Sociedade Brasileira de Computação (SBC) - CNPJ: 29.532.264/0001-78

SBSi 2025

21ª Edição - Recife - Pernambuco

XXI Simpósio Brasileiro de Sistemas de Informação

Inovação com Equidade, Diversidade e Inclusão em Sistemas de Informação

MINICURSOS EM SI

TÓPICOS ESPECIAIS EM SISTEMAS DE INFORMAÇÃO

Organizadoras:
Claudia Cappelli (UERJ)
Fátima de Lourdes dos Santos Nunes (USP)

Organizadoras da Trilha
Claudia Cappelli
Fátima de Lourdes dos Santos Nunes

TÓPICOS ESPECIAIS EM SISTEMAS DE INFORMAÇÃO
Trilha de Minicursos em Sistemas de Informação
SBSI 2025

https://sbsi2025.cesar.school
https://books-sol.sbc.org.br/index.php/sbc/catalog/category/si

Sociedade Brasileira da Computação
Porto Alegre
2025

TÓPICOS ESPECIAIS EM SISTEMAS DE INFORMAÇÃO
Trilha de Minicursos em Sistemas de Informação
SBSI 2025

Sociedade Brasileira de Computação –SBC
CNPJ: 29.532.264/0001-78

Coordenação de Publicações
Allysson Allex Araújo (UFCA)

Coordenação da Trilha de Minicursos em Sistemas de Informação
Claudia Cappelli (UERJ)
Fátima de Lourdes dos Santos Nunes (USP)

Coordenação de Programa
Mônica Ximenes Carneiro da Cunha (IFAL)

Coordenação Geral
George Valença (UFRPE)
Ronnie de Souza Santos (CESAR School e University of Calgary)

Editora
Sociedade Brasileira de Computação – SBC

2025

Realização

Organização

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

Patrocínio

Apoio

Editores

Comitê Técnico

Membros da Comissão Especial de Sistemas de Informação da SBC (CE-SI)

Coordenação da CE-SI (2024-2025)

Célia Ghedini Ralha (UnB) - Coordenadora CE-SI
Rodrigo Pereira dos Santos (UNIRIO) - Vice-coordenador CE-SI

Comitê Gestor da CE-SI (2024-2025)

Alessandreia Marta de Oliveira Julio (UFJF)
Célia Ghedini Ralha (UnB)
Claudia Cappelli (UERJ)
José Maria David (UFJF)
Maria Claudia Figueiredo Pereira Emer (UTFPR)
Mônica Ximenes Carneiro da Cunha (IFAL)
Renata Araujo (Universidade Presbiteriana Mackenzie)
Rodrigo Pereira dos Santos (UNIRIO)
Sean Wolfgand Matsui Siqueira (UNIRIO)
Tadeu Moreira de Classe (UNIRIO)
Valdemar Vicente Graciano Neto (UFG)
Vera Maria Benjamim Werneck (UERJ)
Williamson Alison Freita Silva (UNIPAMPA)

Membros do Comitê Diretivo do SBSI 2025 (CD-SBSI)

Coordenação do Comitê Diretivo (2024-2025)

Williamson Silva (UNIPAMPA) - Coordenador do CD-SBSI
Allysson Allex Araújo (UFCA) - Vice-coordenador do CD-SBSI

Comitê Diretivo (2024-2025)

Allysson Allex Araújo (UFCA)
Davi Viana (UFMA)
George Valença (UFRPE)
Johnny Cardoso Marques (ITA)
José Maria David (UFJF)
Mônica Ximenes Carneiro da Cunha (IFAL)
Rita Suzana Pitangueira Maciel (UFBA)
Ronnie de Souza Santos (CESAR School e University of Calgary)
Victor Ströele (UFJF)
Williamson Alison Freita Silva (UNIPAMPA)

Comitê de Programa – Trilha de Minicursos em Sistemas de Informação do SBSI 2025

Alessandro Cerqueira (FAETERJ)
Alex Borges (UFJF)
André Freire (UFLA)
Andre Martinotto (UCS)
Awdren Fontão (UFMS)
Carla Merkle Westphall (UFSC)
Carlos Santos Pires (UFCG)
Carlos Eduardo de Barros Paes (PUC-SP)
Daniel Notari (UCS)
Edmundo Spoto (UFG)
Emanuel Coutinho (UFC)
Fatima Nunes (USP)
Felipe Cordeiro (UNIRIO)
Fernanda Baião (PUC-Rio)
Fernanda Maria Santos (UFU)
Flavia Maria Santoro (UERJ)
Flávio Soares Corrêa da Silva (USP)
Francisco Henrique Ferreira (UFJF)
Glauco Carneiro (UFS)
Heitor Costa (UFLA)
Jorge Barbosa (Unisinos)
Jorge Júnior (UFPB)
José Maria David (UFJF)
Juliano Lopes de Oliveira (UFG)
Leila Bergamasco (FEI)
Leonardo Silva (UFMS)
Marcos Chaim (USP)
Maria Istela Cagnin (UFMS)
Morganna Diniz (UNIRIO)
Paulo Malcher (UFRA)
Paulo Sérgio Santos (UNIRIO)
Rafael Testa (USP)
Renata Araujo (Universidade Presbiteriana Mackenzie)
Ricardo Choren (IME-RJ)

Dados Internacionais de Catalogação na Publicação (CIP)

S612 Simpósio Brasileiro de Sistemas de Informação (21. : 19 – 23 maio 2025 : Recife)

Minicursos do SBSI 2025 [recurso eletrônico] / organização: Claudia Cappelli... [et al.]. – Dados eletrônicos. – Porto Alegre: Sociedade Brasileira de Computação, 2025.

102 p. : il. : PDF ; 30 MB

Modo de acesso: World Wide Web.
ISBN 978-85-7669-629-2 (e-book)

1. Computação – Brasil – Evento. 2. Sistemas de informação. 3. Inovações. I. Cappelli, Claudia. II. Nunes, Fátima de Lourdes dos Santos. III. Valença, George. IV. Santos, Ronnie de Souza. V. Sociedade Brasileira de Computação. VI. Título.

CDU 004(063)

Ficha catalográfica elaborada por Annie Casali – CRB-10/2339
Biblioteca Digital da SBC – SBC OpenLib

Prefácio:
Comissão Especial de Sistemas de Informação (CESI) da Sociedade Brasileira de Computação (SBC)

Prezados participantes do XXI Simpósio Brasileiro de Sistemas de Informação (SBSI),

Em nome do Comitê Gestor da Comissão Especial de Sistemas de Informação da Sociedade Brasileira de Computação (CESI/SBC), gostaríamos de dar as boas-vindas a mais uma edição do SBSI. A CESI congrega pesquisadores e profissionais de Sistemas de Informação (SI) e realiza a gestão desta área no Brasil no contexto da SBC. O seu trabalho consiste em articular políticas para divulgação, fortalecimento, consolidação e melhoria da qualidade da educação, pesquisa, inovação e atuação em SI no Brasil, promovendo e propondo importantes atividades para o desenvolvimento e consolidação desta área em nosso país. O SBSI é uma das principais ações da CESI. Por esta razão, ficamos felizes que autores submetam seus trabalhos, que avaliadores se esforcem para dar o melhor feedback possível em suas revisões e que coordenadores consigam realizar momentos memoráveis para que, assim, a comunidade se fortaleça, atraia mais participantes e se consolide no país. Neste sentido, a CESI convoca a comunidade de SI a ser cada vez mais ativa e os participantes do SBSI a se envolverem e trazerem novos pesquisadores para o evento, fazendo a comunidade crescer e solidificar as suas pesquisas.

O SBSI é o fórum mais importante do Brasil na área de SI e reúne anualmente pesquisadores de todo o país. Este ano, o SBSI aconteceu em Recife, Pernambuco, sob a coordenação geral dos professores George Valença (UFRPE) e Ronnie de Souza Santos (CESAR School e University of Calgary), em conjunto com os professores Williamson Silva (UNIPAMPA) e Allysson Araújo (UFCA), que coordenaram o Comitê Diretivo do SBSI 2024-2025, e com a professora Mônica Ximenes (IFAL), que coordenou o Comitê de Programa Geral do SBSI 2025. Após vários meses de trabalho e dedicação dos professores e sua equipe de organização local, disponibilizamos à comunidade de SI uma programação rica, diversificada, abrangente, e sólida, de forma a comunicar os resultados mais recentes da pesquisa na área de SI no Brasil. O evento tem crescido consideravelmente nos últimos anos. Tal feito é reflexo da consolidação da área, que somente tem sido possível devido ao apoio crescente de toda a comunidade de SI. O SBSI 2025 é composto por várias atividades em paralelo, que incluem as sessões técnicas, palestras, painéis, master classes e cinco

trilhas: Trilha de Pesquisa em SI; Trilha de Indústria e Inovação em SI; Trilha de Temas, Ideias e Resultados Emergentes em SI; Concurso de Teses, Dissertações e Trabalhos de Graduação em SI; e Trilha de Minicursos em SI. Além disso, esse ano foram adicionados uma competição de inovação para estimular a criação de soluções inclusivas e equitativas em SI (Ideathon) e o GranDSI-BR para discutir os Grandes Desafios de Pesquisa em SI no Brasil para os próximos dez anos (2026-2036). Todos os trabalhos aceitos e apresentados nas demais trilhas além da Trilha de Pesquisa em SI são publicados nos Anais Estendidos do SBSI, também disponibilizados abertamente para a comunidade, e o material didático na forma de capítulos oriundos dos minicursos são publicados como um e-book.

O Comitê de Programa da Trilha de Minicursos em SI, coordenado pelas professoras Claudia Cappelli (UERJ) & Fátima de Lourdes dos Santos Nunes (USP), trabalhou arduamente e de forma exímia para que os trabalhos mais maduros e de maior qualidade pudessem ser trazidos à comunidade brasileira de SI. Tal trabalho de seleção rigoroso foi fruto de uma confiança plena na qualidade dos trabalhos veiculados nesse simpósio em 2025. O impacto do trabalho realizado pelo comitê de programa e pelos autores dos capítulos de minicursos, potencializando a abrangência e alcance da produção científica do SBSI, também é observado pelo fato dos anais do SBSI serem indexados e acessíveis mundialmente pela base DBLP. Em tempo, é importante ressaltar que os anais do SBSI, os anais estendidos do SBSI e o livro de minicursos em SI estão sendo indexados e disponibilizados no Portal de Publicações e Conteúdo Digital da SBC (SBC OpenLib - SOL).

Por fim, agradecemos a todos os participantes, colaboradores, coordenadores, patrocinadores, apoiadores e organizadores que tornaram o evento possível mais uma vez, sobretudo em mais um período repleto de desafios para a humanidade.

Desejamos a todos um excelente SBSI 2025!

Um grande abraço,

Célia Ghedini Ralha (UnB)
Coordenadora da CESI/SBC -2024-2025

Rodrigo Santos (UNIRIO)
Vice-Coordenador da CESI/SBC –2024-2025

Célia Ghedini Ralha holds a PhD from the University of Leeds, England (1996), a master's degree in Electronics and Computer Engineering from the Instituto Tecnológico de Aeronáutica-ITA (1990), and a post-doctorate from the Brandenburgische Technische Universität Cottbus, Germany (2012-2013). Associate Professor IV at the Department of Computer Science at the University of Brasília (UnB, 2002-2017), where she served as coordinator of the Bachelor's Degree in Computer Science (2004-2006) and head of the department during two terms (2006-2010). She collaborated with the Dean of Research and Postgraduate Studies (DPP) at UnB as Director of Institutional Development and Innovation (2010-2012). She has been a member of the Postgraduate Program in Informatics at UnB since its creation in 2003, having been coordinator in the 2015-2017 biennium, when the program received a Grade 5 from CAPES. She was a visiting professor in the Postgraduate Program in Informatics at the Department of Computer Science at the Institute of Exact Sciences at UnB (2020-2022). She was a visiting professor at the Australian National University (ANU) in Canberra, Australia (April-May 2024). She is currently a visiting professor in the Postgraduate Program in Computer Science at the Federal University of Bahia (UFBA). She has broad experience in academic supervision, having supervised 48 undergraduate monographs and 30 scientific initiation works, 8 specialization monographs, 34 master's theses, 9 doctoral theses, and one post-doctorate. She has experience in Computer Science with a focus on intelligent systems, particularly using agent-based models, multi-agent systems, and agent-based simulation. According to the SCOPUS classification, her publications focus on the following areas: Computer Science, Mathematics, Engineering, Decision Science, Business and Management, with topics of greatest contribution 2018-2022, heuristics, linear temporal logic, and planning technology. She leads the research group InfoKnow - Computer Systems for Information and Knowledge Treatment (accredited by CNPq). She is a senior member of the Brazilian Computing Society (SBC) and general coordinator of the Special Information Systems Commission (CESI) in 2013-2015 and 2024-2025, having been vice coordinator in the 2010-2011 biennium. She was coordinator of the Thesis and Dissertation Competition (CTD) of the Congress of the Brazilian Computing Society (CSBC'2024) and General Coordinator of the 18th Workshop-School of Agent Systems, their Environments and Applications (WESAAC'2024) financed by the International Foundation for Autonomous Agents and Multiagent Systems (IFAAMAS). She has been editor-in-chief of SBC's Electronic Journal of Initiation Scientific Computation (REIC) since 2024 and associate editor of Springer's Knowledge and Information Systems (KAIS) since 2022.

Rodrigo Pereira dos Santos is an Associate Professor at the Department of Applied Informatics at the Federal University of the State of Rio de Janeiro (UNIRIO, Brazil) and Head of the Complex Systems Engineering Laboratory (LabESC). He is Research Productivity Fellow Level 2 by the Brazilian National Council for Scientific and Technological Development (CNPq, Brazil) and Young Scientist Fellow by the Carlos Chagas Filho Research Support Foundation of the State of Rio de Janeiro (FAPERJ, Brazil). PhD in Software Engineering from the Federal University of Rio de Janeiro (COPPE/UFRJ, Brazil). He was Academic Visitor at University College London (UCL, UK) and Postdoc Researcher at COPPE/UFRJ. His research interests are Complex Systems Engineering (especially software ecosystems and systems-of-systems), Human and Social Aspects in Software Engineering, Software Business, Software Engineering Education and Training, Requirements Engineering, and Research Methods in Software Engineering and Information Systems. He also worked in several projects related to software process improvement and reuse management in large companies at Coppetec Foundation (2008-2017). He was also lecturer at Brazilian Open University, COPPE/UFRJ, UNIRIO, Infnet Institute, and Santa Úrsula University (2007-2017). He has been a member of the Education Evaluating Commission at the Brazilian Ministry of Education since 2011. He is member of the Association for Computing Machinery (ACM) since 2014 and Brazilian Computer Society (SBC) since 2008, in which he is/was member of the Special Commissions of Information Systems (CE-SI, member since 2017, coordinator 2019-2022, and vice-coordinator 2022-2025), Games and Entertainment Computing (CE-Jogos, 2022-2024), Software Engineering (CE-ES, 2021-2022), and Computer Science Education (GIEC, 2020-2024). He is also a steering committee member for WASHES@CSBC, BraSNAM@CSBC, and SBQS, as well as SBGames (2020-2022). He was Editor-in-Chief (2017-2021) and is associate editor (2021-current) of iSys: Brazilian Journal of Information Systems and of JBCS: Journal of the Brazilian Computer Society (2024-current). He was guest editor for special issues/sections in scientific journals such as Information and Software Technology (Elsevier), Journal of Software: Evolution and Process (Wiley), Communications in Computer and Information Science (Springer), Journal of Internet Services and Applications (SBC Springer), and Journal of the Brazilian Computer Society (SBC Springer). He is the steering committee chair for SESoS@ICSE and also served as PC member for ICSE-RT, ICSE-SEET, CSEET, FSE-SEET, FSE-Demonstrations, ICSE-SCORE, SESoS, ECSA, ECSA-Tools, ECSA-DEI, ICSAW, MODELS, ICSOB, CIbSE, IWSiB, ECIS, ISD, ACM MEDES etc., as well as reviewer for IEEE TSE, EMSE, JSS, IST, COMIND, ESWA, SCP, JSEP, FGCS, IJDRR etc. My ORCID (scientific profile with all social/academic networks): https://orcid.org/0000-0003-4749-2551.

Prefácio:
Trilha de Minicursos em Sistemas de Informação do SBSI 2025

Este livro reúne trabalhos apresentados nos minicursos ministrados no XXI Simpósio Brasileiro de Sistemas de Informação (SBSI 2025). O evento contou com a organização compartilhada entre a Universidade Federal Rural de Pernambuco (UFRPE) e a CESAR School, no período de 19 a 23 de maio de 2025. Participam do SBSI, fórum nacional de debates da área de Sistemas de Informação (SI), estudantes e pesquisadores com apresentação de trabalhos científicos e discussão de temas contemporâneos relacionados à área. Esta edição foi realizada presencialmente. O SBSI 2025 estabeleceu como temática principal "**Inovação com Equidade, Diversidade e Inclusão em Sistemas de Informação**". A escolha desta temática reflete a urgência e a importância de se discutir como os sistemas de informação podem ser desenvolvidos de maneira a promover uma sociedade mais justa e igualitária. Inovação com Equidade, Diversidade e Inclusão (EDI) vai além da criação de novas tecnologias; trata-se de garantir que estas inovações sejam acessíveis e benéficas para todas as pessoas, independentemente de suas origens, identidades ou condições socioeconômicas.

Neste ano, foram submetidas 10 (dez) propostas de minicursos válidos e 3 (três) foram selecionadas, tal qual decidido em reunião da Comissão Especial de Sistemas de Informação. Tais propostas foram avaliadas por, no mínimo, três professores doutores que fizeram parte do comitê científico da trilha de Minicursos do SBSI 2025.

Os três minicursos contidos neste livro abordam tópicos de interesse da comunidade de Sistemas de Informação. O primeiro capítulo, intitulado **"Controles de Segurança para Conformidade baseados em Ferramentas Livres"** apresenta normativas selecionadas do Bureau de Segurança Institucional da Presidência da República do Brasil focadas em gestão de segurança da informação e do Programa de Segurança da Informação e Privacidade do Governo Brasileiro (PPSI) para apresentar e comparar as ferramentas e mecanismos que apoiam um início rápido para a implementação de um programa de segurança em uma organização. O segundo capítulo, intitulado **"A Importância dos Sistemas de Informação para a Participação Pública, o Controle Social e o Controle Interno: Um Estudo de Caso da Prefeitura do Recife"** propõe uma introdução ao uso de Sistemas de Informação como ferramentas para fortalecer a transparência pública e o controle social, sem exigir conhecimentos prévios dos participantes. Já o terceiro e último, intitulado **"MeTA na Prática: Um Método para avaliação Tecnologias Inclusivas"**, propõe um

método inspirado no Design Universal, para promover o entendimento de acessibilidade a partir de uma perspectiva inclusiva, oferecendo 70 normativas e planilhas de avaliação para capacitar e instrumentalizar pessoas em processos de avaliação de tecnologias.

Esperamos que este livro auxilie estudantes, pesquisadores e profissionais da área de Sistemas de Informação na construção do conhecimento em temas específicos relacionados ao que foi aqui apresentado. Para alguns poderá apresentar novos assuntos vinculados à sua área de atuação; para outros, oferecerá um aprofundamento em temas já conhecidos ou a oportunidade para extrair elementos a serem aplicados em sua pesquisa e/ou prática.

Claudia Cappelli (UERJ) & Fátima de Lourdes dos Santos Nunes (USP)
Coordenação da Trilha de Minicursos em Sistemas de Informação

Claudia Cappelli é Professora do curso de Ciência de Computação da UERJ. Professora do Mestrado Profissional em Telemedicina e Telessaúde da UERJ. Colaboradora do programa de Pós Graduação em Sistemas de Informação da UFRJ. Doutora em Ciências - Informática pela PUC-Rio (2009). Mestre em Sistemas de Informação pela Universidade Federal do Rio de Janeiro (2000). Graduada em Informática pela Universidade do Estado do Rio de Janeiro (1985). Realizou estágio Pós-Doutoral junto ao Programa de Pós-Graduação em Informática da Unirio (2010) e na UFRJ (2020). Pesquisadora Jovem Cientista Nosso Estado pela FAPERJ. Fundadora do Instituto Nacional de Ciência e Tecnologia em Democracia Digital (INCT-DD). Pesquisadora em Literacia Digital do IBCIH (Instituto Brasileiro de Cidades Inteligentes e Humanas). Gestora de Conhecimento do Linguagem Simples Lab. Membro do Comitê Gestor do programa Meninas Digitais da SBC. Mentora da Fábrica de Startups. Representante do Brasil na Clarity. Membro da PLAIN. Pesquisadora em Inovação no INEI (Instituto Nacional de Empreendedorismo e Inovação). Foi Gerente da Área de Arquitetura Corporativa e Planejamento de Tecnologia do Citibank (1996 - 2001) e da Telemar (2001 - 2003) e Professora Adjunta do Departamento de Informática Aplicada da Universidade Federal do Estado do Rio de Janeiro (UNIRIO) onde coordenou o NP2Tec (Núcleo de Pesquisa e Prática de Tecnologia) (2003 - 2013) e o CiberDem (Núcleo de Pesquisa em CiberDemocracia) (2015-2017) ambos na Universidade Federal do Estado do Rio de Janeiro (UNIRIO). Foi representante do Comitê de Transparência Organizacional da UNIRIO e Diretora de Articulação com a Indústria na SBC (Sociedade Brasileira de Computação) (2016-2018). Atuou por 8 anos junto a Petrobras em Projeto de Gestão de Processos de Negócio (2008-2016) e por 2 anos na CEF em Data Science com foco em Linguagem Clara (2018-2020). Atua como revisora de diversos periódicos nacionais e internacionais. Atua na área de Sistemas de Informação, principalmente nos seguintes temas: Gestão de Processos de Negócio, Arquitetura Corporativa, Gestão de TI, Transparência, Linguagem Simples e Governo Digital.

Fátima de Lourdes dos Santos Nunes é Professora titular da Universidade de São Paulo (USP). Bacharel em Ciência da Computação pela Universidade Estadual Paulista Júlio de Mesquita Filho, Mestre em Engenharia Elétrica pela Universidade de São Paulo e Doutora em Ciências (Física Computacional) pela Universidade de São Paulo. Livre-docente pela Universidade de São Paulo na área de Processamento Gráfico. Realiza pesquisas na área de Computação, com ênfase em Realidade Virtual, Processamento de Imagens, Recuperação de dados multimídia por conteúdo e Ciências de Dados. Vários de seus trabalhos são aplicados na área de saúde, estabelecendo interfaces com a área de Engenharia Biomédica. Foi Diretora do Centro de Tecnologia da Informação de Sâo Paulo, pertencente à Superintendência de Tecnologia da Informação da Universidade de São Paulo. Coordena o Grupo de Trabalho em Dados Abertos da Universidade de São Paulo, trabalhando com o desenvolvimento de políticas e software para disponibilizar dados de pesquisa. Também coordena o Escritório de Gestão de Indicadores de Desempenho Acadêmico (EGIDA) da USP, cuja missão é "Apoiar a gestão universitária em relação ao aprimoramento da qualidade acadêmica e ao diálogo com a sociedade, definindo estratégias e indicadores a partir de coleta, análise, processamento e uso ético de dados".

Prefácio:
Coordenação Geral e Coordenação de Programa Geral do SBSI 2025

É com grande entusiasmo e expectativa que damos as boas-vindas ao 21º Simpósio Brasileiro de Sistemas de Informação (SBSI 2025). Ao longo dos anos, o SBSI se consolidou como um espaço vibrante para a discussão dos avanços mais recentes em Sistemas de Informação, reunindo pesquisadores de destaque, profissionais da indústria, estudantes e especialistas da área. Este ano, o evento se torna ainda mais especial ao nos encontrarmos em Recife, Pernambuco, de 19 a 23 de maio de 2025, uma cidade rica em história, cultura e inovação. Organizado pela Comissão Especial de Sistemas de Informação (CESI) da Sociedade Brasileira de Computação (SBC), pela Universidade Federal Rural de Pernambuco (UFRPE) e pela CESAR School, esta edição promete ser uma experiência inspiradora e inclusiva.

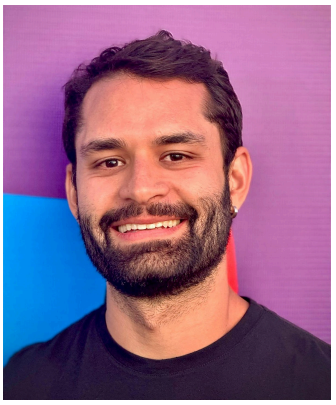
No centro do SBSI 2025 está o tema "Inovação com Equidade, Diversidade e Inclusão em Sistemas de Informação". Este tema reflete um compromisso fundamental: garantir que o progresso tecnológico beneficie a todas as pessoas, independentemente de sua origem, identidade ou condição socioeconômica. Os Sistemas de Informação moldam a maneira como vivemos, trabalhamos e interagimos, influenciando profundamente sociedades e economias. Como pesquisadores e profissionais, temos a responsabilidade de desenvolver sistemas que promovam acessibilidade, justiça e inclusão, assegurando que ninguém fique para trás na era digital.

O simpósio deste ano acontece no dinâmico e histórico bairro do Recife Antigo. Durante cinco dias de intensas trocas de conhecimento, os participantes terão a oportunidade de explorar pesquisas inovadoras, tendências da indústria e ideias emergentes em diversas trilhas, abrangendo desde pesquisa acadêmica e aplicações industriais até teses inovadoras e projetos estudantis. Além do programa técnico, o SBSI 2025 conta com uma programação de palestras excepcionais, incluindo Jeniffer Rode (University College London), abordando diversidade de gênero na computação; Mariza Ferro (Universidade Federal Fluminense), discutindo desafios e oportunidades para inclusão e equidade na Inteligência Artificial; e Mônica Tremblay (William & Mary's Raymond A. Mason School of Business), conduzindo uma MasterClass sobre grupos focais em design science research.

Este evento só é possível graças à paixão e dedicação de uma equipe excepcional. Expressamos nossa mais profunda gratidão a todas as pessoas envolvidas na organização do SBSI 2025, incluindo coordenadores de trilhas, revisores, membros dos comitês, integrantes da CESI e estudantes voluntários, cujo trabalho incansável tornou este evento uma realidade. Mais do que um simpósio, o SBSI 2025 é uma oportunidade para conectar, colaborar e inspirar. Convidamos você a participar ativamente, compartilhar suas ideias, explorar novas perspectivas e contribuir para a construção de um futuro mais inclusivo e equitativo para os Sistemas de Informação. Que este seja um espaço de inovação, discussões ricas e parcerias duradouras. Seja bem-vindo(a) ao SBSI 2025!

George Valença (UFRPE) e Ronnie Santos (CESAR School e University of Calgary)
Coordenação Geral do SBSI 2025

Mônica Ximenes Carneiro da Cunha (IFAL)
Coordenação de Programa Geral do SBSI 2025



George Valença é professor associado I do Departamento de Computação da UFRPE, onde lidera o grupo ASPAS. Atualmente, atua como cientista-chefe de convênios de cooperação técnica com o Instituto Alana, na área de design ético na educação, e com o TCE-PE, na área de inovação aberta, segurança da informação e IA. Seu grupo de pesquisa investiga os desafios sociotécnicos trazidos por plataformas desenvolvidas por Big Techs. Nos últimos anos, tem dedicado atenção especial a reflexões sobre uma TI ética e inclusiva, com estudos sobre a proteção de pessoas trans e não-binárias, bem como de crianças no ambiente digital, analisando temas como racismo algorítmico e design de futuro, ferramentas de controle parental, garantia dos direitos da criança por design e problemas causados pelo reconhecimento facial para pessoas trans. No pós-doutorado, investigou padrões de design manipulativo na PUC-SP.

Ronnie de Souza Santos é professor no programa de pós-graduação da CESAR School (Brasil) e no Departamento de Engenharia Elétrica e de Software da University of Calgary (Canadá), onde lidera o SE-ALL Lab (Software Engineering for All). Sua pesquisa está relacionada com software fairness buscando tornar sistemas de software mais justos, acessíveis e inclusivos, com foco especial em práticas de testes para identificar e mitigar viés em sistemas baseados em IA. Nos últimos anos, tem se dedicado a compreender como equipes de desenvolvimento lidam com desafios de justiça algorítmica, combinando métodos da engenharia de software com perspectivas interdisciplinares.

Mônica Ximenes Carneiro da Cunha possui graduação em Engenharia Elétrica pela Universidade Federal de Campina Grande, mestrado em Engenharia Elétrica pela Universidade Federal de Campina Grande e doutorado em Administração pela Universidade Federal de Pernambuco. É professora titular e atua no Bacharelado em Sistemas de Informação (Campus Maceió) do Instituto Federal de Educação Ciência e Tecnologia de Alagoas (IFAL). Atua em diversos projetos de pesquisa e extensão do IFAL. Áreas de interesse: Sistemas de Informação para o Setor Público, Educação em Informática, Informática na Educação, Jogos Educacionais, Tecnologias Assistivas, Educação Especial e Inclusiva (autismo) e Tecnologias Sociais. Foi coordenadora geral do SBSI 2023, coordenadora do comitê diretivo do SBSI 2024 e coordenadora do comitê de programa do SBSI 2025.

Sumário

Capítulo 1

Controles de Segurança para Conformidade baseados em Ferramentas Livres

Security Controls for Compliance Based on Open-Source Tools

Lucas Alionço Perez, Bernardo Pavloski Tomasi, Yago Yudi Vilela Furuta, Marcos Sfair Sunye e André Grégio

Abstract

Ensuring cybersecurity in real scenarios requires the definition of policies and the deployment of controls. There are several standards and normative instructions available to guide the creation of policies and processes, as well as to put those controls in practice. However, it can be difficult to take the first steps into the effective application of these norms when the organization does not have anything in place yet. In this work, we will present selected normatives related to cybersecurity delve into controls to distinguish those that are theoretical/bureaucratic/management-related from the practical ones in order to present and compare the tools and mechanisms that support a quick start for implementing the program in an organization.

