



ISSN: 1646-9895

Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

D e z e m b r o 2 5 • D e c e m b e r 2 5



©ITMA 2025 <http://www.risti.xyz>

Nº 60

Edição / Edición

Nº 60, 12/2025

Tiragem / Tirage: 1000

Preço por número / Precio por número: 17,5€

Subscrição anual / Suscripción anual: 30€ (2 números)

ISSN: 1646-9895

Depósito legal:

Indexação / Indexación

Academic Journals Database, CiteFactor, Dialnet, DOAJ, DOI, EBSCO, GALE, IndexCopernicus, Index of Information Systems Journals, Web of Science, Latindex, ProQuest, QUALIS, SciELO, SIS, Ulrich's.

Publicação / Publicación

ITMA – Information and Technology Management Association

Pc. 9 de Abril, 26, 4200-422 Porto, Portugal

E-mail: aistic@gmail.com

Web: <http://www.risti.xyz>

Director

Álvaro Rocha, ISEG, University of Lisbon, PT

Coordenadores da Edição / Coordinadores de la Edición

Álvaro Rocha, ISEG, Universidade de Lisboa, PT

Conselho Editorial / Consejo Editorial

Abel Méndez, Technological Institute of Costa Rica, CR

Alejandro Peña, EAFIT University, CO

Alma Gomez-Rodríguez, University of Vigo, ES

Ana Rita Calvao, ESTGA, University of Aveiro, PT

Ania Cravero, Universidad de La Frontera, CL

António Abreu Silva, ISCAP, Polytechnic Institute of Porto, PT

Antonio Garcia, University of Santiago de Compostela, ES

António Godinho, ISEC, Polytechnic Institute of Coimbra, PT

Antonio Jiménez-Martín, Polytechnic University of Madrid, ES

Arturo J. Méndez, University of Vigo, ES

August Climent, Ramon LLull University, ES

Beatriz Rodríguez, Universidad de la Republica, UY

Borja Bordel, Polytechnic University of Madrid, ES

Brenda L. Flores-Rios, Universidad Autónoma de Baja California, MX

Bruno Miguel Ferreira Gonçalves, Polytechnic Institute of Braganca, PT

Carlos Alexandre Silva, Federal Institute of Minas Gerais, BR

Carlos Carreto, Polytechnic Institute of Guarda, PT

Carlos Morais, Polytechnic Institute of Braganza, PT

Carlos Rompante Cunha, UNIAG & CeDRI &

Polytechnic Institute Bragança, PT

Carlos Vaz de Carvalho, Polytechnic Institute of Porto, PT

Célio Marques, Polytechnic Institute of Tomar, PT

Círo Martins, University of Algarve, PT

Concepción Damián-Hernández, Instituto

Tecnológico Superior de Misantla, MX

Cristina Caridade, Polytechnic Institute of Coimbra, PT

Daniel Poland, University of Aveiro, PT
Dante Carrizo, University of Atacama, CL
Edwin Cedeño Herrera, Universidad de Panamá, PA
Fabio Marques, ESTGA, University of Aveiro, PT
Felipe Vasquez, Universidad de La Frontera, CL
Fernando Moreira, REMIT, IJP, Portucalense University & IEETA,
University of Aveiro, PT
Fernando Paulo Belfo, Coimbra Business School – ISCAC, Polytechnic
Institute of Coimbra, PT
Fernando Ribeiro, Polytechnic Institute of Castelo Branco, PT
Fernando Bandeira, PT
Filipe Cardoso, Polytechnic Institute of Viseu, PT
Flor Gomes de María Sánchez Aguirre, Universidad César Vallejo, PE
Francisco Javier Lena-Acebo, University of Cantabria, ES
Gabriel Guerrero-Contreras, University of Cádiz, ES
Gerardo González Filgueira, University of A Coruña, ES
Gloria Valencia, Universidad de las Fuerzas Armadas, EC
Helder Gomes, University of Aveiro, PT
Helder Zagalo, University of Aveiro, PT
Hélia Guerra, University of the Azores, PT
Henrique Gil, Polytechnic Institute of Castelo Branco, PT
Henrique S. Mamede, Open University, PT
Isaias Bianchi, Federal University of Santa Catarina, BR
Ismael Etxeberria-Agiriano, Universidad del País Vasco, ES
Ivan Garcia, Universidad Tecnológica de la Mixteca, MX
Jeimy Cano, Universidad de los Andes, CO
John Emilio Almeida, ISTECS - Porto, PT
João Paulo Ferreira, Polytechnic Institute of Coimbra, PT
Roberto de Toledo Quadros, CEFET/RJ, BR
Joao Tavares, University of Porto, PT
Joaquim Reis, ISCTE - University Institute of Lisbon, PT
Jorge Eduardo Ibarra Esque, Universidad
Autónoma de Baja California, MX

Jorge Hochstetter, Universidad de La Frontera, CL
José Álvarez-García, University of Extremadura, ES
Jose Felipe Cocon Juarez, Universidad Autónoma del Carmen, MX
José Lousado, Polytechnic Institute of Viseu, PT
José Luis Pastrana Brincones, University of Malaga, ES
Jose M. Molina, Carlos III University of Madrid, ES
José Ribeiro, Polytechnic of Leiria, PT
Jose Silvestre Silva, Military Academy, PT
Juan Angel Contreras Vas, University of Extremadura, ES
Juan M. Santos-Gago, University of Vigo, ES
Juan Pablo DAmato, National University of the Center of the
Province of Buenos Aires, AR
Leila Weitzel, Fluminense Federal University, BR
Leonardo Bermón Angarita, National University of Colombia, CO
Lilia Muñoz, Universidad Tecnológica de Panamá, PA
Lucila Romero, Universidad Nacional del Litoral, AR
Luis Alvarez Sabucedo, University of Vigo, ES
Luis Enrique Sánchez Crespo, University of Castilla-la Mancha, ES
Luisa María Romero-Moreno, Universidad Sevilla, ES
Luz María Hernández Cruz, Universidad Autónoma de Campeche, MX
Luz Sussy Bayona Oré, Universidad Nacional Mayor de San Carlos, PE
Marcelo Marciszack, National Technological University, AR
Marcelo Zambrano Vizueté, Universidad Tecnica Del Norte
Marco Painho, NOVA IMS, PT
Margarita Ramirez Ramirez, Universidad Autónoma de Baja California, MX
Maria Cristina Marcelino Bento, UNIFATEA, BR
María de la Cruz del Río-Rama, University of Vigo, ES
Maria de los Milagros Gutierrez, National Technological University, AR
Maria do Rosario Bernardo, Open University, PT
Maria João Ferreira, Portucalense University, PT
Maria João Gomes, University of Minho, PT
Maria Sousa, ISCTE - University Institute of Lisbon, PT
Marisol B. Correia, ESGHT - University of Algarve & CiTUR, PT

Maristela Holanda, University of Brasilia, BR
Martin Llamas Nistal, University of Vigo, ES
Miguel Casquilho, University of Lisbon, PT
Miguel Ramón González Castro, Aimen Technological Center, ES
Mirna Ariadna Muñoz Mata, CIMAT, MX
Nelson Rocha, University of Aveiro, PT
Nuno Melão, Polytechnic Institute of Viseu, PT
Nuno Ribeiro, Fernando Pessoa University, Portugal
Patricia Dias, State University of Minas Gerais, BR
Paula Prata, University of Beira Interior, PT
Paulo Martins, University of Trás-os-Montes and Alto Douro, PT
Paulo Pinto, New University of Lisbon, PT
Paulo Rurato, Fernando Pessoa University, Portugal
Pedro Araújo, University of Beira Interior, PT
Pedro R. Palos-Sanchez, Universidad de Sevilla, ES
Pedro Sanz-Angulo, University of Valladolid, ES
Pedro Sobral, Fernando Pessoa University, Portugal
Pedro Sousa, University of Minho, Portugal
René Faruk Garzozzi-Pincay, Santa Elena Peninsula State University, EC
Ruben Pereira, ISCTE – University Institute of Lisbon, PT
Rui Pedro Marques, University of Aveiro, PT
Rui Silva Moreira, Fernando Pessoa University, PT
Samuel Sepúlveda, Universidad de La Frontera, CL
Sandro Carvalho, Polytechnic of Cávado and Ave, PT
Santiago Raul Gonzales Sanches, Universidad Cesar Vallejo, PE
Sara Balderas-Díaz, University of Cádiz, ES
Sergio Araya Guzmán, Universidad del Bío-Bío, CL
Sergio F. Lopes, University of Minho, PT
Solange N Alves-Souza, University of Sao Paulo, BR
Telmo Silva, DigiMedia, University of Aveiro, PT
Thiago Dias, Federal Center for Technological Education of Minas Gerais, BR
Veronica Vasconcelos, Polytechnic Institute of Coimbra, PT
Vítor Carvalho, Polytechnic Institute of Cávado and Ave, PT

Vitor Santos, New University of Lisbon - NOVA IMS, PT
Wagner Tanaka Botelho, Federal University of ABC, BR
Yamid Hernández Julio, Universidad del Sinú, CO

Índice / Index

EDITORIAL

- Avanços e Aplicações em Sistemas e Tecnologias de Informação 1
Álvaro Rocha

ARTIGOS / ARTICULOS / ARTICLES

- Gobierno Electrónico en Córdoba, Argentina:
Factores predictores de su uso y continuidad5
*Débora J. Mola, Sonia Yamila Dominguez, M. Victoria Ortiz,
Agustín González Marchelli, Cecilia Reyna*

- Institucionalização da telemedicina: a estrutura
iTAM-Health e evidências do sistema de saúde ULSS3 34
Riccardo Maria Santovito, Maria José Sousa

- StopEmailSpoofing: uma solução para detecção de
vulnerabilidade de domínios à ataques falsificação de e-mail57
*Guilherme Dieguez Cândido, Igor Ramos Bezerra da Silva¹, Emílio Gonçalves¹,
Leonardo de Paiva Souza, João Souza Neto, Rafael Rabelo Nunes*

- Processamento de Linguagem Natural Aplicado à
Identificação de Padrões Semânticos em Relatos de
Mulheres Vítimas de Violência Doméstica e Familiar74
Sabrina S. Vasconcellos, Deborah Q. G. Foroni, Peterson A. Belan

- Transformación digital sostenible: la convergencia de
la innovación tecnológica y la sostenibilidad 96
*Díaz González de Mendoza, Pável, Fuentes Prieto Mayda Juana,
Díaz Manresa Karel*

- Reconocimiento de emociones en texto de estudiantes de
educación secundaria rural utilizando algoritmos de clasificación 112
*Fidel Huanco-Ramos, Yesenia Valentin-Ccori, Henry Shuta-Lloclla,
Martha Yucra-Sotomayor, Fredy Aparicio Castillo-Suaquita*

- Madurez en ciberseguridad y resiliencia digital en PYMEs
iberoamericanas: diagnóstico y desafíos estratégicos 127
Hernán Cornejo

Avanços e Aplicações em Sistemas e Tecnologias de Informação

Advances and Applications in Information Systems and Technologies

*Álvaro Rocha*¹

amr@iseg.ulisboa.pt

¹ ISEG, Universidade de Lisboa, Rua Miguel Lupi 20, 1200-109 Lisboa, Portugal.

DOI: 10.17013/risti.60.1-3

O número regular 60 da RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação integra sete artigos científicos, selecionados através de um exigente processo de revisão por pares, que resultou numa taxa de aceitação de 9,72%. Este valor reflete o elevado rigor científico da revista e o seu compromisso contínuo com a qualidade, a relevância e a solidez metodológica dos trabalhos publicados.

Os artigos que compõem este número abordam temáticas atuais e diversificadas no domínio dos Sistemas e Tecnologias de Informação, incluindo governo eletrónico, telemedicina, cibersegurança, processamento de linguagem natural, transformação digital sustentável e aplicações tecnológicas em contextos sociais sensíveis. Em conjunto, estes trabalhos oferecem contributos significativos para a comunidade científica e profissional.

Apresenta-se, de seguida, um breve sumário dos artigos publicados.

O primeiro artigo intitulado “Gobierno Electrónico en Córdoba, Argentina: Factores predictores de su uso y continuidad” analisa os fatores que influenciam a adoção e a continuidade de utilização de serviços de governo eletrónico na província de Córdoba, Argentina. Com base numa abordagem empírica, o estudo identifica determinantes críticos como a confiança, a utilidade percebida e a experiência do utilizador, contribuindo para uma melhor compreensão dos desafios associados à consolidação do e-government em contextos latino-americanos.

O segundo artigo intitulado “Institucionalização da telemedicina: a estrutura iTAM-Health e evidências do sistema de saúde ULSS3” propõe e valida a estrutura iTAM-Health no contexto da institucionalização da telemedicina. Através de um estudo empírico realizado no sistema de saúde público italiano ULSS3, o trabalho demonstra como modelos de aceitação tecnológica podem ser adaptados ao setor da saúde, fornecendo um enquadramento robusto para apoiar decisões estratégicas e operacionais.

O terceiro artigo intitulado “StopEmailSpoofing: uma solução para deteção de vulnerabilidade de domínios a ataques de falsificação de e-mail” apresenta uma solução tecnológica orientada para a identificação automática de vulnerabilidades de domínios a ataques de email spoofing. A proposta contribui para o reforço da cibersegurança organizacional, mitigando riscos associados a ataques de engenharia social e promovendo boas práticas de segurança da informação.

O quarto artigo intitulado “Processamento de Linguagem Natural aplicado à identificação de padrões semânticos em relatos de mulheres vítimas de violência doméstica e familiar” explora a aplicação de técnicas de Processamento de Linguagem Natural na análise de relatos de vítimas de violência doméstica e familiar. O estudo evidencia o potencial das tecnologias de informação no apoio à análise de dados sensíveis, com elevado impacto social, promovendo abordagens interdisciplinares entre tecnologia, justiça e políticas públicas.

O quinto artigo intitulado “Transformación digital sostenible: la convergencia de la innovación tecnológica y la sostenibilidad” analisa a relação entre transformação digital e sustentabilidade, destacando o papel da inovação tecnológica como catalisador de práticas organizacionais sustentáveis. O artigo sublinha a importância do alinhamento entre estratégias digitais e objetivos de desenvolvimento sustentável, particularmente em contextos empresariais e institucionais.

O sexto artigo intitulado “Reconocimiento de emociones en texto de estudiantes de educación secundaria rural utilizando algoritmos de clasificación” centra-se na aplicação de algoritmos de classificação para o reconhecimento automático de emoções em textos produzidos por estudantes do ensino secundário em contextos rurais. O estudo recorre a dados recolhidos e etiquetados a partir de autorrelatos, comparando abordagens de inteligência artificial para identificar o desempenho mais adequado na deteção de emoções, contribuindo para aplicações educativas baseadas em dados e para o avanço de metodologias de análise afetiva em linguagem natural.

Por último, o sétimo artigo intitulado “*Madurez en ciberseguridad y resiliencia digital en PYMEs iberoamericanas: diagnóstico y desafíos estratégicos*” analisa o nível de maturidade em cibersegurança e resiliência digital em pequenas e médias empresas iberoamericanas, propondo um modelo de diagnóstico com base no NIST Cybersecurity Framework, complementado por indicadores organizacionais e de cultura de segurança. O trabalho evidencia lacunas relevantes e desafios estratégicos, oferecendo orientações úteis para o fortalecimento de capacidades, governação e práticas de segurança em organizações particularmente expostas ao aumento de ciberameaças.

Em síntese, o número 60 da RISTI reafirma a missão da revista enquanto espaço de divulgação científica de referência, promovendo investigação rigorosa, metodologicamente sólida e com impacto académico, organizacional e social.

Aos autores, revisores e a toda a equipa editorial, é devido um reconhecimento público pelo contributo determinante para a qualidade e prestígio deste número.

Boa leitura!

Gobierno Electrónico en Córdoba, Argentina: Factores predictores de su uso y continuidad

Débora J. Mola¹, Sonia Yamila Dominguez², M. Victoria Ortiz³,
Agustín González Marchelli⁴, Cecilia Reyna⁵

**deboramola@unc.edu.ar; sonia.dominguez@mi.unc.edu.ar; mv.ortiz@unc.edu.ar;
agustingonzalez@mdp.edu.ar; ceciliareyna@unc.edu.ar**

¹ Instituto de Investigaciones Psicológicas IIPsi – Consejo Nacional de Investigaciones Científicas y Técnicas. Facultad de Psicología, Universidad Nacional de Córdoba, Argentina.

² Facultad de Psicología, Universidad Nacional de Córdoba, Argentina.

³ Instituto de Investigaciones Psicológicas IIPsi – Consejo Nacional de Investigaciones Científicas y Técnicas. Facultad de Psicología, Universidad Nacional de Córdoba, Argentina.

⁴ Instituto de Psicología Básica, Aplicada y Tecnología - Facultad de Psicología Universidad Nacional de Mar del Plata, Argentina.

⁵ Instituto de Investigaciones Psicológicas IIPsi – Consejo Nacional de Investigaciones Científicas y Técnicas. Facultad de Psicología, Universidad Nacional de Córdoba, Argentina

DOI: 10.17013/risti.60.5-33

Resumen: Objetivo. Explorar el rol de variables cognitivas (facilidad, utilidad, satisfacción y competencia digital), sociocognitivas (confianzas en el gobierno, internet y gobierno electrónico [GE]), sociopolíticas (compromiso cívico y participación online) y sociodemográficas (género, edad, nivel educativo, nivel socioeconómico y conexión a internet) en la adopción (uso e intención de continuidad de uso) del GE (*Mi Argentina*, *Ciudadano Digital* y el Portal del Gobierno de la Ciudad). **Método.** Participaron 1.042 personas de 18 a 65 años residentes en Córdoba. Se realizó un estudio correlacional de alcance exploratorio. **Resultados.** Las variables cognitivas fueron consistentes al predecir la adopción del GE. Las confianzas en internet, gobierno y GE predijeron principalmente la intención de continuidad de uso. El compromiso cívico y la participación online predijeron más el uso. También, las variables sociodemográficas explicaron la adopción en algunos casos. **Conclusión.** Los resultados ofrecen insumos relevantes para diseñar políticas públicas que promuevan la adopción del GE en Argentina.

Palabras-clave: factores cognitivos; confianzas; compromiso ciudadano; características sociodemográficas; plataformas digitales públicas.

E-Government in Córdoba, Argentina: Drivers of Use and Continuance Intention to

Abstract: Objective. To examine the role of cognitive variables (perceived ease of use, usefulness, satisfaction, and digital competence), sociocognitive variables (trust

in government, the internet, and e-government [EG]), sociopolitical variables (civic engagement and online participation), and sociodemographic variables (gender, age, educational level, socioeconomic status, and internet access) in the adoption of e-government (EG), understood as use and continuance intention, across the platforms Mi Argentina, Ciudadano Digital, and the Córdoba City Government Portal. **Method.** A correlational study with an exploratory scope was conducted with 1,042 residents of Córdoba aged 18 to 65 years. **Results.** Cognitive variables consistently predicted EG adoption. Trust in the internet, government, and EG primarily predicted continuance intention, whereas civic engagement and online participation were more strongly associated with actual use. Sociodemographic variables also explained adoption in some cases. **Conclusion.** The findings provide relevant evidence to inform the design of public policies aimed at promoting EG adoption in Argentina.

Keywords: cognitive factors; trust; civic engagement; sociodemographic characteristics; digital public platforms.

1. Introducción

En el marco de la Agenda 2030 y del cumplimiento de los Objetivos de Desarrollo Sostenible, diversas dependencias gubernamentales argentinas han impulsado políticas públicas orientadas a la modernización del Estado (Consejo Nacional de Coordinación de Políticas Sociales [CNCPS], 2021). La incorporación de tecnologías de la información y comunicación (TICs), como las aplicaciones móviles, al gobierno (es decir, el gobierno electrónico, [GE]), mejora el acceso a la información pública, la participación, la gestión de problemáticas comunes e incluye a sectores históricamente excluidos (Díaz & Gutiérrez, 2021; Naser et al., 2021). Desde 2007, en América Latina el acceso a las TICs y al GE se reconoce como un derecho ciudadano (Centro Latinoamericano para el Desarrollo [CLAD], 2016). Los derechos de cuarta generación incluyen el acceso equitativo a la información, la formación en nuevas tecnologías y la seguridad digital (Instituto Nacional de la Administración Pública [INAP], 2022).

Aunque el desarrollo de TICs ha crecido significativamente en los últimos años (acelerado por la pandemia de SARS-CoV-2) y el GE se implementa internacionalmente (Morales-Urrutia et al., 2020), las tasas de uso siguen siendo más bajas en el sur global (Mola & Reyna, 2022). En este sentido, la brecha digital (i.e., el acceso, uso y apropiación desigual de las TICs) limita el aprovechamiento de las herramientas digitales (Tellechea, 2018). Según el Índice de Desarrollo de Gobierno Electrónico (EGDI) de Naciones Unidas, en 2020 Argentina ocupaba el puesto 32 de 193 países. Sin embargo, este índice no contempla la perspectiva ciudadana (Alderete et al., 2022). Asimismo, el éxito del GE depende de la adopción (i.e., uso e intención de continuidad de uso; Kumar et al., 2007) por parte de la ciudadanía (Mola & Reyna, 2022; Mustafa et al., 2019; Nguyen et al., 2025), aspecto poco considerado en las estrategias políticas nacionales (Lago Martínez, 2016). Por lo tanto, resulta clave investigar los factores que faciliten la adopción del GE desde la perspectiva ciudadana.

Entre los principales marcos teóricos que explican la adopción tecnológica se destacan la Teoría de la Difusión de la Innovación (TDI; Rogers, 1995) y el Modelo de Aceptación de la Tecnología (MAT; Davis, 1989). La TDI postula que variables sociodemográficas como

el género, la edad y el nivel educativo explican la adopción. Es decir, los varones, las personas más jóvenes y con mayor nivel educativo utilizan más el GE (p.ej., Abu-Shanab, 2015; Idris, 2016; Inzunza Mejía & López Carmona, 2018; Mukonza et al., 2016). Sin embargo, los resultados no son concluyentes, dependen de factores socioculturales y del tipo de herramienta analizada (Mercy et al., 2020; Alderete et al., 2022). En Córdoba, con una herramienta de GE generada por el Municipio (*App Ciudadana*) se observó que personas mayores y/o con menor nivel educativo tuvieron más dificultades y utilizaron menos la *App* (Mola et al., 2021; Sorribas et al., 2022).

El MAT sostiene que la percepción de facilidad de uso (i.e., bajo esfuerzo cognitivo; Carter et al., 2016), utilidad (i.e., contribución del sistema a la vida cotidiana; Botelho, 2019) y satisfacción se relacionan positivamente con la intención de uso (Botelho, 2019), el uso (Inzunza Mejía & López Carmona, 2018) y la intención de continuidad (Hamid et al., 2016). Ahora bien, Botelho (2019) observó que la percepción de facilidad y utilidad predicen la intención de uso, mientras que la satisfacción afecta directamente el uso. Por otro lado, Wangpipatwong et al. (2008) encontraron que la percepción de utilidad media el efecto de la percepción de facilidad sobre la intención de continuidad. Por lo que, el rol de estas variables en la adopción del GE no es claro. A nivel local, se observó que las percepciones de facilidad, utilidad y satisfacción predijeron la intención de continuar usando el GE (Mola et al., 2021; 2022; Sorribas et al., 2022).

Sumado a lo anterior, existen otros factores relevantes en la adopción del GE no considerados por la TDI y el MAT. En primer lugar, una de las principales barreras es el acceso a internet y la frecuencia de uso, que influyen en las habilidades y conocimientos sobre internet y las TICs (Schradié, 2011; Urbina & Abe, 2017). Al respecto, Delfino et al. (2019) encontraron que el uso de internet se relaciona con la edad y el nivel educativo, aunque los estudios en Argentina son escasos. Por su parte, la confianza en internet, en el gobierno y en el GE (i.e., confianza en el servicio digital brindado por el gobierno) incide positivamente en su adopción (Tsui et al., 2019; Khan et al., 2020; Ly & Xue, 2021). Sin embargo, la evidencia sobre el rol de la confianza en el GE es contradictoria (Alderete & Díaz, 2020; Schaupp & Carter, 2010; Teo et al., 2008) y varía según dimensiones evaluadas (calidad del sistema, factores de riesgo, tipo de servicio) (Pérez-Morote et al., 2020; Khan et al., 2020).

Asimismo, el compromiso cívico (i.e., la disposición a ocuparse de las necesidades e intereses cívicos; Bianchini et al., 2016) y la participación online (i.e., realizar actividades sociales y políticas en redes sociales) se asocian a una mayor percepción de utilidad y uso del GE (Mercy et al., 2020). Además, un mayor conocimiento sobre el GE se vincula con niveles más altos de compromiso cívico y participación (López-De Castro & García Alonso, 2016). A su vez, la participación online predice el uso del GE (Basri et al., 2019). Según nuestro conocimiento, en Argentina no existen estudios que analicen de manera conjunta estos factores. Así, nos propusimos explorar el rol de variables cognitivas (percepción de facilidad, utilidad, satisfacción y competencia digital), sociocognitivas (confianza en el gobierno, en internet y en el GE), sociopolíticas (compromiso cívico y participación online), sociodemográficas (género, edad, nivel educativo [NE], socioeconómico [NSE], frecuencia de conexión a internet) en la adopción (uso e intención de continuidad de uso) del GE en habitantes de Córdoba (Argentina). Específicamente, describimos el nivel de uso y la intención de continuidad de uso del GE

y examinamos el rol de las variables mencionadas en el uso y la intención de continuidad de uso del GE. Hipotetizamos que las mujeres y las personas de mayor edad, usarán menos y tendrán menor intención de continuar usando el GE. Asimismo, esperamos que a mayor NE, NSE, percepción de facilidad, utilidad y satisfacción, mayor uso e intención de continuidad de uso del GE. También, a mayor confianza en el gobierno, en internet, en el GE, compromiso cívico y participación online (social y política), mayor adopción.

En este estudio analizamos tres plataformas de GE. Mi Argentina, en sus versiones web y móvil, permite el acceso a servicios digitales de salud y gestión de trámites, y cuenta con más de 10 millones de descargas a nivel nacional (Argentina.gob.ar, s.f.) en Google Play. A nivel provincial, Ciudadano Digital (CiDi) centraliza servicios gubernamentales y su aplicación móvil supera los 3.6 millones de descargas (CIDI, s.f.). Finalmente, el Portal del Gobierno de la Ciudad de Córdoba ofrece trámites, notificaciones electrónicas, turnos y acceso a información pública. Sin embargo, su uso es considerablemente menor en comparación con Mi Argentina y CiDi

2. Método

2.1. Participantes

Participaron 1042 ciudadanos/as cordobeses/as de 18 a 65 años ($M_{\text{edad}} = 29.46$; $DE = 11.75$), el 77.8% eran mujeres ($n = 811$), el 48.4% tenían un NSE medio ($n = 504$) y el 78.7% había completado al menos la escuela secundaria (Tabla 1). El tamaño muestral se determinó en función del estudio de mayor alcance (ver procedimiento), aplicando el criterio de 10 participantes por ítem (Boateng et al., 2018; Morgado et al., 2017). Se utilizó un muestreo auto-elegido, el cual implica que las personas fueron invitadas y decidieron voluntariamente formar parte de la muestra (Bologna, 2022). Los criterios de inclusión fueron: (1) tener entre 18 y 65 años de edad; (2) residir en la ciudad de Córdoba; (3) no haber participado en la fase 1 del estudio de Gobierno Electrónico (estudio psicométrico).

		n	%	M±DE
Género	Mujer	811	77.8	
	Varón	215	20.6	
	No binarie	3	0.3	
	Varón trans	1	0.1	
	Travesti	1	0.1	
	Otro	5	0.5	
	Prefiero no decirlo	6	0.6	
Nivel socioeconómico	alto	69	6.6	
	medio alto	273	26.2	
	medio	504	48.4	
	medio bajo	177	17.0	
	bajo	19	1.8	

		n	%	M±DE
<i>Edad</i>	18 a 65 años	1042		29.46 ± 11.75
	Sin estudios	2	0.2	
	Primaria incompleta	3	0.3	
	Primaria completa	4	0.4	
	Secundaria incompleta	23	2.2	
	Secundaria completa	276	26.5	
<i>Nivel educativo</i>	Terciario o universitario incompleto	512	49.1	
	Terciario completo	77	7.4	
	Universitario completo	94	9.0	
	Posgrado completo o incompleto	51	4.9	
	N	1042		

Nota. Género Otro: no se identifica con las categorías previas. Fuente: elaboración propia.

Tabla 1 – Descripción sociodemográfica de la muestra: Género, NSE, Edad y NE.

2.2. Instrumentos

Este trabajo forma parte de un estudio más amplio que evaluó propiedades psicométricas de instrumentos desarrollados en otros contextos e incluyó variables no analizadas aquí. A continuación, se describen las escalas e ítems utilizados.

Uso del GE. Se empleó un ítem que evaluó la cantidad de veces que se usaron en el último mes cada una de las herramientas de GE (Mi Argentina, CiDi-ciudadano digital y el portal de gobierno de la Ciudad de Córdoba), mediante una escala de respuesta numérica.

Intención de continuidad de uso del GE. Se utilizaron cuatro ítems (Alzharani, 2018; Wangpipatwong et al., 2008; véase Anexo, Tabla 1) que indagaron sobre las mismas herramientas de GE con una escala de respuesta tipo Likert de cinco puntos (1 = Muy en desacuerdo a 5 = Muy de acuerdo). La versión cordobesa demostró tener propiedades psicométricas adecuadas (Mi Argentina: sitio web α (Alfa) = 0.85; ω (Omega) = 0.85; App α = 0.89; ω = 0.89; CiDi: Sitio web α = 0.91; ω = 0.91; App α = 0.91; ω = 0.91 y el portal del gobierno de la ciudad α = 0.95; ω = 0.95).

