para identificar possíveis incoerências ou mesmo contradições (Gil, 2017).

Analisando as diferentes configurações da pesquisa bibliográfica com ênfase na natureza das fontes, Severino (2017) entende que o mapeamento das fontes publicadas com os estudos publicados, ou quase todos, é etapa inicial e fundamental para a realização desse tipo de pesquisa. Segundo o autor:

> A pesquisa bibliográfica é aquela que realiza a partir do registro disponível, decorrente de pesquisas anteriores, em documentos impressos, como livros, artigos, teses etc. Utiliza-se de dados ou de categorias teóricas já trabalhados por outros pesquisadores e devidamente registrados. Os textos tornam-se fontes de temas a serem pesquisados. O pesquisador trabalha a partir das contribuições dos autores dos estudos analíticos constantes dos textos (Severino, 2017, p. 124).

Conforme citação de Severino (2017), pode-se confirmar que a pesquisa bibliográfica se embasa em diferentes fontes, o que torna essencial que o pesquisador detenha grau de competência em informação para buscar em diferentes suportes, físicos ou digitais, as diferentes bibliografias que fundamentem teoricamente o desenvolvimento da pesquisa.

Incialmente, a escolha do tema já justificado anteriormente, teve como principal objeto de estudo os fenômenos da segurança da informação e dele se subdividem subtemas dispostos em seções e subseções para um maior aprofundamento da revisão de literatura e resposta da questão de pesquisa.

O levantamento bibliográfico preliminar levou a identificar como a temática tem sido pesquisada no campo científico e permitiu elaborar um plano provisório de assunto a ser pesquisado nas fontes. As fontes de informação serão pesquisadas para fundamentar o conhecimento sobre a temática e os principais conceitos que trarão elementos para estabelecer os critérios para a análise dos dados quali-quantitativos. Importante que o pesquisador busque embasamento teórico na literatura especializada. Gil (2017) orienta que o pesquisador identifique as fontes de literatura científica validadas para reforçar seu estudo e comparar com outras pesquisas.

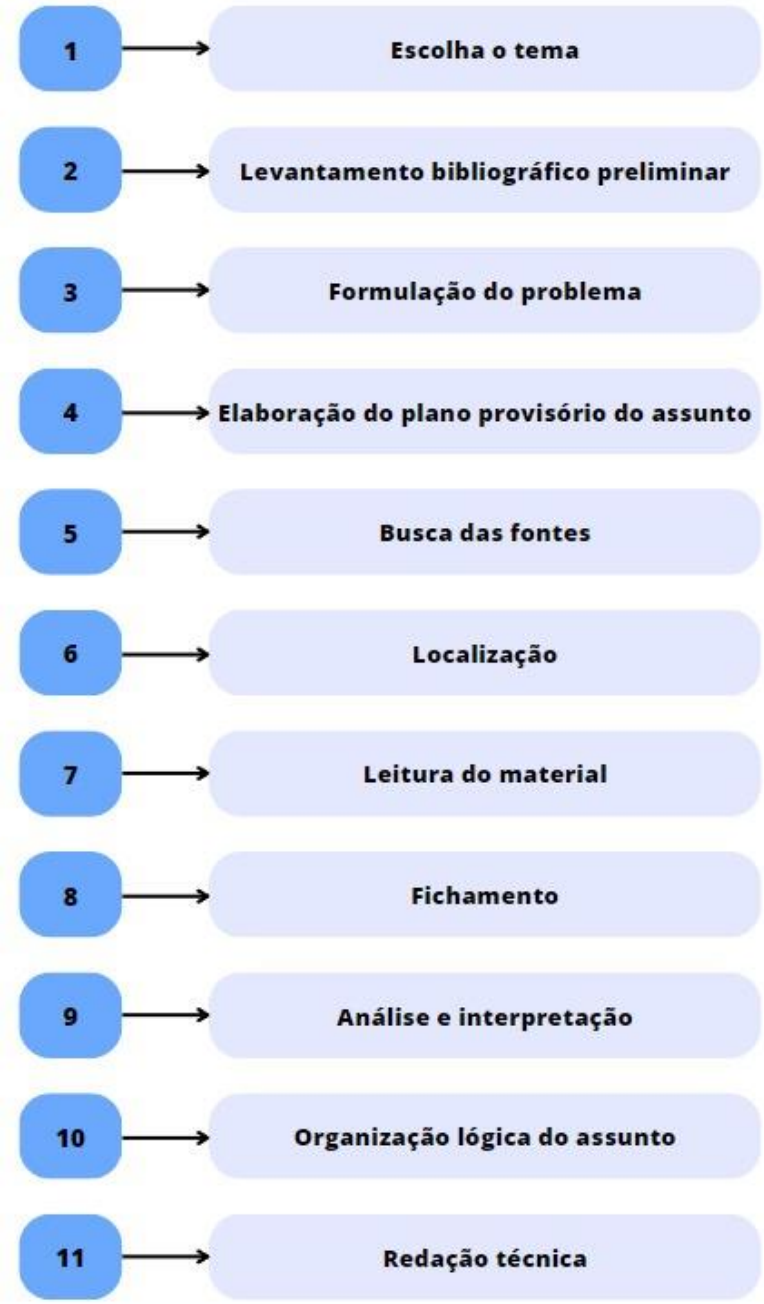
Com relação as fontes de informação, a busca será realizada em biblioteca, para os livros em formato físico, e em bases de dados digitais, para o embasamento teórico do tema e configuração do estado da arte. Os artigos serão pesquisados em base de dados científicas abertas e em Biblioteca Virtual da área da CI e repositórios institucionais, abrangendo ainda a Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), que integra em seus sistemas de informação teses e dissertações de várias áreas do saber.

Para Marconi e Lakatos (2017) a natureza das fontes deve ser associada ao desenvolvimento teórico da pesquisa embasada em produções científicas de livros, artigos científicos, ensaios críticos, teses, dissertações, jornais, revistas, entre outros, destacando os

artigos científicos como fonte de maior interesse pelos pesquisadores. Isso se dá pela publicação atualizada de pesquisas, tidas como conhecimento de ponta (Marconi; Lakatos, 2017).

Sintetizando as ideias corroboradas por Marconi e Lakatos (2017) e Severino (2017), a figura 8 apresenta as principais etapas da pesquisa bibliográfica estabelecidas no bojo dessa pesquisa e descritas para maior entendimento.

Figura 8 – Etapas da pesquisa bibliográfica



Fonte: Adaptado de Gil (2017, p. 60) e Marconi e Lakatos (2017, p. 58).

Marconi e Lakatos (2017) sugerem que as principais fontes, de uma forma geral são: periódicos científicos, bases de dados com indexação de publicações científicas

interdisciplinares, Bibliotecas Virtuais de instituições de ensino superior, BDTD, que integra em seus sistemas de informação teses e dissertações de várias áreas do saber. As fontes formais como livros de referência e publicações atualizadas devem ser utilizadas.

No que diz respeito aos artigos de periódicos, teses e dissertações, foi adotado um recorte temporal de cinco anos a partir da data de publicação. Esse período é amplamente reconhecido pela comunidade científica como relevante, abrangendo trabalhos com resultados consolidados e/ou de natureza inovadora.

Devido à natureza da pesquisa no campo da Ciência da Informação e à abordagem de uma temática que envolve autores de referência, optou-se por não impor um limite temporal às obras reconhecidas como clássicas, mesmo que muitas delas contassem com mais de dez anos de publicação. Essa escolha teve como objetivo abranger adequadamente as contribuições históricas e fundamentais para o campo de estudo, bem como incluir publicações consideradas como marcos referenciais.

Para as estratégias de busca nas bases de dados, foram utilizadas palavras-chave associadas a operadores lógicos (booleanos), tais como: segurança da informação; políticas de informação; comportamento informacional; sistemas de informação; GI e GC. Rowley (2003) explica que os operadores booleanos constituem a base dos computadores digitais que relacionam termos ou palavras para utilização de busca informatizada para recuperação da informação através de um comando de pesquisa.

O quadro 9 apesenta um esquema simplificado de funcionamento dos operadores booleanos adaptados de Rowley (2002).

Quadro 9 - Esquema simplificado de funcionamento dos operadores booleanos

Operador booleano				Tipo de busca	Significado
AND	**A**	**E**	**B**	Conjuntiva	Recupera apensas as páginas ou documentos que contenham A e B
OU	**A**	**OU**	**B**	Aditiva	Recupera todas as páginas ou documentos que contenham somente A, somente B ou mesmo AB
NOT	**A**	**NÃO**	**B**	Subtrativa	Recupera apenas páginas ou documentos que contenham A, ou seja, as que contenham B ou AB, não serão identificados

Fonte: Adaptado de Rowley (2002).

Na condução da pesquisa, foi adotada uma estratégia de busca criteriosa que desempenhou um papel crucial na seleção dos materiais empregados no estudo. Estabeleceu-se como critério de exclusão a limitação do período das publicações periódicas, dissertações e teses a um máximo de cinco anos, ressalvando-se obras de referência e publicações de livros. Não houve imposição de limite geográfico. Posteriormente, os materiais selecionados foram

submetidos à leitura e elaboração de fichamentos, proporcionando maior facilidade na condução da escrita acadêmica.

4.1.2 Perspectiva prática da pesquisa: pesquisa de campo e pesquisa-ação

Nessa etapa do estudo, em que são projetados os procedimentos técnicos, já construído o arcabouço metodológico, torna-se possível o desenvolvimento prático da pesquisa no que tange ao trabalho de campo para coletar dados.

Muito se associa a pesquisa de campo à simples coleta de dados. No entanto, Mattos (2020) argumenta que se trata de um processo muito mais rigoroso, que demanda um planejamento cuidadoso com objetivos preestabelecidos e exige um sólido embasamento científico sobre o objeto de estudo. A autora enfatiza que para identificar variáveis relevantes na pesquisa, é necessário que o pesquisador se aproxime da realidade e dos fenômenos, conduzindo a pesquisa por meio da observação direta.

Corroborando com o pensamento de Mattos (2020), os autores Booth, Colombo e Williams (2008) reforçam que a pesquisa de campo não reflete simplesmente recortes de citações de observações, questionários ou entrevistas, e indicam como prudência: “Use as observações para sustentar sua análise, em vez de substituí-la” (Booth; Colombo; Williams, 2008, p. 207).

A pesquisa de campo, conforme Severino (2017), possibilita ao pesquisador um contato direto com a realidade de seu objeto de estudo. Isso, por sua vez, apresenta o desafio de lidar com o universo de ocorrências imprevisíveis, requerendo o uso de diversos recursos para a coleta de dados, como destacado por Gil (2017).

A justificativa para a utilização da pesquisa de campo, segundo Marconi e Lakatos (2017), reside na obtenção de informações e conhecimentos que auxiliem na coleta de dados, na busca por respostas para os problemas de pesquisa e/ou na confirmação de hipóteses, além de permitir a descoberta de novos fenômenos e a análise de suas relações.

As mesmas autoras entendem que o interesse e aceitação da pesquisa de campo por parte dos pesquisadores acontece por sua abrangência social, ou seja: “O interesse da pesquisa de campo está voltado para o estudo de indivíduos, grupos, comunidades, instituições, visando à compreensão de vários aspectos da sociedade” (Marconi; Lakatos, 2017, p. 217).

Marconi e Lakatos (2017) argumentam ainda que, entre as vantagens da pesquisa de campo, pode-se citar o acervo de informações sobre o fenômeno estudado que podem servir de referência para outros pesquisadores. Como desvantagem, citam o baixo grau de controle

sobre o contexto em que se executa a coleta de dados, somada aos fatores desconhecidos que possam interferir e fugir do controle do pesquisador. Nesse contexto, as autoras sugerem estratégias para aumentar o controle das informações, incluindo a realização de pré-testes e a utilização de instrumentos de coleta de dados mais abrangentes e completos.

Outro método importante para execução do procedimento técnico dessa pesquisa, que ora se desenvolve, é a adoção da pesquisa-ação, a qual vem atender os princípios intervencionistas propostos para a sua execução.

Muito se confunde a denominação da pesquisa-ação com a pesquisa participante, uma vez que ambas carregam, inclusive, uma certa sinonímia que para Thiollent (2011, p. 7), não procede:

> A nosso ver, não o são, porque a pesquisa-ação, além da participação, supõe uma forma de ação planejada de caráter social, educacional, técnico ou outro, que nem sempre se encontra em propostas de pesquisa participante. Seja como for, consideramos que pesquisa--ação e pesquisa participante procedem de uma mesma busca de alternativas ao padrão de pesquisa convencional.

Sob esse ângulo, Picheth, Cassandre e Thiollent (2016) identificam a forte influência da pesquisa-ação sobre a aprendizagem organizacional, atribuindo ao seu caráter interpretativo e de intervenção, uma possibilidade para resolução dos problemas e melhoria das práticas organizacionais no ambiente de trabalho. Segundo esses autores, a pesquisa-ação infere na solução coletiva dos problemas gerando conhecimento, a saber:

> Ademais, o intenso enfoque da pesquisa-ação quanto ao aprendizado, sendo concebida como metodologia que articula o conhecer e o agir e destacando a ação transformadora, permite identificar uma grande proximidade com as metodologias intervencionistas da abordagem histórico-cultural, sugerindo-se que a mesma também seja empregada no contexto de aprendizagem organizacional, na qual os princípios intervencionistas se encontram inseridos (Picheth; Cassandre; Thiollent, 2016, p. 12).

De acordo com Tripp (2005), a pesquisa-ação se manifesta em diversas facetas, impulsionada por aplicações específicas para resolver uma variedade de problemas. Isso significa que ao intervir em um contexto social, o pesquisador desenvolve um plano de ação ou ciclo de investigação que inclui a descrição, avaliação e identificação do recurso que melhor ofereça uma solução prática para o grupo investigado. Para o autor, a pesquisa-ação resulta em uma intervenção efetiva no ambiente estudado.

A perspectiva de Barbier (2004) sobre a pesquisa-ação a apresenta como uma ação planejada de dinâmica social que preenche a lacuna entre a teoria e a prática metodológica. Segundo sua visão, trata-se de uma pesquisa com objetivos práticos bem definidos. O autor enfatiza o papel crucial do pesquisador na pesquisa-ação, destacando a importância de adotar

uma postura autônoma, envolver-se de maneira colaborativa e estabelecer uma interação eficaz com os membros do grupo que compõem o objeto de análise.

Corrêa, Campos e Almagro (2018) enfatizam que a pesquisa-ação, embora tenha potencial para impulsionar mudanças sociais, requer a aprovação das autoridades hierárquicas para institucionalizar seus resultados práticos. Eles argumentam que a pesquisa-ação é intervencionista devido à participação ativa do pesquisador com os participantes, focando na resolução de problemas coletivos. Eles argumentam que:

> Cabe ao pesquisador avaliar a viabilidade do tipo de intervenção pesquisa-ação no meio pretendido, detectando possíveis apoios e resistências, convergências e divergências, posições otimistas ou negativas, além da necessidade de recursos financeiros (Corrêa; Campos; Almagro, 2018, p. 64).

Diante do cenário atual, repleto de variados problemas sociais, Thiollent (2011) atribui à pesquisa-ação uma abordagem coletiva que a caracteriza como uma metodologia de pesquisa social. Nesse sentido, sua base empírica está fundamentada na ação voltada para a resolução de problemas coletivos, o que o autor aponta como uma condição essencial para a prática dessa abordagem. Dentro dessa perspectiva, o autor delineia as principais abordagens da pesquisa-ação (Figura 9).

Figura 9 – Principais características da pesquisa-ação

Fonte: Elaborada pela autora e adaptado de Tiollent (2011, p. 22-23).

De acordo com a descrição feita por Thiollent (2011), a pesquisa-ação compreende a adoção de uma postura proativa e participativa por parte do pesquisador, fomentando a interação com os indivíduos inseridos no contexto da pesquisa e do problema investigado. Além disso, é fundamental que um problema comum seja identificado e que os resultados da pesquisa-ação se direcionem à resolução ou à elucidação desse problema, com o propósito de contribuir significativamente para o bem-estar da coletividade como um todo.

Dessa forma, Thiollent (2011) enfatiza que a abordagem de pesquisa-ação produz resultados que contribuem para a geração de conhecimento e a identificação de boas práticas voltadas para a resolução de problemas de relevância social, com impacto prático significativo. Nessa mesma linha teórica, Tripp (2005, p. 447) apresenta o seu conceito: "pesquisa-ação é uma forma de investigação-ação que utiliza técnicas de pesquisa consagradas para informar à ação que se decide tomar para melhorar a prática".

Na junção das principais alegações dos autores mencionados anteriormente, observa-se que a pesquisa-ação se alinha com as formulações apresentadas nesse estudo, uma vez que envolve a investigação de um problema que afeta um grupo dentro de um contexto organizacional.

Mediante a realização de pesquisa de campo e de uma pesquisa-ação, conduziu-se uma intervenção na PU/SE, envolvendo a colaboração ativa de todos os participantes. O resultado desta intervenção culminou na elaboração de um planejamento sistemático, com o propósito de diagnosticar a situação referente à interação dos usuários dos sistemas, participantes da pesquisa, com as normas já estabelecidas pela organização em relação à segurança da informação.

No decorrer desse processo, procedeu-se à coleta e análise de dados com o objetivo de abordar a questão de pesquisa e gerar um produto científico. Esse esforço conjunto contribuiu significativamente para a apresentação de uma solução prática e para o avanço substancial na área em foco.

4.2 Ambiente social de intervenção

O local onde a intervenção proposta foi realizada, com a prévia autorização, foi a PU/SE, situada na Avenida Beira Mar, nº 53, Bairro Treze de Julho, na cidade de Aracaju, Sergipe.

A PU/SE é órgão integrante da AGU vinculada ao Poder Executivo, órgão que representa o Estado brasileiro, judicial e extrajudicialmente o Poder Executivo (Brasil, 1988,

art. 131), além de defender em juízo a União, com a função social de promover o assessoramento e orientação dos dirigentes do Poder Executivo Federal, de suas autarquias e fundações públicas, para dar fulcro jurídico aos atos administrativos que serão praticados (Brasil, 2021).

A AGU é uma Instituição prevista pela Constituição Federal e tem natureza de Função Essencial à Justiça, para atuar em todos os foros, regiões e instâncias judiciais: Supremo Tribunal Federal (STF), Superior Tribunal de Justiça (STJ), Justiça do Trabalho, Justiça Militar, Justiça Eleitoral, Justiça Federal e Justiças dos Estados e do Distrito Federal.

Nos termos do art. 131 da Constituição,

> A Advocacia-Geral da União (AGU) é a instituição que, diretamente ou através de órgão vinculado, representa a União, judicial e extrajudicialmente, cabendo-lhe, nos termos da lei complementar que dispuser sobre sua organização e funcionamento, as atividades de consultoria e assessoramento jurídico do Poder Executivo (Brasil, 1988).

Quanto à escolha da PU/SE, é crucial enfatizar que se trata de uma instituição de extrema relevância para o país, uma vez que sua missão está alinhada com práticas jurídicas destinadas à proteção dos interesses da União, conforme estipulado em nossa Constituição Federal (Brasil, 1988). Os resultados alcançados por esta organização não apenas desempenham um papel significativo na economia dos recursos públicos, mas também orientam diretamente essas economias para investimentos essenciais em políticas públicas de importância vital para o desenvolvimento da nação.

Como unidade de informação jurídica, é crucial reconhecer que o ambiente social pode ser reconhecido como um campo de experimentação propício ao desenvolvimento de estudos na área da CI. Na PU/SE, a informação jurídica assume um papel central na condução dos processos informacionais.

Dado o considerável volume de informações legais, jurisprudência, regulamentos e documentos relacionados com os quais essa organização lida, torna-se vital que disponham de sistemas altamente eficientes para coletar, armazenar, analisar e utilizar informações jurídicas consolidadas. Essas informações constituem a base fundamental para embasar as ações legais da PU/SE, com uma ênfase especial na segurança da informação, assegurando a devida proteção desses dados sensíveis e estratégicos.

Destaca-se ainda o incentivo que a Escola Superior da AGU (ESAGU) que tem investido no apoio as pesquisas práticas e tecnológicas a qual promove a atualização e o aperfeiçoamento dos profissionais daquele órgão com promoção de acordos de cooperação com outras instituições de ensino, autorização para afastamento para estudo, bolsas de estudo, salas

virtuais de estudo, pós-graduações e a Escola Virtual da AGU (EVA), priorizando o banco de talentos da AGU, como o principal objetivo de promover a inovação através do desenvolvimento de novas técnicas de trabalho voltadas à Advocacia Pública. Outro marco para que novas pesquisas possam ser incentivadas nas unidades da AGU é o credenciamento da ESAGU junto ao Ministério da Educação para oferta de cursos de pós-graduação lato sensu, nos termos da Portaria MEC nº 674, de 13 de julho de 2018 (Brasil, 2018).

Dada a considerável quantidade de informações legais, jurisprudência, regulamentos e documentos correlatos com que essa organização lida, é de importância crítica a implementação de sistemas altamente eficazes para a coleta, armazenamento, análise e aplicação das informações jurídicas consolidadas. Essas informações fundamentam as ações legais da PU/SE, com especial ênfase na segurança da informação, garantindo a proteção adequada desses dados sensíveis e estratégicos.

4.3 População e amostra

A população dessa pesquisa foi constituída pelos servidores que integram o quadro funcional da PU/SE, divididos em diferentes categorias e funções, a saber: 13 (treze) Advogados da União, 16 (dezesseis) servidores técnico-administrativos efetivos, 8 (oito) servidores técnico-administrativos requisitados de outros órgãos do Poder Executivo Federal, 4 (quatro) empregados terceirizados e 1 (um) estagiário, todos lotados naquela unidade administrativa.

A população, conforme esclarecido por Sampieri, Collado e Lucio (2013, p. 193), é uma concepção fundamental na pesquisa, uma vez que ela representa a totalidade dos casos que preenchem critérios específicos e previamente definidos. Para os autores, compreender a composição da população é essencial para assegurar que os resultados da pesquisa sejam representativos e aplicáveis ao contexto ou fenômeno em estudo.

A seleção da amostra foi realizada com base no critério de inclusão de participantes que possuem acesso aos sistemas da AGU, com destaque para o SAPIENS, o sistema eletrônico primordial para o gerenciamento do fluxo informacional. Por outro lado, os servidores que não têm acesso a esse sistema foram deliberadamente excluídos da pesquisa.

Conforme dados publicados pelo site da AGU, o SAPIENS unifica e relaciona os elementos constantes dos processos administrativos, inclusive dossiês judiciais, colocando a AGU definitivamente na era da virtualização e do processo administrativo eletrônico (Brasil, 2018).

Os servidores que se enquadraram nos critérios da pesquisa foram selecionados por meio de uma amostra não probabilística, utilizando o método de conveniência. A pesquisa foi divulgada no site da PU/SE, seguida pelo envio de convites aos potenciais participantes. Durante esse processo, foram enfatizados os critérios éticos adotados para proteger os direitos dos participantes, incluindo a garantia de sigilo quanto à identificação de seus dados pessoais na divulgação dos resultados.

Para identificar os participantes da pesquisa, optou-se por utilizar uma sequência alfanumérica. Os Advogados da União foram identificados como ADV1 e subsequentemente em ordem crescente. Da mesma forma, os servidores técnico-administrativos integrantes do quadro da AGU foram designados como STA1 e subsequentemente STA2 e assim por diante. Os servidores cedidos de outros órgãos foram identificados com a sigla SCD1, enquanto os colaboradores terceirizados receberam identificações começando com ETERC1. Por fim, o estagiário foi identificado como ESTAG.

A categorização desempenhou um papel fundamental devido à ampla gama de tarefas relacionadas às diferentes funções dos membros da organização. Os Advogados da União lideram as atividades mais complexas no contexto dos sistemas judiciários, seguidos pelos servidores técnico-administrativos efetivos e cedidos, que fornecem suporte jurídico com amplo acesso a sistemas, incluindo o SAPIENS AGU, bem como outros sistemas integrados ao Poder Judiciário e Executivo, incluindo aqueles do DCP. Essa categorização reflete a hierarquia funcional e os níveis de interação com os sistemas de informação, o que é essencial para compreender a distribuição de tarefas e responsabilidades dentro da organização.

Ao selecionar a amostra, considerou-se o contexto das funções dos participantes da pesquisa como relevante. A maioria dos membros da PU/SE, com exceção dos colaboradores terceirizados, desempenha suas atividades remotamente por meio do sistema SAPIENS. Suas atividades estão diretamente ligadas às coordenações jurídicas da PRU5, abrangendo estados como Pernambuco, Alagoas, Ceará, Paraíba, Rio Grande do Norte e Sergipe quando regionalizadas. Quando as demandas se estendem a nível nacional, como no caso do DCP, estas são coordenadas pela PGU. Independentemente da modalidade de trabalho escolhida (presencial, semipresencial ou remota), todos os servidores continuam vinculados à PU/SE, com a descentralização das tarefas sendo realizada para promover a equidade.

No que diz respeito aos colaboradores terceirizados, é relevante salientar que eles possuem autorização para acessar e manipular documentos, abrir tarefas e criar documentos no SAPIENS, utilizando suas próprias credenciais de login e senha. No caso dos estagiários, eles

têm acesso completo ao SAPIENS e prestam suporte em atividades específicas dos Advogados da União, com a exceção do processo de peticionamento.

A seleção da amostra potencial pode ser resumida conforme apresentado no Quadro 10 a seguir:

Quadro 10 – Caracterização da amostra potencial da pesquisa

Participantes	Área	Categoria	Função	Nível	Quantidade
ADV	Fim	Advogados da União	Defesa da União	Superior	**13**
STA	Meio	Servidores técnico-administrativos	Apoio Jurídico	Médio e Superior	**16**
SCD	Meio	Servidores cedidos	Apoio jurídico direcionado ao NECAP	Médio e Superior	**8**
ETERC	Meio	Terceirizados	Apoio Administrativo	Médio	**4**
ESTAG	Superior	Estagiários	Apoio Jurídico	Superior	**1**

Fonte: Elaborado pela autora (2022).

Considerando que a organização possui e mantém sua infraestrutura tecnológica atualizada, incluindo a cessão temporária de equipamentos para os servidores que permanecem trabalhando remotamente, não foi necessário fazer investimentos adicionais em infraestrutura para realizar a pesquisa, o que resultou em economia de custos nesse aspecto.

4.4 Procedimentos de coleta de dados

Esta pesquisa empregou uma abordagem mista, que envolveu a coleta de dados tanto quantitativos quanto qualitativos para atender aos seus objetivos o que permitiu uma abordagem mais ampla na exploração dos dados e aumentou o seu rigor científico.

Optou-se por adotar um questionário como instrumento de coleta de dados, subdividido em duas partes, contendo tanto questões abertas quanto fechadas. Conforme observado por Severino (2017), essa abordagem de questionário se mostra capaz de atender de forma abrangente aos diversos objetivos da pesquisa mista, ou seja:

> Podem ser questões fechadas ou questões abertas. No primeiro caso, as respostas serão escolhidas dentre as opções predefinidas pelo pesquisador; no segundo, o sujeito pode elaborar as respostas, com suas próprias palavras, a partir de sua elaboração pessoal (Severino, 2017, p. 140).

No roteiro do questionário aplicado, cuidadosamente alinhado com os objetivos da pesquisa, foram formuladas vinte e uma perguntas. Estas perguntas foram minuciosamente divididas em categorias de variáveis definidas e estruturadas com base nas fontes teóricas

adotadas no contexto da pesquisa, com ênfase especial na NBR ISO/IEC 27002:2022 (ABNT, 2022).

Nas questões fechadas, foi dada ênfase às principais ameaças e preocupações relacionadas à segurança da informação no uso dos sistemas, onde, conforme afirmado por Stake (2011, p. 111), "Os dados são transformados em totais, médias, porcentagens, comparações e correlações". Essas questões exploraram os elementos indicativos do comportamento e das atitudes dos participantes da pesquisa em relação às normas de segurança da informação em SIGAD, permitindo ao pesquisador identificar as principais circunstâncias de risco para os sistemas.

Foram incluídos itens de identificação para capturar as características dos respondentes, como ocupação, modalidade de trabalho, tempo de serviço e faixa etária. Isso permitiu traçar um perfil na análise das respostas.

As questões formuladas em formato aberto foram projetadas com o objetivo de proporcionar aos respondentes a oportunidade de expressar livremente suas percepções sobre os indicadores de falhas de segurança, bem como para receber sugestões relacionadas às boas práticas de segurança da informação, de acordo com a interpretação individual de cada participante. Essa abordagem viabilizou a condução de uma análise qualitativa da percepção dos respondentes colocando-os como pessoas ativas e reflexivas no processo de segurança da informação.

Para a aplicação e ajustes das questões elaboradas no questionário, foram realizados pré-testes, também conhecidos como pilotos, com a participação de dois servidores especialistas em TI da PU/SE. Esses servidores foram selecionados devido ao seu envolvimento com a temática e o problema de pesquisa em questão. Os profissionais envolvidos foram o Sr. Adilson José dos Santos[1], que ocupa o cargo de Gestão de Tecnologia da Informação na Coordenação Nacional de Soluções Tecnológicas (CONATEC), e o Sr. José Wanderclan Gonçalves Chaves[2], Analista de TI, que atua na Coordenação da Secretaria Judiciária (SEJUD) da PRU5.

O questionário utilizado foi elaborado utilizando uma escala do tipo *Likert* intervalar e foi enviado para o e-mail institucional dos participantes, acompanhado do Termo de Compromisso Livre e Esclarecido (TCLE), que pode ser encontrado no apêndice A da página 175. Esse envio foi feito na forma de um convite, que continha todas as informações relevantes sobre a pesquisa, bem como os direitos garantidos aos participantes. Ao concordar com o

[1] O nome do servidor Adilson José dos Santos foi citado com sua anuência prévia.
[2] O nome do servidor José Wanderclan Gonçalves Chaves foi mencionado com sua anuência prévia.

TCLE, o participante automaticamente obteve acesso para responder ao questionário, conforme íntegra disponibilizada no apêndice B (p. 179).

4.5 Método de análise de dados

Os indicadores qualitativos e quantitativos foram analisados de forma independente para facilitar a organização dos dados. A aplicação do questionário possibilitou uma análise final que integrou tanto a análise estatística quanto a textual, proporcionando assim um conjunto mais abrangente de *insights* e evidências. Essa estratégia de análise foi meticulosamente planejada para atingir e combinar eficazmente os objetivos da intervenção para gerar o produto técnico-científico.

A análise quantitativa envolveu a aplicação de uma análise estatística descritiva simples. Isso compreendeu a identificação de padrões de comportamento dos usuários e outras variáveis associadas aos riscos de segurança da informação no contexto das interações entre usuário, tecnologia e sistema. Os resultados das questões fechadas do questionário foram representados de forma gráfica para facilitar essa análise.

Conforme Fávero e Belfiore (2017), a estatística é uma técnica de análise de dados que tem sido empregada para interpretar e descrever os dados de maneira clara e compreensível. Esses autores afirmam que a estatística descritiva, ao representar graficamente o comportamento dos dados, está alinhada com os princípios fundamentais amplamente debatidos e definidos na hierarquia que conecta dados, informação e conhecimento. Nas palavras de Fávero e Belfiore (2017, p. 21): “A estatística descritiva descreve e sintetiza as características principais observadas em um conjunto de dados por meio de tabelas, gráficos e medidas-resumo, permitindo ao pesquisador melhor compreensão do comportamento dos dados”.

Nessa pesquisa, devido à abordagem mista adotada, a análise qualitativa foi realizada usando o método de análise de conteúdo proposto por Laurence Bardin (2011). Essa metodologia possibilitou o tratamento dos dados qualitativos por meio de uma técnica de análise categorial. A análise se fundamentou nas relações identificadas entre as variáveis, conforme percepções dos respondentes, resultando em uma análise descritiva dos resultados obtidos.

A utilização da análise de conteúdo de Bardin (2011) nesta pesquisa, voltada para a análise e interpretação das respostas abertas do questionário que envolveram dados textuais, justificou-se pela ampla aceitação desse método na pesquisa qualitativa. A aplicação das suas

etapas bem definidas possibilitou a identificação consistente de padrões e temas nos textos fornecidos pelos respondentes, reforçando assim a confiabilidade dos resultados desta pesquisa.

Conforme apontado por Bardin (2011), uma das vantagens da análise de conteúdo é a sua flexibilidade, que permite adaptações de acordo com o contexto da pesquisa. No Quadro 11, são apresentadas as diretrizes gerais que orientam as etapas desse processo, com base na adaptação de Bardin (2011):

Quadro 11 – Diretrizes gerais do processo de análise de conteúdo

	Etapa 1	Pré-análise	Definição de objetivos, seleção de material, escolha de unidades de análise, categorização e criação de sistema de codificação.
	Etapa 2	Exploração do material	Leitura completa do material, buscando entender o contexto e as características gerais do conteúdo. Isso ajuda a identificar tendências e temas recorrentes
	Etapa 3	Tratamento dos resultados, a inferência e a interpretação	Inicia-se a categorização do conteúdo, atribuindo códigos às partes do texto que se enquadram nas categorias de análise previamente definidas.
			Definição e categorização de análise conforme a compreensão do conteúdo avança, mantendo um registro claro das categorias
			Interpretação dos resultados em relação aos objetivos de pesquisa, identificando padrões, relações, diferenças e conclusões significativas no conteúdo
			Tratamento dos resultados dados codificados e criação de representações visuais das descobertas.

Fonte: Adaptado de Bardin (2011, p. 125-134).

Embora as etapas do processo pudessem apresentar variações sutis de acordo com o contexto específico, é fundamental reconhecer que os princípios gerais das etapas estabelecidas por Bardin (2011) desempenharam um papel fundamental como diretrizes essenciais do método.

4.6 Considerações éticas

As questões éticas que envolvem uma pesquisa partem de alguns princípios que normatizam a sua aplicação, assegurando assim, garantias éticas aos seus participantes. Por conseguinte, descrever-se-á a seguir os procedimentos éticos que serão aplicados para o desenvolvimento dessa pesquisa, os quais são padrão na submissão de pesquisas na área das Ciências Humanas e Sociais que envolvam seres humanos.

As pesquisas com seres humanos, conforme o item II.14 da Resolução CNS nº. 466 de 12 de dezembro de 2021, podem ser assim definidas:

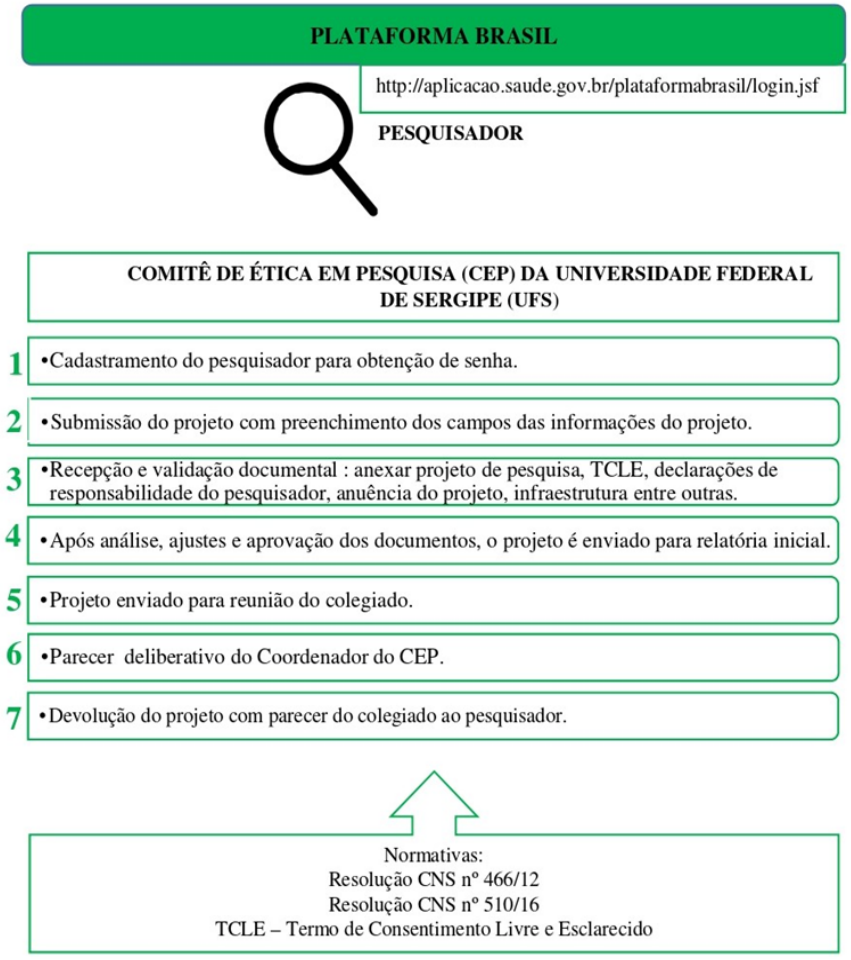
> Pesquisa que, individual ou coletivamente, tenha como participante o ser humano, em sua totalidade ou partes dele, e o envolva de forma direta ou indireta, incluindo o manejo de seus dados, informações ou materiais biológicos (Brasil, 2012).

O Comissão Nacional de Ética em Pesquisa (CONEP) e o CEP (Comitê de Ética em Pesquisa) constituem o Sistema CEP/CONEP, o qual possui caráter fiscalizador, consultivo e creditador das pesquisas com seres humanos, assim definido: “É um sistema descentralizado no qual os CEP possuem autonomia de análise ética, excetuando os protocolos das áreas temáticas especiais” (Brasil, 2017, p. 7).