Resumo

Garantir a cibersegurança em cenários reais requer a definição de políticas e a implementação de controles. Existem vários padrões e instruções normativas disponíveis para orientar a criação de políticas e processos, assim como a aplicação prática desses controles. No entanto, pode ser difícil dar os primeiros passos na aplicação efetiva de tais normas quando a organização ainda não possui nada estabelecido. Neste trabalho, apresentaremos normas selecionadas relacionadas à cibersegurança e exploraremos os controles para distinguir aqueles que são teóricos, burocráticos ou gerenciais dos que são práticos, a fim de apresentar possibilidades de ferramentas e mecanismos que apoiam um início rápido na implementação do programa em uma organização.

1.1. Introdução

A constante evolução dos avanços tecnológicos e do uso de sistemas computacionais para a maioria das atividades diárias (trabalho, compras, finanças, relacionamentos) tornam

a privacidade e a segurança da informação objetos frequentemente desafiados por um amplo espectro de ameaças digitais. Diversos atores mal-intencionados (incluindo indivíduos, organizações criminosas e órgãos de inteligência de várias nações) se aproveitam das características dos sistemas conectados à Internet (acesso remoto, anônimo e de amplo alcance de usuários) para explorar vulnerabilidades a fim de realizar ataques que comprometam a integridade, confidencialidade e/ou disponibilidade das informações. Tais riscos exigem que organizações de todos os tamanhos e setores busquem formas de identificar, acompanhar e preencher lacunas de privacidade e segurança da informação [SGD 2024b]. Para tanto, foram criados *frameworks* cujo propósito é administrar e reduzir tais riscos, como o *CIS Controls* [CIS 2024f], o *NIST Cybersecurity Framework* [NIST 2024e] e o *Framework* de Programa de Privacidade e Segurança da Informação (PPSI) [SGD 2024b], servindo de guia para indivíduos e organizações na defesa contra ataques cibernéticos.

Embora os referidos *frameworks* sejam projetados para atender organizações de todos os níveis de maturidade em relação a processos de cibersegurança [NIST 2024e], entidades que possuem procedimentos e políticas de segurança da informação bem estabelecidos percebem uma maior facilidade na adoção de novos controles trazidos pelos *frameworks*. Por outro lado, organizações que não possuem o mesmo nível de maturidade organizacional (como pode ser o caso de pequenos e médios negócios, por exemplo) podem encontrar dificuldades em estabelecer e adotar as políticas necessárias para atendimento dos controles de segurança da informação.

Os *frameworks* de segurança citados são apresentados em um alto nível de abstração e consideram que: (a) cada organização possui riscos comuns e/ou únicos; e (b) cada organização admite níveis variados de tolerância a riscos. Por conta dessas diferenças e necessidades, o modo de implementação dos controles de segurança varia entre uma organização e outra [NIST 2024e]. A adoção dos controles na prática tem o apoio da comunidade de cibersegurança para torná-los implementáveis, utilizáveis, escaláveis e alinhados com os requisitos da indústria ou de governos.

Nesse cenário, constrói-se a situação em que organizações sem maturidade administrativa se veem obrigadas a seguir controles rígidos de segurança e privacidade. Apesar de ser uma tarefa exaustiva, é possível observar que mesmo organizações sem políticas e procedimentos de segurança bem definidos podem dar os passos iniciais em direção à conformidade, utilizando ferramentas de software livre. O objetivo deste documento é prover uma análise preliminar dos controles que podem ser atendidos por este tipo de ferramenta e listá-las, de forma a fomentar a adequação aos controles de segurança.

1.2. Principais *frameworks* de Segurança

Para fins de delimitação do escopo deste trabalho, optou-se por detalhar os *frameworks* de segurança que inspiraram o desenvolvimento do *Framework* do Programa de Privacidade e Segurança da Informação (PPSI), de adoção obrigatória por órgãos e entidades da administração pública federal. Destarte, os *frameworks* que serão apresentados neste estudo são os *CIS Controls*, o *NIST Cybersecurity Framework* e o próprio *Framework* de Programa de Privacidade e Segurança da Informação (PPSI).

1.2.1. *CIS Controls*

O CIS (*Center for Internet Security*) é uma entidade sem fins lucrativos globalmente reconhecida pelas melhores práticas em segurança para sistemas da informação. A instituição lidera uma comunidade global de profissionais para promover uma evolução contínua dos padrões de segurança e fornecer produtos e serviços contra ameaças emergentes.

Os *CIS Controls* refletem o conhecimento combinado de especialistas de todas as partes do ecossistema de cibersegurança (indústria, governos e indivíduos), de todas as áreas de atuação (times de resposta a incidentes, analistas de ameaças, pesquisadores de vulnerabilidades, desenvolvedores de ferramentas, usuários, auditores) e em muitos setores das sociedade (governamental, financeiro, transporte, academia, consultoria). Os controles em si são desenvolvidos pela obtenção do consenso entre os especialistas sobre as melhores práticas em segurança. De modo geral, trata-se de aproveitar a experiência de uma comunidade de indivíduos e empresas para realmente fazer melhorias na segurança por meio do compartilhamento de ideias, ferramentas, lições e ações coletivas. Os *CIS Controls* são divididos nos 18 controles a seguir:

1. Inventário e controle de ativos corporativos;
2. Inventário e controle de ativos de software;
3. Proteção de dados;
4. Configuração segura de ativos corporativos e software;
5. Gestão de contas;
6. Gestão de controle de acesso;
7. Gestão contínua de vulnerabilidades;
8. Gestão de registros de auditoria;
9. Proteções de e-mail e navegador Web;
10. Defesas contra *malware*;
11. Recuperação de dados;
12. Gestão da infraestrutura de rede;
13. Monitoramento defesa da rede;
14. Conscientização sobre segurança e treinamento de competências;
15. Gestão de provedor de segurança;
16. Segurança de aplicações;
17. Gestão de resposta a incidentes;
18. Testes de invasão.

Para cada controle é apresentada uma visão geral e explicação sobre a sua criticidade, bem como uma descrição de procedimentos e ferramentas que favorecem a implementação e automação do controle. As medidas de segurança em si são exibidas em uma lista de ações específicas que devem ser realizadas para cumprimento do controle.

Há um total de 153 medidas de segurança distribuídas entre os 18 controles. Embora seja um grande número, nem todas as organizações precisam implementar todos os

controles e medidas de segurança. Os *CIS Controls* apresentam uma forma de priorização das medidas de segurança por grupos de implementação, divididos em três níveis, denominados Grupos de Implementação 1, 2 e 3 [CIS 2024c]. Todas as organizações devem buscar atender aos controles indicados no Grupo de Implementação 1, definido como "ciber higiene". Os grupos subsequentes expandem o Grupo 1. Os Grupos de Implementação são descritos da seguinte forma:

- **Grupo de Implementação 1 (IG1)**: geralmente representa organizações de pequeno e médio porte com recursos limitados de tecnologia da informação e cibersegurança. A sensibilidade dos dados com os quais essas entidades trabalham é baixa, normalmente relacionada a privacidade de empregados e informações financeiras. Os controles e medidas de segurança indicados para este grupo são considerados essenciais, representando o que toda organização deveria aplicar para se proteger dos ataques mais comuns. Das 153 medidas de segurança dos *CIS Controls*, 56 são recomendados para este grupo.

- **Grupo de Implementação 2 (IG2)**: este grupo representa organizações que dispõem de uma equipe responsável por administrar e proteger a sua infraestrutura de TI, além de comportar múltiplos departamentos com diferentes perfis de risco. Organizações que se enquadram nesta categoria podem estar sujeitas à conformidade regulatória e usualmente processam dados sensíveis de clientes ou informações confidenciais para o negócio. Uma brecha de segurança pode causar a perda da confiança no serviço por parte de clientes. Para este grupo, há 74 novas medidas de segurança (que se somam às 56 recomendadas para o IG1).

- **Grupo de Implementação 3 (IG3)**: este grupo engloba entidades maduras, que empregam especialistas de várias áreas de cibersegurança. Os ativos e dados dessas organizações contêm informações sensíveis e/ou estão sujeitos a supervisão regulatória e de conformidade. As atividades desenvolvidas devem sempre atender aos princípios da disponibilidade, integridade e confidencialidade. Falhas de segurança para entidades deste grupo podem resultar em dano significativo ao bem público [CIS 2024d]. As 23 novas medidas de segurança recomendadas para este grupo se somam às 56 do IG1 e às 74 do IG2, totalizando as 153 medidas dos *CIS Controls*. Um exemplo de controle é mostrado na Tabela 1.1.

Os *CIS Benchmarks*, uma documentação complementar do *CIS Controls*, trazem um conjunto de recomendações de configurações para mais de 25 famílias de produtos comumente usados na indústria, incluindo serviços em nuvem, contêineres, bancos de dados, aplicativos *desktop*, servidores, dispositivos móveis, dispositivos de rede e sistemas operacionais [CIS 2024b]. Essas recomendações são desenvolvidas a partir do consenso de especialistas em cibersegurança e representam o esforço da comunidade em proteger sistemas de forma confiável e globalmente. Parte das medidas de segurança recomendadas pelos *CIS Controls* podem ser implementadas a partir da aplicação das configurações seguras indicadas nos *CIS Benchmarks*.

Além disso, os *CIS Controls* podem ser mapeados para outros *frameworks* de cibersegurança, como *NIST Cybersecurity Framework*, *MITRE Enterprise ATT&CK*, SOC

Tabela 1.1. Controle 16.13 do *CIS Controls*, para fins de exemplo.

Controle	16 - Segurança de aplicações
Medida de Segurança	16.13
Título	Realizar teste de invasão de aplicação
Descrição	Realize teste de invasão das aplicações. Para aplicações críticas, o teste de invasão autenticado é mais adequado para localizar vulnerabilidades de lógica de negócios do que a varredura de código e o teste de segurança automatizado. O teste de invasão depende da habilidade do testador para manipular manualmente uma aplicação como um usuário autenticado e não autenticado.
Tipo de Ativo	Aplicações
Função de Segurança	Proteger
Grupos de Implementação	IG3

2 (*System and Organization Controls 2*), etc [CIS 2024e]. Essa integração possibilita que múltiplos controles de diferentes fontes sejam atendidos simultaneamente [CIS 2024g]. Nota-se que os *CIS Controls* corroboram a proposta deste trabalho: fornecer um ponto de partida para organizações que não possuem políticas ou procedimentos bem definidos, de baixo e médio porte, cuja priorização de medidas de segurança por grupos de implementação e a aplicação dos guias práticos dos *CIS Benchmarks* contribuem significativamente para um início rápido e prático de um programa de segurança.

1.2.2. *NIST Cybersecurity Framework*

O NIST (*National Institute of Standards and Technology*) foi fundado em 1901 e pertence ao Departamento de Comércio dos Estados Unidos [NIST 2024a]. O Instituto possui programas científicos nas mais diversas áreas do conhecimento, incluindo comunicações, biociência, clima, química, infraestrutura, saúde, dentre outros [NIST 2024g]. Destacam-se as pesquisas do NIST em cibersegurança e tecnologia da informação, contexto em que o *NIST Cybersecurity Framework* (CSF) foi desenvolvido [NIST 2024b].

Atualmente em sua versão 2.0, o *NIST Cybersecurity Framework* possui propósito semelhante ao do *CIS Controls*: fornecer orientação para a indústria, órgãos governamentais e outras organizações para gerenciar riscos de segurança cibernética. É destinado a todos os tipos de organizações, independentemente de tamanho, setor ou maturidade e auxilia no processo de compreender, avaliar, priorizar e comunicar melhor os esforços de segurança cibernética. O público principal do *NIST Cybersecurity Framework* é composto por profissionais responsáveis por desenvolver e liderar programas de segurança cibernética em organizações. Entretanto, o *framework* também pode ser utilizado por outras pessoas envolvidas no gerenciamento de riscos, como executivos, conselhos de administração, advogados, especialistas em recursos humanos e auditores [NIST 2024e].

Da mesma forma que ocorre com os *CIS Controls*, o *NIST Cybersecurity Framework* não prescreve como os resultados devem ser alcançados: em vez disso, ele descreve os resultados desejados, associando recursos *on-line* e orientações adicionais que podem ser usados para alcançar tais resultados [NIST 2024e]. A descrição dos resultados

almejados é neutra em termos de setor, país e tecnologia, o que viabiliza a flexibilidade necessária para a implementação dos controles.

O *CSF Core* (um apêndice complementar ao documento principal do *NIST Cybersecurity Framework*) define o conjunto de controles de segurança e resultados esperados pelas organizações. Ele é estruturado em funções, categorias e subcategorias. As funções representam os objetivos de segurança em seu nível mais abrangente, enquanto as categorias e subcategorias especificam as ações técnicas e de gerenciamento necessárias para atingir esses objetivos. Cada função, categoria e subcategoria abrange uma série de atividades que auxiliam nas etapas de compreensão, avaliação, priorização e comunicação, fundamentais para a implementação eficaz da segurança cibernética [NIST 2024d]. As seis funções do *NIST CSF Core* são:

- **GOVERNAR (*GOVERN* - GV)**: esta função determina que a estratégia, as expectativas e a política de gerenciamento de riscos de segurança cibernética da organização sejam estabelecidas, comunicadas e monitoradas. A função de Governar oferece insumo para informar o que a organização pode fazer para atingir e priorizar os resultados das outras cinco funções. Envolve atividades de estratégia de segurança cibernética, elaboração de políticas e gerenciamento de riscos.
- **IDENTIFICAR (*IDENTIFY* - ID)**: esta função determina que os riscos atuais de segurança cibernética da organização sejam compreendidos. Inclui atividades de compreensão sobre os ativos da organização (dados, hardware, software, sistemas, instalações, serviços), de fornecedores e de riscos relacionados à segurança cibernética, bem como atividades de identificação de oportunidades de melhoria para as políticas, planos, processos e práticas da organização.
- **PROTEGER (*PROTECT* - PR)**: esta função determina que sejam usadas proteções para gerenciar os riscos de segurança cibernética da organização, com o objetivo de proteger os ativos identificados. Inclui atividades de gerenciamento de identidades e controle de acesso, conscientização e treinamento, segurança de dados e de sistemas.
- **DETECTAR (*DETECT* - DE)**: esta função determina que possíveis ataques e comprometimentos de segurança devem ser encontrados e analisados. A detecção oportuna de anomalias, indicadores de comprometimento e outros eventos adversos oferece suporte para as atividades de resposta e recuperação de incidentes.
- **RESPONDER (*RESPOND* - RS)**: esta função determina que ações relacionadas a um incidente de segurança detectado devem ser tomadas. Esta função apoia a capacidade de conter os efeitos de um incidente e envolve atividades de gerenciamento, análise, atenuação e comunicação de incidentes.
- **RECUPERAR (*RECOVER* - RC)**: esta função determina que os ativos e as operações afetadas por um incidente de segurança sejam restaurados, garantindo a operação normal da companhia.

Quando analisadas em conjunto, as funções do CSF fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento de risco de cibersegurança de uma

organização [SGD 2024b]. Por essa razão, o NIST apoia a representação das funções do CSF como uma roda, onde todas as funções estão relacionadas entre si. As ações da função Identificar apoiarão as ações da função Proteger, enquanto as atividades da função Detectar fornecem a base para as ações de Responder e Recuperar, por exemplo. A função de Governar se situa no centro da roda pois guia a forma de implementação das outras funções [NIST 2024e].

As seis funções do CSF abrigam 22 categorias e 107 subcategorias de resultados desejados, que partem de uma descrição de alto nível (funções) e se detalham em categorias e subcategorias [NIST 2024e]. Um exemplo de resultado a ser alcançado em uma organização, de acordo com o *NIST CSF Core*, é o resultado ID.AM-02, apresentado na tabela 1.2.

Tabela 1.2. Controle ID.AM-02 do *NIST CSF Core*, para fins de exemplo.

Função	Identificar (ID): os riscos atuais de segurança cibernética da organização são compreendidos.
Categoria	Gerenciamento de ativos (ID.AM): os ativos (por exemplo, dados, hardware, software, sistemas, instalações, serviços, pessoas) que permitem que a organização atinja seus objetivos comerciais são identificados e gerenciados de acordo com sua importância relativa para os objetivos organizacionais e a estratégia de risco da organização.
Subcategoria	ID.AM-02: os inventários de software, serviços e sistemas gerenciados pela organização são mantidos.

O *NIST Cybersecurity Framework* também se adequa à proposta deste estudo ao oferecer um *Quick Start Guide* para pequenos negócios dentre seus materiais complementares, destinado às organizações com nenhum ou poucos planos para cibersegurança. O guia elenca alguns resultados que podem ser priorizados por essas organizações, facilitando o início rápido na implementação de controles de segurança [NIST 2024d]. Entretanto, não existe o apoio prático como visto nos *CIS Benchmarks*. O NIST oferece uma tabela com exemplos de implementação de medidas que alcançam os resultados desejados, mas todos são descritos em alto nível [NIST 2024c]. Tal como os *CIS Controls*, é possível obter um mapeamento das funções do *NIST CSF Core* para outros *frameworks* [NIST 2024f].

1.2.3. *Framework* de Programa de Privacidade e Segurança da Informação (PPSI)

O Programa de Privacidade e Segurança da Informação (PPSI) foi instituído pelo Ministério da Gestão e da Inovação em Serviços Públicos e sua Secretaria de Governo Digital por meio da Portaria nº 852, de 28 de março de 2023 [SGD 2023b]. Trata-se de um conjunto de projetos e processos distribuídos nas áreas temáticas de governança, maturidade, pessoas, metodologia e tecnologia que têm como objetivo elevar a maturidade e a resiliência dos órgãos e entidades, em termos de privacidade e segurança da informação, no âmbito da administração pública federal direta, autárquica e fundacional.

O artigo 7º da portaria também institui o *Framework* de Privacidade e Segurança da Informação, composto por um conjunto de controles, metodologias e ferramentas de apoio. As bases do *framework* são a Lei Geral de Proteção de Dados Pessoais - LGPD

(Lei nº 13.709 de 14 de agosto de 2018), a Política Nacional de Segurança da Informação - PNSI, os próprios *CIS Controls* e o *Framework* de Privacidade do NIST, normas ISO/IEC e ABNT, normativos emitidos pela Autoridade Nacional de Proteção de Dados - ANPD e pelo Gabinete de Segurança Institucional - GSI, dentre outros [SGD 2023a].

A estratégia adotada pelo *Framework* do PPSI de se apresentar como uma combinação de algumas das referências mais abrangentes viabiliza a complementação e supressão de eventuais lacunas que cada documento base pode trazer. Dessa forma, o *Framework* do PPSI consegue atender a pluralidade de serviços e de tratamento de dados pessoais pelo Poder Público, que possui diversos órgãos com políticas públicas próprias e atribuições institucionais específicas [SGD 2024b].

O *Framework* do PPSI também fornece mecanismos de medição dos índices de maturidade em privacidade e segurança da informação (índices *iSeg* e *iPriv*) do órgão implementador, que podem, por sua vez, subsidiar a implementação e o monitoramento dos controles de privacidade e segurança [SGD 2024b].

O *Framework* do PPSI apresenta um total de 310 medidas de segurança e privacidade, descritas em forma de perguntas, divididas em 31 controles e priorizadas de acordo com grupos de implementação. O PPSI também traz um modelo de avaliação de criticidade de sistemas adaptado do modelo utilizado pelo Tribunal de Contas da União (TCU), a fim de determinar o nível de criticidade e a qual grupo de implementação um órgão implementador do PPSI se enquadra [SGD 2024b]. Os controles do PPSI são divididos da seguinte forma:

- 7 medidas de Controle 0 (Controle de Estruturação Básica em Gestão em Privacidade e Segurança da Informação), aplicáveis a todos os órgãos;
- 56 medidas de cibersegurança e 97 medidas de privacidade para o Grupo 1. Essas medidas são de higiene cibernética e obrigações dispostas na LGPD, também aplicáveis a todos os órgãos;
- 74 medidas de cibersegurança e 32 medidas de privacidade para o Grupo 2. Essas medidas são aplicáveis para órgãos de média criticidade.
- 23 medidas de cibersegurança e 16 medidas de privacidade para o Grupo 3. Essas medidas são aplicáveis para órgãos de alta criticidade.

Um exemplo de controle de cibersegurança trazido pelo PPSI é o controle 6.4, descrito na tabela 1.3.

O *framework* do PPSI é acompanhado de um conjunto de materiais complementares associados aos controles, constituído principalmente por modelos de políticas (como modelos de política de gestão de *logs* de auditoria e de backup) e guias de propósito geral (como um guia de resposta a incidentes de segurança e um guia sobre sobre boas práticas dentro da LGPD). Estes materiais podem ser adotados integralmente ou adaptados ao contexto e necessidade de cada organização [SGD 2024a]. Ressalta-se que apenas a adoção de uma política ou de um guia não cumpre, por si só, o controle de segurança, mas fornece forte embasamento para outras ações.

Tabela 1.3. Controle 6.4 do PPSI, para fins de exemplo.

ID	6.4
ID CIS	6.3
FUNÇÃO NIST CSF	Proteger
MEDIDA	O órgão exige MFA (*Multi-Factor Authentication*) para aplicações expostas externamente?
DESCRIÇÃO DA MEDIDA	Exigir que todas as aplicações corporativas ou de terceiros expostas externamente apliquem o MFA. Impor o MFA por meio de um serviço de diretório ou provedor de SSO (*Single Sign-On*) é uma implementação satisfatória desta medida de segurança.
REFERÊNCIAS LGPD	Art 6º, inciso VII, Art. 46, Art. 47, Art. 49, Art. 50.
REFERÊNCIAS GSI	IN nº 5/2021 NC 01/IN02/NSC/GSIPR e seus anexos (Anexo A e Anexo B).
GRUPOS DE IMPLEMENTAÇÃO	1, 2, 3

Percebe-se que o PPSI se preocupa em expandir os conceitos trazidos por *frameworks* reconhecidos, adaptá-los ao contexto da Administração Pública, aprimorá-los no que for possível e expandi-los nas questões de privacidade, tornando-se um *framework* completo e fundamentado. As correlações entre os controles e as referências legais e administrativas agregam qualidade ao *framework* desenvolvido pela Secretaria de Governo Digital.

1.3. Controles e Medidas de Segurança do *Framework* do PPSI

Atender aos controles de segurança previstos no *CIS Controls*, *NIST CSF Core* e PPSI demanda a utilização de recursos de diversas naturezas. Certos controles podem ser satisfeitos a partir da adoção de políticas dentro da organização, enquanto outros demandam a utilização de ferramentas computacionais específicas para garantir que os padrões de segurança sejam atendidos. Classificar os controles para diferenciar aqueles que são teóricos, burocráticos ou gerenciais daqueles que são práticos e que podem ser prontamente atendidos é necessário para que organizações sem planos em cibersegurança consigam dar seus primeiros passos em direção à conformidade. Ao mesmo tempo, também é preciso se atentar aos controles priorizados de acordo Grupos de Implementação, focando nas ações de higiene cibernética do Grupo 1, descrito na seção 1.2.1.

É importante ressaltar que os controles e as medidas de segurança são sensíveis ao contexto em que se busca implementá-los. Por exemplo, uma medida que indica a necessidade de controle de acesso a dados pode fazer referência a dados no nível do sistema operacional, a dados dentro de um serviço web ou a dados disponíveis em um servidor na nuvem. Em outras palavras, uma mesma medida pode ser implementada de diferentes formas, de acordo o com contexto trabalhado. É o que ocorre quando uma mesma medida é abordada de diferentes formas dentro dos documentos dos *CIS Benchmarks*, que tratam de segurança em níveis distintos (sistemas operacionais, servidores em nuvem,

dispositivos móveis etc). Detalhes sobre cada controle de segurança e suas medidas serão abordados a seguir.

1.3.1. Controle 1: Inventário e Controle de Ativos Institucionais

O primeiro controle de segurança tratado pelo *framework* do PPSI faz referência a ações de inventário e controle de ativos institucionais. Inventariar, rastrear e corrigir os ativos conectados à rede facilita a identificação daqueles que demandam maiores recursos em monitoramento e proteção, ao mesmo tempo em que os ativos não autorizados podem ser selecionados para futura remoção ou tratamento[SGD 2024b].

No contexto deste controle, consideram-se ativos institucionais os dispositivos de usuário final (como computadores e dispositivos móveis), dispositivos de rede (como *switches*), dispositivos não computacionais, dispositivos IoT (Internet das Coisas) e servidores, tanto os conectados à infraestrutura quanto virtuais, remotos e aqueles em ambiente de nuvem.

Mapear os ativos institucionais é uma atividade crucial para garantia da segurança da informação, dado que não é possível proteger aquilo que não é mapeado ou que não se tem conhecimento sobre sua existência [SGD 2024b]. O conceito de *shadow IT* (ou TI invisível) trata de quaisquer dispositivos não autorizados em uso dentro das organizações. Podem ser dispositivos particulares que contenham informações sensíveis do órgão ou repositórios em nuvem não autorizados [IBM 2024]. O problema surge quando esses dispositivos não protegidos são comprometidos, prejudicando as atividades da organização e/ou causando prejuízos.

Este controle de segurança é composto por 5 medidas:

Medida 1.1 - O órgão estabelece e mantém um inventário detalhado de ativos institucionais?

Medida 1.2 - O órgão usa o *Dynamic Host Configuration Protocol* (DHCP) para Atualizar o Inventários de Ativos?

Medida 1.3 - O órgão usa uma ferramenta de descoberta ativa?

Medida 1.4 - O órgão usa ferramenta de Descoberta Passiva?

Medida 1.5 - O órgão endereça ativos não autorizados?

De forma complementar, o *framework* do PPSI também traz um Modelo de Política de Gestão de Ativos que pode auxiliar as organizações a implementar as medidas deste controle de segurança.

Todas as 5 medidas deste controle de segurança admitem uma implementação rápida pelo uso de ferramentas de software livre, indicadas na próxima seção.

1.3.2. Controle 2: Inventário e Controle de Ativos de Software

O segundo controle de segurança abordado pelo PPSI também trabalha questões de inventário e controle de ativos, mas desta vez no âmbito de software. Este controle se preocupa em identificar quais programas se encontram em execução na rede e impedir a execução ou instalação de software não autorizado [SGD 2024b].

Atacantes constantemente fazem varreduras na infraestrutura do alvo em busca de softwares desatualizados ou vulneráveis para explorar vulnerabilidades. Com um inventário de software completo, a organização pode determinar quais as versões dos softwares estão em execução e descobrir aplicações executadas sem permissão [SGD 2024b].

Este controle de segurança é composto por 7 medidas:

Medida 2.1 - O órgão estabelece e mantém um inventário de software?

Medida 2.2 - O órgão assegura que o software autorizado seja atualmente suportado?

Medida 2.3 - O órgão possui lista de permissões de software atualizado?

Medida 2.4 - O órgão possui lista de permissões de bibliotecas autorizadas?

Medida 2.5 - O órgão possui lista de permissões de *Scripts* autorizados?

Medida 2.6 - O órgão utiliza ferramentas automatizadas de inventário de software?

Medida 2.7 - O órgão endereça o software não autorizado?

O mesmo Modelo de Política de Gestão de Ativos trazido pelo PPSI para auxiliar na implementação de medidas do Controle 1 também possui disposições válidas para o Controle 2. Além disso, algumas formas de implementação das medidas deste controle podem ser encontradas nos *CIS Benchmarks* (como, por exemplo, as medidas 2.2, 2.6 e 2.7, que são abordadas no documento *CIS NGINX Benchmark* v2.1.0 [CIS 2024a]).

Das 7 medidas de segurança deste controle, 4 delas favorecem uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.3. Controle 3: Proteção de Dados

O terceiro controle abordado pelo PPSI aborda processos e ferramentas para identificar, classificar, manusear, reter e descartar dados. Neste contexto, o PPSI não se preocupa apenas com dados que estão dentro da estrutura das instituições, mas também com aqueles que estão na nuvem, em dispositivos portáteis do usuário final, compartilhados com terceiros ou serviços *on-line* [SGD 2024b].

A proteção de dados é assunto de destaque em todo o cenário global. Gerenciar os dados de maneira adequada durante todo seu ciclo de vida se tornou uma necessidade e vai além das questões de criptografia [SGD 2024b]. Além disso, regulamentações ressaltam também como os dados pessoais devem ser tratados, a exemplo da LGPD no Brasil e GDPR (*General Data Protection Regulation*) da União Europeia.

A perda do controle sobre os dados protegidos ou sensíveis causa impactos sérios ao negócio, com prejuízos financeiros e reputacionais. Além disso, o vazamento indevido de dados pode ferir direitos e garantias individuais dos seus titulares.

Este controle é composto por 14 medidas de segurança:

Medida 3.1 - O órgão estabelece e mantém um processo de gestão de dados?

Medida 3.2 - O órgão estabelece e mantém um inventário de dados?

Medida 3.3 - O órgão estabelece e mantém um esquema de classificação de dados?

Medida 3.4 - O órgão documenta os Fluxos de Dados?

Medida 3.5 - O órgão configura listas de controle de acesso a dados?

Medida 3.6 - O órgão aplica retenção de dados?

Medida 3.7 - O órgão descarta dados com segurança?

Medida 3.8 - O órgão criptografa dados em dispositivos de usuário final?

Medida 3.9 - O órgão criptografa dados em mídia removível?

Medida 3.10 - O órgão criptografa dados sensíveis em trânsito?

Medida 3.11 - O órgão criptografa dados sensíveis em repouso?

Medida 3.12 - O órgão segmenta o processo e o armazenamento de dados com base na sensibilidade?

Medida 3.13 - O órgão implanta uma solução de prevenção contra perda de dados?

Medida 3.14 - O órgão registra o acesso a dados sensíveis?