Variables sociodemográficas. El género, la edad y el nivel educativo se relevaron mediante un cuestionario estructurado de preguntas cerradas. El NSE se operacionalizó considerando características del principal sostén del hogar (educación, ocupación, cobertura de salud) y la cantidad de miembros del hogar con ingresos (Asociación Argentina de Marketing, Sociedad Argentina de investigadores de Marketing y Opinión, Cámara de Empresas de Investigación Social y de Mercado de Argentina, AAM-SAIMO-CEIM, 2015). La *frecuencia de conexión a internet* se evaluó utilizando tres ítems

(Delfino et al., 2019), a partir de los cuales se construyó un índice de conexión (0–3), donde valores más altos indicaron mayor conexión a internet

Percepciones de facilidad, utilidad y satisfacción. Se emplearon siete ítems (Mola et al., 2021; Wangpipatwong et al., 2008) por cada herramienta de GE. La escala de respuesta a los ítems fue tipo Likert de cinco puntos (percepciones de facilidad y utilidad: 1 = Muy en desacuerdo a 5 = Muy de acuerdo; de satisfacción: 1 = Completamente insatisfecho a 5 = Completamente satisfecho). Estos instrumentos han demostrado adecuados índices de consistencia interna en estudios previos (p.ej., *percepción de facilidad*: $\alpha = 0.87$; Wangpipatwong et al., 2008) y en la versión adaptada en Córdoba, Argentina (*percepción de facilidad*: Mi Argentina: sitio web $\alpha = 0.90$, $\omega = 0.90$; App $\alpha = 0.91$, $\omega = 0.91$; CiDi: Sitio web $\alpha = 0.94$; $\omega = 0.94$, App $\alpha = 0.925$; $\omega = 0.925$, y portal del gobierno de la ciudad $\alpha = 0.93$ $\omega = 0.93$; *percepción de utilidad*: Mi Argentina: sitio web $\alpha = 0.85$; $\omega = 0.88$; App $\alpha = 0.85$; $\omega = 0.865$; CiDi: Sitio web $\alpha = 0.87$; $\omega = 0.875$; App $\alpha = 0.92$; $\omega = 0.92$ y el portal del gobierno de la ciudad $\alpha = 0.92$; $\omega = 0.92$).

Competencia Digital. Se implementó la escala de Jiménez Cortés et al. (2016), conformada por 18 ítems con una escala de respuesta tipo Likert de cinco puntos (1 = Nunca a 5 = Siempre). Este instrumento mostró adecuadas propiedades psicométricas en la versión española ($\alpha = 0.87$) (Jiménez Cortés et al., 2016) y Argentina ($CFI = 0.94$; $TLI = 0.93$; $\alpha = 0.84$; $\omega = 0.84$).

Conocimiento sobre GE. Se utilizó un ítem (Alderete & Díaz, 2020) modificado según cada herramienta de GE. La escala de respuesta fue dicotómica con opción sí/no. Asimismo, para las herramientas Mi Argentina y CiDi, se incluyó una pregunta para conocer la frecuencia de uso de las versiones web o móvil (ver procedimiento y Anexo Tabla 1).

Confianzas en el gobierno, GE e internet. Se preguntó por el nivel de confianza en el gobierno nacional, provincial y municipal (Encuesta Mundial Gallup, 2018; Encuesta Latinobarómetro, 2020). A su vez, para medir las confianzas en el GE y en internet se emplearon seis ítems (Mota et al., 2022; Tsui, 2019). Las versiones originales de las escalas poseen buenos índices de consistencia interna (*confianza en el GE*: $\alpha = 0.89$, Tsui, 2019; Tsui et al., 2019; *confianza en internet*: $\alpha = 0.82$; Mota et al., 2016) y también las versiones adaptadas en Argentina (*confianza en el GE*: $\alpha = 0.93$, $\omega = 0.93$; *confianza en internet*: $\alpha = 0.84$; $\omega = 0.85$; Mola et al., 2023). La escala de respuesta a los ítems fue tipo Likert de cinco puntos (confianza en el gobierno: 1 = Nada de confianza a 5 = Mucha confianza; confianza en el GE y en internet: 1 = Muy en desacuerdo a 5 = Muy de acuerdo).

Compromiso cívico. Se utilizaron cinco ítems (Mota et al., 2016) con una escala de respuesta tipo Likert de 5 puntos (1 = Muy en desacuerdo a 5 = Muy de acuerdo). Las versiones originales y adaptadas en Argentina mostraron adecuadas propiedades psicométricas ($\alpha = 0.88$; Mota et al., 2016) y Argentina ($CFI = .99$; $TLI = .99$; $\alpha = 0.90$; $\omega = 0.91$).

Participación online en actividades políticas y sociales. Se emplearon 10 ítems (Delfino et al., 2019) con una escala de respuesta tipo Likert de 5 puntos (1= Nunca a 5= Siempre). Las versiones adaptadas en Córdoba han demostrado propiedades psicométricas adecuadas (*participación online en actividades políticas*: $CFI = .99$; $TLI = .99$; $\alpha = 0.84$;

$\omega = 0.86$; *participación online en actividades sociales*: $CFI = .99$; $TLI = .98$; $\alpha = 0.75$; $\omega = 0.75$).

2.3. Diseño y procedimiento

Se realizó un estudio empírico cuantitativo correlacional de alcance exploratorio, empleando una encuesta online (Hernández Sampieri et al., 2014, Yuni & Urbano, 2014).

Se invitó a las personas a participar mediante redes sociales (Instagram, Whatsapp y Facebook), correos electrónicos (base de datos del equipo) y difusión en espacios públicos e institucionales. Los datos se recolectaron a través de la plataforma LimeSurvey (disponible a través de la Universidad Nacional de Córdoba). Al comenzar el estudio las personas recibieron información sobre el propósito del estudio, las condiciones de participación, la confidencialidad de los datos y el carácter voluntario de su participación. Inicialmente, respondieron sobre frecuencia de conexión a internet, competencia digital, participación online, compromiso cívico y las confianzas en el gobierno, internet y GE. Luego, indicaron si conocían Mi Argentina, CiDi y el portal municipal, y qué versión utilizaban con mayor frecuencia (aplicación móvil, sitio web o ambas por igual). Según sus respuestas respondieron por las percepciones de facilidad, utilidad y satisfacción, el uso y la intención de continuidad de uso. Quienes seleccionaron la opción *ambas por igual* respondieron sobre la versión móvil de la herramienta. Al finalizar, completaron datos sociodemográficos. El estudio duró aproximadamente 15 minutos. Quienes completaron la encuesta pudieron participar en un sorteo de tres premios. El protocolo cumplió con los principios éticos para investigaciones con seres humanos (American Psychological Association, 2017) y fue aprobado por el Comité de Ética del instituto. El estudio se realizó durante el año 2023 y 2024.

2.4. Análisis de datos

Inicialmente, se realizaron análisis descriptivos de los datos. Se efectuó una inspección de los casos y variables con el fin de identificar posibles incumplimientos de los supuestos estadísticos. Para ello, se calcularon estadísticos descriptivos y se analizaron casos atípicos univariados (puntajes $Z > \pm 3.29$) y multivariados ($p < .01$; Tabachnick y Fidell, 2014). Asimismo, se consideraron aceptables valores de asimetría y curtosis dentro del rango ± 1.5 (George & Mallery, 2001).

Luego, se evaluaron los supuestos de normalidad y multicolinealidad, considerando valores problemáticos de asimetría mayores a ± 3 y de curtosis superiores a ± 10 (Pérez et al., 2013). Además, se examinaron las correlaciones bivariadas entre las variables independientes y se calcularon los índices de tolerancia y el factor de inflación de la varianza (VIF), sin detectarse niveles problemáticos (Hair et al., 2019). Posteriormente, se estimaron análisis de regresión para cada variable dependiente (uso e intención de continuidad de uso) y para cada versión de las herramientas de GE (App y sitio web). Dado que el objetivo no fue validar un instrumento global, sino analizar el rol de explicativo de variables conceptualmente diferenciadas, se estimaron modelos de regresión múltiple mediante el método *stepwise*. En este procedimiento se incluyeron únicamente las variables con un $p < .05$, establecido como criterio de inclusión. Los análisis se realizaron con el Paquete Estadístico para Ciencias Sociales (Statistical Package for the Social Sciences, SPSS) versión 23.

3. Resultados

3.1. Conocimiento y versiones más usadas de las herramientas de GE

Del total de personas que respondieron, el 84% ($n = 877$) indicó conocer Mi Argentina (Tabla 2). De las cuales, el 50% indicó usar con mayor frecuencia la aplicación móvil. Respecto a CiDi, un 91% ($n = 948$) indicó conocer la herramienta, el 32% utilizó más la aplicación móvil, el 31% el sitio web y el 28% ambas por igual. Por último, sólo el 21% expresó conocer el Portal municipal.

	Mi Argentina			CiDi			Portal municipal
	App	Web	Ambas por igual	App	Web	Ambas por igual	
%	50.2	20.3	13.6	32.3	30.6	28	21.2
(n)	523	212	142	337	319	292	221
n	877			948			221

Nota. CiDi = Ciudadano Digital. App = aplicación móvil. Web = sitio web. Portal municipal = Portal de la ciudad de Córdoba. Los porcentajes se calculan considerando la cantidad total de personas que indicaron conocer cada herramienta digital de gobierno. Fuente de elaboración propia.

Tabla 2 – Conocimiento sobre plataformas y versión utilizada con mayor frecuencia.

3.2. Factores predictores del uso e intención de continuidad de uso de las herramientas de GE

Los índices de ajuste de todos los modelos, según variable dependiente y herramienta, así como los pasos intermedios de los análisis de regresión (*stepwise*), se presentan en el Anexo (ver Tablas 2 a 10). A continuación, se reportan únicamente los resultados correspondientes al último modelo seleccionado en cada análisis.

Uso de la herramienta.

Mi Argentina.

Aplicación Móvil.

El modelo 5 presentó el mejor ajuste ($R^2 = .091$, $F(5, 625) = 12.456$ $p = .031$, 95% IC [-1.948, .903]). Esto es, el uso de la aplicación móvil Mi Argentina fue explicada un 9.1% por la satisfacción ($B = .55$), el nivel educativo ($B = -.23$), el género mujer ($B = -.65$), el compromiso cívico ($B = .33$) y la participación online en actividades sociales ($B = .26$). A mayor satisfacción, compromiso cívico y participación online en actividades sociales, mayor uso de la aplicación Mi Argentina. Mientras que las personas que se identificaron como mujeres y quienes tenían más nivel educativo, usaron menos la aplicación (Tabla 3).

Sitio Web.

El modelo 1 presentó el mejor ajuste ($R^2 = .054$, $F(1,195) = 11.035$ $p = .001$, 95% IC [-1.26, .58]). El uso del sitio web Mi Argentina fue explicado un 5.4% por la satisfacción ($B = .44$). Es decir, las personas más satisfechas usaron más veces el sitio web Mi Argentina.

CiDi.**Aplicación Móvil.**

El modelo 4 presentó el mejor ajuste ($R^2 = .137$, $F(4, 595) = 23.614$, $p = .007$, 95% IC [-5.69, -2.04]). Esto es, el uso de la aplicación móvil CiDi fue explicada un 14% por la percepción de facilidad ($B = 1.34$), la edad ($B = .06$), género (otros) ($B = 16.30$) y compromiso cívico ($B = .60$). Es decir, a mayor percepción de facilidad, edad, género (otros) y compromiso cívico, mayor uso de la aplicación de CiDi.

Sitio Web.

El modelo 3 presentó el mejor ajuste ($R^2 = .127$, $F(3, 300) = 14.527$, $p < .001$, 95% IC [-8.74, -.77]). El uso del sitio web CiDi fue explicado un 13% por la percepción de facilidad ($B = 1.69$), el nivel educativo ($B = .96$) y la confianza en internet ($B = -.99$). Es decir, a mayor percepción de facilidad, mayor nivel educativo y menor confianza en internet, mayor uso del sitio web.

Portal del gobierno de la Ciudad de Córdoba.

El modelo 2 presentó el mejor ajuste ($R^2 = .148$, $F(2, 210) = 18.195$, $p = .011$, 95% IC [-1.47, .34]). El uso del portal fue explicado un 15% por la percepción de facilidad ($B = .76$) y el género otros ($B = 6.74$). Es decir, las personas que se identificaron con otro género y quienes percibieron más fácil el uso, usaron más el portal.

Intención de continuidad de uso.**Mi Argentina.****Aplicación Móvil.**

El modelo 5 presentó el mejor ajuste ($R^2 = .423$, $F(5, 625) = 91.787$, $p = .034$, 95% IC [.352, .863]). La intención de continuidad de uso de la aplicación móvil Mi Argentina fue explicada un 42% por la satisfacción ($B = .31$), la percepción de utilidad ($B = .28$), la confianza en el GE ($B = .13$), en internet ($B = .08$) y en el gobierno nacional ($B = .06$). A mayor satisfacción, percepción de utilidad, confianza en internet, en el GE, y en el gobierno nacional, mayor intención de continuar usando la App (Tabla 4).

Sitio Web.

El modelo 5 presentó el mejor ajuste ($R^2 = .474$, $F(5, 191) = 34.359$, $p < .001$, 95% IC [-27, .73]) indicando que la intención de continuidad de uso del sitio web Mi Argentina fue explicada un 47% por la satisfacción ($B = .33$), la percepción de utilidad ($B = .26$), el compromiso cívico ($B = .18$), la confianza en el GE ($B = .14$) y en el gobierno nacional ($B = .10$). Es decir, a mayor satisfacción, percepción de utilidad, compromiso cívico, confianza en el GE y en el gobierno nacional, mayor intención de continuar usando el Sitio web Mi Argentina.

CiDi.**Aplicación Móvil.**

El modelo 4 presentó el mejor ajuste ($R^2 = .527$, $F(4, 594) = 165.230$, $p = .001$, 95% IC [.629, 1.11]). Esto es, el uso de la aplicación móvil CiDi fue explicada fue explicada

Variables	Mi Argentina		Cidi		Portal municipal	
	App	Web	App	Web	Web	
	β	B (IC 95%)	β	B (IC 95%)	β	B (IC 95%)
<i>Cognitivas</i>						
Percepción de facilidad			1.34(.97;1.71)		1.69(1.08;2.30)	.76(.47;1.06)
Percepción de utilidad					.275***	.30***
Satisfacción	-.55(-.34;.77)	.195***	.44(.18;.70)	.23**		
Competencia digital						
<i>Sociocognitivas</i>						
Confianza en el gobierno						
Confianza en internet					-.99(-1.70;-.28)	-.15**
Confianza en el GE						
<i>Sociopolíticas</i>						
Compromiso cívico	.33(.13;.54)	.125**	.60(.16;1.03)		.11**	
Participación online en actividades sociales	.26(.02;.49)	.085*				
Participación online en actividades políticas						

Variables	Mi Argentina		CIDI		Portal municipal	
	App	Web	App	Web	Web	Web
<i>Sociodemográficas</i>						
Género	-0.65(-1.09; -.21)	-0.11**	16.30(6.72;25.86)	.13**	6.74(1.59;11.895)	.17*
Edad			.06(.02; .09)	.125**		
Nivel Educativo	-0.23(-.39; -.06)	-0.105**			.96(.41;1.50)	.19**
Nivel Socioeconómico						
Frecuencia de conexión a internet						
R^2_{Aj}	.08	.05	.13	.12	.14	
N	631	197	600	304	213	

Nota. CIDI = Ciudadano Digital, App = aplicación móvil, Web = sitio web, GE = Gobierno Electrónico, Portal municipal = Portal de la ciudad de Córdoba. * $p < .05$, ** $p < .01$, *** $p < .001$, N = muestra final eliminando casos atípicos uni y multivariado, B = coeficiente no estandarizado, β = coeficiente estandarizado, IC = intervalo de confianza, R^2_{Aj} = coeficiente de determinación ajustado. Fuente de elaboración propia.

Tabla 3 – Modelos finales de regresión múltiple para la variable uso de las herramientas de GE.

un 53% por la percepción de utilidad ($B = .35$), la satisfacción ($B = .25$), percepción de facilidad ($B = .12$, $p = .001$) y confianza en internet ($B = .10$). A mayor percepción de utilidad, facilidad, satisfacción y confianza en internet, mayor intención de continuidad de uso de la aplicación de CiDi.

Sitio Web.

El modelo 5 presentó el mejor ajuste ($R^2 = .549$, $F(5, 298) = 72.410$, $p = .009$, 95% IC [-.42, .52]) indicando que la intención de continuidad de uso del sitio web CiDi fue explicada en un 55% por la percepción de utilidad ($B = .32$), la percepción de facilidad ($B = .21$), la satisfacción ($B = .17$), la competencia digital ($B = .19$) y la confianza en el GE ($B = .16$). Es decir, a mayor percepción de utilidad, percepción de facilidad, satisfacción, competencia digital y confianza en el GE, mayor intención de continuidad de uso del sitio web CiDi.

Portal del gobierno de la Ciudad de Córdoba.

El modelo 3 presentó el mejor ajuste ($R^2 = .497$, $F(3, 209) = 68.845$, $p = .027$, 95% IC [.36, 1.18]) indicando que la intención de continuidad de uso del Portal fue explicada un 50% por la percepción de utilidad ($B = .41$), la satisfacción ($B = .27$) y confianza en internet ($B = .13$). Es decir, a mayor percepción de facilidad, satisfacción y confianza en internet, mayor intención de continuidad de uso del Portal.

5. Discusión

La presente investigación surge de la necesidad de comprender facilitadores en la adopción del gobierno electrónico (GE), desde una perspectiva ciudadana, especialmente en contextos del sur global, donde la brecha digital constituye una barrera significativa (Bwalya, 2017; Tellechea, 2018). A pesar del crecimiento en el desarrollo de herramientas digitales en Argentina, la adopción de estas plataformas continúa siendo desigual y limitada, especialmente en el nivel municipal. Si bien modelos teóricos como la TDI (Rogers, 1985) y el MAT (Davis, 1989) ofrecen marcos explicativos relevantes, los estudios previos han mostrado resultados inconsistentes (Botelho, 2019; Mercy et al., 2020). Por ello, este estudio se propuso explorar el rol de variables cognitivas, sociocognitivas, sociopolíticas y sociodemográficas en la adopción de tres plataformas de GE de diferentes niveles jurisdiccionales en Argentina.

Los resultados indican que las variables cognitivas (percepciones de facilidad, utilidad y satisfacción) son predictores robustos en la adopción del GE, en línea con lo que hipotetizamos, lo planteado por MAT e investigaciones previas a nivel local (Mola et al., 2021; Sorribas et al., 2022) e internacional (Botelho, 2019; Hamid et al., 2016; Inzunza Mejía & López Carmona, 2018). Asimismo, las confianzas en internet, gobierno y GE predijeron la adopción, en consonancia con investigaciones internacionales (p.ej., Tsui et al., 2019, Khan et al., 2020; López Sisniega et al., 2016) y nacionales (Alderete & Díaz, 2020). No obstante, las confianzas predijeron la intención de continuidad de uso y no el comportamiento de uso. Al respecto, Abu-Shanab (2014) resalta que las confianzas tienen un efecto indirecto en el uso, mediado por la intención de uso. Además, el efecto podría verse atenuado por factores cognitivos como el riesgo (Li, 2021). A su vez, para el uso de la versión web de CiDi, contrario a lo hipotetizado, se encontró una asociación

Variables	Mi Argentina			CiDi			Portal municipal		
	App	Web	App	Web	App	Web	App	Web	App
	B (IC 95%)	β	B (IC 95%)	β	B (IC 95%)	β	B (IC 95%)	β	B (IC 95%)
<i>Cognitivas</i>									
Percepción de facilidad			.12(.05;:20)	.14**	.21(.12;:30)	.25***			
Percepción de utilidad	.28(.22;:35)	.32***	.26 (.14;:37)	.285***	.35(.29;:41)	.39***	.32(.225;:41)	.34***	.41(.29;:52)
Satisfacción	.31(.23;:38)	.29***	.33(.195;:465)	.32***	.25(.17;:33)	.27***	.17(.04;:26)	.15**	.27(.14;:405)
Competencia digital					.19(.07;:32)	.12**			
<i>Sociocognitivas</i>									
Confianza en el gobierno	.06(.005;:11)	.07*	.10(.01;:19)	.12*					
Confianza en internet	.08(.01;:16)	.08*			.10(.04;:16)	.10**			.13(.015;:24)
Confianza en el GE	.13(.06;:20)	.14***	.14(.03;:25)	.15*			.16(.085;:24)	.17***	
<i>Sociopolíticas</i>									
Compromiso cívico			.18 (.07;:28)	.18**					
Participación online en actividades sociales									
Participación online en actividades políticas									

Variables	Mi Argentina		CiDi		Portal municipal	
	App	Web	App	Web	Web	
	β	B (IC 95%)	β	B (IC 95%)	β	B (IC 95%)
<i>Sociodemográficas</i>						
Género						
Edad						
Nivel Educativo						
Nivel Socioeconómico						
Frecuencia de conexión a internet						
R^2_{Aj}	.42	.46	.52	.54	.49	
N	631	197	599	304	213	

Nota. CiDi = Ciudadano Digital, App = aplicación móvil, Web = sitio web, GE = Gobierno Electrónico, Portal municipal = Portal de la ciudad de Córdoba * $p < .05$, ** $p < .01$, *** $p < .001$, N = muestra final eliminando casos atípicos uni y multivariado. B = coeficiente no estandarizado, β = coeficiente estandarizado, IC = intervalo de confianza, R^2_{Aj} = coeficiente de determinación ajustado. Fuente de elaboración propia

Tabla 4 – Modelos finales de regresión múltiple para la variable intención de continuar usando las herramientas de GE.

inversa con la confianza en internet. Este resultado podría vincularse con funcionalidades específicas de la herramienta o experiencias particulares de las personas usuarias (Khan et al., 2020).

También, los factores sociopolíticos como el compromiso cívico y la participación online emergieron como predictores en el uso del GE. En línea con lo esperado y con estudios previos, se observó que a mayor compromiso cívico y participación en actividades sociales como, proponer ideas para mejorar la comunidad o seguir y compartir enlaces en los medios sociales, mayor uso de GE (Bianchini et al., 2016; Mercy et al., 2020). Estas variables mostraron capacidad predictiva en las plataformas nacional (Mi Argentina) y provincial (CiDi) pero no en la municipal. Esto podría deberse al bajo nivel de conocimiento del Portal, el solapamiento de servicios con CiDi, y/o la menor diversidad de funcionalidades disponibles en la plataforma municipal.

Las variables sociodemográficas, en consonancia con TDI, explicaron la adopción del GE en algunos casos. Sin embargo, los resultados no son homogéneos, como señalan estudios previos (p.e., Alderete et al., 2024; Idris, 2016; Mukonza et al., 2016). La edad predijo el uso de la aplicación de CiDi, indicando un mayor uso por parte de personas más jóvenes, en línea con lo observado por Inzunza Mejía y López Carmona (2018). Además, el género resultó significativo. Por un lado, las mujeres usaron menos la app Mi Argentina, reflejando brechas digitales de género observadas previamente (Abu-Shanab 2015; Mukonza et al., 2016). Por otro lado, las personas que no se identificaron dentro del binarismo mujer/varón usaron más la app de CiDi y el Portal municipal. Estudios previos sugieren que colectivos disidentes desarrollan mayores competencias digitales para acceder a servicios, evitando interacciones presenciales potencialmente estigmatizantes (Eubanks, 2018; Scheuerman et al., 2019). Sin embargo, estos resultados deben interpretarse con cautela debido al tamaño muestral reducido de este subgrupo y la sobrerrepresentación de mujeres en la muestra (Tabachnick & Fidell, 2013). Futuras investigaciones que se propongan analizar diferencias según géneros podrán contrastar estos resultados empleando muestras equilibradas.

Asimismo, se observó que personas con mayor nivel educativo usaron más la versión web de CiDi y menos la app Mi Argentina. Esta diferencia podría relacionarse con las competencias y las prácticas digitales orientadas al capital cultural. Según Van Deursen y van Dijk (2014), las personas con mayor nivel educativo tienden a usar internet para actividades más complejas, como la búsqueda de información gubernamental. En este sentido, podrían preferir plataformas con interfaces más completas, como las versiones web, mientras que las apps, diseñadas para una navegación más rápida y simplificada, podrían ser más atractivas para otros perfiles de usuarios/as.

Este estudio no está exento de limitaciones. Primero, el muestreo utilizado no probabilístico, limita la representatividad y generalización de los resultados (Bologna, 2022). Además, la implementación online de la encuesta puede excluir a personas con acceso limitado a internet, pudiendo introducir sesgo muestral y reforzando la invisibilización de la desigualdad digital (Van Dijk, 2020). En esta línea, futuras investigaciones podrían incorporar estrategias muestrales mixtas y considerar poblaciones rurales. En Brasil, por ejemplo, se ha observado que los gobiernos locales urbanos cuentan con mayor infraestructura tecnológica, mejor conectividad a internet y mayor disponibilidad de dispositivos digitales. Mientras que, en los gobiernos locales

rurales, se han identificado mayores dificultades estructurales para la adopción del GE (Omweri, 2024).

6. Conclusión

El objetivo del estudio fue explorar los factores predictores de la adopción del GE en Córdoba (Argentina), considerando el uso y la intención de continuidad de uso. Los resultados indican que la adopción depende principalmente de variables cognitivas, como las percepciones de facilidad, utilidad y satisfacción. Asimismo, las confianzas en internet, gobierno y GE predijeron principalmente la intención de continuidad de uso sugiriendo que intervenciones orientadas a generar confianza y experiencias positivas iniciales podrían fortalecer la sostenibilidad del uso. Por su parte, el compromiso cívico y la participación online predijeron el comportamiento de uso, resaltando la importancia de comprender el GE como una práctica de ciudadanía digital. En conjunto, los resultados aportan evidencia empírica relevante para diseñar políticas públicas orientadas a promover la adopción del GE en Argentina, fortaleciendo las percepciones y confianzas e impulsando la participación y compromiso cívico en entornos digitales.

Financiamiento

Para realizar este trabajo se contó con subsidio de la Secretaría de Ciencia y Tecnología de la Universidad Nacional de Córdoba (FORMAR 2023-2025), otorgados a la primera autora.

Referencias

- Abu-Shanab, E. (2014). Antecedents of trust in e-government services: An empirical test in Jordan. *Transforming Government: People, Process and Policy*, 8(4), 480–499. <https://doi.org/10.1108/TG-08-2013-0027>
- Abu-Shanab, E. A. (2015). Gender and age: Moderators or predictors of E-government acceptance?. *International Journal of E-Adoption*, 7(1), 32–51. <http://dx.doi.org/10.4018/IJEA.2015010103>
- Alderete, M. V., & Díaz, L. (2020). ¿Participa la ciudadanía en el gobierno electrónico? El caso de la ciudad de Bahía Blanca, Argentina. *DAAPGE*, 20(34), 77–102. <https://doi.org/10.14409/daapge.v20i34.10058>
- Alderete, M. V., Díaz, L. A., & Álvarez, N. (2022). Gobierno electrónico mediante diferentes plataformas digitales en un grupo de ciudadanos de una ciudad de Argentina. *Revista de Investigación, Desarrollo e Innovación*, 12(2), 157–170. <https://doi.org/10.19053/20278306.v12.n2.2022.15255>
- Alderete, M. V., Díaz, L., & Gutiérrez, E. (2024). Análisis del gobierno electrónico desde el perfil de los ciudadanos: El caso de un municipio de Argentina. *Revista Iberoamericana de Ciencia, Tecnología y Sociedad-CTS*, 19(57), 161–180. <https://doi.org/10.52712/issn.1850-0013-407>

- Basri, N. H., Adnan, W. A. W., & Baharin, H. (2019). E-participation service in Malaysian e-government website: The user experience evaluation. In *Proceedings of the 10th international conference on E-education, E-business, E-management and E-learning* (pp. 342-346). <https://doi.org/10.1145/3306500.3306569>
- Becker, R. (2022). Gender and Survey Participation: An Event History Analysis of the Gender Effects of Survey Participation in a Probability-based Multi-wave Panel Study with a Sequential Mixed-mode Design. *Methods, Data, Analyses*, 16(1), 3–32 <https://majournals.bib.uni-mannheim.de/mda/article/view/2021.08/315>
- Bianchini, D., Fogli, D., & Ragazzi, D. (2016, October). Promoting citizen participation through gamification. In *Proceedings of the 9th Nordic Conference on Human-Computer Interaction* (pp. 1-4). <https://doi.org/10.1145/2971485.2971543>
- Boateng, G. O., Neilands, T. B., Frongillo, E. A., Melgar-Quinonez, H. R., & Young, S. L. (2018). Best practices for developing and validating scales for health, social, and behavioral research: A primer. *Frontiers in Public Health*, 6, 149. <https://doi.org/10.3389/fpubh.2018.00149>
- Bologna, E. (2022). *Un Recorrido por los Métodos Cuantitativos en Ciencias Sociales a bordo de R*. <https://estadisticacienciasocialesr.rbind.io/>
- Bothelo Simões, R. P. (2019). *Citizen engagement through city apps: Technology adoption approach*. Dissertação de mestrado, Iscte-Instituto Universitário de Lisboa. Repositório Iscte. <http://hdl.handle.net/10071/19406>
- Carter, L., Weerakkody, V., Phillips, B., & Dwivedi, Y. (2016). Citizen Adoption of E-Government Services: Exploring Citizen Perceptions of Online Services in the United States and United Kingdom. *Information Systems Management*, 33(2), 124-140, <https://doi.org/10.1080/10580530.2016.1155948>
- Centro latinoamericano para el Desarrollo (2016). Carta Iberoamericana de Gobierno Abierto. <https://clad.org/wp-content/uploads/2020/07/Carta-Iberoamericana-de-Gobierno-Abierto-07-2016.pdf>
- Consejo Nacional de Coordinación de Políticas Sociales (2021). Boletín Oficial. <https://www.boletinoficial.gob.ar/detalleAviso/primera/24263/20210405>
- Comisión de Enlace Institucional AAM-SAIMO-CEIM. (2015). *El nivel socioeconómico en la Argentina, 2015: Estratificación y variables*. Buenos Aires: Observatorio Social de SAIMO. <https://saimo.org.ar/wp-content/uploads/2023/09/Caracteristicas-de-la-Revision-2015-del-NSE-CEI-Junio-2015.pdf> Redalyc.org+4
- Corporación Latinobarómetro. (2020). *Informe Latinobarómetro 2020*. Santiago de Chile: Latinobarómetro. <https://www.latinobarometro.org/latinobarometro-2020>
- Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 319-340. <https://doi.org/10.2307/249008>