Visando avaliar os aspectos éticos dessa pesquisa, as diretrizes e normas regulamentadoras a serem seguidas são fundamentadas pela CONEP, órgão de instância maior, o qual é representado em instâncias regionais, e o CEP/UFS, que é um representante regional entre outros CEP, distribuídos em todo o país (Brasil, 2020).

A título de esclarecimento, baseando-se nas orientações constantes na Plataforma Brasil, a figura 10 apresenta uma síntese do processo de tramitação de protocolos de pesquisa que envolvem seres humanos junto ao CEP. As sete etapas abaixo sequenciadas serão descritas com base nas orientações da Plataforma Brasil, disponibilizadas na Cartilha da CONEP (Brasil, 2017).

Figura 10 – Etapas do processo de tramitação de protocolos de pesquisa no CEP



Fonte: adaptado da Plataforma Brasil (Brasil, 2017).

O pesquisador deve, sob sua responsabilidade, realizar o seu cadastro na Plataforma Brasil, anexando os documentos pessoais de identificação e declarar ao CEP a instituição proponente, nacionalidade do estudo e, essencialmente, que a pesquisa envolve seres humanos.

Segundo dados da Plataforma Brasil, o pesquisador só consegue avançar no cadastramento do projeto se todas as informações obrigatórias dos campos estiverem preenchidas.

Posteriormente, deve-se informar a área temática do projeto seguida da tela dos dados referentes ao desenho da pesquisa, palavras-chave e dados do projeto de pesquisa que abrange: introdução, resumo, hipóteses (se houver), objetivos, critérios de inclusão e exclusão, métodos de análise de dados, tamanho da amostra. Alguns campos não são obrigatoriamente necessários para preencher.

Seguindo na explicação da figura 10, deverá ser anexado o projeto de pesquisa, o TCLE, declarações obrigatórias de responsabilidade de coleta dos dados não iniciada, ofício de encaminhamento à Coordenação do CEP, Termo de Autorização e Existência de Infraestrutura e outros documentos pertinentes para serem assinados pelo pesquisador e anexados em formato PDF (*Portable Document Forma*t). É obrigatório informar o sigilo da pesquisa e o prazo para a sua manutenção.

Após envio dos documentos, o pesquisador deverá acompanhar os trâmites do projeto na plataforma e ficar atento aos prazos das pendências para que o projeto possa ser analisado em reunião do colegiado.

Toda a comunicação de pendências e/ou parecer do CEP serão realizadas através da Plataforma Brasil.

O Sistema CEP/CONEP utiliza a Plataforma Brasil como plataforma de gestão virtual para registro, análise para monitoramento e tramitação eletrônica dos documentos referentes aos projetos de pesquisas que envolvam seres humanos, acompanhando desde a sua submissão à análise da possibilidade de creditamento como conclusão (Brasil, 2017).

Convém destacar que a importância do Sistema CEP/CONEP abrange, além da ética na pesquisa e proteção dos seus participantes, o acesso à informação dos projetos de pesquisa aprovados para a sociedade em geral.

Cabe ao pesquisador depositar o projeto para avaliação no Sistema CEP/CONEP, assumindo a responsabilidade de coordenar e realizar toda a pesquisa, acompanhando os seus trâmites através do acesso ao sistema na Plataforma Brasil até o parecer final do colegiado.

Em termos normativos no Brasil, as principais resoluções destinadas a disciplinar os princípios éticos das pesquisas que envolvem seres humanos são a Resolução nº 466, de 12

de dezembro de 2012, para todas as áreas, e a Resolução nº 510, de 7 de abril de 2016, que se destinam às pesquisas desenvolvidas nas áreas das Ciências Humanas e Sociais. Essas normas buscam assegurar os aspectos éticos e a proteção dos participantes quanto aos riscos e benefícios da pesquisa (Brasil, 2020).

Na UFS, a Portaria nº 444 de 17 de maio de 2022 "Cria Comitê de Ética em Pesquisa com Seres Humanos das Áreas de Ciências Humanas e Sociais Aplicadas (CEP-Humanidades) e nomeia membros". O CEP já possui um Regimento e está em fase de preparação para iniciar as atividades.

Conforme elencado acima, a resolução nº 510/2016 trouxe um reconhecimento para as pesquisas e os seus métodos no campo das Ciências Humanas e Sociais, levando-se em conta que não acontece intervenção direta com o corpo humano. No capítulo dos termos e definições da referida resolução, em seu art. art. 2.º, inciso XVI, apresenta definição do que seja pesquisa em Ciência Humanas e Sociais, a saber:

> Pesquisa em ciências humanas e sociais: aquelas que se voltam para o conhecimento, compreensão das condições, existência, vivência e saberes das pessoas e dos grupos, em suas relações sociais, institucionais, seus valores culturais, suas ordenações históricas e políticas e suas formas de subjetividade e comunicação, de forma direta ou indireta, incluindo as modalidades de pesquisa que envolvam intervenção (Brasil, 2016).

Em termos de princípios éticos das pesquisas no campo das Ciências Humanas e Sociais, a resolução nº 510/2016 está pautada no reconhecimento da liberdade e autonomia para todos os envolvidos no processo da pesquisa, exaltando o respeito aos valores culturais, sociais, morais e religiosos, democracia, confidencialidade das informações, compromisso quanto à segurança das informações obtidas, garantia de não exposição de riscos ou vulnerabilidade individual ou coletiva, excluindo o estigma de preconceito ou descriminação.

Torna-se pertinente trazer a discussão apresentada por Guerriero e Minayo (2019) com relação as principais diferenças entre a resolução 466/2012 e 510/2016. Para os autores, as duas resoluções apresentam conjunto comum de normas que amparam a ética nas pesquisas em seus aspectos sociais, políticos, econômicos e culturais, contudo, identificam seis mudanças que a Resolução nº 510/2016 traz em relação à nº 466/2012, a saber:

> Definição do que não precisa ser avaliado pelo Sistema CEP/Conep; discernimento entre processo e registro de consentimento e assentimento livre e esclarecido; avaliação de mérito científico; explicitação das etapas que antecedem ao projeto completo; relação entre a Resolução nº 510 e a 466; e composição do Sistema CEP/Conep (Guerriero; Minayo, 2019, p. 305).

Segundo a norma, pesquisas de opinião pública, censitária, informações do domínio público, banco de dados, revisão de literatura, pesquisa reflexiva para aprofundamento teórico

de assuntos são exemplos de pesquisas que não necessitam de autorização do CEP (Brasil, 2016).

Com relação ao discernimento entre processo e registro de consentimento e assentimento livre e esclarecido, Guerriero e Minayo (2019) destacam que a resolução vem legitimar diversas formas de registro, seja escrito, sonoro, imagético entre outros. Conforme suas interpretações, os autores ressaltam que, em sua redação, a resolução substituiu a palavre "termo" por "registro" para compor o Consentimento Livre e Esclarecido, contemplando as especificidades das pesquisas das Ciências Humanas e Sociais.

Validando as alegações das autoras, essas mudanças estão descritas na Seção II, art. 15 da Resolução 510/2016, em seu capítulo III, do Processo de Consentimento e do Assentimento Livre e Esclarecido:

> O Registro do Consentimento e do Assentimento é o meio pelo qual é explicitado o consentimento livre e esclarecido do participante ou de seu responsável legal, sob a forma escrita, sonora, imagética, ou em outras formas que atendam às características da pesquisa e dos participantes, devendo conter informações em linguagem clara e de fácil entendimento para o suficiente esclarecimento sobre a pesquisa (Brasil, 2016).

Outro ponto essencial relacionado entre a Resolução nº. 466/2012 e a Resolução nº 510/2016 consiste no texto das disposições finais desta segunda, conforme o disposto em seu art. 32 e em seu parágrafo único, consta que nas situações não contempladas em seu teor, deve-se prevalecer os princípios éticos da primeira (Brasil, 2016).

Em termos de considerações éticas, essa pesquisa deverá seguir todos os princípios éticos das pesquisas que envolvem seres humanos, direcionada para a área das Ciências Sociais e Humanas, principalmente por ter um objetivo direcionado a análise de comportamento de usuários de sistemas com ênfase na observação prática e na percepção dos usuários quanto à segurança da informação.

Os principais instrumentos normativos e legais para proteger os direitos dos participantes da pesquisa serão embasados pelo Sistema CEP/CONEP, de acordo com a Resolução CNS/MS nº. 466/2012, a Resolução CNS/MS nº 510/2016, a Norma Operacional CNS nº 001/2013 e a Carta Circular nº 001/2021 - CONEP/SECNS/MS, de 3 de março de 2021, que trata sobre orientações para procedimentos em pesquisas com qualquer etapa em ambiente virtual, de modo a proporcionar todas as garantias éticas aos participantes da pesquisa.

Na observância do cumprimento das regras, o projeto de pesquisa foi submetido ao CEP da Universidade Federal de Sergipe por meio da Plataforma Brasil, em 1 de novembro de 2022, conforme comprovante de envio do projeto (Anexo, p. 133), com a autorização prévia da organização em que a intervenção será realizada e com o TCLE elaborado em concordância

com o roteiro sugerido pelas Resoluções do CNS/MS nº 466/2012 e nº 510/2016 e também conforme as recomendações da Carta Circular nº 001/2021- CONEP/SECNS/MS, que será apesentado, após a sua a aprovação pelo CEP/UFS, aos convidados a participar da pesquisa, informando-os devidamente sobre os detalhes do estudo, possíveis riscos, contribuições, além das questões éticas e dos seus direitos.

5 DIAGNÓSTICO ORGANIZACIONAL POR ANÁLISE SWOT DA PU/SE – AGU

O diagnóstico da PU/SE teve a finalidade de caracterizar o ambiente e apresentar uma análise do seu desempenho organizacional, identificando principalmente as forças, fraquezas, oportunidades e ameaças que existem naquele ambiente para fins de intervenção, apresentando o seu valor público para a sociedade.

Para que o diagnóstico possa ser elaborado é necessária uma análise ambiental da organização, voltada para os impactos dos ambientes internos e externos, pois somente assim se pode ter um panorama mais completo e o seu monitoramento estratégico (Sobral; Peci, 2013). Para os autores, o termo ambiente organizacional pode ser entendido como: "Conjunto de forças, tendências e instituições, tanto externas como internas à organização, que têm potencial para influenciar seu desempenho" (Sobral; Peci, 2013, p. 104).

Buscando identificar os fatores internos e externos que possam influenciar nas questões relacionadas ao desempenho organizacional da PU/SE, foi realizado um mapeamento do seu ambiente, respaldado na análise apresentada pelo Relatório de Gestão da AGU 2021 (Brasil, 2021).

Como ambiente interno está a AGU, organização hierarquicamente superior a PU/SE, e como ambiente externo, estão os órgãos governamentais dos três poderes da União, relacionando-se diretamente e operacionalmente com o órgão. O ambiente externo está configurado como ambiente independente e sem conexão direta com a instituição, porém as suas variáveis afetam diretamente o ambiente interno.

Retornando a Sobral e Peci (2013), eles explicam que para melhor compreender as diferentes influências da ambiência, o gestor deve ter uma visão equalizadora dos dois ambientes procurando equilibrar e estabilizar suas interações. Esses mesmos autores assim o definem:

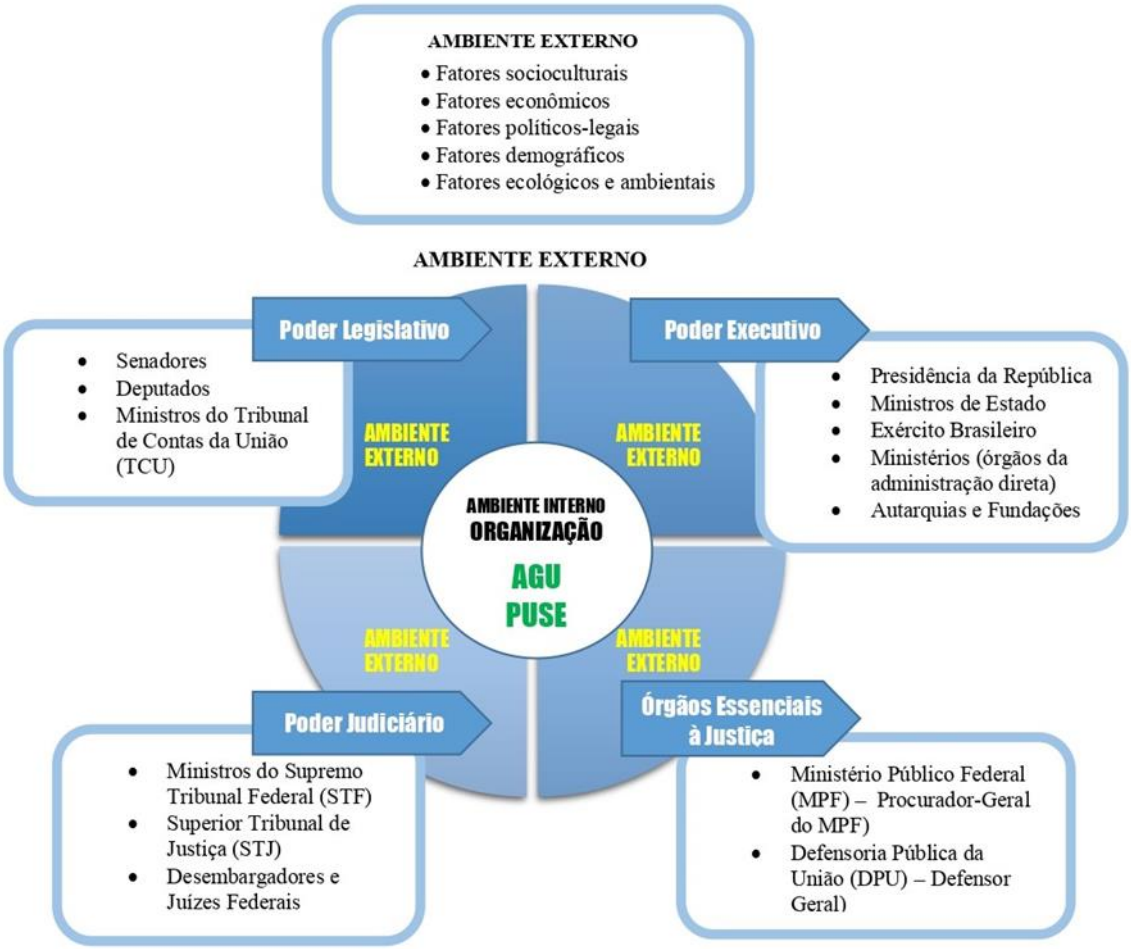
> O ambiente interno é composto pelos elementos internos da organização, como sua força de trabalho, gestores, cultura organizacional, tecnologia, estrutura organizacional, instalações físicas, entre outros. Esses elementos influenciam a adequação da organização ao ambiente externo e, consequentemente, seu desempenho organizacional (Sobral; Peci, 2013, p. 104).

No tocante ao ambiente externo, os autores explicam os elementos que existem fora da organização, mas necessários para sua operacionalização, incluindo "forças, atores e instituições que podem influenciar de forma positiva ou negativa o desempenho da organização" (Sobral; Peci, 2013, p. 104).

Sobral e Peci (2013) ressaltam o ambiente contextual como um substrato do ambiente externo, o qual envolve fatores que estão fora do controle e dos limites da organização, ou seja, estão inseridos em um contexto que a organização precisa enfrentar e superar porque engloba condições que independem da sua ação.

Na análise ambiental da PU/SE desenvolvida nessa pesquisa foi evidenciada, principalmente a área da TI, segurança da informação e usuários dos sistemas. O panorama do ambiente da PU/SE pode ser melhor descrito na figura 11.

Figura 11 – Panorama do ambiente da PU/SE



Fonte: Adaptado do Relatório de Gestão da AGU (2021, p. 27).

Conforme a figura, tem-se como ambiente interno, a AGU, organização que possui a missão de representar judicial e extrajudicialmente os três poderes da União e assessorar juridicamente o Poder Executivo Federal (Brasil, 2021).

Conforme preconiza a Carta Magna da instituição, a representação judicial e extrajudicial da União está voltada para os poderes executivo, legislativo e judiciário, devendo desempenhar a representação judicial diretamente ou por meio das suas unidades descentralizadas nos Estados (Brasil, 1988).

A PU/SE, ambiente social da pesquisa, compõe o ambiente interno da organização e está subordinada hierarquicamente pela PRU5, em Pernambuco, que tem como direção superior a PGU, localizada em Brasília, cuja função está preconizada pelo art. 9º da Lei Complementar nº 73, de 10 de fevereiro de 1993: "representar a União junto ao Poder Judiciário nas suas diferentes instâncias, com exceção do STF" (Brasil, 1993).

Sendo responsável pela representação judicial da Administração Direta da União, que abrange os três Poderes da República e as funções essenciais à Justiça, a PU/SE atua junto às diversas instâncias do Poder Judiciário, bem como o contencioso internacional, ressalvada a matéria tributária e fiscal (Brasil, 1993).

A força de trabalho da PU/SE é composta por Advogados da União, membros da carreira jurídica, a qual foi estruturada pela Lei nº 9.028, de 12 de abril de 1995, atualizada pela Lei 13.327, de 29 de julho de 2016. O quadro de servidores técnico-administrativos é composto por servidores efetivos e redistribuídos para a AGU através da Lei nº 10.480, de 2 de julho de 2002 e servidores requisitados de diferentes órgãos do Poder Executivo em força de cessão, por tempo indeterminado, conforme Lei Complementar nº 73, de 10 de fevereiro de 1993. Constam ainda os prestadores de serviços terceirizados e estagiários.

Evidente que a pretensão de se realizar um diagnóstico em uma organização que representa a União em todo o território nacional requer uma análise mais profunda e ampla do seu ambiente interno e externo. Nas próximas subseções apresentar-se-á um recorte setorial da PU/SE, voltado para o problema da pesquisa, intenção desse estudo em desenvolvimento.

5.1 Caracterização do ambiente interno

Em análise ao ambiente interno da AGU, identificou-se que o seu planejamento estratégico estabeleceu as diretrizes e metas para o plano de gestão e governança do órgão e suas unidades descentralizadas, entre elas a PU/SE, sendo aprovado pelo Comitê de Governança daquele órgão, "com a finalidade de estabelecer a governança corporativa, integridade, riscos e controles, bem como auxiliar o Advogado-Geral da União nas decisões de caráter estratégico" (Brasil, 2022).

O planejamento estratégico é desenvolvido por meio de debates aprofundados e consideração de diversas perspectivas sobre questões relevantes dentro da instituição. Esse processo é altamente colaborativo, fundamentado nas contribuições de seus membros e nas reflexões que resultam na formulação de diretrizes estratégicas sólidas.

Tendo como visão ser reconhecido como função essencial à Justiça Brasileira, a AGU tem como missão “promover a proteção jurídica do Estado Brasileiro em benefício da sociedade” (Brasil, 2022) com metas voltadas para resultados institucionais, governança e inovação.

De forma mais direta, a AGU busca aumentar as decisões judiciais favoráveis à União, suas autarquias e fundações públicas federais, otimizando recursos e defendendo os interesses do Estado. Além disso, promove a resolução de conflitos por meio de mediação e negociação, visando a justiça ágil e eficaz.

Em termos numéricos, de acordo com os dados divulgados no Relatório de Gestão de 2021 da AGU, no ano de 2021, a AGU contribuiu para os cofres públicos revertendo um montante de R$ 761 bilhões. Além disso, obteve uma taxa de sucesso judicial de 62,6% em relação aos 14,8 milhões de processos movidos contra a União que foram executados.

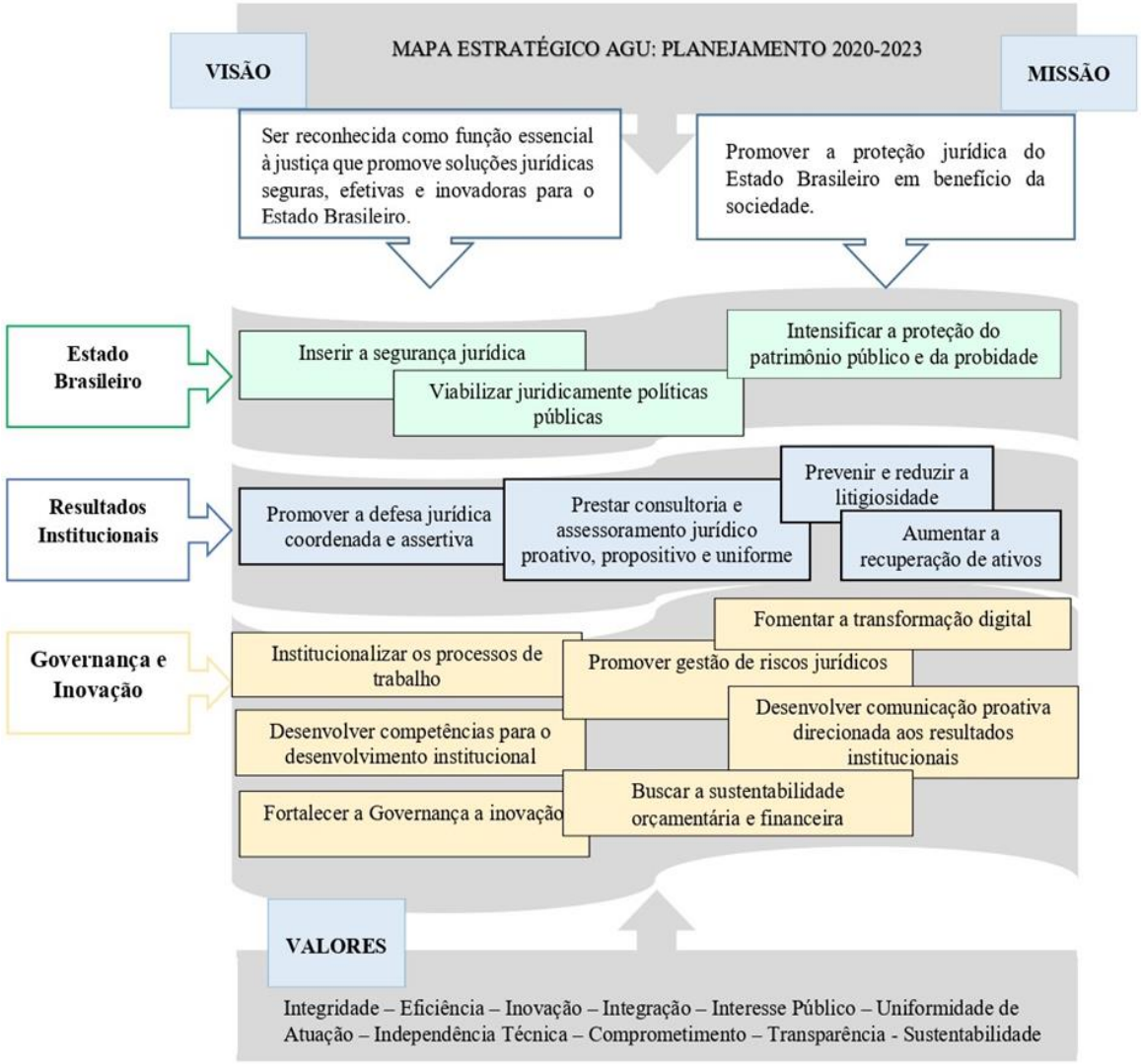
A AGU atribui seu êxito financeiro em 2021 a uma abordagem inovadora e decisiva na resolução de casos, além da utilização eficaz de tecnologia, incluindo o sistema SAPIENS 2.0. Esse sucesso é previsto para ter um impacto benéfico nos investimentos em recursos públicos, permitindo direcioná-los para impulsionar o desenvolvimento econômico e a geração de renda no país (Brasil, 2021).

Dentro do mapa estratégico da AGU, suas metas são abrangentes e abordam não apenas o aumento da taxa de sucesso judicial, mas também áreas-chave como gestão estratégica e jurídica, comunicação organizacional, competência institucional e inovação, que são campos explorados pela área da CI. Além disso, a governança inclui ações voltadas para o fomento da transformação digital, demonstrando um compromisso com a modernização e eficiência dos processos internos e externos da organização.

Dentro da PU/SE, em conformidade com as diretrizes estabelecidas pela PGU, a mais alta instância hierárquica, a questão da transformação digital é enfatizada, especialmente com a meta de alcançar nos próximos anos um índice de 99% de integração com os sistemas do Poder Judiciário. Atualmente, conforme informações fornecidas pelo órgão, esse percentual está em 75% (Brasil, 2022). Essa meta expressa um compromisso sólido com a modernização e eficiência na gestão de processos e informações jurídicas para melhorar a qualidade e acessibilidade dos serviços.

Institucionalmente, a PU/SE assim como todas as unidades da AGU, segue o mapa estratégico do planeamento 2020-2023 (Brasil, 2020), observando os valores e missão estabelecidos (Figura 12).

Figura 12 – Mapa estratégico AGU: planejamento 2020-2023



Fonte: Adaptado do site da AGU (Brasil, 2020) disponível em: https://www.gov.br/agu/pt-br/governanca/planejamento-estrategico/planejamento-estrategico-2020-2023. Acesso em: 12 jul. 2022.

Como instrumento para nortear e acompanhar as práticas da área da Tecnologia de Informação (TI), a PU/SE segue as determinações superiores do DTI da AGU e são monitoradas pelo Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal, que objetiva:

> O planejamento, a coordenação, a organização, a operação, o controle e a supervisão dos recursos de tecnologia da informação dos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, em articulação com os demais sistemas utilizados direta ou indiretamente na gestão da informação pública federal (Brasil, 2011).

Como acompanhamento do desempenho das TIC dos órgãos integrantes, o SISP estabelece a avaliação, direção e monitoramento pelo Plano Diretor de Tecnologia da Informação (PDTIC), elaborado com base na Instrução Normativa STI/MP nº 04/2014, definido em seu artigo 2º, XXVII (Brasil, 2014), como: “Instrumento de diagnóstico, planejamento e

gestão dos recursos e processos de tecnologia da informação que visa atender às necessidades tecnológicas e de informação de um órgão ou entidade para um determinado período".

As principais atribuições e indicadores institucionais do planejamento, conforme estabelecidos pelo PDTIC da AGU e elaborados pelo Comitê de Tecnologia da Informação (CTI) referente ao triênio 2021 a 2023, podem ser encontrados no quadro 12 para referência e acompanhamento.

Quadro 12 – Atribuições institucionais do planejamento dos macroprocessos estabelecidos pelo PDTIC

Macroprocesso de Trabalho	Descrição	Objetivo
Aprimorar os serviços de TIC	Índice de satisfação do usuário.	Medir o percentual de satisfação por meio de pesquisa de satisfação da DTI.
Planejar as necessidades estruturantes	Serviços técnicos especializados para manutenção de equipamentos e operação de centro de dados, segurança da informação e suporte técnico ao usuário.	Garantir que os usuários de TI da AGU sejam plenamente atendidos quando da necessidade eventual de suporte técnico para equipamentos e sistemas corporativos da AGU
Equipamentos para estações de trabalho	Contemplam desktops e notebooks para atuação dos servidores, tanto das áreas meio, quanto das áreas finalísticas da AGU.	Garantir a disponibilidade de estações de trabalho nas unidades da AGU e equipamentos móveis em razão das necessidades dos usuários. Se necessário, distribuir ou redistribuir equipamentos entre Unidades Administrativas e usuários
Equipamentos e acessórios de TIC	Contemplam equipamentos e acessórios de TIC, como: Impressoras, *Scanners*, *RoundTable*s, Roteadores *Wifi*, Monitores e outros.	Garantir a disponibilidade de equipamentos e acessórios de TIC nas unidades e equipamentos móveis para os usuários.
Funcionalidades relacionadas ao SAPIENS e demais sistemas corporativos	Representam os módulos, subsistemas, relatórios, integrações e funcionalidades relacionadas aos SAPIENS e outros sistemas da AGU.	Sistema de chamados para os itens de logística (como já ocorre com TI), possibilitando que os usuários solicitem e acompanhem o andamento de serviços de manutenção, pedidos de bens patrimoniais e demais itens pertinentes ao dia a dia de atendimento nas unidades.
Necessidade Pessoal	As necessidades de pessoal tratam dos recursos humanos necessários para que os serviços de TI estejam disponíveis para todos os usuários da rede AGU.	Adequar a equipe de servidores de acordo com a necessidade da DTI.
Capacitação	Eventos formais ou informais de capacitação técnica ou administrativa de servidores	Capacitar servidores em acordo com o plano de capacitação e as necessidades da DTI.
Equipe de apoio a gestão TI	Profissionais com expertise em gerenciamento de projetos e execução de contratos de TI.	Planejamento e contratação de equipe de profissionais terceirizados para apoio à gestão de projetos de TI.

Fonte: Adaptado do PDTIC AGU (Brasil, 2020).

O PDTIC é elaborado pelo DTI da AGU e revisado a cada três anos, estruturado em macroprocessos, os quais abarcam planejamento quanto da gestão de contratação, estratégia e projetos de TIC, gestão de aquisição e obtenção de TIC, processo de sustentação de sistemas, gestão de armazenamentos de dados, serviços de nuvem e domínio de rede, gestão de incidentes computacionais e processo de suporte técnico aos usuários.

As atribuições institucionais planejadas pelo Diretor do PDIC, conforme apresentadas no quadro acima, consistem em recomendações e diretrizes para o controle organizacional em todas as PUs no âmbito dos Estados. Essa orientação é centralizada no DTI na sede da AGU em Brasília, que também oferece suporte técnico terceirizado em suas unidades regionais e estaduais.

Os treinamentos de utilização do sistema são promovidos de forma remota e não existe assistência setorial quanto às dúvidas de utilização do Sistema SAPIENS e nem aos seus desdobramentos de integração. O suporte técnico é oferecido por meio de abertura de chamados técnicos e, se o trabalho for remoto, faz-se necessário que o servidor leve o equipamento para supervisão e suporte por parte dos técnicos contratados.

Outro fator de suma preocupação é a inexistência de suporte de apoio aos usuários quanto a utilização do sistema SAPIENS e sistemas afins, o que justifica mais ainda a importância dessa pesquisa em curso, porque o PDTIC tem as suas metas voltadas para a segurança do sistema e suporte técnico, faltando incluir em seu escopo a identificação junto aos usuários dos sistemas as possíveis fragilidades identificadas em suas percepções e passíveis de incidentes que tragam riscos para a segurança da informação.

Para evidenciar mais ainda essas questões de transformação digital, muito antes da pandemia da COVID-19, a AGU já praticava a integração de sistemas e o uso da inteligência artificial através do SAPIENS, facilitando ainda mais o uso de plataformas digitais.

O SAPIENS, já discutido anteriormente, é um SIGAD que permite a integração com diversas bases de dados de outras instituições, o que otimiza em tempo os subsídios encaminhados para defesa da União, refletindo no cumprimento dos prazos judiciais e em economia de recursos humanos (Brasil, 2018).

Em sua funcionalidade, o DTI explica que o SAPIENS possui função de produzir, processar e prover o acesso à informação proveniente de fontes internas e externas para apoiar todo o processo de gerenciamento eletrônico da informação jurídica, incluindo informações estruturadas e não estruturadas (Brasil, 2018).

Conforme o DTI, as informações estruturadas são produzidas dentro do sistema SAPIENS, enquanto as informações não estruturadas são aquelas armazenadas em banco de dados, a saber: E-mails, arquivo de texto, imagem ou som, planilhas entre outras (Brasil, 2018).

Considerando-se a importância do Sistema SAPIENS para essa pesquisa, que vai explorar principalmente o comportamento dos seus usuários, apresentamos as principais funcionalidades da versão 1.3.2, a mais atualizada no momento, para entendimento do seu domínio (Quadro 13).

Quadro 13 – Principais funcionalidades do SAPIENS por área de atuação organizacional

Área	Funcionalidade
Administrativa	Gravar as redistribuições em um objeto estruturado que permita a geração de relatórios mais avançados de redistribuição
	Alterar nomenclatura filtro de destinatários nas comunicações para comuns e conveniados
	Nova sistemática para a gestão do afastamento, passando a considerar o dia corrente
	Novo algoritmo para distribuição automática e balanceamento de carga
	Geração automatizada da Folha de Registro de Atividades dos membros
	Ferramenta para alterar o prazo de comunicação em bloco
	Nova sistemática para noticiar o sucesso ou erro das operações, não havendo mais janelas de sucesso
	Na pesquisa de documento o ano da consulta deve ser selecionado, para melhorar a velocidade
Judicial	Ferramenta de análise automatizada de litispendência, com geração de certidão no Número Único de Protocolo (NUP)
	Coluna origem dados do NUP no painel de tarefas
	Possibilidade de ressincronizar prazo de intimações de integração, para atualizar o prazo
	Permitir lançamento em bloco de atividade comum em NUPs com e sem integração simultaneamente
Consultivo	Controlar a tramitação na ferramenta submeter a aprovação
Assinador de documentos	Novo assinador digital opcional utilizando *java web start*, devendo ser ativado pelo usuário nas configurações
Arquivista	Coluna destinação da classificação
	Histórico no lembrete do arquivista
Integração e tarefa	Retornar o sequencial da juntada em que a resposta de comunicação foi armazenada
	Consulta de usuário externo do INSS previamente autorizado pela NUP, sem a exigência da chave de acesso

Fonte: Adaptado do DTI/AGU (2018).

Na caracterização do ambiente dessa pesquisa, procurou-se evidenciar as principais questões voltadas para a área da TI e do SAPIENS, como principal sistema de gestão de informação jurídica, com normas estabelecidas pelas ordenanças centralizadas pela AGU em Brasília.

Importa esclarecer que no âmbito da AGU e da PU/SE existem outros sistemas corporativos, que não são gerenciais, sendo utilizados para diferentes fins, mas que merecem realce, a saber: Sistema de Concessão de Diárias e Passagens (SCDP), Sistema de Gestão de

Convênios (SISCON), Sistema de Cálculos e Perícias da AGU (SICAP), Consulta Pagamentos Judiciais - Precatórios e RPV (PAGJUDICIAIS), Consulta a Cadastro de Notas e Pareceres (NOTAPAR), Sistema de Gerenciamento de Projetos (GPWEB), Sistema de Gestão de Recolhimento da União (SISGRU) para emitir Guia de Recolhimento da União (GRU), Sistema de Ouvidoria (AGUOUVIDORIA), entre outros.

Ao finalizar-se o diagnóstico do ambiente da pesquisa foi possível realizar uma análise mais analítica da PU/SE como organização que representa a União no Estado de Sergipe, descrevendo e identificando suas governanças com destaque para a área de tecnologia.

5.2 Caracterização do ambiente externo

Conforme a gestão estratégica da AGU (Brasil, 2021), o ambiente externo corresponde aos órgãos e autoridades que são representados judicialmente e/ou extrajudicialmente à instituição, ou a ela vinculados.

Evidente que mesmo ao se descrever a análise do ambiente da PU/SE torna-se basilar explicar nos parágrafos dessa discussão que a AGU é uma organização hierarquicamente superior àquela Procuradoria, de onde as decisões de gestão e atribuições institucionais são emanadas e regulam todas as suas unidades.

O ambiente externo da PU/SE é dinâmico e possui diferentes funções sociais e judiciais que estão voltadas para a defesa do interesse da União. Dessa maneira, pode-se afirmar que o principal ativo operacional da PU/SE é a informação jurídica e dela são realizadas as defesas e as resoluções dos litígios.

Mello, Brito e Martínez-Ávila (2022) explicam que na seara jurídica se trabalha com dois elementos essenciais que correm em vias paralelas: informar e ser informado. Para a PU/SE, a colocação das autoras pode ser resumida pelo binômio: informação jurídica e o prazo judicial a ser cumprido.

Chaves, Albuquerque, Farias e Guerra (2022) reforçam que dentro do ambiente jurídico existe uma constante modernização e renovação de sistemas de informação, os quais perpassam por todos os processos informacionais com o intuito de repercutir na melhoria das atividades e seus fluxos. Para os autores, está intrínseco no contexto organizacional a comunicação da informação entre os seus setores internos e entre organizações.

Para Cardoso (2018) a estrutura organizacional da AGU e sua ampla comunicação com órgãos e autoridades por ela representada tem se desenvolvido de maneira muito próxima. Somam-se aos motivos que estreitaram as relações entre as instituições, os fatores de efeito

jurídico, os avanços tecnológicos, inovações e os processos de automação da informação jurídica, superando as barreiras geográficas.

A ação contenciosa da PU/SE se dá por meio do assessoramento e orientação jurídica entre os dirigentes do Poder Executivo Federal. Sua representação judicial é exercida por meio de defesa das ações judiciais figurando como autora, ré ou, ainda, terceira interessada. Extrajudicialmente, representa entidades não vinculadas à justiça, como órgãos administrativos da própria União, Estados ou Municípios (Cardoso, 2018).

Em termos de solicitação de subsídios, a Lei nº 9.028, de 12 de abril de 1995, suscita a responsabilidade dos órgãos em fornecer as respostas das demandas, com tratamento preferencial e em cumprimento aos prazos estabelecidos. Segundo o disposto do seu artigo 4º:

> Na defesa dos direitos ou interesses da União, os órgãos ou entidades da Administração Federal fornecerão os elementos de fato, de direito e outros necessários à atuação dos membros da AGU, inclusive nas hipóteses de mandado de segurança, habeas data e habeas corpus impetrados contra ato ou omissão de autoridade federal (Brasil, 1995).

A comunicação com a sociedade acontece por meio da Assessoria Especial de Comunicação Social (ASCOM), que divulga as atribuições da instituição para a sociedade e amplia a sua visibilidade, sendo todas as demandas de imprensa realizadas através de e-mail institucional e os atendimentos da ouvidoria são disponibilizados por meio do *link* no site da AGU (Brasil, 2021).