A Secretaria de Governo Digital disponibiliza em seu portal um Guia de Elaboração do Processo de Gestão de Dados e o Modelo de Política de Gestão de Registros (*Logs*) de Auditoria, com enfoque na gestão de Dados, no fluxo dos dados e na classificação de dados [SGD 2024b].

Das 14 medidas de segurança deste controle, 10 delas admitem uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção, em nível de sistemas operacionais e sistemas distribuídos.

1.3.4. Controle 4: Configuração Segura de Ativos Institucionais e Software

O controle 4 do *framework* do PPSI trata da configuração segura de ativos institucionais (incluindo dispositivos de usuário final, portáteis, dispositivos de rede, IoT e servidores) e de software. Este controle complementa os controles 1 e 2, buscando utilizar configurações seguras para os dispositivos e software utilizados.

O conjunto padrão de configurações normalmente é voltado para facilidade de implantação e uso, enquanto deixa aspectos de segurança em segundo plano. A configuração padrão pode carregar os sistemas com serviços e portas abertas, contas ou senhas padrão e softwares desnecessários pré-instalados que podem ser explorados por um atacante [SGD 2024b]. Além disso, atualizações de segurança precisam ser gerenciadas para garantir que as configurações seguras não se alterem automaticamente.

Este controle é composto por 12 medidas de segurança:

Medida 4.1 - O órgão estabelece e mantém um processo de configuração segura?

Medida 4.2 - O órgão estabelece e mantém um processo de configuração segura para a Infraestrutura de Rede?

Medida 4.3 - O órgão configura o bloqueio automático de sessão nos ativos?

Medida 4.4 - O órgão implementa e gerencia um *firewall* nos servidores?

Medida 4.5 - O órgão implementa e gerencia um *firewall* nos dispositivos de usuário final?

Medida 4.6 - O órgão gerencia com segurança os ativos corporativos e softwares?

Medida 4.7 - O órgão gerencia contas padrão nos ativos corporativos e software?

Medida 4.8 - O órgão desinstala ou desativa serviços desnecessários nos ativos e software?

Medida 4.9 - O órgão configura servidores DNS (*Domain Name System*) confiáveis nos ativos?

Medida 4.10 - O órgão impõe a capacidade de limpeza remota nos dispositivos portáteis do usuário final?

Medida 4.11 - O órgão separa os Espaços de Trabalho nos dispositivos móveis?

Medida 4.12 - O órgão impõe o bloqueio automático de dispositivos nos dispositivos portáteis de usuário final?

Benchmarks do CIS para *Ubuntu 12.04 LTS Server, NGINX* e *Google Chrome* também mencionam formas de implementar uma parte das medidas deste controle e podem ser utilizados de forma complementar [CIS 2024a].

Das 14 medidas de segurança deste controle, 3 delas viabilizam uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.5. Controle 5: Gestão de Contas

O Controle 5 foca em processos e ferramentas para atribuir e gerenciar autenticação de credenciais para contas de usuário, contas de administrador, conta de serviço para ativos e softwares institucionais. A gestão de contas é tarefa crítica no contexto de segurança da informação pois, sem ela, atacantes podem buscar acesso não autorizado aos recursos da organização por uso de senhas fracas ou repetidas de outros serviços, contas válidas de usuários inativos, etc. Contas administrativas ou com alto privilégio e contas de serviço são críticas, pois seu uso possibilita que atacantes adicionem novas contas e façam alterações nos ativosda organização [SGD 2024b].

Este controle é composto por 6 medidas:

Medida 5.1 - O órgão estabelece e mantém um inventário de contas?

Medida 5.2 - O órgão estabelece e mantém um inventário de contas de serviço?

Medida 5.3 - O órgão usa senhas exclusivas?

Medida 5.4 - O órgão restringe privilégios de administrador a contas de administrador dedicadas?

Medida 5.5 - O órgão centraliza a gestão de contas?

Medida 5.6 - O órgão desabilita contas inativas?

Assim como ocorre nos controles anteriores, a Secretaria de Governo Digital dis-

ponibiliza um Modelo de Política de Controle de Acesso que pode ser usado de forma complementar, focado em diretrizes para gestão de controle de acesso [SGD 2024b]. Os *benchmarks* do CIS para *Ubuntu 12.04 LTS Server* e *NGINX* [CIS 2024a] também mencionam medidas deste controle.

Todas as 6 medidas deste controle de segurança admitem uma implementação rápida pelo uso de ferramentas de software livre, indicadas na próxima seção.

1.3.6. Controle 6: Gestão de Controle de Acesso

O controle 6 do *framework* do PPSI foca em questões de autorização de acesso a recursos da organização por uso de ferramentas e processos para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios. Este controle busca assegurar que os usuários tenham acesso apenas aos dados ou ativos necessários para execução de suas funções [SGD 2024b], seguindo o princípio do privilégio mínimo.

Este controle é composto por 8 medidas:

Medida 6.1 - O órgão estabelece e mantém um inventário de sistemas de autenticação e autorização?

Medida 6.2 - O órgão estabelece Processo de Concessão de Acesso?

Medida 6.3 - O órgão estabelece Processo de Revogação de Acesso?

Medida 6.4 - O órgão exige MFA (*Multi-Factor Authentication*) para aplicações expostas externamente?

Medida 6.5 - O órgão exige MFA para acesso remoto à rede?

Medida 6.6 - O órgão exige MFA para acesso administrativo?

Medida 6.7 - O órgão centraliza o controle de acesso?

Medida 6.8 - O órgão define e mantém o controle de acesso baseado em funções?

O mesmo Modelo de Política de Controle de Acesso tratado no Controle 5 também pode ser aproveitado para este Controle, seguindo a recomendação da Secretaria de Governo Digital. Uma das medidas também é tratada pelo *Benchmark* do CIS para *Ubuntu 12.04 LTS Server*.

Das 8 medidas de segurança deste controle, 3 delas possibilitam uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.7. Controle 7: Gestão Contínua de Vulnerabilidades

O sétimo controle do PPSI trata da gestão de vulnerabilidades. O gerenciamento delas envolve o desenvolvimento de um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos dentro da infraestrutura, a fim de remediar e minimizar as janelas de oportunidade para atacantes. A inteligência sobre novas vulnerabilidades pode vir de *patches* de segurança, atualizações de software, avisos de segurança, boletins de ameaça e outros [SGD 2024b].

Este controle é composto por 7 medidas de segurança:

Medida 7.1 - O órgão realiza varreduras automatizadas de vulnerabilidades em ativos institucionais internos?

Medida 7.2 - O órgão realiza varreduras automatizadas de vulnerabilidades em ativos institucionais expostos externamente?

Medida 7.3 - O órgão estabelece e mantém um processo de gestão de vulnerabilidades?

Medida 7.4 - O órgão executa a gestão automatizada de *patches* do sistema operacional?

Medida 7.5 - O órgão executa a gestão automatizada de *patches* de aplicações?

Medida 7.6 - O órgão estabelece e mantém um processo de remediação?

Medida 7.7 - O órgão corrige vulnerabilidades detectadas?

Há um Guia de Gerenciamento de Vulnerabilidades e um Modelo de Política de Gerenciamento de vulnerabilidades disponibilizado como material complementar ao *framework* do PPSI, com enfoque na construção de processos de gerenciamento de vulnerabilidades [SGD 2024b]. Os três *benchmarks* do CIS estudados (*Ubuntu 12.04 LTS Server, NGINX* e *Google Chrome*) também abordam medidas deste controle.

Das 8 medidas de segurança deste controle, 2 delas viabilizam uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.8. Controle 8: Gestão Registros de Auditoria

O oitavo controle do PPSI trata da coleta, alerta, análise e retenção de *logs* com o objetivo de detectar, compreender ou se recuperar de um ataque. Muitas vezes, registros de *log* são a única evidência de um ataque bem-sucedido contra a organização. A falta ou insuficiência de um processo de análise de *logs* pode possibilitar que um atacante controle um ativo institucional por meses ou anos sem que seja detectado [SGD 2024b].

No contexto deste controle, um *log* de sistema tipicamente fornece registros de eventos que mostram vários dados de processos, como tempo de início e fim, *crashes*, e etc. *Logs* de auditoria tipicamente incluem informações a nível de usuário, como informações sobre quando um login é feito e quando um arquivo é acessado, por exemplo.

Este controle é composto por 12 medidas de segurança:

Medida 8.1 - O órgão estabelece e mantém um processo de gestão de *log* de auditoria?

Medida 8.2 - O órgão garante o armazenamento adequado do registro de auditoria?

Medida 8.3 - O órgão padroniza a sincronização de tempo?

Medida 8.4 - O órgão retém os *logs* de auditoria?

Medida 8.5 - O órgão coleta *logs* de auditoria?

Medida 8.6 - O órgão coleta *logs* de auditoria detalhados?

Medida 8.7 - O órgão coleta *logs* de auditoria de consulta de DNS?

Medida 8.8 - O órgão coleta *logs* de auditoria de requisição de URL?

Medida 8.9 - O órgão coleta *logs* de auditoria de linha de comando?

Medida 8.10 - O órgão centraliza os *logs* de auditoria?

Medida 8.11 - O órgão conduz revisões de *log* de auditoria?

Medida 8.12 - O órgão coleta *logs* do provedor de serviços?

Há um Modelo de Política de Gestão de Registros (*Logs*) de Auditoria disponibilizado como material complementar ao *framework* do PPSI. Além disso, os três *benchmarks* do CIS estudados *(Ubuntu 12.04 LTS Server*, *NGINX* e *Google Chrome*) também abordam medidas deste controle.

Das 12 medidas de segurança deste controle, 4 delas admitem uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.9. Controle 10: Defesas contra *Malware*

O décimo controle de segurança do PPSI trata da defesa contra instalação, execução e disseminação de aplicações, códigos ou *scripts* maliciosos em ativos da organização.

Softwares maliciosos estão em constante evolução e adaptação, exigindo que as ferramentas de defesa contra *malware* sejam capazes de operar neste ambiente dinâmico. Ferramentas antivírus deve contar com funcionalidades de automação, atualização rápida, oportuna e integração com outros processos, como de gestão de vulnerabilidades e resposta a incidentes. Esses softwares de defesa devem ser instalados em todos os possíveis pontos de entrada e ativos institucionais, considerando que grande parte dos ataques ocorre por conta de comportamento inseguro dos usuários finais, como cliques em links estranhos e uso de dispositivos USB infectados [SGD 2024b].

Este controle é composto por 7 medidas:

Medida 10.1 - O órgão instala e mantém um software *antimalware*?

Medida 10.2 - O órgão configura atualizações automáticas de assinatura *antimalware*?

Medida 10.3 - O órgão desabilita a execução e produção automática para mídias removíveis?

Medida 10.4 - O órgão habilita funções antiexploração?

Medida 10.5 - O órgão gerencia o software *antimalware* de maneira centralizada?

Medida 10.6 - O órgão configura a varredura *antimalware* automática de mídia removível?

Medida 10.7 - O órgão utiliza software *antimalware* baseado em comportamento?

O documento *CIS Ubuntu 12.04 LTS Server Benchmark v1.1.0* trata de parte das medidas deste controle e pode ser usado como referência na configuração de um sistema operacional, principalmente nas questões sobre execução de mídias removíveis. Além

disso, a SGD disponibiliza um Modelo de Política de Defesas contra *Malware*, que pode ser utilizado de forma complementar [SGD 2024b].

Das 7 medidas de segurança deste controle, 2 delas apoiam uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.10. Controle 11: Recuperação de Dados

O controle 11 se atenta à capacidade da organização de recuperar seus dados e os ativos em situações de incidentes para um estado anterior confiável. Nos casos em que um atacante obtém acesso a um ativo da instituição e o torna inseguro, é necessário ter a possibilidade de se valer de *backups* confiáveis para restaurar o dispositivo ou dados para um momento conhecido e seguro.

Nota-se também que um ativo institucional pode ser alvo de um *ransomware*, um tipo de *malware* que criptografa e sequestra os dados de um órgão, exigindo o pagamento de uma quantia para desbloqueio. Embora a utilização de um *backup* confiável possa recuperar o ativo ou os dados, os atacantes ainda podem vender ou divulgar os dados sequestrados.

Este controle é composto por 5 medidas:

Medida 11.1 - O órgão protege os dados de recuperação?

Medida 11.2 - O órgão estabelece e mantém um processo de recuperação de dados?

Medida 11.3 - O órgão executa backups automatizados?

Medida 11.4 - O órgão estabelece e mantém uma instância isolada de dados de recuperação?

Medida 11.5 - O órgão testa os dados de recuperação?

A secretaria de Governo Digital disponibiliza um Modelo de Política de Backup focado na construção das políticas de *backup* e restauração de dados digitais da instituição, que pode ser utilizado como material complementar na implementação das medidas [SGD 2024b].

Das 5 medidas de segurança deste controle, 4 delas apoiam uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.11. Controle 12: Gestão de Infraestrutura de Rede

Este controle foca em estabelecer, implementar e gerenciar ativamente os dispositivos de rede para evitar a exploração de serviços e pontos de acesso vulneráveis por atacantes. Uma infraestrutura de rede segura constitui uma defesa essencial contra atacantes e inclui aspectos de arquiteturas seguras, monitoramento de alterações ao longo do tempo e reavaliação regular das configurações atuais.

Além disso, a rede de um órgão pode estar em constante mudança, o que exige a análise regular dos diagramas de arquitetura, configurações, controles de acesso e fluxos de tráfego, tudo a fim de evitar que atacantes se aproveitem de pontos vulneráveis não

identificados. Este controle se relaciona com outros, como de gestão de ativos, proteção contra *malware* e registros de *logs*, por exemplo.

Este controle é composto por 8 medidas:

Medida 12.1 - O órgão elabora e mantém diagramas de arquitetura?

Medida 12.2 - O órgão garante que a infraestrutura de rede está atualizada?

Medida 12.3 - O órgão garante níveis de segurança para a arquitetura de rede?

Medida 12.4 - O órgão gerencia a infraestrutura de rede e segurança?

Medida 12.5 - O órgão centraliza a autenticação, autorização e auditoria de rede (AAA)?

Medida 12.6 - O órgão utiliza protocolos de comunicação e gestão de rede seguros?

Medida 12.7 - O órgão garante que os dispositivos remotos utilizam uma VPN (*Virtual Private Network*) e se conectem em uma infraestrutura AAA segura da organização?

Medida 12.8 - O órgão utiliza e mantém recursos cibernéticos dedicados para todo o trabalho administrativo?

Como mencionado, medidas deste controle podem ser complementadas pelos Modelos de Política de Gestão de Ativos, de Controle de Acesso, de gestão de Registros (*Logs*) de Auditoria e de Defesas contra *Malware*, todos disponibilizados pela SGD.

Das 8 medidas de segurança deste controle, 1 delas viabiliza uma implementação rápida pelo uso de ferramentas de software livre e será abordada na próxima seção.

1.3.12. Controle 13: Monitoramento e Defesa da Rede

O controle 13 se atenta aos processos e ferramentas para monitoramento e defesa da rede do órgão contra ataques em sua infraestrutura. Um monitoramento eficaz das atividades da rede garante que a equipe seja alertada sobre atividades suspeitas e responda prontamente a incidentes de segurança, como quando um *malware* é descoberto, credenciais são roubadas ou quando dados sensíveis são comprometidos [SGD 2024b].

Este controle é composto por 11 medidas:

Medida 13.1 - O órgão realiza filtragem de tráfego entre os segmentos de rede?

Medida 13.2 - O órgão aplica o gerenciamento de controle de acesso em ativos remotos?

Medida 13.3 - O órgão implanta soluções de prevenção de intrusão baseada em *host*?

Medida 13.4 - O órgão implanta soluções para prevenção de intrusão de rede?

Medida 13.5 - O órgão implanta controle de acesso a nível de porta?

Medida 13.6 - O órgão realiza a filtragem de camada de aplicação?

Medida 13.7 - O órgão centraliza alertas de eventos de segurança?

Medida 13.8 - O órgão implanta soluções de detecção e intrusão baseada em *host*?

Medida 13.9 - O órgão realiza filtragem de tráfego entre os segmentos de rede?

Medida 13.10 - O órgão coleta *logs* de fluxo e tráfego de rede?

Medida 13.11 - O órgão ajusta os limites de alertas de eventos de segurança?

Das 11 medidas de segurança deste controle, 3 delas admitem uma implementação rápida pelo uso de ferramentas de software livre e serão abordadas na próxima seção.

1.3.13. Controle 16: Segurança de Aplicações

Partindo para o nível de aplicação, o controle 16 se atenta à segurança ao longo do ciclo de vida dos softwares desenvolvidos e adquiridos internamente, a fim de detectar e corrigir falhas de segurança.

Além de se aproveitar das credenciais adquiridas por técnicas de engenharia social, um atacante podem explorar vulnerabilidades que encontrar nas aplicações desenvolvidas pelo próprio órgão para gerenciar seus dados e demais recursos. O processo de desenvolvimento de software é complexo, diverso, dinâmico e aplicado em várias plataformas como web, móvel e nuvem. Essa amplitude de espaços que as aplicações podem ocupar também representa uma vasta superfície de ataque para indivíduos mal intencionados. Vulnerabilidades podem existir em um projeto ou infraestrutura insegura, erros de codificação, autenticação fraca e falha nos testes de software [SGD 2024b].

No contexto em que grande parte dos softwares utilizados são providos por terceiros, a organização precisa conhecer os riscos envolvidos na utilização desses programas.

Este controle é composto por 14 medidas:

Medida 16.1 - O órgão estabelece e mantém um processo de desenvolvimento de aplicações?

Medida 16.2 - O órgão estabelece e mantém um processo para aceitar e endereçar vulnerabilidades de software?

Medida 16.3 - O órgão executa análise de causa raiz em vulnerabilidades de segurança?

Medida 16.4 - O órgão estabelece e gerencia um inventário de componentes de software de terceiros?

Medida 16.5 - O órgão usa componentes de software de terceiros atualizados e confiáveis?

Medida 16.6 - O órgão estabelece e mantém um processo para a classificação de severidade de vulnerabilidades?

Medida 16.7 - O órgão usa modelos de configurações de segurança padrão para infraestrutura de aplicações?

Medida 16.8 - O órgão separa sistemas de produção e não produção?

Medida 16.9 - O órgão treina desenvolvedores em conceitos de segurança de aplica-

ções e codificação segura?

Medida 16.10 - O órgão aplica princípios de design seguro em arquiteturas de aplicações?

Medida 16.11 - O órgão aproveita os módulos ou serviços controlados para componentes de segurança de aplicações?

Medida 16.12 - O órgão implementa verificações de segurança em nível de código?

Medida 16.13 - O órgão realiza teste de invasão de aplicação?

Medida 16.14 - O órgão realiza a modelagem de ameaças?

Há guias de requisitos mínimos de segurança para o desenvolvimento de aplicações web, APIs e aplicações móveis disponibilizados pela SGD como material complementar [SGD 2024a]. Além disso, duas medidas são contempladas no contexto da aplicação de servidor web pelo documento *CIS NGINX Benchmark v2.1.0* [CIS 2024a]. **Das 14 medidas de segurança deste controle, 1 delas apoia uma implementação rápida pelo uso de ferramentas de software livre e será abordada na próxima seção**.

1.4. Ferramentas

Este trabalho voltará sua atenção justamente aos controles e medidas que admitem uma rápida implementação. Embora nem todas as medidas do Grupo 1 sejam abordadas aqui, as que são consideradas críticas e não envolvem adoção de políticas ou são atividades gerenciais serão trabalhadas. Ainda assim, material complementar sobre a implementação de outras medidas podem ser encontradas nos documentos dos *CIS Benchmarks* [CIS 2024a]. Das 153 medidas de segurança previstas nos *CIS Controls* e no *framework* do PPSI, entende-se que 53 são críticas e apoiam uma implementação rápida com auxílio de ferramentas de software livre. Essas 53 medidas pertencem aos controles 1–8, 10–13 e 16 e podem ser atendidas a partir da utilização das ferramentas de software livre.

1.4.1. Controle 1 - Inventário e controle de ativos corporativos

Medida 1.1. As medidas do *Framework* do PPSI relacionadas à criação de um inventário detalhado de ativos institucionais podem ser implementadas pelo **NetBox** [NetBox 2025], uma ferramenta que auxilia a gerenciar e documentar ativos, como dispositivos de rede, servidores, endereços IP, conexões de rede e outros elementos de forma eficiente e organizada. A plataforma também admite automação e integração via APIs REST (*Representational State Transfer*) e *GraphQL*, viabilizando a atualização e revisão periódica do inventário. A instalação do **NetBox** pode ser feita de forma simplificada por meio de contêineres *Docker* ou em servidores dedicados, enquanto o inventário pode ser dirigido diretamente pela interface web ou por meio de *scripts*.

Um recurso útil do **NetBox** reside em seus *webhooks*, que são acionados toda vez que um ativo é modificado. Isso viabiliza a especificação de *pipelines* que integram diferentes sistemas e ativam outros utilitários de gerenciamento de configurações, como **Ansible**, que aplicam alterações.

Medida 1.2 e 1.5. O **Kea** [ISC 2025] é uma solução moderna para o gerenciamento de endereços IP, auxiliando na atribuição dinâmica e eficiente de endereços e na coleta de

informações detalhadas sobre os dispositivos conectados à rede.

O **Kea** também oferece funcionalidades avançadas para gerenciar e registrar informações a respeito da alocação de endereços IP baseadas em *logs* DHCP, nos moldes previstos na medida 1.2 do PPSI. A ferramenta é capaz de escrever *logs* com informações sobre endereço MAC (*Media Access Control*), *hostname*, data/hora e o identificador do cliente DHCP, além de se integrar a outros serviços de gerenciamento de ativos.

Além disso, o **Kea** pode ser utilizado para implementar a medida 1.5, que exige a remoção de dispositivos não autorizados da rede, negar a conexão, e/ou colocar ativos em quarentena. Isso pode ser alcançado com as listas de controle (*allowlist/denylist*) que a aplicação utiliza para permitir ou negar concessões de endereços IP.

Medida 1.3. O **Nmap** [Lyon 2025] é uma ferramenta amplamente utilizada para a descoberta ativa e mapeamento de redes, sendo ideal para identificar dispositivos conectados a uma rede institucional. No contexto do PPSI, o **Nmap** implementa a medida 1.3, que especifica o uso de uma ferramenta de descoberta ativa configurada para executar varreduras de forma diária ou com maior frequência. Dentre as possibilidades de varredura ofercidas pelo **Nmap**, destaca-se a varredura de *ping*, que identifica *hosts* ativos na rede; a detecção de serviços, que determina quais serviços estão sendo executados e em quais portas; e a varredura com precisão, capaz de indicar sistemas operacionais e versões de software.

Medida 1.4. O **Netdiscover** [Kali 2025] é uma ferramenta simples e eficaz para a descoberta passiva de dispositivos conectados a uma rede local, podendo ser utilizado para atender às necessidades da medida 1.4, que exige a identificação de ativos na rede de forma não intrusiva. Diferentemente de ferramentas de descoberta ativa, como o **Nmap**, o **Netdiscover** opera capturando pacotes ARP (*Address Resolution Protocol*) transmitidos na rede, facilitando a determinação de dispositivos conectados sem gerar tráfego adicional significativo.

1.4.2. Controle 2 - Inventário e controle de ativos de software

Medidas 2.1 e 2.6. O **OCS Inventory** [OCS 2025] é uma solução robusta utilizada para inventário e gerenciamento de ativos de TI. Projetada para simplificar o inventário de hardware e software em redes institucionais, a ferramenta consegue automatizar a coleta de informações sobre os softwares instalados, bem como criar relatórios que categorizam e identificam os programas autorizados, não autorizados e desatualizados, seguindo as medidas 2.1 e 2.6 do PPSI. Para isso, o **OCS Inventory** conta com um agente que deve ser instalado em todo dispositivo monitorado, garantindo que as informações sejam atualizadas regularmente.

Medidas 2.3, 2.4 e 2.5. O **Security Enhanced Linux (SELinux)** [Red Hat 2025b] consiste de um módulo de segurança do *kernel* do Linux, projetado para implementar o Controle de Acesso Mandatório (MAC - *Mandatory Access Control*). Ele é responsável por restringir e regular como processos e usuários interagem com o sistema, adicionando uma camada extra de segurança contra acessos não autorizados e potenciais vulnerabilidades. No contexto do PPSI, o **SELinux** consegue definir quais programas e bibliotecas podem ser executados/carregados no sistema, atendendo às medidas 2.3 e 2.4, que exigem o con-

trole de permissões sobre softwares e bibliotecas, prevenindo execuções não autorizadas. Esse mesmo sistema também pode ser utilizado para regular o uso de *scripts*, implementando a medida 2.5.

1.4.3. Controle 3 - Proteção de Dados

Medidas 3.1, 3.2, 3.3 e 3.4. O **Apache Atlas** [Apache 2025] é uma plataforma de governança e catalogação de dados projetada para ajudar organizações a gerenciar, organizar e proteger seus dados de maneira centralizada. Ele fornece recursos avançados para rastrear metadados, gerenciar classificações de dados, criar linhagens e estabelecer políticas de governança.

Medida 3.6. O **PostgreSQL** [Citusdata 2025] é um banco de dados relacional *open-source*, conhecido por sua robustez, extensibilidade e apoio a transações *ACID* (*Atomicity, Consistency, Isolation, and Durability*). Ele admite tipos avançados (como *JSON* e *arrays*, por exemplo), índices eficientes, replicação e escalabilidade, sendo amplamente usado em aplicações críticas e modernas. Para gerenciar a retenção de dados de uma aplicação organizacional armazenados no PostgreSQL, é possível usar a extensão `pg_cron` para realizar exclusões automáticas de dados com a periodicidade desejada, de acordo com a medida 3.6 do *Framework* do PPSI.

Medida 3.7. Conhecido como o destruidor de discos, o **dd** [Sysxplore 2025] é uma ferramenta poderosa e versátil amplamente utilizada em sistemas baseados em Unix/Linux para copiar, converter e manipular dados em baixo nível. Ele opera diretamente em blocos de dados, sendo capaz de realizar operações em discos, partições, sistemas de arquivos e dispositivos de armazenamento. No contexto do PPSI, o **dd** pode desempenhar um papel importante na implementação de medidas relacionadas ao descarte seguro de dados de forma irrecuperável, garantido pela sobrescrita de dispositivos de armazenamento inteiros com dados aleatórios ou padrões específicos, em conformidade com a medida 3.7.

Medida 3.10. O **OpenSSL** [OpenSSL 2025] é uma biblioteca amplamente utilizada que fornece ferramentas para a implementação de criptografia, gerenciamento de certificados e comunicação segura em sistemas de informação. Com apoio a protocolos como TLS (*Transport Layer Security*) e SSL (*Secure Sockets Layer*), o **OpenSSL** é essencial para proteger dados em trânsito e assegurar a confidencialidade, integridade e autenticidade das comunicações. No contexto do Programa de Privacidade e Segurança da Informação, o **OpenSSL** desempenha um papel fundamental no atendimento das medidas relacionadas à proteção de dados em trânsito, principalmente na comunicação HTTPS e no gerenciamento seguro de chaves e certificados digitais.

Medidas 3.8, 3.9 e 3.11. O **LUKS** (*Linux Unified Key Setup*) [Gite 2025] é uma solução de criptografia de disco projetada para proteger dados sensíveis armazenados em dispositivos Linux. Extensivamente utilizado, o **LUKS** oferece apoio a vários algoritmos de criptografia modernos, como AES, cast5 e cast6, bem como é compatível com múltiplos sistemas de arquivos, EXT4, XFS e BTRFS. No contexto do PPSI, o **LUKS** pode ser utilizado na implementação das medidas de proteção de dados das medidas 3.8 e 3.9, dada a sua capacidade de criptografar dados em dispositivos de usuário final, como *notebooks*, *desktops* e mídias removíveis. Além disso, o **LUKS** também é uma solução eficaz para implementar a medida 3.11, que aborda a criptografia de informações críticas em

repouso, garantindo que dados armazenados em servidores e estações de trabalho estejam protegidos contra acessos não autorizados.

1.4.4. Controle 4 - Configuração segura de ativos corporativos e software

Medidas 4.4 e 4.5. O **nftables** [Red Hat 2025a] é uma ferramenta avançada de filtragem de pacotes para sistemas Linux. Ele oferece recursos avançados para a criação de tabelas, cadeias e regras personalizadas destinadas ao gerenciamento eficiente do tráfego de rede. Com essa ferramenta, é possível bloquear tráfego não autorizado enquanto somente as portas e serviços essenciais para o funcionamento normal e seguro do sistema são liberados. O **nftables** é especialmente útil na implementação das medidas 4.4 e 4.5 do *Framework* do PPSI pois auxilia na implementação e gestão de *firewalls* em servidores e dispositivos de usuários finais. Assim, com o **nftables**, por exemplo, é possível implementar uma política padrão "*deny-all*" para bloquear todo o tráfego, enquanto apenas portas específicas, como SSH (22), HTTP (80) e HTTPS (443), são liberadas.

As mesmas medidas também podem ser atentidas pelo uso da ferramenta **firewalld** [Firewalld 2025], outro recurso moderno para gerenciamento de *firewalls*. Ele oferece uma interface simplificada para configurar políticas de *firewall*, utilizando um modelo baseado em zonas para segmentar diferentes interfaces de rede e aplicar regras adaptáveis de acordo com o contexto. A ferramenta, além de admitir o uso de configurações padrão (como a política "*deny-all*"), também oferece a vantagem de liberar aplicações específicas, Essa abordagem viabiliza o controle mais granular do tráfego dentro da rede, permitindo acesso a serviços de impressão e compartilhamento de arquivos ao mesmo tempo em que mantém bloqueado todo o tráfego não autorizado.