- Delfino, G., Beramendi, M., & Zubieta, E. (2019). Participación social y política en Internet y brecha generacional. *Revista de Psicología (PUCP)*, 37(1),195-216. <https://doi.org/10.18800/psico.201901.007>
- Díaz, L. A., & Gutierrez, E. M. (2021). Adopción de gobierno electrónico en Bahía Blanca durante el período 2019–2020: Un análisis exploratorio. Universidad de Buenos Aires, Facultad de Ciencias Sociales, Instituto de Investigaciones “Gino Germani”. <https://publicaciones.sociales.uba.ar/index.php/argumentos/article/view/6980>
- Ellard-Gray, A., Jeffrey, N. K., Choubak, M., & Crann, S. E. (2015). Finding the hidden participant: Solutions for recruiting hidden, hard-to-reach, and vulnerable populations. *International Journal of Qualitative Methods*, 14(5), 1-10. <https://doi.org/10.1177/1609406915621>
- Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
- Gallup Inc. (2018). *Gallup World Poll 2018*. Gallup Analytics. <https://news.gallup.com/reports/225587/rating-world-leaders-2018.aspx>
- George, D., & Mallery, P. (2001). *SPSS for Windows step by step: A simple guide and reference* (Version 11.0). Allyn & Bacon.
- Hamid, A. A., Razak, F. Z. A., Bakar, A. A., & Abdullah, W. S. W. (2016). The effects of perceived usefulness and perceived ease of use on continuance intention to use e-government. *Procedia economics and finance*, 35, 644-649. [https://doi.org/10.1016/S2212-5671\(16\)00079-4](https://doi.org/10.1016/S2212-5671(16)00079-4)
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.
- Hernández Sampieri R., Fernández C., & Baptiste L. (2014). *Metodología de la investigación* (6.ª ed.). McGraw Education.
- Idris, S. H. M., (2016). Significant Factors Determining E-government Adoption in Selangor, Malaysia. *Acta Universitatis Danubius*, 12(3), 163-172. <https://ideas.repec.org/a/dug/actaec/y2016i3p163-172.html>
- Instituto Nacional de la Administración Pública. (2022). *Tecnologías, información y derechos: Hacia una gestión documental con perspectiva archivística en la Administración Pública Nacional. Parte I. Cuadernos del INAP*, (97). https://www.argentina.gob.ar/sites/default/files/cuinap_97.pdf
- Inzunza Mejía, C., & López Carmona, A. M. (2018). Gobierno electrónico, accesibilidad y uso de la plataforma ciudadano digital en Sinaloa. *Revista Avacient*, 2(5), 27-45. <http://itchetumal.edu.mx/images/2019/Avacient/REVISTA-AVACIENT-VOL-5-JUL-DIC-2018-A.pdf#page=28>
- Jiménez Cortés, R., Vega Caro, L., & Vico Bosch, A. (2016). Habilidades en Internet de mujeres estudiantes y su relación con la inclusión digital: Nuevas brechas digitales. *Education in the Knowledge Society*, 17(3), 29-48. <https://www.torrossa.com/en/resources/an/3183403>

- Khan, S., Zairah, A., Rahim, N., & Maarop, N. (2020). A systematic literature review and a proposed model on antecedents of trust to use social media for e-government services. *International Journal of Advanced and Applied Sciences*, 7(2), 44–56. <https://doi.org/10.21833/ijaas.2020.02.007>
- Kumar, K., Mukerji, B., Butt, I., & Persaud, A. (2007). Factors for successful e-government adoption: A conceptual framework. *Electronic Journal of e-Government*, 5(1), 63–76. https://www.researchgate.net/publication/228796407_Factors_for_Successful_E-government_Adoption_A_Conceptual_Framework
- Lago Martínez, S. (2016). La inclusión digital como inclusión social: El papel de las políticas de estado. *Horizontes Sociológicos*, 4(8), 82-93. <http://aass.org.elsevier.com/ojs/index.php/hs/article/view/129>
- Li, W. (2021). The role of trust and risk in Citizens' E-Government services adoption: A perspective of the extended UTAUT model. *Sustainability*, 13(14), 7671. <https://doi.org/10.3390/su13147671>
- Li, W., & Xue, L. (2021). Analyzing the Critical Factors Influencing Post-Use Trust and Its Impact on Citizens' Continuous-Use Intention of E-Government: Evidence from Chinese Municipalities. *Sustainability*, 13(14), 7698. <https://doi.org/10.3390/su13147698>
- López-De Castro, S., & García Alonso, R. (2016). Ciudadanos y gobierno electrónico: la orientación al ciudadano de los sitios Web municipales en Colombia para la promoción de la participación. *Universitas humanística*, (82), 279-304. <https://doi.org/10.11144/Javeriana.uh82.cgeo>
- López-Sisniega, C., Gutierrez-Diez, M. C., & Arras-Vota, A. M. G., & Bordas-Beltrán, J. (2016). Barriers to the Use of Electronic Government as Perceived by Citizens at the Municipal Level in México. *International Journal of Management Excellence*, 7, 846-854. <https://doi.org/10.17722/ijme.v7i3.859>
- Mercy, S., Gayatri, G., Perez C., Manvita, B. (2020). Drivers and barriers to e- government adoption in Indian cities. *Journal of Urban Management*, 9(4), 408-417. <https://doi.org/10.1016/j.jum.2020.05.002>
- Mola, D. J., González, G., Molina, G., Ceaglio, S., & Reyna, C. (2021). Experiencia de los/as ciudadanos/as de Córdoba con la aplicación móvil “App Ciudadana”: Resultados preliminares. Presentado en el *Congreso Internacional de Gobierno Electrónico*, Universidad de la Sierra Sur, México. <https://gobiernoabierto.cordoba.gov.ar/conocimiento-abierto/informes/>
- Mola, D. J., González, G., & Reyna, C. (2022). Análisis teórico y empírico de indicadores de desigualdad en el Gobierno Electrónico. Presentado en *XVIII Reunión Nacional y VII Encuentro Internacional de la Asociación Argentina de Ciencias del Comportamiento*, Mar del Plata. <https://doi.org/10.32348/1852.4206.v.n.37344>
- Mola, D. J., & Reyna, C. (2022). Indicadores de desigualdad y Gobierno Electrónico: revisión sistemática y estado del arte. *Gestión Y Análisis De Políticas Públicas*, (30), 45–55. <https://doi.org/10.24965/gapp.10987>

- Morales-Urrutia, X., Morales-Urrutia, D., Simbaña-Taípe, L., & Guerrero-Valástegui, C. (2020). Desempeño del gobierno electrónico desde una perspectiva comparada a nivel mundial. *Revista Iberica de Sistemas e Tecnologías de Informacao*, (E29), 214-224.
- Morgado, F. F., Meireles, J. F., Neves, C. M., Amaral, A., & Ferreira, M. E. (2017). Scale development: ten main limitations and recommendations to improve future research practices. *Psicologia: Reflexão e Crítica*, 29(1), 1–15. <https://doi.org/10.1186/s41155-016-0057-1>
- Mota, E., Silva, R., & Pereira, L. (2022). Adoção do governo eletrônico: um estudo sobre o papel da confiança. *Revista de Administração Pública*, 54(1), 123–140. <https://doi.org/10.1590/0034-761220220027>
- Mukonza, R., M., Maserumule, M. H., & Moeti, K. B. (2016). A critical examination of socioeconomic and demographic factors as determinants of e-government adoption among residents in Zimbabwe's two local authorities. *African Journals Online*, 46(2), 1-16. <https://hdl.handle.net/10520/EJC196337>
- Mustafa, A. A., Faizal, M. A. & Nurul, A. Z. (2019). E-government adoption success factors and their weight analysis: A citizen perspective. *Journal of Theoretical and Applied Information Technology*, 97, 583-597.
- Naser, A., Williner, A., & Sandoval, C. (2021). *Participación ciudadana en los asuntos públicos: Un elemento estratégico para la Agenda 2030 y el gobierno abierto* (Documentos de Proyectos, LC/T.S.2020/184). Comisión Económica para América Latina y el Caribe (CEPAL). <https://www.cepal.org/es/publicaciones/46645-participacion-ciudadana-asuntos-publicos-un-elemento-estrategico-la-agenda-2030>
- Nguyen, D. T., Bui, N. M., Pham, T. N., Vuong, L. L., Dao, M. P., & Nguyen, H. A. (2025). Understanding continuous intention to use e-government services: integration of expectation confirmation theory and technology acceptance theory 2. *Journal of Science and Technology Policy Management*, 2(12). <https://doi.org/10.1108/JSTPM-11-2024-0434>
- Omweri, F. S. (2024). A Systematic Literature Review of E-Government Implementation in Developing Countries: Examining Urban-Rural Disparities, Institutional Capacity, and Socio-Cultural Factors in the Context of Local Governance and Progress towards SDG 16.6. *International Journal of Research and Innovation in Social Science*, 8(8), 1173-1199. <https://dx.doi.org/10.47772/IJRISS.2024.808088>
- Pérez, J., Martínez, R., & Gómez, L. (2013). *Análisis estadístico aplicado a las ciencias sociales*. Editorial Académica Española.
- Pérez-Morote, R., Pontones-Rosa, C., & Núñez-Chicharro, M. (2020). The effects of e-government evaluation, trust and the digital divide in the levels of e-government use in European countries. *Technological Forecasting and Social Change*, 154, 119973. <https://doi.org/10.1016/j.techfore.2020.119973>.
- Rogers, E. M. (1995). *Diffusion of innovations*. (4th ed). The Free Press.

- Schaupp, L., & Carter, L. (2010). The impact of trust, risk and optimism bias on e-file adoption. *Information Systems Frontiers*, 12(3), 299–309. <https://doi.org/10.1007/s10796-008-9138-8>
- Schradie, J. (2011). The digital production gap: The digital divide and Web 2.0 collide. *Poetics*, 39(2), 145–168. <https://doi.org/10.1016/j.poetic.2011.02.003>
- Scheuerman, M. K., Paul, J. M., & Brubaker, J. R. (2019). How computers see gender: An evaluation of gender classification in commercial facial analysis services. *Proceedings of the ACM on Human-Computer Interaction*, 3, 1-33. <https://doi.org/10.1145/3359246>
- Sorribas, P. M., Gutierrez, M. C., Mola, D. J., & Reyna, Z. M. G. (2022). Dos caras de la participación ciudadana: análisis sobre la inclusión-exclusión política en instancias presenciales y mediadas por aplicaciones. *Administración Pública y Sociedad*, (13), 141-175. <https://revistas.unc.edu.ar/index.php/APyS/article/view/37496/38096>
- Tabachnick, B. G., & Fidell, L. S. (2014). *Using multivariate statistics* (6th ed.). Pearson.
- Tellechea, T. (2018). *El gobierno electrónico como derecho y la brecha digital en Argentina*. Informe Integrar. http://sedici.unlp.edu.ar/bitstream/handle/10915/72251/Documento_completo.pdf-PDFA.pdf?sequence=1
- Teo, T., Srivastava, S. & Jiang, L. (2008). Trust and electronic government success: An empirical study. *Journal of Management Information Systems*, 25(3), 99–131. <https://doi.org/10.2753/MISO742-1222250303>
- Tsui, H. D. (2019). Trust, perceived usefulness, attitude and continuance intention to use e-government service: An empirical study in Taiwan. *IEICE Transactions on Information and Systems*, 102(12), 2524–2534. <https://doi.org/10.1587/transinf.2019EDP7055>
- Urbina, A. U., & Abe, N. (2017). Citizen-centric perspective on the adoption of E-government in the Philippines. *Electronic Journal of eGovernment*, 15(2), 63–83. <https://academic-publishing.org/index.php/ejeg/article/view/641>
- Van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2014). The digital divide shifts to differences in usage. *New Media & Society*, 16(3), 507–526. <https://doi.org/10.1177/1461444813487959>
- Van Dijk, J. A. G. M. (2020). *The Digital Divide*. Polity Press.
- Wangpipatwong, S., Chutimaskul, W., & Papisratorn, B. (2008). Understanding citizen's continuance intention to use e-government website: A composite view of technology acceptance model and computer self-efficacy. *The Electronic Journal of e-Government*, 6(1), 55–64.
- Yuni, J. A. & Urbano, C.A. (2014). *Técnicas para investigar. Recursos metodológicos para la preparación de proyectos de investigación*. Editorial Bruja

Anexos

Variables	Ítems	Autor
Frecuencia de conexión a internet	1. ¿Cuántos días a la semana te conectas a Internet?	Delfino et al. (2019)
	2. En un día típico, ¿cuántas horas estás conectado/a a Internet?	
	3. En el transcurso de un día normal, ¿Siempre estás conectado/a a Internet?	
Percepción de facilidad	1. Me resulta fácil obtener la información que quiero de (nombre de la herramienta de GE).	Wangpipatwong et al., (2008)
	2. Me resulta fácil completar una transacción a través de (nombre de la herramienta de GE).	
	3. Me resulta fácil seguir la organización y la estructura de (nombre de la herramienta de GE).	
Percepción de utilidad	1. El uso de (nombre de la herramienta de GE) me permite realizar más rápido las tareas.	Wangpipatwong et al. (2008)
	2. El uso de (nombre de la herramienta de GE) puede reducir los gastos de viaje.	
	3. El uso de (nombre de la herramienta de GE) puede reducir el tiempo de viaje y las filas.	
Percepción de satisfacción	En general, ¿cómo califica el grado de satisfacción de la experiencia que tuvo con (nombre de la herramienta)?	Mola et al. (2021)
Competencia digital	1. Administro y consulto mi cuenta bancaria.	Jimenez Cortés et al. (2016)
	2. Realizo compras online de productos y servicios (viajes, hoteles, ropa, libros, teatros, cine, etc.).	
	3. Realizo gestiones administrativas por Internet (estudios, salud, etc.).	
	4. Me comunico por Internet para preguntar por productos y servicios.	
	5. Marco como favoritos los sitios web y servicios que veo útiles.	
	6. Publico contenidos originales propios en Internet.	
	7. Creo y comparto fotos y/o vídeos por Internet.	
	8. Creo y mantengo páginas webs, blogs y/o canales de YouTube propios sobre temas de mi interés.	
	9. Participo en foros y redes sociales para comunicarme y estar informado/a.	
	10. Aprendo a resolver tareas usando tutoriales de Internet.	
	11. Utilizo los comentarios de otras personas en Internet para resolver dudas.	
	12. Acudo a servicios de ayuda técnica para resolver problemas.	
	13. Realizo copias periódicas de seguridad en dispositivos externos (como pendrives o discos externos).	

Variables	Ítems	Autor
Competencia digital	14. Configuro las opciones de privacidad para proteger mis datos personales.	Jimenez Cortés et al. (2016)
	15. Descargo e instalo programas de sitios web que son seguros.	
	16. Comparto contenidos en Internet respetando la propiedad intelectual (es decir, informando que son de otras personas).	
	17. Utilizo Google (u otro motor de búsqueda) para encontrar la información que necesito.	
	18. Uso correo electrónico, videollamadas y mensajería instantánea (como Messenger) para comunicarme por Internet.	
Conocimiento en el GE	1. Conozco (nombre de la herramienta de GE).	Alderete & Díaz, (2020)
	2. Indica qué versión utilizas con mayor frecuencia.	
Confianza en el gobierno	A continuación, indica tu nivel de confianza para cada una de las siguientes instituciones:	Segovia et al. (2008)
	1. Gobierno Nacional	
	2. Gobierno Provincial	
	3. Gobierno Municipal	
Confianza en internet	1. Internet es lo suficientemente seguro para que me sienta cómodo/a al usarlo en interacciones con el gobierno.	Mota et al. (2016)
	2. Estoy seguro/a de que los recursos legales y tecnológicos son suficientes para protegerme de los problemas en Internet.	
	3. En general, Internet es un entorno sólido y seguro para realizar transacciones con el gobierno.	
Confianza en el GE	1. El servicio de gobierno electrónico es confiable.	Tsui et al. (2019)
	2. El servicio de gobierno electrónico me parece honesto y fidedigno.	
	3. Creo que el servicio de gobierno electrónico no me perjudicará.	
Compromiso cívico	1. Me siento parte de la comunidad donde vivo.	Mota et al. (2016)
	2. Propongo ideas para mejorar la comunidad donde vivo.	
	3. Participo en actividades para mejorar la comunidad donde vivo.	
	4. Trabajo con otras personas para mejorar la comunidad donde vivo.	
	5. Siento la necesidad de ayudar a mejorar mi comunidad/localidad.	
Participación online en actividades sociales	1. Leer lo que postean otros/as.	Delfino et al. (2019)
	2. Postear sus comentarios.	
	3. Mirar videos creados por otros/as.	
	4. Seguir y compartir links de sitios de Internet en los medios sociales.	
	5. Compartir información no política en Internet (comercial, social).	

VARIABLES	Ítems	Autor
Participación online en actividades políticas	1. Firmar o compartir una petición en Internet.	Delfino et al. (2019)
	2. Compartir información política en Internet (noticias, fotos, videos, etc.).	
	3. Poner “me gusta” o seguir temas o grupos políticos en los medios sociales.	
	4. Unirse a un grupo político o a un grupo relacionado con una causa social en los medios sociales.	
	5. Crear un grupo político o relacionado con una causa social en los medios sociales.	
Uso de GE	1. En el último mes, ¿cuántas veces has utilizado (nombre de la herramienta de GE)?	Mola et al. (2021); Urbina & Abe, (2017)
Intención de continuidad de uso de GE	1. En el futuro no dudaría en usar (nombre de la herramienta de GE).	Alzharani, (2018); Wangpipatwong et al. (2008)
	2. En el futuro consideraré (nombre de la herramienta de GE) como primera opción para contactar al gobierno.	
	3. En el futuro aumentaré el uso de (nombre de la herramienta de GE).	
	4. Tengo la intención de continuar usando (nombre de la herramienta de GE) en vez de usar medios alternativos (por ejemplo, relacionarme presencialmente con el gobierno)	

Nota. GE = Gobierno Electrónico. Fuente: elaboración propia.

Tabla 1 – Ítems para medir las variables estudiadas.

Pasos y predictores					
	B (IC 95%)	EE	β	R²	R²Aj
<i>Modelo 1</i>				.049	.047
Satisfacción	.63 (.41, .85)	.11	.22***		
<i>Modelo 2</i>				.062	.059
Satisfacción	.58 (.36, .80)	.11	.20***		
Compromiso Cívico	.31 (.10, .51)	.10	.115**		
<i>Modelo 3</i>				.074	.070
Satisfacción	.575 (.36, .79)	.11	.20***		
Compromiso Cívico	.35 (.14, .56)	.105	.13**		
Nivel educativo	-.24 (-.40, -.08)	.08	-.11***		
<i>Modelo 4</i>				.084	.078
Satisfacción	.57 (.35, .78)	.11	.20***		
Compromiso cívico	.37 (.16, .57)	.10	.14***		
Nivel educativo	-.25 (-.41, -.08)	.08	-.11***		
Género Mujer	-.58 (-1.02, -.14)	.22	-.10*		

Pasos y predictores					
	B (IC 95%)	EE	β	R²	R²Aj
<i>Modelo 5</i>				.091	.083
Satisfacción	.55 (.34, .77)	.11	.195***		
Compromiso cívico	.33 (.13, .54)	.105	.125**		
Nivel educativo	-.23 (-.39, -.06)	.08	-.105***		
Género Mujer	-.65 (-1.09, -.21)	.23	-.11***		
Participación online en actividades sociales	.26 (.02, .49)	.12	.085*		

Nota. N = 631. EE = error estándar, * $p < .05$, ** $p < .01$, *** $p < .001$. Fuente: elaboración propia.

Tabla 2 – Modelos de regresión para predecir el uso de la App mi Argentina.

Pasos y predictores					
	B (IC 95%)	EE	β	R²	R²Aj
<i>Modelo 1</i>				.288	.287
Satisfacción	.57 (.50, .64)	.035	.54***		
<i>Modelo 2</i>				.377	.375
Satisfacción	.38 (.30, .455)	.04	.36***		
Percepción de utilidad	.31 (.25, .38)	.03	.35***		
<i>Modelo 3</i>				.413	.410
Satisfacción	.32 (.25, .40)	.04	.31***		
Percepción de utilidad	.285 (.22, .35)	.03	.32***		
Confianza GE	.19 (.13, .255)	.03	.20***		
<i>Modelo 4</i>				.419	.416
Satisfacción	.32 (.24, .39)	.04	.30***		
Percepción de utilidad	.29 (.22, .35)	.03	.32***		
Confianza en el GE	.15 (.07, .22)	.04	.15***		
Confianza en internet	.09 (.02, .16)	.04	.09*		
<i>Modelo 5</i>				.423	.419
Satisfacción	.31 (.23, .38)	.04	.29***		
Percepción de utilidad	.28 (.22, .35)	.03	.32***		
Confianza en el GE	.13 (.06, .20)	.04	.14***		
Confianza en internet	.08 (.01, .16)	.04	.08*		
Confianza en el gobierno nacional	.06 (.005, .11)	.03	.07*		

Nota. N = 631. EE = error estándar, GE = Gobierno Electrónico, * $p < .05$, ** $p < .01$, *** $p < .001$. Fuente: elaboración propia.

Tabla 3 – Modelos de regresión para predecir la intención de continuar usando la App Mi

Argentina.

Pasos y predictores					
	B (IC 95%)	EE	β	R²	R²Aj
<i>Modelo 1</i>				.320	.317
Satisfacción	.59 (.47, .71)	.06	.57***		
<i>Modelo 2</i>				.392	.386
Satisfacción	.39 (.25, .53)	.07	.38***		
Percepción de utilidad	.29 (.17, .42)	.06	.33***		
<i>Modelo 3</i>				.435	.426
Satisfacción	.385 (.25, .52)	.07	.37***		
Percepción de utilidad	.27 (.15, .39)	.06	.30***		
Compromiso Cívico	.21 (.10, .32)	.055	.21***		
<i>Modelo 4</i>				.460	.449
Satisfacción	.35 (.21, .48)	.07	.33***		
Percepción de utilidad	.25 (.14, .37)	.06	.28***		
Compromiso cívico	.19 (.08, .30)	.05	.19**		
Confianza en el GE	.16 (.055, .27)	.05	.17**		
<i>Modelo 5</i>				.474	.460
Satisfacción	.33 (.195, .465)	.07	.32***		
Percepción de utilidad	.26 (.14, .37)	.06	.285***		
Compromiso cívico	.18 (.07, .28)	.05	.18**		
Confianza en el GE	.14 (.03, .25)	.055	.15*		
Confianza en el gobierno nacional	.10 (.01, .19)	.05	.12*		

Nota. N = 197. EE = error estándar, GE = Gobierno Electrónico, *p < .05, **p < .01, ***p < .001. Fuente: elaboración propia.

Tabla 4 – Modelos de regresión para predecir la intención de continuar usando del Sitio web Mi Argentina.

Pasos y predictores					
	B (IC 95%)	EE	β	R²	R²Aj
<i>Modelo 1</i>				.092	.091
Percepción de facilidad	1.48 (1.11, 1.86)	.19	.30***		
<i>Modelo 2</i>				.112	.109
Percepción de facilidad	1.44 (1.07, 1.18)	.19	.30***		
Edad	.06 (.03, .10)	.02	.14***		
<i>Modelo 3</i>				.126	.122

Pasos y predictores					
	B (IC 95%)	EE	β	R²	R²Aj
Percepción de facilidad	1.43 (1.06, .1.80)	.19	.29***		
Edad	.06 (.03, .10)	.02	.14***		
Género (Otros)	15.55 (5.93, .25.16)	4.89	.12**		
<i>Modelo 4</i>				.137	.131
Percepción de facilidad	1.34 (.97, 1.71)	.19	.275***		
Edad	.06 (.02, .09)	.02	.125***		
Género (Otros)	16.30 (6.72, 25.88)	4.88	.13***		
Compromiso cívico	.60 (.16, 1.03)	.22	.11**		

Nota. N = 600. EE = error estándar, *p < .05, **p < .01, ***p < .001. Fuente: elaboración propia.

Tabla 5 – Modelos de regresión para predecir el uso de la App CiDi.

Pasos y predictores					
	B (IC 95%)	EE	β	R²	R²Aj
<i>Modelo 1</i>				.417	.416
Percepción de utilidad	.57 (.52, .63)	.03	.65***		
<i>Modelo 2</i>				.509	.507
Percepción de utilidad	.37 (.31, .44)	.03	.42***		
Satisfacción	.35 (.29,.42)	.03	.38***		
<i>Modelo 3</i>				.518	.516
Percepción de utilidad	.37 (.31, .44)	.03	.42***		
Satisfacción	.33 (.27, .40)	.03	.36***		
Confianza en internet	.11 (.05, .17)	.03	.10***		
<i>Modelo 4</i>				.527	.523
Percepción de utilidad	.35 (.29, .41)	.03	.39***		
Satisfacción	.25 (.17, .33)	.04	.27***		
Confianza en internet	.10 (.04, .16)	.03	.10**		
Percepción de facilidad	.12 (.05, .20)	.04	.14**		

Nota. N = 599. EE = error estándar, *p < .05, **p < .01, ***p < .001. Fuente: elaboración propia.

Tabla 6 – Modelos de regresión para predecir la intención de continuar usando la App CiDi

Pasos y predictores					
	B (IC 95%)	EE	β	R²	R²Aj
<i>Modelo 1</i>				.07	.067
Percepción de facilidad	1.50 (.88, 2.12)	.31	.26***		

Pasos y predictores					
	B (IC 95%)	EE	β	R²	R²Aj
<i>Modelo 2</i>				.105	.099
Percepción de facilidad	1.56 (.95, 2.17)	.31	.27***		
Nivel educativo	.96 (.41, 1.51)	.28	.19***		
<i>Modelo 3</i>					.118
Percepción de facilidad	1.69 (1.08, 2.30)	.31	.30***		
Nivel educativo	.96 (.41, 1.50)	.28	.19**		
Confianza en internet	-.99 (-1.70, .28)	.36	-.15**		

Nota. N = 304. EE = error estándar, * $p < .05$, ** $p < .01$, *** $p < .001$. Fuente: elaboración propia

Tabla 7 – Modelos de regresión para predecir el uso del Sitio web CiDi

Pasos y predictores					
	B (IC 95%)	EE	β	R²	R²Aj
<i>Modelo 1</i>				.394	.392
Percepción de utilidad	.59 (.51, .68)	.04	.63***		
<i>Modelo 2</i>				.493	.49
Percepción de utilidad	.40 (.31, .49)	.05	.43***		
Percepción de facilidad	.31 (.23, .39)	.04	.37***		
<i>Modelo 3</i>				.523	.519
Percepción de utilidad	.38 (.29, .47)	.04	.40***		
Percepción de facilidad	.29 (.21, .37)	.04	.34***		
Confianza GE	.18 (.10, .26)	.04	.18***		
<i>Modelo 4</i>				.538	.532
Percepción de utilidad	.35 (.27, .44)	.04	.37***		
Percepción de facilidad	.27 (.20, .35)	.04	.33***		
Confianza GE	.18 (.10, .25)	.04	.18***		
Competencia digital	.20 (.07, .33)	.06	.13**		
<i>Modelo 5</i>				.549	.541
Percepción de utilidad	.32 (.225, .41)	.05	.34***		
Percepción de facilidad	.21 (.12, .30)	.05	.25***		
Confianza GE	.16 (.08, .24)	.04	.17***		
Competencia digital	.19 (.07, .32)	.06	.12**		
Satisfacción	.17 (.04, .26)	.06	.15**		

Nota. N = 304. GE = Gobierno Electrónico, EE = error estándar, * $p < .05$, ** $p < .01$, *** $p < .001$. Fuente: elaboración propia

Tabla 8 – Modelos de regresión para predecir la intención de continuar usando el Sitio web CiDi.

Pasos y predictores					
	B (IC 95%)	EE	β	R²	R²Aj
<i>Modelo 1</i>				.121	.117
Percepción de facilidad	.81 (.515, 1.11)	.15	.35***		
<i>Modelo 2</i>				.148	.140
Percepción de facilidad	.76 (.47, 1.06)	.15	.33***		
Género (otros)	6.74 (1.59, 11.895)	2.61	.17*		

Nota. N = 213. EE = error estándar, * $p < .05$, ** $p < .01$, *** $p < .001$. Fuente: elaboración propia

Tabla 9 – Modelos de regresión para predecir el uso del Portal del gobierno de la Ciudad de Córdoba.

Pasos y predictores					
	B (IC 95%)	EE	β	R²	R²Aj
<i>Modelo 1</i>				.448	.445
Percepción de utilidad	.58 (.49, .67)	0.04	.70***		
<i>Modelo 2</i>				.485	.48
Percepción de utilidad	.43 (.32, .54)	0.06	.49***		
Satisfacción	.27 (.13, .40)	0.07	.26***		
<i>Modelo 3</i>				.497	.49
Percepción de utilidad	.41 (.29, .52)	0.06	.47***		
Satisfacción	.27 (.14, .405)	0.07	.26***		
Confianza en internet	.13 (.015, .24)	0.06	.11*		

Nota. N = 213. EE = error estándar, * $p < .05$, ** $p < .01$, *** $p < .001$. Fuente: elaboración propia

Tabla 10 – Modelos de regresión para predecir la intención de continuar usando del Portal del gobierno de la Ciudad de Córdoba.

Institucionalização da telemedicina: a estrutura iTAM-Health e evidências do sistema de saúde ULSS3

Riccardo Maria Santovito¹, Maria José Sousa²

riccardom.santovito@unive.it; maria.jose.sousa@iscte-iul.pt

¹ Venice School of Management, Università Ca' Foscari Venezia, 30121 Venezia, Italia

² ISCTE – University Institute of Lisbon, Business Research Unit (BRU-IUL), 1649-026 Lisboa, Portugal

DOI: [10.17013/risti.60.34-56](https://doi.org/10.17013/risti.60.34-56)

Resumo: A adoção da telemedicina nos sistemas públicos de saúde é um processo complexo, moldado por dinâmicas institucionais, organizacionais e relacionais mais do que pela tecnologia. Este estudo investiga os mecanismos que influenciam a confiança, a utilidade percebida, a facilidade de uso, as condições facilitadoras e a eficiência na implementação da telemedicina, aplicando o modelo iTAM-Health e uma lente realista crítica ao caso ULSS 3 Serenissima (Véneto, Itália). Utilizou-se um desenho qualitativo de múltiplas fontes, incluindo entrevistas com chefes de cardiologia, análise documental e triangulação empírica. A codificação assistida por IA identificou quatro mecanismos geradores: (1) estabilização normativa; (2) alinhamento sociotécnico; (3) valorização funcional; e (4) feedback institucional. Os resultados mostram a adoção como um ciclo coprodutivo no qual tecnologias e instituições se reforçam mutuamente. A integração entre iTAM-Health e realismo crítico oferece uma estrutura para compreender e governar a saúde digital com foco em sustentabilidade, valor público e responsabilidade institucional.

Palavras-chave: Telemedicina; Confiança Institucional; iTAM-Health; Sistemas Sociotécnicos; Governação da Saúde Digital.