Em relação as mídias digitais, no ano de 2021 foi alcançada uma marca de 1 milhão de seguidores nas redes sociais da AGU, presente no *Linkedin*, *Instagram*, *Spotify*, *Youtube.* Esse engajamento pode ter sido intensificado com o acesso das mídias digitais verificado no período de isolamento da pandemia da COVID-19 (Brasil, 2021).

Junto ao engajamento das redes sociais da AGU passou a existir uma preocupação por parte da instituição quanto aos seus conteúdos e postagens, principalmente no que tange o risco à imagem da função pública ou da instituição (Brasil, 2021).

À visto disso, a AGU estabeleceu as diretrizes para políticas de uso e convivência pela Portaria nº 124, de 28 de março de 2012, no âmbito da AGU, para normatizar o uso e publicação dos conteúdos institucionais nos seus sítios de Internet, Intranet e redes sociais, a qual prevê em seu art. 2º: “O sítio da Internet, de acesso público, www.agu.gov.br, destina-se à veiculação de conteúdos de caráter institucional precipuamente voltados ao público externo da AGU” (Brasil, 2012).

A Portaria nº 124/2012 está embasada em princípios de conduta dos membros, servidores e colaboradores nas mídias sociais, observando: responsabilidade e observância dos

direitos autorais, garantias à privacidade e intimidade, transparência, ética e legalidade, sendo dever guardar o decoro pessoal e a conduta pública, moralidade administrativa, boa convivência, entre outros (Brasil, 2012).

Andrade (2016) identifica diversos canais de comunicação institucional da AGU, incluindo o AGU Brasil na TV Justiça, um programa de rádio na Rádio Justiça disponível em mais de dez mil emissoras via satélite por meio da Empresa Brasil de Comunicação (EBC), o site institucional, YouTube, Facebook e a publicação Panorama AGU. A autora enfatiza o papel crucial desempenhado pela ASCOM na disseminação da importância da AGU para o cidadão e a sociedade.

Destacam-se também as reuniões institucionais, consultivas e as audiências judiciais, presenciais ou remotas, que permitem um contato direto e contínuo de assessoramento e representação judicial junto aos tribunais de justiça e órgãos de vinculação direta e operacional com a PU/SE.

Na concepção do ambiente externo contextual, os anos de 2020 e 2021 foram atípicos em função da pandemia global da COVID-19. Na PU/SE não foi diferente: implantação do trabalho remoto e da desterritorialização, a realização de reuniões e audiências remotas foram as principais adequações que aprimoraram as relações institucionais virtuais (Brasil, 2021).

Sobre esse fato, houve impactos no ambiente interno e externo na mesma medida, conforme citado no Relatório de Gestão da AGU 2021-2023:

> O contexto da pandemia global de Covid-19 apresentou grandes desafios para a AGU, tanto do ponto de vista interno, com foco nas adaptações ao trabalho remoto e nas dinâmicas necessárias para adequação ao cenário, quanto do ponto de vista externo, refletindo na sua atuação finalística (Brasil, 2021).

O regime de jornada de trabalho remoto, de forma excepcional e temporário, foi aplicado para os membros, servidores, empregados públicos, estagiários e prestadores de serviços terceirizados na AGU através da Portaria nº 84, de 17 de março de 2020, como medida de proteção para o enfrentamento do novo coronavírus.

Com a retomada gradativa das atribuições, através da Portaria Normativa nº 17, de 16 de julho de 2021, a SGA (SGA/AGU) instituiu o Programa de Gestão e a adoção dos regimes presencial, semipresencial e teletrabalho, referente à atuação profissional dos servidores técnico-administrativos e a Portaria Normativa nº 3, de 28 de janeiro de 2021, relativa ao exercício dos membros de carreiras jurídicas da AGU. As duas portarias igualmente indicam a instituição dos regimes de trabalho acima citados.

A Portaria Normativa nº 17/2021, em seu Art. 15, estabelece três modalidades de desenvolvimento do Programa de Gestão com diferentes critérios de adesão pré-estabelecidos, e em vigor a partir de 5 de setembro de 2022, a saber:

> I - teletrabalho: o cumprimento da jornada de trabalho ocorre externamente às dependências físicas da UP, sem prejuízo de periódica ou eventual convocação para realização de atividade em caráter presencial;
> II - semipresencial: o cumprimento da jornada de trabalho ocorre de forma mista, externa ou internamente às dependências físicas da UP, de acordo com o que estabelecido no PEE e no PPI; e
> III - presencial: o cumprimento da jornada de trabalho ocorre nas dependências físicas da UP (Brasil, 2021).

Outra grande mudança na estrutura organizacional, dentro desse contexto pandêmico, foi a desterritorialização adotada através da Portaria nº 26, de 14 de outubro de 2020, como plano de governança da PGU.

A desterritorialização na AGU foi estabelecida para todos os membros e objetivou equalizar o volume de trabalho, sem alterar a lotação dos servidores administrativos e Advogados da União, embora estejam sob a coordenação das Procuradorias-Regionais no âmbito dos seus territórios de atuação. Entre os seus objetivos, salienta-se a uniformização dos atendimentos, a equalização do volume de trabalho e promoção da defesa coordenada da União (Brasil, 2020).

Nas lentes da CI, pode-se destacar o objetivo do art. 4º, inciso VIII da Portaria nº 26/2020: "a valorização da gestão do conhecimento, com disponibilização, em ambientes digitais, das orientações, informações e documentos necessários às atividades" (Brasil, 2020).

Em associação ao texto supracitado, identifica-se a preocupação da organização como os processos de GD e GC, o que na prática se observa com o gerenciamento do fluxo documental no SAPIENS, o sumário de conhecimento com modelos de petições e outras peças de embasamento jurídico, elaborados por seu corpo jurídico e formalizados no sistema para compartilhamento e os modelos de documentos oficiais classificados por assunto e área temática.

Enfatiza-se que o sítio tecnológico da AGU e os processos de inovação já vinham em pleno desenvolvimento muito antes da pandemia global no ano de 2020. As transformações tecnológicas promoveram a digitalização de documentos e dossiês, os processos judiciais eletrônicos, os sistemas de GED e SIGAD entre outros que foram implantados.

Com base nesses fatores acima relacionados, iniciativas realizadas pela AGU nos anos de 2016 e 2018, anteciparam a desterrritorialização, trazendo a melhoria e acertos para novas experiências, conforme justifica o Procurador-Geral da União, Vinicius Torquetti

Domingos Rocha (2020), em consulta pública encaminhada aos membros e servidores da AGU sobre a minuta de portaria que promove a governança da PGU:

> Lembramos que a desterritorialização de nossa atuação não é uma novidade. As Equipes Virtuais de Alto Desempenho – E-QUADs foram instituídas em fevereiro de 2016 pela Portaria PGU nº 01/2016. Temos, também, experiências com a estadualização nos estados de Santa Catarina, Paraná e Rio Grande do Sul, além de diversas equipes de trabalho desterritorializado, autorizadas pela Portaria PGU nº 02/2018. Todas essas experiências nos permitiram, no decorrer dos anos, identificar acertos e pontos passíveis de melhorias dessas iniciativas (Rocha, 2020, p. 10).

Em termos operacionais, a pandemia da COVID-19 trouxe alguns resultados marcantes quanto as ações judiciais. Houve um aumento de ações sobre o auxílio emergencial, o equivalente a 20% do total de processos judiciais no ano de 2021 (Brasil, 2021).

Destaca-se ainda, o aumento do assessoramento específico devido à pandemia da COVID-19, classificadas como prioridade judicial, e outras ações de tutela antecipada que versavam sobre a pandemia e a disponibilidade de leitos de Unidades de Terapia Intensiva (UTI) e sobre o Plano Nacional de Imunização (PNI). Citando-se ainda, as demandas de atuação conjunta da AGU com o Ministério da Saúde para conciliação dos litígios (Brasil, 2021).

Em prática, vislumbra-se na desterritorialização, o compartilhamento e a disseminação de informações, a formalização de orientações baseadas no conhecimento dos seus membros e a inovação da gestão pública, com acesso em ambiente digitais de diferentes unidades da AGU, o que antes não era plausível porque o conhecimento era retido nas unidades e setores físicos.

Para promover o diagnóstico e possíveis soluções direcionadas ao problema dessa pesquisa será desenvolvido a seguir uma análise setorial da PU/SE, no modelo SWOT com a finalidade de identificar as forças, fraquezas, oportunidades e ameaças que existam naquele ambiente.

5.3 Considerações sobre a análise SWOT como ferramenta estratégica

Recorrendo a comunicação organizacional e a análise crítica do ambiente, as organizações têm criado estratégias para melhor acompanhar as mudanças dos ambientes empresariais por meio da inovação e de planejamento estratégico.

Paixão (2012) explica que esse planejamento não acontece de forma simples porque as organizações estão inseridas em um ambiente de incertezas e constantes mudanças, por isso o autor identifica como salutar elaborar ações que proporcionem às organizações o alcance dos seus objetivos e uma visão de futuro mais estável.

Para Wright, Kroll e Parnel (2000), o grande desafio da gestão estratégica consiste em ir além dos objetivos e metas traçados, dependendo muito mais de uma avaliação criteriosa das oportunidades e ameaças do ambiente externo, relacionando-os com a identificação dos pontos fortes e fracos do seu ambiente interno, incluindo nesta visão uma estratégia ampla de todo o macroambiente em que a organização se insere.

Oliveira (2007) entende que o planejamento estratégico deve avaliar os recursos e capacidade financeira e humana disponíveis nas instituições e como o nível desses fatores poderão mudar no futuro. Para tanto, identificar e promover o diagnóstico de questões e problemas podem evidenciar objetivos e planos alternativos.

Existem variadas ferramentas que auxiliam na análise do ambiente, utilizadas principalmente na identificação de problemas para gerir a tomada de decisão estratégica, permitindo identificar situações que possam influenciar a instituição, ajudando ou prejudicando o seu desempenho. Entre esses métodos destaca-se o SWOT.

Muitos teóricos, como Chiavenato e Sapiro (2009) e Gupta e Mishra (2016), argumentam que a Matriz SWOT surgiu como ferramenta clássica da Administração, no berço da Universidade Stanford na década de 60, assim definida:

> Ferramenta que auxilia no reconhecimento do desempenho atual (pontos fortes e fracos) e o futuro da organização (oportunidades e ameaças) levando em conta os fatores que existem no contexto externo" (Gupta; Mishra, 2016, p. 132, tradução nossa).

Gupta e Mishra (2016), advertem que a análise SWOT somente alcança o sucesso ideal se realizado um diagnóstico abrangente, considerando-se a interdependência de fatores de gestão, organizacionais, culturais, sociais, de recursos humanos, políticos e geográficos, capazes de transformar o desempenho organizacional, tanto em receitas como em valor.

Chiavenato e Sapiro (2009), concordam que a análise SWOT, ou FOFA (Forças, Oportunidades, Fraquezas e Ameaças), é uma ferramenta de gestão organizacional, que possui a função de identificar e cruzar as oportunidades e ameaças do seu ambiente externo com seus pontos fortes e fracos para interpretar suas inter-relações para um planejamento estratégico. Segundo definição dos autores:

> A Matriz SWOT (acrônimo Strengths = forças; Weaknesses = fragilidades; Opportunities = oportunidades; Threats = ameaças) foi desenvolvida como uma metodologia capaz de abordar tanto o ambiente externo como o ambiente interno da organização em termos de oportunidades e ameaças exógenas e de forças e fragilidades endógenas (Chiavenato; Sapiro, 2009, p. 181).

Para os autores supracitados, o modelo SWOT permite mapear simultaneamente todas as situações que possam fortalecer os seus pontos positivos, monitorar os seus pontos

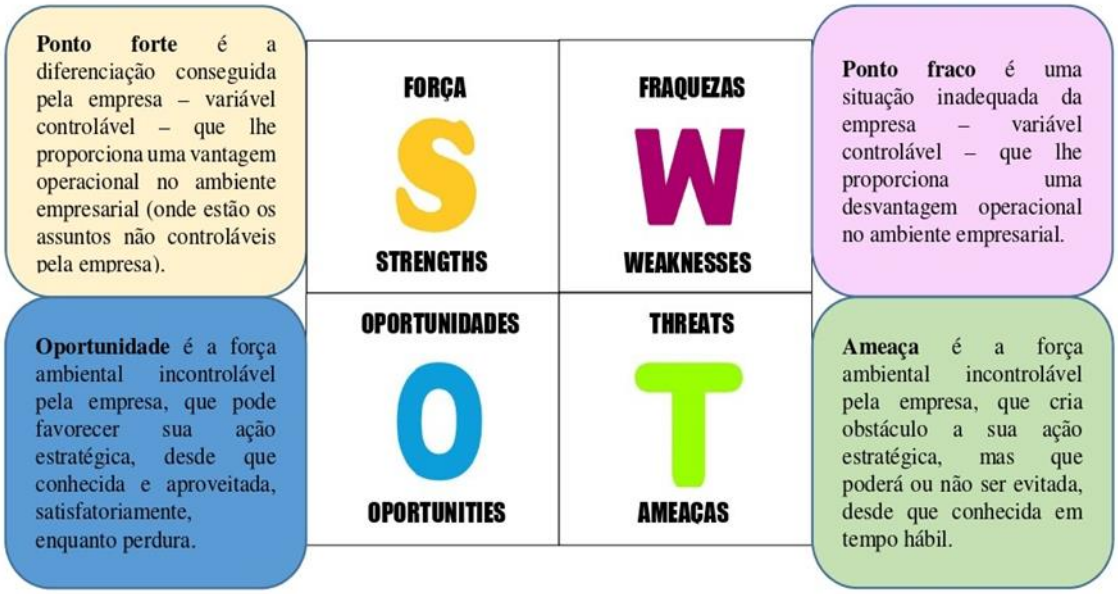
fracos, reconhecer as ameaças e potencializar as oportunidades do seu entorno externo para elaboração de estratégias que tragam êxito a organização (Chiavenato; Sapiro, 2009).

Pontes (2019) explica que a SWOT é uma metodologia que permite o diagnóstico organizacional para identificar os aspectos favoráveis e desfavoráveis para a gestão de uma empresa no âmbito interno e externo. Para o autor, a análise SWOT possibilita, principalmente, "conhecer a situação de sua empresa frente aos seus concorrentes, possibilitando um estudo para mudança de comportamento e melhorias no âmbito empresarial" (Pontes, 2019, p. 22).

Oliveira (2007) entende que as decisões de uma empresa devem ser estruturadas em estratégicas, que ao seu ver, torna-se imprescindível a implantação de metodologias desenvolvidas a partir da análise do ambiente interno e externo da organização.

Face a explicação, a figura abaixo associa as definições do autor aos quadrantes de uma matriz SWOT.

Figura 13 – Definições dos quadrantes do SWOT

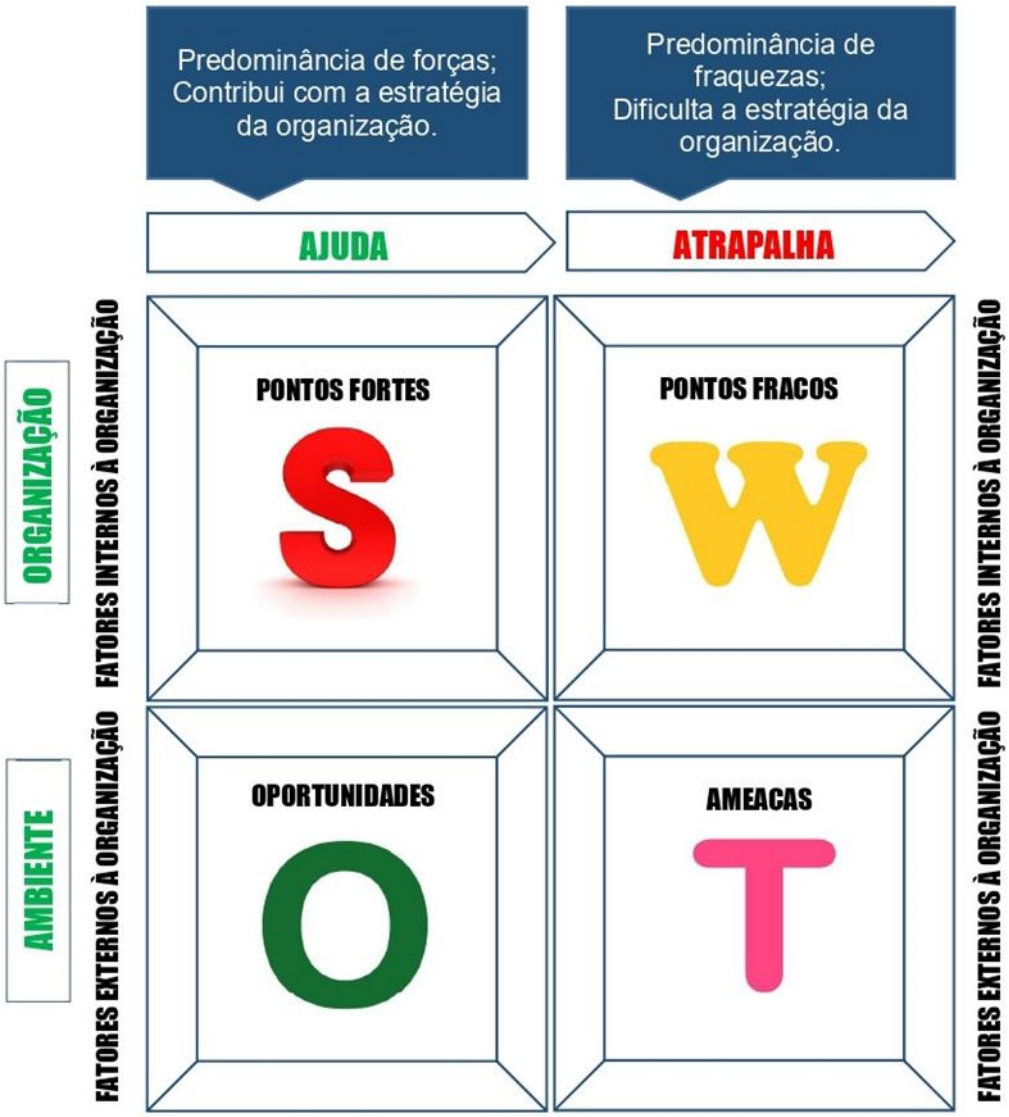


Fonte: Adaptado da Oliveira (2007, p. 37-38).

Para o autor, a SWOT permite a realização de um planejamento estratégico da organização, apresentando um diagnóstico para melhor utilizar os seus pontos fortes, tentar eliminar ou adaptar estratégias para os seus pontos fracos, usufruindo das oportunidades externas enquanto existirem e evitar as ameaças (Oliveira, 2007).

Matos, Matos e Almeida (2007) entendem que a matriz SWOT é o principal direcionamento estratégico da organização porque resulta em uma análise do ambiente organizacional para melhoria do seu desempenho. A figura 14 ilustra o modelo da matriz SWOT adaptado com base nesses autores.

Figura 14 – Diagrama clássico da Matriz SWOT



Fonte: Adaptado de Matos., Matos. e Almeida (2007).

Conforme a figura 14, Matos, Matos e Almeida (2007), explicam que a matriz SWOT é constituída de quatro pilares que se inter-relacionam para direcionamento estratégico. O cruzamento desses quadrantes pode intensificar os resultados positivos para organização, confrontando suas fragilidades para evitar, minimizar e transformar as ameaças em vantagem competitiva.

Segundo os mesmos autores, a matriz SWOT é realizada em dois diferentes passos: inicialmente com a análise do ambiente externo, o qual direciona as atividades futuras por meio da identificação das oportunidades disponíveis e as ameaças potenciais; como segundo passo, deve-se realizar o cruzamento do ambiente interno com o externo, considerando como ponto forte os elementos que a organização pode enfrentar para o seu bom desempenho organizacional

e, como ponto fraco, as ameaças que não está preparada para enfrentar (Matos; Matos; Almeida, 2007).

Chiavenato e Sapiro (2009) corroborando com os quadrantes da figura adaptada de Oliveira (2007), discutem que cada quadrante da SWOT possibilita identificar a situação da organização e o rumo a ser tomado, capacitando-a a tratar das tendências, oportunidades, crises e ameaças do ambiente externo, fortalecendo a gestão estratégica.

Remetendo-se ainda aos autores, no quadrante 1 está a força, sendo o momento da organização aproveitar as oportunidades e agir ofensivamente através das suas competências para fortalecer estratégias; no quadrante 2, as fraquezas da organização podem impedir e/ou desperdiçar as oportunidades, devendo-se agir com políticas defensivas; partindo-se para o quadrante 3, a organização deve identificar as oportunidades e aproveitar o seu potencial; seguindo-se para o quadrante 4, identifica-se um momento de crise, indicativo para desinvestimento e/ou blindar (Chiavenato; Sapiro, 2009)

Sob esta perspectiva, entende-se que a análise do ambiente externo e interno é que vai permitir o diagnóstico dos problemas e questões a serem enfrentadas para um planejamento e plano de ação, e elaborou-se uma análise SWOT da PU/SE descrito em seguida.

5.4 Descrição da análise SWOT da TI na PU/SE

Com a caracterização do ambiente organizacional da PU/SE promoveu-se a análise SWOT da TI dando-se ênfase à política de segurança da informação.

Indica-se como fundamental explicar um pouco sobre a evolução dos SI na AGU para melhor compreensão da análise SWOT da TI no órgão. No ano de 2002 foi implantado o Sistema de Controle de Documentos da AGU (AGUDOC), por onde toda a documentação produzida em seu âmbito interno e externo era cadastrada e tramitada por meio de um NUP (Número Único de Protocolo).

No AGUDOC, a tramitação de documentos se dava em formato físico, com controle baseado no NUP de entrada (Brasil, 2010). Contudo, mais tarde, o Sistema Integrado de Controle das Ações da União (SICAU) foi introduzido, sob a regulamentação da Portaria AGU nº 81, datada de 14 de fevereiro de 2003. O SICAU controlava documentos administrativos e processuais, gerava relatórios gerenciais e mantinha um dossiê judicial, mas não permitia a criação de documentos eletrônicos, não se integrava com sistemas externos e tinha foco no registro e controle de documentos administrativos e jurídicos.

Em termos de digitalização, a Portaria nº 169, de 25 de abril de 2013, determinou os padrões a serem adotados por todas as Unidades da AGU para a digitalização dos documentos e processos judiciais físicos, assim definindo: O processo de digitalização é o ato de transformar um documento físico em digital, que por sua vez pode ser armazenado em vários tipos de mídias (Brasil, 2013, p. 7). A digitalização trouxe a implantação do SIGAD e com ela a modernização e inovação da GI.

Muitas vezes essas mudanças provêm de ajustes para eficiência da GI em SI, a exemplo, a própria AGU tem trabalhado para modernizar sempre a interface do SAPIENS AGU, que tem por objetivo apoiar a produção jurídica interna, bem como controlar fluxos e processos administrativos e judiciais internos e externos (Cardoso, 2018).

O SAPIENS, devido à sua funcionalidade, foi o grande vencedor da 17ª Edição do Prêmio *Innovvare* na categoria Advocacia em 2020. Esse prêmio, de acordo com informações divulgadas em seu site institucional, tem como objetivo identificar, divulgar e promover práticas que aprimoram o Sistema Judiciário, focando em ações que beneficiem o bem público (AGU, 2020).

Esse reconhecimento, a diretoria do Departamento de Gestão Estratégica da AGU (DGE), está nos resultados do sucesso judicial alcançados, tanto por sua funcionalidade, quanto pelos profundos avanços de integração e inovação de ações com o Poder Judiciário Brasileiro, que tem proporcionado por meio da inteligência artificial uma maior agilidade em seus argumentos e respostas (AGU, 2020).

Em termos organizacionais, o SAPIENS integrou e aperfeiçoou os sistemas informatizados do Poder Judiciário e do Poder Executivo fomentando o desempenho institucional alinhado ao seu planejamento estratégico (AGU, 2020). Acredita-se que antes que esta pesquisa em andamento se finalize já esteja implantada uma nova versão do SAPIENS na AGU, o Super SAPIENS.

A AGU (2021) relatou melhorias significativas em seu sistema, incluindo uma interação mais simples e prática para gerenciar demandas alinhadas ao planejamento estratégico. As atualizações também permitem a assinatura de documentos sem certificado digital, geram subsídios para defesa judicial automaticamente, aumentam a velocidade em 70%, oferecem suporte em diversos dispositivos e são compatíveis com sistemas operacionais, incluindo iOS e Android.

Voltando-se para a análise SWOT da TI na PU/SE, para assegurar uma análise mais criteriosa, contou-se com o apoio do Servidor Adilson José dos Santos, lotado na PU/SE que atua na CONATEC, como colaborador Técnico Especializado.

A opção de contar com o apoio do servidor foi estratégica, tanto em função da praxe especializada por ele desenvolvida junto a TI na AGU, quanto por sua experiência na área de Ciência da Computação, voltada para os estudos em Sistemas de Informação, em Ciência de Dados, Inteligência Artificial e Aprendizagem de máquinas.

Outro ponto positivo para assegurar uma análise SWOT com mais eficiência foi a formação acadêmica de Adilson José dos Santos, a saber: Mestre em CI pela Universidade Federal de Sergipe (2020), pós-graduado em Gestão de Tecnologia da Informação pela Faculdade Futura (2017), graduação em Formação Específica em Desenvolvimento Web pela Universidade Tiradentes (2008).

O diagnóstico visou identificar os pontos fortes e fracos, além das ameaças e oportunidades com base na segurança da informação, conforme quadro 14.

Quadro 14 – Diagnóstico por análise SWOT da PU/SE

AMBIENTE INTERNO	
PONTOS FORTES	**PONTOS FRACOS**
FORÇAS	**FRAQUEZAS**
Procedimentos de segurança da informação implantados em sistemas.	**Ausência de um programa de capacitação em segurança da informação para os integrantes da AGU e suas unidades descentralizadas**.
Engajamento da equipe de TI, com respostas rápidas aos problemas de TI.	Redundância do Centro de dados da AGU ainda não implantada em sua totalidade.
Prospecção de novas tecnologias	**Ausência de treinamento programados e contínuos dos servidores no uso de sistemas e computadores**
Integração dos sistemas de informação e consolidação do processo eletrônico por meio do SAPIENS.	Deficiência na gestão de configuração e mudanças.
Aumento da quantidade de colaboradores de TI.	**Parcela significativa do parque tecnológico sem garantia e obsoleta.**
Disponibilidade de uso externo dos equipamentos tecnológicos com fins de trabalho remoto.	Alta dependência dos profissionais terceirizados.
	Ausência de equipes qualificadas de TI nas unidades descentralizadas da AGU.
	Procedimentos de segurança da informação implantados parcialmente quanto ao uso dos equipamentos por parte dos seus usuários.
AMBIENTE EXTERNO	
PONTOS POSITIVOS	**PONTOS NEGATIVOS**
OPORTUNIDADES	**AMEAÇAS**
Integração de sistemas com outros órgãos do poder executivo e do judiciário.	Novos cortes e contingenciamentos orçamentários podem impactar nos contratos atuais e futuros de TI.
Interação com outros órgãos objetivando a troca de conhecimentos, intercâmbio de dados e sistemas, entre outras soluções	Restrições financeiras poderão ocasionar inadimplência com fornecedores de TI.
Pesquisa e desenvolvimento por novas soluções, mais racionais e econômicas.	**Falhas nos sistemas e serviços de outras entidades da Administração Pública, gerando problemas de integração e troca de informações**.
Novas tecnologias de computação em nuvem permitiriam redução da complexidade de gestão.	**Ataques cibernéticos podem afetar a segurança da informação e a disponibilidade dos serviços.**
	Mudanças recorrentes de sistemas de informação sem tempo para treinamento dos membros da AGU.

Fonte: Elaborado pela autora (2022).

Com base na análise do diagnóstico SWOT e elencados os principais elementos identificados nos pontos positivos e negativos do ambiente interno e do ambiente externo, formulou-se estratégias para determinação de ações que possam melhorar o desempenho da PU/SE. Os itens elencados correspondem a pontos que se relacionam com a intervenção proposta nessa pesquisa, contudo, deu-se maior destaque aos itens que se relacionam com as questões de segurança da informação envolvendo os usuários dos sistemas, destacadas em negrito.

Em relação ao ambiente interno, com indicativo nas forças, observou-se que o sítio tecnológico é uma força presente na organização, principalmente com a possibilidade de prospecção de novas tecnologias e disponibilidade de uso externo dos equipamentos tecnológicos por seus membros que atuam na modalidade de trabalho remoto.

Por se tratar de uma organização jurídica, que tem como objetivo principal o cumprimento de prazos judiciais, seja para resposta das diferentes fases dos litígios ou para atuação extrajudicial da União, a integração dos sistemas de informação e consolidação do processo eletrônico por meio do SAPIENS constitui atualmente uma das maiores forças no âmbito da AGU em todo o território nacional.

Nessa mesma vertente, outra força identificada é o engajamento da equipe de TI, com respostas rápidas aos problemas de TI e suporte, tendo a organização uma preocupação em aumentar a quantidade de colaboradores de TI. Embora listados no quadrante força, os procedimentos de segurança da informação implantados na AGU estão voltados para a proteção dos sistemas e, com certeza, são de grande valia, mas não foram identificadas as questões voltadas para a segurança do usuário do sistema, nem mesmo no plano de governança da AGU.

Observa-se que as questões que envolvem os usuários estão direcionadas ao suporte técnico e índice de satisfação dos usuários, promovidos pelos serviços técnicos especializados, o que valida ainda mais a importância e os objetivos traçados no corpus dessa pesquisa.

Pôde-se identificar como componentes dos pontos fracos voltados para a segurança da informação: ausência de um programa de capacitação em segurança da informação para os integrantes da AGU e das suas unidades descentralizadas e procedimentos de segurança da informação quanto ao uso inadequado dos sistemas por parte dos seus usuários.

Sob esse ponto negativo é preciso adotar uma estratégia de confronto com esses problemas de segurança da informação, porque são situações que ameaçam o desempenho do ambiente interno da organização trazendo riscos e fragilidades na área da TI.

A partir da análise SWOT, na concepção dos usuários dos sistemas da PU/SE, sugere-se adotar estratégias que ampliem a qualidade dos serviços prestados e suporte,

principalmente aos membros que estão desenvolvendo suas atribuições na modalidade de trabalho remoto, dando condições para que os usuários possam obter informações confiáveis, úteis e com redução de riscos que possam interferir na segurança da informação.

Embora exista um sítio tecnológico desenvolvido, identificou-se a presença de parcela significativa do parque tecnológico sem garantia e obsoleta, visto que a tecnologia se renova constantemente e, muitas vezes, fatores externos trazem ameaças para o ambiente, como restrições financeiras, cortes e contingenciamentos orçamentários que podem impactar nos contratos atuais e futuros de TI.

Para esses fatores externos, que caracterizam ameaças, é recomendado adotar estratégia defensiva no que tange a garantia de orçamento e a execução financeira adequada para manutenção da infraestrutura da TI. Dentro dessa perspectiva financeira, incluir na governança digital da organização o gerenciamento dos riscos de TI é relevante.

Determinadas ameaças podem afetar diretamente a segurança da informação, destacando-se: os riscos cibernéticos, falhas nos sistemas e serviços de outras entidades da administração pública, gerando problemas de integração e troca de informações.

As ameaças relacionadas ao suporte técnico foram identificadas, em destaque, relacionadas à ausência de equipes qualificadas de TI nas unidades descentralizadas da AGU. Esse problema foi intensificado com a implantação das equipes virtuais de trabalho, estabelecidas pela desterritorialização, não mais existindo o suporte direcionado e individualizado que acontecia por parte da TI no ambiente físico da PU/SE.

Estando os servidores da TI desterritorializados, aconteceu a alta dependência dos profissionais terceirizados, os quais atendem nas unidades físicas através da abertura de chamados para soluções tecnológicas e não se estendem ao suporte remoto.

Destacam-se ainda as falhas nos sistemas e serviços de outras entidades da administração pública, gerando problemas de integração e troca de informações e as mudanças recorrentes de sistemas de informação sem tempo para treinamento dos membros da AGU.

As maiores oportunidades identificadas pela análise SWOT correspondem ao aprendizado e crescimento institucional com identificação de competências e inovações de gestão e as novas tecnologias de computação em nuvem que permitiriam redução da complexidade de gestão. Sugere-se como recomendação de estratégia de reforço, investir no desenvolvimento de competências, para interação e GC, e a troca de conhecimentos, intercâmbio de dados e sistemas com outros órgãos, entre outras soluções.

A análise SWOT ajudou a identificar questões práticas de segurança da informação que podem fortalecer o ambiente interno da PU/SE e favorecer medidas de segurança no órgão.

6 RESULTADO DA INTERVENÇÃO E DISCUSSÃO

A intervenção foi fundamentada nas bases da pesquisa-ação e norteada por um plano de ação coordenado em metas seguidas sistematicamente para culminar na resolução do problema dessa pesquisa e nos seus objetivos.

Os requisitos legais e éticos da pesquisa foram integralmente cumpridos, o que iniciou com a anuência da intervenção pela Procuradora-Chefe da União em Sergipe, Andrea Carla Veras Lins, conforme termo inserido no anexo C (p. 192). Além disso, o projeto foi apresentado à organização, com o propósito de sensibilizar seus membros quanto à importância da pesquisa de mestrado e sua relevância social. Posteriormente, um diagnóstico do ambiente da PU/SE foi elaborado, e após a submissão e aprovação da pesquisa pelo CEP (p. 182), e a concessão das garantias éticas aos participantes da pesquisa, a pesquisadora foi inserida no campo da pesquisa, onde aplicou e concluiu a intervenção.

Como instrumento de coleta de dados, o questionário desempenhou um papel crucial ao fornecer informações que permitiram a identificação e investigação dos indicadores de falhas de segurança da informação sob diversas óticas. Esse processo envolveu uma análise abrangente, que abarcou tanto a vertente qualitativa quanto a quantitativa dos dados coletados.

O questionário foi enviado por e-mail para os 42 servidores da PU/SE e ficou disponível para resposta por um período de 30 dias, com o prazo final de submissão em 20 de maio de 2023. Após essa data, o acesso ao questionário foi desativado, impedindo novas respostas.

Após o prazo preestabelecido, foram coletados 25 questionários respondidos, representando 59,52% dos 42 servidores da PU/SE. Os resultados obtidos estão detalhados no quadro 15.

Quadro 15 – Amostra real dos participantes de pesquisa

Participantes	Área	Categoria	Função	Nível	Quantidade
ADV	Fim	Advogados da União	Defesa da União	Superior	**7**
STA	Meio	Servidores técnico-administrativos	Apoio Jurídico	Médio e Superior	**10**
SCD	Meio	Servidores cedidos	Apoio jurídico direcionado ao NECAP	Médio e Superior	**4**
ETERC	Meio	Terceirizados	Apoio Administrativo	Médio	**3**
ESTAG	Superior	Estagiários	Apoio Jurídico	Superior	**1**
Total da Amostra					**25**

Fonte: Elaborado pela autora (2023).

Após receber 25 questionários respondidos iniciou-se a análise dos dados. Essa análise teve o objetivo de validar a pesquisa de acordo com seus objetivos e também serviu como base para a criação do produto final da pesquisa: um Manual de Boas Práticas de Segurança da Informação. Esse manual foi elaborado com cuidado e destina-se aos usuários dos sistemas de informação. A discussão dos resultados da intervenção será minuciosamente abordada nas subseções subsequentes.

6.1 Resultado da análise qualitativa

Para investigar a percepção dos participantes, realizou-se a análise das respostas textuais das questões abertas e descritivas, por meio de uma análise categorial de conteúdo de Bardin (2011). Essa abordagem proporcionou não apenas uma compreensão mais aprofundada das experiências práticas dos respondentes, mas também deu a eles a oportunidade de se expressarem e de se tornarem protagonistas ao descrever e compartilhar relatos baseados em suas vivências como usuários dos sistemas na PU/SE.

Além de abordar a percepção dos respondentes, a análise das respostas abertas permitiu uma abordagem prospectiva, através de perguntas que incentivaram a formulação de sugestões concretas de boas práticas em segurança da informação, adaptadas ao cenário de suas atividades laborais.

O objetivo principal era criar um questionário de pesquisa que minimizasse a influência das percepções pessoais da pesquisadora, considerando sua posição na organização onde a pesquisa ocorreu. Para atingir esse objetivo foram incluídas questões discursivas, permitindo que os respondentes expressassem suas perspectivas individuais de forma independente. Isso resultou em um conteúdo textual rico, categorizado de acordo com as variáveis das perguntas do questionário, conforme detalhado no quadro 16.

Quadro 16 – Classificação da variável “ameaça” no questionário

Questão 20	Questão 20 – Relate resumidamente quais as principais ameaças e preocupações relativas à segurança da informação em suas práticas de trabalho na AGU
Classificação	**PERCEPÇÃO**
Categoria	**AMEAÇA**
Codificação	Termos encontrados nos textos dos respondentes foram codificados por temas ou padrões emergentes que indicaram as possíveis ameaças considerando a interface usuário, tecnologia e sistema.
Objetivo	Descrever os indicativos da percepção dos usuários da PU/SE em relação às ameaças à segurança da informação**.**

Fonte: Elaborado pela autora (2023).

Dos 25 respondentes dos questionários, somente 19 optaram por responder às questões abertas, o que formou a base para a análise qualitativa. Isso explica a diferença entre o número total de questionários respondidos nas seções de questões abertas e fechadas.