Medida 4.7. **Ansible** [Ansible 2025] é uma ferramenta de automação de TI baseada no paradigma de Infraestrutura como Código (IaC), projetada para gerenciar configurações, implantar aplicações e orquestrar sistemas. Diferentemente de outras tecnologias, como o *SaltStack*, o **Ansible** opera sem a necessidade de agentes, utilizando conexões seguras, como SSH para sistemas baseados em Unix/Linux e WinRM para sistemas Windows. Com essa ferramenta, é possível definir uma série de *playbooks* escritos em formato *YAML*, que descrevem o estado desejado dos sistemas e automatizam tarefas repetitivas e complexas. Esses *playbooks* possibilitam que os administradores de TI implementem políticas padronizadas em toda a infraestrutura, reduzindo o risco de erros manuais e garantindo consistência operacional. Uma aplicação concreta dessa ferramenta está no gerenciamento de contas padrão, conforme definido pela medida 4.7 do PPSI. Nesse contexto, o **Ansible** facilita a automatização do controle de acesso a contas como *root*, bem como a criação, a remoção e o gerenciamento de diferentes usuários.

1.4.5. Controles 5 e 6 - Gestão de Contas e Gestão de Controle de Acesso

Medidas 5.1, 5.2, 5.4, 5.5, 5.6 e 6.2. O **FreeIPA** (*Free Identity, Policy, and Audit*) [FreeIPA 2025] é uma solução robusta para o gerenciamento de identidades e políticas de acesso que reúne diversos serviços, como *LDAP* e *Kerberos*, em uma mesma plataforma. Essa ferramenta auxilia a centralizar de forma eficiente a administração de usuários, grupos, autenticação e políticas de segurança, oferecendo uma interface simplificada para gerenciar identidades, atendendo às medidas 5.1, 5.2 e 5.5 do PPSI. O **FreeIPA** também

atende a medida 5.4 ao facilitar a criação de políticas específicas que limitam privilégios a determinados usuários ou funções, como administradores. Esse utilitário facilita a automação de processos de gestão de identidades, abrangendo a criação, modificação e desativação de contas, bem como a concessão e revogação de acessos. Além disso, viabiliza a configuração de fluxos automatizados que asseguram que novos usuários recebam os direitos apropriados, em conformidade com as medidas 5.6 e 6.2.

Uma configuração básica do **FreeIPA** parte da instalação dos pacotes necessários, seguido da execução do instalador interativo com o comando `ipa-server-install`. Durante a configuração inicial, são definidos o domínio principal, o nome do servidor e as credenciais do administrador. Após a instalação, é possível adicionar usuários e grupos, configurar políticas de acesso e definir regras como a desativação automática de contas após revogações.

Medidas 5.5, 5.6, 6.4, 6.5 e 6.6. O **Keycloak** [Keycloak 2025] é uma poderosa ferramenta de gerenciamento de identidades e acesso projetada para simplificar e aprimorar os processos de autenticação e autorização em aplicações modernas. Ele oferece uma ampla gama de recursos avançados, como autenticação centralizada e *Single Sign-On* (SSO), que possibilita aos usuários acessarem diversas aplicações com uma única autenticação. Essa ferramenta também inclui o controle de acesso baseado em funções (RBAC), que assegura uma administração granular de permissões, bem como fornece apoio à autenticação multifator (MFA). O **Keycloak** se destaca por sua capacidade de implementar autenticação centralizada (atendendo a medida 5.5), exigir autenticação multifator (atendendo as medidas 6.4, 6.5 e 6.6) e gerenciar contas e permissões de forma eficiente. Além disso, o **Keycloak** também apresenta configurações personalizadas para a desativação de contas inativas (Medida 5.6). A ferramenta é disponibilizada para distribuições Linux, conta com uma imagem oficial no *Docker Hub* e também uma implantação em *Kubernetes*.

Medidas 5.1, 5.2, 5.3, 5.6, 6.1, 6.2 e 6.3. **OpenBao** [OpenBao 2025] é uma solução avançada para o gerenciamento seguro de segredos, autenticação e políticas de controle de acesso, centralizando o armazenamento de credenciais, como senhas, tokens, certificados e chaves de API, em um ambiente seguro, garantindo que segredos sejam acessados e gerenciados de forma controlada e auditável. Ele também oferece apoio à geração dinâmica de senhas únicas e *tokens*, garantindo que credenciais sejam sempre exclusivas, com uso de autenticação multifator (MFA) e controle de acesso baseado em politicas (RBAC). Além disso, o **OpenBao** facilita a revogação de acessos por meio da desativação automática de segredos expirados ou desnecessários, de acordo com as políticas configuradas.

A ferramenta é compatível com as principais distribuições Linux e pode ser facilmente implantado em ambientes baseados em contêineres, utilizando o *Docker* para simplificar a configuração e a escalabilidade.

1.4.6. Controle 7 - Gestão Contínua de Vulnerabilidades

Medidas 7.1 e 7.2. As medidas 7.1 e 7.2 do *Framework* do PPSI tratam sobre a varredura automatizada dos ativos institucionais para descoberta de vulnerabilidades. Essa atividade pode ser apoiada pelo uso do **OpenVAS** (*Open Vulnerability Assessment Scanner*), um mecanismo de varredura que executa Testes de Vulnerabilidade (VTs) nos sistemas-alvo utilizando informações adquiridas a partir de um *feed* atualizado diariamente. O

OpenVAS suporta testes de vulnerabilidade autenticados e não autenticados, testes em protocolos de rede de alto e baixo nível e testes customizados [Greenbone 2025b].

A instalação da ferramenta pode ser simplificada pelo uso de um contêiner *Docker* disponibilizado na página de documentação da ferramenta [Greenbone 2025a] e possui interface gráfica, possibilitando o uso facilitado de suas funcionalidades. A varredura parte da seleção da faixa de rede a ser escaneada, o horário de início e inserção opcional de credenciais, seguindo para a verificação de vulnerabilidades nos *hosts* encontrados. A primeira execução da ferramenta demanda uma sincronização inicial do *feed* de testes, o que pode levar de 15 a 45 minutos e precisa ser feita antes da primeira varredura. Os resultados obtidos pela varredura são exibidos em um relatório que indica as vulnerabilidades encontradas, o grau de severidade delas e formas de correção. A ferramenta também suporta o agendamento de varreduras, cumprindo o que estabelece as medidas de segurança 7.1 e 7.2.

1.4.7. Controle 8 - Gestão de registros de auditoria

Medida 8.3. O **Chrony** [Chrony 2024] é um serviço de sincronização de tempo para sistemas operacionais baseados em Linux, projetado para substituir o tradicional NTP (*Network Time Protocol*). Ele é ideal para ambientes modernos, oferecendo uma solução eficiente, rápida e precisa para manter os relógios dos sistemas sincronizados e de acordo com a medida 8.3 do *Framework* do PPSI.

Medidas 8.5, 8.6 e 8.9. O **auditd** [Grubb 2024] é uma ferramenta de auditoria no Linux que registra eventos de segurança, como execução de comandos e alterações no sistema. Ele viabiliza monitorar atividades de usuários e processos, ajudando a detectar comportamentos maliciosos e a garantir conformidade com políticas de segurança. As principais ferramentas são `auditctl` (para gerenciar regras), `ausearch` (para buscar `logs`) e `aureport` (para gerar relatórios).

1.4.8. Controle 10 - Defesas contra Malware

Medidas 10.1 e 10.2. O **ClamAV** [ClamAV 2025] é um antivírus de código aberto, projetado para detectar *malwares* como vírus, *trojans* e *worms*. Ele suporta múltiplos formatos de arquivos, incluindo compactados, e realiza varreduras em tempo real ou sob demanda. É amplamente utilizado em servidores de e-mail e arquivos e é compatível com Linux, macOS e Windows. Seus principais componentes são: (a) `clamscan` para varreduras manuais de arquivos; (b) `freshclam` para atualização automática de assinaturas; e (c) `clamd`, que oferece varredura contínua de arquivos.

É possível usar o `clamscan` para fazer a varredura do todos os arquivos do sistema, o *daemon* `clamd` para varreduras em segundo plano e o `freshclam` para atualizar o banco de assinaturas automaticamente. Para realizar varreduras em e-mails, é possível usar o `amavis` junto com o **ClamAV**. O `amavis` é um filtro de conteúdo de e-mail, utilizado para integrar verificações de vírus e outros tipos de escaneamento (como antivírus, spam, etc.) em servidores de e-mail. Ele funciona como um intermediário entre um servidor de e-mail e programas de verificação de conteúdo, como o **ClamAV**. Para fazer essa ligação, o `amavisd` deve se conectar com o socket do `clamd`.

1.4.9. Controle 11 - Recuperação de dados

Medidas 11.1, 11.3, 11.4 e 11.5. O **Bacula** [Bacula 2025] é uma solução robusta e modular para o gerenciamento de *backups*, recuperação e verificação de dados. Projetado para suportar múltiplos sistemas operacionais, como Linux, Windows e MacOS, o **Bacula** oferece compatibilidade com diversos tipos de armazenamento, incluindo discos locais, fitas magnéticas e serviços de armazenamento na nuvem.

No contexto do PPSI, o **Bacula** pode desempenhar um papel central no atendimento às medidas do Controle 11, relacionadas à recuperação e backup de dados. A ferramenta, por exemplo, facilita a execução de *backups* automatizados (medida 11.3), garantindo que os dados críticos da organização sejam salvos regularmente. Além disso, o **Bacula** propicia a criação de instâncias isoladas para armazenamento de dados de recuperação (medida 11.4), como *backups* em dispositivos off-line, locais remotos ou na nuvem. Adicionalmente, o **Bacula** oferece suporte à criptografia de dados em trânsito e em repouso, atendendo à medida 11.1, que exige a proteção adequada dos dados de recuperação. Por fim, essa ferramenta é capaz de realizar testes regulares de integridade e recuperação (medida 11.5), sendo possível verificar a usabilidade dos *backups* e garantindo que os dados possam ser restaurados corretamente em caso de necessidade.

1.4.10. Controle 12 - Gestão da infraestrutura de rede

Medida 12.1. O **PlantUML** [PlantUML 2025] é uma ferramenta avançada para a criação de diagramas a partir de texto, amplamente acessível em diversas plataformas e ferramentas modernas, como IDEs (*Integrated Development Environment*), sistemas de controle de versão e editores de texto. Ele oferece recursos poderosos para a geração de diagramas de sequência, classes, casos de uso e muitos outros, de forma eficiente e personalizável. Com essa ferramenta, é possível documentar sistemas complexos de maneira clara e estruturada, garantindo que equipes de desenvolvimento e *stakeholders* compreendam e mantenham a arquitetura e os fluxos de trabalho com facilidade. Portanto, o **PlantUML** é uma ferramenta especialmente útil para atender à medida 12.1 do PPSI, que recomenda elaborar e manter diagramas da arquitetura de rede.

1.4.11. Controle 13 - Monitoramento e defesa da Rede

Medida 13.6. Para tratar da filtragem na camada de aplicação prevista na medida 13.6, pode-se utilizar ferramentas do tipo WAF (*Web Application Firewall*), como o **open-appsec**, para realizar a filtragem de requisições que um servidor web NGINX recebe. O **open-appsec** é um software livre e possui planos gratuitos básicos, mas capazes de detectar e prevenir ataques Web baseado em técnicas de *machine-learning* e ataques contra APIs. Por utilizar fundamentos de *machine-learning*, este software é capaz de detectar os principais ataques da OWASP Top 10 (*Open Worldwide Application Security Project*) e também ataques *0-day*.Documentos sobre a instalação, uso e visualização de alertas da ferramenta podem ser verificados na sua página na internet [CheckPoint 2025]. Outra opção de WAF é **Modsecurity**, uma extensão para o serviço NGINX capaz de filtrar requisições HTTP [Zimmerle and Belov 2024].

Medida 13.8. O **AIDE** (*Advanced Intrusion Detection Environment*) é uma ferramenta de software livre capaz de checar e monitorar a integridade de arquivos e diretórios dentro de

sistemas Linux, oferecendo recursos como verificação de atributos de arquivos, checagem de múltiplos *checksums*, arquivos de configuração e banco de dados em texto simples, além de admitir o uso de expressões regulares para personalizar o que será monitorado.O **AIDE** é software livre, disponível no *github* [AIDE 2025]. A ferramenta está incluída em várias distribuições Linux, como Debian, Ubuntu, FreeBSD, Gentoo e outros, podendo ser instalado a partir da linha de comando. As configurações da ferramenta se encontram no arquivo `aide.conf` localizado em `/etc/aide` e é neste documento que se indica os arquivos e diretórios monitorados [Kastning 2024]. O uso da ferramenta ocorre por meio da linha de comando do sistema operacional e sua automatização pode ser feita por meio do utilitário `cron` do Linux. As checagens podem ser feitas diariamente, enquanto novos bancos de dados podem ser criados semanalmente. A capacidade de verificar a alteração não autorizada em arquivos e diretórios do sistema se adequa à medida de segurança 13.3 do *framework* do PPSI, detectando ataques ao *host*.

Medida 13.9. O **Suricata** [Suricata 2025] é uma conhecida ferramenta desenvolvida para ser um mecanismo de detecção de intrusão moderno, aproveitando de arquiteturas *multi-thread* nativamente. O funcionamento do Suricata é baseado na criação de regras compostas por ações, cabeçalho dos protocolos de rede e opções extras. As ações podem ser dos tipos `alert` (que gera um alerta), `pass` (que interrompe a inspeção adicional do pacote), `drop` (que descarta o pacote e gera um alerta) e `reject` (que responde um pacote com *flag* RST). O Suricata também suporta os protocolos de rede e de aplicação, como TCP, UDP, ICMP, HTTP, SSH e FTP, dentre outros [Bueno 2024]. A ferramenta pode ser instalada a partir da linha de comando na maioria das distribuições Linux, e suas configurações podem incluir indicações das interfaces de rede que capturarão pacotes, regras a serem importadas, formatos dos *logs*, etc. As funções da ferramenta Suricata são capazes de implementar a medida 13.4 do *framework* do PPSI, fornecendo uma possibilidade de implementação de sistema de detecção de intrusão de rede.

1.4.12. Controle 16 - Segurança de aplicações

Medida 16.4. A atividade de estabelecer e gerenciar um inventário de componentes de software de terceiros é facilitada pela extração de um **SBOM** (*software bill of materials*). A plataforma de versionamento de código **Github** disponibiliza um utilitário para todos os seus usuários que possibilita a extração de um relatório de componentes a partir de um repositório [Github 2025].

Medida 16.8. O **OpenTofu** [OpenTofu 2025] é uma ferramenta de Infraestrutura como Código (IaC) de código aberto que possibilita criar, gerenciar e versionar infraestrutura de maneira declarativa. Ele oferece uma alternativa totalmente aberta, com foco na comunidade, para gerenciar infraestrutura em nuvem e ambientes *on-premises*. Semelhante ao *Terraform*, o *OpenTofu* utiliza uma abordagem declarativa e configurações em HCL *(HashiCorp Configuration Language)* para descrever a infraestrutura.

A medida 16.8 do PPSI enfatiza a separação entre sistemas de produção e não produção, promovendo estabilidade e segurança. O uso conjunto do **OpenTofu** e **Ansible** auxilia no cumprimento dessa exigência ao tornar a infraestrutura reproduzível e consistente. O **OpenTofu** contribui automatizando a criação e a destruição de ambientes, enquanto o **Ansible** contribui automatizando configurações específicas de um serviço

dentro de cada ambiente criado. Ao combinar o uso das ferramentas **OpenTofu** e **Ansible**, a separação entre ambientes é garantida.

1.5. Conclusão

Implementar controles e medidas de segurança previstas em *frameworks* pode ser uma tarefa complexa, principalmente para entidades que não possuem políticas e procedimentos de segurança bem definidos. A fim de evitar medidas de cunho gerencial e focando em atividades práticas de rápida implementação, este trabalho buscou fornecer uma base sólida para que as organizações possam dar seus primeiros passos em direção à conformidade com o uso de software livre. Entende-se que a implementação das medidas aqui abordadas possibilita alcançar um patamar satisfatório de cibersegurança no contexto dessas organizações.

Referências

[AIDE 2025] AIDE (2025). Aide. https://github.com/aide/aide.

[Ansible 2025] Ansible (2025). Ansible documentation. https://docs.ansible.com/.

[Apache 2025] Apache (2025). Apache atlas quick start. https://atlas.apache.org/#/QuickStart.

[Bacula 2025] Bacula (2025). Bacula systems backup software main manual 15.0.x. https://www.bacula.org/15.0.x-manuals/en/main/index.html.

[Bueno 2024] Bueno, C. I. (2024). Um estudo de caso sobre a implantação de um sistema de detecção de intrusões aplicado a um projeto em parceria com o sus. Trabalho de Conclusão de Curso.

[CheckPoint 2025] CheckPoint (2025). Getting started. https://docs.openappsec.io/getting-started/getting-started.

[Chrony 2024] Chrony (2024). Chrony homepage. https://chrony-project.org/.

[CIS 2024a] CIS (2024a). Cis benchmarks. https://learn.cisecurity.org/benchmarks.

[CIS 2024b] CIS (2024b). Cis benchmarks overview. https://www.cisecurity.org/cis-benchmarks-overview.

[CIS 2024c] CIS (2024c). Cis critical security controls implementation. https://www.cisecurity.org/controls/implementation-groups/.

[CIS 2024d] CIS (2024d). Cis critical security controls implementation group 2. https://www.cisecurity.org/controls/implementation-groups/ig3.

[CIS 2024e] CIS (2024e). Cis critical security controls navigator. https://www.cisecurity.org/controls/cis-controls-navigator.

[CIS 2024f] CIS (2024f). Cis critical security controls version 8.1.

[CIS 2024g] CIS (2024g). Mapping and compliance. https://www.cisecurity.org/cybersecurity-tools/mapping-compliance.

[Citusdata 2025] Citusdata (2025). pg_cron github. https://github.com/citusdata/pg_cron.

[ClamAV 2025] ClamAV (2025). Clamav. https://www.clamav.net/.

[Firewalld 2025] Firewalld (2025). Firewalld documentation. https://firewalld.org/documentation/.

[FreeIPA 2025] FreeIPA (2025). Freeipa quick start guide. https://www.freeipa.org/page/Quick_Start_Guide.

[Gite 2025] Gite, V. (2025). How to: Linux hard disk encryption with luks cryptsetup command. https://www.cyberciti.biz/security/howto-linux-hard-disk-encryption-with-luks-cryptsetup-command/.

[Github 2025] Github (2025). Como exportar uma lista de materiais de software para seu repositório. https://docs.github.com/pt/code-security/supply-chain-security/understanding-your-software-supply-chain/exporting-a-software-bill-of-materials-for-your-repository.

[Greenbone 2025a] Greenbone (2025a). Greenbone community containers. https://greenbone.github.io/docs/latest/22.4/container/.

[Greenbone 2025b] Greenbone (2025b). Greenbone openvas. https://www.openvas.org/.

[Grubb 2024] Grubb, S. (2024). auditd(8) - linux man page. https://linux.die.net/man/8/auditd/.

[IBM 2024] IBM (2024). What is shadow it? https://www.ibm.com/topics/shadow-it.

[ISC 2025] ISC, I. S. C. (2025). Kea dhcp documentation - version 2.6.1. https://kea.readthedocs.io/en/kea-2.6.1/.

[Kali 2025] Kali (2025). Netdiscover - kali linux tools. https://www.kali.org/tools/netdiscover/.

[Kastning 2024] Kastning, J. (2024). Introduction to the advanced intrusion detection environment (aide). https://www.opensourcerers.org/2024/04/15/introduction-to-the-advanced-intrusion-detection-environment-aide/.

[Keycloak 2025] Keycloak (2025). Keycloak server administration guide (latest version). https://www.keycloak.org/docs/latest/server_admin/index.html.

[Lyon 2025] Lyon, G. (2025). Nmap homepage. https://nmap.org/.

[NetBox 2025] NetBox (2025). Netbox documentation (stable version). https://netboxlabs.com/docs/netbox/en/stable/.

[NIST 2024a] NIST (2024a). About us. https://www.nist.gov/about-nist.

[NIST 2024b] NIST (2024b). Cybersecurity. https://www.nist.gov/cybersecurity.

[NIST 2024c] NIST (2024c). Nist csf 2.0 implementation examples. https://www.nist.gov/system/files/documents/2024/02/21/CSF%202.0%20Implementation%20Examples.pdf.

[NIST 2024d] NIST (2024d). Nist cybersecurity framework 2.0: Small business quick-start guide. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf.

[NIST 2024e] NIST (2024e). The nist cybersecurity framework (csf) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[NIST 2024f] NIST (2024f). Node-link diagram of the cybersecurity framework v2.0 mapped to controls. https://csf.tools/visualizations/node-link-diagram-of-the-cybersecurity-framework-v2-0-mapped-to-controls/.

[NIST 2024g] NIST (2024g). Topics. https://www.nist.gov/topics.

[OCS 2025] OCS (2025). Ocs inventory ng wiki. https://wiki.ocsinventory-ng.org/.

[OpenBao 2025] OpenBao (2025). Openbao documentation. https://openbao.org/docs/.

[OpenSSL 2025] OpenSSL (2025). Openssl library. https://linux.die.net/man/1/openssl.

[OpenTofu 2025] OpenTofu (2025). Opentofu. https://opentofu.org/.

[PlantUML 2025] PlantUML (2025). Plantuml nwdiag. https://plantuml.com/nwdiag.

[Red Hat 2025a] Red Hat, I. (2025a). Getting started with nftables - configuring and managing networking - red hat enterprise linux 8. https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/configuring_and_managing_networking/getting-started-with-nftables_configuring-and-managing-networking#getting-started-with-nftables_configuring-and-managing-networking.

[Red Hat 2025b] Red Hat, I. (2025b). Selinux users and administrators guide - red hat enterprise linux 7. https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/index#idm140415566801680.

[SGD 2023a] SGD (2023a). Cartilha do programa de privacidade e segurança da informação (ppsi). https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908.

[SGD 2023b] SGD (2023b). Portaria sgd/mgi nº 852, de 28 de marÇo de 2023. https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908.

[SGD 2024a] SGD (2024a). Framework, guias e modelos. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos.

[SGD 2024b] SGD (2024b). Guia do framework de privacidade e segurança da informação. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf.

[Suricata 2025] Suricata (2025). Suricata homepage. https://suricata.io/.

[Sysxplore 2025] Sysxplore (2025). The complete guide to the dd command in linux. https://blog.kubesimplify.com/the-complete-guide-to-the-dd-command-in-linux.

[Zimmerle and Belov 2024] Zimmerle, F. and Belov, A. (2024). Modsecurity-nginx. https://github.com/owasp-modsecurity/ModSecurity-nginx.

Capítulo

2

A Importância dos Sistemas de Informação para a Participação Pública, Controle Social e Controle Interno: Um Estudo de Caso da Prefeitura do Recife

Marcelo L. Perrucci, Ricardo Neves Cardoso e Rodrigo Brayner

Abstract

This chapter explores how information systems strengthen public participation, social control, and inclusion in governance, focusing on the case of Recife. Based on the Theory of Absorptive Capacity, it argues how structured data systems promote transparency, participation, accountability, and citizen-centered policies. By integrating technologies such as storytelling and accessible, cutting-edge interfaces, Recife fosters active citizenship, reduces informational asymmetries, and empowers marginalized groups, establishing itself as a model of participative and inclusive democracy.

Resumo

Este capítulo explora como os sistemas de informação fortalecem a participação pública, o controle social e a inclusão na governança, com foco no caso de Recife. Com base na Teoria da Capacidade de Absorção, argumenta-se como sistemas estruturados de dados promovem transparência, participação, accountability e políticas centradas no cidadão. Ao integrar tecnologias como storytelling e interfaces acessíveis, com tecnologia de ponta, Recife incentiva a cidadania ativa, reduz assimetrias informacionais e empodera grupos marginalizados, consolidando-se como um modelo de democracia participativa e inclusiva.

1. Introdução

No contexto de sociedade moderna, a administração pública enfrenta o desafio de atender a uma população cada vez mais participativa e exigente, especialmente quando falamos das gestões municipais, que atuam diretamente na execução das políticas públicas e prestam serviço direto à população. Para fazer frente a esse novo momento, a gestão do conhecimento e da informação passaram a ser cruciais para garantir o pleno exercício do controle social, bem como viabilizar a execução de políticas públicas de forma eficaz.

Nesse cenário, de volume de dados excessivo, os sistemas de informação surgem como alternativas fundamentais para viabilizar e facilitar a interação governo-sociedade permitindo uma maior velocidade na disponibilização desses dados e, com isso, viabilizar uma gestão mais participativa, inclusiva e cidadã.

A utilização desses sistemas busca proporcionar uma forma ágil, confiável e sólida para a garantia da transparência na administração pública, pois possibilitam o armazenamento, a análise e a disponibilização de forma estruturada de dados de modo a permitir que os cidadãos acessem informações de gastos públicos, investimentos, fornecedores, contratações e, inclusive, a priorização dada pela gestão estratégica do ente. É verdade que ainda existe um longo caminho a ser percorrido, pois a simples disponibilização dos dados, mesmo que de forma estruturada e organizada, não garante a transparência. A implementação de ferramentas como Storytelling e o investimento em painéis visualmente mais leves atrás da análise de experiência dos usuários, são estratégias dos entes para dar um passo além da simples disponibilização, mas ainda demandam de mais mudanças para garantir a efetiva mudança que colocará o usuário do serviço público como verdadeiro protagonista.

Um ambiente propício para a *accountability* é aquele em que a população pode ter acesso às informações públicas de forma clara, em linguagem cidadã, criando um ambiente propício ao controle social, à fiscalização dos gastos públicos e atos praticados pelos governantes. Não se trata somente de abertura de dados, mas de um processo de transferência de protagonismo, gerando cidadãos mais engajados, atuantes e condutores de transformações sociais.

Portanto, o investimento, por parte da administração pública, em sistemas de informação e fortalecimento dos instrumentos de participação social é fundamental para a construção de uma lógica de controle social verdadeiramente representativa, atuante e eficaz. A lógica desses investimentos devem ser guiadas sempre pelo olhar do cidadão, pensando no melhor formato de acesso, em disponibilidade, em integridade. Com isso, o conceito de sociedade sai fortalecido e o propósito dos governos na busca do atendimento dos preceitos fundamentais da Constituição, em especial em seu artigo 3º, que trata dos objetivos fundamentais da República Federativa do Brasil.

A ausência desses investimentos dificulta bastante a atuação cidadã no exercício do seu papel fiscalizador e agente indutor de mudanças, pois sem sistemas de informação sólidos, a disponibilização dos dados necessários para que aconteça essa atuação, é inviabilizada. Isso dificulta não só o controle social mas, também, a atuação dos gestores públicos, impedindo-os

uma tomada de decisão assertiva, embasada e segura, ampliando assim o risco na gestão de suas áreas de atuação. Assim, este capítulo discorre com profundidade acerca da importância destes sistemas, evidenciando sua relevância para a participação ativa da sociedade no acompanhamento da atuação da administração pública, para o fortalecimento do controle social e a relevância da atuação do controle interno para viabilizar a eficácia e efetividade na execução das políticas públicas.

2. A importância do controle interno para a eficácia, eficiência e efetividade das políticas públicas.

Importante, antes de adentrar no detalhamento da importância do controle interno para a consecução de políticas públicas, faz-se necessário apresentar uma breve linha do tempo dos principais marcos legais e, em complemento, alguns conceitos elaborados pelas principais organizações profissionais internacionais que possuem relação com a área.

A evolução do controle interno na administração pública no Brasil foi marcada, inicialmente, pela edição da Lei nº 4.320, de 17 de março de 1964, que determinou, dentre outros aspectos, a verificação dos atos de execução orçamentária de forma prévia, concomitante e posteriori, constituindo, do ponto de vista legal, a formalização das primeiras rotinas de controle. Além disso, a referida legislação também previu a necessidade do controle da legalidade dos atos praticados pela administração.

Segundo Carvalho Filho, o controle de legalidade dos atos da Administração:

> *"pode ser interno ou externo, vale dizer pode ser processado pelos órgãos da mesma Administração ou por órgãos de Poder diverso. Pode dizer-se, assim, que Legislativo, Judiciário e a própria Administração podem exercer o controle de legalidade. O judiciário, por exemplo, examina a legalidade de atos administrativos em mandado de segurança (art. 5º, LXIX, CF). O Legislativo pelo seu Tribunal de Contas aprecia a legalidade dos atos de admissão de pessoal (art. 71, III, CF). E a Administração, em qualquer esfera, controla a legalidade de seus próprios atos: se uma autoridade age em desconformidade com a norma jurídica válida, pode o Secretário controlar a legalidade da ação administrativa."*

Com a reforma administrativa instituída pelo Decreto Lei nº 200, de 25 de fevereiro de 1967, novas diretrizes foram incorporadas à administração pública, entre elas, a elevação do controle como princípio fundamental da administração federal e a determinação de que o mesmo deveria ser exercido em todos os níveis e órgãos da administração federal. A modernização introduzida pelo supracitado Decreto permitiu não só a ampliação da relevância do controle como permitiu o acompanhamento mais célere da gestão. Desse marco em diante o controle passou a atuar em outras perspectivas que não aquelas relacionadas aos aspectos formais, passando a guiar-se pelos princípios da eficiência, eficácia, economicidade e efetividade.

As mudanças advindas deste novo conceito de controle influenciaram na redação da Carta Magna de 5 de outubro de 1988, sobretudo, no que se refere à instituição dos controles interno e externo aos poderes Executivo, Legislativo e Judiciário e quanto ao modo de condução das políticas financeira, orçamentária, contábil, patrimonial e operacional da administração:

> *Art. 70. A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta,*

> *quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder.*
>
> *Art. 71. O controle externo, a cargo do Congresso Nacional, será exercido com o auxílio do Tribunal de Contas da União [...]*
>
> *Art. 74. Os Poderes Legislativo, Executivo e Judiciário manterão, de forma integrada, sistema de controle interno com a finalidade de:*
>
> *I avaliar o cumprimento das metas previstas no plano plurianual, a execução dos programas de governo e dos orçamentos da União;*
>
> *II comprovar a legalidade e avaliar os resultados, quanto à eficácia e eficiência, da gestão orçamentária, financeira e patrimonial nos órgãos e entidades da administração federal, bem como da aplicação de recursos públicos por entidades de direito privado;*
>
> *III exercer o controle das operações de crédito, avais e garantias, bem como dos direitos e haveres da União;*
>
> *IV apoiar o controle externo no exercício de sua missão institucional.*
>
> *§1º Os responsáveis pelo controle interno, ao tomarem conhecimento de qualquer irregularidade ou ilegalidade, dela darão ciência ao Tribunal de Contas da União, sob pena de responsabilidade solidária.*

Em relação ao Município de Recife, objeto discorrido neste capítulo, o normativo que regula o tema é a Constituição Estadual de Pernambuco em seu Artigo 31, que estabelece a obrigatoriedade dos Controles Internos de cada Poder dar conhecimento ao Tribunal de Contas do Estado de Pernambuco de eventual irregularidade que se tenha conhecimento.