Institutionalization of telemedicine: the iTAM-Health structure and evidence from the ULSS3 healthcare system

Abstract: The adoption of telemedicine in public healthcare systems is a complex and multilayered process shaped less by technology than by institutional, organizational, and relational dynamics. This study examines the mechanisms influencing trust, perceived usefulness, perceived ease of use, facilitating conditions, and efficiency in the implementation of telemedicine, applying the iTAM-Health model and a critical realist lens to the case of ULSS 3 Serenissima (Veneto, Italy). A multi-source qualitative design was used, including interviews with cardiology department heads, document analysis, and empirical triangulation. AI-assisted coding identified four generative mechanisms: (1) normative stabilization; (2) sociotechnical alignment; (3) functional valorization; and (4) institutional feedback. Findings show adoption as a co-productive cycle in which technologies and institutions mutually reinforce each other. The integration of iTAM-Health with

critical realism offers a comprehensive framework to understand and govern digital health as an ecosystem grounded in sustainability, public value, and institutional accountability.

Keywords: Telemedicine; Institutional Trust; iTAM-Health; Sociotechnical Systems; Digital Healthcare Governance.

1. Introdução

Nos últimos anos, os serviços de saúde públicos europeus passaram por uma transformação digital sem precedentes. A pandemia da COVID-19 atuou como um catalisador para um processo já em andamento, forçando os sistemas de saúde a garantir a continuidade dos cuidados, a segurança dos pacientes e a sustentabilidade organizacional por meio do uso de soluções digitais (Comissão Europeia, 2022; Greenhalgh et al., 2020). Na Itália, o Plano Nacional de Recuperação e Resiliência (PNRR) e a reforma dos cuidados comunitários posicionaram a telemedicina no centro das estratégias de modernização do Serviço Nacional de Saúde, promovendo a sua integração estável nas vias clínicas e nos níveis essenciais de cuidados (Ministero della Salute, 2023).

No entanto, essa transformação não pode ser reduzida a um problema puramente técnico ou infraestrutural. A adoção de tecnologias digitais na área da saúde requer uma profunda reformulação das relações de confiança, das formas de coordenação institucional e das competências profissionais que tornam possível o atendimento mediado digitalmente (Ross et al., 2021; Shaw et al., 2018). A literatura sobre o Modelo de Aceitação da Tecnologia (TAM) (Davis, 1989) e as suas extensões no domínio da saúde eletrônica (Holden & Karsh, 2010; Maillet et al., 2015) mostrou que a utilidade percebida, a facilidade de utilização percebida e a confiança são antecedentes fundamentais da intenção comportamental e do comportamento relacionado com a tecnologia. No entanto, em contextos públicos complexos, estas dimensões ao nível individual entrelaçam-se com fatores estruturais — normas, recursos, infraestruturas e culturas profissionais — que modulam a sua força e direção. Compreender tais interdependências significa mudar o foco analítico de se as tecnologias são adotadas para como e por que razão a sua adoção ocorre, persiste ou falha.

Nesse cenário, o caso da ULSS 3 Serenissima — que inclui os hospitais de Veneza, Mestre e Mirano — oferece um contexto empiricamente significativo. A organização foi uma das primeiras na região de Veneto a integrar a telemedicina aos serviços de cardiologia e cuidados comunitários, desenvolvendo programas de telemonitoramento e teleconsulta que agora envolvem centenas de pacientes crónicos. A região de Veneto, por meio da Azienda Zero e da Resolução 775/2023, também definiu um modelo de governança digital que promove a interoperabilidade, a segurança e a padronização de plataformas. A combinação de impulso institucional, maturidade tecnológica e resistência organizacional torna a experiência da ULSS 3 um laboratório ideal para explorar os mecanismos que possibilitam ou dificultam a adoção sustentável da telemedicina na saúde pública.

Para interpretar essa dinâmica, este estudo aplica o modelo iTAM-Health (Integrated Technology Acceptance Model for Healthcare), uma extensão do TAM projetada especificamente para o setor de saúde. O modelo propõe uma interpretação sistémica

da adoção de tecnologia, estruturada em torno de seis conceitos principais: confiança/segurança percebida, condições facilitadoras, facilidade de uso percebida, utilidade percebida, intenção comportamental e resultados de eficiência. A interação entre esses conceitos permite compreender não apenas as motivações individuais para o uso, mas também os resultados organizacionais decorrentes da operação sustentada das tecnologias digitais de saúde.

Epistemologicamente, o estudo baseia-se no realismo crítico (Bhaskar, 1978; Danermark et al., 2019), uma perspectiva que concebe a realidade social como estratificada e governada por mecanismos geradores que operam abaixo da superfície empírica. Nesta visão, a adoção da telemedicina não é interpretada como uma mera decisão ou comportamento, mas como o resultado de interações multifacetadas entre atores, tecnologias e estruturas institucionais. O realismo crítico permite-nos, assim, distinguir entre o que é observável – práticas, atitudes, dados de utilização – e as condições subjacentes que os tornam possíveis: confiança institucional, capacidades organizacionais, recursos tecnológicos e normas profissionais. A análise destes níveis revela os mecanismos causais que geram a adoção, resistência ou transformação das práticas digitais.

Empiricamente, a investigação segue um desenho qualitativo multissource realizado dentro da ULSS 3 Serenissima. Foram realizadas entrevistas semiestruturadas com chefes de departamentos de cardiologia, complementadas por análise documental e triangulação com dados de desempenho institucional. A análise de dados empregou a Análise de Estrutura (Ritchie & Spencer, 1994), apoiada por codificação assistida por IA (OpenAI, 2025), o que permitiu a combinação de rigor metodológico e profundidade interpretativa.

O estudo aborda três questões principais de investigação: (1) como é que a confiança é construída e mantida na telemedicina pública? (2) Que relações existem entre as condições facilitadoras, a usabilidade e a utilidade percebida na formação da intenção comportamental? (3) Em que medida a telemedicina gera resultados de eficiência organizacional no contexto dos cuidados de saúde comunitários de Veneto?

De modo geral, este artigo tem como objetivo fornecer uma compreensão integrada dos processos de adoção digital na saúde pública, oferecendo uma extensão empiricamente fundamentada do modelo iTAM-Health e uma estrutura epistemológica capaz de explicar não apenas se as tecnologias são adotadas, mas como e por que a adoção se desenrola. Através da análise do caso ULSS 3 Serenissima, este trabalho contribui para o debate internacional sobre confiança, governança e sustentabilidade da telemedicina, fornecendo evidências relevantes tanto para a reflexão teórica sobre a aceitação da tecnologia na saúde quanto para a formulação de políticas públicas orientadas para a inovação e o atendimento centrado na pessoa.

2. Estrutura teórica

A adoção da telemedicina nos sistemas públicos de saúde representa um campo privilegiado para observar como a inovação tecnológica, a confiança institucional e a cultura profissional interagem na transformação da prestação de cuidados de saúde. A literatura sobre a adoção da saúde eletrônica tem demonstrado amplamente que o

sucesso das inovações digitais não depende apenas da disponibilidade tecnológica, mas da capacidade das organizações de construir ambientes propícios baseados na confiança, usabilidade e utilidade percebida (Greenhalgh et al., 2017; Ross et al., 2021).

Neste contexto mais amplo, modelos teóricos como o Modelo de Aceitação da Tecnologia (TAM) (Davis, 1989) e as suas extensões subsequentes (Venkatesh et al., 2003, 2012) forneceram ferramentas analíticas sólidas, mas muitas vezes revelaram-se demasiado limitadas para captar a natureza sistémica e multinível dos cuidados de saúde públicos, onde as decisões individuais estão incorporadas em processos institucionais e lógicas de governação.

Para superar essas limitações, o presente estudo adota o iTAM-Health (Modelo Integrado de Aceitação de Tecnologia para Cuidados de Saúde), concebido para integrar as contribuições do TAM com perspetivas organizacionais e sociotécnicas específicas do domínio dos cuidados de saúde. O iTAM-Health pressupõe que a adoção de tecnologias de saúde não pode ser explicada apenas por variáveis individuais, mas deve ser entendida como o resultado de um equilíbrio dinâmico entre mecanismos cognitivos, organizacionais e institucionais de confiança. A sua arquitetura conceitual não é, portanto, uma mera adaptação, mas uma reformulação da teoria da aceitação da tecnologia à luz das características estruturais da saúde pública — alta interdependência profissional, restrições regulatórias, responsabilidade coletiva e expectativas de equidade e transparência.

2.1. Trust / Perceived Security

No âmbito da iTAM-Health, a confiança (confiança/segurança percebida) constitui a dimensão fundamental e o principal antecedente da utilidade percebida. Num domínio em que os riscos incluem a proteção de dados clínicos e, em última instância, a vida dos pacientes, a confiança não é apenas um sentimento subjetivo, mas uma construção institucional. Ela surge da confiabilidade das infraestruturas digitais, da clareza das estruturas de governança e da transparência dos processos de gestão de dados (Gefen et al., 2003; Bélanger & Carter, 2008). Quando essas garantias são fracas ou opacas, a incerteza tecnológica gera resistência, apesar de um reconhecimento superficial da utilidade. Nesse sentido, a confiança funciona como um mecanismo gerador — uma condição de possibilidade que permite que outras variáveis do modelo produzam efeitos observáveis.

2.2. Facilitating Conditions

Entrelaçadas com esta base fiduciária estão as condições facilitadoras, definidas como o conjunto de recursos materiais, organizacionais e cognitivos necessários para que a tecnologia seja utilizada de forma eficaz. Na saúde pública, estas condições adquirem um valor sistémico: incluem infraestruturas interoperáveis, formação da força de trabalho, suporte técnico e liderança institucional. Elas refletem o grau de capacidade organizacional que um sistema de saúde possui para traduzir a estratégia digital na prática clínica diária (Holden & Karsh, 2010). As condições facilitadoras também moldam as perceções individuais de facilidade de uso e utilidade, atuando como uma ponte entre o nível micro da experiência profissional e o nível meso das estruturas institucionais.

2.3. Perceived Ease of Use and Perceived Usefulness

A facilidade de utilização percebida (PEOU) e a utilidade percebida (PU) constituem o núcleo cognitivo do modelo, em continuidade com a tradição TAM, mas reinterpretadas no âmbito dos cuidados de saúde. A primeira mede até que ponto um sistema de telemedicina é percebido como intuitivo, estável e consistente com as rotinas clínicas, reduzindo assim o esforço de aprendizagem e a complexidade operacional (Venkatesh & Davis, 2000). A segunda diz respeito à percepção de que a tecnologia melhora não só a produtividade individual, mas também a qualidade dos cuidados, a segurança dos pacientes e a coordenação interprofissional (DeLone & McLean, 2003). Em contextos públicos, a utilidade percebida estende-se, portanto, para além da esfera individual, incluindo benefícios organizacionais e sociais, tais como uma gestão mais eficiente dos recursos e uma maior acessibilidade dos serviços.

2.4. Behavioral Intention and Efficiency Outcomes

A interação entre confiança, condições facilitadoras, usabilidade e utilidade gera a intenção comportamental (BI) — a transição da atitude para a ação. No entanto, nas organizações de saúde, essa intenção não é um ato individual isolado, mas o produto de processos coletivos, normas profissionais e incentivos institucionais. As decisões individuais estão situadas dentro de um ecossistema de políticas, regulamentos e recursos que moldam o comportamento organizacional. Quando as intenções se consolidam em práticas rotineiras, elas produzem resultados de eficiência (EFF), refletindo a dimensão sistémica da adoção. Esses resultados incluem reduções em hospitalizações evitáveis, melhorias na pontualidade do diagnóstico, otimização de custos e aumento da satisfação do utilizador. A eficiência torna-se, assim, não apenas um resultado da digitalização, mas um indicador da capacidade do sistema de aprender e evoluir, fechando um ciclo virtuoso no qual o desempenho reforça a confiança e o envolvimento.

2.5. Arquitetura sistémica do modelo iTAM-Health

Na sua formulação madura, o iTAM-Health pode ser representado como um sistema multinível no qual as relações entre Confiança, Condições Facilitadoras, Facilidade de Utilização Percebida, Utilidade Percebida, Intenção Comportamental e Resultados de Eficiência operam de forma interdependente. Em resumo, esta arquitetura pode ser expressa da seguinte forma:

$$TR \rightarrow PU \rightarrow BI \rightarrow EFF; PEOU \rightarrow PU$$

FC como uma estrutura de apoio transversal.

2.6. Uma perspetiva realista crítica

A escolha do iTAM-Health como estrutura teórica é sustentada pelo seu alinhamento com o paradigma realista crítico, que fornece a base ontológica para compreender a complexidade da adoção tecnológica na área da saúde. De acordo com o realismo crítico (Bhaskar, 1978; Danermark et al., 2019), a realidade social está estruturada em três estratos: empírico, real e concreto. Os fenómenos observáveis (por exemplo, percepções de confiança ou frequência de utilização da telemedicina) pertencem ao nível empírico;

os eventos e interações organizacionais que os geram constituem o nível factual; e as estruturas subjacentes e mecanismos geradores, muitas vezes invisíveis, formam o nível real. Analisar um fenómeno social requer, portanto, raciocinar retroativamente a partir de dados empíricos até aos mecanismos que os produzem.

Aplicado ao iTAM-Health, o realismo crítico permite interpretar a confiança não apenas como uma percepção, mas como o resultado de mecanismos profundos — transparência institucional, consistência entre política e prática — que geram fiabilidade. Da mesma forma, a facilidade de utilização percebida não pode ser reduzida ao design técnico; ela reflete o alinhamento entre infraestrutura, rotinas profissionais e cultura organizacional. Essa abordagem concebe a tecnologia como parte de um sistema relacional causal — não um artefato neutro, mas uma manifestação de processos de poder, competência e confiança.

2.7. Integração do iTAM-Health e do Realismo Crítico

A integração do modelo iTAM-Health com o realismo crítico produz, assim, uma perspectiva teórica unificada. O primeiro fornece a estrutura analítica para identificar relações observáveis entre os conceitos; o segundo fornece a lógica explicativa para compreender como e por que tais relações surgem, se consolidam ou fracassam em contextos institucionais específicos.

Essa sinergia permite que a adoção da telemedicina seja vista não como um comportamento linear, mas como um processo gerador em vários níveis, no qual fatores cognitivos, organizacionais e estruturais se entrelaçam para produzir — e, às vezes, restringir — a inovação digital. Em última análise, interpretar o iTAM-Health através de uma lente realista crítica muda o foco analítico da aceitação para a institucionalização da tecnologia, reconhecendo que confiança, eficiência e sustentabilidade não são resultados contingentes, mas propriedades emergentes de um sistema sociotécnico em evolução.

3. Metodologia

Esta investigação adota uma abordagem qualitativa baseada no realismo crítico, com o objetivo de explorar os mecanismos geradores que influenciam a adoção da telemedicina no sistema público de saúde da região de Veneto. O objetivo não é apenas descrever como os profissionais de saúde percebem e utilizam as tecnologias digitais, mas compreender por que esses processos assumem formas diferentes, dependendo das estruturas institucionais, organizacionais e relacionais nas quais se desenvolvem. A perspectiva realista permite que a realidade seja concebida como um sistema estratificado, no qual experiências empíricas — como confiança, utilidade percebida ou facilidade de uso percebida — são o resultado de eventos e mecanismos mais profundos, muitas vezes não diretamente observáveis, que determinam a sua forma (Bhaskar, 1978; Danermark et al., 2019).

3.1. Desenho da investigação e orientação epistemológica

O desenho da investigação é de natureza explicativa-interpretativa e procura integrar a dimensão fenomenológica das experiências profissionais com a dimensão estrutural

das condições contextuais. Em consonância com os princípios do realismo crítico, o processo analítico seguiu uma lógica retrodictiva, movendo-se iterativamente dos dados para a teoria e vice-versa, com o objetivo de rastrear os fenômenos observados até aos mecanismos que os geram. Esta orientação difere de uma abordagem puramente construtivista: embora o investigador reconheça a natureza social das percepções e narrativas, presume-se que estas também refletem — ainda que parcialmente — estruturas reais do sistema de saúde, tais como normas, infraestruturas e culturas organizacionais. O conhecimento produzido dentro desta perspectiva é falibilista, mas cumulativo, resultado de um processo contínuo de confronto entre teoria e realidade.

A pesquisa foi realizada dentro da ULSS 3 Serenissima, que abrange os territórios de Veneza, Mestre, Mirano e Dolo. O período de análise, entre setembro e dezembro de 2024, coincide com uma fase crucial na evolução da telemedicina na região de Veneto: a transição da resposta à emergência pandémica para a integração estrutural de plataformas digitais nos processos clínicos e administrativos. Este contexto ofereceu um cenário particularmente relevante para investigar como as políticas de digitalização se traduzem em práticas operacionais e formas de confiança institucional.

A amostra, de natureza teórica e proposital (Patton, 2002), é composta por três diretores de unidades complexas de cardiologia, identificados como atores-chave na governança da telemedicina. A escolha reflete o objetivo de coletar perspectivas especializadas e reflexivas sobre um processo de inovação em andamento, privilegiando a profundidade analítica em detrimento da amplitude da amostra. Cada participante ocupa uma posição central na cadeia de tomada de decisões e possui uma visão integrada dos fatores tecnológicos, clínicos e gerenciais que moldam a adoção de soluções digitais.

Apesar de a amostra incluir apenas três diretores de unidades de cardiologia, esta composição reduzida constitui uma limitação relevante, sobretudo no que respeita à transferibilidade dos resultados. Ainda assim, em estudos qualitativos orientados pelo realismo crítico, a opção por participantes estrategicamente posicionados é metodologicamente adequada, dado que privilegia a profundidade explicativa sobre a representatividade estatística. Assim, embora a generalização direta seja limitada, a natureza experiencial e reflexiva dos dados permite identificar mecanismos geradores plausíveis, oferecendo contributos sólidos para uma compreensão teórica da adoção da telemedicina em contextos públicos.

3.2. Recolha de dados

A recolha de dados foi realizada por meio de entrevistas semiestruturadas e análise documental. As entrevistas foram realizadas entre setembro e dezembro de 2024, presencialmente, com duração média de cerca de sessenta minutos. O protocolo de entrevista orientou uma exploração aprofundada das seis dimensões principais da estrutura: confiança, condições facilitadoras, utilidade percebida, intenção comportamental e resultados de eficiência. O objetivo era obter narrativas reflexivas e ligações causais percebidas entre as dimensões tecnológicas, organizacionais e relacionais.

Todas as entrevistas foram gravadas, totalmente transcritas e anonimizadas. Paralelamente, foi recolhido e analisado um corpus documental, incluindo resoluções

regionais (DGR 775/2023), diretrizes operacionais da Azienda Zero, relatórios de implementação, planos estratégicos e protocolos internos da ULSS 3 Serenissima. Esses materiais permitiram situar as percepções dos profissionais dentro de um quadro institucional e regulatório, possibilitando uma comparação contínua entre a representação vivida e a representação organizacional da telemedicina.

3.3. Análise de dados

A análise foi realizada utilizando a Análise de Estrutura (Ritchie & Spencer, 1994), uma metodologia particularmente adequada à investigação aplicada em serviços públicos, uma vez que combina rigor sistemático com abertura interpretativa. Esta abordagem inclui uma sequência de etapas interdependentes: familiarização com os dados, identificação da estrutura temática, indexação, mapeamento e interpretação. Nesta investigação, a Análise de Estrutura foi aprimorada através do uso de ferramentas de codificação assistidas por IA (OpenAI, 2025), empregadas para facilitar o reconhecimento de padrões linguísticos e coocorrências semânticas dentro do corpus textual.

O uso da inteligência artificial desempenhou um papel de apoio, não de substituição: a codificação automática forneceu um mapa preliminar das relações entre os conceitos, posteriormente refinado através do trabalho interpretativo humano. Cada categoria foi verificada, reelaborada e discutida à luz do quadro teórico e do contexto empírico, através de um processo iterativo de comparação entre dados e conceitos. Este duplo nível — analítico e reflexivo — permitiu integrar o rigor computacional com a sensibilidade hermenêutica, em total coerência com a lógica realista, que valoriza a triangulação entre evidências empíricas, teorias explicativas e julgamento interpretativo.

Durante a fase interpretativa, as evidências empíricas foram organizadas em matrizes analíticas que conectavam cada constructo do iTAM-Health aos fragmentos textuais e evidências documentais correspondentes. Esse processo possibilitou identificar configurações causais plausíveis, por exemplo, como a confiança emergiu de formas de transparência organizacional ou como as condições facilitadoras influenciaram as percepções de utilidade e resultados de eficiência. A partir dessa perspectiva, a Análise de Estrutura tornou-se uma ferramenta para a reprodução empírica, permitindo ao investigador passar dos temas observados para os mecanismos geradores hipotéticos.

3.4. Triangulação e fiabilidade interpretativa

A qualidade da investigação foi assegurada através da triangulação metodológica (Denzin, 2012), que integrou fontes de natureza diferente — entrevistas, documentos e dados institucionais — a fim de comparar perspectivas individuais e estruturais. As convergências entre as fontes foram consideradas indicadores de robustez interpretativa, enquanto as divergências proporcionaram oportunidades para explorar desalinhamentos ou tensões entre os níveis de governação.

Para reforçar a credibilidade, foram realizadas sessões de verificação com os membros, partilhando interpretações preliminares com os participantes, bem como sessões de debriefing com colegas pesquisadores experientes em saúde digital. Essas práticas permitiram refinar as inferências e garantir a coerência interna entre os dados e a interpretação. Todo o processo foi documentado numa trilha de auditoria digital,

incluindo notas de campo, versões intermediárias de codificação, mapas temáticos e comentários reflexivos, garantindo transparência e replicabilidade.

3.5. Síntese metodológica

De modo geral, a metodologia empregada combina a profundidade interpretativa do realismo crítico com a estrutura sistemática da Análise de Estrutura, articulando um processo de investigação que prioriza a explicação em detrimento da descrição. A integração da análise assistida por IA e da reflexão teórica tornou possível alcançar uma leitura multinível do fenômeno, na qual as percepções individuais, as condições organizacionais e as lógicas institucionais são entendidas como partes de um único sistema causal. Esta perspectiva metodológica não só fornece uma base robusta para a análise dos resultados, como também representa uma contribuição inovadora para o debate sobre o papel da inteligência artificial e do realismo crítico na investigação qualitativa aplicada à saúde pública.

4. Resultados

A análise qualitativa, apoiada por triangulação empírica e teórica, confirmou a estrutura causal do modelo iTAM-Health, revelando um processo circular de institucionalização da telemedicina na ULSS 3 Serenissima. Os seis constructos — Confiança (TR), Condições Facilitadoras (FC), Facilidade de Utilização Percebida (PEOU), Utilidade Percebida (PU), Intenção Comportamental (BI) e Resultados de Eficiência (EFF) — funcionam como mecanismos geradores interdependentes que abrangem os três níveis ontológicos realistas críticos (real, factual, empírico). Evidências documentais e entrevistas realizadas em Veneza, Mestre e Mirano mostram que a adoção digital não se desenrola como uma sequência linear, mas sim como um circuito autopoético de confiança institucional, coordenação sociotécnica e valor público.

4.1. Trust / Perceived Security (TR)

A confiança constitui a condição de possibilidade para a telemedicina pública, funcionando como uma propriedade emergente resultante da coerência entre a infraestrutura normativa, a transparência organizacional e a relação de cuidados.

A evidência empírica correspondente encontra-se sintetizada na Tabela 1, que apresenta a matriz multinível de evidências para o constructo TR.

Nível	Evidência Empírica (ULSS 3)	Mecanismo Gerador	Referências Teóricas
<i>Real</i>	Governança da segurança – DGR 775/2023; Carta de Serviços ULSS3; FSEr 2.0 – padrões security-by-design e rastreabilidade automática.	Confiança institucional como propriedade sistêmica derivada de normas, certificações e accountability pública.	Bélanger & Carter (2008); Gefen et al. (2003)

Nível	Evidência Empírica (ULSS 3)	Mecanismo Gerador	Referências Teóricas
<i>Actual</i>	«Il dato è certificato, prodotto da aziende multinazionali, tracciato e firmato digitalmente: questo genera fiducia nel sistema.» (Mestre). «Os dados são certificados, produzidos por empresas multinacionais, rastreados e assinados digitalmente: isso gera confiança no sistema.» (Mestre)	Confiança performada: coerência entre fiabilidade técnica e reconhecimento profissional.	Venkatesh et al. (2012). Perceived credibility \square PU (Venkatesh et al., 2012)
<i>Empírico</i>	«Il paziente si sente più protetto, più seguito, anche se non è fisicamente qui.» (Venezia). «O paciente sente-se mais protegido, mais acompanhado, mesmo que não esteja fisicamente presente.» (Veneza)	Confiança relacional como percepção de proximidade digital.	Holden & Karsh (2010)

Tabela 1 – Matriz Multinível de Evidências: TR

No nível real, a confiança representa estabilidade institucional: normas, auditorias e interoperabilidade definem um campo de legitimidade.

No nível real, os médicos reinterpretem a segurança como confiabilidade epistêmica – “fidarsi, ma verificare” (“confiar, mas verificar”) –, estabelecendo uma tensão generativa entre confiança e controle.

No nível empírico, a confiança se traduz em continuidade afetiva: a distância tecnológica se torna proximidade relacional.

«Il grosso limite alla telemedicina è la competenza digitale dei pazienti. Molti non riescono a gestire smartphone, email o piattaforme, e senza un familiare “smart” non possono entrare nel sistema» (Venezia) (“A principal limitação da telemedicina é a competência digital dos pacientes. Muitos não conseguem gerir smartphone, e-mail ou plataformas, e sem um familiar mais ‘smart’ não conseguem entrar no sistema.” – Veneza).

O mecanismo emergente de institucionalização fiduciária conecta a segurança sistêmica ao reconhecimento profissional, estabelecendo a legitimidade da tecnologia digital como uma prática de cuidado.

4.2. Facilitating Conditions (FC)

As condições facilitadoras constituem a estrutura infraestrutural e relacional que torna a inovação eficaz. Elas determinam a capacidade organizacional de traduzir o projeto político-tecnológico em prática cotidiana.

A evidência empírica correspondente encontra-se sintetizada na Tabela 2, que apresenta a matriz multinível de evidências para o constructo FC.

Nível	Evidência Empírica (ULSS 3)	Mecanismo Gerador	Referências Teóricas
<i>Real</i>	Estruturas habilitadoras: Centro Operacional Territorial (COT), Azienda Zero, PNRR – Missão 6, padrões interoperáveis.	Facilitating Conditions como capacidade institucional e infraestrutural	Holden & Karsh (2010); Venkatesh et al. (2003)
<i>Actual</i>	«Abbiamo due infermieri che a tempo pieno fanno questo.» (Mestre); «Serve più formazione e un help-desk tecnico unico, perché ora ogni reparto si arrangia.» (Mirano); «Temos duas enfermeiras a trabalhar a tempo inteiro nisto.» (Mestre); «Precisamos de mais formação e de um único serviço de assistência técnica, porque neste momento cada departamento gere a sua própria assistência.» (Mirano)	Mediação humana e coordenação informal como pré-requisitos funcionais.	Ross et al. (2021)
<i>Empírico</i>	«Caregiver come ponte operativo.» (Mirano) «Os cuidadores atuam como uma ponte operacional.» (Mirano)	Lacunas infraestruturais que geram um desfasamento entre intenção e comportamento	Parretti et al. (2022)

Tabela 2 – Matriz Multinível de Evidências: FC

4.3. Perceived Ease of Use (PEOU)

A usabilidade surge como uma variável-limite entre o desenho político, a estrutura organizacional e a cognição profissional, medindo o grau de consonância entre o sistema e o utilizador. A evidência empírica correspondente encontra-se sintetizada na Tabela 3, que apresenta a matriz multinível de evidências para o constructo PEOU.

Nível	Evidência Empírica (ULSS 3)	Mecanismo Gerador	Referências Teóricas
<i>Real</i>	Padronização regional: “Sanità km Zero”, identidade digital SPID/ CIE, checklist <i>DGR</i> 775/2023.	Usabilidade institucionalizada como direito de acesso digital.	Davis (1989); Venkatesh & Davis (2000)
<i>Actual</i>	«La piattaforma è un po’ macchinosa, non immediata per chi non è pratico.» (Mirano) «A plataforma é um pouco complicada, não é muito intuitiva para quem não está habituado.» (Mirano)	Atrito cognitivo entre a interface e as rotinas clínicas.	Goodhue & Thompson (1995)
<i>Empírico</i>	«Stiamo sperimentando Dr. Marco, che filtra le richieste H24.» (Venezia) «Estamos a testar o Dr. Marco, que filtra os pedidos dos pacientes 24 horas por dia, 7 dias por semana.» (Venezia)	Automação adaptativa e redução da carga cognitiva.	Triangulação ULSS3 (2024)

Tabela 3 – Matriz Multinível de Evidências: PEOU

No nível real, a PEOU é construída como um valor regulador: a simplificação é um requisito de equidade.

No nível factual, os operadores deparam-se com um atributo cognitivo: interfaces desalinhasdas com a lógica clínica interrompem o fluxo operacional.

No nível empírico, a introdução de sistemas assistidos por IA (Venice) inaugura uma nova forma de “facilidade delegada”.

Contradição geradora: simplificação algorítmica vs. perda de agência profissional.

Mecanismo: automação adaptativa, na qual a facilidade de uso se torna uma propriedade coevolutiva do sistema sociotécnico.

«Il punto fondamentale è il personale: per rendere la telemedicina sostenibile servono più infermieri e più tempo dedicato» (Mirano) (“O ponto fundamental é o pessoal: para tornar a telemedicina sustentável são necessários mais enfermeiros e mais tempo dedicado.” – Mirano).

4.4. Perceived Usefulness (PU)

A utilidade percebida surge como uma expressão do valor público, integrando a dimensão clínica, a eficiência organizacional e a proximidade relacional. A evidência

empírica correspondente encontra-se sintetizada na Tabela 4, que apresenta a matriz multinível de evidências para o constructo PU.

Nível	Evidência Empírica (ULSS 3)	Mecanismo Gerador	Referências Teóricas
<i>Real</i>	A telemedicina reconhecida nos Níveis Essenciais de Cuidados Digitais – DGR 775/2023; valorização pública através do Plano Nacional de Recuperação e Resiliência (PNRR).	Utilidade institucionalizada como valor de política de saúde pública.	DeLone & McLean (2003); Maillet et al. (2015)
<i>Actual</i>	«Le aritmie vengono viste subito, si modifica la terapia e si evita un ricovero o un ictus.» (Mirano) «As arritmias são detetadas imediatamente, a terapia é ajustada e evita-se a hospitalização ou o AVC.» (Mirano)	Utilidade clínico-funcional e otimização do processo.	Greenhalgh et al. (2017)
<i>Empírico</i>	«Il paziente si sente più seguito, più sereno.» (Venezia) «O paciente sente-se mais cuidado e mais tranquilo.» (Veneza)	Utilidade relacional como confiança incorporada.	Holden & Karsh (2010)

Tabela 4 – Matriz Multinível de Evidências: PU

No nível real, a utilidade é institucionalizada como um bem coletivo e um critério de legitimidade.