As etapas da análise de conteúdo seguiram as diretrizes gerais propostas por Bardin (2011) e foram conduzidas com o auxílio do software NVivo, na versão Release 14.23.3 (46), que agilizou a categorização e classificação dos dados da pesquisa. Para a classificação e codificação, antes de importar os textos para o NVivo, optou-se por conduzir uma análise minuciosa e extensiva do conteúdo dos textos. O objetivo foi organizar os dados, minerar e identificar os principais termos nos 19 questionários respondidos para proceder à categorização das percepções nas categorias "ameaça" e "boas práticas".

Na categoria “ameaça”, a análise dos arquivos gerou um grande número de termos dentro de cada questão respondida. Inicialmente, conduziu-se uma análise de frequência de palavras para relacionar as principais percepções mencionadas. Essa abordagem permitiu identificar a ocorrência de palavras ou termos específicos relacionados aos indicadores de falhas de segurança da informação, proporcionando uma análise mais precisa. A frequência de palavras é uma métrica útil para identificar as palavras mais comuns, facilitando a compreensão de temas, tendências e padrões nos dados, conforme descrito por Bardin (2011).

Para a análise de frequência de palavras ou termos, optou-se por selecionar as 20 palavras mais frequentes em cada código. Foram aplicados filtros para limitar a análise a palavras com pelo menos 5 caracteres, excluindo conjunções, advérbios e pronomes. O quadro 17 descreve a análise que envolve a frequência com que determinados termos aparecem durante a categorização das ameaças.

Quadro 17 – Frequência de palavras na categorização do termo “ameaças”

Palavra	Extensão	Frequência	Percentual %
Malware	7	14	011
Phishing	8	14	011
Senhas	6	10	008
Despreparo	10	9	007
Inexperiência	13	9	007
Teletrabalho	12	9	007
Dúvidas	7	5	004
Financeiro	10	3	002
Incomunicação	13	3	002
Desatenção	10	2	002
Hiperlinks	10	2	002
Infectados	10	2	002
Denúncias	9	1	001
Download	8	1	001
Equipamentos	12	1	001

Fonte: Elaborado pela autora (2023).

Ao analisar a frequência das palavras categorizadas, identificou-se uma maior preocupação em relação aos ataques lançados por cibercriminosos que se aproveitam da vulnerabilidade dos sistemas. No entanto, é importante destacar que os ataques cibernéticos têm uma relação direta com os usuários dos sistemas, uma vez que muitos desses ataques visam explorar vulnerabilidades relacionadas às interações humanas ou às ações dos próprios usuários.

Os ataques de *makware* e *phishing* são muitas vezes desencadeados por ações decorrentes da interação dos usuários com sistemas e podem ter relação direta com a falta de atenção ou despreparo. Dada a frequência crescente desses ataques, principalmente porque esses ataques quando bem elaborados podem enganar o servidor, é fundamental que as organizações promovam uma discussão mais aberta e compartilhem informações sobre essas ameaças em nível organizacional. Alguns participantes da pesquisa mencionaram a falta de comunicação eficaz para compartilhar informações quando identificam esses ataques e a ausência de um canal de divulgação pela DTI.

Outra categoria com maior destaque na percepção dos usuários foi a "senha," e essa percepção está relacionada a uma questão antiga e recorrente dentro das organizações, bem como na proteção dos dados pessoais dos usuários em geral: senhas fracas ou comprometidas. Os trechos transcritos dos respondentes abaixo demonstram como essa vulnerabilidade foi identificada como a terceira categoria mais comum:

> Minha preocupação está relacionada à gestão de senhas. A utilização de senhas repetidas para facilitar a memorização é uma prática arriscada, mas que tem facilitado o meu acesso principalmente com relação a outros sistemas do judiciário que não são sincronizados com o sistema SAPIENS/AGU, a exemplo do Sistema Creta dos Juizados Especiais Federais dos Estados de Alagoas, Ceará, Paraíba, Pernambuco, Rio Grande do Norte e Sergipe. Esse sistema não possui política de mudança periódica de senha e nem MFA. Reconheço que a diversificação das senhas é fundamental para proteger as contas e os sistemas contra ataques cibernéticos, mas são muitas senhas para decorar (STA4, 2023).

> Eu nunca troquei a senha inicial do sistema Creta em nenhum dos Juizados Especiais dos diversos estados nos quais acesso os processos, nunca senti necessidade e nunca me foi cobrado. Repito a mesma senha em todos os tribunais. Não tenho como mudar porque são muitas senhas e eles não permitem o uso do Token (STC1, 2023).

Muitos ataques exploram senhas fracas ou roubadas. Os usuários frequentemente escolhem senhas fracas ou reutilizam senhas em vários sites, o que facilita para os invasores adivinharem ou testarem senhas até obterem acesso não autorizado a contas. Lembrando que a informação jurídica tem um valor imensurável com dados relevantes que precisam de proteção.

Convém esclarecer que existe uma política de troca de senha obrigatória e periódica estabelecida pela DTI na AGU. No entanto, é fundamental destacar que essa política se aplica

apenas ao acesso à Rede AGU e não abrange as senhas do SAPIENS, da autenticação do token ou de sistemas externos relacionados às atividades jurídicas.

É importante ressaltar que a Autenticação Multifator (MFA) não é uma exigência obrigatória dentro da organização. Os servidores que desejam adotar essa prática podem fazê-lo de forma voluntária, mediante expressão de interesse junto à DTI. Compreende-se que a MFA desempenha um papel crucial na segurança cibernética e na proteção de dados sensíveis, notadamente na prevenção de fraudes relacionadas à segurança de contas online. Essa abordagem teria o potencial de fortalecer significativamente a segurança, reduzindo o risco de acessos não autorizados e garantindo a proteção de informações confidenciais.

Outras duas categorias que se destacaram na codificação das "ameaças" na percepção dos servidores foram o despreparo e a inexperiência, refletindo a falta de treinamento que a maioria dos respondentes associou às ameaças identificadas. Esses fatores estão diretamente relacionados à maior percepção de ameaças após a transição para o teletrabalho, quando atuaram sem o suporte direto anteriormente disponível, quando a organização trabalhava presencialmente e contava com uma equipe de TI para auxiliar. Algumas respostas discursivas do questionário representam esse fato:

> Sinto a carência de treinamentos direcionados aos servidores e colaboradores, especialmente no que diz respeito à segurança da informação. Essa deficiência se tornou ainda mais notável com a implementação do teletrabalho, uma realidade com a qual agora convivemos no ambiente profissional. Faltam recursos e apoio da equipe de TI para nos manter bem informados e para esclarecer dúvidas referentes às potenciais ameaças com as quais, por vezes, nos deparamos. Além disso, persistem questionamentos sobre como aprimorar as práticas de segurança no uso do Sapiens e nos sistemas interconectados (ADV1, 2023).

A organização implementou um plano de gestão válido até agosto de 2024, com 50% dos servidores em teletrabalho, 25% em um modelo semipresencial e 25% trabalhando presencialmente. O suporte de TI interno foi substituído por um serviço terceirizado, mas esse suporte não atende às necessidades dos usuários que usam equipamentos pessoais, tornando os servidores responsáveis por adquirir software de segurança por conta própria.

Essa problemática foi discutida na pesquisa quando abordadas as questões financeiras relacionadas ao teletrabalho. Além disso, há uma tendência de que todos os equipamentos usados no teletrabalho sejam devolvidos à organização, sem substituição de equipamentos obsoletos. O processo de devolução dos equipamentos já está em andamento.

> O teletrabalho tem sido vantajoso em termos de gerenciamento de tempo e eficiência. No entanto, implica em custos adicionais para os servidores, como equipamentos, manutenção e consumo de energia. Manter o sistema atualizado também pode representar uma despesa que, em alguns casos, ultrapassa os padrões financeiros estabelecidos pela organização em relação às remunerações oferecidas (STC8, 2023).

O conjunto de termos pode também ser visualizado na nuvem de palavras gerada na categorização “ameaça” e oferece uma visão dos termos discutidos e sua relevância para maior compreensão.

Figura 15 – Nuvem de palavras na categorização do termo “ameaças”

Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

A nuvem de palavras confirma debates anteriores e revela uma relação hierárquica baseada na frequência de termos na pesquisa. A falta de comunicação é um problema recorrente, muitas vezes resultando da ausência de canais adequados para compartilhar dúvidas ou denunciar links suspeitos. Os usuários estão preocupados com essa lacuna na comunicação e a ausência de canais apropriados para relatar problemas de segurança. Isso destaca a necessidade de aprimorar a comunicação interna e estabelecer canais de denúncia eficazes.

Da mesma forma, questões de desatenção e presença de ameaças cibernéticas estão claramente relacionadas à necessidade de uma comunicação mais integrada e direcionada, como evidenciado nos textos ADV5 e SCD3:

> Falta clareza sobre a quem recorrer para questões de segurança da informação, uma vez que o suporte online não aborda esses problemas. Com o teletrabalho, a equipe de suporte local não está disponível, e os servidores carecem de orientações e treinamento específico sobre segurança da informação. Não há um manual prático e acessível para guiar uma conduta segura em relação aos sistemas de informação da AGU (ADV5, 2023).

> Ao acessar minha conta de e-mail institucional diariamente, tenho notado a presença de e-mails maliciosos que não foram detectados pela equipe de Tecnologia da Informação (DTI). Em algumas situações, essas ameaças são mantidas em nível setorial e não são comunicadas a todos os servidores, o que aumenta o risco de infecções por vírus. Quando tenho dúvidas ou preocupações, encaminho pessoalmente esses e-mails suspeitos para o colega Valdomiro da PRU5 (SCD3, 2023).

Foi fundamental permitir que os participantes da pesquisa compartilhassem suas sugestões de boas práticas em segurança da informação. Isso possibilitou que eles adotassem uma abordagem crítica e inclusiva como parte do processo. Essa abordagem, ao confrontar a categoria "ameaça" com "boas práticas", incentivou os respondentes a refletirem sobre seu

comprometimento com a melhoria da segurança da informação. Além disso, proporcionou indicativos valiosos para a pesquisa, como identificados nas discussões que se seguem.

Os indicativos da percepção dos usuários da PU/SE em relação às boas práticas de segurança da informação foram abordados conforme descrito no quadro 18:

Quadro 18 – Classificação da variável "boas práticas" no questionário

Questão 21	Questão 21 – Considerando o seu protagonismo como pessoa usuária dos sistemas de informação na AGU contribua com sugestões de melhorias para a segurança da informação.
Classificação	**PERCEPÇÃO**
Categoria	**BOAS PRÁTICAS**
Codificação	Os termos identificados nos textos dos respondentes foram agrupados em temas ou padrões emergentes, fornecendo sugestões de boas práticas em segurança da informação, com foco na interação entre o usuário e o sistema.
Objetivo	Descrever os indicativos da percepção dos usuários da PU/SE em relação às boas práticas de segurança da informação.

Fonte: Elaborado pela autora (2023).

A análise da frequência das palavras relacionadas às boas práticas em segurança da informação proporciona uma visão detalhada da percepção dos servidores. Essa abordagem prática e centralizada destacou a importância crítica dos usuários de sistemas para a organização. O quadro 19 ilustra como os participantes da pesquisa percebem seu papel na promoção de uma cultura de segurança informacional e como isso pode resultar em benefícios substanciais para toda a organização.

Quadro 19 – Frequência de palavras na categorização do termo "boas práticas"

Palavra	**Extensão**	**Frequência**	**Percentual %**
Treinamento	11	13	019
Manual	6	7	010
Conscientização	15	5	007
Comunicação	11	4	006
Informação	10	4	006
Backup	6	3	004
Compartilhamento	16	3	004
Multifator	10	3	004
Política	8	3	004
Suporte	7	2	003
Capacitação	11	1	001

Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

Para aprimorar a demonstração dos resultados apresentados no quadro acima, optou-se por incluir uma nuvem de palavras que visualmente consolida a representação gráfica do quadro percentual resultante da análise de frequência das palavras categorizadas como "boas práticas" na análise de conteúdo. Essa representação gráfica oferece uma visão imediata das palavras-chave ou dos temas mais destacados no conjunto de dados, tornando mais fácil a compreensão das principais tendências e ênfases.

Figura 16 – Nuvem de palavras na categorização do termo “boas práticas”

Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

Na análise do critério de boas práticas é evidente que a grande maioria dos respondentes enfatiza a importância do treinamento como um indicativo fundamental para a segurança da informação. Isso confirma sua relação direta com uma das maiores ameaças identificadas por eles, que é a falta desse treinamento. A percepção dos respondentes claramente destaca a necessidade de estabelecer diretrizes padronizadas para orientar ações de boas práticas, seguidas de perto pelos termos "conscientização" e "comunicação".

Essa análise tem despertado inquietações reflexivas por parte também da pesquisadora e confirmada na análise do conteúdo da pesquisa, de que quanto mais se multiplicam os sistemas para o âmbito jurídico, mais frequente é a necessidade de um treinamento e mais forte se torna as possíveis fragilidades de riscos para os usuários. Alguns trechos das respostas do questionário foram relevantes nesse aspecto:

> Sugiro a implementação de um software oficialmente contratado pela AGU para a compactação de arquivos em PDF. Isso garantiria a segurança das informações, eliminando o risco associado ao uso de sites gratuitos não confiáveis. Além disso, é importante criar um manual completo de segurança da informação para orientar os usuários na utilização do SAPIENS e outros sistemas, tanto internos quanto externos à organização (ADV6, 2023);
>
> Como sugestão de boas práticas em segurança da informação, proponho que a disseminação das informações relacionadas às práticas de segurança seja uma prática comunicada em todos os níveis da organização. Isso pode ser alcançado por meio da adoção de um manual ou guia contendo normas para padronizar as ações voltadas à segurança da informação. Essa abordagem pode orientar, em linguagem simples, sobre os perigos do ciberespaço. (STA10, 2023).

Segundo as análises acima observa-se que o tema tem despertado reflexões e inquietações por parte dos servidores conforme percepções identificadas na pesquisa. Fica evidente que quanto mais sistemas são introduzidos no contexto jurídico, mais ocorre a necessidade de treinamento, e as possíveis fragilidades e riscos para os usuários se tornam mais evidentes e preocupantes.

Quando os respondentes expressam suas percepções e sugerem ações que enfatizam a conscientização, comunicação e informação de forma igualmente significativa, isso pode indicar que a conscientização já está bem enraizada ao longo dos anos de prática. No entanto, a cultura organizacional, que deveria ser o meio de comunicação e disseminação de informações, para facilitar a adoção das boas práticas em segurança da informação, parece não estar suficientemente desenvolvida. Isso ressalta a necessidade de fortalecer os aspectos culturais relacionados à segurança da informação dentro da organização.

Essa observação sugere que, embora os indivíduos reconheçam a importância da segurança da informação, a organização pode ainda não ter criado um ambiente propício para uma comunicação eficaz e a disseminação de informações cruciais necessárias para a adoção dessas boas práticas.

Também foi observado que há preocupações relacionadas às práticas de *backup*, à adoção da MFA, que não é obrigatória na AGU, e questões relacionadas ao suporte técnico, bem como à falta de divulgação das políticas de segurança da informação, como mencionado anteriormente nas questões sobre ameaças.

Analisando o conteúdo das respostas, por meio da sua categorização foi possível atingir um dos primeiros objetivos específicos da pesquisa: investigar elementos indicadores de falhas de segurança a partir da percepção dos participantes da pesquisa propondo estratégias alternativas de GSI que envolva a interface usuário, tecnologia e sistema.

6.2 Resultados da análise quantitativa

Para a análise dos resultados das questões fechadas dos questionários, foi adotada a abordagem de tratamento dos dados por meio de estatística descritiva simples. Essa metodologia possibilitou a construção de um perfil dos usuários e orientou os resultados em direção às questões diretamente associadas à interação entre o usuário, tecnologia e sistema. Além disso, a utilização de gráficos e tabelas permitiu a apresentação das informações de forma clara e sucinta.

Foram analisados 25 questionários entregues pelos respondentes no intervalo de tempo estabelecido, que ocorreu de 20 de abril de 2023 a 20 de maio de 2023, representando uma adesão de 59,52% da amostra total, como anteriormente já mencionado.

As questões fechadas do questionário abordaram diversas variáveis, incluindo o perfil do usuário, o comportamento dos usuários e a utilização de sistemas de informação. Essas variáveis foram elaboradas com base na literatura consolidada e nas normas de segurança da

informação. O quadro a seguir descreve as variáveis utilizadas para mapear os riscos de segurança da informação.

Quadro 20 – Descrição das variáveis das perguntas fechadas do questionário

Questões fechadas – 19 questões		
Classificação	**Mapeamento de riscos**	
Categoria	**Descrição das questões**	**Objetivo**
Pessoas/Perfil	Traçar um perfil dos usuários.	Identificação que buscou elaborar um perfil dos usuários e situá-los na organização.
Usuários/Comportamento	Abordar o comportamento dos usuários de sistemas de informação com relação aos riscos de segurança da informação.	Identificar a compreensão dos usuários sobre segurança da informação e o grau de comprometimento deles com esse aspecto.
Sistemas de informação/Uso	Descrever como os sistemas de informação são utilizados em uma organização no âmbito da segurança da informação.	Identificar a postura de segurança cibernética em relação à utilização dos sistemas e à conscientização dos usuários sobre os riscos envolvidos.

Fonte: Elaborado pela autora (2023).

Os critérios éticos do TCLE foram respeitados e garantidos assim que o respondente concordou em participar da pesquisa ao clicar na opção: “Li o TCLE, compreendi e concordo em participar da pesquisa”. Essa opção respaldou tanto o pesquisador quanto o participante de pesquisa.

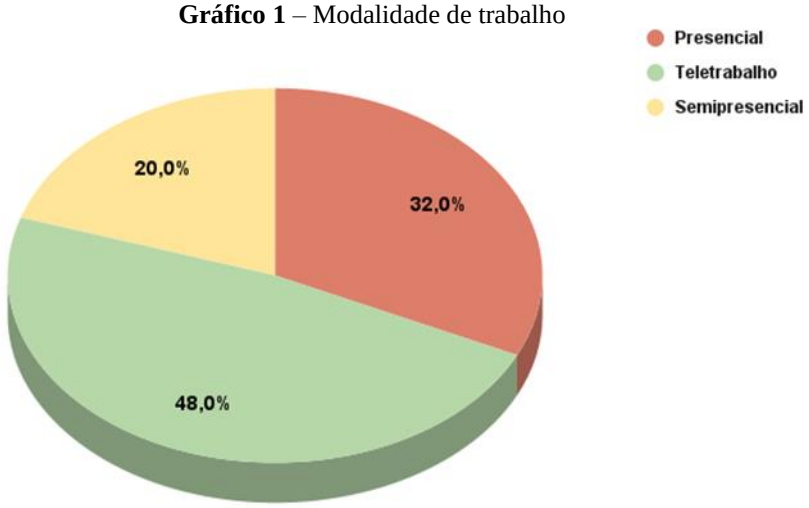
Inicialmente, buscou-se traçar o perfil dos usuários dos sistemas identificando-se a sua ocupação ou função exercida na organização. A seleção da amostra intencional e não probabilística foi importante para a pesquisa, pois deu acesso a diferentes servidores com perfis de atuação diferentes, inclusive, enriquecendo e diversificando diferentes percepções e indicadores.

Dentre os participantes da pesquisa, 28% eram Advogados da União, 40% servidores técnico-administrativos, 16% servidores técnico-administrativos requisitados e 16% colaboradores terceirizados, incluindo estagiários nesta categoria. Em termos de pesquisa, essa amostra revelou-se significativa tanto em número quanto em diversidade de atividades e funções exercidas. Todos os membros da amostra são usuários do sistema SAPIENS e desempenham tarefas relacionadas à produção e ao fluxo de documentos e processos no sistema. Além disso, todos os participantes acessam os sistemas judiciários, exceto os colaboradores terceirizados, que não possuem senhas nem token para acessar os sistemas judiciários externos à AGU.

No contexto do perfil dos servidores, na segunda questão priorizou-se identificar a modalidade de trabalho por eles adotadas na organização, no sentido de se agregar a modalidade

das suas atribuições laborais indicativos de elementos que influenciem na segurança da informação quando comparado a organização e o trabalho remoto (Gráfico 1).

Gráfico 1 – Modalidade de trabalho



Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

Destaca-se que do percentual de servidores em teletrabalho é importante considerar que aqueles que adotam a modalidade semipresencial também dedicam um total de 20 horas semanais ao trabalho remoto. A diferença principal reside no fato de que os servidores em estação híbrida de trabalho contam com equipamentos fornecidos pela organização e suporte técnico adicional, inclusive com a possibilidade de substituir equipamentos obsoletos.

Quando a organização considera em seu plano de gestão o percentual de 50% de servidores em teletrabalho, deve observar que dos 25% dos servidores na modalidade semipresencial, alguns também exercem suas atividades em teletrabalho em determinados momentos. Isso implica que algumas ameaças já consideradas na pesquisa também se aplicam a esse percentual. Vale ressaltar que ao cruzar os índices associados ao termo "teletrabalho" no critério ameaça, na análise de conteúdo, com a quantidade de respondentes que atuam nessa modalidade de trabalho, confirma-se a importância de observar com maior cuidado as questões de suporte e treinamento dos servidores em teletrabalho por parte da organização.

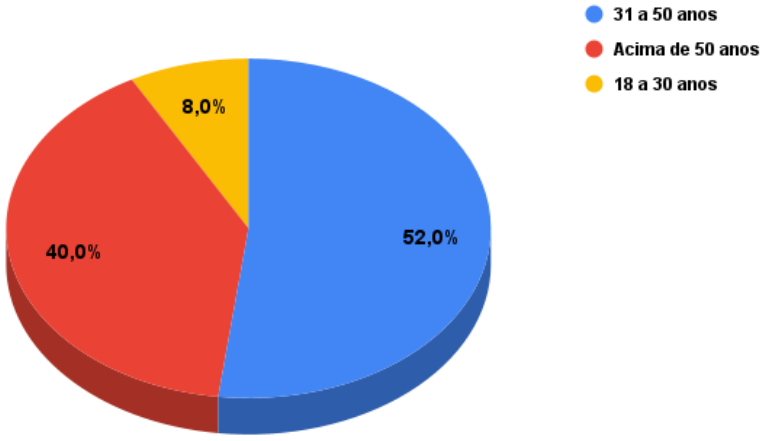
Na questão 3 foi solicitado que os respondentes selecionassem o tempo de serviço na PU/SE. A pergunta foi formulada com o intuito de traçar na análise do marco temporal de implantação do SAPIENS AGU no ano de 2012. Os resultados apontaram para um percentual de 80% dos servidores com mais de 10 anos de tempo de serviço e 20% com até 5 anos. Esse cenário indica que a grande maioria dos respondentes estão na PU/SE muito antes da implantação dos sistemas informatizados e, certamente, acompanharam toda a transformação tecnológica com a chegada da internet conforme observado graficamente:

Os usuários que participaram desta pesquisa trouxeram não apenas suas percepções, mas também uma rica bagagem de experiência e perspectivas pessoais. Isso confere uma maior validade a esta pesquisa, uma vez que eles vivenciaram na prática, os desafios das transformações tecnológicas e continuam a enfrentar novos desafios. Enquanto esta pesquisa atinge seu ponto culminante, é relevante destacar que está em andamento a implementação do "Super SAPIENS". Esse sistema já foi implantado com êxito na PGU em Brasília e possui datas programadas para ser implementado nas Procuradorias Regionais da União.

A ênfase na faixa etária, conforme abordado na questão 4, teve como objetivo investigar a possível influência da idade nas percepções dos participantes e como ela pode contribuir para a pesquisa.

A análise da amostra revelou que 52% dos respondentes estão na faixa etária entre 31 e 50 anos, seguidos por 40% com mais de 50 anos, enquanto apenas 8% têm entre 18 e 30 anos. É importante notar que os terceirizados, em sua maioria, pertencem ao grupo mais jovem, enquanto os demais participantes têm idade superior a 30 anos.

Gráfico 2 – Faixa etária dos participantes da pesquisa



Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

As distintas faixas etárias proporcionaram uma visão mais abrangente do perfil dos respondentes, que representam uma amostra real da pesquisa. Isso nos permitiu considerar as experiências de vida, as disparidades entre gerações e as idades dos entrevistados. Esse contexto enriqueceu a interpretação dos resultados, fornecendo insights preciosos sobre como grupos de diferentes idades percebem e lidam com os desafios da segurança da informação.

A análise revela que a maioria dos usuários é composta por servidores que estão próximos da aposentadoria, abrangendo aproximadamente 40% do grupo. Os restantes 52% demonstram possuir maturidade e considerável experiência profissional. No que se refere à

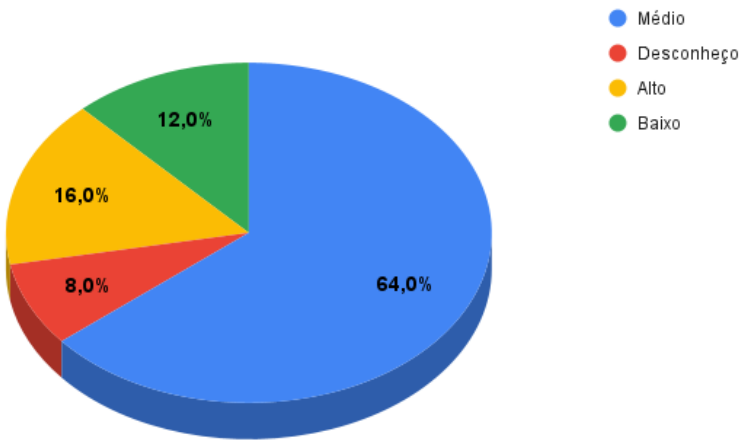
percepção de segurança da informação, esses dois grupos desempenharam um papel ativo na adoção de mudanças tecnológicas.

Ao combinar esse perfil com a discussão anterior sobre o tempo de serviço, torna-se evidente que praticamente todos os servidores estiveram envolvidos desde a implantação do Sapiens, indicando um notável grau de expertise em relação ao sistema e suas evoluções.

As questões de 5 a 9 da pesquisa analisaram as pessoas habilitadas pela administração para acessar os ativos de informação da PU/SE, identificando esses indivíduos como usuários e explorando como eles desempenham papéis de destaque nas ações relacionadas à segurança da informação.

Na questão 5 perguntou-se qual o nível de entendimento sobre o tema segurança da informação. O gráfico 3 representa os índices identificados pelas respostas.

Gráfico 3 – Nível de entendimento sobre segurança da informação



Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

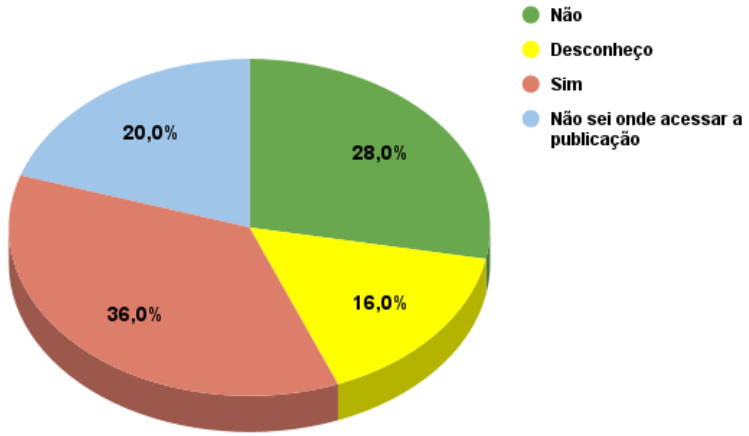
No que diz respeito ao nível de entendimento sobre segurança da informação é notável que a maioria dos participantes, representando 64%, relatou ter um conhecimento médio, o que se destacou em relação aos demais níveis. Aqueles que indicaram possuir um alto nível de conhecimento foram ligeiramente superiores aos que apontaram um conhecimento baixo. Surpreendentemente, 8% admitiram não ter qualquer conhecimento sobre o tema segurança da informação.

Essas respostas são de grande relevância, principalmente ao considerar que, ao analisar os dados qualitativos, ficou evidente que a maior preocupação dos respondentes se concentra nas ameaças de ataques cibernéticos por vírus, juntamente com a percepção de falta de preparo.

Certamente, esses dados não refletem necessariamente uma falta de conhecimento, mas sim um ponto crítico relacionado à sensação de insegurança que leva a maioria dos participantes da pesquisa a se classificarem majoritariamente como tendo um conhecimento mediano.

Ainda no mesmo bloco de perguntas a questão 6 perguntou se os participantes conheciam as normas de segurança da informação preestabelecidas pela AGU. Conforme o gráfico 4, pode-se comentar:

Gráfico 4– Conhecimentos sobe as normas de segurança da informação estabelecidas pela AGU



Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

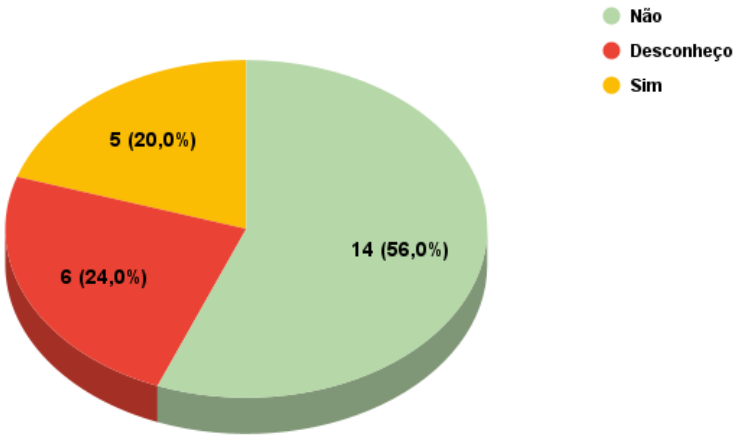
Essa pergunta foi formulada para investigar o nível de interesse dos servidores em se familiarizarem com as normas institucionais relacionadas à política de informação. Ela visou, sobretudo, determinar se os servidores estavam cientes de onde localizar essas informações ou se admitiam não saber como acessá-las. Como já discutido na questão de percepção pela análise de conteúdo eles identificam que as dúvidas e a denúncia de possíveis ameaças de falhas na segurança da informação não estão devidamente padronizadas e nem orientadas quanto aos procedimentos. Nessa questão encontramos dentro de uma margem de mesmo percentual a opção de não saber onde encontrar X não conhecer, 36% afirmam que conhecem as normas preestabelecidas pela AGU e 28% não as conhecem.

Ao afirmar que não conhecem, cruzando as análises qualitativas e quantitativas, é possível identificar que os servidores não têm conhecimento de um canal formal por meio do qual possam informar incidentes de segurança da informação. Além disso, eles desconhecem onde acessar, caso exista, um diretório ou base de dados em que estão consolidadas as normas preestabelecidas pela organização. Ocasionalmente, recebem informações sobre procedimentos de mudança de senha e a opção para solicitar MFA, por meio de e-mails circulares enviados

pela DTI, que opera em Brasília. No entanto, não há discussão local, suporte ou treinamento relacionados a essas questões.

Na questão 7 foi perguntado se a instituição já promoveu algum treinamento ou capacitação sobre a segurança da informação. A grande maioria, 56% foi incisiva sobre a negativa e 24% desconhece sobre o fato, contudo, 20% aponta que já houve treinamento (Gráfico 5).

Gráfico 5 – Promoção de treinamento ou capacitação sobre segurança da informação



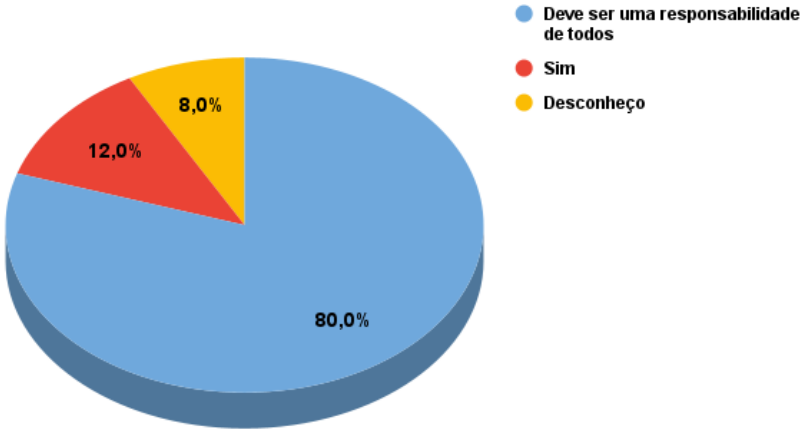
Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

Para melhor esclarecimento, a ESAGU tem promovido ciclos de treinamentos voltados para as áreas administrativa e jurídica, conhecidos como "Trilhas de Capacitação". No entanto, ao investigar a existência de treinamentos específicos relacionados ao escopo desta pesquisa foi identificado apenas um curso com duração de 19 horas-aula, composto por sete vídeos sobre "Direito e Proteção de Dados: Marco Legal da Proteção de Dados - LGPD".

Não foram identificados outros cursos relacionados a essa temática no último trimestre. No contexto desta pesquisa, não foi possível encontrar qualquer local onde a PGSI estivesse disponível para acesso e esclarecimento. Além disso, no que diz respeito à conscientização e ao treinamento, não foram identificadas ações ou iniciativas relacionadas a esses aspectos.

A questão 8 do questionário indaga: "Em sua percepção, a segurança da informação no âmbito da AGU compete exclusivamente à DTI, departamento responsável pela segurança de rede e sistemas de informação, em casos de possível ocorrência de risco?" Esta pergunta objetivou entender como os servidores percebem suas responsabilidades e seu papel colaborativo em relação à DTI, no contexto da segurança da informação na AGU (Gráfico 6).

Gráfico 6 – Percepção da segurança da informação e competências da DTI



Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

De acordo com as respostas foi possível identificar, de forma positiva, que 80% das respostas demonstram que a responsabilidade deve ser de forma colaborativa e coordenada com a DTI. Observou-se um percentual de 12% atribuindo as responsabilidades para a DTI e 8% desconhecem.

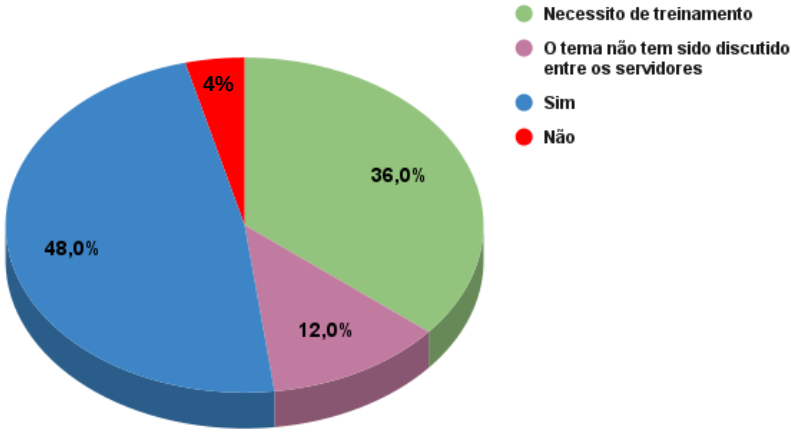
Na análise realizada, fica evidente que existe um espaço valioso para o fortalecimento da comunicação entre a DTI e os usuários dos sistemas. Acredita-se firmemente que, ao promover um diálogo mais aberto e contínuo, será possível conceber e executar ações direcionadas com ainda mais eficácia, especialmente voltadas para a promoção de boas práticas entre os usuários, tornando a segurança da informação um objetivo compartilhado e amplamente compreendido.

Conforme previamente abordado no contexto da análise SWOT, a necessidade premente de salvaguardar e valorizar a integridade dos sistemas diante das ameaças cibernéticas é uma prioridade inegável para o DTI. No entanto, não se trata somente de proteger os sistemas, mas também de estabelecer um compromisso genuíno com a promoção de uma cultura de cibersegurança em toda a organização.

Nesse sentido, é vital reconhecer a importância de priorizar a conscientização das ameaças e incentivar a adoção de boas práticas por parte dos usuários. Afinal, as lacunas que podem surgir entre os sistemas e os seus utilizadores são, muitas vezes, os pontos fracos que os adversários cibernéticos exploram.

Na questão 9, foi perguntado aos usuários sobre como percebiam seu próprio comportamento em relação às práticas de segurança da informação na organização, cujos resultados podem ser visualizados no Gráfico 7.

Gráfico 7 – Percepção dos usuários sobre segurança da informação

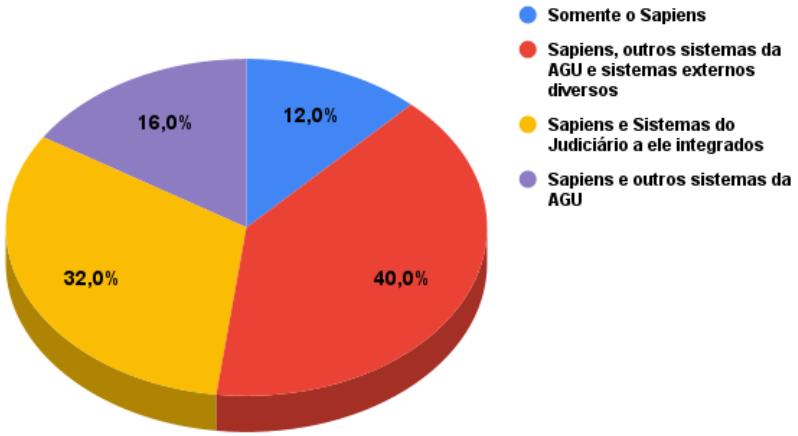


Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

A grande maioria, cerca de 48%, considerou que tinha um comportamento seguro, enquanto 36% reconheceram a necessidade de treinamento. Observou-se que 12% afirmaram que o tema não estava sendo discutido na organização, o que foi um indicativo importante para investigações futuras. Apenas 4% identificaram que possuíam um comportamento não seguro. Vale ressaltar que o treinamento emergiu na análise qualitativa como uma necessidade evidente, reforçando sua importância na promoção da segurança da informação na organização.