Além legislação indicar como papel do Controle Interno ser garantidor dos princípios da eficiência, eficácia e efetividade, importantes instituições conceituam a área como fundamental nesse processo de fortalecimento de políticas públicas, com destaque para a CGU, através do Artigo 2º da Instrução Normativa 01/2016, que aponta os controles internos como:

> *Conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade, os seguintes objetivos gerais serão alcançados:*
>
> *a) execução ordenada, ética, econômica, eficiente e eficaz das operações; b) cumprimento das obrigações de accountability; c) cumprimento das leis e regulamentos aplicáveis; e d) salvaguarda dos recursos para evitar perdas, mau uso e danos. O estabelecimento de controles internos no âmbito da gestão pública visa essencialmente aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados, de forma eficaz, eficiente, efetiva e econômica; (...)*

Destarte, compete aos controles internos garantir razoável assertividade quanto ao alcance dos objetivos organizacionais em termos de efetividade e eficiência, com estabelecimento de metas de desempenho e racionalização de recursos, em conformidade com as legislações. Já a

International Organization of Supreme Audit Institutions (2004) conceitua o controle interno como um processo integrado, projetado para lidar com os riscos e fornecer garantia razoável de que, no prosseguimento da missão da entidade, serão alcançados os seguintes objetivos gerais: execução ordenada, ética, econômica, eficiente e eficaz das operações; cumprimento das obrigações de prestação de contas (*accountability*); das leis e regulamentos aplicáveis; e salvaguarda de recursos contra a perda, mau uso e danos.

Para fazer frente a esse desafio, o município do Recife vem investindo de forma expressiva em tecnologia da informação e tem destinado importantes recursos para fortalecimento dessa área estratégica, com destaque para a ampliação dos cargos na área com a criação de uma Unidade do Portal da Transparência e uma Gerência de TI e, também, capacitou cerca de 40 colaboradores em PowerBi e adquiriu licenças a workspaces, que viabilizaram projetos importantes que estão sendo desenvolvidos pela Controladoria-Geral do Recife.

O olhar desses projetos é voltado especialmente para participação cidadã no processo decisório e de fiscalização do município, como preceituam as boas práticas definidas na Lei de Usuário do Serviço Público, das quais destacamos em relação ao Portal da Transparência: a automação de consultas e disponibilização de dados em PowerBi, ferramentas de inclusão e acessibilidade, uso da chatbot e Inteligência Artificial.

Na área de Ouvidoria, destacam-se a criação Conselho de Usuário do Serviço Público de forma totalmente digital e o Projeto Ouvidoria 4.0 que utilizam-se de IA para classificação das manifestações e avaliações dos cidadãos, transformando dados desestruturados em importantes inputs no processo de governança de serviços, a partir da retroalimentação, dessa vez em dados estruturados, que permitem aos gestores estratégicos da capital Pernambucana uma tomada de decisão com base em informações consistentes capturadas diretamente da população e, com isso, efetivando políticas públicas, garantindo sua eficiência e eficácia.

3. A importância do controle interno para a eficácia, eficiência e efetividade das políticas públicas.

Os notáveis avanços apresentados pela legislação na área de controle são evidentes, porém, ainda existem discussões no que se refere a seus conceitos, funções e formas de atuação. As controladorias possuem atribuições distribuídas entre subfunções de controle, que, na perspectiva interna, são chamadas macrofunções (Ribeiro; Bliacheriene; Santana, 2019), por agruparem as atividades em grandes blocos. Apesar de ainda não existir consenso sobre as macrofunções da controladoria, Bona (2021) aponta que o modelo de controladoria pública que predomina no Brasil é composto por até 6 (seis) macrofunções, a saber: 1) controle interno (controladoria); 2) auditoria governamental; 3) corregedoria (atividades correcionais); 4) ouvidoria e acesso à informação; 5) gestão da transparência e integridade; e 6) apoio ao controle externo.

No município de Recife, discorrido neste capítulo, em recente atualização legislativa, considerou 4 (quatro) macrofunções em seu redesenho de competências, são elas: 1) controladoria; 2) auditoria governamental; 3) correição; 4) ouvidoria. Que são definidas da seguinte forma:

> *I - ouvidoria - quando recebe, registra e trata denúncias e manifestações do cidadão, encaminhadas pela Ouvidoria-Geral do Município, sobre os serviços*

> *prestados à sociedade e a adequada aplicação de recursos públicos, visando à melhoria da sua qualidade, eficiência, resolubilidade, tempestividade e equidade;*
>
> *II - controladoria - quando orienta e acompanha a gestão governamental para subsidiar a tomada de decisões a partir da geração de informações, de maneira a garantir a melhoria contínua da qualidade do gasto público;*
>
> *III - auditoria governamental - quando examina a legalidade e legitimidade e avalia os resultados da gestão contábil, financeira, orçamentária, operacional e patrimonial quanto à economicidade, eficiência, eficácia e efetividade, bem como da aplicação de recursos públicos por entidades de direito privado;*
>
> *IV - correição - quando apura os indícios de ilícitos praticados no âmbito da Administração pública, e promove a responsabilização dos envolvidos, por meio da instauração de processos e adoção de procedimentos, visando, inclusive, ao ressarcimento nos casos em que houver dano ao erário.*

Para fins de delimitação e posterior detalhamento de conceitos, utilizaremos a base normativa da Controladoria-Geral do Recife, utilizada tanto em seu Manual de Auditoria Interna como em sua legislação de regência.

Em nível nacional, a CGU é responsável por assistir direta e imediatamente ao Presidente da República. Sua organização administrativa da Controladoria Geral da União (CGU) é composta por 6 (seis) órgãos específicos singulares: Secretaria Federal de Controle Interno, a Ouvidoria-Geral da União, a Corregedoria-Geral da União, a Secretaria Nacional de Acesso à Informação, Secretaria de Integridade Privada e a Secretaria de Integridade Pública.

A definição dessas macrofunções passou por uma série de evoluções ao longo do tempo que, além de serem mudanças conceituais, demonstram o crescimento na importância do papel das controladorias, que antes era considerada uma função mais restrita à análise de contas e ao processamento de registros contábeis e passou a assumir uma função estratégica, contribuindo diretamente na elaboração do planejamento organizacional, subsidiando as gestões com informações estratégicas e orientando suas diretrizes (Assis; Silva; Catapan, 2016).

No que tange às atribuições específicas definidas nas perspectivas macrofunções, Castro (2018), aponta que a função de Auditoria Governamental busca a confirmação da legalidade e da legitimidade dos atos e fatos administrativos, e avaliar os resultados alcançados, conforme os aspectos de eficiência, eficácia e economicidade da gestão orçamentária, financeira, patrimonial, operacional, contábil e finalística. As atribuições trazidas se assemelham diretamente com o modelo adotado pelo Município do Recife, conforme detalhado na Lei 19.082/2023.

Em relação à Ouvidoria, destacamos como uma forma valorosa de interação com sociedade, que servirá como importante ferramenta para aperfeiçoar a governança dos serviços prestados pela administração pública e que, através das manifestações prestadas pelos seus usuários, funcionará como instância de integridade e promoção do controle social, através da participação ativa e efetiva. Um outro aspecto importante dos dados coletados a partir desse canal é a possibilidade

de retroalimentar o planejamento das gestões na construção e aperfeiçoamento das políticas públicas.

Quanto à atuação da correição, destacam-se a defesa da integridade e da normalidade do funcionamento do serviço público, atuando de forma preventiva, detectiva e punitiva, especialmente, neste último caso, em processos administrativos disciplinares e processos administrativos de responsabilização. Como aponta Di Pietro (2000), o poder disciplinar é o que cabe à Administração Pública para apurar infrações e aplicar penalidades aos servidores públicos e demais agentes sujeitos à disciplina administrativa.

Quanto ao Controle Interno, ou Controladoria, as atividades dessa função tem papel estratégico na atuação do Órgão, pois tem o olhar voltado para o aperfeiçoamento dos controles internos, da gestão de riscos, da aplicação correta dos recursos públicos, com o foco na efetividade, eficácia e eficiência da gestão pública.

A atuação articulada e integrada entre suas macrofunções, proporciona aos gestores municipais, nas suas diversas esferas de competências, uma gestão com mais governança, estratégica e íntegra, proporcionando confiabilidade na sua atuação e segurança jurídica nas suas ações.

4. *Accountability* social, participação pública e a transparência.

A necessidade de segurança e desenvolvimento social levou os indivíduos a se organizarem sob a égide de leis comuns, garantidas por um Estado soberano. Nesse processo, conforme argumenta Hobbes (1651), o cidadão abdica de parte de sua liberdade individual, agora regulada pelas normas e leis instituídas pelo Estado.

Com o crescimento das sociedades humanas, a participação direta de todos na administração das comunidades tornou-se impraticável, especialmente em grupos maiores do que tribos ou clãs. Assim, como observado por Bobbio (2009), surge o modelo de participação representativa, no qual indivíduos são escolhidos para atuar em nome do coletivo. No contexto do Estado brasileiro, essa representação ocorre por meio de eleições que designam os ocupantes dos poderes Executivo e Legislativo em suas diferentes esferas.

O mandato conferido aos representantes eleitos, como os deputados federais, é legitimado pelo voto popular, que autoriza esses indivíduos a defender os interesses dos eleitores. Dessa delegação emerge a responsabilidade de prestação de contas, garantindo que as ações dos representantes estejam alinhadas às expectativas e compromissos assumidos durante o processo eleitoral.

Bairral et al. (2015), por sua vez, ampliam a discussão ao incluir gestores e servidores públicos no escopo de controle pela sociedade. Para os autores, esses agentes, ao administrar os recursos públicos em busca do bem comum, também devem ser responsabilizados, dado que sua atuação se fundamenta no contrato social implícito, conforme os princípios delineados por Rousseau (2003).

Assim, o modelo de democracia representativa organiza a sociedade de maneira a delegar a uma parcela específica de indivíduos a tarefa de atuar em nome do coletivo, permitindo que a maioria da população se dedique a outras atividades cotidianas, como trabalho, consumo e vida pessoal. Nesse arranjo, os representantes eleitos – tanto no poder Legislativo, como deputados, senadores e vereadores, como no poder Executivo, com presidente, governadores e prefeitos – são responsáveis por formular políticas públicas, enquanto os servidores públicos efetivos executam, monitoram e avaliam essas políticas, além de prover serviços essenciais à população (PERRUCCI, 2019).

Esse sistema, entretanto, não isenta os representantes e servidores públicos de mecanismos de controle. Os servidores efetivos estão vinculados a normas e princípios que regem a administração pública, com destaque para o princípio da legalidade, que delimita sua atuação ao que está expressamente permitido pela legislação. Já os representantes eleitos enfrentam não apenas o controle da legalidade, mas também a necessidade de alinhar suas ações às demandas sociais. Caso falhem nesse alinhamento ou nas entregas esperadas pela população, correm o risco de não serem reconduzidos a seus cargos em eleições futuras.

Dessa relação entre representantes e sociedade emerge a obrigação de prestar contas, de atender às expectativas coletivas e de respeitar o ordenamento jurídico, configurando o conceito de *accountability*. Esse princípio pressupõe que a sociedade tenha acesso às informações sobre a gestão pública, permitindo-lhe avaliar os resultados das políticas, verificar a legalidade e a relevância dos atos governamentais e participar das instâncias deliberativas. A transparência – compreendida tanto em sua dimensão ativa, por meio da divulgação espontânea de dados pelo governo, quanto na forma passiva, por meio de respostas a solicitações de informação – é um elemento fundamental para assegurar a *accountability* e fortalecer a participação cidadã.

A transparência, compreendida como a divulgação ativa e passiva de informações públicas sobre a execução orçamentária e os resultados de políticas públicas, empodera a sociedade, não apenas a exercer o seu papel de controle social, com a verificação dos resultados de políticas públicas e a conformidade dos gastos governamentais, como também qualifica o debate público e a participação da população no processo de tomada de decisões, na medida em que a sociedade passa a conseguir dialogar após uma redução na assimetria de informações em relação ao governo (PERUZZOTTI; SMULOVITZ, 2002).

Nesse sentido, Giordano da Silva Rossetto (2007) argumenta que a publicidade constitui um princípio estruturante do Estado Democrático de Direito. Na mesma linha, Celso Antônio Bandeira de Mello (2003) complementa ao afirmar que a publicidade decorre da indisponibilidade do interesse público, especialmente pela necessidade de que a sociedade acompanhe e avalie as ações realizadas pelo poder público. Para que tal controle e participação sejam efetivos, é imprescindível que os cidadãos tenham acesso ao conhecimento das iniciativas governamentais, o que demanda transparência e a garantia do direito à informação (MATIAS-PEREIRA, 2010).

Garantido o acesso a informações públicas e a transparência os gastos e resultados da im plementação das políticas públicas, tem-se garantida a *accountability*, termo que não possui uma

tradução direta para o português, mas refere-se à responsabilização e à prestação de contas (CAMPOS, 1990).

Peruzzotti e Smulovitz (2002), com base em O'Donnell (1999), classificam a *accountability* em três tipos: horizontal, vertical e social. A *accountability* horizontal ocorre no âmbito do governo, por meio de mecanismos legais e institucionais, como o controle interno e externo exercido por órgãos como a Controladoria-Geral da União (CGU) e o Tribunal de Contas da União (TCU). A *accountability* vertical, também chamada de eleitoral, manifesta-se pelo controle exercido pela sociedade no momento das eleições, quando os cidadãos podem aprovar ou reprovar, pelo voto, o desempenho de seus representantes. A não reeleição, por exemplo, é uma resposta ao descumprimento de promessas eleitorais (ARBELÁEZ, 2014).

No entanto, O'Donnell (1994), citado por Peruzzotti e Smulovitz (2002), observa que as democracias latino-americanas frequentemente apresentam deficiências na *accountability* vertical. Ele descreve tais sistemas como "Democracias Delegativas", destacando que, nesses contextos, os eleitores geralmente não acompanham as ações de seus representantes eleitos nem cobram a execução dos compromissos assumidos. No caso brasileiro, verifica-se uma forte atuação da *accountability* horizontal, especialmente em virtude da crescente atenção à transparência e ao controle social, ainda que a *accountability* vertical permaneça insuficiente.

A *accountability* social, por sua vez, refere-se aos esforços da sociedade para assegurar a boa gestão dos recursos públicos e a representatividade dos interesses coletivos (PERUZZOTTI; SMULOVITZ, 2002). Essa dimensão destaca a relevância da transparência e do acesso à informação, que são essenciais para viabilizar a participação cidadã e o controle social.

A transparência no setor público abrange tanto a divulgação proativa de informações (transparência ativa) quanto a resposta às solicitações feitas pela sociedade com base em marcos como a Lei de Acesso à Informação (transparência passiva). Além disso, há a transparência proativa, caracterizada pela divulgação espontânea de dados de interesse geral, mesmo sem exigência legal (CGU, 2013; 2015). Tal transparência, por sua vez, permite o controle social e qualifica a participação pública.

A participação pública na elaboração de políticas públicas é um componente essencial para fortalecer a democracia e ampliar a legitimidade das decisões governamentais. Por meio de mecanismos como consultas públicas, audiências, conselhos participativos e plataformas digitais, os cidadãos têm a oportunidade de influenciar diretamente a formulação de políticas que atendam às suas necessidades e expectativas. Essa interação não apenas aumenta a representatividade, mas também possibilita que o poder público incorpore diferentes perspectivas e conhecimentos ao processo decisório, tornando as políticas mais eficazes e alinhadas com a realidade social.

A integração da sociedade civil no ciclo de políticas públicas reforça o princípio da corresponsabilidade entre Estado e cidadão. Ao participar das etapas de diagnóstico, planejamento e avaliação, os indivíduos se tornam agentes ativos na busca por soluções coletivas, ampliando o controle social e a transparência do processo. Essa colaboração também contribui para reduzir assimetrias de poder, permitindo que grupos historicamente marginalizados tenham voz na definição das prioridades governamentais. No entanto, para que essa participação seja

efetiva, é imprescindível que o governo adote estratégias de comunicação acessíveis e promova a capacitação da sociedade para compreender e intervir nas políticas públicas.

Apesar das vantagens, a participação pública enfrenta desafios significativos, como a baixa mobilização social, a falta de recursos técnicos e a desconfiança mútua entre cidadãos e instituições públicas. Muitos cidadãos desconhecem os mecanismos disponíveis ou consideram que sua contribuição não terá impacto real nas decisões. Por outro lado, governos podem tratar a participação como mera formalidade, limitando-se a ouvir demandas sem incorporá-las de maneira substantiva. Superar essas barreiras exige esforços coordenados para fortalecer a educação cívica, ampliar o acesso à informação e criar espaços efetivos e inclusivos de diálogo, assegurando que a participação seja não apenas um direito, mas uma prática consolidada na gestão pública.

5. **A participação pública como indutor de mudanças, promovendo a equidade, a diversidade e a inclusão.**

No contexto governamental, as políticas públicas representam o principal instrumento para transformar as propostas aprovadas pela sociedade em ações concretas. Embora o conceito de políticas públicas varie entre estudiosos, neste trabalho, o termo é entendido como uma ação governamental estruturada e planejada, direcionada a atingir objetivos específicos delineados pelos representantes eleitos. Além de sua legitimidade oriunda do voto, as políticas públicas podem ser enriquecidas pela participação direta da sociedade, por meio de consultas públicas, audiências, conselhos participativos e outras formas de controle e deliberação social. Diferentemente de atividades procedimentais rotineiras, as políticas públicas requerem um planejamento estratégico que articule recursos, metas e indicadores de desempenho, promovendo soluções que reflitam tanto as prioridades do governo quanto as demandas da população. Assim, a participação cidadã direta complementa o mandato representativo, fortalecendo a conexão entre Estado e sociedade e ampliando a efetividade das políticas públicas governamentais.

Os objetos das políticas públicas abrangem uma ampla gama de temas, que vão desde a proteção da flora e da fauna até a defesa dos direitos humanos, incluindo também iniciativas para o aumento da produção industrial e a geração de empregos. A implementação dessas políticas se dá por meio de diferentes instrumentos, variando desde legislações e programas governamentais até parcerias com a sociedade civil e o setor privado, e com distintos níveis de interação com a população. Essa diversidade de instrumentos reflete a complexidade das demandas sociais e a necessidade de abordagens multifacetadas.

Independentemente de seu escopo ou instrumento, as políticas públicas se desenvolvem no âmbito governamental e têm como foco, direto ou indireto, a população brasileira. Essa população, no entanto, é marcada por um alto grau de heterogeneidade, manifestado em aspectos como religião, orientação sexual, classe social, nível educacional e local de moradia. Essa diversidade impõe desafios significativos à formulação e implementação das políticas, uma vez que soluções uniformes podem não ser adequadas para atender às distintas realidades e necessidades que coexistem no país.

Dessa forma, as desigualdades sociais estão intrinsecamente ligadas às políticas públicas, tanto como elementos do contexto em que são concebidas quanto como alvos de suas intervenções. Mesmo quando o objetivo declarado das políticas é a redução de desigualdades, essas mesmas desigualdades podem influenciar seu desenho, execução e impacto, reproduzindo, em alguns casos, as próprias disparidades que buscam combater. Isso ressalta a importância de uma análise criteriosa e de uma abordagem inclusiva na formulação de políticas públicas, que considere as especificidades de diferentes grupos sociais e promova a equidade de forma efetiva.

> *A acumulação ou potencialização simultânea de desigualdades relacionadas com a classe social (ou com o nível socioeconômico), o gênero, a raça ou etnia, o território ou a etapa do ciclo de vida cria um complexo esquema de relações sociais com discriminações múltiplas que se manifestam como desigualdades de autonomia, bem-estar e empoderamento, bem como com marcadas diferenças no exercício de direitos e oportunidades, nas capacidades e no tratamento. 4 (Cepal, 2016, p. 20 – Tradução nossa)*

Long (1999) utiliza o conceito de "interface" para descrever o intrincado emaranhado de relações, interesses e intenções que permeiam a interação entre cidadãos e Estado. Segundo ele, a análise dessas interfaces é essencial para todas as etapas do ciclo de políticas públicas, abrangendo o desenho, a implementação, o monitoramento e a avaliação. Essa abordagem permite compreender como diferentes atores sociais, com perspectivas, recursos e poderes variados, negociam, influenciam e transformam as políticas em contextos específicos.

Além disso, Long destaca que o desenho e a execução das políticas públicas estão intimamente conectados aos discursos dominantes que prevalecem nas interfaces contemporâneas. Esses discursos refletem as dinâmicas de poder, os valores culturais e as prioridades sociais do momento, moldando tanto os objetivos das políticas quanto os meios utilizados para alcançá-los. Assim, as interfaces entre cidadãos e Estado não apenas configuram os processos de governança, mas também revelam os desafios e as oportunidades para a promoção de maior inclusão e equidade.

> *A análise das interfaces nos permite compreender como discursos dominantes são endossados, transformados ou desafiados. Discursos dominantes são caracteristicamente repletos de reificação (geralmente do tipo "naturalística") que pressupõe a existência e significância de certos traços sociais e agrupamentos, pertencentes, por exemplo, a estruturas "comunitárias", "hierárquicas" ou "igualitárias", e de construções culturais de etnicidade, gênero e classe. Tais discursos servem para promover determinados preceitos políticos, culturais e morais, e são comumente mobilizados em disputas sobre significados sociais e recursos estratégicos.5 (Long, 1999 – Tradução nossa)*

A análise proposta por Long reforça a necessidade de um olhar crítico e contextualizado sobre as interações sociais no âmbito das políticas públicas. Identificar as interfaces predominantes e os discursos que as sustentam é fundamental para superar barreiras estruturais, ampliar a participação cidadã e garantir que as políticas sejam mais eficazes, responsivas e alinhadas às demandas da sociedade.

> *Essas formas e mecanismos de discriminação se baseiam também nos estereótipos que hierarquizam e desqualificam determinados grupos sociais em razão de seu sexo, etnia, raça ou cor da pele, orientação sexual, situação socioeconômica ou outra condição presente em diversos âmbitos da vida*

> *social e que, assim como as discriminações, permeiam as próprias instituições e são reproduzidas por estas.6 (Cepal, 2016, p. 20 – Tradução nossa).*

No mesmo sentido:

> *A natureza reprodutora desse processo impõe-nos o desafio de questionar e avaliar em que medida a implementação de políticas públicas não seria também um locus importante de reforço e estabilização de relações sociais marcadas por desigualdades. Até que ponto e por meio de que processos a operação cotidiana dos serviços públicos, a atuação dos agentes executores e as interações entre estes e os destinatários das políticas não estariam contribuindo para uma distribuição desigual de oportunidades e para a continuidade e a consolidação de formas de exclusão já existentes? (Pires, 2017)*

Verifica-se, portanto, que constitui elemento mister de combate à desigualdade, e a luta pela inclusão e pelo respeito à diversidade, a divulgação de informações de interesse social em transparência, a existência de mecanismos de participação pública, e a capacidade da administração pública de absorver as informações e anseios da população a partir dessa participação, com posterior conversão disso em políticas públicas efetivas.

6. A necessidade de um SI estruturado para o melhor funcionamento do controle interno e da participação pública.

Considerando a eficiência e a transparência na administração pública como princípios essenciais para o fortalecimento das democracias contemporâneas, os sistemas de informações estruturados tornam-se imprescindíveis para a operacionalização efetiva de mecanismos de controle interno e de participação cidadã, na medida que organizam as complexas relações entre o governo e a sociedade. Para além disso, a Teoria da Capacidade de Absorção, oriunda do campo de sistemas de informação (SI), oferece um arcabouço teórico útil para compreender como as organizações públicas podem transformar dados oriundos da participação pública em políticas públicas alinhadas com as necessidades da população.

Os sistemas estruturados, ao organizarem e centralizarem dados, garantem que as informações estejam acessíveis para análise e tomadas de decisão. Em um contexto de controle interno, a disponibilidade de dados de alta qualidade possibilita auditorias mais eficazes, identificação de desvios e a geração de relatórios que auxiliam na prevenção de fraudes e corrupção.

As manifestações de ouvidoria e outras formas de interação entre cidadãos e governo oferecem uma relevante fonte de dados sobre as demandas e expectativas da população. Quando organizadas de forma estruturada, essas informações podem embasar decisões mais assertivas, permitindo ao governo identificar problemas, priorizar políticas e ajustar estratégias conforme as necessidades da sociedade.

Para que a administração pública consiga transformar esses inputs em ação é necessário que sua capacidade de absorção seja alta. Tal capacidade reflete-se na habilidade de coletar dados provenientes de ouvidorias e interações sociais, processá-los de maneira eficaz e utilizá-los para

desenvolver políticas públicas e estratégias administrativas alinhadas às necessidades reais da população.

7. A Teoria da Capacidade de Absorção como medidor do nível de aprendizagem organizacional.

Lane e Lubatkin (1998) destacam que o aprendizado organizacional desempenha um papel crucial na ampliação da capacidade de absorção de novas informações. Esse processo envolve não apenas a compreensão, mas também a incorporação de novos conhecimentos, que, ao serem integrados, elevam o repertório da organização. Esse incremento no conhecimento organizacional não apenas potencializa as possibilidades de aprendizagem, mas também prepara a instituição para lidar com desafios futuros, ampliando sua capacidade de inovar e se adaptar a novos contextos.

Nesse sentido, Picoli e Takahashi (2016) argumentam haver recursividade entre capacidade de absorção e aprendizagem organizacional por meio dos mecanismos de integração social, sendo esses mecanismos formais ou informais. Em âmbito formal, temos políticas, procedimentos e sistemas estruturados de compartilhamento de informações entre os diversos atores dentro de uma organização, ao passo que as informais dizem respeito a interações de troca de conhecimento que ocorrem sem uma previsão expressa que a preveja.

No setor público, essa dinâmica é especialmente relevante, pois a incorporação de dados provenientes de interações sociais e ouvidorias exige um esforço contínuo de aprendizado e adaptação. Quando essas informações são processadas e transformadas em conhecimento organizacional, elas servem de base para ações mais eficazes, alinhadas às demandas sociais. Assim, a capacidade de absorção se torna um alicerce para uma administração pública mais responsiva e eficiente, ao conectar o aprendizado à tomada de decisão e à inovação em políticas públicas.

8. As dimensões da Capacidade de Absorção do Sistema de Informações

Entendendo a capacidade de absorção como um conceito fundamental para entender como as organizações identificam, assimilam e aplicam conhecimentos externos para aprimorar suas operações e alcançar vantagem competitiva, torna-se míster o aprofundamento nas classificações teóricas das dimensões e capacidades. Originalmente definida por Cohen e Levinthal (1990) como "a habilidade em reconhecer o valor de novas informações externas, assimilá-las e aplicá-las para fins comerciais", essa capacidade foi posteriormente expandida por Zahra e George (2002), que a dividiram em quatro dimensões agrupadas em capacidades de absorção potencial e realizada.

Capacidade de Absorção Potencial:

Aquisição: Refere-se à habilidade da organização de identificar e adquirir conhecimento externo relevante para suas operações. Isso envolve a busca ativa por informações que possam contribuir para o desenvolvimento organizacional.

Assimilação: Envolve o processo de análise, interpretação e compreensão das informações obtidas externamente. Somente por meio de uma compreensão efetiva é possível internalizar novos conhecimentos.

Capacidade de Absorção Realizada:

Transformação: Diz respeito à habilidade de combinar o conhecimento existente com o novo, avaliando semelhanças e diferenças para gerar modificações que permitam desenvolver e refinar rotinas organizacionais.

Exploração: Consiste em aplicar o conhecimento adquirido, assimilado e transformado para estender ou criar novas competências, resultando em bens, sistemas e processos inovadores.

No contexto da administração municipal, a aplicação do conceito adequa-se a realidade do serviço público da seguinte forma:

A aquisição de informações passa a ocorrer de forma ativa e passiva, ao passo que parte das informações coletadas advém de interlocução com a sociedade civil através dos canais de participação pública. Destarte, conforme evidenciado anteriormente, o desenvolvimento de normativos e práticas de transparência e de acesso à informação que empoderem a sociedade, facilitando e qualificando a participação constituem pré-requisitos para a aquisição de informações relevantes.

De forma complementar, compete ao município a atribuição de, além de receber de forma passiva e estruturada tais informações, buscar ativamente informações externas para incorporá-las ao escopo de aprendizagem institucional.

A dimensão de assimilação encerra a capacidade potencial de absorção ao passo que os integrantes da administração pública interpretam o conjunto de dados reunidos na dimensão anterior. Tem-se, portanto, a análise do conjunto de informações adquiridas pelo município que pode ou não ser convertida em ações efetivas.

A administração pública, então, deverá iniciar a absorção real das informações a partir da transformação das informações recebidas. Durante essa etapa, as informações recebidas serão contrastadas com os projetos já em curso, bem como com todo o arcabouço legal e o conjunto de políticas públicas já existentes, de forma a perceber possíveis pontos de intersecção entre a nova informação e a realidade municipal existente.

Por fim, na dimensão exploração, o governo municipal poderá agregar o conhecimento recém-adquirido às políticas públicas e procedimentos já em curso, de forma a aprimorá-los e aproximá-los dos anseios e necessidades da população.