No nível factual, ela se traduz em resultados tangíveis — diagnóstico precoce, redução das consultas hospitalares e melhoria na adesão terapêutica.

No nível empírico, ela se torna uma experiência afetiva de tranquilidade e cuidado.

Contradição geradora: utilidade sistémica vs. utilidade vivida.

Mecanismo: valorização funcional, em que a tecnologia cria valor na medida em que produz significado, não apenas eficiência.

4.5. Behavioral Intention (BI)

A intenção comportamental representa o limiar de conversão entre aceitação e institucionalização, o ponto em que a adoção se transforma numa norma partilhada. A evidência empírica correspondente encontra-se sintetizada na Tabela 5, que apresenta a matriz multinível de evidências para o constructo BI.

Nível	Evidência Empírica (ULSS 3)	Mecanismo Gerador	Referências Teóricas
<i>Real</i>	Obrigações e marcos do PNRR; diretrizes de implementação regional.	Intenção institucionalizada orientada por políticas públicas.	UTAUT – influência social → BI
<i>Actual</i>	«Non è più un progetto, ormai è la nostra routine clinica.» (Mestre) «Não é mais um projeto; agora faz parte da nossa rotina clínica.» (Mestre)	Normalização organizacional e aprendizagem cumulativa.	Greenhalgh et al. (2017) – Normalization Process Theory
<i>Empírico</i>	Diferenças locais observadas: Veneza (IA), Mirano (recursos humanos), Mestre (padronização).	Intenções diferenciadas e institucionalização plural.	Triangulação ULSS3 (2024)

Tabela 5 – Matriz Multinível de Evidências: BI

No nível real, a intenção comportamental é impulsionada por um imperativo político-administrativo.

No nível factual, o uso diário traduz a intenção em rotina.

No nível empírico, a motivação varia: Veneza depende da tecnologia, Mirano dos recursos humanos, Mestre da padronização.

Contradição geradora: intenção prescrita vs. motivação autónoma.

Mecanismo: normalização digital, que transforma a política em cultura, mas pode limitar a criatividade profissional.

4.6. Efficiency Outcomes (EFF)

A eficiência representa o encerramento sistémico do ciclo, medindo simultaneamente a sustentabilidade material e simbólica da digitalização. A evidência empírica correspondente encontra-se sintetizada na Tabela 6, que apresenta a matriz multinível de evidências para o constructo EFF.

Nível	Evidência Empírica (ULSS 3)	Mecanismo Gerador	Referências Teóricas
<i>Real</i>	+23% de telemonitorização em 2024; redução de hospitalizações evitáveis; consolidação do Centro de Operações Territoriais (COT).	Eficiência sistémica e redistribuição de recursos.	DeLone & McLean (2003); Bhaskar (1978)

Nível	Evidência Empírica (ULSS 3)	Mecanismo Gerador	Referências Teóricas
Actual	«Il kit costa sui 2300 euro, ma il paziente evita ricoveri e viaggi continui.» (Venezia)	Paradoxo da eficiência: equilíbrio entre custo, carga de trabalho e valor produzido.	Ross et al. (2021)
	«O kit custa cerca de 2300 euros, mas o paciente evita internamentos hospitalares e deslocações contínuas.» (Veneza)		
Empírico	«Riduzione degli accessi e miglioramento psicologico del paziente.» (Venezia)	Eficiência relacional e bem-estar percebido.	Greenhalgh et al. (2020)
	«Redução das visitas ao hospital e melhoria psicológica do paciente.» (Veneza)		

Tabela 6 – Matriz Multinível de Evidências: EFF

No nível real, a eficiência é um objetivo político e uma métrica de responsabilidade.

No nível factual, ela se manifesta através da contradição entre o desempenho organizacional e a fadiga profissional.

No nível empírico, ela assume a forma de bem-estar percebido e confiança renovada.

Contradição geradora: eficiência sistémica versus sustentabilidade individual.

Mecanismo: feedback institucional, no qual a melhoria percebida reforça a confiança e fecha o ciclo causal do modelo iTAM-Health.

4.7. Integrated Synthesis of Generative Mechanisms

A Tabela 7 apresenta uma síntese integrada dos seis mecanismos geradores identificados ao longo da análise — articulando o nível causal, a contradição gerativa e o respetivo resultado sistémico associado a cada constructo do modelo iTAM-Health.

Construção	Mecanismo Gerador	Direção Generativa	Contradição Generativa	Resultado Sistémico
TR	Institucionalização fiduciária	Real → Empírico	Confiança ↔ Controlo	Legitimação digital
FC	Capacitação relacional	Atual → Real	Empoderamento ↔ Sobrecarga	Capacidade organizacional

Construção	Mecanismo Gerador	Direção Generativa	Contradição Generativa	Resultado Sistémico
<i>PEOU</i>	Automação adaptativa	Atual → Empírico	Simplificação ↔ Agência	Simplificação cognitiva
<i>PU</i>	Valorização funcional	Real → Atual	Utilidade sistémica ↔ Utilidade vivida	Valor público
<i>BI</i>	Normalização digital	Atual → Real	Prescrição ↔ Intenção autónoma	Institucionalização
<i>EFF</i>	Feedback institucional	Empírico → Real	Eficiência ↔ Sustentabilidade	Estabilização do sistema

Tabela 7 – Síntese integrada dos mecanismos geradores

4.8. Discussão sintética

A interação entre os seis constructos forma um ciclo gerativo fechado, no qual cada dimensão reforça a seguinte, produzindo um movimento contínuo de estabilização institucional:

TR → FC → PEOU → PU → BI → EFF → TR

A confiança institucional gera condições propícias; essas condições estruturam a usabilidade; a usabilidade produz utilidade; a utilidade alimenta a intenção coletiva; a intenção gera resultados eficientes; a eficiência retroalimenta, consolidando a confiança.

Esse circuito descreve um processo de institucionalização reflexiva, no qual a telemedicina não é meramente adotada, mas incorporada como uma forma organizacional estável.

As tensões observadas empiricamente — confiança/controlo, automação/agência, eficiência/carga de trabalho — funcionam como motores geradores de mudança, em vez de anomalias.

No contexto da ULSS 3 Serenissima, a telemedicina surge como um espaço sociotécnico de confiança reflexiva, onde a tecnologia se torna um meio de reciprocidade institucional e aprendizagem coletiva.

O modelo iTAM-Health, empiricamente confirmado, demonstra que a adoção digital na saúde pública é um processo crítico-realista de coprodução entre estruturas, atores e valores públicos: um ecossistema no qual a confiança gera eficiência e a eficiência restaura a confiança.

5. Discussão

5.1. A adoção como um processo generativo e ciclo sociotécnico de coprodução

A análise do caso ULSS 3 Serenissima evidencia que a adoção da telemedicina não se desenvolve como um percurso linear centrado no indivíduo, mas como um processo

gerativo multinível em que dimensões institucionais, organizacionais e relacionais coevoluem num circuito sociotécnico de coprodução.

À luz do realismo crítico, esta dinâmica estrutura-se em três estratos causais:

- Um nível real composto por normas, recursos e poderes institucionais (RGPD, DGR 775/2023, governança da Azienda Zero), que definem o espaço de possibilidades da adoção;
- Um nível factual, no qual essas condições se concretizam em práticas profissionais, configurações organizacionais e formas de cooperação;
- E um nível empírico, onde se manifestam efeitos observáveis — eficiência, confiança e continuidade dos cuidados (Bhaskar, 1978; Danermark et al., 2019) Corresponde ao estilo *Numbered Item*.

As narrativas recolhidas ilustram essa articulação causal: «Il paziente si sente più seguito, più protetto» (Veneza) (“O paciente sente-se mais cuidado, mais protegido.” – Veneza); «Abbiamo due infermieri che a tempo pieno fanno questo» (Mestre) (“Temos dois enfermeiros que trabalham a tempo inteiro nisso.” – Mestre). Estas perceções refletem empiricamente mecanismos de confiança e capacitação ativados por um enquadramento institucional robusto.

Deste modo, a adoção configura-se como um ciclo sociotécnico composto por quatro mecanismos interdependentes: institucionalização fiduciária → capacitação relacional → automação adaptativa → feedback de eficiência. Em consonância com Greenhalgh et al. (2017) e Holden & Karsh (2010), tal ciclo não representa uma sucessão linear de antecedentes, mas um sistema gerativo no qual a confiança estrutural molda as práticas e é simultaneamente reforçada por elas, produzindo um processo de estabilização reflexiva da telemedicina.

5.2. Mecanismos geradores do realismo crítico: confiança institucionalizada, capacitação relacional e automação adaptativa

A triangulação dos dados permite identificar três mecanismos geradores que explicam a passagem da aceitação individual para a institucionalização organizacional da telemedicina.

- Confiança institucionalizada. A confiança constitui o princípio organizacional que converte a conformidade normativa em legitimidade percebida. Fontes documentais e entrevistas convergem na sua definição como um bem público institucionalizado: «È un sistema certificato, con tutela della privacy» (Mestre) (“É um sistema certificado, com proteção da privacidade.” – Mestre). Neste enquadramento, a confiança não atua como uma variável psicológica, mas como um poder causal incorporado em regras, normas de segurança e práticas de transparência. Ela cria as condições estruturais para a segurança percebida e funciona como mecanismo sistémico facilitador que sustenta perceções positivas de facilidade e utilidade (PEOU, PU). De uma perspetiva realista, o nível real manifesta-se no nível factual sob a forma de confiança relacional, fundamento da agência digital (Gefen et al., 2003; Bélanger & Carter, 2008) Corresponde ao estilo *Bullet Item*.

- Capacitação relacional. As condições facilitadoras não correspondem apenas a recursos técnicos, mas configuram capacidades relacionais distribuídas. Enfermeiros, técnicos, centros de coordenação territorial (COTs) e cuidadores atuam como mediadores cognitivos entre a infraestrutura e o paciente. A afirmação «Mettere più personale e formare di più il personale» (Mirano) (“Contratar mais pessoal e dar mais formação ao pessoal.” – Mirano) expressa a consciência de que a eficácia tecnológica depende fundamentalmente de infraestruturas humanas, e não apenas digitais. Este mecanismo traduz a transição do suporte estritamente técnico para o suporte sociotécnico, em consonância com DeLone & McLean (2003), segundo os quais a qualidade e a eficiência do serviço emergem da interação entre tecnologia e capital humano. De um ponto de vista realista, a capacitação relacional corresponde à ativação, no nível factual, de capacidades causais enraizadas numa estrutura de confiança previamente institucionalizada.
- Automação adaptativa. O terceiro mecanismo refere-se à transformação da facilidade de uso (PEOU) em uso inteligente. A adoção de ferramentas como o “Dr. Marco”, um agente de IA que filtra solicitações clínicas e prioridades («Dr. Marco sarà disponibile h24..., filtra le richieste dei pazienti», Venezia) (“O Dr. Marco estará disponível 24 horas por dia, 7 dias por semana... ele filtra as solicitações dos pacientes.” – Venezia) evidencia uma fase avançada de automação cognitiva. Neste contexto, a tecnologia não se limita a simplificar a interação: ela aprende com as rotinas humanas, reduz a carga cognitiva, aumenta a acuidade do diagnóstico e adapta-se progressivamente aos fluxos clínicos. A automação adaptativa configura, assim, um mecanismo de coevolução cognitiva entre humanos e máquinas, redefinindo a usabilidade como propriedade relacional e dinâmica, e não como um atributo estritamente técnico.

A estes três mecanismos acrescenta-se um quarto elemento transversal: o feedback de eficiência, que articula ganhos percebidos («riduzione di ricoveri, miglioramento psicologico», Venezia) (“redução das internações hospitalares, melhoria psicológica” – Venezia) com a legitimação organizacional. A eficácia empírica reforça a confiança estrutural, completando o ciclo gerativo de institucionalização.

5.3. Extensão teórica do iTAM-Health: causalidade multinível e aprendizagem institucional

O iTAM-Health representa uma evolução substantiva do TAM clássico (Davis, 1989; Venkatesh et al., 2003), ao incorporar uma ontologia estratificada de causalidade. Enquanto no TAM original as relações entre PEOU, PU e BI se apresentam como associações lineares centradas no indivíduo, no presente modelo essas relações assumem a forma de interdependências causais distribuídas por diferentes níveis ontológicos:

1. No nível real, a confiança e as condições facilitadoras operam como poderes estruturais que moldam o espaço de possibilidades da adoção;
2. No nível factual, a facilidade de uso percebida e a utilidade percebida emergem como eventos cognitivos e organizacionais desencadeados por esses poderes;
3. No nível empírico, a eficiência manifesta-se como resultado observável e como mecanismo de feedback que retroalimenta a estrutura.

Esta arquitetura configura um modelo dinâmico de causalidade retroductiva, no qual os efeitos contribuem para regenerar as suas causas através de processos de aprendizagem institucional. Assim, a eficiência não constitui um fim em si mesma, mas um indicador da maturidade gerativa do sistema sociotécnico.

Esta perspetiva transcende o reducionismo comportamental do TAM clássico, situando a tecnologia numa abordagem ontológica mais profunda e compatível com a teoria realista crítica dos sistemas (Danermark et al., 2019).

No caso da ULSS 3 Serenissima, o modelo evidencia que a eficiência percebida — redução de visitas hospitalares, diagnósticos oportunos e satisfação dos pacientes — atua como um mecanismo de feedback de confiança: o desempenho operacional reforça a confiança e incentiva novas adoções. O iTAM-Health transforma-se, assim, numa estrutura de aprendizagem institucional, na qual a tecnologia é simultaneamente causa, meio e produto da transformação organizacional.

5.4. Convergências e divergências europeias: a confiança como infraestrutura pública

O caso Veneto alinha-se com a literatura europeia sobre sustentabilidade da saúde eletrónica (Greenhalgh et al., 2020; Ross et al., 2021; Parretti et al., 2022), mas evidencia um traço distintivo: uma confiança institucional antecipada, assente na governança e na transparência, mais do que na experiência prévia do utilizador.

Enquanto os modelos nórdicos sustentam a normalização na integração sistémica e no capital digital amplamente difundido, a Itália — e, em particular, a ULSS 3 Serenissima — constrói a legitimidade da telemedicina antes da sua completa rotinização. Este mecanismo de institucionalização fiduciária preventiva explica a integração da telemedicina nos percursos clínicos («più che progetto, è nostra routine clinica», Mestre — “já não é realmente um projeto, é a nossa rotina clínica” — Mestre), mesmo face a limitações infraestruturais persistentes.

Persistem, porém, tensões estruturais características dos contextos mediterrânicos: assimetrias entre política e prática, insuficiente interoperabilidade e cargas de trabalho inalteradas («non è un risparmio di tempo, anzi...», Mestre — “não é uma poupança de tempo, pelo contrário...” — Mestre). Estas fricções revelam que o ciclo gerador ainda não alcançou plena estabilização, uma vez que o feedback de eficiência permanece aquém de um limiar consistente de equilíbrio.

Comparativamente a outros países europeus, a ULSS 3 Serenissima distingue-se pela rapidez da institucionalização normativa, embora apresente uma eficiência operacional ainda em consolidação. Tal constatação sugere que a sustentabilidade da saúde digital exige uma articulação permanente entre confiança regulatória e confiança experiencial.

Uma perspetiva internacional reforça esta interpretação: nos Estados Unidos predominam modelos orientados pelo mercado e pela eficiência individual; em ecossistemas asiáticos tecnologicamente avançados, como Singapura, observa-se forte centralização regulatória e uma padronização digital elevada. Em contraste, o caso ULSS 3 assenta numa lógica de confiança pública e governança institucional, oferecendo

uma trajetória alternativa de adoção digital. Estas comparações apontam caminhos promissores para a expansão internacional do modelo iTAM-Health.

5.5. Síntese teórica e implicações para a estrutura visual

Em síntese, o caso ULSS 3 Serenissima evidencia que a adoção da telemedicina evolui da aceitação individual para a institucionalização organizacional, configurando um sistema gerativo estratificado. O nível real (confiança, governança, infraestruturas) estabelece as condições de possibilidade; o nível factual (práticas, cooperação, usabilidade adaptativa) ativa os respetivos poderes causais; e o nível empírico (eficiência, valor público, aprendizagem) manifesta os seus efeitos, retroalimentando as estruturas num circuito coerente de coevolução fiduciária.

O iTAM-Health propõe, assim, uma teoria da transformação digital institucional ancorada em mecanismos generativos de confiança e aprendizagem. A tecnologia deixa de ser apenas um objeto a ser aceite e passa a atuar como agente epistémico, reconfigurando as relações entre instituições, profissionais e cidadãos e produzindo sustentabilidade e legitimidade organizacional.

A estrutura visual crítico-realista do iTAM-Health, apresentada de seguida, traduz graficamente este ciclo estratificado de causalidade, evidenciando como a confiança institucional e o feedback de eficiência fecham o círculo da adoção sustentável na saúde pública digital. A Figura 1 representa a arquitetura sistémica do modelo.

Importa ainda reconhecer que a institucionalização da telemedicina implica desafios éticos e regulatórios que ultrapassam a dimensão estritamente tecnológica. Entre estes destacam-se a necessidade de assegurar equidade de acesso, garantir a proteção e governança de dados sensíveis e promover transparência nos processos algorítmicos associados à automação adaptativa. Embora tais implicações não constituam o foco central deste estudo, representam dimensões essenciais para futuras aplicações e avaliações do modelo iTAM-Health em ecossistemas de saúde digital.

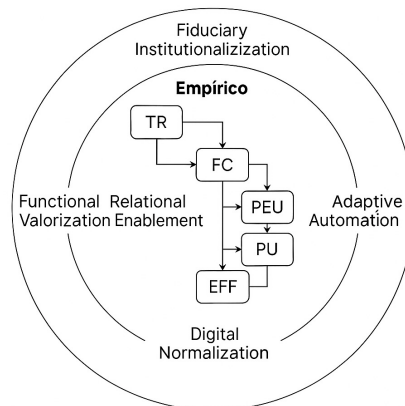


Figura 1 – Arquitetura Sistémica do Modelo iTAM-Health

O Mapa Conceitual iTAM-Health integra a Teoria da Aceitação da Tecnologia com uma ontologia realista crítica para explicar a institucionalização das práticas de saúde digital. Organizado em três níveis concêntricos — real, factual e empírico —, o modelo descreve como mecanismos institucionais, relacionais e experienciais se articulam para gerar uma adoção digital sustentável.

O círculo externo (nível real) reúne os fundamentos estruturais e normativos da transformação digital — governança, confiança regulatória e infraestruturas de recursos. É neste nível que opera o mecanismo de institucionalização fiduciária, por meio do qual credibilidade e transparência institucionais estabelecem as condições de possibilidade para o desenvolvimento da confiança e do envolvimento dos utilizadores.

O círculo intermédio (nível factual) representa o domínio operacional onde as interações sociotécnicas se materializam. Dois mecanismos — Capacitação Relacional e Automação Adaptativa — ilustram como capacidades humanas, colaboração profissional e tecnologias responsivas concretizam o potencial inscrito na camada estrutural. Este nível acolhe o núcleo funcional da cadeia causal iTAM-Health:

TR → FC → PEOU → PU → BI → EFF

Estas construções articulam um ciclo recursivo no qual a Confiança (TR) ativa as Condições Facilitadoras (FC), que moldam a Facilidade de Utilização Percebida (PEOU) e a Utilidade Percebida (PU), desencadeando a Intenção Comportamental (BI) e, subsequentemente, os Resultados de Eficiência (EFF).

O círculo interno (nível empírico) expressa os efeitos observáveis da adoção — maior eficiência, continuidade dos cuidados e reforço da confiança do utilizador. Três mecanismos geradores — Valorização Funcional, Normalização Digital e Feedback Institucional — operam neste nível, demonstrando como os resultados empíricos consolidam a legitimidade das práticas digitais e retroalimentam a camada estrutural.

6. Conclusões

A investigação demonstrou que a adoção da telemedicina não representa um mero episódio de mudança tecnológica, mas sim um processo gerador de institucionalização fiduciária, no qual estruturas normativas, práticas profissionais e percepções subjetivas são coproduzidas dentro de um ciclo sociotécnico multinível.

Ao abordar a questão de como a aceitação individual evolui para a estabilidade organizacional, os resultados indicam que a digitalização dos cuidados de saúde não está enraizada em intenções comportamentais, mas na capacidade das instituições de gerar confiança como uma forma de infraestrutura pública.

O modelo iTAM-Health amplia a clássica Teoria da Aceitação da Tecnologia (Davis, 1989; Venkatesh et al., 2003), traduzindo-a em uma lógica crítico-realista de causalidade estratificada e circular. As variáveis da TAM não funcionam como fatores preditivos, mas como poderes causais emergentes localizados em três níveis ontológicos: (1) o real (confiança institucional, governança, recursos); (2) o factual (práticas sociotécnicas e relações profissionais); (3) e o empírico (eficiência, legitimidade, valor público).

O ciclo TR → FC → PEOU → PU → BI → EFF → TR, ilustrado na secção anterior, representa um mecanismo generativo no qual a confiança institucional permite a utilização, a utilização produz eficiência e a eficiência retroalimenta para reforçar a confiança.

Assim, a adoção configura-se como uma forma de aprendizagem institucional reflexiva, em vez de uma sequência linear de percepções individuais.

O caso ULSS 3 Serenissima permitiu observar, em termos concretos, a transição da emergência para a normalidade por meio de mecanismos interdependentes de institucionalização fiduciária, capacitação relacional e automação adaptativa. A confiança regulatória (DGR 775/2023, GDPR) e a governança regional atuam como poderes reais; as práticas profissionais — enfermeiros dedicados, Centros de Operações Territoriais (COT) e telemonitorização — representam a sua implementação efetiva; a eficiência empírica, expressa na redução das admissões, na continuidade dos cuidados e na satisfação dos pacientes, constitui a manifestação observável e o motor de feedback do processo. A telemedicina torna-se assim uma rotina institucional generativa, na qual a eficiência não encerra o ciclo, mas o reativa.

Ao nível da gestão e das políticas, as evidências empíricas enfatizam que a sustentabilidade dos cuidados de saúde digitais depende da institucionalização da confiança como um bem comum. A governança pública deve atuar como um mecanismo facilitador, e não como uma forma de controle, direcionando investimentos e regulamentação para três dimensões geradoras: interoperabilidade técnica, competência relacional e transparência de processos. As estratégias organizacionais devem reconhecer que a transformação digital é, antes de tudo, uma transformação institucional, na qual a capacidade de coordenação e aprendizagem coletiva se torna o principal impulsionador da eficiência.

Esta análise, centrada num único contexto regional, privilegia a profundidade interpretativa em detrimento da generalização. Estudos futuros poderiam testar os mecanismos geradores do iTAM-Health a partir de perspetivas comparativas e longitudinais, avaliando a sua força causal em diferentes contextos e o impacto de novas formas de automação cognitiva na confiança institucional.

Em última análise, o iTAM-Health propõe uma teoria da transformação digital na saúde pública como um processo crítico-realista de coevolução entre confiança, tecnologia e instituições.

A telemedicina surge não como um instrumento técnico, mas como uma forma de governança reflexiva capaz de produzir valor público por meio da convergência de eficiência, legitimidade e aprendizagem coletiva. A adoção é concretizada quando a tecnologia se torna simultaneamente o objeto e a condição da confiança institucional — a sua normalização coincide com a plena maturidade do sistema sociotécnico.

Referências

Agarwal, R., Gao, G., DesRoches, C., & Jha, A. K. (2020). The digital transformation of healthcare: Current status and the road ahead. *Information Systems Research*, 31(2), 249–260. <https://doi.org/10.1287/isre.2019.0906>

- Bhaskar, R. (1978). *A realist theory of science* (2nd ed.). Harvester Press.
- Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *Journal of Strategic Information Systems*, 17(2), 165–176.
- Danermark, B., Ekström, M., Jakobsen, L., & Karlsson, J. C. (2019). *Explaining society: Critical realism in the social sciences*. Routledge.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
- DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, 19(4), 9–30.
- Gefen, D. (2003). TAM or just plain habit: A look at experienced online shoppers. *Journal of End User Computing*, 15(3), 1–13.
- Greenhalgh, T., Rosen, R., Shaw, S. E., & Byng, R. (2020). The infrastructural work of health service innovation: A qualitative case study. *BMC Health Services Research*, 20(1), 1–12.
- Greenhalgh, T., Wherton, J., Papoutsis, C., Lynch, J., & Hughes, G. (2017). Beyond adoption: A new framework for theorizing and evaluating nonadoption, abandonment, and challenges to the scale-up, spread, and sustainability of health and care technologies. *Journal of Medical Internet Research*, 19(11), e367.
- Holden, R. J., & Karsh, B.-T. (2010). The technology acceptance model: Its past and its future in health care. *Journal of Biomedical Informatics*, 43(1), 159–172.
- Maillet, É., Mathieu, L., & Sicotte, C. (2015). Modeling factors explaining the acceptance, actual use and satisfaction of nurses using an Electronic Patient Record in acute care settings: An extension of the TAM model. *International Journal of Medical Informatics*, 84(1), 36–47.
- Parretti, C., et al. (2022). Digital healthcare ecosystems and the challenge of interoperability. *Health Policy and Technology*, 11(4), 100627.
- Ross, J., Stevenson, F., Lau, R., & Murray, E. (2021). Factors that influence the implementation of e-health: A systematic review of systematic reviews (an update). *BMC Health Services Research*, 21, 1150.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science*, 46(2), 186–204.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478.
- Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), 157–178.

StopEmailSpoofing: uma solução para detecção de vulnerabilidade de domínios à ataques falsificação de e-mail

Guilherme Dieguez Cândido¹, Igor Ramos Bezerra da Silva¹, Emílio Gonçalves¹,
Leonardo de Paiva Souza¹, João Souza Neto¹, Rafael Rabelo Nunes¹

**guilherme.candido@aluno.unb.br; igorbramos1@unb.br; emilio.goncalves@aluno.unb.br;
leonardops@unb.br; neto.joao@unb.br; rafaelrabelo@unb.br**

¹ Departamento de Engenharia Elétrica, Universidade de Brasília (UnB), Campus Darcy Ribeiro, 70.910-900, Brasília – DF, Brasil

DOI: 10.17013/risti.60.57–73

Resumo: O e-mail permanece sendo o principal meio de comunicação contemporâneo, constituindo vetor frequente de ataques cibernéticos. Apesar da evolução dos sistemas de proteção, o fator humano continua sendo o elo mais fraco da segurança cibernética, sendo explorado por técnicas de engenharia social. Este trabalho apresenta a ferramenta de código aberto *StopEmailSpoofing*, desenvolvida para automatizar a detecção de vulnerabilidades de falsificação de e-mail em domínios. A ferramenta analisa todas as 295 combinações possíveis entre os protocolos SPF e DMARC, realizando consultas DNS para avaliar a suscetibilidade dos domínios. Diferentemente de soluções existentes, oferece cobertura completa dos protocolos de autenticação e sugere ações imediatas de correção. Uma validação foi realizada através de estudo de caso com instituições públicas de ensino superior brasileiras, demonstrando eficiência na identificação de falhas e contribuindo para o fortalecimento da resiliência das comunicações digitais organizacionais.

Palavras-chave: Falsificação de e-mail; SPF; DMARC; segurança cibernética; segurança das comunicações.

StopEmailSpoofing: a solution for detecting domains vulnerability to email spoofing attacks

Abstract: Email remains the primary means of contemporary communication, becoming a frequent vector for cyberattacks. Despite the evolution of protection systems, the human factor continues to be the weakest link in cybersecurity, being exploited by social engineering techniques. This work presents the open-source tool *StopEmailSpoofing*, developed to automate the detection of email spoofing vulnerabilities in domain names. The tool analyzes all 295 possible combinations between SPF and DMARC protocols, performing DNS queries to assess domain susceptibility. Unlike existing solutions, it offers complete coverage of authentication protocols and provides immediate corrective actions. Validation was performed through a case study with Brazilian public higher education institutions,

demonstrating efficiency in identifying failures and contributing to strengthening the resilience of organizational digital communications.

Keywords: Email spoofing; SPF; DMARC; Cybersecurity; Communications security.

1. Introdução

O e-mail tornou-se um dos principais meios de comunicação da sociedade contemporânea. Estima-se que, até 2027, cerca de 408,2 bilhões de mensagens sejam enviadas diariamente (Statista, 2025). Por ser fundamental na comunicação individual e corporativa, o e-mail também se torna um vetor de ataque amplamente explorado por fontes de ameaça (Shen et al., 2021).

A despeito da constante evolução da proteção de redes e sistemas, o fator humano permanece sendo o elo mais fraco da segurança cibernética. Em decorrência disso, atores maliciosos se valem cada vez mais de técnicas de engenharia social para conseguirem comprometer seus alvos (Hu & Wang, 2018). Neste sentido, a segurança de e-mails tem se tornado um tema central devido à dependência das comunicações digitais e ao surgimento de ameaças cada vez mais sofisticadas. Em um cenário em que grande parte das interações empresariais e pessoais ocorre via correio eletrônico, a garantia da autenticidade das mensagens e a proteção contra fraudes têm implicações diretas na continuidade dos negócios, na privacidade dos usuários e na salvaguarda de dados sensíveis (Carvalho et al., 2023).

Combinando conteúdo de e-mails de *phishing* sofisticados com técnicas de engenharia social, o ataque de falsificação de endereços de e-mail (também conhecido como *e-mail spoofing*) afeta bilhões de usuários em todo o mundo. Trata-se de uma atividade maliciosa que adultera o remetente de um e-mail e engana os destinatários, fazendo-os acreditar que a mensagem foi enviada por um remetente confiável, quando, na realidade, o remetente é o atacante (Yu et al., 2022). Desta forma, protocolos de autenticação, como SPF (*Sender Policy Framework*), DKIM (*DomainKeys Identified Mail*) e DMARC (*Domain-based Message Authentication, Reporting and Conformance*), tornaram-se ferramentas essenciais para organizações que buscam atestar a legitimidade de suas mensagens de e-mail (Carvalho et al., 2023).