No bloco das questões de 10 a 18 foi analisada a postura de segurança cibernética proativa dos usuários quanto ao uso de sistemas de informação. A princípio, na Questão 10 foi perguntado: quais sistemas de informação internos e externos ao órgão utiliza, em média, para executar as suas tarefas? As respostas estão representadas no gráfico 8.

Gráfico 8 –Sistemas de informação internos e externos ao órgão utilizados para executar as tarefas



Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

O uso dos sistemas é um indicativo significativo para traçar o perfil da postura que os servidores devem adotar para proteger os dados e controlar o acesso. Esse perfil é especialmente relevante ao lidar com sistemas externos, sincronizados ou não com o SAPIENS, pois pode fornecer informações valiosas à organização sobre como aprimorar ou adaptar as boas práticas e ações de segurança contra ameaças.

Na pesquisa, observou-se que a maioria dos servidores, representando 40% dos respondentes, desempenha o papel de usuários do sistema SAPIENS, bem como de outros sistemas da AGU e sistemas externos do judiciário. Enquanto isso, 32% dos participantes relataram acessar apenas o SAPIENS e os sistemas do judiciário. É importante ressaltar que esses sistemas adicionais são necessários para fornecer dados à PU/SE, muitas vezes não relacionados estritamente a assuntos jurídicos. O pequeno percentual que somente acessa o SAPIENS é composto de colaboradores terceirizados, correspondendo a 12% do estimado.

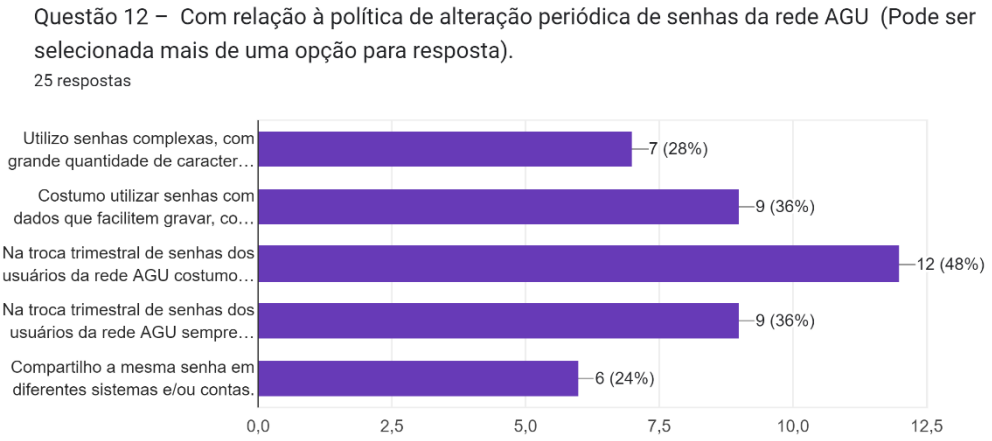
Como mencionado anteriormente, alguns sistemas estão interligados, permitindo a sincronização e acesso com o uso de token. Entretanto, sistemas cruciais como os do JEF e sistemas da Justiça do Trabalho requerem senhas autorizadas. Adicionalmente, devido à diversidade de sistemas em diferentes estados, os usuários acabam tendo que criar múltiplas senhas. Essa questão das senhas como uma possível ameaça já foi destacada anteriormente no contexto das ameaças, o que reforça a importância de analisar o perfil dos usuários.

Na questão 11, a pesquisa examinou o tempo diário que os participantes dedicam a acessar sistemas de informação online para suas atividades profissionais. A média encontrada foi de 8 horas diárias, o que é considerado ergonomicamente apropriado. No entanto, 16% dos respondentes admitiram passar de 8 a 12 horas diárias, o que excede o tempo ideal. Essa situação suscita preocupações relacionadas à fadiga mental e física, especialmente no contexto do teletrabalho, o que pode aumentar a ocorrência de erros, incluindo questões de segurança da informação. Portanto, é fundamental considerar o impacto de uma carga horária extensa nos sistemas de informação.

Devido ao grande número de servidores em teletrabalho não é possível afirmar se estão sendo realizadas as pausas regulares a cada 60 a 90 minutos de uso contínuo dos sistemas de informação, nem se seus ambientes de trabalho são ergonomicamente adequados para reduzir o risco de lesões musculoesqueléticas. Portanto, além das pausas, a configuração correta do local de trabalho desempenha um papel importante na promoção da saúde e do conforto durante o uso dos sistemas de informação. Esse é um aspecto que necessita de mais estudos no contexto organizacional.

Retornando ao elemento senha, na questão de número 12, foi perguntado sobre a política de alteração periódica de senhas da Rede AGU. Dando-se a opção de múltipla escolha aos respondentes identificou-se os seguintes comportamentos (Gráfico 9).

Gráfico 9 – Percentual sobre comportamento de alteração periódica de senhas da rede AGU



Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

Quando se trata de segurança e uso de senhas para acessar o sistema, a análise revela uma situação alarmante. Cerca de 48% dos participantes, aproximadamente 12 respondentes, admitiram o hábito de utilizar senhas contendo informações fáceis de memorizar, como nomes, sobrenomes, datas comemorativas e números de telefone. Além disso, cerca de 36% (9 respondentes) declararam que continuam usando senhas simplificadas, tanto nos sistemas internos quanto externos, ignorando a política de segurança da informação da AGU.

Ainda em relação aos riscos, 24%, correspondendo a aproximadamente 6 respondentes, revelaram que compartilham a mesma senha em diferentes sistemas e/ou contas. Esse comportamento é particularmente preocupante à luz das percepções de ameaças identificadas na análise de conteúdo mencionada anteriormente, em que a maioria dos participantes afirmou o uso de senhas de baixa segurança.

Como aspecto positivo para a organização, destaca-se que 36% das respostas indicaram que, na troca trimestral de senhas dos usuários da Rede AGU, uma nova senha é sempre adotada sem qualquer relação com a senha anterior. Esse resultado é significativo para a organização, especialmente considerando os outros 28% que afirmaram o uso de senhas complexas, compostas por um grande número de caracteres e que não contêm informações pessoais.

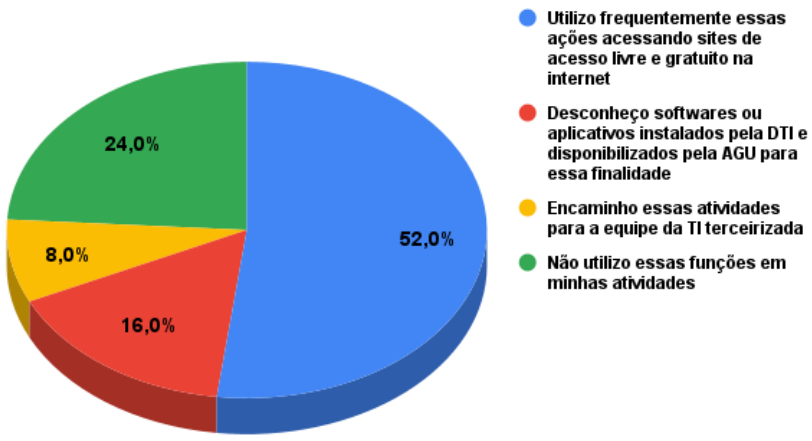
Os resultados do gráfico 6 indicam um conflito entre dois grupos de respondentes, com diferentes práticas no uso de senhas de acesso a sistemas. Isso destaca a necessidade de maior conscientização sobre o uso de senhas, não apenas na Rede AGU, mas também em outros sistemas. É importante considerar que o SAPIENS e a senha do token não exigem troca regular, enquanto a senha da Rede AGU e do e-mail institucional estão sujeitas a uma política de troca trimestral. Essa questão está intimamente relacionada com a conscientização dos usuários sobre boas práticas de segurança da informação.

Na questão 13, os participantes foram questionados se já haviam identificado e-mails suspeitos em suas contas de e-mail corporativo, como *phishing*, spam, ou distribuição de programas maliciosos. Os resultados mostram que 72% apagaram esses e-mails imediatamente, 24% nunca receberam tais e-mails, 16% receberam e não souberam como reportar e 12% informaram à DTI ou a seus coordenadores administrativos.

Mais uma vez, observa-se que os dois maiores índices confirmam a ausência de uma política que atribua a devida importância a essas ocorrências de hiperlinks maliciosos, que por vezes conseguem burlar o sistema de segurança. Torna-se, portanto, emergente a criação e divulgação de um canal de comunicação e denúncia para possíveis ameaças identificadas pelos usuários. Acredita-se que é fundamental ouvir o usuário para que ele possa desempenhar seu papel colaborativo dentro da organização.

A questão 14 analisa os riscos considerando o quesito das normas de segurança da informação, questionando se o usuário utiliza algum aplicativo ou site para implementar algumas ações como compactar, juntar e dividir arquivos a serem inseridos no SAPIENS. Os resultados podem ser visualizados no gráfico 10.

Gráfico 10 – Uso de aplicativos ou site de acesso livre e gratuito na internet



Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

O gráfico mostra que 52% dos participantes afirmaram usar ações de acesso a sites livres e gratuitos na internet como suporte ao trabalho. Por outro lado, 24% não fazem uso dessas ações, 16% desconhecem software ou aplicativos instalados oficialmente pela DTI/AGU que oferecem esses serviços, e 8% relatam delegar essas atividades à equipe de TI terceirizada.

A pesquisa revela que na AGU, especialmente em relação aos documentos digitalizados no SAPIENS, existem normas comuns e bem estabelecidas, como a limitação de tamanho de arquivo para 10 MB (megabytes). Por outro lado, em outros sistemas, como o protocolo eletrônico da Justiça Federal, a capacidade máxima de recebimento de arquivos é ainda mais restrita, limitada a 2 MB.

Mesmo arquivos zipados precisam ser descompactados para atender ao limite de tamanho permitido no sistema, antes de serem anexados. Além disso, é importante notar que em comunicações enviadas por e-mail com solicitações de subsídios, às vezes, há restrições de tamanho de arquivo que precisam ser consideradas.

Os resultados em percentagens mostram que muitos participantes da pesquisa utilizam sites ou softwares gratuitos para comprimir arquivos, uma vez que não há um site oficialmente disponível para uso dos servidores da PU/SE e na AGU para essa finalidade.

O risco de acessar sites livres e gratuitos na internet para comprimir arquivos está relacionado à possível exposição a ameaças de segurança. Sites desconhecidos ou não confiáveis podem usar serviços de compressão como uma maneira de distribuir *malware* e vírus. Ao enviar arquivos sensíveis para esses sites existe o risco de comprometer a segurança dos dados, incluindo informações sensíveis e sistemas.

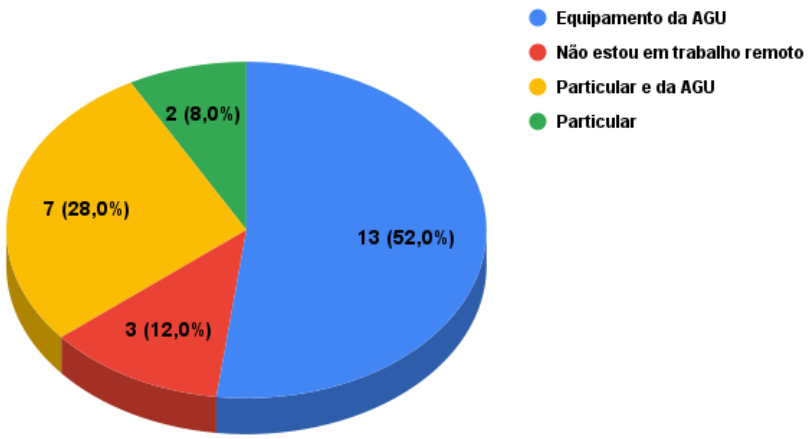
Na questão 15, discutiu-se a propriedade dos equipamentos tecnológicos utilizados em teletrabalho para a realização das atividades, ressaltando a preocupação com o suporte técnico para equipamentos pessoais, como discutido na análise de conteúdo.

A modalidade de trabalho em si não está diretamente ligada ao aumento dos riscos de segurança da informação. No entanto, é importante destacar que o investimento em segurança da informação, geralmente é uma responsabilidade da organização e pode não ser equiparado às condições financeiras individuais dos servidores, que podem não ter os mesmos recursos para manter seus equipamentos pessoais em conformidade com os padrões de segurança da organização. Isso pode criar discrepâncias na segurança da informação que precisam ser gerenciadas adequadamente.

A pesquisa indicou que, entre os participantes, 52% utilizam equipamentos do patrimônio da AGU, 28% utilizavam equipamentos tanto da AGU quanto particulares,

enquanto 12% dos respondentes estavam trabalhando presencialmente e, portanto, utilizavam os equipamentos da AGU. (Gráfico 11).

Gráfico 11 – Propriedade dos equipamentos tecnológicos utilizados em teletrabalho



Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

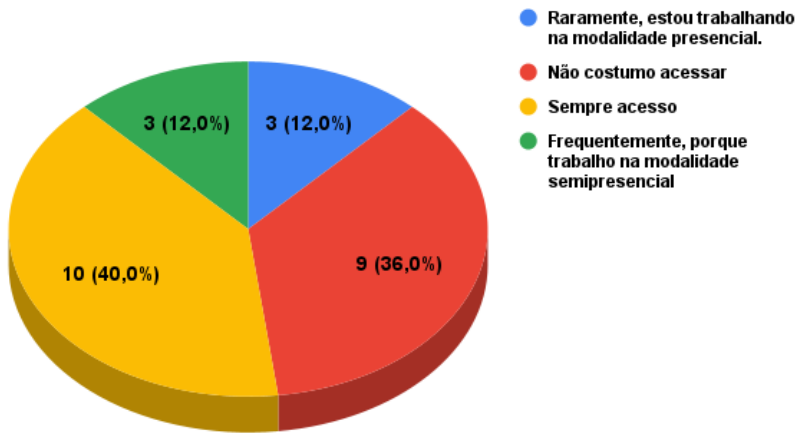
No entanto, é importante enfatizar que a organização está atualmente em processo gradual de recuperação de seus equipamentos patrimoniados, seguindo o cronograma estabelecido em seu plano de gestão, com o objetivo de finalizar esse processo até o final de 2023. Isso implica que, a partir desse ponto, todos os custos relacionados ao suporte tecnológico e equipamentos serão de responsabilidade financeira dos servidores em teletrabalho, de acordo com a determinação da organização.

Até o momento desta análise não foram realizadas discussões sobre as condições tecnológicas e estruturais dos servidores para garantir que o teletrabalho esteja em conformidade com os padrões mínimos de ergonomia, equipamentos e ferramentas necessárias para fortalecer a segurança da informação dos sistemas e ativos informacionais da AGU. É possível que essa questão se torne mais relevante após a conclusão do processo de devolução dos equipamentos patrimoniados, o que pode resultar em um diálogo mais direto com a gestão para abordar esse tema.

Nesse sentido, é fundamental considerar a importância de assegurar que os servidores tenham acesso a recursos tecnológicos adequados para realizar suas atividades de forma segura, especialmente no contexto do teletrabalho, em que a responsabilidade pela infraestrutura pode recair em parte sobre o servidor. Portanto, é imprescindível que haja um acompanhamento contínuo das condições tecnológicas e ergonômicas para apoiar a segurança da informação e o bem-estar dos servidores.

Na questão 16, investigou-se se os participantes da pesquisa têm o costume de acessar os sistemas de informação corporativos por meio de dispositivos pessoais, como celulares e notebooks, fora do ambiente institucional, independentemente da modalidade de trabalho (presencial, semipresencial ou teletrabalho). Os resultados dessa prática são apresentados no Gráfico 12.

Gráfico 12 – Acesso aos sistemas de informação corporativos em dispositivos particulares



Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

Observou-se que 40% dos usuários sempre acessam os sistemas de informação corporativos em dispositivos tecnológicos particulares, seguidos por 36% que não costumam acessar. Em igual proporção, 12% dos usuários acessam sempre e outros o fazem frequentemente, justificando essa prática pela necessidade surgida a partir da modalidade de trabalho semipresencial. O objetivo dessa questão foi obter uma visão quantitativa dessa prática e, com ela, identificar indicativos de riscos, principalmente relacionados às vulnerabilidades que podem surgir em dispositivos particulares, como o uso de redes inseguras, acesso não autorizado aos sistemas corporativos por terceiros, perda ou roubo do dispositivo, licenças expiradas de antivírus e falta de conscientização em relação às melhores práticas por parte dos usuários.

Na questão 17 foi abordado o acesso à VPN (*Virtual Private Network*), ou rede privada virtual da AGU, utilizada por alguns servidores que necessitam acessar a rede da PU/SE estabelecendo uma conexão com a rede corporativa da PU/SE, através do acesso remoto pela internet. De acordo com os resultados, observou-se que 64% dos participantes da pesquisa não usam a rede VPN, enquanto 28% confirmam que utilizam a VPN, mas com limitação de perfil, inclusive de atualização da rede e 8% afirmam que utilizam a rede local através da VPN, mas não têm conhecimento da garantia que o equipamento possui quanto à segurança da informação.

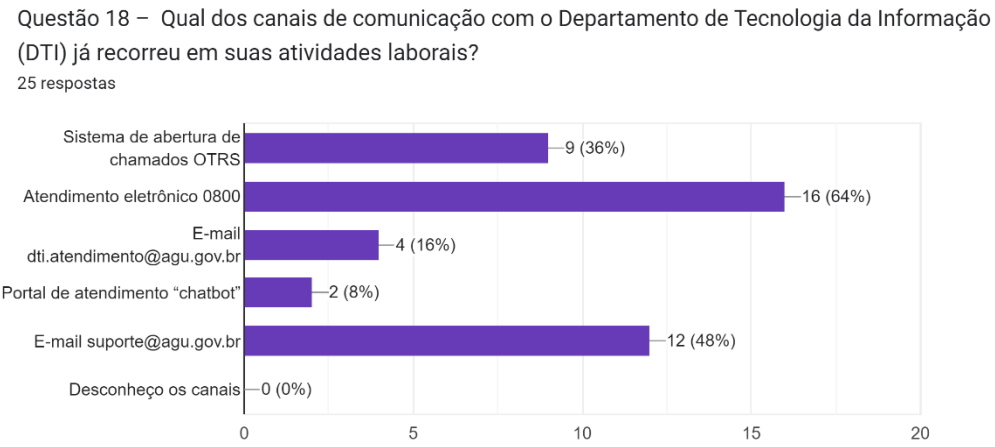
A VPN não foi muito discutida na análise qualitativa porque não houve incidências de termos sobre o tema, contudo, é uma ferramenta fundamental, especialmente para Advogados da União e gestores na AGU.

Na PU/SE, a VPN é essencial para o acesso remoto a recursos exclusivos da Rede AGU, com seu uso rigidamente controlado pela DTI. A aprovação da chefia e a assinatura de um termo de compromisso pelos servidores compõem parte desses procedimentos regulatórios. Esse termo estabelece normas para garantir a segurança dos sistemas e dados, incluindo medidas de monitoramento, auditoria, responsabilidade do servidor na manutenção da confidencialidade das credenciais e sanções administrativas, se necessário.

Os riscos estão alinhados com os de outros sistemas em relação às ameaças à segurança da informação, sendo a diferença principal a sensibilidade dos dados acessados via VPN. O equipamento com utilização de VPN, em que o usuário está conectado com a rede de trabalho, implica em que a preocupação deve ser redobrada, para evitar contaminação local e que será repassada para rede de trabalho.

Abordando a comunicação, ou cultura de segurança da informação, a questão de nº 18 explorou junto aos respondentes os canais utilizados para suporte das atividades tecnológicas junto à DTI. Perguntou-se: Qual dos canais de comunicação com o DTI já recorreu em suas atividades laborais? O resultado pode ser representado no gráfico 13.

Gráfico 13 – Principais canais de comunicação com a DTI usados como suporte



Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

O principal canal de comunicação, apontado por 64% dos respondentes, é o Atendimento Eletrônico 0800AGU, que oferece acesso à Central de Atendimento de Tecnologia da Informação e outros setores. No entanto, esse canal não se destina a dúvidas de

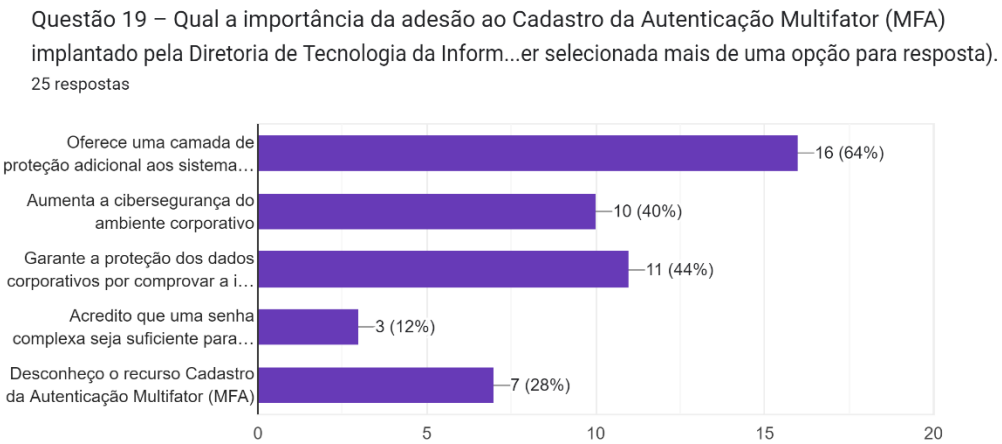
uso ou denúncias de segurança da informação, mas sim a questões logísticas, como problemas de acesso a sistemas e recuperação de senhas. O segundo canal mais utilizado é o e-mail suporte@agu.gov.br (48%), que lida com questões relacionadas à TI, como a estabilidade de sistemas, instalação de software e configurações. Esse sistema de chamados é registrado na AGU e encaminhado para a equipe terceirizada local.

Com 36% das respostas, o Sistema de abertura de chamados OTRS (*Open-source Ticket Request System*) é uma solução de gerenciamento de chamados de código aberto amplamente adotada na AGU. Ele oferece uma plataforma centralizada para registrar, monitorar e resolver questões reportadas pelos servidores, com priorização por senhas e acompanhamento das demandas.

Outro canal selecionado por 16% dos respondentes foi o e-mail dti.atendimento@agu.gov.br (16%) como um canal semelhante ao e-mail suporte@agu.gov.br, utilizado para resolver questões relacionadas ao fluxo de trabalho e problemas nos sistemas, especialmente no SAPIENS AGU. Ambos os canais desempenham funções semelhantes, mas o primeiro é um canal direto com a DTI.

Finalmente, na questão 19 perguntou-se qual a importância da adesão ao cadastro da MFA implantada pela Diretoria de Tecnologia da Informação (DTI) para segurança da informação corporativa em regime de teletrabalho ou semipresencial? As respostas estão graficamente representadas abaixo:

Gráfico 14– Importância da adesão ao cadastro da MFA



Fonte: Elaborado pela autora a partir de dados da pesquisa (2023).

Os resultados gráficos revelam que a maioria dos participantes da pesquisa reconhece os benefícios do recurso da MFA. Cerca de 64% acreditam que ele oferece uma camada adicional de proteção aos sistemas, enquanto 44% afirmam que é essencial para garantir

a segurança dos dados corporativos ao comprovar a identidade do usuário. Além disso, 40% destacam que a MFA contribui para a cibersegurança no ambiente corporativo, ressaltando aspectos positivos para a segurança da informação. No entanto, 28% dos servidores admitiram desconhecer a MFA e 12% acreditam que uma senha complexa por si só é suficiente para proteger o sistema.

Esses resultados enfatizam a importância de conscientizar os servidores sobre a utilidade e eficácia da MFA como uma medida de segurança adicional, além de promover a sua adoção para reforçar a proteção dos sistemas e dos dados corporativos.

É importante destacar que os membros da AGU que trabalham remotamente em regime de teletrabalho ou híbrido e acessam recursos como o Office 365, portais administrativos e VPN fora das instalações da AGU têm a opção de realizar voluntariamente o cadastro da MFA.

Essa análise ressalta que, embora a MFA reforce a segurança cibernética e reduza riscos como fraudes e invasões, sua ausência em normativas e a natureza voluntária de seu cadastro podem criar lacunas, como evidenciado nos gráficos explicativos.

A análise quantitativa detalhada permitiu traçar um perfil comportamental abrangente dos usuários do sistema, representados na amostra ativa desta pesquisa. Através dos dados quantitativos coletados pôde-se identificar tendências, padrões e preferências dos participantes em relação a uma variedade de tópicos relacionados à segurança da informação e ao uso de sistemas corporativos.

6.3 Validando os objetivos da pesquisa

Com base na análise de dados qualitativos e quantitativos, seguida pela triangulação dos resultados, a pesquisa proporcionou uma investigação aprofundada das principais convergências e divergências relacionadas às ameaças e às melhores práticas nos fenômenos e variáveis ligados à segurança da informação. Essa abordagem enriqueceu nossa compreensão, oferecendo uma visão mais abrangente e detalhada das complexidades inerentes a esse campo de estudo.

A análise da percepção dos usuários desempenhou um papel fundamental na obtenção de uma compreensão aprofundada de como o processo de segurança da informação era percebido em seu ambiente de trabalho na PU/SE. Através da exploração das impressões dos usuários, as principais ameaças percebidas por eles puderam ser claramente identificadas. Isso permitiu que a pesquisa não apenas fornecesse uma visão mais abrangente sobre a

percepção de segurança da informação na organização, mas também estabelecesse as bases para a proposição de medidas de aprimoramento. A coleta das visões e sugestões dos usuários para o aprimoramento desse processo complexo foi uma etapa crucial na investigação. Graças a essas análises minuciosas, o primeiro objetivo específico da pesquisa foi atingido com êxito: "investigar elementos indicadores de falhas de segurança a partir da percepção dos participantes da pesquisa propondo estratégias alternativas de gestão de segurança da informação que envolva a interface usuário, tecnologia e sistema".

Por outro lado, a análise quantitativa, fundamentada em resultados numéricos e percentagens, proporcionou uma visão sólida e objetiva do comportamento e das práticas dos usuários na PU/SE. Essa abordagem quantitativa forneceu informações concretas e mensuráveis que poderão ser utilizadas para aprimorar a segurança e a eficácia dos sistemas de informação na organização. Através do tratamento e análise dos dados obtidos, com a análise quantitativa foi possível atingir o segundo objetivo específico traçado na pesquisa: "analisar o comportamento e as atitudes dos usuários dos sistemas com relação as normas de segurança da informação preestabelecidas pela organização com o objetivo de identificar as principais circunstâncias em que ocorrem as falhas de segurança e como prevenir os incidentes".

Salienta-se, ainda, que os resultados provenientes da análise mista da pesquisa possibilitaram a identificação precisa dos incidentes de risco existentes, ao mesmo tempo que revelaram um conjunto de boas práticas que, em alguns casos, poderiam não ter sido devidamente consideradas pela organização anteriormente. Essa ampla gama de *insights* contribui de maneira significativa para o aprimoramento das estratégias de segurança da informação e para o fortalecimento da proteção de dados sensíveis no ambiente de estudo. Adicionalmente, essa abordagem enfatiza a relevância da pesquisa para o avanço do conhecimento e para a contínua melhoria das práticas de segurança da informação na PU/SE.

A triangulação das abordagens qualitativa e quantitativa desempenhou um papel fundamental na obtenção de uma compreensão abrangente e aprofundada do cenário de segurança da informação na PU/SE. Essa abordagem meticulosa permitiu atingir com êxito o terceiro objetivo da pesquisa: "mapear os principais incidentes de risco para a segurança da informação identificados através de levantamento do trabalho de campo para propor boas práticas de segurança da informação não vislumbradas pela organização".

Para ilustrar de forma abrangente os resultados da triangulação da pesquisa e o cumprimento do terceiro objetivo específico, derivado dos dois primeiros objetivos específicos, o Quadro 21 foi desenvolvido. Nesse quadro, é apresentado um mapeamento minucioso dos principais elementos identificados, representando ameaças e falhas na segurança da

informação. Além disso, são descritas as medidas de controle e as boas práticas que surgiram como resultado da intervenção realizada nesta pesquisa na PU/SE.

Quadro 21 – Mapeamento das ameaças X boas práticas em segurança da informação

MAPEAMENTO DAS AMEAÇAS, CONTROLE E BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO				
	Categorias			
Ameaças		**Boas Práticas**		
Indicadores de falhas	Ocorrências	Controle	Estratégias alternativas de segurança da informação	Atribuição
Vírus/programas maliciosos	Anexos de e-mail infectados, downloads de sites não confiáveis, dispositivos USB ou outras mídias removíveis.	Manter sistemas e aplicativos atualizados com patches de segurança e ter precaução ao abrir anexos de e-mail ou baixar arquivos de fontes desconhecidas.	Gerenciamento de senhas	Organização e usuários dos sistemas
Uso de sites livres para compressão, conversão e outras atividades de arquivos	Distribuição de malware, como vírus ou programas maliciosos, roubo de dados, uso indevido de dados e violação dos direitos e proteção dos dados.	Verificar se o site usa conexão segura (HTTPS) e evitar compartilhar informações pessoais/confidenciais em sites de terceiros. Manter um antivírus atualizado em seu dispositivo para proteção adicional	Uso de sites confiáveis e manter um antivírus atualizado.	Organização e usuários dos sistemas
Indicadores de falhas	Ocorrências	Controle	Estratégias alternativas de segurança da informação	Atribuição
Senhas	Senhas fracas, compartilhamento ou falta de atualização podem comprometer a segurança dos sistemas.	Desenvolver políticas de senhas com requisitos de complexidade, comprimento, expiração e diretrizes para os usuários.	Gerenciamento de senhas.	Organização e usuários dos sistemas
Treinamento	Golpes de *phishing*, instalação de *malware*, vazamento de informações confidenciais.	Capacitar os funcionários a reconhecer e mitigar ameaças cibernéticas, com práticas seguras e conscientização.	Treinamento contra ameaças cibernéticas e uso seguro dos sistemas.	Organização
Falta de comunicação de incidentes cibernéticos	Pode abranger diversos tipos de incidentes, desde violações de dados até *malware*, *phishing*, intrusões, fraudes e muito mais.	Estabelecer um canal de incidentes bem divulgado, de fácil acesso, seguro, confidencial e com processos de resposta bem definidos.	Disseminação e conscientização do uso de um canal de incidentes.	Organização e usuários dos sistemas

(Conclusão do quadro 21).

Suporte técnico em teletrabalho em dispositivos pessoais	Perda de dados confidenciais, roubo de informações críticas ou comprometimento da rede.	Garantir aos dispositivos pessoais dos servidores o mesmo nível de proteção de segurança do existente nos equipamentos da organização.	Suporte técnico abrangente para o teletrabalho, independentemente da propriedade dos dispositivos utilizados.	Organização
Conscientização	A ausência de consciência dos riscos de segurança da informação torna sistemas e redes digitais mais vulneráveis a ameaças e ataques cibernéticos.	Manter uma cultura dialógica e pesquisas sobre o perfil de risco e adoção de medidas de segurança mais eficazes.	Promover uma cultura de segurança cibernética.	Organização e usuários dos sistemas

Fonte: elaborado pela autora a partir dos dados da pesquisa (2023).

O mapeamento das ameaças, controles e melhores práticas de segurança da informação desempenhou um papel central e essencial na análise e nos resultados desta pesquisa. Podemos compará-lo figurativamente ao coração do estudo, uma vez que foi concebido com base nos dois primeiros objetivos específicos, que delinearam o perfil do comportamento dos usuários investigados no estudo e a percepção que eles tinham em relação à segurança da informação. Essa abordagem concedeu o devido protagonismo aos usuários. Assim, o mapeamento se revelou como a base sólida sobre a qual construímos um entendimento mais profundo das questões de segurança da informação, oferecendo uma estrutura sólida para futuras melhorias e estratégias.

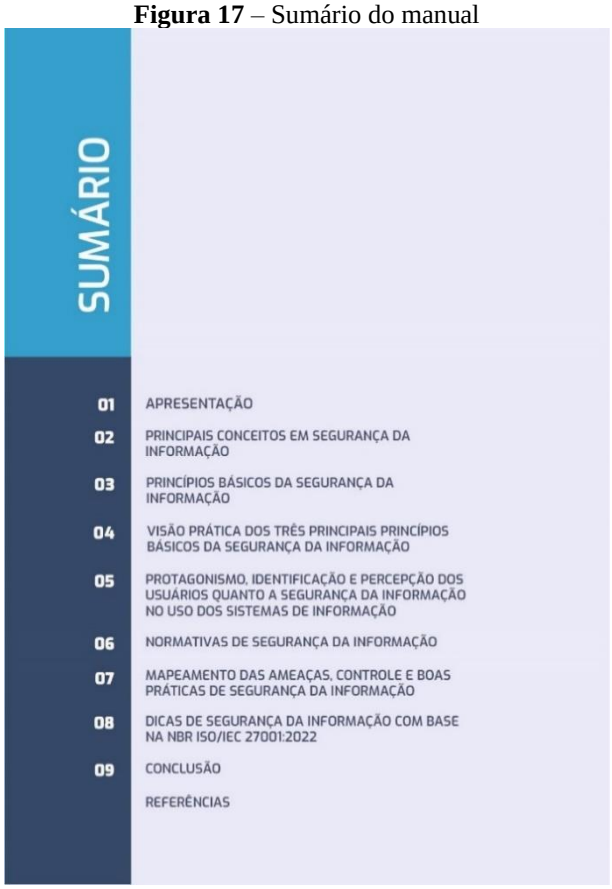
O mapeamento, assim, proporcionou uma representação completa do fenômeno da segurança da informação, abordado de maneira científica e holística. Além disso, essa análise teve um caráter intervencionista, contribuindo para uma compreensão mais profunda e objetiva do tema em questão. Isso permitiu que os objetivos da pesquisa fossem alinhados e validados por meio da criação de um produto educacional, o “Manual de Boas Práticas de Segurança da Informação”, que consolidou os resultados obtidos.

7 PRODUTO DA INTERVENÇÃO

Com base nos resultados desta pesquisa e no alcance dos objetivos estabelecidos, foram obtidos elementos substanciais respaldados por um embasamento técnico fundamentado nas contribuições teóricas e científicas. Esses elementos emergiram da triangulação dos dados qualitativos e quantitativos, que foram devidamente tratados e analisados, combinados ao referencial teórico que norteou a pesquisa.

Por ser um produto acadêmico e, ao mesmo tempo, técnico-científico, o manual foi organizado em diversos capítulos resumidos de maneira clara e concisa. Ele incorpora fundamentos teóricos, mas acima de tudo, busca utilizar uma linguagem acessível que seja compreensível por uma ampla variedade de usuários, não apenas na PU/SE, mas também em outras organizações. (Figura 17).

Figura 17 – Sumário do manual



Fonte: elaborado pela autora (2023).

Conforme o resumo do manual evidenciado na figura 17, sua estrutura inicial incorpora uma introdução meticulosamente elaborada com o propósito de aprimorar a compreensão do conteúdo do documento, delineando com clareza seus objetivos e sua finalidade. Essa abertura introdutória não apenas fornece uma visão abrangente do que os

leitores podem antever ao longo do manual, mas também enfatiza sua relevância, visando instigar e motivar os leitores a imergirem no conteúdo e a aplicá-lo de maneira proveitosa.

O segundo capítulo abordou os principais conceitos em segurança da informação, os quais funcionaram como um ponto de partida para os leitores, fornecendo uma base sólida e necessária em relação aos fundamentos da segurança da informação. Essa base foi essencial, por ser imprescindível uma compreensão clara dos conceitos subjacentes à segurança da informação e sua importância, sendo um desafio motivar e envolver os leitores na adoção das medidas recomendadas à época em que o manual foi elaborado.

O terceiro capítulo, que abordou os princípios básicos da segurança da informação, desempenhou um papel central e indispensável em um manual de boas práticas. Nesse capítulo, foram estabelecidas as bases sólidas necessárias para a compreensão, orientação estratégica e aplicação prática da segurança da informação. O capítulo explorou os três pilares que compuseram os princípios fundamentais da segurança da informação, os quais serviram como o alicerce essencial desse campo.

Esses pilares orientaram o desenvolvimento de políticas, práticas e tecnologias destinadas a proteger os ativos de informação contra ameaças e riscos. Ao internalizar e compreender profundamente esses princípios, as organizações e profissionais puderam forjar estratégias de segurança mais eficazes e adaptáveis às necessidades específicas de suas operações. Isso resultou na promoção de um ambiente que valorizou e priorizou a segurança e integridade dos dados críticos, contribuindo para a proteção contínua e eficiente da informação.

No quarto capítulo, após a discussão anterior, foi apresentada a visão prática dos três principais princípios básicos da segurança da informação, seus objetivos, indicadores de alerta, causas de ameaças e ações para manter a integridade, confidencialidade e disponibilidade da informação, com foco na segurança da informação prática e acionável.

No quinto capítulo, enfocando o protagonismo, identificação e percepção dos usuários em relação à segurança da informação ao utilizar os sistemas de informação, discute-se o papel fundamental dos usuários como protagonistas. Identifica-se quem são esses protagonistas e, com base nos dados analisados na pesquisa da autora, apresenta-se de maneira concisa a percepção dos usuários sobre a segurança da informação no uso dos sistemas de informação.