Compreendendo que a Capacidade de Absorção para entidades públicas possui como objetivo o aprimoramento de suas políticas públicas e procedimentos, incentivando o controle social e a participação pública, e não, como no caso de entidades privadas, objetivando vantagens competitivas, verifica-se que, no restante, a teoria aplica-se perfeitamente à realidade da

administração pública e que uma alta capacidade de absorção de conhecimentos por órgãos públicos se reflete em uma maior *accountability* e em serviços públicos de melhor qualidade.

9. Estudo de Caso: ações da Controladoria-Geral do Recife voltadas à participação social inclusiva e igualitária

Não é de hoje que Recife se destaca como uma das cidades com mais potencial tecnológico do mundo. Em 2021, conforme matéria publicada pelo portal internacional "Rest of Word", Recife, juntamente com Lagos (Nigéria), Bangalor (Índia), Shenzhen (China), Tel Aviv (Israel) e Medellín (Colômbia), se consolidava com uma das seis cidades que lideravam o futuro da indústria de TI no mundo.

Como apontado no portal "Connected Smart Cities", nos últimos anos o município tem direcionado investimentos em soluções tecnológicas para setores essenciais como saúde, educação e mobilidade urbana, incorporando inteligência artificial em diversas fases dos processos públicos. Recife abriga o maior *hub* privado de tecnologia do Brasil, o Porto Digital.

Além disso, a capital Pernambucana também vem se consolidando como uma das cidades mais transparentes dos país, alcançando, somente no ano 2024, 3 excelentes resultados nacionais; o selo Ouro no Levantamento da Transparência Pública da Associação dos Membros dos Tribunais de Contas (Atricon), o nível "Ótimo" no Índice da Transparência e Governança Pública pela ONG Transparência Internacional Brasil, coroando a cidade como a segunda mais transparente do Brasil e o primeiro lugar entre as capitais do nordeste segundo o Índice de Dados Abertos para Cidades aplicado pela Open Knowledge Brasil.

Todos esses reconhecimentos fazem parte de um rol de decisões estratégicas que tem a gestão municipal como preceptora ao alinhar o planejamento às reais necessidades do município e de sua população, estimulando a inovação, a participação e o controle social.

A inovação e a transparência são usadas, pela Prefeitura, como alicerces para construção e fortalecimento de sistemas de informação que beneficiem a gestão e os diversos grupos sociais que fazem parte do Recife. Embora pareça evidente tal premissa, não é raro encontrar sistemas que não dialoguem com a população e que não passem de meros agrupamentos de dados subaproveitados pelos Órgãos.

Para que esses sistemas sejam efetivos dentro da esfera pública, a gestão municipal considera importante a estruturação de dados potencialmente relevantes para a tomada de decisão, com base na aquisição de informação a partir da interação com os usuários das políticas públicas.

Nesse sentido, as plataformas do "Portal da Transparência", do "Conecta Recife", da Gestão de Conhecimento da Ouvidoria - GCON e do Conselho de Usuários do Serviço Públicos "CMUSP"; juntamente com o Sistema Eletrônico do Serviço de Acesso à Informação - e-SAI, e o Sistema de Avaliação do Serviços Públicos "Ouvidoria 4.0", foram concebidos para contribuir com a gestão de conhecimento organizacional, a partir de dados orientados em um grupo de normativos e pela busca ativa e passiva de informações pela população.

O Portal da Transparência, ao disponibilizar de forma ativa informações de toda a gestão municipal, estimula o controle social e garante a transparência pública. Em toda sua dimensão foram desenvolvidas consultas para facilitar a compreensão de seu conteúdo a seus diversos públicos. Ainda, evidenciando sua preocupação com foco na população, em 2024, foi realizado um workshop com segmentos da sociedade civil para a elaboração conjunta de um esboço que dará subsídios para a atualização do Portal da Transparência. Dentre os participantes estavam estudantes, professores e pessoas com necessidades especiais.

Além de disponibilizar as informações, a Prefeitura, por meio da Controladoria-Geral do Município, realiza mensalmente uma análise das informações mais buscadas, bem como das dúvidas recebidas relacionadas ao Portal. Tais informações são analisadas e convertidas em melhorias para o Portal, de forma que acessos e interações com a CGM acerca do Portal da Transparência são transformados em conhecimento e absorvidos na política pública de transparência e participação.

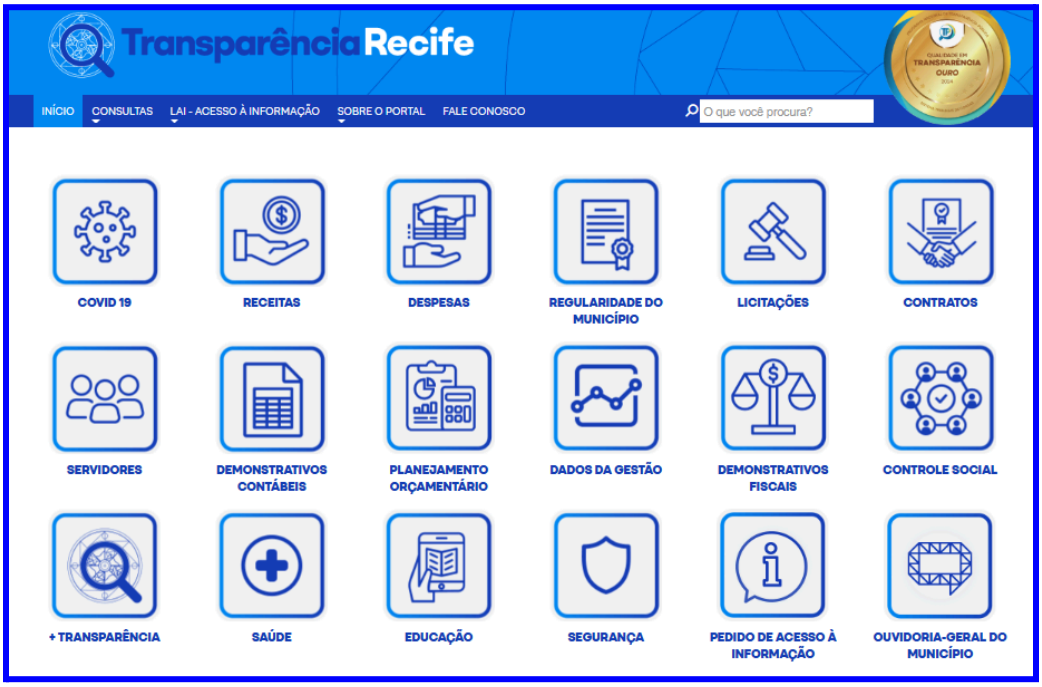


Figura 1.1. Tela inicial do Portal de Transparência do Recife, disponível em ww.transparencia.recife.pe.gov.br

O Portal do Conecta Recife apresenta ativamente em seu site informações dos serviços públicos prestados de forma direta ou indireta pelos órgãos e entidades da administração municipal, em consonância com as exigências estabelecidas na Lei Federal de n° 13.460 de 26 de junho de 2017.

Em seu formato online, a Prefeitura se destaca e se diferencia de outras entidades ao apresentar de forma dinâmica e acessível a todos os usuários que, além de conhecer sobre todos os serviços públicos oferecidos pelo município, podem agendar consultas, vacinas, cuidados com animais, atividades em academias, entre outros serviços. Sendo que a participação social se concretiza

com a realização das pesquisas e comentários dos serviços utilizados, além de mensagens enviadas por meio do aplicativo e pelo whatsapp. Novamente, a análise do uso do sistema e das interações com a sociedade permite à Prefeitura aprimorar constantemente a plataforma, tornando-a mais inclusiva, responsiva e relevante na vida dos munícipes.

Figura 1.2. Tela inicial do Portal de Conecta Recife, disponível em www.conecta.recife.pe.gov.br

A Plataforma de Gestão de Conhecimento da Ouvidoria - GCON e o Sistema Eletrônico do Serviço de Acesso à Informação - e-SAI, se consolidam, hoje, como duas das mais eficazes formas de participação cidadã, e tornando-se um dos principais indicadores para propor políticas e melhorias de serviços prestados pelo município. De forma passiva, em que o cidadão realiza algum tipo de manifestação à prefeitura, é possível observar as pautas e necessidades da comunidade. Por intermédio do GCON, entram no sistema dados relacionados à sugestões, reclamações, solicitações, elogios e denúncias sobre serviços ou agentes públicos. Enquanto que pelo e-SAI são assimilados dados referentes a pedidos de informações públicas em conformidade com a Lei de Acesso à Informação, Lei Federal n. 12.527.

Os Relatórios de Ouvidoria e de Pedidos de Acesso à Informação permitem à CGM sugerir aos órgãos e entidades municipais melhorias e adaptações em suas políticas públicas com base na interação com a população.

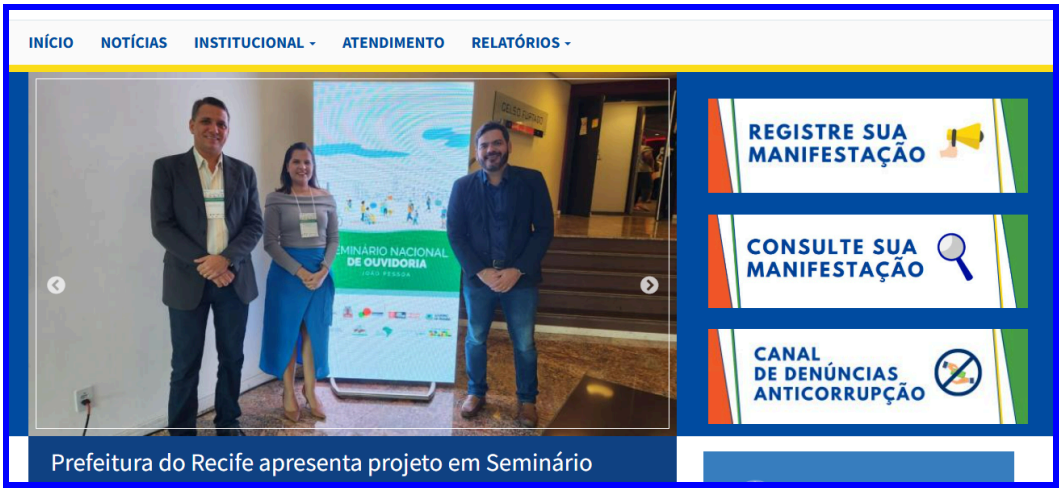


Figura 1.3. Tela inicial do Sistema GCON de Ouvidoria do Município do Recife, disponível em www.ouvidoria.recife.pe.gov.br

Figura 1.4. Tela do Sistema de Pedidos de Acesso à Informação do Município do Recife, disponível em www.transparencia.recife.pe.gov.br

O Conselho Municipal de Usuários de Serviços Públicos, CMUSP, tem o objetivo de facilitar o diálogo entre a Prefeitura e os cidadãos. De forma simples e virtual, os Conselheiros poderão analisar a qualidade dos serviços prestados pela gestão municipal, participar de consultas e sugerir melhorias. O CMUSP difere da avaliação de serviços realizados pelo Portal do Conecta ao estabelecer alguns critérios para a sua participação como: ser maior de 18 anos e se cadastrar voluntariamente na plataforma para avaliar o serviço utilizado. Essa forma de participação cidadã está prevista na Lei 13.460/17.

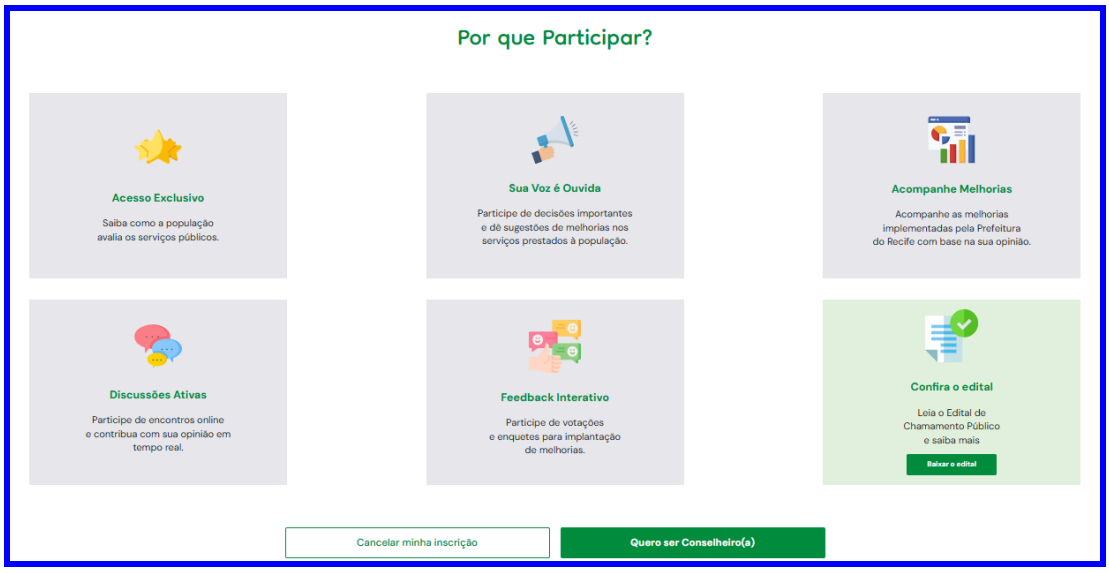


Figura 1.5. Tela do Sistema do Conselho Municipal de Usuários de Serviços Públicos - CMUSP do Município do Recife, disponível em www.cmusp.recife.pe.gov.br

A aquisição e assimilação do conjunto de dados distribuídos em cada uma dessas ferramentas, por si só, já seria capaz de gerar relatórios de gestão altamente qualificados capazes de municiar e estabelecer as diretrizes da política pública municipal com foco nos diversos grupos da sociedade. Em parte, já são realizados relatórios consolidados com informações quantitativas e qualitativas, principalmente com os dados consolidados pelas Plataforma de Ouvidoria e pelo Sistema de Acesso à Informação, no intuito de subsidiar os gestores com as demandas da sociedade.

Muitos dos dados oriundos da Ouvidoria e da Transparência, seja por intermédio do Portal da Transparência ou pela interação nas diversas redes sociais da prefeitura, foram responsáveis por mudanças em tomadas de decisões ao observar os anseios de grupos locais. Um exemplo simples, mas também significativo, foi a manutenção do Campo de Futebol do Onze, em Santo Amaro, bairro do Recife, em formato divergente daquele observado nos demais campos de futebol da cidade. Inicialmente a ideia prevista pelo programa “Gramadão no Recife” era de reformar o campo modificando sua forma torta para a um retângulo perfeito, conforme padrão para quadras de futebol. Porém, devido à grande participação popular, na qual a população local solicitou a manutenção do formato peculiar do campo, que, apesar de inusitado, trazia relevância cultural e regional para seus usuários, foi mantido o seu formato original após as obras de melhorias. O “Campo Torto” foi reformado, respeitando o seu formato único e seguiu sendo símbolo relevante da voz do povo na tomada de decisões públicas.

Figura 1.6. Imagem aérea do "Campo Torto" - Campo de Futebol do Onze, em Santo Amaro, bairro do Recife - imagem original disponível em https://www.tiktok.com/@joaocampos/video/7329501393096641825

Verifica-se, portanto, a aplicação prática de todas as etapas previstas na Teoria de Capacidade de Absorção. Desde a habilidade de identificar e adquirir conhecimento externo, por intermédio dos sistemas e portais da Prefeitura; quanto a capacidade de analisar, interpretar e compreender essas informações, a partir da elaboração de relatórios, onde se verifica a transformação de dados em informações relevantes para a gestão e para a sociedade, com posterior tomada de decisão no âmbito das mais variadas políticas públicas municipais.

Com objetivo de ampliar a capacidade de absorção da Prefeitura, bem como para aprimorar o fluxo de gestão da informação, foi criado um sistema capaz de integrar grande parte dos canais de entrada de qualquer tipo de manifestação do usuário de serviços da Prefeitura do Recife.

Esse sistema, denominado "Ouvidoria 4.0", ao integrar e consolidar os dados das manifestações e avaliações recebidas pelos diversos meios de entrada, se apresenta como uma ferramenta robusta de gerenciamento de informações aos gestores públicos. Cada serviço utilizado e avaliado estará presente nessa grande rede e trará subsídios à aplicação de melhorias cada vez mais pontuais e focadas na qualidade de vida dos diversos grupos do município.

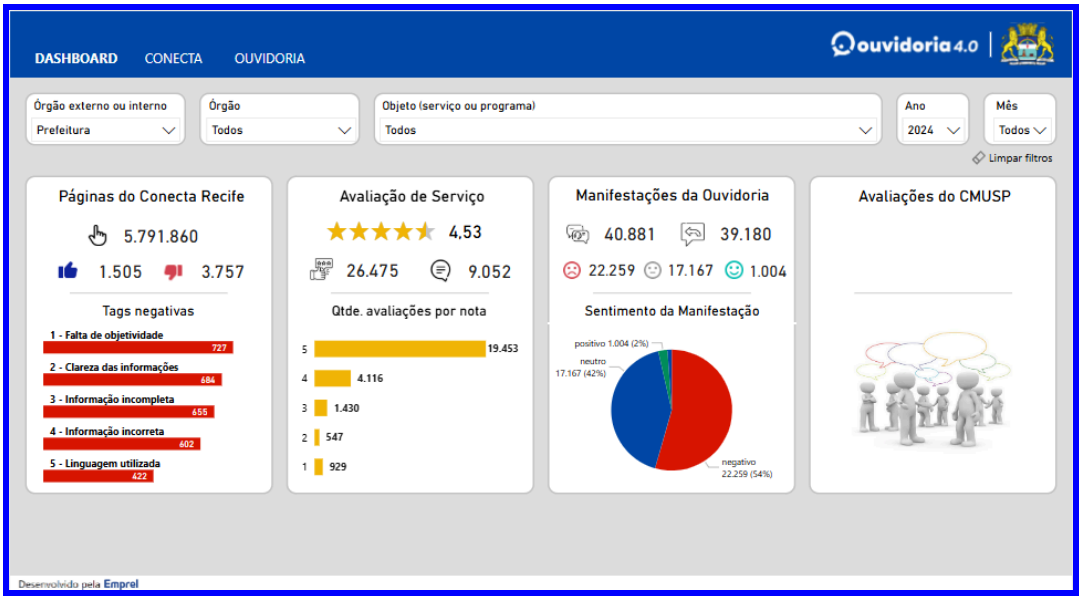


Figura 1.7. Painel da Ouvidoria 4.0

Estarão integrados na "Ouvidoria 4.0", com perfeita comunicação entre os sistemas (interoperabilidade), dados da Ouvidoria-Geral do Município e dos canais de avaliação de Serviços da Prefeitura e do Conselho Municipal de Usuários de Serviços Públicos.

Os dados coletados são processados e orquestrados para possibilitar sua análise e posterior categorização. Com a utilização de Inteligência Artificial os dados dão formas à informações e percepção de sentimentos de cada usuário com base no conteúdo e teor da manifestação. Além disso, são gerados relatórios para os gestores municipais e relatórios individuais para as equipes gestoras dos serviços. Cada órgão e entidade da Prefeitura tem acesso às respectivas informações de sua competência e poderá acompanhar em tempo real informações gerenciais por meio dos painéis BI dinâmicos e relatórios convencionais, se preferir. Em contrapartida à participação cidadã, serão criados mecanismos de feedback aos usuários do serviço público. Os resultados contendo as ações de melhorias nos serviços e nas políticas públicas serão apresentados à população na forma de relatórios e publicados nos sites, portais e redes sociais da Prefeitura. Esse retorno ao cidadão representa um pilar importante para difundir e consolidar esse sistema, tornando o Recife um exemplo de democracia participativa, quando observa as necessidades de todos, incluindo os grupos que muitas vezes são deixados de lado, respeitando a diversidade e a pluralidade. Assim, todos terão voz.

Em resumo, a gestão pública de Recife tem se destacado como exemplo de inovação e transparência, implementando soluções tecnológicas que melhoram a qualidade dos serviços prestados à população. A integração de plataformas e sistemas, como o Portal da Transparência, Conecta Recife, GCON, e-SAI, e o Conselho Municipal de Usuários de Serviços Públicos, facilita o acesso às informações, promove a participação cidadã e aprimora a governança municipal. A constante análise dos dados coletados, a interação com a sociedade e o uso de tecnologias como Inteligência Artificial contribuem para a construção de políticas públicas mais eficientes, adaptadas às necessidades locais. O caso do "Campo Torto" é um exemplo claro de como a voz da comunidade pode impactar diretamente a tomada de decisões. Com o lançamento da Ouvidoria 4.0, Recife reafirma seu compromisso com a democratização da informação e a melhoria contínua dos serviços, consolidando-se como uma referência em participação cidadã e gestão pública inteligente, onde todos os grupos sociais, sem exceção, são ouvidos e respeitados. Dessa forma, a cidade caminha para um futuro mais inclusivo e tecnicamente avançado, refletindo a capacidade da gestão pública em absorver, analisar e aplicar conhecimentos que promovam o bem-estar coletivo.

10. Considerações Finais

A aplicação da Teoria da Capacidade de Absorção no contexto da administração pública, encontra uma correspondência clara nos processos de gestão e inovação que têm sido implementados pela Prefeitura do Recife. A Prefeitura demonstra uma sólida capacidade de absorção de informações externas por meio de suas diversas plataformas, como o Portal da Transparência, Conecta Recife, e a Ouvidoria 4.0, que permitem o recebimento ativo e passivo de dados provenientes da sociedade civil e dos usuários dos serviços públicos. Essa capacidade de adquirir dados, por meio de interações e manifestações da população, é fundamental para o processo de aprendizagem organizacional no setor público.

A assimilação dessas informações ocorre quando a administração municipal analisa e interpreta os dados adquiridos, buscando transformá-los em conhecimento útil. Na administração pública municipal do Recife, isso é evidenciado pelos esforços contínuos de aprimoramento dos sistemas de informação com base nas interações dos cidadãos, como ocorre com a atualização do Portal

da Transparência e a implementação de mudanças nos serviços com base no feedback da população, como o exemplo da manutenção do "Campo Torto". A capacidade de absorção do município é ampliada à medida que se busca compreender e integrar as informações recebidas de forma a torná-las parte das políticas públicas existentes, alinhando-as às necessidades da comunidade.

Na dimensão de transformação, a administração pública de Recife demonstra seu compromisso em transformar as informações coletadas em melhorias concretas. Ao integrar os dados e as análises nos processos de decisão, como exemplificado pela utilização da Ouvidoria 4.0 para criar relatórios de gestão e subsidiar as políticas públicas, a Prefeitura demonstra a capacidade de transformar conhecimento em ação. Esse processo é fundamental para assegurar que as informações adquiridas e assimiladas sejam aplicadas de forma a otimizar os serviços públicos e garantir que as políticas públicas estejam em sintonia com os anseios da população.

Por fim, a exploração do conhecimento adquirido é refletida na aplicação prática das mudanças nos serviços públicos. Ao integrar dados em tempo real e utilizar inteligência artificial para identificar sentimentos e percepções dos cidadãos, a administração municipal está continuamente aprimorando a qualidade dos serviços oferecidos. O uso desses dados para gerar melhorias em áreas como saúde, educação e mobilidade urbana exemplifica a aplicação da dimensão de exploração da Capacidade de Absorção.

Dessa forma, percebe-se a importância do alinhamento da administração pública com os conceitos e práticas de Sistemas de Informação, como no caso da Teoria da Capacidade de Absorção na Prefeitura do Recife, que utiliza o aprendizado organizacional para transformar a gestão pública, promover a inovação e atender melhor às necessidades de seus cidadãos. A partir da absorção, transformação e uso dessas informações para a tomada de decisão, a Prefeitura do Recife favorece o controle social e a participação pública, bem como aprimora instrumentos de controle interno, permitindo a diminuição de desigualdades e uma inclusão equitativa da população no processo decisório.

Referências

ALFONSÍN, R. **Fundamentos de la República Democrática**. Buenos Ayres,

Argentina: Eudeba, 2006.

ARBELÁEZ, Alejandro Cortés. **El concepto de accountability: una mirada desde la Ciencia Política**. Cuadernos de Ciencias Políticas, Colômbia: Universidad EAFIT, Departamento de Gobierno y Ciencias Políticas, v. 6, 2014.

ASSIS, L.; SILVA, C. L.; CATAPAN, A. As funções da controladoria e sua aplicabilidade na administração pública: uma análise da gestão dos órgãos de controle. **Revista Capital Científico - Eletrônica**, v. 14, n. 3, p. 26-43, 2016.

BOBBIO, Norberto. **O futuro da democracia.** Rio de Janeiro: Paz e Terra, 2009.

BOVENS, M. **Analysing and Assessing Accountability: a conceptual framework**. European Law Journal, Chichester, v. 13, n. 4, 2007.

BONA, R. S.; BORBA, J. A.; MIRANDA, R. G. **Barômetro de risco da governança municipal: aplicação de um modelo de avaliação nas prefeituras catarinenses**. Revista da CGU, v. 12, n. 21, p. 45-63, 2020.

BRASIL. **Constituição**. República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988. http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm.

BRASIL. CGU. **Coletânea de Acesso à Informação**. 3ª Edição. Brasília: CGU, 2017.

http://www.cgu.gov.br/Publicacoes/ouvidoria/arquivos/coletanea-acesso-ainformacao .pdf.

BRASIL. **Lei n. 12.527 de 18 de Novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. http://www.planalto.gov.br/ccivil_03/_ato20112014/2011/lei/l12527.htm.

BRASIL. **Lei n. 13.460 de 26 de Junho de 2017**. Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13460.htm.

BRASIL. RECIFE - PE. **Lei n. 17.108/2005.** Dispõe sobre a adequação da estrutura da administração direta e indireta do município do recife às novas diretrizes administrativas e consolida atribuições.

https://leismunicipais.com.br/a/pe/r/recife/lei-ordinaria/2005/1711/17108/lei-ordinaria-n-17108-2005-dispoe-sobre-a-adequacao-da-estrutura-da-administracao-direta-e-indireta-do-municipio-do-recife-as-novas-diretrizes-administrativas-e-consolida-atribui coes.

BRASIL. RECIFE - PE. **Lei n. 19.082, de 28 de junho de 2023**. Dispõe sobre o sistema de controle interno, as competências da Controladoria-Geral do Município -

CGM e dá outras providências. https://leismunicipais.com.br/a/pe/r/recife/lei-ordinaria/2023/1909/19082/lei-ordinaria-n-19082-2023-dispoe-sobre-o-sistema-de-controle-interno-as-competencias-da-controladoria-geral-do-municipio-cgm-e-da-outras-providencias

BRASIL. RECIFE - PE. **Manual de Auditoria Interna.** Versão 1.0. Recife, 2024. https://transparencia.recife.pe.gov.br/uploads/pdf/FINAL_MANUAL%20DE%20AUDITORIA%20INTERNA%20-%20CGM%20RECIFE_dea00927361d20e34bf5d3d5c76174c9.pdf

CADENAS, Carlos. **Beyond Silicon Valley: The six cities building the future of the global tech industry.** By Rest of World Staff. 2021. https://restofworld.org/2021/beyond-silicon-valley/

CARVALHO FILHO, José dos Santos. **Manual de direito administrativo**. 17. ed. Rio de Janeiro: Lumen Juris, 2007.

CASTRO, D. P. **Auditoria, contabilidade e controle interno no setor público**. 7. ed.São Paulo: Atlas, 2018.

D'ALMEIDA, Bernardo. **Recife Como Protagonista No Uso De Inteligência Artificial No Brasil.** Connected Smart Cities. 2024. https://portal.connectedsmartcities.com.br/2024/10/09/recife-como-protagonista-no-uso-de-inteligencia-artificial-no-brasil/

FILGUEIRAS, Fernando. **A Política Pública de Transparência no Brasil: Tecnologias, publicidade e accountability**: In Democracia Digital: Publicidade, instituições e Confronto político. Belo Horizonte: UFMG, 2016.

FILGUEIRAS, Fernando. **Transparency and accountability: principles and rules for the construction of publicity**. Journal of Public Affairs, 2015.

FOX, Jonathan. **The uncertain relationship between transparency and accountability**. Development in Practice, v. 17, n. 4-5, 2007.

GERALDES, Elen; SOUSA, Janara. **As dimensões comunicacionais da Lei de Acesso à Informação Pública.** Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, 2013, http://www.intercom.org.br/papers/nacionais/2013/resumos/R8-1502-1.pdf

LANE, P. J., & LUBATKIN, M. (1998). **Relative absorptive capacity and interorganizational learning.** Strategic Management Journal 19(5), 461-477. doi: 10.1002/(SICI)1097-0266(199805)19:5<461::AID-SMJ953>3.0.CO;2-L

LIMA, Caio; PERRUCCI, Marcelo L.; ARAÚJO, Marco Aurélio; BRAYNER, Rodrigo. **Trilhas de Auditoria de Folha de Pessoal a partir de cruzamento com Dados Abertos Federais: Uma ferramenta desenvolvida a partir da experiência exitosa da CGM-Recife a ser disponibilizada a outros entes subnacionais**. In:

WORKSHOP ON DATA SCIENCE AGAINST CORRUPTION IN THE PUBLIC

SECTOR (DS-COPS) - SIMPÓSIO BRASILEIRO DE BANCO DE DADOS (SBBD), 39. , 2024, Florianópolis/SC. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2024 . p. 212-219. DOI: https://doi.org/10.5753/sbbd_estendido.2024.243625.

PERRUCCI, Marcelo L. (2019), **A LAI é para todos?**, IPEA. Brasília, https://repositorio.cgu.gov.br/bitstream/1/74019/3/Dissertacao_de_Mestrado_marcelo _levy

SMULOVITZ, C.; PERUZZOTTI, E. **Societal Accountability in Latin America**. Journal of Democracy, 2000.