1.1. Problema

Apesar da evolução das metodologias de detecção de mensagens com endereço de remetente falsificado, vulnerabilidades técnicas e operacionais persistem no que diz respeito à adoção e à correta configuração de protocolos como SPF e DMARC (Hu & Wang, 2018). Além disso, estudos como o de Nmachi (2023) destacam a importância de não concentrar esforços apenas nas características técnicas, mas também em como usuários e administradores compreendem o funcionamento desses mecanismos. Autores como Maroofi et al. (2021) apontam que grande parte das falhas decorre de implementações parciais ou configurações incorretas dos referidos protocolos, o que, em última análise, permite que invasores forjem remetentes de forma efetiva. Embora tenha havido avanços consideráveis, a elaboração de diretrizes práticas e de ferramentas

de suporte para a configuração e a manutenção desses protocolos ainda representam um desafio.

Neste trabalho, apresenta-se uma ferramenta de fácil utilização e de código aberto - denominada *StopEmailSpoofing* - que cobre todas as combinações possíveis entre as configurações dos referidos protocolos de autenticação, auxiliando administradores na automatização da detecção de vulnerabilidades de falsificação de e-mails em seus domínios e sugerindo ações detalhadas para a mitigação imediata do problema.

2. Referencial Teórico

Nesta seção, discorre-se sobre o funcionamento do ecossistema de correio eletrônico; mecanismos de autenticação de remetente em mensagens de e-mail; ataques de falsificação de endereço de e-mail e sua utilização em campanhas de *phishing*; e sobre as extensões *Simple Mail Transfer Protocol* (SMTP) criadas para a mitigação do problema. Por fim, elencam-se trabalhos correlatos.

2.1. Funcionamento do ecossistema de e-mail

O e-mail é amplamente utilizado em comunicações diárias, exercendo papel fundamental em conversas e transações confidenciais. Em muitos países e organizações, ele é o principal recurso para comunicações oficiais (Nmachi, 2023). Além disso, representa a ferramenta de comunicação mais adotada no mundo, sobretudo em ambientes empresariais (Gallo et al., 2024).

O SMTP é o principal protocolo para serviços de correio eletrônico. Quando um remetente redige uma mensagem, seu *Mail User Agent* (MUA) a transmite ao seu *Mail Transport Agent* (MTA) por meio dos protocolos SMTP ou HTTP. Em seguida, o MTA de origem encaminha o e-mail ao MTA de destino utilizando SMTP (Shen et al., 2021). Para isso, o servidor MTA de saída utiliza o *Domain Name System* (DNS) para encontrar o MTA do destinatário (Meshram et al., 2024). Por fim, o MTA de destino entrega a mensagem ao MUA do destinatário, usando protocolos como HTTP, IMAP ou POP3 (Shen et al., 2021).

2.2. Mecanismos de autenticação de remetente em mensagens de e-mail

A autenticação do remetente em uma troca de e-mails é fundamental para verificar se a mensagem realmente foi originada da fonte declarada (Maroofi et al., 2021).

Segundo Shen et al. (2021), a autenticação no processo de transmissão de e-mails envolve quatro etapas importantes: **(1) Autenticação no envio:** ao enviar um e-mail a partir do MUA via protocolo SMTP, o remetente precisa inserir seu nome de usuário e senha para autenticação. Nessa etapa, o MTA do remetente deve não apenas verificar a identidade do usuário, mas também garantir que o campo '*Mail From*' seja consistente com o '*Auth username*'; **(2) Verificação no recebimento:** o MTA do destinatário recebe o e-mail e valida a autenticidade do remetente por meio dos protocolos SPF, DKIM e DMARC; **(3) Renderização de interface:** o MUA fornece ao destinatário uma exibição amigável do e-mail. A maioria dos clientes de e-mail populares não

apresenta os resultados da verificação de autenticidade ao usuário; **(4) Verificação no encaminhamento de e-mails:** um servidor de encaminhamento reenvia automaticamente um e-mail, devendo verificar o endereço do remetente. Se a assinatura DKIM estiver ativa, o status original da verificação deve ser *'pass'* antes que uma nova assinatura DKIM seja adicionada.

2.3. Falsificação de endereço de e-mail em campanhas de *phishing*

As especificações do correio eletrônico datam da década de 1970, período em que aspectos de segurança não foram priorizados, deixando lacunas que persistem até hoje (Blechsmidt & Stock, 2023). Devido a sua importância e ampla utilização, o e-mail tornou-se um dos vetores de ataque mais explorados por atores maliciosos (Shen et al., 2021). As vulnerabilidades são exploradas de diversas maneiras, aproveitando tanto as fraquezas técnicas quanto as vulnerabilidades cognitivas dos usuários (Gallo et al., 2024).

Vítimas de ataques de *phishing* são frequentemente atraídas por mensagens que contêm anexos maliciosos ou levam a sites falsos cuidadosamente elaborados. A construção dos e-mails de *phishing* é a principal preocupação dos atacantes, que aplicam técnicas para aumentar a credibilidade de suas mensagens e utilizam estratégias para enganar as percepções da vítima (Gallo et al., 2024). Muitas vezes, as mensagens transmitem um senso de urgência ou autoridade, imitando comunicações de organizações conhecidas e confiáveis (D'Angelone, 2022).

Maroofi et al. (2020) classificam a falsificação de e-mail em dois tipos: **(1) Comprometimento de servidores legítimos**, quando os invasores comprometem servidores e utilizam seu MTA para enviar e-mails às vítimas; e **(2) Falsificação de domínio** (*domain spoofing*), quando os atacantes conseguem enviar e-mails, a partir de seus próprios servidores, em nome de domínios legítimos. A falsificação de endereços de e-mail é frequentemente utilizada por inúmeros cibercriminosos em tentativas de *phishing*. Ao criar uma mensagem, o ator malicioso pode fraudar os cabeçalhos *'From'* e *'Return-path'* da mensagem para que a mensagem pareça ter sido enviada de uma conta legítima e confiável (Sethuraman et al., 2024).

A segurança na transmissão de e-mails depende de uma cadeia de confiança multilateral, mantida por diversos serviços, o que aumenta sua vulnerabilidade sistêmica a ataques cibernéticos. No processo de comunicação via SMTP, as informações de identidade do remetente estão distribuídas de forma complexa em vários campos: **(1) Auth username**, o nome de usuário utilizado no comando *'AUTH'* para autenticar o cliente no MTA de envio; **(2) MAIL From**, o remetente que constará no envelope do e-mail, usado principalmente para verificação de identidade durante o processo de entrega da mensagem ao MTA de destino; **(3) From**, o remetente exibido no corpo do e-mail, sendo o endereço que o MUA mostra ao destinatário; e; **(4) Sender**, utilizado para identificar o remetente real quando há vários endereços no campo *'From'*. A inconsistência entre esses campos fornece a base para ataques de falsificação de endereços de e-mail (Shen et al., 2021).

2.4. Extensões SMTP: SPF, DKIM e DMARC

Para combater a falsificação de endereços e-mail, os servidores podem empregar extensões SMTP, como SPF, DKIM e DMARC para autenticar a identidade do remetente e exibir uma garantia de credibilidade para os usuários que lêem as mensagens (Chen, Paxson & Jiang, 2020). As extensões são publicadas em forma de registros TXT no DNS do domínio remetente. Como a implementação destes protocolos não é mandatória e depende exclusivamente do provedor de e-mails, os usuários finais não possuem influência sobre sua adoção (Hu & Wang, 2018).

Essas extensões definem regras sobre quem está autorizado a enviar mensagens em nome de um domínio e fornecem estratégias para combater e-mails falsificados. Quando configuradas adequadamente, podem eliminar o problema de falsificação de domínio por completo (Maroofi et al., 2020). Desta forma, a segurança de e-mail exige esforços bidirecionais: uma configuração correta dos protocolos por parte do remetente e uma validação rigorosa por parte do destinatário (Zhang et al., 2023). Configurações incorretas ou ausentes expõem as organizações a riscos de falsificação de domínios em ataques de *phishing* (Shen et al., 2021).

SPF

O SPF é um protocolo de autenticação baseado em endereço IP. Ele registra o domínio do remetente e vincula esse domínio a um IP específico, permitindo que o destinatário verifique, por meio de consulta DNS, se o e-mail realmente veio de um servidor autorizado (Shen et al., 2021). Durante a entrega do e-mail via SMTP, o servidor do destinatário autentica o MTA do remetente com base na identidade fornecida nos campos 'HELO' ou 'MAIL From', comparando o registro SPF publicado com o endereço IP do remetente (Maroofi et al., 2020). Um registro SPF versão 1 válido deve começar com a string *v=spf1*, seguida por outros mecanismos, qualificadores e modificadores. Os mecanismos descrevem o conjunto de servidores de e-mail autorizados para um domínio e podem ser prefixados com um dos quatro qualificadores: + (*Pass*), - (*Fail*), ~ (*SoftFail*) e ? (*Neutral*). Os mecanismos SPF mais comuns são:

- **ip4** e **ip6**: especificam um endereço, ou um conjunto de endereços, IPv4 (ou IPv6) a serem comparados com o endereço IP do remetente;
- **a** e **mx**: instruem a realizar primeiro uma consulta DNS para registros A (ou MX) de um determinado domínio e, em seguida, comparar os endereços IP retornados com o endereço IP do remetente;
- **include**: instrui a incluir a regra SPF de outro domínio na avaliação; e
- **all**: sempre corresponde; ou seja, seu qualificador correspondente determina a decisão final.

DKIM

O DKIM, por sua vez, baseia-se em assinaturas digitais. Utilizando criptografia de chave assimétrica, o remetente insere uma assinatura digital no cabeçalho do e-mail, o que possibilita a identificação de tentativas de falsificação ou adulteração durante a transmissão. O destinatário, ao receber a mensagem, consulta o DNS do remetente para obter a chave pública e verificar a assinatura, atestando se o e-mail foi ou não adulterado (Shen et al., 2021).

DMARC

Já o DMARC é um mecanismo de autenticação que atua com base nos resultados de SPF e DKIM. Especificamente, o DMARC adota uma lógica de ‘OR’: se a mensagem for aprovada em ao menos um dos protocolos (SPF ou DKIM) e o campo *From* estiver alinhado com o identificador autenticado, o e-mail será considerado válido (Shen et al., 2021). A extensão compara os domínios verificados pelo SPF aos que estão listados no campo ‘*From*’ do cabeçalho do e-mail por meio de um mecanismo de alinhamento que exige que esses domínios correspondam totalmente ou parcialmente. Por exemplo, o DMARC verifica se o domínio em ‘*MAIL From*’ e em ‘*From*’ são ou não compatíveis. No caso de falha no teste de alinhamento, a política DMARC pode definir o que fazer com a mensagem: aceitar, rejeitar ou colocar em quarentena (Maroofi et al., 2020). A seguir, elenca-se as *tags* DMARC que, quando configuradas incorretamente, podem ser exploradas por um adversário:

- **aspf (alinhamento para SPF)**: especifica se o modo de alinhamento estrito ‘s’ ou relaxado ‘r’ é exigido pelo proprietário do domínio. O valor padrão é o modo relaxado. No modo estrito, o nome de domínio usado no SPF deve ser exatamente o mesmo que o domínio utilizado no campo ‘*From*’ do cabeçalho. No modo relaxado, qualquer subdomínio pode ser usado no campo ‘*From*’ e ainda assim resultar em uma checagem válida;
- **p (política)**: define a ação a ser tomada pelo destinatário caso o teste de alinhamento resulte em ‘*FAIL*’. Os valores possíveis para essa *tag* são (1) *none*, nenhuma ação específica; (2) *quarantine*, a mensagem é considerada suspeita e pode ser entregue como *spam*; e (3) *reject*, o proprietário do domínio deseja rejeitar e-mails ainda durante a transação SMTP; e
- **sp (política para subdomínios)**: possui a mesma sintaxe da *tag* ‘p’, mas se aplica aos subdomínios do domínio principal. Na ausência da *tag* ‘sp’, a política definida na *tag* ‘p’ deve ser aplicada a todos os subdomínios. Se os subdomínios não forem usados para enviar e-mails, o proprietário pode definir essa *tag* com o valor *reject* para evitar falsificação de endereços de e-mails a partir de subdomínios.

Autenticação no Recebimento

O processo completo de verificação de autenticidade no recebimento da mensagem inicia-se pelo SPF, que faz a extração do domínio presente no campo ‘*Return-Path*’ do cabeçalho da mensagem, juntamente com o endereço IP do servidor remetente. Em seguida, realiza uma consulta DNS para identificar a existência de um registro SPF associado a esse domínio. Caso o registro não exista, o resultado da verificação é ‘*SPF=NONE*’. Se o registro estiver presente, procede-se à validação para determinar se o endereço IP está autorizado a enviar mensagens em nome do domínio, conforme as regras especificadas no próprio registro (*-all, ~all, ?all, +all*). Quando o endereço IP está explicitamente autorizado, a autenticação resulta em ‘*SPF=PASS*’; caso contrário, ou se o registro estiver malformatado, o resultado é ‘*SPF=FAIL*’.

O fluxo de autenticação continua com a validação DKIM, que se inicia verificando a presença do cabeçalho ‘*DKIM-Signature*’ na mensagem. Caso ele esteja ausente ou malformatado, o resultado é ‘*DKIM=NONE/ERROR*’. Se o cabeçalho existir, prossegue-

se à consulta DNS para o domínio especificado no parâmetro ‘d=’, utilizando o seletor ‘s=’, a fim de obter a chave pública correspondente. A ausência desse registro ou de uma chave pública válida resulta em ‘DKIM=FAIL’. Quando o registro é encontrado, verifica-se a **integridade** da mensagem calculando o *hash* do corpo da mensagem e comparando-o com o valor indicado no campo ‘bh=’. Se houver divergência, o resultado é ‘DKIM=FAIL’. Em caso de correspondência, passa-se à etapa de **autenticidade**, na qual o valor do campo ‘b=’ é descryptografado com a chave pública e comparado ao *hash* dos cabeçalhos especificados no campo ‘h=’. Se os valores coincidirem, a autenticação é bem-sucedida e ‘DKIM=PASS’; caso contrário, o resultado é ‘DKIM=FAIL’.

Por fim, o DMARC verifica se existe um registro DMARC associado ao domínio que consta no campo ‘From’. Caso o registro esteja ausente ou malformatado, o resultado é ‘DMARC=NONE’. Se o registro existir, o mecanismo avalia os resultados de SPF e DKIM. Quando ambos falham, ou seja, ‘SPF=FAIL’ e ‘DKIM=FAIL’, a autenticação é considerada mal-sucedida e ‘DMARC=FAIL’. Contudo, se pelo menos um deles tiver sucesso e estiver alinhado com o domínio em ‘From’ — isto é, se ‘SPF=PASS’ e simultaneamente o domínio em ‘Return-Path’ corresponder ao domínio em ‘From’; ou se ‘DKIM=PASS’ e simultaneamente o domínio no parâmetro ‘d=’ também corresponder ao de ‘From’ —, o resultado é ‘DMARC=PASS’. Com base nesse resultado e na política ‘p=’ definida no registro DMARC, o servidor de e-mail aplicará a ação especificada: **reject** (mensagem rejeitada), **quarantine** (mensagem enviada para quarentena ou pasta de *spam*) ou **none** (nenhuma ação específica, permitindo a entrega). Destaca-se que outras regras de filtragem *antispam* do servidor ou de ferramentas externas podem complementar o tratamento da mensagem, inclusive se sobrepondo à decisão final de DMARC.

Desta forma, observa-se ser fundamental que os domínios estabeleçam políticas apropriadas de SPF e DMARC para reduzir a chance de ataques bem-sucedidos. Por exemplo, a inexistência ou a definição de uma política fraca junto à extensão DMARC pode colocar um servidor de e-mails em uma posição difícil, pois nenhuma instrução para rejeitar um e-mail é dada quando SPF, DKIM ou ambos falham durante o processo de autenticação (Maroofi et al., 2021). Além disso, se o MTA do destinatário não oferecer suporte à verificação de SPF ou DMARC, independentemente do quão rigorosas sejam as regras adotadas pelo domínio remetente, elas não serão eficazes. Uma configuração incorreta de SPF ou DMARC é tão perigosa quanto a ausência dessas regras, pois o resultado da avaliação não levará a uma decisão acertada (Maroofi et al., 2020).

2.5. Trabalhos Correlatos

Diversas ferramentas para detecção de vulnerabilidades relacionadas à falsificação de endereços de e-mail já foram propostas. A solução *MXToolbox SuperTool*¹, por exemplo, constitui um utilitário unificado de avaliação de serviços de e-mail e DNS, integrando múltiplas funcionalidades de verificação em uma interface web. O sistema aceita domínios, endereços IP ou *hostnames* como entrada, mantendo histórico cronológico dos resultados para referência futura.

¹ <https://mxtoolbox.com/SuperTool.aspx>

D'Angelone (2022) desenvolveu uma ferramenta de medição em larga escala para pesquisas sobre adoção dos protocolos SPF e DMARC. O sistema, implementado em Python com arquitetura modular, opera através de um *crawler* de domínios que coleta dados de mais de 1,4 milhão de domínios utilizando APIs comerciais ou arquivos CSV. A ferramenta executa consultas DNS automatizadas para verificar a presença, configuração e políticas dos registros SPF e DMARC, normalizando os resultados e identificando erros de configuração. Os dados são processados e armazenados em formato CSV padronizado, permitindo análises comparativas e reprodução experimental.

Porém, a ferramenta de maior destaque é o *Spoofy*² (2023). Desenvolvida e disponibilizada em código-aberto por Matthew Keeley, é uma evolução das soluções *SpoofCheckSelfTest*³ (2015) e *SpoofCheck*⁴ (2016) da empresa Bishop Fox e oferece um diagnóstico automatizado da vulnerabilidade de domínios à falsificação de e-mail através da análise das configurações SPF e DMARC. O sistema executa consultas DNS autoritativas e implementa um algoritmo de decisão para determinar a suscetibilidade dos domínios à falsificação. Os resultados são processados através de uma tabela de combinações SPF e DMARC. Contudo, a referida tabela foi construída a partir de testes empíricos que consistiram no envio de mensagens falsificadas utilizando a ferramenta *EmailSpoofTest.com*⁵ e na observação do comportamento de serviços como Gmail, ProtonMail e Microsoft 365 ao receber estas mensagens. Esta abordagem apresenta algumas limitações metodológicas.

Haja vista o objetivo de detectar a vulnerabilidade de domínios (e não de MTAs/MUAs), as medidas efetivas para reduzir a exposição a ataques de *spoofing* baseiam-se unicamente na correta configuração das extensões SMTP no DNS do domínio. Realizar o diagnóstico a partir do comportamento específico de determinados MTAs/MUAs pode levar a uma falsa conclusão de segurança. Isso porque o destinatário das mensagens falsificadas pode utilizar qualquer outro MTA/MUA que não tenha sido contemplado nos testes. É válido ressaltar que as decisões de autenticação de cada MTA/MUA podem diferir das orientações configuradas pelas extensões SMTP e serem complementadas, ou mesmo sobrepostas, por mecanismos de filtragem *antispam*.

Na mesma linha, a partir da abordagem escolhida, o *Spoofy* agrupa os estados de vulnerabilidade em 8 categorias, sendo algumas dessas classificadas como “Dependendo do *Mailbox*”. Repisa-se que não se pode depender do comportamento do MTA/MUA para a avaliação da vulnerabilidade intrínseca a um domínio. Logo, uma ferramenta com o objetivo de avaliar a vulnerabilidade de um domínio a *spoofing* deveria concentrar-se unicamente nas configurações declaradas no DNS por meio das extensões SMTP, sem requerer resultados observados a partir da interpretação de MTAs/MUAs específicos. Somente assim seria possível fornecer uma avaliação alinhada às reais possibilidades de intervenção por parte dos administradores de domínio. Por fim, a tabela de combinações

² <https://github.com/MattKeeley/Spoofy>

³ <https://github.com/BishopFox/SpoofcheckSelfTest>

⁴ <https://web.archive.org/web/20220211170519/https://github.com/BishopFox/spoofcheck>

⁵ <https://emailspooftest.com/>

do *Spoofy* não leva em consideração todas as combinações possíveis entre ‘all’, ‘aspf’, ‘p’ e ‘sp’.

Desta forma, o presente estudo propõe um aprimoramento das soluções já existentes por: (1) cobrir todas as 295 possibilidades de combinação entre ‘all’, ‘aspf’, ‘p’ e ‘sp’ que podem influenciar na suscetibilidade de um domínio principal, bem como de seus subdomínios, à falsificação; (2) oferecer sugestões imediatas e precisas de mitigação personalizadas para cada domínio avaliado; e (3) verificar a possível adoção de DKIM e *Catch-All*.

3. Metodologia

Esta é uma pesquisa de natureza aplicada, haja vista ser uma investigação científica que busca resolver um problema prático e desenvolver uma solução específica para uma questão concreta, visando a aplicação imediata do conhecimento gerado. Tem caráter utilitário, direcionado a melhorias tecnológicas, processos ou intervenções em contextos reais.

A partir desta perspectiva, optou-se por uma abordagem qualitativa, que dispensa o uso de métodos e técnicas estatísticas, concentrando-se principalmente no seu processo e significado. Dessa forma, busca-se interpretar e atribuir sentido a um fenômeno do mundo real (Silva e Menezes, 2005).

Este estudo possui caráter exploratório, uma vez que tem como objetivo proporcionar maior familiaridade com o problema da falsificação de endereços de e-mail, com vistas a torná-lo mais explícito e construir hipóteses, aprimorando ideias e soluções (Gil, 2017).

4. Método, Resultados e Discussões

Com o objetivo de ajudar administradores a automatizar a detecção de vulnerabilidades a ataques de falsificação de endereço de e-mail contra seus domínios, propõe-se a ferramenta de código-aberto *StopEmailSpoofing*⁶.

Os usuários podem fornecer uma lista ou um único domínio para a avaliação. Por meio de consultas DNS, além de verificar se os domínios fornecidos são principais ou subdomínios e obter registros SOA (*Start of Authority*), NS (*Nameserver*) e MX (*Mail Exchange*), a ferramenta coleta os registros SPF e DMARC e, considerando a configuração combinada desses registros, realiza conclusões quanto à suscetibilidade dos domínios analisados às categorias de vulnerabilidade à falsificação dispostas na Tabela 1. Por fim, a partir da conclusão quanto à vulnerabilidade do domínio, a ferramenta aponta ações detalhadas de mitigação para que o administrador possa sanar o problema, como exemplificado na Figura 1.

As conclusões sobre o estado de vulnerabilidade e as sugestões de mitigação são feitas a partir do que se dispõe em uma tabela⁷ que relaciona todas as 295 combinações possíveis

⁶ <https://github.com/v1sco/stopemailspoofing>

⁷ https://github.com/v1sco/stopemailspoofing/blob/main/ULTIMATE_TABLE.xlsx

entre o mecanismo ‘all’ do registro SPF e as tags ‘p’, ‘aspf’ e ‘sp’ do registro DMARC, tanto para domínio principal quanto para subdomínios, conforme mostrado na Figura 2.

Para testes e confirmações empíricas, dois domínios foram adquiridos: um para agir como remetente e outro como destinatário. As extensões SMTP do domínio remetente foram configuradas no DNS de acordo com cada caso analisado. O domínio destinatário foi vinculado a um servidor de e-mails *mailcow*⁸ com a solução *antispam Rspamd*⁹ embutida, o que permitiu o controle personalizado da autenticação, análise e regras de processamento das mensagens.

Categoria	
1	A falsificação do domínio principal e de subdomínios é possível
2	Apenas a falsificação do domínio principal é possível
3	Apenas a falsificação de subdomínios é possível
4	Condição desconhecida (possivelmente vulnerável devido a erro de sintaxe nos registros)
5	A falsificação não é possível

Tabela 1 – Categorias de vulnerabilidade à falsificação consideradas pela ferramenta

```

SPF:
[*] SPF Record: v=spf1 ip4:████████████████████ ip4:████████████████████ ip4:████████████████████ -all
All Mechanism: -all
DNS Query Count: 0
Too Many DNS Queries: false

DMARC:
[*] DMARC Record: v=DMARC1; p=quarantine; rua=mailto:suporte@████████████████████
Policy: quarantine
Pct:
ASPF:
Subdomain Policy:
Forensic Reports:
Aggregate Reports: mailto:suporte@████████████████████

Spoofing:
[*] Spoofability: Spoofing is not possible.

For additional security it is recommended:
SPF All Mechanism: Keep it the way it is.
DMARC Policy (p=): Keep it the way it is or replace it by "p=reject".
DMARC ASPF (aspf=): Add "aspf=s" or "aspf=r".
DMARC Subdomain Policy (sp=): Add "sp=reject" or "sp=quarantine".
DMARC PCT: Consider adding pct=100.
DMARC RUF: Consider adding an email address like ruf=example@example.mail
BIMI: Consider setting up a BIMI record.

Results saved in results.csv
    
```

Figura 1 – Exemplo de saída da ferramenta com sugestões de mitigação

⁸ <https://mailcow.email/>

⁹ <https://rspamd.com/>

	ALL	P	ASPF	SP	DOMAIN TYPE	RESULT	SPOOFABILITY
261	-all	none	No aspf=	quarantine	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
					SUBDOMAIN	QUARANTINE	
262	-all	none	No aspf=	reject	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
					SUBDOMAIN	REJECT	
263	-all	none	r	No sp=	ORG. DOMAIN	INBOX	Organizational domain spoofing and subdomain spoofing are possible.
					SUBDOMAIN	INBOX	
264	-all	none	r	none	ORG. DOMAIN	INBOX	Organizational domain spoofing and subdomain spoofing are possible.
					SUBDOMAIN	INBOX	
265	-all	none	r	quarantine	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
					SUBDOMAIN	QUARANTINE	
266	-all	none	r	reject	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
					SUBDOMAIN	REJECT	
267	-all	none	s	No sp=	ORG. DOMAIN	INBOX	Organizational domain spoofing and subdomain spoofing are possible.
					SUBDOMAIN	INBOX	
268	-all	none	s	none	ORG. DOMAIN	INBOX	Organizational domain spoofing and subdomain spoofing are possible.
					SUBDOMAIN	INBOX	
269	-all	none	s	quarantine	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
					SUBDOMAIN	QUARANTINE	
270	-all	none	s	reject	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
					SUBDOMAIN	REJECT	
271	-all	quarantine	No aspf=	No sp=	ORG. DOMAIN	QUARANTINE	Spoofing is not possible.
					SUBDOMAIN	QUARANTINE	
272	-all	quarantine	No aspf=	none	ORG. DOMAIN	INBOX	Only subdomain spoofing is possible.
					SUBDOMAIN	QUARANTINE	
273	-all	quarantine	No aspf=	quarantine	ORG. DOMAIN	QUARANTINE	Spoofing is not possible.
					SUBDOMAIN	QUARANTINE	
274	-all	quarantine	No aspf=	reject	ORG. DOMAIN	QUARANTINE	Spoofing is not possible.
					SUBDOMAIN	REJECT	

Figura 2 – Exemplo de combinações de mecanismos e tags SPF/DMARC e a situação de vulnerabilidade correspondente consideradas pela ferramenta

Incrementalmente, a ferramenta também coleta os registros DKIM e BIMi (*Brand Indicators for Message Identification*). Ressalta-se que para a coleta de DKIM é necessário que se conheça o seletor ‘s=’ utilizado, o que somente seria possível com acesso a uma mensagem de e-mail legítima enviada a partir do domínio analisado. Desta forma, a ferramenta utiliza uma lista de 100 seletores conhecidos para realizar as consultas DNS e tentar identificar a presença de DKIM. Logo, a conclusão da ferramenta refere-se a ter ou não encontrado o registro DKIM e, em caso negativo, sugerir que o administrador certifique-se de ter configurado a extensão, uma vez que não é possível determinar com certeza que ela não foi adotada.

A ferramenta ainda verifica se o servidor de e-mail do domínio adota uma política de *catch-All*. *Catch-all* é uma configuração que permite que o servidor aceite mensagens enviadas para endereços inexistentes dentro do domínio. Em vez de rejeitar ou devolver as mensagens que foram enviadas para endereços errados, o servidor redireciona todas essas mensagens para uma conta de e-mail designada, chamada de *catch-all*. Isso pode ser útil para reduzir a enumeração e validação de endereços de e-mail por parte de atacantes, uma vez que a resposta dada pelo servidor SMTP não permitirá aos atacantes confirmarem a existência de endereços de e-mail coletados e que se tornariam alvos em uma campanha de *phishing*.

Todos os resultados das avaliações feitas pela ferramenta são apresentados em interface textual e exportados em formato CSV, permitindo integração com outras aplicações de tratamento e análise de dados. A ferramenta foi desenvolvida em Go (Golang), por ser uma linguagem de programação que oferece vantagens quanto a utilização, alteração e acréscimo de módulos. Um fluxograma da solução e uma descrição dos módulos desenvolvidos para a aplicação podem ser encontrados na Figura 3 e Tabela 2, respectivamente.

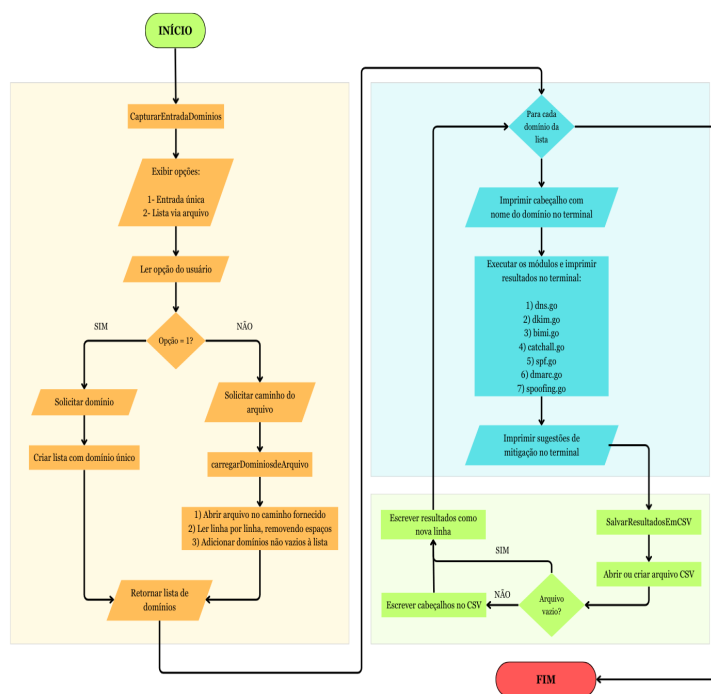


Figura 3 – Fluxograma de funcionamento da ferramenta proposta

Módulo	Descrição
dns.go	Classifica o nome informado como domínio ou subdomínio usando a biblioteca publicsuffix . Em seguida, ObterSOARecord consulta o registro SOA do domínio; se encontrado, armazena o nome do <i>nameserver</i> e procura seu endereço IP. Já ObterMXRecords busca registros MX para listar os servidores de e-mail associados.
catchall.go	Usa a biblioteca AfterShip/email-verifier para verificar se um domínio aceita e-mails para qualquer endereço. A função NovoCatchAllVerifier cria um verificador com checagem SMTP habilitada. O método VerificarCatchAll consulta se o domínio possui registro MX; em caso afirmativo, faz uma verificação SMTP para determinar se a caixa é <i>catch-all</i> e preenche a estrutura CatchAllResult .
dkim.go	Define a estrutura DKIMResult e a lista de 100 seletores padrão usados por muitos provedores. A função VerificarDKIM recebe uma lista de domínios, valida o nome de cada domínio e, para cada seletor padrão, monta uma consulta do tipo selector._domainkey.<domínio> ; se encontrar um registro TXT contendo a chave DKIM, marca o resultado como "SIM" e armazena o registro. Caso nenhum seletor retorne, indica que o DKIM não foi encontrado.
bimi.go	Define a estrutura BIMI com campos para domínio, servidor DNS e informações extraídas do registro BIMI. O construtor NovoBIMI consulta default._bimi.<domínio> via DNS, salvando o registro textual se este contiver "v=BIMI" e extraíndo a versão, a localização do logotipo e a autoridade por meio das funções ExtrairVersao , ExtrairLocalizacao e ExtrairAutoridade . Caso o registro não exista, o campo BIMIRecord é definido como "BIMI não encontrado".