O sexto capítulo ofereceu uma análise das normativas de segurança da informação, destacando particularmente a família ISO 27000 e as normas correlatas relacionadas à segurança da informação.

O capítulo mais significativo e de maior relevância foi o sétimo, uma vez que desempenhou um papel central na compreensão da segurança da informação. Esse capítulo ofereceu um profundo mergulho no mapeamento das ameaças, nos controles essenciais e nas melhores práticas que constituem a base para garantir a segurança da informação. Vale ressaltar que essa análise foi rigorosamente fundamentada nos resultados empíricos da pesquisa realizada, consolidando assim, a validade e a aplicabilidade prática das conclusões na época em que o manual foi elaborado.

Nesse capítulo, destacaram-se ameaças e riscos, além de oferecer um guia prático para implementar medidas de segurança da informação de forma eficaz. Essas diretrizes permitem que os leitores protejam suas informações de maneira abrangente e eficiente.

No oitavo capítulo, a autora apresentou dicas de segurança da informação que tiveram como objetivo principal fornecer aos usuários o conhecimento e as ferramentas necessárias para proteger informações vitais e manter a segurança dos sistemas, contribuindo para um ambiente mais seguro e resiliente em relação à segurança da informação. Em seguida, foram apresentadas as considerações finais e as referências, encerrando o manual.

Esse manual pode representar uma ferramenta para orientar e capacitar os usuários a adotarem práticas de segurança sólidas no ambiente de trabalho, contribuindo assim para a proteção eficaz dos ativos informacionais da PU/SE. Além disso, a pesquisa proporcionou uma compreensão mais profunda das percepções, preocupações e comportamentos dos usuários em relação à segurança da informação, destacando áreas de melhoria e conscientização necessárias para fortalecer ainda mais a postura dinâmica da equipe em relação à segurança cibernética.

Além de fornecer um diagnóstico claro e detalhado das variáveis relacionadas à segurança da informação, com foco na PU/SE, a intervenção resultou na criação de um produto: o Manual de Boas Práticas de Segurança da Informação. Este manual foi elaborado para guiar os usuários dos sistemas da organização, podendo ser ajustado para ser aplicado em diferentes ambientes institucionais, tanto em órgãos da administração pública, independentemente da esfera, quanto em setores privados.

Em termos prospectivos, o objetivo é institucionalizar o manual, impulsionado pela sua abordagem de segurança da informação e seu caráter exploratório e inovador, com a intenção de demonstrar a importância fundamental dessa iniciativa.

8 CONSIDERAÇÕES FINAIS

A pesquisa revelou um cenário que inicialmente não se imaginava ser de tamanha relevância e preocupação para os usuários dos sistemas da PU/SE em relação à segurança da informação. Surpreendentemente, não houve resistência e a intervenção foi conduzida com a plena concordância de toda a gestão.

Ao abordar os comportamentos, ameaças e controles relacionados à segurança da informação, esta pesquisa não apenas descreveu a realidade de uma organização, mas também forneceu valiosos *insights* que poderão orientar futuras intervenções e melhorias nas práticas de segurança. Essas conclusões têm como base as percepções dos próprios usuários e os perfis comportamentais identificados no estudo, oferecendo referências sólidas para orientar aprimoramentos futuros.

A análise de termos e temas emergentes ofereceu uma visão abrangente da percepção dos usuários em relação à segurança da informação na PU/SE. Essa abordagem permitiu uma compreensão holística, considerando não apenas as preocupações relacionadas às ameaças cibernéticas, mas também as sugestões de boas práticas que podem fortalecer a segurança da informação. Isso não apenas contribui para uma visão mais clara dos desafios enfrentados, mas também oferece um roteiro para ações orientadas pela experiência e perspectiva dos próprios usuários.

Ao identificar as principais preocupações dos usuários e relacioná-las com as práticas recomendadas, a pesquisa contribuiu para fortalecer a conscientização sobre a importância da segurança cibernética. Além disso, incentivou a participação dos usuários na proteção dos ativos de informação da organização. Essa interação foi fundamental para engajar os usuários no processo de desenvolvimento de melhoria da segurança da informação e também os colocarem como protagonistas e pessoas ativas com o potencial de uma contribuição significativa para a compreensão do processo de segurança da informação na PU/SE.

A pesquisa não apenas forneceu informações significativas, mas também estabeleceu as bases para a implementação de medidas mais eficazes quanto à segurança da informação e para o cultivo de uma cultura de segurança sólida na PU/SE. É incontestável que o elemento humano desempenha um papel crucial nesse contexto. A pesquisa enfatizou a importância contínua da educação e da conscientização dos usuários para enfrentar os desafios dinâmicos no campo da segurança cibernética.

Pode-se concluir que a triangulação dos resultados da pesquisa destaca a necessidade de uma abordagem abrangente em segurança da informação, a qual engloba

aspectos como comunicação eficaz, treinamento, conscientização e adoção de boas práticas. Além disso, é imperativo garantir a segurança nos ambientes de teletrabalho e no uso de equipamentos pessoais.

Em suma, os resultados desta pesquisa evidenciam a importância do conhecimento em segurança da informação, embora revelem a necessidade de aprimoramentos, sobretudo acerca da conscientização e da capacidade de lidar com as ameaças que a cada dia surgem no ambiente digital. Essas conclusões fornecem uma base sólida para a implementação de estratégias aprimoradas de segurança da informação e para o cultivo de uma cultura organizacional resiliente e vigilante em relação às ameaças cibernéticas em permanente mutação.

É fundamental estabelecer uma cultura organizacional que promova a confiança e, ao mesmo tempo, mantenha os servidores atualizados sobre os riscos. Além disso, é essencial fornecer treinamento e capacitação a todos os membros da organização, destacando a importância do protagonismo tanto como profissional da informação jurídica quanto como usuário dos sistemas. Essa abordagem contribuirá significativamente para aumentar a conscientização e preparar a equipe para enfrentar os desafios da segurança da informação, fortalecendo, assim, a postura autônoma de todos os envolvidos.

Portanto, os resultados desta pesquisa não são apenas conclusões acadêmicas, mas sim um impulso para a ação. Eles fornecem uma estrutura sólida que visa aprimorar as práticas de segurança da informação, protegendo os ativos da PU/SE das ameaças cibernéticas em um ambiente digital cada vez mais dinâmico e complexo.

Por meio desse estudo de intervenção foi possível trazer à tona algumas preocupações, muitas vezes não expressas devido as dúvidas ou hesitações na comunicação sobre o uso dos sistemas de informação. Ficou evidente, especialmente através do alto número de pedidos de treinamento, que há uma forte vontade de aprimorar o conhecimento nesse campo desafiador e emergente que é a segurança da informação na organização.

Pode-se afirmar ousadamente que existe uma fragilidade ainda mais latente do que os suportes e ferramentas direcionados à segurança dos sistemas, uma fragilidade frequentemente negligenciada: os próprios usuários. São eles que estão na linha de frente dos principais ativos da PU/SE, incluindo seus sistemas e, em especial, o principal ativo informacional, o SAPIENS AGU.

À medida que os desafios em segurança cibernética continuam a evoluir, esta pesquisa destaca a necessidade contínua de educação e preparo dos usuários para enfrentar ameaças emergentes no ambiente digital. A PU/SE pode se beneficiar ao investir na

conscientização e no empoderamento de sua equipe, fortalecendo assim uma postura proativa em relação à segurança da informação, que é uma responsabilidade compartilhada por todos.

Em última análise, esta pesquisa não se limitou a abordar os aspectos fundamentais da segurança da informação; ela também estabeleceu um caminho para promover uma cultura de segurança sólida dentro da organização. Além disso, a pesquisa proporcionou soluções práticas por meio da criação do Manual de Boas Práticas de Segurança da Informação. Portanto, os resultados desta pesquisa têm o potencial de contribuir significativamente para a melhoria da segurança da informação e a conscientização dos usuários, não apenas dentro desta organização, mas também em contextos similares.

A pesquisa não encerra questões; ao contrário, ela suscita inúmeras indagações que transformam o ambiente organizacional em um laboratório rico para explorar os fenômenos relacionados ao tema da segurança da informação e os fenômenos que o circundam. Dentro desses fenômenos, que abrangem desde a eficiente gestão dos dados organizacionais até a preservação da integridade da informação em face de incidentes cibernéticos, ética na informação, segurança de software e técnicas contra ameaças digitais, há uma intrincada rede de comunicação. Essa rede tem como foco primordial resguardar as informações de organizações ou indivíduos contra acessos não autorizados, alterações indevidas e indisponibilidade.

Recomenda-se promover uma abordagem mais colaborativa entre usuários, sistemas e tecnologia, com o objetivo de assegurar a integridade, confidencialidade e disponibilidade dos dados. Essa iniciativa reconhece a importância vital de proteger informações sensíveis e garantir o funcionamento seguro e contínuo dos sistemas, destacando a necessidade de uma cooperação efetiva entre os diversos elementos envolvidos.

Sugere-se uma investigação mais aprofundada voltada para a CI, focando nos usuários de sistemas de informação, mediação da informação, gestão de dados, GC, GD, GI, especialmente em relação aos sistemas de informação e SIGAD. Propõe-se também explorar temas emergentes no contexto do problema de pesquisa abordado.

Ao finalizar esse trabalho é essencial destacar um conselho fundamental: Desconfiança, vigilância, senso crítico e prevenção são pilares na proteção da informação, tanto pessoal quanto organizacional, em um mundo digital repleto de ameaças. Esse trabalho serve como um aprendizado de que a segurança da informação não é uma responsabilidade de poucos, mas sim de todos. Ela demanda atenção constante e ação proativa para evitar incidentes de segurança e proteger os ativos digitais valiosos.

REFERÊNCIAS

ALCOFORADO, Ivan. Prefácio. *In:* SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

ALENCAR, Thayane; ARAÚJO JÚNIOR, Rogério Henrique de. Estudo das necessidades informacionais dos usuários de sistemas informatizados de gestão arquivística de documentos como subsídio para o planejamento estratégico. **Ágora: Arquivologia em debate**, Florianópolis, v. 32, n. 64, p. 01-24 jan./jun. 2022. Disponível em: https://agora.emnuvens.com.br/ra/article/view/1052/997. Acesso em: 20 set. 2022.

ALMEIDA, Jobson Louis Santos de; PERUCCHI, Valmira; FREIRE, Gustavo Henrique de Araújo. Ciência-ação em ciência da informação: um método qualitativo em análise. **Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação**, Florianópolis, v. 25, p. 01-24, 2020. Disponível em: https://brapci.inf.br/index.php/res/download/134555. Acesso em: 20 jun. 2022.

ALMEIDA, Maria Fabiana Izídio de; BIAGGI, Camila de; VITORIANO, Marcia Cristina de Carvalho Pazin. Identificação dos fluxos informacionais: contribuições para a gestão do conhecimento. **Ágora: Arquivologia em Debate**, Florianópolis, v. 31, n. 63, p. 01-11, jul./dez. 2021. Disponível em: https://agora.emnuvens.com.br/ra/article/view/994. Acesso em: 13 ago. 2022.

ALMEIDA, Maurício Barcellos. Memória organizacional: como as organizações armazenam e recuperam informações para fins de gestão. *In:* OLIVEIRA, Eliane Braga de; RODRIGUES, Georgete Medleg (org.). **Memória:** interfaces no campo da informação. Brasília: Editora UNB, 2017. p. 215-247

ANDRADE, Karla Soares. **Sistema de Mídia Indoor e Informativo AGU Brasil**: os canais de comunicação interna da Advocacia-Geral da União. 2016. 56 f. Monografia (Curso de Pós-Graduação Latu Sensu em Gestão da Comunicação nas Organizações) – Centro Universitário de Brasília, Brasília: UNICEUB, 2016. Disponível em: https://repositorio.uniceub.br/jspui/handle/235/11927?mode=full. Acesso em: 12 jul. 2022.

ANDRADE, Robéria de Lourdes de Vasconcelos; ANDRADE, Wendia Oliveira de. Usuários da informação: sujeitos perfilados com base na ciência da informação. **Revista Conhecimento em Ação**, Rio de Janeiro, v. 1, n. 1, jan./jun. 2016. Disponível em: https://revistas.ufrj.br/index.php/rca/article/download/2875/2788. Acesso em: 20 jun. 2022.

ANDRADE, Rui Otávio Bernardes de Andrade; AMBONI, Nério. **Estratégias de gestão**: processos e funções do administrador. Rio de Janeiro: Elsevier, 2010. 272 p.

ARAÚJO, Carlos Alberto Àvila. Paradigma social nos estudos de usuários da informação: abordagem interacionalista. **Informação. & Sociedade: Estudos**, João Pessoa, v.22, n.1, p. 145-159, jan./abr. 2012. Disponível em: https://periodicos.ufpb.br/ojs/index.php/ies/article/view/9896. Acesso em: 25 nov. 2022.

ASSIS, Wilson Martins de. **Gestão da informação nas organizações**: como analisar e transformar em conhecimento informações captadas no ambiente de negócios. Belo Horizonte: Autêntica, 2008. 182 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27000 de 11/2022**: segurança da informação, segurança cibernética e proteção à privacidade - sistemas de gestão da segurança da informação – requisitos. Rio de Janeiro: ABNT, 2022. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/25074/abnt-nbriso-iec27001-tecnologia-da-informacao-tecnicas-de-seguranca-sistemas-de-gestao-da-seguranca-da-informacao-requisitos. Acesso em: 12 dez. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**:**2022**. Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2022. Disponível em: https://www.abntcatalogo.com.br/grd.aspx. Acesso em: 20 set. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002**:**2022** Tecnologia da informação-Técnicas de segurança-Código de prática para a gestão da segurança da informação (Conteúdo técnico idêntico ao da ABNT NBR ISO/IEC 17799). Rio de Janeiro: ABNT, 2022. Disponível em: https://www.target.com.br/produtos/normas-tecnicas/36572/nbriso-iec27002-seguranca-da-informacao-seguranca-cibernetica-e-protecao-a-privacidade-controles-de-seguranca-da-informacao. Acesso em: 20 set. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27003:** tecnologia da informação – técnicas de segurança – diretrizes para implantação de um sistema de gestão da segurança da informação Exemplar para uso exclusivo - ABNT - Associação Brasileira de Normas Técnicas - 33.402.892/0001-06. Disponível em: https://pdfcoffee.com/27003pdf-pdf-free.html. Acesso em: 20 ago. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27004:2010:** tecnologia da informação - técnicas de segurança - gestão da segurança da informação - medição. Disponível em: https://www.skoob.com.br/livro/pdf/abnt-nbr-isoiec-27004/348487/edicao:391122. Acesso em: 20 ago. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005:2008**: tecnologia da informação: técnicas de segurança: gestão de riscos de segurança da informação
Disponível em: https://iso31000.net/riscos-ciberneticos/.Acesso em: 20 ago. 2023.

AVEDON, Don. **GED de A a Z**: tudo sobre gerenciamento eletrônico de documentos. São Paulo: Cenadem, 2002. 200 p.

BALDISSERA, Olívia. ISO 77000: tudo o que você precisa saber para se destacar na segurança da informação. **PUCPR Digital**, Curitiba, PR, nov. 2021. Disponível em: https://posdigital.pucpr.br/blog/iso-27000#significado. Acesso em: 22 set. 2022.

BAPTISTA, Fabrício. **Uma proposta de interface de resultados de buscas em sistemas de recuperação de informação**: a semiótica e a interação humano computador como aporte teórico. 2019. 171 p. Tese (Doutorado em Ciência da Informação) – Programa de Pós-Graduação em Ciência da Informação da Universidade Paulista, Marília, SP, 2019. Disponível em: https://repositorio.unesp.br/handle/11449/181135. Acesso em: 25 out. 2022.

BARBOZA, Elder Lopes. Gestão da informação nas organizações e a atuação do profissional da informação. **Revista Brasileira de educação em Ciência da Informação**, São Paulo, v. 6,

n. esp., p. 9-101, 1. sem. 2019. Disponível em: https://portal.abecin.org.br/rebecin/article/view/103/pdf_1. Acesso em: 12 jul. 2021.

BARBOZA, Elder Lopes; FADEL, Bárbara. Fluxos de informação na gestão do conhecimento: por uma cultura de compartilhamento. *In*: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 18., 2017. **Anais** [...]. Marília: UNESP, 2017. p. 1-20. Disponível em: https://www.brapci.in f.br/index.php/res/download/124991. Acesso em: 10 mar. 2020.

BARBIER, René. **A pesquisa-ação**. Tradução de Lucie Didio. Brasília: Liber Livro Editora, 2004. 159 p.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2011. 229 p.

BEAL, Adriana. **Gestão estratégica da informação**: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas, 2012.

BEAL, Adriana. **Segurança da informação.** São Paulo: Atlas, 2005.

BERTALANFFY, Ludwig Von**. Teoria geral dos sistemas**: fundamentos, desenvolvimento e aplicações. Tradução de Francisco M. Guimarães. 5. ed., Petrópolis, RJ: Vozes, 2010.

BOOTH, Wayne Clayson; COLOMB, Gregory G; WILIAMS, Joseph M. **A arte da pesquisa**. Tradução de Henrique A. Rego Monteiro. São Paulo: Martins Fontes, 2008.

BORTOLOTI, Karen Fernanda. **Metodologia da pesquisa**. Rio de Janeiro: SESES, 2015. 192 p.

BRAGA, Kátia Soares. Aspectos relevantes para a seleção da metodologia adequada à pesquisa social em Ciência da Informação. *In:* MUELLER, Suzana Pinheiro Machado (org.). **Métodos para a pesquisa em ciência da informação**. Brasília: Thesaurus, 2007. p. 17-38.

BRASIL. Advocacia-Geral da União. **Comunicado nº 16/SGA, de 16 de março de 2020**. Coronavírus (COVID-19): Recomendações. Brasília: PGU: SGA: AGU, 2020. Disponível em: https://agudf.sharepoint.com/sites/sga/SitePages/COMUNICADO-N%C2%BA-16-SGA,-DE-16-DE-MAR%C3%87O-DE-2020-.aspx. Acesso em: 20 ago. 2021.

BRASIL. Advocacia-Geral da União. **Conheça o planejamento estratégico da AGU para os próximos anos**. Brasília: AGU, 29 mar. 2022. Disponível em: https://www.gov.br/agu/pt-br/comunicacao/noticias/conheca-o-planejamento-estrategico-da-agu-para-os-proximos-anos--960636. Acesso em: 22 out. 2022.

BRASIL. Advocacia-Geral da União. **Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC**: triênio – 2021-2023. Brasília: AGU: Comitê de Tecnologia da Informação, dez. 2020. Disponível em: https://www.gov.br/agu/pt-br/governanca/PDTIC20212023.pdf. Acesso em: 20 ago. 2022.

BRASIL. Advocacia-Geral da União. **E-mail Circular nº 157, de 14 de set. 2020**. Consulta Pública. Portaria que promove a governança da PGU mediante a coordenação, a especialização e a desterritorialização da representação judicial da União no âmbito das suas competências. Mensagem recebida por: ana.almeida@agu.gov.br. Acesso em: 20 dez. 2022.

BRASIL. Advocacia-Geral da União. **Manual de Procedimentos da Digitalização da Advocacia-Geral da União**. 2. ed. Brasília: Coordenação Geral de Gestão da Documentação e Informação, 2013. Disponível em: https://www.gov.br/agu/pt-br/assuntos-1/Publicacoes/cartilhas/manualdedigitalizacao.pdf. Acesso em: 20 ago. 2022.

BRASIL. Advocacia-Geral da União. **Manual para usuários sapiens – Sistema AGU de Inteligência Jurídica:** versão 1.3.2. Brasília, 2018. Disponível em: http://sapienswiki.agu.gov.br/index.php/P%C3%A1gina_principal#Consulte_os_Manuais_do_SAPIENS. Acesso em: 20 ago. 2022.

BRASIL. Advocacia-Geral da União. **Planejamento estratégico 2020-2023**. Brasília: AGU, 15 dez. 2020. Disponível em: https://www.gov.br/agu/pt-br/governanca/planejamento-estrategico/planejamento-estrategico-2020-2023. Acesso em: 18 jul. 2022.

BRASIL. Advocacia-Geral da União**. Portaria nº 26, de 14 de outubro de 2020**. Promove a governança da Procuradoria-Geral da União mediante a coordenação, a especialização e a desterritorialização da representação judicial da União no âmbito de suas competências. Brasília: Advocacia-Geral da União, 2012. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-26-de-14-de-outubro-de-2020-282696474. Acesso em: 22 ago. 2022.

BRASIL. Advocacia-Geral da União. **Portaria nº 84, de 17 de março de 2020**. Dispõe sobre medidas de proteção e redução de riscos para enfrentamento da emergência de saúde pública de importância internacional decorrente do Coronavírus (COVID-19). Brasília, DF, 2020. Disponível em: https://www.gov.br/agu/pt-br/comunicacao/noticias/agu-adotara-nova-rotina-de-trabalho-para-reforcar-cuidado-e-prevencao-ao-coronavirus--902036/Portaria84pdfpdf.pdf. Acesso em: 12 fev. 2022.

BRASIL. Advocacia-Geral da União. **Portaria nº 124, de 28 de março de 2012**. Regula a publicação de conteúdos institucionais nos sítios de internet e intranet da Advocacia-Geral da União, bem como nas redes sociais e demais serviços de publicação de conteúdos disponíveis na rede mundial de computadores, e dá outras providências. Brasília: Advocacia-Geral da União, 2012. Disponível em: https://sintse.tse.jus.br/documentos/2012/Mar/30/diario-oficial-da-uniao-secao-1/portaria-no-124-de-28-de-marco-de-2012-regula-a. Acesso em: 20 jun. 2022.

BRASIL. Advocacia-Geral da União. **Portaria Normativa AGU nº 3, de 28 de janeiro de 2021**. Regulamenta o teletrabalho para membros de carreiras jurídicas no âmbito da Advocacia-Geral da União - AGU e da Procuradoria-Geral Federal - PGF e dá outras providências. Brasília; AGU, 2021. Disponível em:

BRASIL. Advocacia-Geral da União. **Portaria Normativa AGU nº 17, de 16 de julho de 2021**. Autoriza e regulamenta a implementação de Programa de Gestão no âmbito dos órgãos da Advocacia-Geral da União e dá outras providências. Brasília: AGU, 2021. Acesso em: https://www.in.gov.br/en/web/dou/-/portaria-normativa-agu-n-17-de-16-de-julho-de-2021-332688102. Acesso em: 22 ago. 2022.

BRASIL. Advocacia-Geral da União. **Portaria Normativa PGU/AGU nº 5, de 3 de agosto de 2021**. Regulamenta os processos de seleção e autorização ao teletrabalho pelos Advogados da União em exercício nos órgãos da Procuradoria-Geral da União. Brasília: AGU, 2021. Disponível em: https://www.gov.br/agu/pt-

br/governanca/PORTARIANORMATIVAPGU_AGUN5_03.08.2021_Regulamentaprocessos deseleoeautorizaoaoteletrabalhopelosAdvogadosdaUnioemexerccionosrgosdaPGU.pdf. Acesso em: 22 de ago. 2021.

BRASIL. Advocacia-Geral da União. **Relatório de gestão 2021**. Brasília: Secretária-Geral de Consultoria: Comitê de Governança da Advocacia-Geral da União, 2021. Disponível em: https://www.gov.br/agu/pt-br/acesso-a-informacao/auditorias/processo-de-contas-anuais/processos-de-contas-anuais-2021. Acesso em:12 ago. 2022.

BRASIL. Advocacia-Geral da União. **Sistema AGU de Inteligência Jurídica**: sapiens. Brasília: AGU, [2022?]. Disponível em: https://sapiens.agu.gov.br/login. Acesso em: 18 jul. 2022.

BRASIL. Advocacia-Geral da União. **Sobre a Advocacia-Geral da União**. Brasília: AGU, 13 out. 2021. Disponível em: https://www.gov.br/agu/pt-br/acesso-a-informacao/institucional/sobre. Acesso em: 18 jul. 2022.

BRASIL. **Cartilha dos direitos dos participantes de pesquisa**: versão 1.0. Brasília: Ministério da Saúde. Conselho Nacional de Saúde. Comissão Nacional de Ética em Pesquisa, 2020. Disponível em: https://conselho.saude.gov.br/images/comissoes/conep/img/boletins/Cartilha_Direitos_Participantes_de_Pesquisa_2020.pdf. Acesso em: 9 set. 2022.

BRASIL **Conheça a CONEP**. Brasília: Editora MS/CGDI, 2017. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/conheca_conep_comissao_nacional_etica.pdf. Acesso em: 20 set. 2022.

BRASIL. Conselho Nacional de Justiça. **Justiça em números 2022**. Brasília: CNJ: Coordenadoria de Gestão da Informação e Memória do Poder Judiciário, 2022. 331 p.

BRASIL. Conselho Nacional de Justiça. **Resolução nº 4, de 16 de agosto de 2005**. Cria o Sistema de Estatística do Poder Judiciário e dá outras providências. Brasília, DF: CNJ, 2005. Disponível em: https://atos.cnj.jus.br/atos/detalhar/188. Acesso em: 12 maio 2023.

BRASIL. Conselho Nacional de Saúde. **Guia de perfis da Plataforma Brasil**. Brasília: Brasília: Ministério da Saúde. Conselho Nacional de Saúde, [2021]. Disponível em: http://conselho.saude.gov.br/images/comissoes/conep/documentos/PLATAFORMA_BRASIL_MANUAIS/3_-_Guia_de_Perfis.PDF. Acesso em: 25 jul. 2022.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília: Senado Federal, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso: 04 jun. 2018.

BRASIL. **Decreto nº. 11.072, de 17 de maio de 2022**. Dispõe sobre o Programa de Gestão e Desempenho - PGD da administração pública federal direta, autárquica e fundacional. Brasília: Presidência da República, 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.072-de-17-de-maio-de-2022-401056788. Acesso em: 20 jun. 2022.

BRASIL. **Lei nº 9.028, de 12 de abril de 1995**. Dispõe sobre o exercício das atribuições institucionais da Advocacia-Geral da União, em caráter emergencial e provisório, e dá outras

providências. Brasília: Presidência da República, 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9028.htm. Acesso em: 12 jul. 2022.

BRASIL. **Lei nº 10.480, de 2 de julho de 2002**. Dispõe sobre o Quadro de Pessoal da Advocacia-Geral da União, a criação da Gratificação de Desempenho de Atividade de Apoio Técnico-Administrativo na AGU – GDAA e dá outras providências. Brasília: Senado Federal, 03 jul. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10480.htm Acesso em: 01 jul. 20228.

BRASIL. **Lei nº 12.682 de 9 de julho de 2012**. Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. Brasília: Presidência da República, 2012. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/leis-e-decretos-leis/lei-no-12-682-de-9-de-julho-de-2012. Acesso em: 20 ago. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 8 de janeiro de 2022.

BRASIL. **Lei nº 13.327, de 29 de julho de 2016**. Institui o Plano Especial de Cargos da Cultura e a Gratificação Específica de Atividade Cultural - GEAC; cria cargos de provimento efetivo; altera dispositivos das Leis nºs 10.862, de 20 de abril de 2004, 11.046, de 27 de dezembro de 2004, 11.094, de 13 de janeiro de 2005, 11.095, de 13 de janeiro de 2005, e 11.091, de 12 de janeiro de 2005; revoga dispositivos da Lei nº 10.862, de 20 de abril de 2004; e dá outras providências. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/Lei/L13327.htm#anexoxxxv... Acesso em: 12 fev. 2019.

BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337. Acesso em: 25 janeiro 2022.

BRASIL. **Lei Complementar nº 73, de 10 de fevereiro de 1993**. Institui a Lei Orgânica da Advocacia-Geral da União e dá outras providências. Brasília: Presidência da República, [1993]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp73.htm. Acesso em: 08 set. 2022

BRASIL. Ministério da Economia. **Sistema de Organização e Inovação Institucional do Governo Federal – SIORG**. Brasília, DF: ME, dez. 2022. Disponível em: https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/transformagov/catalogodesolucoes/siorg. Acesso em :20 dez. 2022.

BRASIL. Ministério da Justiça. Tribunal de Contas da União. **Boas práticas em segurança da informação**. 4. ed. Brasília: TCU: Secretaria de Fiscalização de Tecnologias da Informação, 2012. 103 p.

BRASIL. Ministério da Justiça. Tribunal Regional da 4ª Região. **SEI**: sistema do TRF4 adotado em mais de 40 órgãos dos três Poderes reúne representantes em Porto Alegre. Porto Alegre: TRF4, dez. 2014. Disponível em:

https://www.trf4.jus.br/trf4/controlador.php?acao=noticia_visualizar&id_noticia=10667. Acesso em: 15 dez. 2022.

BRASIL. Ministério da Saúde. **Resolução nº 466, de 12 de dezembro de 2012**. Aprova as diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos. Brasília: CNS, [2016]. Disponível em: https://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf. Acesso em: 12 jul. 2020.

BRASIL. Ministério da Saúde. **Resolução nº 506, de 03 de fevereiro de 2016**. Aprovar a seguinte Resolução referente ao processo de acreditação de comitês de ética em Pesquisa (CEP) que compõem o Sistema CEP/Conep. Brasília: CNJ, [2016]. Disponível em: http://conselho.saude.gov.br/images/comissoes/conep/documentos/NORMAS-RESOLUCOES/Resoluo_n_506_-_2016_-__Acreditao_CEP.pdf. Acesso em: 12 jan. 2020.

BRASIL. Ministério da Saúde. **Resolução nº 510, de 07 de abril de 2016**. Dispõe sobre as normas aplicáveis a pesquisas em Ciências Humanas e Sociais cujos procedimentos metodológicos envolvam a utilização de dados diretamente obtidos com os participantes ou de informações identificáveis ou que possam acarretar riscos maiores do que os existentes na vida cotidiana, na forma definida nesta Resolução. Brasília: CNJ, [2016]. Disponível em: http://conselho.saude.gov.br/resolucoes/2016/Reso510.pdf. Acesso em: 12 jan. 2020.

BRASIL. Ministério do Planejamento. **Instrução Normativa nº 4, de 11 de setembro de 2014**. Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração de Recursos de Tecnologia da Informação e Informática (SISP) do Poder Executivo Federal. Brasília: Secretaria Logística e Tecnologia da Informação: Ministério do Planejamento, Orçamento e Gestão, [2014]. Disponível em: https://licitacoes.ufsc.br/files/2014/10/IN-SLTI-MPOG-n%C2%BA-04-2014.pdf. Acesso em: 20 jun. 2022.

BRASIL. Presidência da República. **Certificado digital**. Brasília: Instituto Nacional de Tecnologia da Informação, jun. 2017. Disponível em: https://www.gov.br/iti/pt-br/assuntos/certificado-digital/certificado-digital. Acesso em: 20 jul. 2022.

BRASIL. Presidência da República. **Glossário de segurança da informação**. Brasília: Presidência da República, 26 nov. 2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1. Acesso em: 20 jul. 2022.

BRASIL. Presidência da República. **Instrução Normativa nº 1, de 27 de maio de 2020**. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. Brasília: Presidência da República: Gabinete de Segurança Institucional, [2020]. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215. Acesso em: 20 nov. 2022.

BRASIL. Presidência da República. **Norma Complementar nº 10/IN01/DSIC/GSIPR**, **de 30 de janeiro de 2012**. Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal. Brasília: Presidência da República: Gabinete de Segurança Institucional, [2012]. Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-10IN01DSICGSIPR.pdf. Acesso em :20 set. 2022.

BRASIL. Presidência da República. **Portaria nº 93, de 26 de setembro de 2019**. Aprova o glossário de segurança da informação. Brasília, DF: Gabinete de Segurança Institucional, 2019. Disponível em: https://www.semesp.org.br/legislacao/portaria-no-93-de-26-de-setembro-de-2019/. Acesso em: 20 ago. 2023.

BRASIL. Presidência da República. **Portaria GSI/PR nº 93, de 18 de outubro de 2021**. Aprovar o Glossário de Segurança da Informação, na forma do Anexo a esta Portaria. Brasília, DF: Presidência da República, [2021]. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370. Acesso em: 12 set. 2022.

CARDOSO, Deiser Mara Rezende. Advocacia-Geral da União 25 Anos: uma instituição essencial à segurança e à solução das relações jurídicas controvertidas de interesse Público. **Revista da Escola da AGU**, Brasília, DF, v. 10, n. 3, jul./set. 2018. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/Publ-Esc-AGU_v.10_n.03.pdf. Acesso em: 20 out. 2022.

CARDOSO, Gustavo. Sociedades em transição para a sociedade em rede. *In*: CASTELLS, Manuel; CARDOSO, Gustavo (org.). **A sociedade em rede**: do conhecimento à acção política – conferência promovida pelo presidente da república. Lisboa, PT: Imprensa Nacional, 2005. p. 36-61.

CARNEIRO, Luciana Emirena dos Santos. **Gestão da informação e do conhecimento no âmbito das práticas de segurança da informação**: pessoas, processos e tecnologia. 2012. 187 f. Dissertação (Mestrado em Ciências da Informação) - Universidade Federal de Minas Gerais, Belo Horizonte, 2012. Disponível em: http://www.bibliotecadigital.ufmg.br/dspace/handle/1843/ECID-943P97. Acesso em: 01 jun. 2022.

CARVALHO, Gilda Maria Rocha de; TAVARES, Márcia da Silva e. **Informação e conhecimento**: uma abordagem organizacional. Rio de Janeiro: Qualitymark, 2001. 152 p.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. São Paulo: Zahar, 2003. 339 p.

CASTELLS, Manuel. **Sociedade em rede**: a era da informação, economia, sociedade e cultura. Tradução de Roneide Venâncio Majer e Klauss Brandini Gerhardt. 23 ed. São Paulo: Paz e Terra, 2013. 630 p.

CASTRO, Cosette (org.). **Democracia e representatividade**: novas formas de representação diante da transformação digital. São Paulo: Instituto Lula, 2022. *E-Book* (68 p.). Disponível em: https://institutolula.org/2022_politicaerepresentacao_revista01.pdf. Acesso em: 20 jun. 2022.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **Pesquisa TIC domicílio**: Resumo Executivo – Covid 19. São Paulo: CETIC.BR: Comitê Gestor da Internet no Brasil, 2020. E-book. Disponível em: https://cetic.br/media/docs/publicacoes/2/20211124201505/resumo_executivo_tic_domicilios_2020.pdf. Acesso em: 12 abr. 2022.

CERVO, Amado Luiz.; BERVIAN, Pedro Alcino; SILVA, Roberto da. **Metodologia científica**. 6. ed. São Paulo: Pearson Prentice Hall, 2007.

CHAVES, Ítalo Teixeira; ALBUQUERQUE, Rejane Maria Façanha de; FARIAS, Gabriela Belmont de; GUERRA, Maria Aurea Montenegro Albuquerque. Mapeamento de processos em biblioteca jurídica: perspectiva de melhoria na gestão da informação organizacional. **AtoZ: Novas Práticas em Informação e Conhecimento**, Curitiba, v. 11, p. 1-10, jan. 2022. Disponível em: https://revistas.ufpr.br/atoz/article/view/79074/44047. Acesso em: 6 set. 2022.

CHIAVENATO, Idalberto; SAPIRO, Arão. **Planejamento estratégico**. 2. ed. Rio de Janeiro: Elsevier, 2009.

CHOO, Chun Wei. **A organização do conhecimento**: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. Tradução Eliana Rocha. São Paulo: Editora Senac, 2003.

CHOWDHURY, Gobinda. Usuários da recuperação da informação. **InCID: Revista de Ciência da Informação e Documentação**, Ribeirão Preto, v. 5, n. 2, p. 4-33, set. 2014/fev. 2015. Disponível em: https://brapci.inf.br/index.php/res/download/53511. Acesso em: 15 nov. 2022.

COELHO, Flávia Estélia Silva; ARAÚJO, Luiz Geraldo Segadas; BEZERRA, Edson Kowask. **Gestão da segurança da informação:** NBR 27001 e NBR 27002. Rio de Janeiro: Rede Nacional de Ensino e Pesquisa, 2014.

CONSELHO NACIONAL DE ARQUIVOS. **e-Arq. Brasil**: modelos de requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. Rio de Janeiro: CONARQ: CTDE: Arquivo Nacional, 2022. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F6364D83701642351A57E436B. Acesso em: 20 out. 2022.

CONSELHO NACIONAL DE ARQUIVOS. **Glossário**: Documentos Arquivísticos Digitais. Rio de Janeiro: CONARQ: CTDE: Arquivo Nacional, 2020. Disponível em: https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/glosctde_2020_08_07.pdf. Acesso em: out. 2022.

CORRÊA, Giovana Camila Garcia; CAMPOS, Isabel Cristina Pires de; ALMAGRO, Ricardo Campanha. Pesquisa-ação: uma abordagem prática de pesquisa qualitativa. **Ensaios Pedagógicos**, Sorocaba, SP, v. 2, n.1, jan./abr. 2018, p.62-72. Disponível em: https://www.ensaiospedagogicos.ufscar.br/index.php/ENP/article/view/60. Acesso em: 20 ago. 2022.

COUTINHO, Clara Pereira. **Metodologia da investigação em ciências sociais e humanas**: teoria e prática. Coimbra, PT: Almedina, 2011. 343 p.

CRESWELL, John Ward; CLARK, Vicki Plano. **Pesquisa de métodos mistos**. Tradução Magda França Lopes. 2. ed. Porto Alegre: Editora Penso, 2013. 288 p.