VASSILIADIS, PANOS, and ALKIS SIMITSIS. **Extraction, Transformation, and Loading.** Encyclopedia of Database Systems 10 (2009): 14.

Capítulo 3

MeTA na Prática: Um Método para Avaliação de Tecnologias Inclusivas

MeTA in Practice: A Method for Evaluating Inclusive Technologies

Krissia Menezes e Roberto Pereira

Abstract

Inspired by Universal Design, the Method for Assessing Accessible Educational Technologies (MeTA) was created with the aim of promoting the understanding of accessibility from an inclusive perspective, offering 70 supporting standards and artifacts to equip the evaluation process. Created with a focus on the evaluation of educational technologies, as it is based on Universal Design and well-established W3C accessibility guidelines, MeTA can be used to evaluate other technologies, enabling a comprehensive evaluation. This mini-course aims to introduce MeTA and equip people to conduct evaluations from an inclusive perspective, raising awareness and empowering them with a notion of accessibility that benefits the largest possible number of people.

Resumo

Inspirado no Design Universal, o Método para Avaliação de Tecnologias Educacionais Acessíveis (MeTA) foi criado com o objetivo de promover o entendimento de acessibilidade a partir de uma perspectiva inclusiva, oferecendo 70 normativas e artefatos de apoio para instrumentalizar o processo de avaliação. Criado com foco na avaliação de tecnologias educacionais, por ser fundamentado no Design Universal e em diretrizes bem estabelecidas de acessibilidade do W3C, o MeTA pode ser utilizado para avaliar outras tecnologias, viabilizando uma avaliação abrangente. Este minicurso tem como objetivo apresentar o MeTA e instrumentalizar pessoas a conduzirem avaliações de uma perspectiva inclusiva, sensibilizando-as e capacitando-as para uma noção de acessibilidade que beneficia a maior extensão possível de pessoas.

1.1. Introdução

O Artigo 1º da Declaração Universal dos Direitos Humanos estabelece que todas as pessoas nascem livres e iguais em dignidade e direitos [ONU 1948]. Atrelada a isso, a Constituição Federal Brasileira tem entre seus fundamentos a cidadania e a dignidade da pessoa humana e, em seu artigo 3º, inciso IV, determina que "*promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação*" está entre os objetivos fundamentais da República Federativa do Brasil [BRASIL 2016].

No cenário mundial e brasileiro, existem diversas iniciativas para promover debates e sensibilização sobre a temática da inclusão e a consequente promoção de ambientes mais diversos, equitativos e inclusivos. Adicionalmente, o objetivo 10 da "Agenda 2030 para o Desenvolvimento Sustentável" da ONU (2015) que trata da redução das desigualdades. Este objetivo tem como uma de suas metas o fortalecimento do empoderamento e a promoção da inclusão social, econômica e política de todas as pessoas, sem discriminação por idade, gênero, deficiência, raça, etnia, origem, religião, condição econômica ou qualquer outra característica.

No cenário brasileiro, o Simpósio Brasileiro de Sistemas de Informação (SBSI 2025), que tem como tema "*Inovação com Diversidade, Equidade e Inclusão em Sistemas de Informação*", é uma destas iniciativas. No entanto, ainda é difícil que tecnologias desenvolvidas por instituições públicas e privadas consigam abranger a diversidade de necessidades de acesso de todas as pessoas. Parte deste problema se deve ao fato de que o cenário brasileiro é especialmente desafiador, pois o Brasil é um país de dimensões continentais, com uma ampla variedade de recursos e condições de acesso e infraestrutura. Portanto, projetar e construir espaços, físicos ou digitais, alinhados às demandas inclusivas não é trivial [Menezes 2021; Menezes e Pereira 2022]. É necessário que a acessibilidade seja considerada e avaliada de forma abrangente, que reconheça as diferentes habilidades, necessidades e condições de acesso das pessoas na sua maior extensão possível.

Consequentemente, para promover ambientes que sejam de fato mais diversos, equitativos e inclusivos, precisamos adotar métodos de design e avaliação explicitamente alinhados a esta perspectiva e que favoreçam a redução ou eliminação de barreiras de inclusão. A Organização Mundial da Saúde (OMS) define estas barreiras como *"fatores que dificultam ou impedem a participação plena de indivíduos, especialmente pessoas com deficiências, em atividades sociais, econômicas e políticas. Essas barreiras podem ser de natureza física, social, comunicacional ou atitudinal, e representam obstáculos à igualdade de oportunidades e ao acesso universal a serviços e direitos."* [OMS, 2011].

No entanto, avaliar sistemas de informação para uma ampla diversidade de pessoas não é uma tarefa trivial. Por este motivo propomos o minicurso "MeTA na Prática: Método para Avaliação de Tecnologias Inclusivas", com o objetivo de apresentar uma alternativa para avaliar soluções e considerar uma ampla gama de questões que podem representar barreiras à inclusão. O MeTA é inspirado na Avaliação Heurística de Nielsen, composto de normativas e etapas, com o propósito de avaliar Tecnologias Inclusivas [Menezes 2021]. Com o MeTA, é disponibilizado um conjunto de 70 normativas e materiais de apoio, que incluem um *website*[1] e *templates*, para auxiliar nos processos de avaliação. As próximas seções deste capítulo estão organizadas da

[1] https://krissiamenezes.github.io/meta/ ultimo acesso em 14 de março de 2025

seguinte forma: na Seção 1.2 é apresentado o MeTA, com a explicação de todos os passos para a aplicação do método, exemplos de normativas e explicação dos *templates* de avaliação; finalmente, na Seção 1.3 é proposto um exercício para a utilização do MeTA.

1.2. MeTA

O MeTA foi criado para apoiar a avaliação de acessibilidade em Tecnologias Educacionais e promover o entendimento da acessibilidade a partir de uma perspectiva inclusiva, oferecendo diretrizes para capacitar e instrumentalizar os avaliadores durante o processo de avaliação, com passos flexíveis às necessidades de uso [Menezes e Pereira 2022]. Devido a esse caráter inclusivo e ao fato de o MeTA ser inspirado em uma série de princípios e diretrizes de acessibilidade - como o WCAG 2.0 [W3C Brasil 2014], Leis da Simplicidade e o eMAG [Brasil 2014]- ele pode ser utilizado para avaliar toda uma diversidade de tecnologias e não somente Tecnologias Educacionais. A Figura 1 apresenta os Princípios e Diretrizes que inspiram o MeTA.

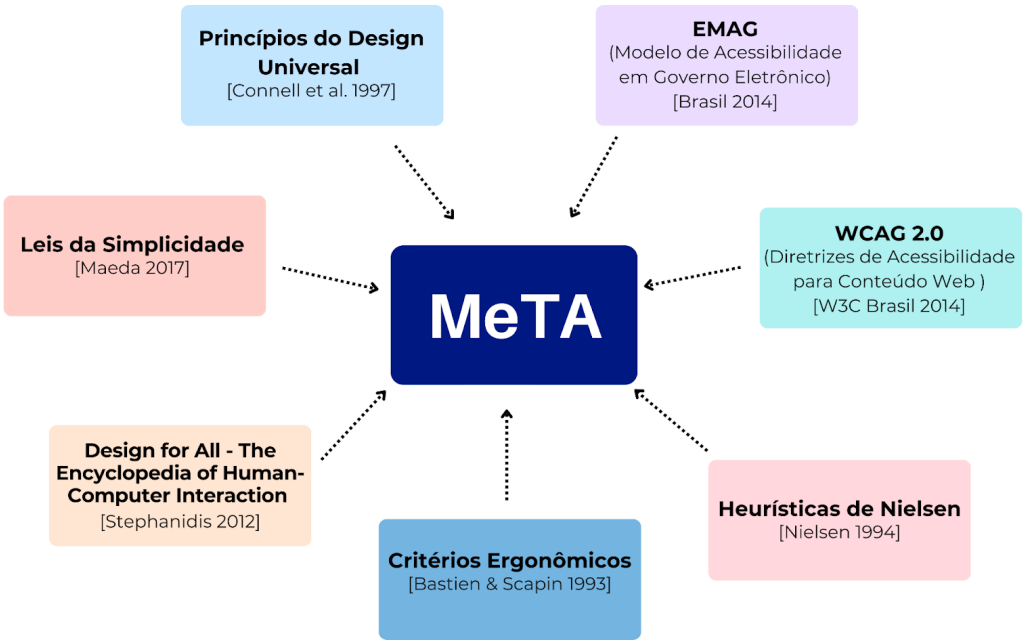


Figura 1. Princípios e Diretrizes que inspiram o MeTA

Vivemos rodeados por tecnologias, que precisamos utilizar para satisfazer uma série de necessidades do nosso cotidiano. Para fazer pagamentos, por exemplo, precisamos utilizar um caixa eletrônico ou um aplicativo de celular. Precisamos utilizar uma urna eletrônica para votar. Também precisamos de um dispositivo móvel ou computador para realizar a declaração de imposto de renda, agendar consultas e diversas outras atividades. Considerando que estas tecnologias possuem componentes físicos e digitais e que possibilitam diferentes formas de interação, avaliações de acessibilidade precisam considerar uma ampla gama de fatores, como as diferentes modalidades de acesso, que podem ser auditivas, motoras, cognitivas e/ou visuais. Como as avaliações nem sempre são conduzidas por especialistas em inclusão ou acessibilidade, promover o entendimento da acessibilidade a partir de uma perspectiva inclusiva, oferecendo diretrizes e normativas para capacitar e instrumentalizar os avaliadores durante o processo de aplicação também é objetivo do MeTA. Este método já foi avaliado por profissionais com

experiência em Interação Humano-Computador, estudantes de graduação e pós-graduação [Menezes 2021; Menezes e Pereira 2022] e para avaliar diferentes tecnologias, incluindo um protótipo de Caixa Eletrônico e a plataforma MEC de Recursos Educacionais Digitais [Menezes et al. 2023; Menezes et al. 2024], nos quais foi possível constatar a utilidade, importância e facilidade de uso para avaliação de acessibilidade em tecnologias, e implementar melhorias para facilitar sua utilização, como as diferentes formas de organização das normativas e a disponibilização do MeTA, com todo o passo a passo e artefatos de avaliação no *website* do MeTA.

As normativas e sua estrutura padrão foram propostas por um grupo de especialistas em acessibilidade e educação. O conteúdo com explicações e exemplos de cada normativa foi desenvolvido por Menezes (2021) tendo como base os Princípios do Design Universal [Connell et al. 1997], Modelo de Acessibilidade em Governo Eletrônico (EMAG) [Brasil 2014], Diretrizes de Acessibilidade para Conteúdo Web (WCAG 2.0) [W3C Brasil 2014], Heurísticas de Nielsen [Nielsen, 1994], os Critérios Ergonômicos [Bastien & Scapin 1993], o Design for All - The Encyclopedia of Human-Computer Interaction [Stephanidis 2012] e As Leis da Simplicidade [Maeda 2017]. A Figura 2 mostra esses princípios com a quantidade de normativas associadas e temas centrais que as representam.

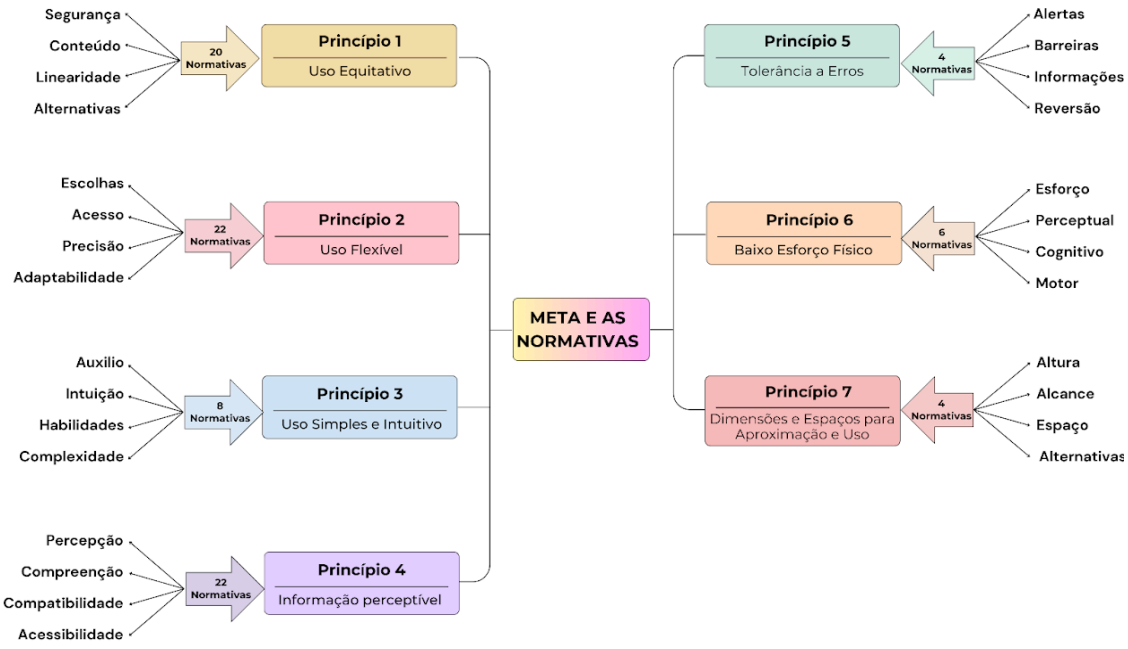


Figura 2. Princípios, quantidade de normativas e temas centrais do MeTA

A abrangência do MeTA também pode facilitar processos de avaliação quando se leva em consideração que os mesmos avaliadores podem precisar avaliar diferentes tipos de tecnologias e, com o MeTA, não precisam aprender diferentes métodos para avaliar diferentes tecnologias. O MeTA visa apoiar a aplicação dos 7 Princípios do Design Universal, que possuem 30 diretrizes para facilitar o entendimento de cada princípio [Connell et al. 1997], disponibilizando normativas com explicações e exemplos para facilitar o entendimento do que e como deve ser avaliado para

cada uma destas diretrizes. Relacionado a cada Princípio do Design Universal existem as Diretrizes e, para cada Diretriz, existem as Normativas.

A Figura 3 ilustra o esquema geral de organização das normativas, no qual cada Normativa apresenta um "Por quê?", com um ou mais contextos de uso em que são exemplificadas situações nas quais ocorrem barreiras no uso de uma Tecnologia, para facilitar o sentimento de empatia nos avaliadores e a identificação de barreiras à inclusão. Também é apresentado um "Como?", que é uma indicação de como o avaliador poderá encontrar esta barreira. Por fim, são apresentados os "Resultados esperados:", que é o comportamento que se espera da Tecnologia para que não exista a barreira apresentada no "Contexto de Uso".

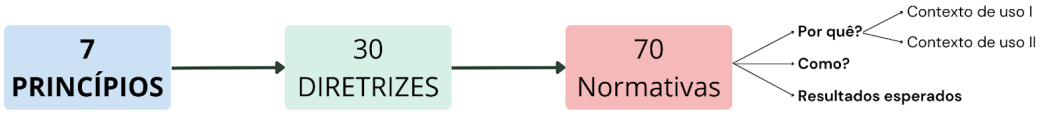


Figura 3. Esquema geral de organização das normativas

As normativas ainda podem ser classificadas e filtradas de três outras formas de acordo com: 1. o tipo de Tecnologia, 2. a Modalidade de Acesso, e 3. os Princípios do WCAG.

1. Tipo de Tecnologia

    a. *Físico*: analisa as funcionalidades de Tecnologias que possuem uma estrutura material tangível e desempenham funções sem a necessidade de interação com dispositivos digitais, eletrônicos ou Internet. Ex: Jogo de Tabuleiro, livros impressos e ferramentas manuais.
    b. *Digital*: analisa as funcionalidades de tecnologias que funcionam por meio de componentes eletrônicos e são acessadas por meio de dispositivos digitais. Ex: aplicativos, sites, vídeos e plataformas online.

2. Modalidade de Acesso

    a. *Visual*: analisa as funcionalidades da tecnologia que satisfazem as necessidades de pessoas com visão limitada ou sem visão para perceber, compreender e operar a referida tecnologia.
    b. *Auditiva*: diante da restrição do uso da modalidade auditiva, as possibilidades de acesso à informação baseiam-se no uso da Libras como língua de acesso ou no uso do Português como língua de acesso, na modalidade escrita.
    c. *Motora*: analisa as funcionalidades da tecnologia que satisfazem as necessidades de pessoas com restrição motora para operar a referida tecnologia.
    d. *Cognitiva*: analisa as funcionalidades da tecnologia que satisfazem as necessidades de pessoas com formas alternativas de perceber, compreender e operar a referida tecnologia.

3. Princípios do WCAG

    a. *Perceptível*: as informações e os componentes da tecnologia devem estar disponíveis de maneiras que as pessoas possam percebê-las.
    b. *Operável*: os componentes da tecnologia e a navegação devem ser operáveis.

c. *Compreensível*: a informação e a operação da tecnologia têm de ser compreensíveis.
d. *Robusto*: o conteúdo da tecnologia deve ser robusto o suficiente para poder ser interpretado de forma concisa por diversos agentes do usuário, incluindo recursos de tecnologia assistiva.

A Figura 4 sintetiza as diferentes classificações das normativas e, a seguir, é apresentado um exemplo de diretriz e normativa para cada princípio do Design Universal, com suas respectivas classificações. O conteúdo completo das normativas e diferentes classificações pode ser acessado no *website* do MeTA.

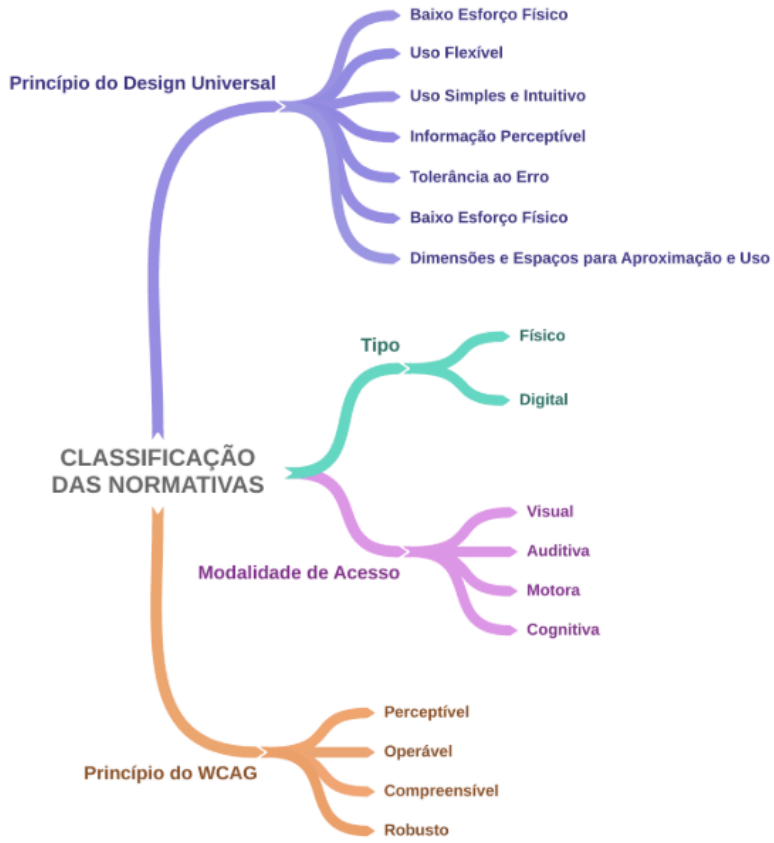


Figura 4. Classificação das normativas

Princípio 1: Uso Equitativo

Diretriz 1a. Fornecer os mesmos meios para todos os usuários: idêntico quando possível, equivalente quando não for.

Normativa 1a.7 Apresentar formato alternativo de áudio ou tátil para feedback visual das operações do usuário na interface.

Por quê?

Exemplo de uso: uma pessoa cega usando um computador para preencher um formulário de inscrição. Barreira: ao enviar o formulário, ele não enviar por ter um

erro de preenchimento e a tecnologia não informar em qual campo do formulário ocorreu o erro, apenas marcar os campos em vermelho.

Como?

Verificar se a tecnologia oferece feedback em formato alternativo sonoro ou tátil perceptível ao usuário.

Resultados esperados:

1. Apresenta formato alternativo sonoro ou tátil de feedbacks visuais de operações da interface;
2. O feedback apresentado contém uma descrição textual do seu conteúdo ou sinais sonoros/táteis diferentes para cada tipo de retorno da operação do usuário.

Classificações: Uso Equitativo, Digital, Cognitiva, Operável, Perceptível, Compreensível.

Princípio 2: Uso Flexível

Diretriz 2b. Acomodar acesso e uso por destros e canhotos.

Normativa 2b1. Possibilitar uso por pessoas destras e canhotas (permanentes ou temporárias).

Por quê?

Exemplo de uso: uma pessoa canhota usando um software para selecionar figuras geométricas e emparelhar a utensílios que possuam forma correspondente. Barreira: o software não é compatível com a alteração da configuração do *mouse* para uso por pessoa canhota.

Como?

Utilizando um *mouse* convencional ou acionador especial, verificar se o software permite configurar seu uso por pessoa destra ou canhota.

Resultados esperados:

1. A tecnologia deve ser compatível com o uso direto ou com recurso de tecnologia assistiva por pessoas destras ou canhotas.

Classificações: Uso Flexível, Físico, Digital, Motora, Operável.

Princípio 3: Uso Simples e Intuitivo

Diretriz 3d. Organizar informação de maneira consistente de acordo com sua importância.

Normativa 3d.1 Possibilitar que o primeiro atalho da tecnologia leve à página de informações sobre acessibilidade.

Por quê?

Exemplo de uso: uma pessoa cega usando um computador com leitor de telas para acessar um site para inscrição em concurso público. Barreira: ao teclar tab, o

primeiro link encontrado não é o de informações de acessibilidade e a pessoa não saber como navegar.

Como?

Utilizando a tecla tab ao entrar na página, verificar se o primeiro link acionado é o de informações sobre acessibilidade.

Resultados esperados:

1. O primeiro link leva à página com informações sobre acessibilidade.

Classificações: Uso Simples e Intuitivo, Digital, Visual, Operável, Perceptível.

Princípio 4: Informação Perceptível

Diretriz 4e. Fornecer compatibilidade com uma variedade de técnicas ou dispositivos usados por pessoas com limitações sensoriais.

Normativa 4e.1 Possibilitar o uso de periféricos de tecnologia assistiva.

Por quê?

Exemplo de uso: uma pessoa usando um aplicativo de computador para realizar a declaração de imposto de renda. Barreira: não é possível utilizar o aplicativo com mouse adaptado.

Como?

Verificar se a tecnologia possibilita o uso de periféricos de tecnologia assistiva (ex: mouses, teclados, lupas).

Resultados esperados:

1. Possibilita a utilização de periféricos com tecnologia assistiva;
2. Fornece compatibilidade de periféricos e acessórios (mouse, teclado, lupas, decodificadores cerebrais) com tecnologia assistiva.

Classificações: Informação Perceptível, Físico, Digital, Visual, Auditiva, Motora, Cognitiva, Operável, Robusto, Compreensível.

Princípio 5: Tolerância a Erros

Diretriz 5c. Fornecer recursos seguros contra falhas.

Normativa 5c.1 Possibilitar que uma ação seja revertida.

Por quê?

Exemplo de uso: uma pessoa com baixo controle motor, usando um recurso de completar em um aplicativo de celular. Barreira: a pessoa pulsar teclas/funções indevidamente e não haver a possibilidade de voltar ou corrigir.

Como?

Verificar se a tecnologia possibilita retornar após uma tecla e/ou função ser pulsada.

Resultados esperados:

1. Possibilidade de correção/ retorno, antes de efetivar a ação, ao clicar ou pressionar uma tecla;
2. Possibilidade de correção/ retorno, antes de efetivar a ação, ao pulsar uma função.

Classificações: Tolerância ao Erro, Físico, Digital, Motora, Operável, Cognitiva.

Princípio 6: Baixo Esforço Físico

6d.2 Exigir baixo esforço cognitivo.

Normativa 5c.1 Possibilitar que uma ação seja revertida.

Por quê?

Exemplo de uso: uma pessoa usando um aplicativo de quiz. Barreira: o quiz possuir 50 questões e não poder ser pausado sem perder o progresso.

Como?

Verificar se as atividades fornecidas pela tecnologia exigem um gasto razoável de tempo e raciocínio.

Resultados esperados:

1. Disponibiliza atividades separadas em fases ou etapas de forma que sejam necessárias poucas pausas;
2. Disponibiliza atividades que exijam gasto razoável de raciocínio e tempo.

Classificações: Baixo Esforço Físico, Digital, Cognitiva, Compreensível, Robusto.

Princípio 7: Dimensões e espaços para aproximação e uso

7a. Fornecer uma linha de visão direta a elementos importantes para qualquer usuário sentado ou em pé.

7a.1 Disponibilizar a Tecnologia Educacional na altura do alcance do olhar das pessoas que irão utilizá-la.

Por quê?

Exemplo de uso: uma pessoa cadeirante utilizando um tabuleiro com peças para estudar operações matemáticas. Barreira: o tabuleiro ser fixo em uma mesa alta e a pessoa não conseguir ter uma boa visualização, havendo dificuldade para identificar as peças ou mesmo as características do tabuleiro e realizar as operações.

Como?

Verificar se a tecnologia e todos os seus componentes podem ser posicionados para ficarem dispostos na linha de visão direta das pessoas.

Resultados esperados:

1. Pode ser visualizada e manipulada por pessoas que estão em pé;
2. Pode ser visualizada e manipulada por pessoas que estão sentadas;
3. Pode ser visualizada e manipulada por pessoas que estão deitadas;

Classificações: Dimensões e Espaços para Aproximação e Uso, Físico, Digital, Motora, Operável, Compreensível, Perceptível.

A lista completa de normativas está disponível no *website* do MeTA. O conteúdo e a classificação das normativas não é definitivo e imutável. Evoluções das tecnologias interativas ou especificidades de contextos de aplicação produzem tanto insumos quanto demandas, incluindo novos exemplos ou novas normativas para que o método seja o mais abrangente e, ao mesmo tempo, específico possível.

1.2.1 Aplicação do MeTA

O MeTA é composto de três fases, conforme ilustrado na Figura 5 que apresenta o resumo das fases do MeTA e suas respectivas atividades: 1. Organização do Grupo de Avaliadores, 2. Avaliação Individual, e 3. Consolidação das Avaliações, evidenciando a entrega final de cada fase.

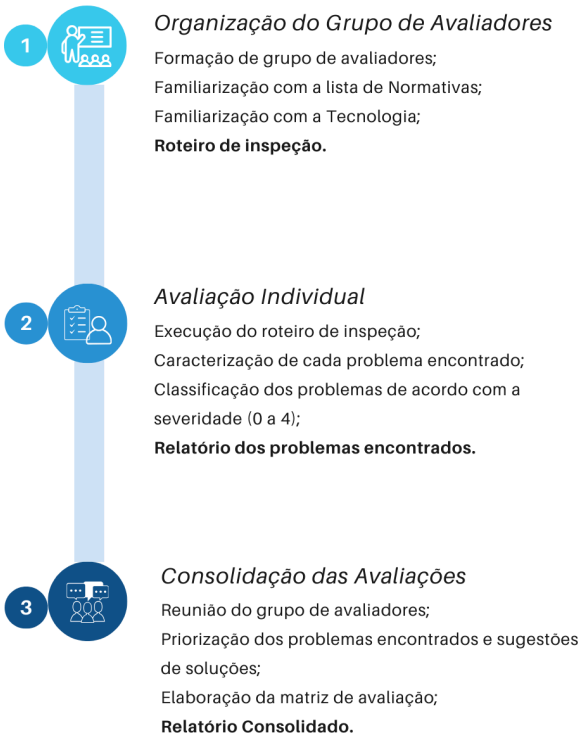


Figura 5. Fases do MeTA

1.2.1.1 Organização do Grupo de Avaliadores

Nesta fase, deve ser formado um grupo de três a cinco avaliadores, pois de acordo com estudos realizados por Nielsen (1994) este é um número adequado para uma boa relação custo-benefício em avaliações com especialistas. Embora o público-alvo do MeTA não seja necessariamente especialistas em avaliação de acessibilidade, a recomendação de 3-5 avaliadores é válida, especialmente devido à dificuldade de se realizar a fase de consolidação com um número muito grande de avaliadores.

Após formado, o grupo de avaliadores deve se familiarizar com as normativas e com a tecnologia a ser avaliada. Também se recomenda que, se possível, seja dado aos avaliadores um roteiro contendo sugestões de atividades que devem ser executadas com a tecnologia durante as inspeções.

1.2.1.2 Avaliação Individual

Nesta fase, o avaliador deve explorar a tecnologia a ser inspecionada a partir da lista de normativas, procurando violações dentro de cada normativa, focando em necessidades específicas que as pessoas possam ter, para conseguir encontrar o máximo de problemas ou barreiras. Após a execução das inspeções, deve ser elaborado um relatório individual dos problemas encontrados, que devem ser classificados de acordo com um grau de severidade, cuja mensuração utiliza uma escala de 0 a 4, na qual:

0: representa um problema estético, não pode ser considerado uma barreira,
1: representa uma barreira que pode ser contornada sem necessidade de apoio,
2: uma barreira que pode ser superada com o uso de tecnologia assistiva,
3: uma barreira que causa grande dificuldade para a utilização da tecnologia,
4: problema ou barreira grave que impede a utilização da tecnologia.

O ideal para um processo de avaliação com o MeTA é que haja pelo menos um especialista em avaliações de acessibilidade para organizar o grupo de avaliadores e coordenar a consolidação das avaliações. No entanto, o objetivo do método é que qualquer pessoa interessada em fazer avaliações de acessibilidade consiga utilizar o MeTA, e que possa aprender sobre acessibilidade e soluções mais inclusivas enquanto o aplica. Para casos em que uma única pessoa avaliadora precise realizar avaliações de acessibilidade, recomendamos seguir um processo simplificado de avaliação, conforme os passos estabelecidos no item 1. Organização do Grupo de Avaliadores, e 2. Avaliação Individual e, ao final, revise os problemas encontrados e, caso necessário, faça alterações no seu relatório, pois não é possível aplicar todos os passos do método com apenas um avaliador.