Módulo	Descrição
spf.go	A estrutura SPF inclui o domínio, registro SPF e informações derivadas. NovoSPF chama ObterSPFRecord , que procura nos registros TXT um início com “v=spf1”; se encontrado, armazena o registro. Depois, ObterMecanismoAll identifica o mecanismo all ; ContarConsultasDNS analisa recursivamente as diretivas <i>include</i> e <i>redirect</i> , bem como mecanismos a , mx , ptr e exists , para contar quantas consultas DNS o SPF realiza. Se esse número exceder 10, TooManyDNSQueries é marcado como verdadeiro.
dmarc.go	A estrutura DMARC guarda o domínio, servidor DNS e campos extraídos. NovoDMARC chama ObterDMARCRecord para consultar _dmarc.<domínio> ; se o domínio for um subdomínio sem registro DMARC, tenta o domínio organizacional (eTLD+1). Após localizar um registro contendo “DMARC1”, a estrutura extrai política (p=), percentual (pct=), alinhamento SPF (aspf=), política para subdomínios (sp=) e endereços para relatórios forenses e agregados.
spoofing.go	Define a estrutura Spoofing para combinar informações de SPF e DMARC. A função CheckSpoofing verifica várias combinações dessas configurações para determinar se é possível falsificar o domínio. Ela usa a tabela de condições para identificar cenários em que <i>spoofing</i> não é possível, é possível apenas para o domínio organizacional ou apenas para subdomínios, ou é totalmente possível. Retorna uma mensagem explicativa indicando o nível de vulnerabilidade.
suggestion.go	Oferece recomendações de segurança. A função Suggestion avalia o mecanismo <i>all</i> do SPF e as opções DMARC (<i>p</i> , <i>aspf</i> e <i>sp</i>). Dependendo dos valores, sugere manter, corrigir ou adicionar configurações

Tabela 2 – Módulos

As pesquisas sobre engenharia social e *phishing* têm levado ao desenvolvimento de técnicas de prevenção e capacitação em empresas, mas ainda existem áreas inexploradas, como ataques a instituições educacionais e abordagens específicas voltadas para docentes e estudantes (Camacho Coronel et al., 2024). Considerando-se que a segurança cibernética vem ganhando papel de destaque e mostrando-se imprescindível para os avanços na transformação digital brasileira, inclusive no setor público (Georg et al., 2022), realizou-se um estudo de caso com os domínios relacionados a todas as instituições públicas de ensino superior brasileiras a fim de validar a eficiência da ferramenta desenvolvida. Este grupo específico de instituições foi escolhido por constituir uma área da administração pública que desenvolve pesquisas, tecnologias e conhecimentos sensíveis, sendo flagrante a importância da mitigação de vulnerabilidades de falsificação de endereços de e-mail para combater campanhas de *phishing* que possam comprometer esta produção.

Uma lista das instituições de ensino superior brasileiras foi obtida a partir do *website* do Ministério da Educação¹⁰. A lista foi filtrada para conter apenas as instituições públicas, resultando num universo de 345 instituições. Os nomes de domínio destas instituições foram coletados utilizando-se técnicas de Inteligência de Fontes Abertas (OSINT). Por fim, a lista final com os 345 nomes de domínio foi submetida à ferramenta *StopEmailSpoofing*. Os resultados são apresentados na Tabela 3 e referem-se a agosto de 2025. Nota-se que cerca de 80% dos nomes de domínio das instituições públicas de ensino superior brasileiras estão vulneráveis a falsificação de e-mail. Isso comprova

¹⁰ https://dadosabertos.mec.gov.br/images/conteudo/Ind-ensino-superior/2022/PDA_Lista_Instituicoes_Ensino_Superior_do_Brasil_EMEC.csv

a persistência do problema e implica dizer que, na grande maioria destas instituições, atacantes podem enviar mensagens de e-mail se passando por reitores, alunos, professores e pesquisadores para aumentar a credibilidade de campanhas de *phishing* e obter acesso a conhecimentos e tecnologias sensíveis produzidos por institutos e universidades.

		Parâmetros	Quantidade	Porcentagem
Nome de Domínio		Domínio	288	83,48%
	Subdomínio		57	16,52%
SPF		Inexistente	71	20,58%
	+all	0	0,00%	
	-all	106	30,72%	
	~all	151	43,77%	
	?all	16	4,64%	
DKIM		Encontrado	155	44,93%
	Não encontrado	190	55,07%	
DMARC	p	Inexistente	136	39,42%
		none	113	32,75%
		quarantine	77	22,32%
		reject	18	5,22%
		Inexistente	291	84,35%
	sp	none	37	10,72%
		quarantine	11	3,19%
		reject	6	1,74%
Vulnerabilidade		Não vulnerável	71	20,58%
	Apenas domínio principal vulnerável	0	0,00%	
	Apenas subdomínios vulneráveis	23	6,67%	
	Domínio principal e subdomínios vulneráveis	249	72,17%	
	Erro de sintaxe (vulnerável)	2	0,58%	

Tabela 3 – Análise dos domínios de instituições públicas federais brasileiras de ensino superior a partir da ferramenta proposta (ago. 2025)

5. Conclusões

Este trabalho teve como objetivo desenvolver uma ferramenta para detecção da vulnerabilidade de domínios a ataques de falsificação de endereços de e-mail, ataques estes que - a despeito de configurarem um problema antigo - ainda são muito explorados atualmente. A ferramenta foi projetada para avaliar a implementação e configuração de protocolos como SPF, DKIM e DMARC, oferecendo diagnósticos detalhados sobre

a exposição de domínios a ataques de *spoofing*. Os testes demonstraram que a solução é oportuna e que pode auxiliar administradores e equipas de segurança na detecção de falhas e na pronta adoção de medidas corretivas. A principal contribuição deste estudo está na automatização e na completude da verificação das extensões de autenticação de e-mails, fornecendo um mecanismo eficiente e acessível para fortalecer a segurança e a resiliência das comunicações digitais. Entretanto, algumas limitações foram observadas. A solução apresentada cobre apenas a autenticação no recebimento de mensagens de e-mail. Ataques avançados - que não foram considerados na atual abordagem da ferramenta - exploram falhas durante a renderização do remetente pelo MUA do destinatário.

Para trabalhos futuros, sugere-se a ampliação do escopo da ferramenta para poder atuar como um MTA destinatário e avaliar mensagens de e-mail submetidas pelos usuários. Além disso, a integração de técnicas de aprendizado de máquina na detecção de padrões suspeitos em tráfego de e-mail também se apresenta como uma possibilidade futura de estudo. Essas melhorias poderão tornar a ferramenta *StopEmailSpoofing* ainda mais robusta e eficaz na mitigação e no combate a ameaças associadas à falsificação de endereços de e-mail.

Referências

- Blechsmidt, B., & Stock, B. (2023). Extended Hell(o): A comprehensive large-scale study on email confidentiality and integrity mechanisms in the wild. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23) (pp. 4895–4912). USENIX Association. <https://www.usenix.org/conference/usenixsecurity23/presentation/blechsmidt>
- de Carvalho, F. N., Tramontina, P. R., da Silva, W. R., & Misaghi, M. (2023). O emprego de DMARC para aprimoramento de proteção de e-mail: Um relato de caso. *Revista Foco*, 16(10), e3123. <https://doi.org/10.54751/revistafoco.v16n10-074>
- Chen, J., Paxson, V., & Jiang, J. (2020). Composition kills: A case study of email sender authentication. In Proceedings of the 29th USENIX Security Symposium (USENIX Security 20) (pp. 2183–2199). USENIX Association. <https://www.usenix.org/conference/usenixsecurity20/presentation/chen-jianjun>
- Camacho Coronel, A., Erazo Ayón, J. M., Salazar Tovar, C., & Pardo Centanaro, B. (2024). Ingeniería social: Revisión sistemática de phishing y pretexting en plataformas académicas. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (E72), 122–136. <https://www.risti.xyz/issues/ristie72.pdf>
- D'Angelone, M. (2022). Email spoofing defence techniques: A comprehensive review and development of a novel measurement tool. School of Computing, National College of Ireland. <https://norma.ncirl.ie/7116/1/marcellodangelone.pdf>
- Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers & Security*, 139, 103671. <https://doi.org/10.1016/j.cose.2023.103671>

- Georg, M. A. C., Rodrigues, W. M. S., Alves, C. A. M., Silveira Junior, A., & Nunes, R. R. (2023). Os desafios da segurança cibernética no setor público federal do Brasil: Estudo sob a ótica de gestores de tecnologia da informação. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (E54), 602–616. <https://doi.org/10.5281/zenodo.7855320>
- Gil, A. C. (2017). Como elaborar projetos de pesquisa (6th ed.). Atlas.
- Hu, H., & Wang, G. (2018). End-to-end measurements of email spoofing attacks. In *Proceedings of the 27th USENIX Security Symposium (USENIX Security 18)* (pp. 1095–1112). <https://www.usenix.org/conference/usenixsecurity18/presentation/hu>
- Maroofi, S., Korczyński, M., & Duda, A. (2020). From defensive registration to subdomain protection: Evaluation of email anti-spoofing schemes for high-profile domains. In *Traffic Monitoring and Analysis*. <https://api.semanticscholar.org/CorpusID:219956390>
- Maroofi, S., Korczyński, M., Hölzel, A., & Duda, A. (2021). Adoption of email anti-spoofing schemes: A large-scale analysis. *IEEE Transactions on Network and Service Management*, 18(3), 3184–3196. <https://doi.org/10.1109/TNSM.2021.3065422>
- Meshram, B. B., Mendhe, V., & Singh, M. K. (2024). Tracing the invisible threads: A deep dive into email security and forensics. *International Journal of Enhanced Research in Science, Technology & Engineering*, 13(1), 14-42. <https://doi.org/10.55948/IJERSTE.2024.0104>
- Nmach, W. P. (2023). A framework for securing email entrances and mitigating phishing impersonation attacks. *International Journal of Network Security & Its Applications*, 15(6), 15-35. <https://doi.org/10.5121/ijnsa.2023.15602>
- Silva, E. L., & Menezes, E. M. (2005). Metodologia da pesquisa e elaboração de dissertação. Universidade Federal de Santa Catarina.
- Sethuraman, S. C., V. S., D. P., Reddi, T., Reddy, M. S. T., & Khan, M. K. (2024). A comprehensive examination of email spoofing: Issues and prospects for email security. *Computers & Security*, 137, 103600. <https://doi.org/10.1016/j.cose.2023.103600>
- Shen, K., Wang, C., Guo, M., Zheng, X., Lu, C., Liu, B., Zhao, Y., Hao, S., Duan, H., Pan, Q., & Yang, M. (2021). Weak links in authentication chains: A large-scale analysis of email sender spoofing attacks. In *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)* (pp. 3201–3217). <https://www.usenix.org/conference/usenixsecurity21/presentation/shen-kaiwen>
- Statista. (n.d.). Daily number of e-mails worldwide. Retrieved April 5, 2025, from <https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide>

- Yu, B., Li, P., Liu, J., Zhou, Z., Han, Y., & Li, Z. (2022). Advanced analysis of email sender spoofing attack and related security problems. In 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud) / 2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 80–85). IEEE. <https://doi.org/10.1109/CSCloud-EdgeCom54986.2022.00023>
- Zhang, H., Chen, L., Liu, M., Shi, Y., Wu, S., & Xue, Z. (2023). Both sides needed: A two-dimensional measurement study of email security based on SPF and DMARC. In 2023 19th International Conference on Mobility, Sensing and Networking (MSN) (pp. 855–861). IEEE. <https://doi.org/10.1109/MSN60784.2023.00126>

Processamento de Linguagem Natural Aplicado à Identificação de Padrões Semânticos em Relatos de Mulheres Vítimas de Violência Doméstica e Familiar

Sabrina S. Vasconcellos¹, Deborah Q. G. Foroni¹, Peterson A. Belan¹

sabrina.vasconcellos@uni9.edu.br; belan@uni9.pro.br,

¹ Universidade Nove de Julho (UNINOVE), Rua Vergueiro, 235/249 – São Paulo/SP – Brasil

DOI: 10.17013/risti.60.74–95

Resumo: A violência doméstica e familiar (VDF) contra a mulher é um problema persistente e subnotificado. Com o avanço das mídias sociais, relatos espontâneos de vítimas tornaram-se fontes relevantes de dados, embora seu volume e complexidade exijam técnicas automatizadas de análise. Este estudo busca identificar tópicos emergentes em relatos não estruturados de mulheres vítimas de VDF publicados no *YouTube*, aplicando Processamento de Linguagem Natural (PLN), aprendizado de máquina não supervisionado e modelagem de tópicos. A metodologia incluiu coleta via *API* do *YouTube*, pré-processamento textual, geração de *embeddings*, redução de dimensionalidade (*PCA* e *UMAP*), clusterização (*K-means* e *HDBSCAN*) e extração de tópicos com *BERTopic*. O melhor desempenho foi obtido com a combinação *UMAP* + *HDBSCAN* sem *stopwords*, revelando temas como ciclo da violência, ameaças e apoio familiar. Os resultados evidenciam a viabilidade do PLN e do *BERTopic* para análise automatizada e apoio à formulação de políticas públicas e pesquisas sociais.

Palavras-chave: Processamento de linguagem natural; Topic modeling; *BERTopic*; Violência doméstica e familiar.

Natural Language Processing Applied to the Identification of Semantic Patterns in Reports of Women Victims of Domestic and Family Violence

Abstract: Domestic and family violence (DFV) against women remains a persistent and underreported problem. With the rise of social media, spontaneous victim reports have become valuable data sources, although their volume and complexity require automated analytical techniques. This study aims to identify emerging topics in unstructured reports from women victims of DFV published on *YouTube*, using Natural Language Processing (NLP), unsupervised machine learning, and topic modeling. The methodology included data collection via the *YouTube API*, text preprocessing, embedding generation, dimensionality reduction (*PCA* and *UMAP*), clustering (*K-means* and *HDBSCAN*), and topic extraction using *BERTopic*. The best performance was achieved with the *UMAP* + *HDBSCAN* combination without *stopwords*, revealing themes such as the cycle of violence, threats, and family

support. The results highlight the feasibility of NLP and BERTopic for automated analysis and their potential to support public policy development and social research.

Keywords: Natural language processing; Topic modeling; BERTopic; Domestic and family violence.

1. Introdução

A violência doméstica e familiar contra a mulher é um fenômeno global que persiste em diferentes sociedades, sendo um problema social e de saúde pública. No Brasil, a Lei nº 11.340/2006, conhecida como Lei Maria da Penha, define a VDF como qualquer ação ou omissão baseada no gênero que resulte em morte, lesão, sofrimento físico, sexual ou psicológico, bem como dano moral ou patrimonial (BRASIL, 2006).

Em escala mundial, a Organização Mundial da Saúde (OMS) estima que uma em cada três mulheres já sofreu violência de gênero ao longo da vida, sendo que aproximadamente 27% das mulheres entre 15 e 49 anos relatam terem sido vítimas de violência física e/ou sexual praticada por parceiros (WHO, 2021).

As mídias sociais têm se consolidado como espaços de auto relatos de violência, oferecendo material importante para análise. Embora estudos sobre auto relatos não sejam novos (ESTROFF et al., 1994; LEVENDOSKY et al., 2004), a expansão dessas plataformas, que reúnem cerca de 4,7 bilhões de usuários no mundo (KEIPOS, 2022), ampliou a geração de dados públicos (GIGLIETTO; ROSSI; BENNATO, 2012). Nesse cenário, técnicas computacionais, como o Aprendizado de Máquina (AM), permitem o reconhecimento automático de padrões nesses relatos. Segundo Samuel (1959), o AM confere aos computadores a capacidade de aprender sem programação explícita, favorecendo análises mais robustas e reproduzíveis, inclusive em casos de VDF (ALGARADI et al., 2022).

O uso de AM e PLN tem crescido em diversas áreas, incluindo saúde, marketing e biologia (CHEN et al., 2018), ampliando para as áreas de ciências sociais (MULLAH; ZAINON, 2021; NI et al., 2020). Enquanto ramo da Inteligência Artificial, o PLN aplica princípios linguísticos e métodos computacionais para construir modelos capazes de analisar e interpretar textos de forma automatizada (RUSSELL; NORVIG, 2004). Entre suas aplicações, destacam-se os métodos de *topic modeling*, que organizam grandes coleções de documentos a partir da identificação de temas latentes (BLEI, 2012; EGGER; YU, 2022).

Tradicionalmente, os dados sobre VDF são obtidos por meio de registros da saúde ou da segurança pública, como boletins de ocorrência (PREVIATTI; MILANI, 2016). No entanto, existem limitações na coleta, profissionais não se sentem preparados (ACOSTA et al., 2017; DE SOUZA et al., 2018; SOUZA; MARIN; RODRIGUES, 2021), além de protocolos oficiais simplificar os relatos, priorizando classificações legais (BORBUREMA et al., 2017) e deixando de capturar nuances contextuais, as quais podem ser resgatadas em entrevistas mais detalhadas (SCHRAIBER et al., 2007).

Assim, diante da ampla geração de dados não estruturados nas mídias sociais como textos, vídeos, imagens e áudios (ELSAIED; ABDELWAHAB; AHDELKADER, 2019),

essas plataformas se apresentam como fontes complementares de pesquisa (BOYD; CRAWFORD, 2012; GHANI et al., 2019). O volume de informações ultrapassa a capacidade de processamento humano (MUSTAK et al., 2021), o que torna as técnicas de AM, PLN e *topic modeling* fundamentais para identificar estruturas semânticas e padrões em relatos públicos de mulheres vítimas de violência doméstica e familiar.

Dessa forma, o presente estudo tem como objetivo explorar o potencial das mídias sociais como fonte complementar de dados sobre violência doméstica e familiar contra a mulher, aplicando técnicas de Aprendizado de Máquina e PLN para identificar padrões, estruturas semânticas e temas recorrentes nos relatos públicos.

2. Referencial Teórico

2.1. Violência Doméstica e Familiar

A violência doméstica e familiar contra a mulher é um problema global e recorrente, intensificado durante a pandemia da SARS-CoV-2, quando fatores como isolamento social, estresse econômico e convivência elevaram os índices de agressões (VIERIA; GARCIA; MACIEL, 2020; FORNARI et al., 2021).

No Brasil, instrumentos legais como a Convenção de Belém do Pará (1994) e a Lei Maria da Penha (Lei nº 11.340/2006) estabeleceram avanços no enfrentamento da VDF, sendo a Lei Maria da Penha considerada uma das legislações mais abrangentes do mundo (BRASIL, 2006; LISBOA; ZUCCO, 2022). Entretanto, desafios persistem quanto à efetividade das políticas públicas e à destinação de recursos para sua implementação (LISBOA; ZUCCO, 2022).

Do ponto de vista psicológico, Walker (1979) os episódios de violência seguem um ciclo repetitivo de três fases, o aumento da tensão, ato de violência e arrependimento, representados na Figura 1. A compreensão desse ciclo ajuda identificar padrões de reincidência e subsidiar tanto políticas públicas quanto intervenções preventivas e de proteção às vítimas.

A primeira fase, chamada “aumento da tensão”, é marcada pela irritabilidade do agressor diante de situações banais, enquanto a vítima busca evitar conflitos, muitas vezes assumindo a culpa para não “provocá-lo”.

Na segunda fase, ocorre a “explosão”, caracterizada pela perda de controle do agressor e a materialização da violência física, psicológica, verbal, moral ou patrimonial, gerando na vítima sentimentos de medo, vergonha, solidão e dor, além de possíveis reações como afastamento, denúncia ou até ideia suicida.

Já a terceira fase, denominada “arrependimento», envolve a tentativa do agressor de reconciliação por meio de promessas de mudança, o que pode confundir a vítima e dificultar a ruptura do ciclo, especialmente em relações com filhos.

Esse processo cíclico contribui para a perpetuação da violência e para o silêncio das vítimas, motivado por vergonha, medo e constrangimento, fatores que resultam na subnotificação de casos e na discrepância entre registros oficiais e a real dimensão do problema (FERREIRA; MORAES, 2020).



Figura 1 – Ciclo da Violência Doméstica Contra a Mulher

2.2. Aprendizado de Máquina

Desde o surgimento dos computadores, pesquisadores têm buscado desenvolver sistemas capazes de aprender a partir de dados, o que deu origem ao campo do Aprendizado de Máquina (AM) (MICHALSKI; CARBONELL; MITCHELL, 1983). O conceito foi inicialmente proposto por Arthur Samuel (1959), que o definiu como a capacidade dos computadores de aprenderem sem serem explicitamente programados. Posteriormente, Mitchell (1997) apresentou uma definição formal, afirmando que um programa “aprende a partir de experiências e com respeito a uma tarefa T é medida de desempenho P , se o desempenho em T , medido por P , melhora com a experiência E ”.

O AM abrange três principais abordagens: supervisionado, não supervisionado e semi-supervisionado (SARAVANAN; SUJATHA, 2018). No aprendizado supervisionado, o modelo aprende a partir de pares de entrada e saída para realizar previsões sobre novos exemplos (RUSSELL; NORVIG, 2004; XIE et al., 2018). Já o aprendizado não supervisionado busca identificar padrões em dados não rotulados, agrupando informações de forma autônoma (ALLOGHANI et al., 2020; RUSSELL; NORVIG, 2004). Por fim, o aprendizado semi-supervisionado combina dados rotulados e não rotulados para aprimorar o desempenho em cenários com escassez de rótulos (LIU et al., 2015; VAN DER MAATEN; HINTON, 2008).

Neste estudo, foi adotado algoritmos de aprendizado não supervisionado aplicados a dados textuais, com o objetivo de identificar padrões semânticos e estruturas latentes por meio da combinação das técnicas *Uniform Manifold Approximation and Projection (UMAP)* e *Hierarchical Density-Based Spatial Clustering of Applications with Noise (HDBSCAN)*.

A manipulação de dados textuais gera representações vetoriais de alta dimensionalidade, o que impõe desafios aos algoritmos de agrupamento e visualização. Para contornar esse problema, utilizam-se técnicas de redução de dimensionalidade, que simplificam o espaço de características mantendo a estrutura relevante dos dados.

Entre as técnicas existentes, o *UMAP* (McInnes et al., 2018) destaca-se por combinar fundamentos matemáticos da geometria riemanniana e da topologia algébrica, permitindo reduzir a dimensionalidade de *embeddings* de centenas de dimensões para espaços bidimensionais ou tridimensionais, sem comprometer a coerência semântica. Essa redução possibilita que algoritmos de clusterização, como o *HDBSCAN*, operem de maneira mais eficiente.

O *HDBSCAN* (Campello, Moulavi & Sander, 2013) é um algoritmo de aprendizado não supervisionado baseado em densidade que identifica regiões densas em conjuntos de dados sem a necessidade de definir previamente o número de clusters. Diferentemente do *K-means*, o *HDBSCAN* é capaz de lidar com ruídos, detectar *outliers* e extrair *clusters* hierárquicos estáveis, tornando-o ideal para a análise exploratória de dados textuais complexos.

A combinação das técnicas *UMAP* e *HDBSCAN* representa uma solução robusta e eficaz para lidar com dados textuais de alta dimensionalidade. O *UMAP* reduz o espaço vetorial preservando a estrutura semântica, enquanto o *HDBSCAN* identifica agrupamentos densos e significativos de forma autônoma. Essa integração metodológica resulta em modelos mais interpretáveis, coerentes e aplicáveis em múltiplos domínios, mineração de tópicos, detecção de padrões sociais e identificação de tendências comportamentais.

Assim, a adoção combinada dessas técnicas demonstra o potencial do aprendizado não supervisionado em descobrir relações latentes e revelar estruturas semânticas emergentes em grandes volumes de dados textuais, contribuindo para o avanço das aplicações de Processamento de Linguagem Natural em contextos de análise social e da segurança pública.

2.2.1. Clusterização

A clusterização é uma técnica de aprendizado não supervisionado que busca identificar estruturas ocultas em conjuntos de dados sem rótulos pré-definidos. Seu objetivo é agrupar elementos com alta similaridade dentro de um mesmo grupo e alta dissimilaridade entre grupos distintos (SINAGA; YANG, 2020). Além disso, representa um processo que visa organizar dados de modo a facilitar a interpretação e a compreensão humana (MCINNES; HEALY, 2017).

Os algoritmos de clusterização podem ser classificados em duas categorias: ordem conhecida e ordem desconhecida. No primeiro caso, o número de clusters é definido como parâmetro de entrada, enquanto no segundo, esse número é determinado automaticamente com base em critérios como densidade ou proximidade dos dados (MOUTON; FERREIRA; HELBERG, 2020).

2.2.2. Processamento de Linguagem Natural

O Processamento de Linguagem Natural (PLN) constitui uma área interdisciplinar que integra conhecimentos da computação, da inteligência artificial e da linguística, voltada à compreensão e ao tratamento automático da linguagem humana (RESHAMWALA; MISHRA; PAWAR, 2013; KHURANA et al., 2022). Desde os anos 2000, técnicas como

representações vetoriais e modelos baseados em aprendizado profundo ampliaram significativamente as aplicações em PLN (KHURANA et al., 2022).

Com o crescimento dos grandes volumes de dados digitais, surgiu a necessidade de representações numéricas capazes de transformar textos em vetores compreensíveis para máquinas. O modelo de espaço vetorial permanece como uma das abordagens mais utilizadas para a representação de documentos, possibilitando a análise automatizada e a classificação de textos (BAFNA; PRAMOD; VAIDYA, 2016; SINOARA et al., 2019).

2.2.3. Topic Modeling

O *topic modeling* é uma técnica de aprendizado de máquina não supervisionado utilizada para extrair significado de textos, identificando temas latentes a partir das palavras-chave mais representativas em coleções de documentos não estruturados (RAO; TABOADA, 2021). Essa abordagem permite organizar e resumir grandes volumes de informações, tornando possível uma análise que seria inviável manualmente (BLEI, 2012).

Neste estudo, foi utilizado o algoritmo *BERTopic*, desenvolvido por Maarten Grootendorst (2022), que se baseia em arquiteturas *Transformer* e aproveita o modelo de linguagem *BERT* para gerar *embeddings*, ou seja, representações numéricas que capturam o significado semântico das palavras e frases em um espaço vetorial contínuo. Esses *embeddings* são posteriormente utilizados na clusterização de tópicos, permitindo identificar padrões semânticos em grandes conjuntos de textos.

Além de modelos baseados em embeddings (como BERT) e abordagens de modelagem de tópicos, observa-se o avanço do uso de modelos de linguagem de grande porte (LLMs) em tarefas de apoio à produção e estruturação textual. Uma revisão recente sobre o impacto do ChatGPT em processos criativos reporta benefícios como ganho de produtividade e auxílio na geração de diálogos e tramas, mas ressalta limitações relacionadas à profundidade emocional e à originalidade, além de desafios éticos e laborais associados ao uso acrítico dessas ferramentas. Assim, em contextos sensíveis, como narrativas de violência, recomenda-se que a IA seja empregada de forma complementar e com supervisão humana, de modo a preservar nuances semânticas e reduzir riscos interpretativos (ZALDÍVAR-COLADO; TRIPP-BARBA; AGUILAR-CALDERÓN, 2025).

Conforme Figura 2 – Fluxo do algoritmo *BERTopic*, o processo é dividido em três etapas principais. Na primeira, cada documento é convertido em sua representação vetorial (*embedding*) por meio de um modelo pré-treinado. Na segunda, ocorre a redução de dimensionalidade para otimizar a clusterização dos dados. Por fim, na terceira etapa, as representações de tópicos são extraídas com base em uma variação do *TF-IDF*, denominada *c-TF-IDF*, que identifica os termos mais relevantes em cada grupo (GROOTENDORST, 2022).

A flexibilidade do *BERTopic* permite substituir as técnicas utilizadas em cada etapa sem comprometer o desempenho do modelo. Essa característica o torna uma ferramenta eficiente e inovadora para a identificação e organização de tópicos emergentes em relatos de mulheres vítimas de violência doméstica e familiar, contribuindo para uma análise automatizada e semanticamente consistente dos dados coletados.

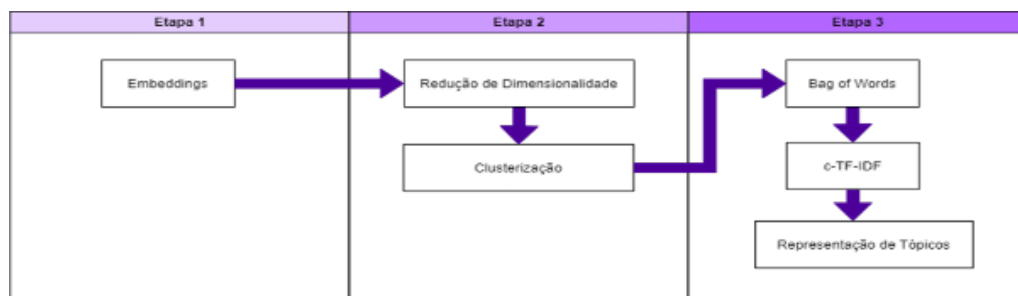


Figura 2 – Fluxo do Algoritmo *BERTopic*

2.3. Trabalhos Correlatos

Embora ainda seja um campo emergente, os estudos que utilizam PLN e IA no fenômeno da violência doméstica e familiar contra a mulher têm se expandido, sobretudo a partir de dados de mídias sociais, registros públicos e bases clínicas.