CUNHA, Murilo Bastos da. A exclusão digital no Brasil e seus reflexos no acesso à informação. **Revista Ibero Americana de Ciência da Informação**, Brasília, v. 14, n. 2, p. 362-366, maio /ago.de 2021. Disponível em: https://periodicos.unb.br/index.php/RICI/article/view/37819/29651. Acesso em: 20 jun. 2022.

DAVENPORT, Thomas. **Ecologia da informação:** por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

DAVENPORT, Thomas; MARCHAND, Donald; DICKSON, Tim. **Dominando a gestão da informação**. Porto Alegre: Bookman, 2004. p.64-69.

DAVENPORT, Thomas; PRUSAK, Laurence. **Conhecimento empresarial**. Tradução de Lenke Peres. Rio de Janeiro: Campus, 1998. 237 p.

DELBIANCO, Natalia Rodrigues; VALENTIM, Marta Lígia Pomim. Sociedade da informação e as mídias sociais no contexto da comunicação científica. **AtoZ: Novas Práticas em Informação e Conhecimento**, Curitiba, v. 11, p. 1-11, 2022. Disponível em: https://revistas.ufpr.br/atoz/article/view/78778/45678. Acesso em: 12 jul. 2022

DEMO, Pedro. **Metodologia científica em ciências sociais**. 3. ed. São Paulo: Atlas, 1995.

DHILLON, Gurpreet. Realizing benefits on an information security program. **Business Process Management Journal**, Indiana, EUA, v. 10, n. 3, p. 260-261, 2004. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/bpmj.2004.15710caa.002/full/html. Acesso em: 20 abr. 2020.

DINIZ, Bárbara Carvalho; SILVA, Alzira Karla Araújo da. Gestão da Informação no sistema de Processo Judicial Eletrônico em um Tribunal Regional do Trabalho. **P2P & Inovação**, Rio de Janeiro, v. 7, n. 1, p. 186-204, set.2020/fev. 2021. Disponível em: https://revista.ibict.br/p2p/article/view/5408/5046. Acesso em:

DUTRA, Frederico Giffoni de Carvalho; BARBOSA, Ricardo Rodrigues. Modelos e etapas para a gestão da informação: uma revisão sistemática de literatura. **Em Questão**, Porto Alegre, v. 26, n. 2, maio/ago. 2020; p. 06-131. Disponível em: https://brapci.inf.br/index.php/res/v/139420. Acesso em: 15 nov. 2022.

EVÊNCIO, Kátia Maria de Moura; TEIXEIRA, Shearly Lima; RODRIGUES, Kátissa Galgania Feitosa Coutinho; FEITOSA, Flaviana Araújo; FONTES, Wesley Jonh da Silva. Dos tipos de conhecimento às pesquisas qualitativas em educação. **Revista Multidisciplinar e de Psicologia**, São Paulo, v.13, n. 47, p. 440-452, out. 2019. Disponível em: Acesso em: 12 dez. 2022.

FAUVEL, Thais Helena Freitas; VALENTIM, Marta Lígia Pomim. Informação orgânica como subsídio para o processo de inteligência competitiva organizacional. *In*: VALENTIM, Marta (org.). **Gestão da informação e do conhecimento no âmbito da ciência da informação**. São Paulo: Polis: Cultura Acadêmica, 2008. p. 229-241.

FÁVERO, Luiz Paulo; BELFIORE, Patrícia. **Manual de análise de dados**: estatística e modelagem multivariada com Excel, SPSS e Stata. Rio de Janeiro: Elsevier, 2017. 1219 p.

FERREIRA, Sérgio da Costa**. Sistemas de informação em segurança**. Londrina: Editora e Distribuidora Educacional S.A., 2017. 224 p.

FLORES, Daniel. Uma ruptura de paradigma para os arquivos: a custódia digital ininterrupta, distribuída e compartilhada, para os nossos produtores. **Boletín digital Arkhé de la Asociación Latinoamericana de Archivos**, Lima, PE, n. 81, jul. 2023. Disponível em:

https://www.alaarchivos.org/wp-content/uploads/2023/07/Editorial2023-Daniel-Flores.pdf. Acesso em: 30 ago. 2023.

FRAGA, Bruno. **Técnicas de invasão: aprenda as técnicas usadas por hackers em invasões reais**. São Paulo: Labrador, 2019. 296 p.

FURNELL, Steven; THOMSON, Kerry-Lynn. From Culture to disobedience: recognising the varying user acceptance of it security. **Computer Fraud & Security,** Chicago, EUA, v. 2, p.5-10, 2009. Disponível em: https://doi.org/10.1016/S1361-3723(09)70019-3. Acesso em: 20 abr. 2020.

GAIVÉO, José Manuel. **As pessoas nos sistemas de gestão da segurança da informação**. 2008, 668 f. Tese (Doutoramento em Informática) – Universidade Aberta. Lisboa: Universidade Aberta: Lisboa, 2008. Disponível em: http://repositorioaberto.uab.pt/handle/10400.2/1272. Acesso em: 12 maio 2020.

GARCIA, Elias. Pesquisa bibliográfica versus revisão bibliográfica: uma discussão necessária. **Revista Línguas & Letras**, Cascavel, PR, v. 17, n. 35, p. 291-294, 2016. Disponível em: https://e-revista.unioeste.br/index.php/linguaseletras/article/view/13193/10642. Acesso em: 22 jul. 2022.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2017. 128 p.

GONÇALVES, Janice. **Como classificar e ordenar documentos de arquivos**. São Paulo: Associação dos Arquivistas de São Paulo: Arquivo do Estado, 1998. 38 p.

GONZÁLEZ DE GÓMEZ, Maria Nélida. Metodologia de pesquisa no campo da Ciência da Informação. **DataGramaZero**, Porto Alegre, v. 1, n. 6, dez. 2000. Disponível em: file:///C:/Users/Windows/Desktop/livros%20metodologia/GomesDataGramaZero2000%20(1).pdf. Acesso em: 12 maio 2022.

GONZÁLEZ DE GÓMEZ, Maria Nélida. Reflexões sobre ética da informação: panorama contemporâneo. *In*: GONZÁLEZ DE GOMEZ, Maria Nélida; CIANCONI, Regina de Barros. **Ética da Informação: Perspectivas e Desafios**, Rio de Janeiro: Garamond, 2017. p. 19-44.

GOUVEIA, Luís Borges. **Gestão da Segurança da Informação**. Porto, PT: Universidade Fernando Pessoa, 2016. Disponível em: https://bdigital.ufp.pt/bitstream/10284/5954/1/securv1_1_mar2016.pdf. Acesso em: 12 abr. 2022.

GUERRIERO, Iara Coelho Zito; MINAYO, Maria Cecília. A aprovação da Resolução CNS nº. 510/2016 é um avanço para a ciência brasileira. **Saúde Sociedade**, São Paulo, v. 28, n. 4, p. 299-310, 2019. Disponível em: https://www.scielo.br/j/sausoc/a/NktsFDpGm7mDPpc8q8J6YcD/?format=pdf&lang=pt. Acesso em: 20 jul. 2022.

GUPTA, Gajanand; MISHRA, Rajesh. A SWOT analysis of reliability centered maintenance framework. **Journal of Quality in Maintenance Engineering**, Indiana, USA, v. 22, n. 2, p. 130 – 145, may 2016. Disponível em:

https://www.researchgate.net/publication/301596467_A_SWOT_analysis_of_reliability_centered_maintenance_framework. Acesso em: 12 nov. 2022.

HITCHINGS, Jean. Deficiencies of the traditional approach to information security and the requirements for a new methodology. **Computers & Security**, Indiana, USA, v. 14, n. 5, p. 377–383, may 1995. Disponível em: https://www.sciencedirect.com/science/article/pii/016740489597088R. Acesso em :20 ago. 2022.

JENKINS, Henry. **Cultura da convergência**. Tradução de Susana Alexandria. São Paulo: Aleph, 2013. 478 p.

JUCÁ, Mario Cesar. Prefácio. *In*: MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. **Segurança da informação**: uma visão sistêmica para implantação em organizações. João Pessoa, PB: Editora UFPB, 2019. p. 6-9.

KLEINSORG, Cláudia Reis de Paula. **A efetividade dos sistemas de informação nas organizações.** 2015. 98 f. Dissertação (Mestrado em Sistemas de Informação e Gestão do Conhecimento) – Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento da FUMEC, 2015, Belo Horizonte: FUMEC. Disponível em: http://www.fumec.br/revistas/sigc/article/view/3320/1897. Acesso em: 10 maio 2020.

KLETTENBERG, Josiane. **Segurança da informação**: um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de instituições bancárias. 2013. 160 f. Dissertação (Mestrado em Ciência da Informação) – Cetro de Ciências da Educação da Universidade Federal de Santa Catarina, Florianópolis, SC, 2016. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/172575/343623.pdf?sequence. Acesso em:12 set. 2022.

KOCHE, José Carlos. **Fundamentos de metodologia científica**. Petrópolis: Vozes, 2011. 185 p.

LAUDON, Kenneth; LAUDON, Jane. **Sistemas de informações gerenciais**. Tradução de Luciana do Amaral Teixeira. 9. ed., São Paulo: Pearson Prentice Hall, 2010.

LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 2009.

LIMA, Paulo Ricardo Silva; FERREIRA, Leonardo Matheus Marques; PEIXOTO, Ana Lydia Vasco de Albuquerque. Gestão de Segurança da informação: análise de políticas de defesa cibernética e estratégias para a proteção de dados e informações da administração pública brasileira. **P2P & Inovação**, Rio de Janeiro, v. 9, n.1, p. 206-221, set. 2022/fev.2023. Disponível em: https://brapci.inf.br/index.php/res/download/204320. 30 set. 2022.

MACEDO, Neusa Dias de Macedo. **Iniciação à pesquisa bibliográfica**: guia do estudante para a fundamentação do trabalho de pesquisa. 2. ed. São Paulo: Edições Loyola, 1994, 56 p.

MACHADO JÚNIOR, Dorival Moreira. **Segurança da informação**: uma abordagem sobre proteção da privacidade em internet das coisas. 2018. 159 f. Tese (Doutorado em Tecnologia da Inteligência e Design Digital) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2018. Disponível em: https://tede2.pucsp.br/handle/handle/21366. Acesso em: 20 ago. 2022.

MARCIAL, Viviana Fernández; GOMES, Liliana Isabel Esteves; MARQUES, Maria Beatriz. Perspectiva teórica e metodológica em sistemas de informação complexos. **Páginas A&B**, Porto, PT, n. 3. v. 4, p. 3-21, 2015. Disponível em: https://brapci.inf.br/index.php/res/v/64130. Acesso em: 12 out. 2022.

MARCIANO, João Luiz Pereira. **Segurança da Informação**: uma abordagem social. 2006. 212 f. Tese (Doutorado em Ciência da Informação) – Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, DF, 2006. Disponível em: http://www.enancib.ppgci.ufba.br/premio/UnB_Marciano.pdf. Acesso em: 12 ago. 2022.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos da metodologia científica**. 8. ed. São Paulo: Atlas, 2017. 372 p.

MARQUES, Fabrício. Os impactos do investimento. **Revista Pesquisa FAPESP**, São Paulo, v. 246, ago. 2016. Disponível em: https://revistapesquisa.fapesp.br/os-impactos-do-investimento/. Acesso em: 15 maio 2022.

MARTELETO, Regina Maria. Redes sociais, mediação e apropriação de informações: situando campos, objetos e conceitos na pesquisa em Ciência da Informação. **Pesquisa Brasileira Ciência da Informação**, Brasília, DF, v.3, n.1, p. 27- 46, jan./dez. 2010. Disponível em: https://www.arca.fiocruz.br/handle/icict/2247. Acesso em: 20 jun. 2022.

MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. **Segurança da informação**: uma visão sistêmica para implantação em organizações. João Pessoa, PB: Editora UFPB, 2019. 160 p.

MATOS, José Gilvomar; MATOS, Rosa Maria; ALMEIDA, Josimar Ribeiro de. **Análise do ambiente corporativo**: do caos organizado ao planejamento estratégico das organizações. Rio de Janeiro: E-papers, 2007. 478 p.

MATTOS, Sandra Maria Nascimento de. **Conversando sobre metodologia da pesquisa científica**. Porto Alegre: Editora Fi, 2020. 256 p.

MCGEE, John Vernon; PRUSAK, Laurence. **Gerenciamento estratégico da informação**: aumente a competitividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. Rio de Janeiro: Campus, 1994.

MELLO, Mariana Rodrigues Gomes de; BRITO, Jean Fernandes; MARTÍNEZ-ÁVILA, Daniel. Direitos humanos, informação jurídica e arquitetura da informação no website da Associação Nacional de Travestis e Transexuais**. InCID: Revista Ciência da Informação e Documentação**, Ribeirão Preto, v. 13, n. 1, p. 257-281, mar./ago. 2022. Disponível em: https://www.revistas.usp.br/incid/article/view/184574/183729. Acesso em: 10 set. 2022

MOLINA, Letícia Gorri. Gestão da informação e do conhecimento e as TICs aplicadas aos portais corporativos. *In*: VALENTIM, Marta (org.). **Gestão da informação e do conhecimento no âmbito da ciência da informação**. São Paulo: Polis: Cultura Acadêmica, 2008. p. 71-92.

MONTEIRO, Samuel Alves; DUARTE, Emeide Nóbrega. Bases teóricas da gestão da informação: da gênese às relações interdisciplinares. **InCID: Revista de Ciência de Informação e Documentação**, Ribeirão Preto, v. 9, n. 2, p. 89-106, set. 2018/fev. 2019. Acesso em: https://www.revistas.usp.br/incid/article/view/133677. Acesso em: 20 jul. 2022.

MORAES, Cássia Regina Bassan de; FADEL, Bárbara. A informação no contexto organizacional: tipos, características e usos. **Ibersid: Revista de Sistemas de Informacíon y Documentación**, Saragoza, ES, v. 3, p. 61-65, 2009. Disponível em: https://www.ibersid.eu/ojs/index.php/ibersid/article/view/3724/3485. Acesso em: 20 jan. 2022.

MORESI, Eduardo Amadeu Dutra. Delineando o valor do sistema de informação de uma organização. **Ciência da Informação,** Brasília, v. 29, n. 1, p. 14-24, jan./abr. 2000. Disponível em: https://www.scielo.br/j/ci/a/pzj7MLqJc6jX5zHLxH5PFwq/?format=pdf&lang=pt. Acesso em: 20 jan. 2022.

NONATO, Rafael dos Santos; AGANETTE, Elisângela Cristina. Gestão da informação: rumo a uma proposta de definição atual e consensual para o termo. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 27, n. 1, p. 133-159, jan./mar. 2022. Disponível em: https://brapci.inf.br/index.php/res/v/203838. Acesso em: 14 set. 2022.

OLETO, Ronaldo Ronan. Percepção da qualidade da informação. **Ciência da Informação**, Brasília, v. 35, n. 1, p. 57-62, jan./abr. 2006. Disponível em: https://www.scielo.br/j/ci/a/pDnBv4ywKw5Sp7Dqy9tnFxz/?lang=pt. Acesso em: 20 ago. 2022.

OLIVEIRA, Djalma de Pinho Rebouças de. **Planejamento estratégico**: conceitos, metodologia e práticas. 23. ed., São Paulo: Atlas, 2007.

OLIVEIRA, Wilson. **Segurança da informação**: técnicas e soluções. São Paulo: Atlas, 2001.

ORTEGA, Cristina Dotta. Surgimento e consolidação da documentação: subsídios para compreensão da história da ciência da informação no Brasil. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 14, n. esp., p. 57-59, 2009. Disponível em: https://brapci.inf.br/index.php/res/v/199058. Acesso em: 14 jul. 2022.

PAIXÃO, Márcia Valéria. **Administração estratégica. Paraná**: Instituto Federal de Educação, Ciência e Tecnologia, 2012. 160 p. Disponível em: http://redeetec.mec.gov.br/images/stories/pdf/proeja/administracao_estrat.pdf. Acesso em: 12 ago. 2018.

PALETTA, Francisco Carlos; MOREIRO-GONZÁLEZ, José Antônio; VERGUEIRO, Waldomiro de Castro Santos. A ciência da informação e o mercado de trabalho na era digital: desafios na formação do profissional da informação. *In:* MARQUES, Maria Beatriz; GOMES, Liliana Esteves (coord.). **Ciência da informação**: visões e tendências. Coimbra, PT: Imprensa Universidade de Coimbra, 2020. p. 343-364.

PALUDO, Augustinho Vicente; PROCOPIUCK, Mario. **Planejamento Governamental**. São Paulo: Atlas, 2011.

PELTIER, Thomas. **Information security policies, procedures, and standards**: Establishing an Essential Code of Conduct. USA: Aurebach Publications, 2001.

PICHETH, Sara Fernandes; CASSANDRE, Marcio Pascoal; THIOLLENT, Michel Jean Marie. Analisando a pesquisa-ação à luz dos princípios intervencionistas: um olhar comparativo. **Educação**, Porto Alegre, v. 39, n. esp. (supl.), s3-s13, dez. 2016. Disponível

em: https://revistaseletronicas.pucrs.br/ojs/index.php/faced/article/view/24263/15415. Acesso em: 20 ago. 2022.

PIMENTA, Alexandre Manuel Santareno; QUARESMA, Rui Filipe Cerqueira. A segurança dos sistemas de informação e o comportamento dos usuários. **Revista de Gestão da Tecnologia e Sistemas de Informação**, São Paulo, v. 13, n. 3, set/dez., 2016, p. 533-552. Disponível em: Acesso em: https://www.scielo.br/pdf/jistm/v13n3/1807-1775-jistm-13-03-0533.pdf. Acesso em: 12 maio 2020.

PIZARRO, Daniella Camara; POLEZA, Mariângela; LOPES, Maura Paula Miranda. Ética na ciência da informação: abordagem da temática no ensino dos programas de pós-graduação brasileiros. *In*: MATOS, José Claudio; PIZARRO, Daniella Câmara; SANTOS, Ana Carolina de Melo dos; SILVEIRA, Crislaine Zurilda; SILVEIRA, Luhilda Ribeiro; CHAGAS, Ricardo de Lima (org.). **Reflexões sobre ética na gestão da informação**. Florianópolis: UNESC, 2018. *E-book* (p. 102-128). Disponível em: https://sistemabu.udesc.br/pergamumweb/vinculos/00007c/00007c29.pdf. Acesso em: 20 ago. 2021.

PONJUÁN DANTE, Glória. **Gestión de información en las organizaciones**: princípios, conceptos y aplicaciones. Santiago do Chile: CECAPI, Universidade de Chile, 1998

PONTES, Kaio Deyvid Souza. **Análise SWOT**: uma contribuição para a gestão de uma microempresa familiar revendedora do ramo alimentício do agreste paraibano. 2019. 65 f. Monografia (Graduação em Ciências Contábeis) – Centro de Ciências Sociais Aplicadas, Universidade Federal da Paraíba. João Pessoa: UFPB, 2019. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/17307/1/KDSP23042020.pdf. Acesso em: 20 ago. 2022.

POPOVA, Alla. The impact of the digital divide on the development of socio-economic systems. **International AgroScience Conference**, Cheboksary, RU, v. 433, 1-2 jun. 2020. Disponível em: https://iopscience.iop.org/article/10.1088/1755-1315/433/1/012022. Acesso em: 12 jun. 2022.

POZZEBOM, Fábio Rodrigues. **AGU devolve mais de R$ 761 bilhões para os cofres públicos em 2021**. [Entrevista cedida a] Bruno Bianco. Agência Brasil, Brasília, 30 maio 2022. Disponível em: https://economia.ig.com.br/2022-05-30/agu-reverteu-cofres-publicos.html. Acesso em: 23 jul. 2022.

PROBST, Gilberto; RAUB, Steffen; ROMHARDT, Kai. **Gestão do conhecimento**: os elementos construtivos do sucesso. Porto Alegre: Bookman, 2002.

ROCHA, Heloísa Vieira da; BARANAUSKAS, Maria Cecília Calani. **Design e avaliação de interface homem-computador**. São Paulo: UME: USP, 2000.

ROCHA, Vinícius Torquetti Domingos. **Consulta pública aos membros e servidores da Procuradoria-Geral da União**: minuta portaria de desterritorialização. Brasília: ANAUNI, 2020. Disponível em: https://www.anauni.org.br/wp-content/uploads/2020/09/Minuta-Portaria-Desterritorializac%CC%A7a%CC%83o-v7-14-09-2020-consulta-pu%CC%81blica.pdf.

RODRIGUES, Luís. **Arquiteturas dos sistemas de informação**. Lisboa: FCA Editora de Informática, 2002.

ROZA, Rodrigo Hipólito. Ciência da Informação, tecnologia e sociedade. **Biblos: Revista do Instituto de Ciências Humanas e da Informação**, Rio Grande, RS, v. 32, n. 2, p. 177-190, jul./dez. 2018. Disponível em: https://periodicos.furg.br/biblos/article/view/7546. Acesso em: 12 jun. 2022.

REGINATO, Carlos Eduardo Roehe; GRACIOLI, Odacir Deonísio. Gerenciamento estratégico da informação por meio da utilização da inteligência competitiva e da gestão do conhecimento: um estudo aplicado à indústria moveleira do RS. **Revista Gestão e Produção**, São Carlos, RS, v. 19, n. 4, dez. 2012. Disponível em: https://www.scielo.br/j/gp/a/cjCWmqjJBcJ5fgjfq3W798P/?lang=pt. Acesso em: 20 set. 2022.

ROSINI, Alessandro Marco; PALMISANO, Ângelo. **Administração de sistemas de informação e a gestão do conhecimento**. 2. ed. São Paulo: Cengage Learning, 2012.

ROWLEY, Jennifer. **A biblioteca eletrônica**. Tradução de Antônio Agenor Briquet de Lemos. 2. ed. Brasília: Briquet de Lemos, 2002. 399 p.

SAMPIERI, Roberto Hernández; COLLADO; Carlos Fernández; LUCIO; Maria Del Pilar Baptista. **Metodologia de pesquisa**. Tradução de Daisy Vaz de Moraes. 5. ed. Porto Alegre: Penso, 2013. 624 p.

SAMPIERI, Roberto Hernández; TORRES, Christian Paulina Mendoza. **Metodologia de la investigación**: las rutas cuantitativa, cualitativa y mixta. Espanha, ES: McGraw-Hill Interamericana de España S.L., 2018. 752 p.

SANTANA, Fausta Joaquina Clarinda de. **A segurança da informação na ciência da informação no Brasi**l. 2021. 318 f. Tese (Doutorado em Ciência da Informação) – Universidade Federal da Bahia, Instituto de Ciência da Informação, 2021. Disponível em: https://repositorio.ufba.br/handle/ri/34280. Acesso em: 20 set. 2022.

SANTOS, Juliana Cardoso dos. Gestão documental e gestão da informação: abordagens, modelos e etapas. **Informações@Profissões**, Londrina, v. 10, n. 1, p. 99 – 120, jan./abr. 2021. Disponível em: https://brapci.inf.br/index.php/res/download/164320. Acesso em: 20 jul. 2022.

SANTOS, Juliana Cardoso dos; VALENTIM, Marta Lígia Pomim. Gestão documental e gestão da informação como ferramentas da memória organizacional: foco na memória repositório. **Ágora: Arquivologia em debate**, Florianópolis, v. 31, n. 62, p. 01-X, jan./jun. 2021. Disponível em: https://brapci.inf.br/index.php/res/download/157182. Acesso em: 20 fev. 2022.

SANTOS, Juliana Cardoso dos; VALENTIM, Marta Lígia Pomim. Informação, conhecimento e valor da informação. **Informação & Informação**, Londrina, v. 25, n. 4, p. 574-598, out./dez. 2020. Disponível em: https://brapci.inf.br/index.php/res/download/156409. Acesso em: 12 jul. 2022.

SANTOS, Vanderlei Batista dos. **A arquivística como disciplina científica**: princípios, objetivos e objetos. Salvador: 9bravos, 2015.

SANTOS, Vanderlei Batista dos. Preservação de documentos arquivísticos digitais. **Ciência da Informação**, Brasília, DF, v. 41 n. 1, p.114-126, jan./abr. 2012. Disponível em: https://revista.ibict.br/ciinf/article/view/1357/1536. Acesso em: 20 ago. 2022.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. 24. ed. São Paulo: Cortez, 2017. 359 p.

SILVA, Jonathas Luiz Carvalho. **Fundamentos da informação I**: perspectivas em ciência da informação. São Paulo: ABECIN Editora, 2017a. 271 p.

SILVA, Jonathas Luiz Carvalho. Informação e valor: inter-relações conceituais e a formação das tipologias valorativas da informação. **Transinformação**, Campinas, SP, v. 29, n. 3, set./dez. 2017b. Disponível em: https://www.scielo.br/j/tinf/a/B7RSLGJvC5mSzTtJybJgxvP/abstract/?lang=pt. Acesso em: 20 ago. 2022.

SILVA, Marconi Gomes da; PEREIRA, William Eufrásio Nunes; MORAIS, Ana Cristina dos Santos. A revolução da tecnologia e a emergência de "uma" nova economia. **Revista de Economia Regional, Urbana e do Trabalho**, Natal, RN, v. 7, n. 2, 2018. Disponível em: https://periodicos.ufrn.br/rerut/article/view/16717. Acesso em: 20 jul. 2022.

SOBRAL, Filipe; PECI, Alketa. **Administração**: teoria e prática no contexto brasileiro. São Paulo: Pearson Prentice Hall, 2013.

SORDI, José Osvaldo de. **Administração da informação**: fundamentos e práticas para uma nova gestão do conhecimento. São Paulo: Saraiva, 2015.

SOUSA, Angélica Silva de; OLIVEIRA, Guilherme Saramago de; ALVES, Laís Hilário. A pesquisa bibliográfica: princípios e fundamentos. **Cadernos da Fucamp**, Monte Carmelo, MG, v.20, n.43, p.64-83, 2021. Disponível em: https://revistas.fucamp.edu.br/index.php/cadernos/article/view/2336. Acesso em: 20 jun. 2022.

SOUZA, Terezinha de Fática Carvalho de; RESENDE, Ana Paula de. O impacto das novas tecnologias nos arquivos de processos jurídicos nos escritórios de advocacia. **Cadernos de Informação Jurídica**, Brasília, v. 6, n. 1, p. 182-198, jan./jun. 2019. Disponível em: Disponível em: http://www.cajur.com.br/index.php/cajur/article/view/230. Acesso em: 12 abr. 2020.

STAKE, Robert E. **Pesquisa qualitativa**: estudando como as coisas funcionam. Tradução de Karla Reis. Porto Alegre: Penso, 2011. 263 p.

TARAPANOFF, Kira. Referencial teórico: introdução. *In*: TARAPANOFF, Kira (org.). **Inteligência organizacional e competitiva**. Brasília: Editora UnB, 2001. p. 33-49.

TEIXEIRA, Rômulo de Barros. **A Gestão do Conhecimento no contexto do teletrabalho em função da COVID-19.** 2022. 99 f. Dissertação (Mestrado em Ciência da Informação) – Programa de Pós– Graduação em Gestão e Organização do Conhecimento, Escola de Ciência da Informação da Universidade Federal de Minas Gerais, Belo Horizonte, 2022. Disponível em: https://repositorio.ufmg.br/handle/1843/45241. Acesso em: 20 dez. 2022.

THIOLLENT, Michel. **Metodologia da pesquisa-ação**. 18. ed. São Paulo: Cortez Editora, 2011. 68 p.

TRIPP, David. Pesquisa-ação: uma introdução metodológica. **Educação e pesquisa**, São Paulo, v. 31, n. 3, p. 443-466, 2005. Disponível em: https://www.scielo.br/j/ep/a/3DkbXnqBQqyq5bV4TCL9NSH/?format=pdf&lang=pt. Acesso em: 12 jul. 2022.

UNIVERSIDADE FEDERAL DE SERGIPE. **Portaria nº 444, de 17 de maio de 2022**. Cria Comitê de Ética em Pesquisa com Seres Humanos das Áreas de Ciências Humanas e Sociais Aplicadas (CEP-Humanidades) e nomeia membros. Aracaju, SE: Universidade Federal de Sergipe: Gabinete do Reitor, 2022. Disponível em: https://cep.ufs.br/pagina/3768. Acesso em: 2 dez. 2022.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE. **UFRN recebe homenagem pela criação de sistema de gestão**. Natal, RN: UFRN, nov. 2016. Disponível em: https://www.ct.ufrn.br/ufrn-recebe-homenagem-pela-criacao-de-sistema-de-gestao/. Acesso em: 12 dez. 2022.

VALENTIM, Marta Lígia Pomim. Gestão da informação e do conhecimento: especificidades e convergências. **Infohome,** Londrina, 2004. Disponível em: http://www.ofaj.com.br/colunas_conteudo.php?cod=88. Acesso em: 10 set. 2018

VALENTIM, Marta Lígia Pomim. Informação e conhecimento em organizações complexas. *In*: VALENTIM, Marta Lígia Pomim (org.). **Gestão da informação e do conhecimento no âmbito da ciência da informação**. São Paulo: Polis: Cultura Acadêmica, 2008. p. 11-25.

VALENTIM, Marta Lígia (org.). **Métodos qualitativos de pesquisa em Ciência da Informação**. São Paulo: Polis, 2005.

VALENTIM, Marta Lígia Pomim; ANÇANELLO, Juliana Venancio. Análise de conceitos sobre valor da informação no âmbito da ciência da informação. **ConCI: Convergências em Ciências da Informação**, São Cristóvão/SE, v. 1, n. 1, p. 26-46, jan./abr. 2018. Disponível em: https://seer.ufs.br/index.php/conci/article/view/9343/8783. Acesso em: 12 fev. 2022.

VIANA, Márcio Aparecido Nogueira; VALLS, Valéria Martin. O papel da gestão documental nos processos de gestão do conhecimento. **Future Studies Research Journal**, São Paulo, v. 8, n. 2, p. 3-26, abr./ago. 2016. Disponível em: https://www.revistafuture.org/FSRJ/article/view/209. Acesso em: 22 ago. 2022.

VIEIRA, Sônia Chagas. **Difusão do conhecimento em Paul Otlet - a Rede Universal de Documentação**: uma história em movimento. 2021. 215 f. Tese (Doutorado em Difusão do Conhecimento) – Programa de Pós-Graduação Multi-institucional em Difusão do Conhecimento, Salvador, 2021. Disponível em: https://repositorio.ufba.br/handle/ri/34863. Acesso em: 12 jan. 2022.

WEITZEL, Simone da Rocha; O desenvolvimento de coleções e a organização do conhecimento: suas origens e desafios. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 7, n. 1, p. 61-67, jan./jun. 2002. Acesso em: https://periodicos.ufmg.br/index.php/pci/article/download/23411/18886/66740; Acesso em: 20 ago. 2021.

WOIDA, Luana Maia. Cultura informacional: um modelo de realidade social para a ICO. *In*: VALENTIM, Marta Lígia Pomim (org.). **Gestão da informação e do conhecimento no âmbito da ciência da informação**. São Paulo: Polis: Cultura Acadêmica, 2008. 11-25.

WRIGHT, Peter.; KROLL, Mark. PARNEL, John. **Administração estratégica**: conceitos. 4. ed. São Paulo: Atlas, 2000.

ZUCATTO, Luis Carlos; FREITAS, Rodrigo Uszacki Carvalho de; MARZZONI, David Nogueira Silva. Pesquisa básica e pesquisa aplicada: uma análise a partir da produção científica sobre COVID-19. **Research, Society and Development**, Vargem Grande, SP, v. 9, n. 11, 2020. Disponível em: https://rsdjournal.org/index.php/rsd/article/download/10179/9186/141009. Acesso em: 20 ago. 2022.

APÊNDICE A – Termo de Consentimento livre e Esclarecido – TCLE

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA (POSGRAP)
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO
MESTRADO PROFISSIONAL EM GESTÃO DA INFORMAÇÃO E DO CONHECIMENTO

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

Convidamos o (a) Sr. (a) a participar da pesquisa "**GESTÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO ELETRÔNICA:** INTERFACE USUÁRIO, TECNOLOGIA E SISTEMA", sob a responsabilidade da pesquisadora mestranda **Ana Paula Monteiro Almeida Chagas** e orientação da **Profa. Dra. Telma de Carvalho**, do Mestrado Profissional do Programa de Pós-Graduação em Ciência da Informação (PPGCI) da Universidade Federal de Sergipe (UFS), que tem como objetivos identificar o comportamento dos usuários do sistema de informação eletrônica da Procuradoria da União em Sergipe (PU/SE)/Advocacia-Geral da União (AGU) em relação a interface usuário, tecnologia e sistema, com ênfase na Segurança da Informação visando criar um Manual de Boas Práticas de Segurança da Informação para os seus usuários.

A sua participação é voluntária, isto é, ela não é obrigatória e o (a) Sr. (a) tem plena autonomia para decidir concordar ou não em participar, bem como retirar sua participação a qualquer momento e não será penalizado (a) de nehuma maneira, caso decida não consentir sua participação ou desistir da mesma. Contudo, ela é muito importante para a execução da pesquisa. É assegurada a plena liberdade ao participante da pesquisa para, a qualquer momento e sem nenhum prejuízo, solicitar a retirada do consentimento de utilização dos seus dados. Nessa situação a pesquisadora responsável o enviará a resposta de ciência do seu interesse em retirar o consentimento.

São garantidos os direitos ao participante da pesquisa de não responder qualquer questão, sem necessidade de explicação ou justificativa para tal; não responder à (s) pergunta (s) de caráter obrigatório constante (s) no questionário online; decidir se sua identidade será divulgada e quais são, dentre as informações que forneceu, as que podem ser tratadas de forma pública (Res. CNS nº 510/2016, art. 9º, V) e ter acesso ao teor do conteúdo do instrumento de coleta de dados (tópicos que serão abordados) antes de responder as perguntas, para uma tomada de decisão informada.

É garantida a manutenção do sigilo e da privacidade dos participantes durante todas as fases da pesquisa, exceto quando houver sua manifestação explícita em sentido contrário, mesmo após o término da pesquisa, sendo asseguradas "a confidencialidade e a privacidade, a proteção da imagem e a não estigmatização dos participantes da pesquisa, garantindo a não utilização das informações em prejuízo das pessoas e/ou das comunidades, inclusive em termos de autoestima, de prestígio e/ou de aspectos econômico-financeiros". (Res. CNS nº 466/2012, III.2 i).

Qualquer dado que possa identificá-los será omitido na divulgação dos resultados da pesquisa a fim de evitar danos aos participantes, portanto os questionários serão codificados por uma sequência alfanumérica, seguindo uma ordem crescente de participantes (Ex.: ADV1; ADV2; STA1; STA2; SCD1; SCD2; ETERC1; ETERC2; ESTAG1). Ao final da pesquisa, todo o material será armazenado em local seguro com o intuito de garantir o sigilo do participante e mantido em arquivo digital, por pelo menos 5 anos, conforme Resolução CNS nº 466/2012.

É importante que fique claro que, quando **não** for possível a identificação do questionário do participante (quando a coleta de dados for anônima), **não será possível a exclusão dos dados da pesquisa, caso seja concluído o preenchimento do questionário e em seguida seja acionada a opção "clique em enviar"**. Desse modo, caso o participante **desista de participar da pesquisa, deverá fechar o formulário e não concluir e nem enviar as respostas**. Para isso é necessário que apenas feche a página do questionário da pesquisa na Internet.

O consentimento para participar da pesquisa será feito mediante a anuência deste Termo de Consentimento Livre e Esclarecido (TCLE) e caso **concorde** em participar, será considerada **anuência** quando quando **responder ao questionário/formulário da pesquisa.**

A qualquer momento, durante a pesquisa o (a) Sr. (a) poderá solicitar da pesquisadora informações sobre sua participação e/ou sobre a pesquisa, o que poderá ser feito através dos meios de contato explicitados neste Termo. **O (a) Sr. (a) terá acesso ao registro do consentimento sempre que solicitado.**

A sua participação consistirá em responder à pesquisadora perguntas de um questionário estruturado online via Google Formulários que não vai identificar individualmente seus dados, cujo teor das perguntas estarão em consonância com os objetivos propostos na pesquisa. O tempo de duração do questionário é de aproximadamente 15 (quinze) minutos.

Os resultados da pesquisa serão analisados e divulgados em artigos científicos e dissertação provenientes da pesquisa, desenvolvida no Mestrado Profissional do PPGCI/UFS, preservando-se a identidade dos seus participantes.

De acordo com a Res. 466/2012 do CNS/MS "toda pesquisa com seres humanos acarreta riscos" e um risco comum a todas essas pesquisas é a quebra de sigilo involuntário e não intencional, mesmo com a busca dos pesquisadores pela garantia da manutenção deste, a exemplo de "riscos caraterísticos do ambiente virtual, meios eletrônicos, ou atividades não presenciais, em função das limitações das tecnologias utilizadas, pois existem limitações dos pesquisadores para assegurar total confidencialidade e potencial risco de sua violação", conforme item 1, 1.2.1, da Carta Circular nº 1/2021-CONEP/SECNS/MS, de 03/03/2021.

Todo experimento com seres humanos apresenta risco de constrangimento pela observação social, que escapa ao senso comum. O risco de cunho emocional poderá ser proporcional à frustração na conseução da atividade proposta, porém esse risco será minimizado pelo BENEFÍCIO DIRETO a partir da contribuição que o (a) Sr. (a) está dando, pois através da análise gerada pelos dados coletados nessa pesquisa espera-se colaborar com os seus participantes em seu ambiente organizacional, com o objetivo de contribuir por meio dos critérios científicos com as boas práticas para a Segurança da Informação.