Para facilitar a elaboração do relatório individual dos problemas encontrados, o MeTA disponibiliza o *Template* de Avaliação individual, que é apresentado na subseção 1.3.2.

1.2.1.3 Avaliação Consolidada

Nesta fase, o grupo de avaliadores deve se reunir para discutir os problemas encontrados em cada avaliação individual. O grupo de avaliadores também deve discutir e chegar a um consenso sobre

a relevância de cada problema encontrado, as normativas violadas, o grau de severidade e respectivas sugestões de adequações, consolidando tudo em um único relatório, que deve conter:

a) o subconjunto de normativas utilizado,
b) lista de problemas encontrados, indicando para cada um:
    i) o local onde ocorre,
    ii) descrição,
    iii) normativa violada,
    iv) severidade do problema, e
    v) recomendações de soluções.

Os problemas encontrados também devem ser priorizados a partir da lista consolidada e de seus respectivos níveis de severidade. Se não houver consenso sobre a relevância de um problema entre os avaliadores, todos os problemas devem ser levados em consideração. Para facilitar a elaboração deste relatório individual dos problemas encontrados, o MeTA disponibiliza o *Template* de Avaliação Consolidada, que é apresentado na Subseção 1.3.3.

Uma matriz de avaliação que relaciona avaliadores versus problemas (de diferentes graus de dificuldade) encontrados pode ser elaborada após a consolidação. Nela é possível observar quais problemas foram encontrados por quais avaliadores. O MeTA também disponibiliza um *template* para facilitar a elaboração da Matriz de avaliação, que é apresentada na Subseção 1.3.4.

1.3 Artefatos de Avaliação

O MeTA disponibiliza uma série de artefatos para auxiliar o processo de avaliação de uma tecnologia. Todos estes artefatos podem ser encontrados no *website* do MeTA (Figura 6), que foi desenvolvido obedecendo os padrões de acessibilidade *Web* estabelecidos pelo W3C. O *website* também possui uma barra de acessibilidade, com opções de atalhos para o conteúdo principal, menu e rodapé. Há, ainda, a opção de alterar o tamanho da fonte e o contraste da página.

Figura 6. *Website* do MeTA

Os artefatos e conteúdos a seguir também podem ser encontradas no *website* do MeTA: Informações sobre a origem, o propósito e o passo a passo completo para a utilização do MeTA, incluindo a explicação de cada fase do método e dos diferentes níveis de severidade; a lista completa de normativas, com filtros para as diferentes classificações (Princípios do Design Universal, Tipo de Tecnologia, Modalidade de Acesso e Princípios do WCAG 2.0). Nesta seção do *website* ainda é possível imprimir a lista completa de normativas ou uma lista filtrada de acordo com uma das classificações. Também é disponibilizado um conjunto de *templates*[2] para facilitar a identificação dos problemas e a entrega final das avaliações. Há um link, no *website*, no qual os *templates* são disponibilizados em um documento compartilhado contendo oito abas detalhadas na sequência: na primeira aba há o 1. Guia Rápido de Avaliação com o MeTA, as abas de dois a seis são destinadas às 2. *Templates* de Avaliação Individual, a sétima aba apresenta a 3. *Template* de Avaliação Consolidada, a oitava e última aba apresenta a 4. Matriz de avaliação. Para utilizar os *templates*, o time de avaliadores deve fazer uma cópia e editar conforme os seus dados.

1.3.1 Guia Rápido de Avaliação com o MeTA

Apresenta um passo a passo com instruções para utilização do MeTA e campos para o preenchimento de informações referentes à avaliação, conforme a Figura 7.

Figura 7. Informações Referentes à Avaliação

Avaliadores	
Tecnologia Avaliada	
Data de início da avaliação	
Data de término da avaliação	
Tempo total gasto na avaliação (em horas)	
Observações	

1.3.2 Template de Avaliação Individual

Este documento contém 11 campos para auxiliar o avaliador no processo de avaliação individual e que devem ser preenchidos com os itens detalhados na sequência.

- Nome do avaliador: identificação da pessoa responsável pela avaliação para que seja possível identificar o avaliador responsável por identificar os problemas / barreiras;
- Data da avaliação: identificação da data em que ocorreu a avaliação para que fique documentada e possa ser consultada futuramente;
- Hora de início e fim da avaliação: identificação do horário em que o avaliador iniciou e terminou a avaliação para que seja contabilizado o total de horas gasto por cada avaliador;
- Para facilitar a identificação e reprodução de cada problema, deve ser informado:

[2] https://docs.google.com/spreadsheets/d/14smK3GZWWk9ZGDC4onBRGxKJFoxPbVo3F5bWLiISLPg/ último acesso em 14 de março de 2025

    - identificador,
    - descrição,
    - local onde ocorre,
    - link para arquivo ou imagem que descreva o problema (se houver),
    - normativa(s) violada(s);
- Para facilitar a consolidação das avaliações, também devem ser informados:
    - o grau de severidade,
    - sugestões de melhorias,
    - comentários e observações do avaliador.

1.3.3 Template de Avaliação Consolidada

Este documento contém 15 campos para auxiliar os avaliadores no processo de consolidação das avaliações e que devem ser preenchidos com os itens detalhados na sequência.

- Data da avaliação: identificação da data em que ocorreu a avaliação para que fique documentada e possa ser consultada futuramente;
- Hora de início e fim da avaliação: identificação do horário em que o avaliador iniciou e terminou a avaliação para que seja contabilizado o total de horas gasto por cada avaliador;
- Para facilitar a identificação e reprodução de cada problema, deve ser informado:
    - identificador,
    - descrição,
    - local onde ocorre;
- Para informar o consenso dos avaliadores sobre os problemas consolidados:
    - normativa(s) violada(s);
    - grau de severidade definido por cada avaliador;
    - grau de severidade final, sugestões de melhorias,
    - comentários e observações dos avaliadores;

1.3.4 Matriz de Avaliação

Esta matriz pode ser elaborada de duas formas: a primeira forma é utilizar uma cópia dos *templates* disponibilizados pelo MeTA, o *template* da Matriz de Avaliação preencherá automaticamente os dados inseridos no *Template* de Avaliação Consolidada. A segunda forma é disponibilizar manualmente as informações referentes aos problemas consolidados. Para cada problema deve ser informado o ID, a descrição, o grau de severidade definido por cada avaliador e a severidade final. A Tabela 1 apresenta um fragmento de uma de Matriz de avaliação preenchida.

Tabela 1. Fragmento de uma Matriz de Avaliação

ID	Problema	Avaliadores e Severidades			Severidade Final
		Avaliador(a) 1	Avaliador(a) 2	Avaliador(a) 3	
1	O vídeo de apresentação do site, não possui intérprete de libras.	2	3	4	3
2	Não há opção para alteração do contraste.	2	3	3	3

3	Não há informações dispostas em Libras, apenas no formato texto.	4	4	4	4

1.4 Exemplo de Aplicação do MeTA

O MeTA já foi utilizado em diversos contextos e para avaliar diferentes sistemas de informação. Nesta seção apresentamos uma atividade de avaliação com o MeTA, com o objetivo de explicar um caso real de avaliação utilizando o método e facilitar o seu entendimento e aplicação. Nesta atividade foi avaliado um Simulador de Saque em Banco 24 horas que já havia sido utilizado em um contexto de uso real da Educação de Jovens e Adultos de uma escola pública da cidade de Curitiba e que precisaria ser acessível para a maior diversidade possível de pessoas. Este simulador foi desenvolvido de forma construtiva, no contexto do projeto de pesquisa aprovado pelo Comitê de Ética em Pesquisa da Universidade Federal do Paraná, parecer de nº 20184842, por pesquisadores que já conheciam a realidade dos estudantes. A Figura 8 apresenta a estrutura do simulador, composta de uma caixa de papelão com compartimentos para inserir o cartão de crédito, retirar recibo e dinheiro, um tablet e cartões personalizados.

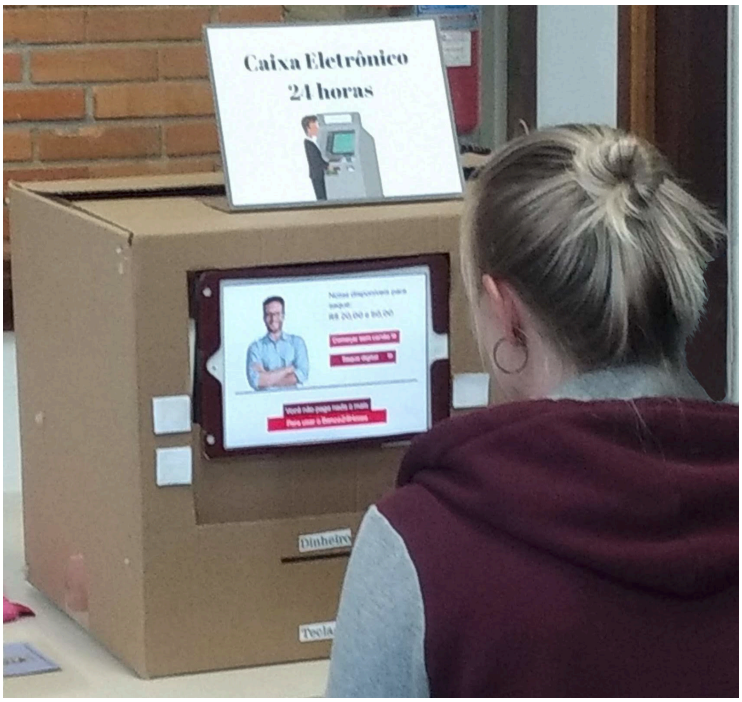


Figura 8. Simulador de Saque em Banco 24 horas

O estudo envolveu um grupo de 10 avaliadores com experiência em avaliação de interfaces, selecionados por conveniência por serem todos estudantes do Programa de Pós-graduação em Informática da Universidade Federal do Paraná, pesquisando na área de Interação Humano-Computador (IHC). A Tabela 2 apresenta as características dos avaliadores que participaram do experimento.

Tabela 2. Características dos Avaliadores

Avaliador	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
Nível de instrução (em andamento)	Mestrado	Doutorado	Mestrado	Doutorado	Mestrado	Mestrado	Doutorado	Doutorado	Mestrado	Mestrado
Gênero	Masculino	Feminino	Masculino	Feminino	Masculino	Masculino	Feminino	Masculino	Masculino	Feminino
Experiência com avaliação de acessibilidade	Média	Média	Média	Média	Baixa	Média	Média	Baixa	Alta	Média

1.4.1 Materiais e Métodos

Os avaliadores assinaram o Termo de Consentimento Livre e Esclarecido (TCLE) para assegurar a confidencialidade e privacidade dos dados coletados. Os materiais utilizados para apoiar a avaliação foram: TCLE; Apresentação de *slides* sobre o MeTA; Simulador de Saque em Banco 24 horas; Site do MeTA; Template de Avaliação Individual, Template de Avaliação Consolidada e Matriz de Avaliação. O estudo de avaliação foi conduzido seguindo as 3 fases estabelecidas pelo MeTA: 1. Organização do Grupo de Avaliadores, 2. Avaliação Individual, e 3. Avaliação Consolidada.

1. Organização do Grupo de Avaliadores (30 minutos): A primeira autora atuou como organizadora durante o encontro e foi responsável por apresentar as informações da avaliação, o MeTA, e o sistema de informação a ser avaliado (o Simulador de Saque em Banco 24 horas). Após as apresentações, os avaliadores foram informados de que o simulador já havia sido utilizado em um contexto de uso real da Educação de Jovens e Adultos de uma escola pública da cidade de Curitiba, e que precisariam garantir que a tecnologia possa ser utilizada pela maior diversidade possível de pessoas. A Figura 9 apresenta a sequência de telas e operações que podem ser realizadas no simulador.

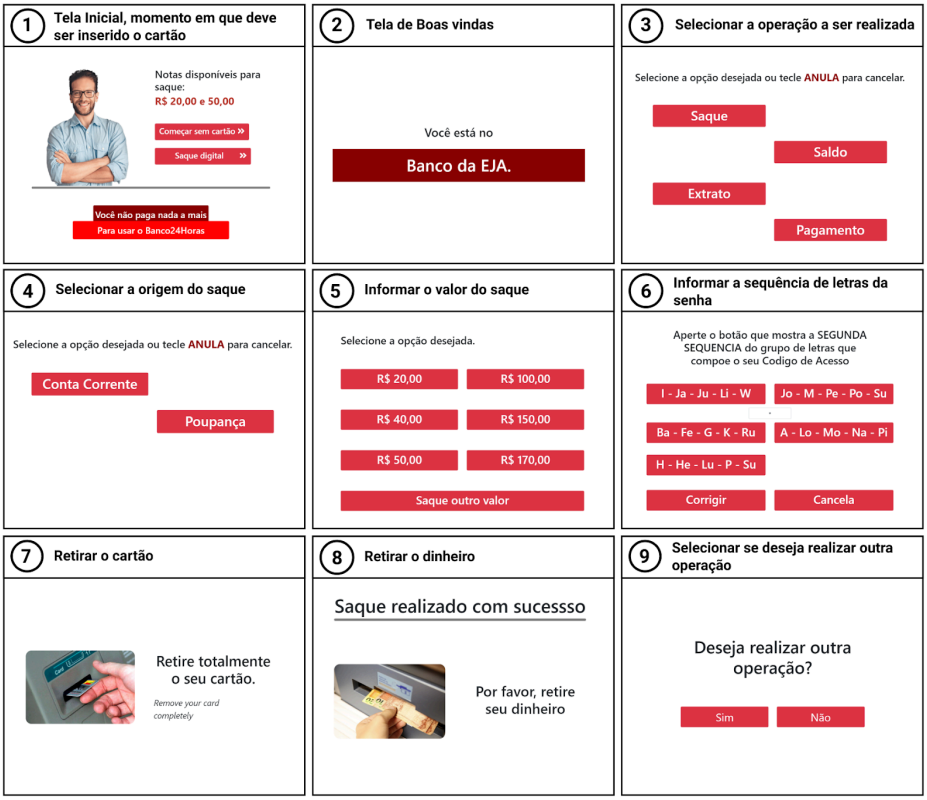


Figura 8. Sequência de telas e operações do Simulador de Saque em Banco 24 horas

2. Avaliação Individual (1 hora e 30 minutos): Os avaliadores tiveram acesso ao site do MeTA, aos materiais de apoio, e avaliaram o simulador executando os seus roteiros de inspeção, caracterizando os problemas encontrados e os graus de severidade no Template de Avaliação Individual. A Tabela 3 apresenta um fragmento do Template de Avaliação Individual preenchido pela A4.

Tabela 3. Fragmento de Template de Avaliação Individual preenchida

ID	Descrição do Problema	Diretriz(es) Violada(s)	Sugestão de solução do problema	Grau de severidade			
				0	1	2	3
1	A tela inicial não solicita a inserção do cartão. Apenas dá a opção de iniciar sem cartão.	3b. 1	*"A tela inicial deveria informar as opções "insira seu cartão" e "iniciar sem cartão", do contrário, um usuário leigo não saberá que deve inserir o cartão para realizar operações."*		x		
2	A interface não fornece qualquer opção de personalização de cores, contraste e ajuste de fonte.	2a. 4, 2a. 10	*"Fornecer opções de personalização em todas as telas da interface, para que o usuário possa fazer o ajuste a qualquer momento de sua utilização."*				x
3	A interface não apresenta alternativas de comando por voz ou formato de áudio para utilização de pessoas surdas.	2a. 13, 1a. 10, 1a. 7	*"Incluir a opção na primeira tela do aplicativo."*				x

3. Avaliação Consolidada (1 hora): Seguindo as recomendações do MeTA com relação à quantidade de avaliadores por grupo, os avaliadores foram divididos em dois subgrupos de cinco pessoas cada. A distribuição dos avaliadores foi feita aleatoriamente conforme a Tabela 4.

Tabela 4. Distribuição dos Avaliadores em Grupos

Grupo	Avaliadores
Grupo 1	A1, A2, A4, A5, A9
Grupo 2	A3, A6, A7, A8, A10

Os dois grupos receberam o Template de Avaliação Consolidada e instruções para fazerem a atividade de consolidação, revisando cada problema para encontrar similaridades e divergências nas Avaliações Individuais, resolvê-las em possíveis oportunidades de convergência e então produzirem os resultados da avaliação. A Tabela 5 apresenta um fragmento do Template de Avaliação Consolidada preenchido pelo Grupo 1, no qual para cada problema é informado um identificador (ID), um link para um arquivo ou imagem que descreva o problema (Imagem ou arquivo), as diretrizes ou normativas violadas (Diretriz(es) Violada(s)), uma sugestão de solução (Sugestão de solução), as severidades atribuídas por cada avaliador (Avaliadores e severidades) e a severidade final (SF).

Tabela 5. Fragmento do Template de Avaliação Consolidada preenchido pelo Grupo 1

ID	Descrição do Problema	Diretriz(es) Violada(s)	Sugestão de Solução	Avaliadores e Severidades					
				A1	A2	A3	A4	A5	SF
1	A tela inicial não solicita a inserção do cartão. Apenas dá a opção de iniciar sem cartão.	3b. 1	*"A tela inicial deveria informar as opções "insira seu cartão" e "iniciar sem cartão", do contrário, um usuário leigo não saberá que deve inserir o cartão para realizar operações."*	1	1	1	2	1	1
2	A interface não fornece qualquer opção de personalização de cores, contraste e ajuste de fonte.	2a. 4, 2a. 10	*"Fornecer opções de personalização em todas as telas da interface, para que o usuário possa fazer o ajuste a qualquer momento de sua utilização."*	0	1	2	1	0	1
3	A interface não apresenta alternativas de comando por voz ou formato de áudio para utilização de pessoas surdas.	2a. 13, 1a. 10, 1a. 7	*"Incluir a opção na primeira tela do aplicativo."*	2	1	3	1	2	2

1.4.2 Resultados e Discussão

Após avaliarem individualmente o Simulador de Saque em Banco 24 horas, cada grupo elaborou um relatório consolidado. Ao todo foram identificados 16 problemas de acessibilidade no simulador. A Tabela 6 apresenta os 5 problemas que foram avaliados com maior severidade por pelo menos um dos grupos (G), com suas respectivas sugestões de melhorias, a normativas violadas (NV) e severidades (S).

Tabela 6. Problemas avaliados com maior severidade

#	Problema	G	NV	Sugestão de Melhoria	S
02	Falta de personalização de cores, contraste e ajuste de fonte.	G1	2a.4, 2a.10	*"Apresentar controle para brilho e contraste".*	3
		G2	2a.4, 2a.10	*"Fornecer opções de personalização em todas as telas da interface, para que o usuário possa fazer o ajuste a qualquer momento de sua utilização".*	1
03	Teclado numérico e botões 'anula' e 'limpar' não funcionam.	G1	5c.1, 1a.5, 4a	*"Adicionar um botão 'anula' que permita voltar a etapas anteriores".*	1
		G2	1a.5, 3b.1	*"Incluir a opção 'anula' na interface".*	3
08	A opção "Saque outro valor" redireciona para a tela de inserção de senha.	G1	3b.1	*"Incluir uma tela para informar o valor de saque desejado".*	3
11	Não há opção de ajuste de velocidade para a execução dos passos e leitura das telas.	G1	2d.2	*"Inserir opção de controle de velocidade das telas".*	3
12	Falta de responsividade.	G1	2a.2, 2a.12	*"Criar opção para aumentar e diminuir o layout".*	3

Com a utilização do MeTA, os dois grupos de avaliadores encontraram diferentes problemas com diferentes severidades. Dos 16 problemas encontrados, somente quatro (01, 02, 03, 04) foram encontrados pelos dois grupos e mesmo estes quatro problemas tiveram diferentes classificações conforme as normativas e diferentes graus de severidade atribuídos. Ao observar os problemas encontrados, é possível constatar que o MeTA auxilia as pessoas a pensarem em possíveis especificidades ou necessidades que diferentes pessoas usuárias de sistemas de informação possam ter.

A quantidade de problemas encontrados pode estar relacionada ao fato de que o Simulador de Saque em Banco 24 horas foi projetado considerando as especificidades do público-alvo e a atividade que seria realizada, por exemplo: em consonância com a normativa *"6a.1 Permitir que a pessoa permaneça sentada ou em pé de forma alinhada durante todo o tempo"* o artefato poderia ter sua altura e posição ajustadas de acordo com as necessidades da pessoa que tivesse utilizando.Além disso, não havia tempo limite para execução da atividade, em consonância com a normativa *"2d.2 Possibilitar opções de ajuste de temporização no caso de exigência de tempo na operação do conteúdo, funcionalidades ou navegação relevantes aos objetivos pedagógicos ou de gestão."*

Embora os avaliadores tenham identificado uma quantidade considerável de problemas, o simulador foi projetado de forma construtiva, com base no conhecimento que o grupo de pesquisadores tinha sobre as habilidades e limitações dos estudantes daquela turma da EJA. Contudo, o artefato não foi desenvolvido para atender a outras especificidades. Por exemplo, como não havia alunos cegos ou surdos na turma, o uso de leitores de tela ou outras tecnologias

assistivas específicas para essas deficiências não foi considerado no desenvolvimento do simulador.

O simulador de Saque em Banco 24 horas é um artefato complexo que envolve tanto componentes físicos quanto digitais. Embora o MeTA tenha sido projetado para avaliar essas tecnologias, as partes físicas do simulador não foram analisadas pelos avaliadores. A cor, o formato e a distribuição dos botões e da interface, por exemplo, podem não ser adequados para todos os tipos de usuários, especialmente para aqueles com deficiência visual ou dificuldades cognitivas. Além disso, não foram identificados problemas relacionados à sua estrutura física, à forma, à posição, ao material utilizado ou às instruções escritas na caixa.

1.5 Conclusão

Este capítulo apresentou o Método para Avaliação de Tecnologias Educacionais Acessíveis (MeTA), que, embora tenha sido projetado para avaliar Tecnologias Educacionais, também pode ser utilizado para avaliar outras tecnologias devido ao seu caráter universal e inclusivo. Por este motivo, o MeTA é apresentado como uma solução para instrumentalizar pessoas a conduzirem avaliações em Sistemas de Informação de uma perspectiva inclusiva, sensibilizando-as e capacitando-as para uma noção de acessibilidade que beneficia a maior extensão possível de pessoas. O caráter inclusivo do MeTA também está no seu desenvolvimento que, além das pessoas autoras, envolveu pessoas com deficiências e especialistas em educação e acessibilidade.

Promover a inclusão para garantir a equidade para uma maior diversidade de pessoas é um desafio global e está entre as metas da Agenda 2030 para o Desenvolvimento Sustentável da ONU. O Brasil é um país particularmente desafiador, com dimensões continentais e desigualdades de acesso e infraestrutura, que impactam no desenvolvimento e implementação de Sistemas de Informação inclusivos. A diversidade de necessidades de acesso e a inclusão de diferentes públicos exigem uma abordagem mais adaptada e flexível no design e na avaliação de tecnologias. Iniciativas como o MeTA são importantes para garantir que os Sistemas de Informação atendam a maior diversidade de habilidades e necessidades, promovendo a inclusão, a equidade e o acesso universal.

O MeTA está alinhado à ABNT NBR 17225:2025 [ABNT 2025], que também estabelece requisitos de acessibilidade para conteúdos e aplicações Web com base nas WCAG 2.2. Ambos compartilham o objetivo de garantir inovação com diversidade e inclusão, avaliando aspectos como navegação por teclado, contraste, textos alternativos e compatibilidade com tecnologias assistivas. O MeTA também pode ser utilizado como uma importante ferramenta educacional para que as pessoas aprendam sobre o que avaliar e como conduzir processos de avaliação de acessibilidade para a inclusão da maior diversidade possível de pessoas ao disponibilizar 70 normativas, planilhas e um passo a passo para aplicação do método.

Referências

Associação Brasileira de Normas Técnicas – ABNT. (2025) “ABNT NBR 17225:2025. Acessibilidade em conteúdo e aplicações web – Requisitos”. Rio de Janeiro, Brasil.

Bastien, C. e Scapin, D. (1993) “Critérios Ergonômicos para Avaliação de Interfaces Homem–Computador”. Disponível em: http://www.labiutil.inf.ufsc.br. Acesso em: 11 de janeiro de 2025.

Brasil. [Constituição (1988)]. “Constituição da República Federativa do Brasil de 1988”. Brasília, DF: Presidência da República, [2016]. http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituiçao.htm. Acesso em: 03 de janeiro de 2025.

Brasil. (2014) “e-MAG: Modelo de Acessibilidade em Governo Eletrônico”, Brasília - DF: MP, SLTI. Disponível em: http://emag.governoeletronico.gov.br, junho. Acesso em 11 de janeiro de 2025.

Connell, B. R. et al. (1997) “The principles of Universal Design”. Disponível em: https://projects.ncsu.edu. Acesso em: 11 de janeiro de 2025.

Maeda, J. (2007) “As leis da simplicidade”, Novo Conceito.

Menezes, K. (2021) “MeTA: Um Método para Avaliação de Tecnologias Educacionais Acessíveis sob a perspectiva do Design Universal”, 172p., Dissertação (Mestrado em Informática), Programa de Pós-graduação em Informática, Universidade Federal do Paraná, Curitiba.

Menezes, K. e Pereira, R. (2022). “MeTA: Um Método para Avaliação de Tecnologias Educacionais Acessíveis”. In Anais Estendidos do XI Congresso Brasileiro de Informática na Educação, pp. 52-61. DOI: https://doi.org/10.5753/cbie_estendido.2022.226355.

Menezes, K.; Ortiz, J. e Pereira, R. (2023). “Avaliando a acessibilidade a partir de uma perspectiva inclusiva: o caso da Plataforma MEC de Recursos Educacionais Digitais”. In Anais do XXXIV Simpósio Brasileiro de Informática na Educação (SBIE), novembro 06, 2023, Passo Fundo/RS, Brasil. SBC, Porto Alegre, Brasil, p. 1018-1029. DOI: https://doi.org/10.5753/sbie.2023.234693.

Menezes, K; Guerra, J; Ferreira, R; Gonçalves, A. e Pereira, R. (2024). “Diagnóstico da Plataforma MEC RED: combinando diferentes métodos de avaliação para informar o redesign”. In Anais Estendidos do XXIII Simpósio Brasileiro de Fatores Humanos em Sistemas Computacionais, outubro 07, 2024, Brasília/DF, Brasil. SBC, Porto Alegre, Brasil, 33-38. DOI: https://doi.org/10.5753/ihc_estendido.2024.243710.

Nielsen, J. (1994). “Heuristic Evaluation”, in Mack, R. & Nielsen, J. (eds.) Usability Inspection Methods. New York, NY: John Wiley & Sons, p. 25-62.

NCSU. (2023) “Universal Design Principles”, http://www.ncsu.edu, julho.

ONU. (1948) “Declaração Universal dos Direitos Humanos”. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 3 de janeiro de 2025.

ONU. (2015) “Transformando Nosso Mundo: A Agenda 2030 para o Desenvolvimento Sustentável", Brasília, https://nacoesunidas.org/pos2015/agenda2030. Acesso em 15 de janeiro de 2024.

Stephanidis, C. (2012) “The encyclopedia of human-computer interaction. The encyclopedia of human-computer interaction”. Disponível em: https://www.interaction-design.org. Acesso em 11 de janeiro de 2025.

W3C BRASIL. (2018) “Web Content Accessibility Guidelines 2.0”. Disponível em: https://www.w3c.br. Acesso em 11 de janeiro de 2025.

Agradecimentos

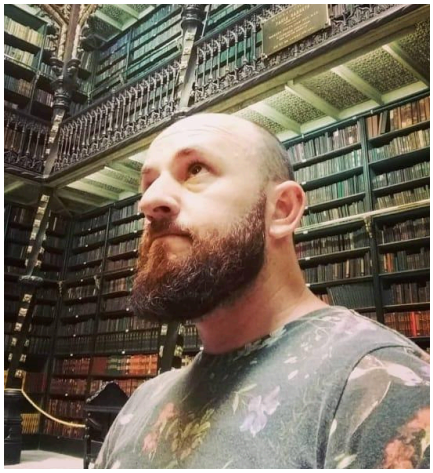
Krissia Menezes possui bolsa de doutorado CAPES e Roberto Pereira possui bolsa de Produtividade em Pesquisa CNPq (#306423/2023-5). Os autores também agradecem o apoio parcial da CAPES PROEX e aos colegas do Laboratório de IHC da UFPR pelo apoio diário e por terem participado do estudo.

Autores

Krissia Menezes

Doutoranda em Ciência da Computação no Programa de Pós-graduação em Informática (PPGInf) da Universidade Federal do Paraná (UFPR), possui mestrado em Informática também pelo PPGInf UFPR, especialização em Desenvolvimento de Sistemas Web pela Estácio e é graduada em Análise e Desenvolvimento de Sistemas pela Universidade do Estado do Pará. Possui experiência com a avaliação de Tecnologias inclusivas e criou o Método para Avaliação de Tecnologias Educacionais Acessíveis.

Currículo Lattes: http://lattes.cnpq.br/1004231276752932



Roberto Pereira

Professor do Departamento de Informática da UFPR e Coordenador do PPGInf da UFPR. Doutor em Ciência da Computação pela Universidade Estadual de Campinas (UNICAMP). Em 2022, recebeu o Prêmio 'Associado Destaque do Ano' da SBC e em 2024 recebeu o Prêmio 'Atuação de Destaque' em IHC' pelas suas contribuições com a SBC e a Comunidade Brasileira de IHC. Atualmente é Editor Chefe do Journal on Interactive Systems (JIS) e Editor Associado da JRC - ACM Journal on Responsible Computing.

Currículo Lattes: http://lattes.cnpq.br/1607596289960868