No caso dessa pesquisa também podem haver riscos de constrangimento por parte do participante, por se tratar de sua participação em resposta a um questionário online com perguntas relativas ao comportamento dos usuários dos sistemas de informação em relação as variáveis que implicam na Segurança da Informação e dos seus riscos.

Entretanto, a pesquisadora compromete-se a respeitar e cumprir os critérios da ética em pesquisa, bem como seguir as orientações para procedimentos em pesquisas com qualquer etapa em ambiente virtual, e acredita que adotando uma atitude respeitosa e cuidadosa com o participante poderá contornar constrangimentos. Desse modo, visando reduzir quaisquer riscos ou incômodos, orienta que o (a) Sr. (a) **não participe** dessa pesquisa caso não esteja confortável com a temática abordada, se mesmo ciente da confidencialidade de sua participação isso possa levar a conflitos de qualquer natureza, se ao preencher o questionário online perceba algum tipo de desconforto, constrangimento ou alterações de comportamento.

É garantido ao participante indenização diante de eventuais danos decorrentes da pesquisa: "o participante da pesquisa, que vier a sofrer qualquer tipo de dano decorrente do estudo, previsto ou não no Termo de Consentimento Livre e Esclarecido, tem direito à

indenização, por parte do pesquisador, do patrocinador e das instituições envolvidas nas diferentes fases da pesquisa" (Res. 466/2012 do CNS/MS, V.7), com previsão originalmente no Código Civil (Lei nº 10.406/2002, artigos 927 a 954, capítulos I e II, título IX) e Resolução CNS nº 510/2016, Art. 19, § 2º.

O (a) Sr. (a) não terá nenhuma despesa, ou seja, terá assistência gratuita e integral, visto que a sua participação em resposta ao questionário online ocorrerá com a utilização da Internet do seu ambiente de trabalho, seja na PU/SE ou em trabalho remoto e, caso necessite, em qualquer tempo a pesquisadora responsável juntamente com o apoio da equipe da Diretoria de Tecnologia da Informação da AGU - DTI/AGU fornecerá ao participante da pesquisa a assistência e suporte necessários, com a abertura de chamado por meio do e-mail: suporte@agu.gov.br. Caso haja alguma despesa diretamente decorrente de sua participação na pesquisa esta será prontamente ressarcida ao participante pela pesquisadora responsável.

Para qualquer outra informação, o (a) Sr. (a) poderá entrar em contato com a pesquisadora e obter maiores esclarecimentos pelos endereços eletrônicos: **ana.almeida@agu.gov.br** e **anapaulamonteiroac@gmail.com** ou pelo telefone/Whatsapp (79) 99907-9230 ou entrar em contato com o Programa de Pós-Graduação em Ciência da Informação, do Centro de Ciências Sociais Aplicadas da Universidade Federal de Sergipe, por meio do E-mail: **ppgci@academico.ufs.br** ou pelos telefones (79) 3194-7550, 3194-7208 e 3194-6228.

O Comitê de Ética é a instância que tem por objetivo defender os interesses dos participantes da pesquisa em sua integridade e dignidade e para contribuir no desenvolvimento da pesquisa dentro de padrões éticos, com o papel de avaliar e monitorar o andamento do projeto, de modo que a pesquisa respeite os princípios éticos de proteção aos direitos humanos, da dignidade, da autonomia, da não maleficência, da confidencialidade e da privacidade.

Em caso de dúvida quanto à condução ética do estudo, entre em contato com o Comitê de Ética em Pesquisa envolvendo Seres Humanos da Universidade Federal de Sergipe (CEP/CONEP/UFS), situado à Rua Cláudio Batista, S/N, Bairro Sanatório, Aracaju-SE, 49060-108, Brasil, Centro de Pesquisas Biomédicas/Campus da Saúde Prof. João Cardoso Nascimento Júnior - UFS; telefone (79) 3194-7208; E-mail: **cep@academico.ufs.br**.

Este Termo de Consentimento Livre e Esclarecido (TCLE), elaborado em duas vias originais, rubricadas em todas as suas páginas e assinadas pelo convidado (a) a participar da pesquisa, ou por seu representante legal, assim como pelo pesquisador responsável, pretende assegurar seus direitos e deveres como participante da pesquisa, por isso é importante que o (a) Sr. (a) guarde em seus arquivos uma via assinada desse documento que lhe será entregue, e ainda poderá imprimir a página do TCLE online marcando a opção imprimir "cabeçalhos e rodapés", para ter o *link* fonte e a paginação do TCLE e para ter acesso a sua via, basta fazer o download deste documento em formato PDF clicando no *link* abaixo:

https://docs.google.com/uc?export=download&id=1z2HLfxCE2jVROwbTEwEONbcS1Dve-aeY

Nestes termos, agradecemos a sua colaboração.

Esta pesquisadora declara o cumprimento das exigências contidas no item IV.3 da Res. nº 466/2012 do CNS/MS.

_____

Ana Paula Monteiro Almeida Chagas
Pesquisadora responsável

Consentimento:

Eu, _____,
fui informado (a) sobre o que a pesquisadora quer fazer e precisa da minha colaboração, e entendi a explicação. Pude esclarecer todas as minhas dúvidas com a pesquisadora e, por isso, eu concordo em participar do projeto, sabendo que não vou ser remunerado por isso e que posso sair quando quiser sem prejuízo.

Nome do participante: _____ Data: ____/____/_____

Assinatura do participante da pesquisa: _____

"Ao clicar no botão abaixo, o (a) Sr. (a) **concorda** em participar da pesquisa nos termos deste TCLE.

Caso **não concorde** em participar, apenas feche essa página no seu navegador".

"Li o TCLE, compreendi e concordo em participar da pesquisa"

São Cristóvão/SE, ____ de_____ de 2023.

APÊNDICE B – Questionário

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA (POSGRAP)
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO
MESTRADO PROFISSIONAL EM GESTÃO DA INFORMAÇÃO E DO CONHECIMENTO

QUESTIONÁRIO

Pesquisa GESTÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO ELETRÔNICA:

BLOCO DE PERGUNTAS: PERFIL DOS USUÁRIOS

As questões 1 a 4 visam identificar quem são os usuários dos sistemas de informação no âmbito da PU/SE e compreender sua ocupação e modalidade de trabalho.

Questão 1 – Selecione a sua ocupação na AGU

( ) Membro da carreira
( ) Servidor
( ) Requisitado
( ) Colaborador (outros)

Questão 2 – Selecione sua modalidade de trabalho atual

( ) Presencial
( ) Semipresencial
( ) Teletrabalho

Questão 3 – Selecione o tempo de serviço na PU/SE e/ou AGU

( ) Até 5 anos
( ) Entre 5 a 10 anos
( ) Acima de 10 anos

Questão 4 – Qual sua faixa etária

( ) 18 a 30 anos
( ) 31 a 50 anos
( ) Acima de 50 anos

BLOCO DE PERGUNTAS: USUÁRIOS DO SISTEMA DE INFORMAÇÃO NA PU/SE

As questões 5 a 9 visam analisar as pessoas habilitadas pela administração para acessar os ativos de informação da PU/SE.

Questão 5 – Qual seu nível de entendimento sobre o tema segurança da informação?

( ) Alto
( ) Médio
( ) Baixo

( ) Desconheço

Questão 6 – Conhece as normas de segurança da informação preestabelecidas pela Advocacia-Geral da União?

( ) Sim
( ) Não
( ) Não sei onde acessar a publicação
( ) Desconheço

Questão 7 – A Instituição já promoveu algum treinamento ou capacitação sobre a Segurança da Informação?

( ) Sim
( ) Não
( ) Não tenho interesse
( ) Desconheço

Questão 8 – Em sua percepção a segurança da informação no âmbito da AGU compete exclusivamente a DTI, departamento responsável pela segurança de rede e sistemas de informação, em casos de possível ocorrência de risco?

( ) Sim
( ) Não
( ) Deve ser uma responsabilidade de todos
( ) Desconheço

Questão 9 – Considera o seu comportamento seguro quanto às ações de Segurança da Informação na organização?

( ) Sim
( ) Não
( ) Necessito de treinamento
( ) O tema não tem sido discutido entre os servidores

BLOCO DE PERGUNTES: CATEGORIA SISTEMAS DE INFORMAÇÃO NA PU/SE

As questões 10 a 18 visam analisar a postura de segurança cibernética proativa dos usuários de sistemas de informação

Questão 10 – Quais sistemas de informação internos e externos ao órgão utiliza, em média, para executar as suas tarefas?

( ) Somente o Sapiens
( ) Sapiens e Sistemas do Judiciário a ele integrados
( ) Sapiens e outros sistemas da AGU
( ) Sapiens, outros sistemas da AGU e sistemas externos diversos

Questão 11 – Qual o período de acesso diário de utilização dos sistemas de informação conectado à Internet necessários para realizar suas atividades profissionais?

( ) Média de 4 horas diárias
( ) Média de 8 horas diárias
( ) De 8 a 12 horas diárias
( ) Mais de 12 horas

Questão 12 – Com relação à política de alteração periódica de senhas da rede AGU (Pode ser selecionada mais de uma opção para resposta).

( ) Utilizo senhas complexas, com grande quantidade de caracteres e que não contenham dados pessoais.
( ) Costumo utilizar senhas com dados que facilitem gravar, como nomes, sobrenomes, datas comemorativas, números de telefones e similares.
( ) Na troca trimestral de senhas dos usuários da rede AGU costumo alternar senhas antigas e/ou a mesma senha acrescentando pequenas mudança de caracteres.
( ) Na troca trimestral de senhas dos usuários da rede AGU sempre adoto nova senha desvinculada a qualquer caractere com a anterior.
( ) Compartilho a mesma senha em diferentes sistemas e/ou contas.

Questão 13 – Já identificou algum sinal de e-mail com conteúdo suspeito com campanhas maliciosas, e-mails de phishing ou spam, golpes ou distribuição de programas maliciosos feitos pelos hackers em seu e-mail corporativo? (Pode ser selecionada mais de uma opção para resposta).

( ) Nunca recebi nenhum e-mail suspeito.
( ) Já recebi e deletei.
( ) Recebi e acessei o link.
( ) Recebi, mas não soube a quem informar acerca do incidente.
( ) Recebi e informei a equipe da DTI, coordenador e/ou administrador de rede.

Questão 14 – Considerando que dentro das normas de segurança da instituição, os softwares e aplicativos devem ser instalados pela TI do órgão, existe algum aplicativo ou site que utiliza para implementar algumas ações como compactar, juntar e dividir arquivos a serem inseridos no Sapiens?

( ) Não utilizo essas funções em minhas atividades.
( ) Utilizo frequentemente essas ações acessando sites de acesso livre e gratuito na Internet.
( ) Desconheço softwares ou aplicativos instalados pela DTI e disponibilizados pela AGU para essa finalidade.
( ) Encaminho essas atividades para a equipe da TI terceirizada.

Questão 15 – Qual a propriedade dos equipamentos tecnológicos utilizados para a prestação do teletrabalho?

( ) Particular
( ) Equipamento da AGU
( ) Não estou em trabalho remoto
( ) Particular e da AGU

Questão 16 – Costuma acessar os sistemas de informação corporativos em dispositivos tecnológicos particulares (celulares e notebooks) fora do ambiente institucional, independente da modalidade de trabalho (presencial, semipresencial ou teletrabalho)?

( ) Sempre acesso.
( ) Frequentemente, porque trabalho na modalidade semipresencial.
( ) Raramente, estou trabalhando na modalidade presencial.
( ) Não costumo acessar.

Questão 17 – Utiliza o acesso a VPN (Virtual Private Network) da AGU para se conectar à rede da AGU através da integração de redes remotas, e qual sua preocupação com segurança do equipamento em relação ao acesso pela VPN?

( ) Não utilizo VPN.
( ) Utilizo VPN e não tenho perfil para atualizar o equipamento da AGU.
( ) Utilizo VPN, mas não tenho conhecimento de segurança do meu equipamento.

Questão 18 – Qual dos canais de comunicação com o Departamento de Tecnologia da Informação (DTI) já recorreu em suas atividades laborais?

( ) Sistema de abertura de chamados OTRS
( ) Atendimento eletrônico 0800
( ) E-mail dti.atendimento@agu.gov.br
( ) Portal de atendimento "chatbot"
( ) E-mail suporte@agu.gov.br
( ) Desconheço os canais

Questão 19 – Qual a importância da adesão ao cadastro da Autenticação Multifator (MFA) implantado pela Diretoria de Tecnologia da Informação (DTI) para segurança da informação corporativa em regime de teletrabalho ou semipresencial? (Pode ser selecionada mais de uma opção para resposta).

( ) Oferece uma camada de proteção adicional aos sistemas corporativos da AGU.
( ) Aumenta a cibersegurança do ambiente corporativo.
( ) Garante a proteção dos dados corporativos por comprovar a identidade do usuário ao acessar dados, aplicativos, serviços web, VPN e serviços confidenciais na nuvem.
( ) Acredito que uma senha complexa seja suficiente para a proteção do sistema.
( ) Desconheço o recurso cadastro da Autenticação Multifator (MFA).

IDENTIFICAÇÃO DA PERCEPÇÃO E PROTAGONISMO DOS USUÁRIOS DE SISTEMAS DE INFORMAÇÃO

As questões discursivas (abertas) possibilitarão trazer indicativos para analisar a percepção dos servidores da PU/SE em relação as interfaces usuário-tecnologia-sistema, com ênfase na Segurança da Informação.

Questão 20 – Relate resumidamente quais as principais ameaças e preocupações relativas à segurança da informação em suas práticas de trabalho na AGU.

Questão 21 – Considerando o seu protagonismo como pessoa usuária dos sistemas de informação na AGU contribua com sugestões de melhorias para a segurança da informação.

Caso seja do seu interesse, deixe aqui seu e-mail para que receba a pesquisa concluída.
Obrigada por responder!
Por favor clique em **enviar.**

ANEXO A – Comprovante do envio do projeto junto ao Comitê de Ética em Pesquisa Envolvendo Seres Humanos (CEP) da Universidade Federal de Sergipe/UFS

UNIVERSIDADE FEDERAL DE SERGIPE - UFS

Plataforma Brasil

COMPROVANTE DE ENVIO DO PROJETO

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: GESTÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO ELETRÔNICA: interfaces homem-máquina-sistema

Pesquisador: Ana Paula Monteiro Almeida Chagas

Versão: 1

CAAE: 64677622.0.0000.5546

Instituição Proponente: FUNDACAO UNIVERSIDADE FEDERAL DE SERGIPE

DADOS DO COMPROVANTE

Número do Comprovante: 122916/2022

Patrocionador Principal: Financiamento Próprio

Informamos que o projeto GESTÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO ELETRÔNICA: interfaces homem-máquina-sistema que tem como pesquisador responsável Ana Paula Monteiro Almeida Chagas, foi recebido para análise ética no CEP Universidade Federal de Sergipe - UFS em 01/11/2022 às 08:51.

Endereço: Rua Cláudio Batista s/nº
Bairro: Sanatório **CEP:** 49.060-110
UF: SE **Município:** ARACAJU
Telefone: (79)3194-7208 **E-mail:** cep@academico.ufs.br

ANEXO B – Parecer consubstanciado do CEP

UNIVERSIDADE FEDERAL DE SERGIPE - UFS

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: GESTÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO ELETRÔNICA: interfaces homem-máquina-sistema

Pesquisador: Ana Paula Monteiro Almeida Chagas

Área Temática:

Versão: 2

CAAE: 64677622.0.0000.5546

Instituição Proponente: FUNDACAO UNIVERSIDADE FEDERAL DE SERGIPE

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 5.877.043

Apresentação do Projeto:

As informações elencadas nos campos “Apresentação do Projeto”, “Objetivo da Pesquisa” e “Avaliação dos Riscos e Benefícios” foram retiradas do arquivo “Informações Básicas da Pesquisa” (PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_1546521.pdf) e do "Projeto Detalhado / Brochura Investigador" (ProjetoCEP.pdf), postados em 02/01/2023.

Introdução:

Novas diretrizes têm fundamentado o uso da informação como valor para as organizações, principalmente com a globalização e a Internet. Essas transformações conduziram a informação ao cerne dos processos informacionais contribuindo para as transformações sociais, econômicas, científicas, tecnológicas e culturais. De uma forma geral, entende-se que são as novas concepções da informação na Sociedade da Informação e do Conhecimento. Diante da relevância dessa temática e das constantes mudanças de sistemas de informação que são duramente implantados e facilmente substituídos, a segurança da informação ocupa um espaço de pesquisa vasto em fenômenos que necessitam um olhar científico que possa contribuir e esclarecer lacunas que carecem de um estudo mais direcionado aos usuários dos sistemas. No campo jurídico, as mudanças tecnológicas se tornaram mais complexas e determinantes, necessitando que os membros e servidores detenham os mais elevados níveis de conhecimento, habilidades técnicas e operacionais que os qualifiquem para atuar de modo ágil e inteligente nas respostas às dificuldades de um panorama judicial com incertezas e de uma administração pública que requer

Endereço: Rua Cláudio Batista s/nº
Bairro: Sanatório **CEP:** 49.060-110
UF: SE **Município:** ARACAJU
Telefone: (79)3194-7208 **E-mail:** cep@academico.ufs.br

Continuação do Anexo B

superiores padrões de eficiência e o máximo de segurança jurídica.

Nesse contexto de mudanças, pode-se ter uma visão mais precisa dessas transformações e observar problemas vivenciados na prática profissional, principalmente no que tange a questão da gestão da segurança da informação no contexto das interfaces usuário-máquina-sistema. A informação jurídica hoje é produzida, organizada e compartilhada por meio de Sistemas de Gerenciamento Eletrônico de Documentos e processos integrados entre os poderes executivo e judiciário. A motivação dessa proponente está voltada para as práticas institucionais, assim como todos os servidores da AGU que trabalham com sistemas de informação integrados com outros sistemas externos e desconhecem em que nível podem estar vulneráveis, podendo provocar danos aos Sistemas de Informação. Esta lacuna foi observada e instigou essa pesquisa voltada para a necessidade de um estudo com intervenção para verificar a percepção dos usuários quanto as questões de vulnerabilidade e possíveis danos nos Sistemas de Informação e sua relação com os sistemas, a partir das normas de Segurança da Informação já estabelecidas pela Advocacia-Geral da União (AGU). Essa pesquisa se justifica pela importância da temática face a incidência de uma série de ataques cibernéticos a organizações mundiais, o que levanta a discussão sobre a relevância de não somente implantar investimentos na área de segurança da informação como forma de proteger os sistemas de informação, mas também de se debruçar de forma mais científica sobre o comportamento do usuário em relação as interfaces homem-máquina-sistema.

Hipótese:

Não se aplica.

Metodologia Proposta:

Com relação a natureza prática da pesquisa, por se tratar de uma intervenção que resulta em um produto técnico-científico, permite-se o seu enquadramento como pesquisa aplicada. Com base em seus objetivos, foi possível classificar esta pesquisa com alcance descritivo, a qual “descreve tendências de um grupo ou população” (SAMPIERI; COLLADO; LUCIO, 2013, p. 102). Os objetivos dessa pesquisa pretendem descrever uma situação real estabelecendo diferentes variáveis. A abordagem escolhida para este estudo foi direcionada junto aos objetivos traçados, os quais, envolvem dados numéricos e análise de texto. Determinou-se a abordagem quali-quantitativa por potencializar a análise dos dados e “conseguir uma perspectiva mais ampla e profunda do fenômeno” (SAMPIERI; COLLADO; LUCIO, 2013, p. 552).

Em síntese, essa pesquisa está caracterizada como pesquisa aplicada, de abordagem quali-quantitativa, de objetivos descritivos, realizada por meio de uma pesquisa bibliográfica, de campo e pesquisa-ação por se tratar de uma intervenção. O local de aplicação da intervenção proposta,

Continuação do Anexo B

com anuência prévia, é a Procuradoria da União em Sergipe (PU/SE), localizada na Avenida Beira Mar, nº 53, Treze de Julho, na cidade de Aracaju em Sergipe. A população dessa pesquisa será constituída pelos servidores que integram o quadro funcional da Procuradoria da União no Estado de Sergipe (PU/SE), divididos em diferentes categorias e funções, a saber: 13 (treze) Advogados da União, 16 (dezesseis) servidores técnico administrativos efetivos, 8 (oito) servidores técnico-administrativos requisitados (cedidos à União), 4 (quatro) empregados terceirizados e 1 (um) estagiário (a), todos lotados naquela unidade administrativa. Optou-se por atribuir siglas aos participantes da pesquisa seguindo uma sequência alfanumérica, em que: 13 Advogados da União (ADV1), 16 servidores técnico-administrativos (STA1), 8 servidores cedidos (SCD1), 4 empregados terceirizados (ETERC1) e 1 estagiário (a) (ESTAG1), todos seguindo uma ordem crescente de participantes. Esta divisão em categorias se faz importante porque a atuação dos Advogados da União possui maior complexidade de acesso aos sistemas judiciários, seguido dos trabalhos desenvolvidos pelos servidores técnico-administrativos, que assessoram a atividade fim com acesso a todos os sistemas. Os servidores cedidos de outros órgãos, em sua maioria, desempenham suas funções no Núcleo de Cálculos e Perícias, os quais acessam além do SAPIENS, outros sistemas específicos e os empregados terceirizados utilizam o sistema da AGU com perfil para cadastro e tramitação de processos. A coleta dos dados será feita através de questionário estruturado, online, aplicado junto aos participantes incluídos nos critérios de seleção da amostra da pesquisa, os quais tem acesso aos sistemas gerenciais da PU/SE para desempenharem suas funções. Para elaboração das questões serão utilizadas as fontes teóricas de referência que tratem da temática para se explorar o comportamento dos usuários sob a perspectiva da sua percepção prática em confronto com a análise das normas de segurança da informação estabelecidas pela organização da pesquisa e pela literatura científica. Dessa forma, pode-se compreender e monitorar os principais riscos e incidências. O questionário deverá explorar questões objetivas e subjetivas, haja visto a pesquisa possui uma abordagem quali-quantitativa, sendo as perguntas formuladas a partir das bases teóricas dos estudos no campo da Segurança da Informação, com ênfase no comportamento dos usuários nas interfaces homem-máquina-sistema. Nesse sentido, o questionário contará com perguntas do tipo aberta, para analisar os dados qualitativos e perguntas fechadas para analisar os dados quantitativos. Será utilizado o questionário com escala do tipo Likert.

Critério de Inclusão:

Participantes que possuem acesso ao Sistema AGU de Inteligência Jurídica (SAPIENS).

Critério de Exclusão:

Continuação do Anexo B

Participantes que não possuem acesso ao Sistema AGU de Inteligência Jurídica (SAPIENS).
Metodologia de Análise de Dados:
As variáveis que se pretende explorar correspondem ao usuário na pessoa do homem, o comportamento dos usuários dos sistemas na variável máquina e os sistemas quanto aos riscos da segurança da informação no acesso e utilização. Será dado o anonimato aos participantes da pesquisa.
Analisar-se-á a percepção e comportamento dos usuários do sistema Sapiens AGU e, por último, quanto ao uso do sistema de informação, na variável máquina, serão mapeados os principais riscos identificados na análise qualitativa e quantitativa das respostas às perguntas. O link para acesso ao questionário online será encaminhado através do e-mail institucional dos participantes inclusos na amostra selecionada, acompanhado do Termo de Consentimento Livre e Esclarecido (TCLE), em forma de convite, contendo todas as informações sobre a pesquisa e os direitos que são assegurados aos seus participantes. Para fins de análise de dados, após aplicação dos questionários será realizada a análise estatística com representação gráfica dos dados, identificando o comportamento dos usuários e demais variáveis que apontem a ocorrência de riscos de segurança da informação envolvendo o homem, máquina e sistema. Devido a abordagem mista da pesquisa, a análise qualitativa será realizada através do método análise de conteúdo, categorizando as variáveis identificadas pela percepção dos participantes de pesquisa, usuários dos sistemas.

Objetivo da Pesquisa:
Objetivo Primário:
Identificar o comportamento dos servidores da Procuradoria da União em Sergipe em relação as interfaces homem-máquina-sistema, a partir das normas e políticas de segurança estabelecidas pela Advocacia Geral da União (AGU), visando criar um Manual de Boas Práticas de Segurança da Informação para os usuários dos sistemas.
Objetivo Secundário:
• Investigar elementos indicadores de falhas de segurança a partir da percepção dos participantes da pesquisa propondo estratégias alternativas de gestão de segurança da informação que envolva as interfaces homem-máquina-sistema;
• Analisar o comportamento e as atitudes dos usuários dos sistemas com relação as normas de segurança da informação preestabelecidas pela organização com o objetivo de identificar as principais circunstâncias em que ocorrem as falhas de segurança e como prevenir os incidentes;
• Mapear os principais incidentes de risco para a segurança da informação identificados através de

Continuação do Anexo B

levantamento do trabalho de campo para propor boas práticas de segurança da informação não vislumbradas pela organização.

Avaliação dos Riscos e Benefícios:

Riscos:

Quanto à avaliação dos riscos e benefícios estão fundamentados nas Resoluções vigentes (Res. 466/2012 do CNS e Res. 510/2016 do CNS), conforme a Metodologia do Estudo. Dessa forma serão cumpridas e respeitadas todas as normas e exigências contidas no Capítulo V da Resolução CNS nº 466/2012 (Dos Riscos e Benefícios), bem como do Capítulo IV da Resolução CNS nº 510/2016 (Dos Riscos).De acordo com a Res. 466/2012 da CNS/MS "toda pesquisa com seres humanos acarreta riscos" e um risco comum a todas essas pesquisas é a quebra de sigilo involuntário e não intencional, mesmo com a busca dos pesquisadores pela garantia da manutenção deste, a exemplo de "riscos caraterísticos do ambiente virtual, meios eletrônicos, ou atividades não presenciais, em função das limitações das tecnologias utilizadas, pois existem limitações dos pesquisadores para assegurar total confidencialidade e potencial risco de sua violação", conforme item 1, 1.2.1, da Carta Circular nº 1/2021- CONEP/SECNS/MS, de 03 de março de 2021.Todo experimento com seres humanos apresenta risco de constrangimento pela observação social, que escapa ao senso comum. O risco de cunho emocional poderá ser proporcional à frustração na consecução da atividade proposta, porém esse risco será minimizado pelo BENEFÍCIO DIRETO a partir da contribuição que o (a) Sr. (a) está dando, pois através da análise gerada pelos dados coletados nessa pesquisa espera-se colaborar com os seus participantes em seu ambiente organizacional, com o objetivo de contribuir por meio dos critérios científicos com as boas práticas para a Segurança da Informação. No caso dessa pesquisa também podem haver riscos de constrangimento por parte do participante, por se tratar de sua participação em resposta a um questionário com perguntas relativas ao comportamento dos usuários dos sistemas em relação as variáveis que implicam na segurança da informação e dos seus riscos.Entretanto, a pesquisadora compromete-se a respeitar e cumprir os critérios da ética em pesquisa, bem como seguir as orientações para procedimentos em pesquisas com qualquer etapa em ambiente virtual e acredita que adotando uma atitude respeitosa e cuidadosa com o participante poderá contornar constrangimentos. Desse modo, visando reduzir quaisquer riscos ou incômodos, orienta que o (a) Sr. (a) não participe dessa pesquisa caso não esteja confortável com a temática abordada, se mesmo ciente da confidencialidade de sua participação isso possa levar a conflitos de qualquer natureza, se ao preencher o questionário online perceba algum tipo de desconforto, constrangimento ou alterações de comportamento.

Benefícios:
Espera-se colaborar com os seus participantes em seu ambiente organizacional, com o objetivo de contribuir por meio dos critérios científicos com as boas práticas para a segurança da informação. Outro benefício dessa pesquisa se justifica pela importância da temática face a incidência de uma série de ataques cibernéticos a organizações mundiais, o que levanta a discussão sobre a relevância de não somente implantar investimentos na área de segurança da informação como forma de proteger os sistemas de informação, mas também de se debruçar de forma mais científica sobre o comportamento do usuário em relação as interfaces homem-máquina-sistema. Nesse contexto, acredita-se que a pesquisa, por seu caráter exploratório e de intervenção, possa promover mudanças na cultura organizacional da Procuradoria da União em Sergipe, por sua proposta em identificar o comportamento dos usuários com relação a gestão de segurança dos sistemas de informação eletrônica com ênfase nas interfaces homem-máquina-sistema.

Comentários e Considerações sobre a Pesquisa:
Considerando que os usuários podem provocar ou estarem vulneráveis a eventuais danos nos Sistemas de Informação, torna-se pertinente verificar se estão sensibilizados para a utilização de práticas corretas e seguras no desempenho das suas tarefas quanto à Segurança da Informação (SI), a presente pesquisa tem à intenção de Identificar o comportamento dos servidores da Procuradoria da União em Sergipe (PU/SE), em relação as interfaces homem-máquina-sistema, a partir das normas e políticas de SI estabelecidas pela Advocacia-Geral da União (AGU), visando criar um Manual de Boas Práticas de Segurança da Informação para os usuários dos sistemas. Essa pesquisa está caracterizada como pesquisa aplicada, de abordagem quali-quantitativa, de objetivos descritivos, realizada por meio de uma pesquisa bibliográfica, de campo e pesquisa ação por se tratar de uma intervenção.
Tamanho da Amostra no Brasil: 42
*22 PARTICIPANTES POTENCIAIS - Apresentação do projeto, esclarecendo sobre a temática e seus objetivos junto aos membros, servidores e prestadores de serviços terceirizados da
Procuradoria da União em Sergipe.
*PARTICIPANTES REAIS - Encaminhar questionário através do e-mail institucional aos participantes da pesquisa.

Considerações sobre os Termos de apresentação obrigatória:
Vide campo "Conclusões ou Pendências e Lista de inadequações"

Continuação do Anexo B

UNIVERSIDADE FEDERAL DE SERGIPE - UFS

Continuação do Parecer: 5.877.043

Conclusões ou Pendências e Lista de Inadequações:

Análise das respostas (arquivo: "CARTA_RESPOSTA_AS_PENDENCIAS.pdf", postado na Plataforma Brasil em 02/01/2023) ao Parecer Consubstanciado n°5.793.469 emitido em 05/12/2022 não foram observados óbices éticos.

Considerações Finais a critério do CEP:

Conforme Resolução CNS 466/2012, itens X.1.- 3.b. e XI.2.d, e Resolução CNS 510/2016, Art. 28, inc. V, os pesquisadores responsáveis deverão apresentar relatórios parcial semestral e final do projeto de pesquisa, contados a partir da data de aprovação do protocolo de pesquisa inicial.

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_2035973.pdf	02/01/2023 20:33:37		Aceito
Outros	CARTA_RESPOSTA_AS_PENDENCIAS.pdf	02/01/2023 20:30:58	Ana Paula Monteiro Almeida Chagas	Aceito
Projeto Detalhado / Brochura Investigador	PROJETO_DE_PESQUISA_ADEQUADO.pdf	02/01/2023 20:29:17	Ana Paula Monteiro Almeida Chagas	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TERMO_DE_CONSENTIMENTO_LIVRE_E_ESCLARECIDO_ADEQUADO.pdf	02/01/2023 20:27:59	Ana Paula Monteiro Almeida Chagas	Aceito
Projeto Detalhado / Brochura Investigador	PROJETO_DE_PESQUISA.pdf	27/10/2022 22:53:11	Ana Paula Monteiro Almeida Chagas	Aceito
Declaração de Pesquisadores	DECLARACAO_QUE_A_PESQUISA_E_A_COLETA_DE_DADOS_AINDA_NAO_FORAM_INICIADAS.pdf	27/10/2022 22:12:51	Ana Paula Monteiro Almeida Chagas	Aceito
Folha de Rosto	FOLHA_DE_ROSTO_PARA_PESQUISA_ENVOLVENDO_SERES_HUMANOS.pdf	27/10/2022 22:06:08	Ana Paula Monteiro Almeida Chagas	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TERMO_DE_CONSENTIMENTO_LIVRE_E_ESCLARECIDO.pdf	27/10/2022 21:11:49	Ana Paula Monteiro Almeida Chagas	Aceito
Declaração de Pesquisadores	DECLARACAO_DE_COMPROMISSO_EM_OBSERVAR_A_RESOLUCAO_N_196_DE_10_10_1996.pdf	27/10/2022 12:39:58	Ana Paula Monteiro Almeida Chagas	Aceito
Declaração de Pesquisadores	TERMO_DE_COMPROMISSO_PARA_UTILIZACAO_DE_DADOS.pdf	23/10/2022 21:13:55	Ana Paula Monteiro Almeida Chagas	Aceito

Endereço: Rua Cláudio Batista s/nº
Bairro: Sanatório **CEP:** 49.060-110
UF: SE **Município:** ARACAJU
Telefone: (79)3194-7208 **E-mail:** cep@academico.ufs.br

Conclusão do Anexo B

UNIVERSIDADE FEDERAL DE SERGIPE - UFS

Continuação do Parecer: 5.877.043

Declaração de Pesquisadores	TERMO_DE_COMPROMISSO_E_CONFIDENCIALIDADE.pdf	23/10/2022 21:13:35	Ana Paula Monteiro Almeida Chagas	Aceito
Orçamento	ORCAMENTO.pdf	23/10/2022 21:12:33	Ana Paula Monteiro Almeida Chagas	Aceito
Declaração de Instituição e Infraestrutura	DECLARACAO_DE_INSTITUICAO_E_INFRAESTRUTURA.pdf	23/10/2022 21:05:08	Ana Paula Monteiro Almeida Chagas	Aceito
Cronograma	CRONOGRAMA.pdf	23/10/2022 21:03:31	Ana Paula Monteiro Almeida Chagas	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

ARACAJU, 06 de Fevereiro de 2023

Assinado por:
FRANCISCO DE ASSIS PEREIRA
(Coordenador(a))

Endereço: Rua Cláudio Batista s/nº
Bairro: Sanatório **CEP:** 49.060-110
UF: SE **Município:** ARACAJU
Telefone: (79)3194-7208 **E-mail:** cep@academico.ufs.br

ANEXO C – Termo de anuência e existência de infraestrutura

ADVOCACIA-GERAL DA UNIÃO
PROCURADORIA DA UNIÃO EM SERGIPE
GABINETE
Avenida Beira Mar, nº 53, 13 de julho – Aracaju/SE, CEP: 49.020-010
Telefone n. º: (79) 3301-6850

TERMO DE ANUÊNCIA E EXISTÊNCIA DE INFRAESTRUTURA

Eu, **Andrea Carla Veras Lins, Procuradora Chefe da União na Procuradoria da União no Estado de Sergipe,** autorizo a realização do projeto intitulado "**GESTÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO ELETRÔNICA: INTERFACES HOMEM-MÁQUINA-SISTEMA**" pela pesquisadora **Ana Paula Monteiro Almeida Chagas**, Servidora cedida pela Universidade Federal de Sergipe– Campus São Cristóvão/SE a esta Procuradoria, que envolve uma pesquisa de Mestrado Profissional do Programa de Pós-Graduação em Ciência da Informação pela Universidade Federal de Sergipe (UFS) para a obtenção do título de Mestre em Gestão da Informação e do Conhecimento.

O objetivo da pesquisa consiste **identificar o comportamento dos usuários da Procuradoria da União em Sergipe em relação a interface homem-máquina-sistema a partir das normas e políticas de segurança estabelecidas pela Advocacia Geral da União, visando criar um Manual de Boas Práticas de Segurança da Informação para os usuários dos sistemas,** contando como participantes da pesquisa os servidores que trabalham na Procuradoria da União no Estado de Sergipe, sendo a amostra selecionada a partir dos servidores técnico-administrativos, Advogados da União e servidores cedidos, todos em exercício na PU/SE e que possuam acesso ao sistema Sapiens e sistemas integrados, mediante o compromisso firmado pela pesquisadora no termo de compromisso de pesquisador responsável e no termo de compromisso e confidencialidade, e com a adoção das **MEDIDAS DE PROTEÇÃO AO ENFRENTAMENTO DA COVID-19**, sendo o projeto totalmente desenvolvido virtualmente, sem necessidade de contato físico ou direto, através da aplicação de questionários encaminhados via e-mail institucional, e será iniciada após aprovação pelo Comitê de Ética em Pesquisa da Universidade Federal de Sergipe (CEP/UFS).

Estamos cientes de seu compromisso no resguardo da segurança e bem-estar dos participantes da pesquisa, dispondo de infraestrutura necessária para desenvolvê-la em conformidade às diretrizes e normas éticas. Ademais, ratifico que não haverá quaisquer implicações negativas aos servidores técnico-administrativos, Advogados da União e servidores cedidos que não desejarem ou desistirem de participar do projeto.

Declaro, outrossim, na condição de representante desta Instituição, conhecer e cumprir as orientações e determinações fixadas nas Resoluções nos 466, de 12 de dezembro de 2012, e 510, de 07 de abril de 2016, e Norma Operacional no 001/2013, pelo CNS.

Conclusão do Anexo E[3]

2

Aracaju, 8 de março de 2022.

ANDREA CARLA VERAS LINS [redacted] Assinado de forma digital por ANDREA CARLA VERAS LINS:[redacted] Dados: 2022.03.18 20:03:42 -03'00'

ANDREA CARLA VERAS LINS
PROCURADORA-CHEFE DA UNIÃO EM SERGIPE

2 de 2

[3] De acordo com a Lei Geral de Proteção de Dados - LGPD (Lei n. 13709/2018), o número do CPF na assinatura do documento foi devidamente marcado e coberto com tinta azul, a fim de preservar os direitos relacionados aos dados pessoais da subscritora.