Na literatura internacional, destacam-se investigações que exploram o potencial do PLN na identificação de padrões de discurso associados à violência. Xue, Chen e Gelles (2019) analisaram 322.863 mensagens do *Twitter* entre outubro de 2015 e janeiro de 2016, aplicando o método *Latent Dirichlet Allocation (LDA)* para revelar tópicos latentes e estruturas temáticas sobre violência doméstica. O estudo demonstrou a eficácia do aprendizado de máquina não supervisionado na detecção de padrões semânticos em grandes volumes de texto.

Em uma linha similar, Soldevilla e Flores (2021) desenvolveram um classificador baseado no modelo *BERT* com *fine-tuning*, aplicado a mensagens do *Reddit* e *Twitter*, para distinguir conteúdos relacionados à violência de gênero. Utilizando o modelo *bert-base-uncased*, os autores obtiveram acurácia de 0,8909 e AUC de 0,9603, validando a aplicabilidade dos transformadores em contextos sensíveis e socialmente relevantes.

No contexto brasileiro, Corrêa e Faria (2021) utilizaram técnicas de mineração de texto, como nuvem de palavras, modelagem de tópicos (*LDA*) e classificação automática (*Naive Bayes*), sobre 125 relatos de violência extraídos de notícias em português, alcançando 71,2% de acurácia na classificação de casos como “constantes” ou “esporádicos”.

Ampliando essa vertente nacional, Campos e Andréo (2024) propuseram a análise automatizada de notícias online por meio de *web crawling*, análise de sentimentos e redes neurais artificiais, com o objetivo de quantificar ocorrências de violência contra a mulher noticiadas na internet. O estudo apresentou o potencial das *RNA* como ferramenta para geração de indicadores sociais e apoio a políticas públicas de enfrentamento.

Em um recorte mais conceitual, Santos (2025) discute as possíveis aplicações da IA na segurança pública, destacando seu papel estratégico na redução dos índices de violência contra a mulher. Por meio de uma revisão qualitativa, o autor argumenta que a IA, quando estruturada de modo integrado a dados institucionais e sociais, pode fortalecer políticas de prevenção e ampliar a capacidade preditiva do Estado no monitoramento de casos de VDF.

No cenário global contemporâneo, observa-se o avanço do uso de modelos de linguagem de grande porte (*LLMs*) para a compreensão e apoio a vítimas de violência. Guan et al. (2025) desenvolveram um modelo *GPT-3.5* ajustado para identificar necessidades de informação de sobreviventes de violência doméstica em comunidades de saúde online (*Reddit*). O modelo classificou oito tipos de necessidades, alcançando *F1-score* de 70,49% em textos reais e 84,58% em textos sintéticos, superando modelos como *Llama 2-7B*, *Llama 3-8B* e *LSTM*, o que evidencia a eficácia dos *LLMs* em classificação multicategórica contextualizada.

Na mesma direção, Kouzani e Nouman (2025) propuseram um modelo híbrido de aprendizado profundo combinando *BERT*, *BiLSTM* e *BiGRU* para detecção de indicadores de violência em textos digitais, utilizando 39.650 postagens do X (antigo *Twitter*). O modelo obteve performance preditiva, demonstrando capacidade de capturar dependências de longo prazo e contextos linguísticos complexos, o que reforça a utilidade de arquiteturas híbridas na análise semântica de violência online.

Em ambientes institucionais, Botelle et al. (2022) e Zeidan et al. (2022) aplicaram modelos *BioBERT* e análises de notas clínicas para identificar casos de violência interpessoal em registros eletrônicos de saúde, revelando o aumento da violência por parceiro íntimo (VPI) durante a pandemia de COVID-19. Esses estudos ampliam a compreensão da VDF como problema multidimensional, apontando a relevância do PLN aplicado a dados clínicos e sociais.

Em síntese, observa-se a consolidação de um ecossistema interdisciplinar que une dados textuais de mídias sociais, registros públicos e fontes médicas, evidenciando a eficácia da Inteligência Artificial e do Processamento de Linguagem Natural na detecção automatizada, análise semântica e previsão de padrões de violência. As abordagens revisadas demonstram não apenas o potencial técnico dos modelos de linguagem, mas também sua contribuição ética e social na formulação de políticas públicas e estratégias de intervenção preventiva.

3. Materiais e Métodos

Nesta seção, estão apresentados os materiais e métodos empregados na condução da pesquisa, com detalhamento das etapas dos experimentos computacionais.

3.1. Etapas Metodológicas

A Figura 3 apresenta o fluxo metodológico adotado, composto por três etapas principais: (1) Coleta de Dados, (2) Pré-processamento dos Dados e (3) Modelagem de Tópicos (*Topic Modeling*).

O processo inicial consistiu na definição de uma estratégia de busca capaz de extrair, com o mínimo de ruído, conteúdos autênticos sobre relatos de mulheres vítimas de violência doméstica e familiar (VDF). Foram combinados os termos “relato”, “violencia” e “mulher” sem acentuação para capturar narrativas públicas relevantes.

A escolha da plataforma *YouTube* foi considerada com base em três critérios:

- a. quantidade de material disponível;

- b. profundidade dos relatos, geralmente mais longos e descritivos;
- c. disponibilidade de *API* pública para extração de dados.

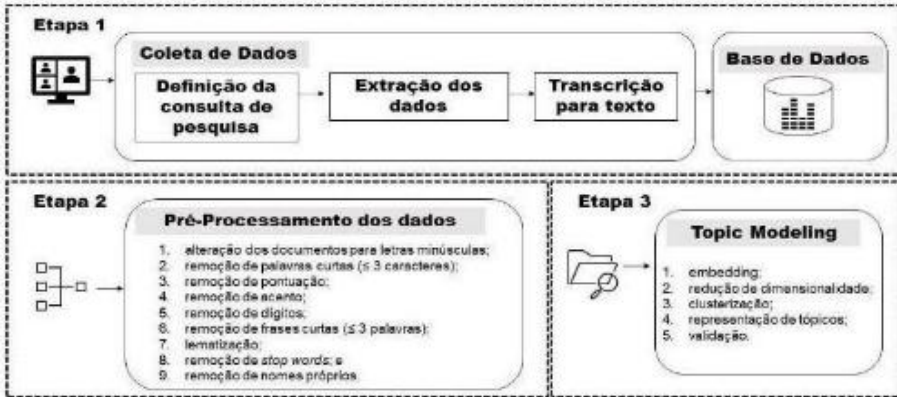


Figura 3 – Processo Metodológico e Experimental

A coleta foi realizada com o módulo *urllib.request* (*Python* 3.8), utilizando as palavras-chave “relato+violencia+mulher”. Devido às limitações da *API*, que indexa apenas títulos e descrições, foi necessário complementar a busca com uma seleção manual de vídeos.

Em seguida, foi aplicado o modelo *Whisper* (Radford et al., 2022), desenvolvido pela *OpenAI*, para transcrever automaticamente o áudio dos vídeos em texto. O *Whisper* é um sistema de reconhecimento automático de fala (*Automatic Speech Recognition – ASR*) treinado em 680 mil horas de dados multilíngues, sendo gratuito e de código aberto.

As transcrições resultantes foram validadas manualmente para garantir precisão semântica e exclusão de partes irrelevantes como perguntas de repórteres. Apenas os relatos das vítimas, em português do Brasil, foram mantidos.

Com as transcrições validadas, foi construída uma base de dados estruturada em *Python*, contendo as colunas:

- ID do Vídeo (identificação única);
- Título do Vídeo;
- Transcrição completa; e
- Transcrição validada (apenas o relato da vítima).

Essa estrutura assegura rastreabilidade e controle de qualidade sobre o material analisado. Os trechos que não pertenciam aos relatos, como introduções jornalísticas ou comentários de terceiros, foram eliminados. Assim, cada registro da base representa um documento textual limpo, pronto para o processamento linguístico.

O pré-processamento é uma etapa essencial em análises de PLN, especialmente quando se lida com dados textuais não estruturados. O objetivo é normalizar e limpar os textos para reduzir ruído e aumentar a precisão das etapas posteriores de modelagem.

As operações aplicadas incluíram:

1. conversão para letras minúsculas;
2. remoção de palavras curtas (≤ 3 caracteres);
3. remoção de pontuação, acentos e dígitos;
4. exclusão de frases curtas (≤ 3 palavras);
5. lematização, conforme Lucca e Nunes (2002), para representar palavras em suas formas canônicas;
6. remoção de *stopwords* (Fox, 1989), incluindo termos genéricos e palavras específicas do fenômeno, “violência”, “contra”, “mulher” e “doméstica”, que poderiam enviesar a análise;
7. exclusão de nomes próprios, visando à proteção da identidade das mulheres.

Essas transformações resultaram em um conjunto textual limpo, anonimizado e normalizado, pronto para as análises semânticas e estatísticas subsequentes.

Por fim, foi aplicada a etapa de modelagem de tópicos, voltada à identificação de temas latentes nos relatos coletados. O processo seguiu as fases metodológicas conforme demonstrado na Figura 4.

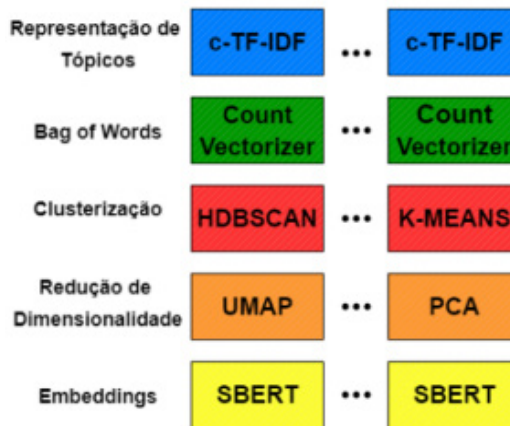


Figura 4 – Etapas para criar as representações de tópicos

Esses procedimentos permitiram agrupar automaticamente relatos com similaridades semânticas, possibilitando a extração de tópicos emergentes relacionados às experiências de VDF. O método mostrou-se adequado para identificar padrões discursivos, emoções recorrentes e aspectos sociais e psicológicos subjacentes aos relatos.

O processo metodológico adotado, representado na Figura 3, reflete uma estrutura de experimentação replicável e transparente, composta por três macro etapas integradas:

- Coleta e transcrição automatizada de dados autênticos (*YouTube*);
- Tratamento e limpeza textual com foco em qualidade linguística e ética; e
- Modelagem não supervisionada de tópicos, como ferramenta exploratória de padrões narrativos.

Essa sequência de procedimentos assegura a validade empírica e a reprodutibilidade científica da pesquisa, consolidando sua natureza experimental e aplicada no campo de Processamento de Linguagem Natural aplicado às Ciências Sociais.

4. Resultados e Discussão

O método adotado é flexível e modular, permitindo a escolha de diferentes algoritmos em cada etapa. Foram coletados 119 vídeos no *YouTube* com relatos de mulheres vítimas de VDF, dos quais 70 foram selecionados para análise e 49 descartados por não tratarem do fenômeno.

Dois experimentos foram conduzidos: (i) *UMAP + HDBSCAN* com *stopwords*; e (ii) *UMAP + HDBSCAN* sem *stopwords*. O segundo experimento apresentou melhor coerência semântica, identificando tópicos recorrentes relacionados ao ciclo da violência, ameaças, impactos psicológicos, apoio familiar e busca por ajuda institucional.

A análise demonstrou que a remoção de *stopwords* aumentou a clareza dos tópicos gerados.

4.1. *UMAP + HDBSCAN + com stopwords*

Nessa configuração, foi utilizado o *UMAP* para a redução de dimensionalidade e o *HDBSCAN* para a clusterização, destacando a vantagem de não ser necessário informar previamente o número de clusters, aspecto essencial para este estudo, uma vez que o total de agrupamentos a serem identificados não era conhecido a princípio (GROOTENDORST, 2022).

A aplicação do modelo, com o conjunto de dados sem remoção de *stopwords*, resultou na identificação de 40 tópicos, os quais estão apresentados os 20 primeiros no Quadro 1 devido a sua extensão e assim estamos apresentando os mais significativos.

Tópicos	Palavras por tópicos	Quantidade
-1	ter, meu, de, muito, porque, esse, falar, para, estar, ele	1750
0	estar, isso, ter, para, porque, gente, falar, muito, de, meu	174
1	voce, falar, assim, poder, ninguem, este, pessoa, querer, morrer, nada	142
2	entao, situacao, conhecer, esse, tudo, decisao, em, ter, sensacao, gente	114
3	para, meu, poder, isso, porque, percebi, falar, pessoa, demonio, ter	92
4	nunca, querer, mais, voltar, momento, viver, medo, terminar, tudo, aquele	89
5	gente, acontecer, isso, achar, luxo, coisa, tudo, aqui, comum, sociedade	67
6	tapa, soco, olho, cabelo, braco, puxar, murro, chao, sequela, facao	62

Tópicos	Palavras por tópicos	Quantidade
7	ser, sempre, estar, relacao, perdao, agressoes, ter, coisa, perdoar, algum	61
8	mulher, como, basear, perguntar, acreditar, apoio, quem, ajudar, ele, saber	60
9	delegacia, policia, medida, protetivo, denunciar, chamar, queixa, procurar, para, dizer	60
10	fiquei, medo, lembro, muito, calado, ficar, tempo, aquilo, aquele, cheguei	58
11	começar, namorar, começo, gente, começa, anal, complicar, virgem, partir, começar	55
12	chegar, ir, cima, ligar, carona, jogar, telefone, pegar, afiliar, presa	52
13	gente, meia, noite, cafe, tomar, dormer, hora, tar, tarde, conversar	45
14	violencia, mulher, contra, violenciar, feminismo, genero, sobre, negro, luta, sofrer	42
15	peguei, cheguei, carro, casa, lembrar, meu, voltar, quando, ela, pai	42
16	casa, droga, sair, onde, chegar, semana, voltar, quando, embora, saer	40
17	muito, gente, pessoa, gentil, carinhoso, educado, sempre, atencioso, simpatico, prestativo	39
18	casamento, ano, familia, casado, casar, marido, emprego, trabalhei, virgem, meu	38
19	agredir, controle, totalmente, indelicado, alcoolisar, agressivo, beber, beber, bebar, verbalmente	38
20	violencia, domestico, saude, violenciar, familiar, mulher, tipo, enfrentamento, cadastrar, contra	37

Quadro 1 – Resultado dos tópicos identificados (*UMAP + HDBSCAN com stopwords*)

Observa-se uma elevada concentração no tópico -1, classificado pelo *HDBSCAN* como *outlier*. Esse comportamento favorece a qualidade da representação, pois evita a alocação forçada de documentos em *clusters* inadequados.

Apesar disso, apenas 25 tópicos destacados no Quadro 2 apresentaram coerência semântica interpretável, correspondendo a 27,30% do total de documentos analisados. Os demais não revelaram clareza suficiente quanto aos temas representados, o que limita a análise interpretativa.

Diante dessa baixa representatividade, uma nova abordagem metodológica será apresentada na seção seguinte, buscando maior consistência nos resultados.

4.2. *UMAP + HDBSCAN + sem stopwords*

Nesta configuração, foi aplicado o *UMAP* para redução de dimensionalidade em conjunto com o *HDBSCAN* para a clusterização, desta vez com a remoção de *stopwords*, em comparação ao experimento anterior, seção 5.2.

A Figura 5 apresenta a distribuição visual dos tópicos gerados, apresentando uma concentração significativa de documentos nos tópicos 0 e 1, além da presença da cor

cinza-claro, correspondente ao tópico -1, que reúne outliers e ruídos identificados nos documentos.

Esse resultado indica que, mesmo após a remoção de *stopwords*, há uma parcela de registros não alocados em clusters semanticamente claros.

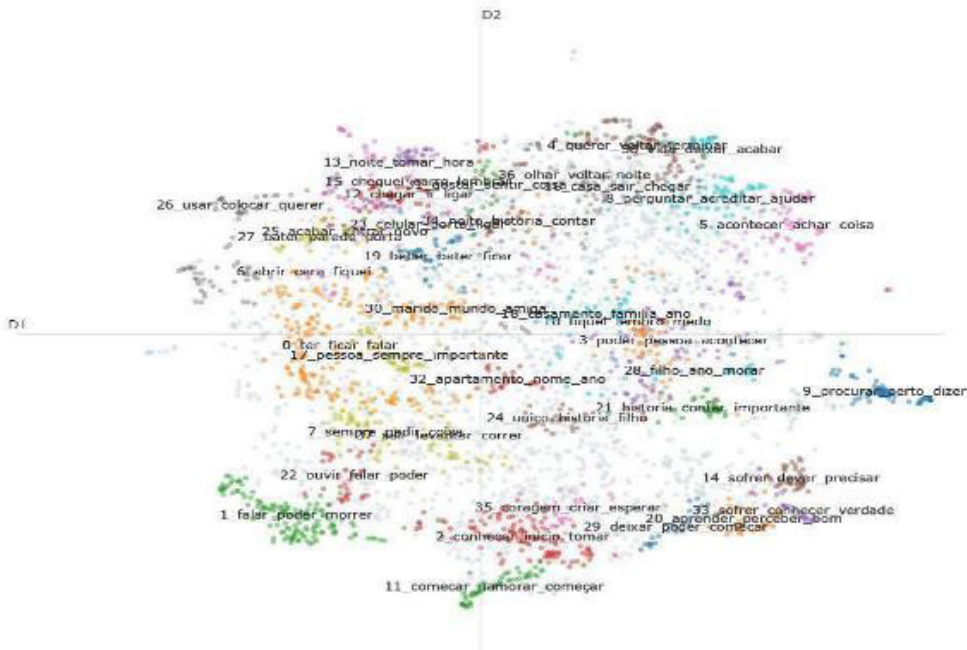


Figura 5 – Distribuição dos Tópicos

A etapa seguinte complementa a análise com a Figura 5, que apresenta um mapa de calor das similaridades entre tópicos. Observa-se que a maioria apresenta similaridade ($\geq 0,90$), o que sugere redundância entre os clusters e limita a diversidade semântica dos tópicos extraídos.

Com a remoção de *stopwords*, o modelo *UMAP + HDBSCAN* apresentou uma melhora na qualidade semântica dos tópicos gerados. A Figura 6 demonstra que os tópicos 10, 11 e 21 possuem menor similaridade em relação aos demais, ainda que mantenham níveis consideráveis de proximidade. Essa configuração resulta em interpretações mais consistentes do que as obtidas nas seções anteriores.

O Quadro 3 apresenta os tópicos identificados, nos quais foi possível interpretar 27 tópicos semanticamente relevantes, representando 31,54% do total de documentos analisados. Esse valor indica um avanço em relação ao resultado obtido com *stopwords*, Quadro 2. Vale ressaltar que neste quadro também são apresentados os primeiros 20 tópicos por sua maior representatividade.

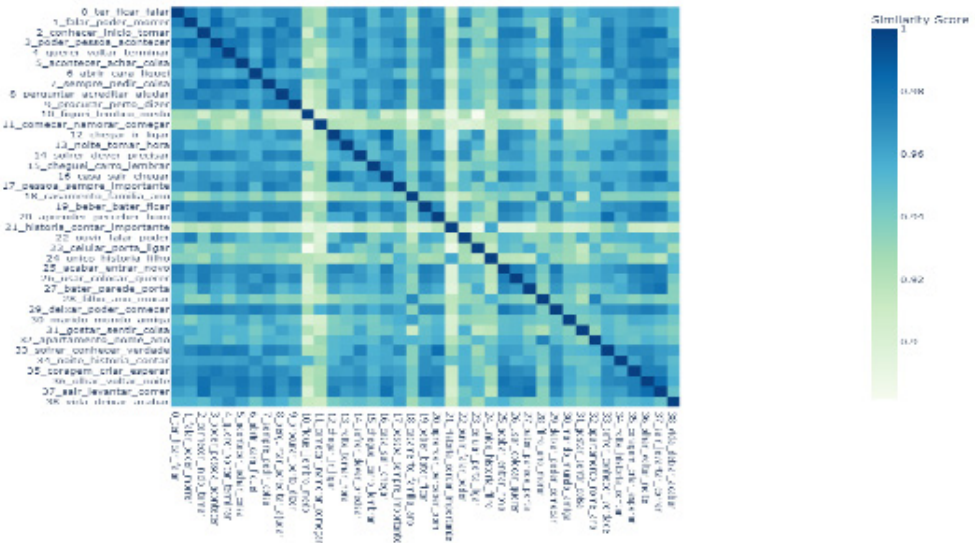


Figura 6 – Matriz de Similaridade

Tópicos	Palavras por tópicos	Quantidade
-1	ter, falar, ficar, dizer, casa, começar, fazer, querer, passar, ano	1750
0	ter, ficar, falar, morar, dizer, filha, pessoa, fazer, sentir, trabalhar	174
1	falar, poder, morrer, entaar, pessoa, perguntar, voltar, passar, querer, saber	142
2	conhecer, inicio, tomar, separar, bater, achar, pensar, mudar, ter, entaar	114
3	poder, pessoa, acontecer, pensar, falar, mudar, comigo, problema, filho, acabar	92
4	querer, voltar, terminar, momento, viver, medo, amor, feliz, poder, acontecer	89
5	acontecer, achar, coisa, menina, vez, mundo, normal, forte, vida, saber	67
6	abrir, cara, fiquei, pegar, continuar, dar, parede, briga, correr, hora	62
7	sempre, pedir, coisa, ter, trabalho, momento, acontecer, aceitar, conseguir, grande	61
8	perguntar, acreditar, ajudar, saber, aceitar, pessoa, bom, chegar, olhar, trabalhar	60
9	procurar, perto, dizer, caso, perguntar, precisar, ter, olhar, chegar, dar	60
10	fiquei, lembro, medo, tempo, ficar, cheguei, comigo, sofrer, beber, momento	58
11	começar, namorar, começar, novo, afastar, usar, sair, amigo, amiga, momento	55
12	chegar, ir, ligar, jogar, pegar, deixar, sair, casa, perguntar, porta	52
13	noite, tomar, hora, conversar, dormir, trabalhar, chegar, casa, conhecer, sair	45
14	sofrer, dever, precisar, existir, vir, direito, dia, falar, conversar, ano	42

Tópicos	Palavras por tópicos	Quantidade
15	cheguei, carro, lembrar, pai, voltar, casa, comprar, pegar, embora, porta	42
16	casa, sair, chegar, voltar, embora, ponto, dizer, trabalho, ir, entrar	40
17	pessoa, sempre, importante, conversar, mundo, início, pensar, perto, amigo, ajudar	39
18	casamento, família, ano, marido, filho, morar, comprar, feliz, criar, acabar	38
19	beber, bater, ficar, chegar, jogar, sempre, voltar, noite, passar, pessoa	38
20	aprender, perceber, bom, lugar, direito, sofrer, contar, conhecer, mundo, começar	37

Quadro 2 – Resultado dos tópicos identificados (UMAP + HDBSCAN sem stopwords)

A análise mostra que a remoção das *stopwords* contribuiu para uma representação mais precisa das palavras nos tópicos, favorecendo sua compreensão semântica.

Assim como observado no Quadro 1, o tópico -1 concentrou o maior número de documentos, classificados como ruído ou *outliers*, com menor relevância para a representação dos tópicos. Diante disso, o aprofundamento da análise está sobre os tópicos destacados (2, 4, 5, 6 e 8) por apresentarem maior clareza semântica, conforme apresentado na Figura 7.

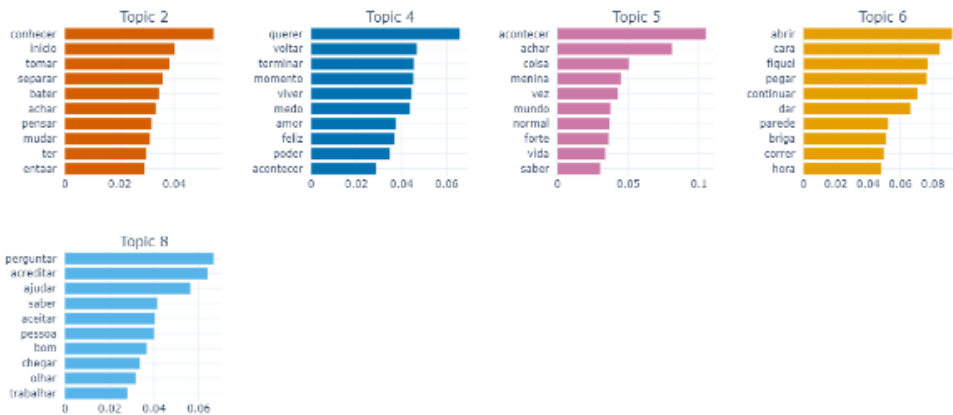


Figura 7 – Representação dos Tópicos 2, 4, 5, 6 e 8

A análise revelou tópicos com interpretação mais clara e consistente a partir da aplicação do UMAP + HDBSCAN com remoção de stopwords. O tópico 2, Quadro 3 traz narrativas de mulheres que buscaram forças para romper relacionamentos abusivos, refletindo decisões de separação e superação.

Tópico	Palavras por tópico	Documento
2	conhecer - início - tomar - separar - bater - achar - pensar - mudar - ter - entaar	“Então, eu tive muitas perdas até eu conseguir sair disso.”
2	conhecer - início - tomar - separar - bater - achar - pensar - mudar - ter - entaar	“Então eu passei por várias situações que já estavam ali me dando dica de que o relacionamento não era legal.”

Quadro 3 – Documentos associados ao tópico 2

O tópico 4, apresentado no Quadro 4, retrata a confusão emocional em relações violentas, onde sentimentos de medo, amor e arrependimento coexistem na fase do ato de violência do ciclo de Walker (1979).

Tópico	Palavras por tópico	Documento
4	querer - voltar - terminar - momento - viver - medo - amor - feliz - poder - acontecer	“Eu não queria que meu pai e minha mãe soubessem o que eu estava passando...”
4	querer - voltar - terminar - momento - viver - medo - amor - feliz - poder - acontecer	“Ele queria que eu acreditasse que o fato de ele ter ciúme demais era amor.”

Quadro 4 – Documentos associados ao tópico 4

O tópico 5, mostrado no Quadro 5, desta relatos de empoderamento e incentivo, nos quais as vítimas reafirmam a possibilidade de sair de situações abusivas e encorajam outras mulheres a buscarem ajuda.

Tópico	Palavras por tópico	Documento
5	acontecer - achar - coisa - menina - vez - mundo - normal - forte - vida - saber	“Eu saí e eu digo para as mulheres que a gente pode sair dessa.”
5	acontecer - achar - coisa - menina - vez - mundo - normal - forte - vida - saber	“Quem passa por isso vai me entender.”

Quadro 5 – Documentos associados ao tópico 5

O tópico 6, Quadro 6, concentra descrições explícitas de violência física severa, incluindo agressões, ameaças e sequelas permanentes, caracterizando o ápice da explosão violenta.

Tópico	Palavras por tópico	Documento
6	abrir - cara - fiquei - pegar - continuar - dar - parede - briga - correr - hora	“E... hoje eu sou uma mulher... que não consegue trabalhar... porque eu fiquei com sequelas.”
6	abrir - cara - fiquei - pegar - continuar - dar - parede - briga - correr - hora	“Ele socava a minha barriga, ele batia a minha cabeça na parede...”

Quadro 6 – Documentos associados ao tópico 6

Por fim, o tópico 8, Quadro 7 mostra a descrença social nos relatos das vítimas, expondo a dificuldade de reconhecimento da violência e o estigma que contribui para a perpetuação do ciclo abusivo.

Tópico	Palavras por tópico	Documento
8	perguntar - acreditar - ajudar - saber - aceitar - pessoa - bom - chegar - olhar - trabalhar	“Se eu falasse às vezes para algumas pessoas, elas não iam acreditar.”
8	perguntar - acreditar - ajudar - saber - aceitar - pessoa - bom - chegar - olhar - trabalhar	“A sociedade aponta o dedo muito e colabora para isso.”

Quadro 7 – Documentos associados ao tópico 8

No geral, os resultados confirmam que a estratégia adotada possibilitou a extração de tópicos semanticamente mais precisos, evidenciando os impactos da violência na vida das mulheres, e ao mesmo tempo, os desafios sociais e emocionais enfrentados por elas.

6. Conclusões

Este estudo apresentou técnicas de aprendizado de máquina e processamento de linguagem natural para identificar padrões semânticos em relatos de mulheres vítimas de violência doméstica e familiar coletados no *YouTube*, suprindo a ausência de repositórios disponíveis para esse tipo de dado, uma vez que, embora o PLN já tenha sido utilizado em estudos sobre violência doméstica em mídias sociais e registros institucionais (Xue, Chen & Gelles, 2019; Soldevilla & Flores, 2021; Corrêa & Faria, 2021; Campos & Andréo, 2024; Kouzani & Nouman, 2025), não foram identificados trabalhos anteriores que aplicassem técnicas de extração automatizada diretamente a relatos espontâneos das próprias vítimas em língua portuguesa.

Entre os experimentos realizados, a combinação das técnicas *UMAP + HDBSCAN*, associada à remoção de *stopwords*, apresentou melhor desempenho na extração de tópicos semanticamente coerentes, permitindo identificar padrões discursivos e temas recorrentes nos relatos. Esses resultados demonstram a capacidade do método em revelar estruturas latentes de significado, oferecendo subsídios para compreender dimensões psicológicas, sociais e culturais da violência. Além disso, evidenciam a relevância da IA como ferramenta analítica e exploratória na investigação de fenômenos humanos complexos, conforme também observado por Guan et al. (2025) e Kouzani & Nouman (2025) em contextos internacionais de detecção de violência e apoio a sobreviventes.

O estudo reafirma o potencial de generalização do PLN e do aprendizado de máquina para outros contextos sociais e institucionais, como denúncias corporativas, discursos de ódio, injúria racial e LGBTfobia, contribuindo para o avanço de soluções baseadas em dados para o monitoramento de vulnerabilidades e comportamentos de risco. De forma alinhada aos achados de Campos & Andréo (2024) e Santos (2025), reforça-se que o uso ético e supervisionado da IA pode favorecer estratégias de enfrentamento à violência e apoiar políticas públicas baseadas em evidências.

Entretanto, este artigo apresenta limitações. Nem todas as vítimas compartilham relatos em plataformas digitais, o que restringe a representatividade da amostra. Além disso,

a ausência de dados sociodemográficos e de bases comparativas limita a inferência estatística e a extrapolação dos resultados para populações mais amplas. Há, portanto, um desafio metodológico em equilibrar a riqueza qualitativa dos relatos espontâneos com a necessidade de padronização dos dados para análises quantitativas robustas.

Como trabalho futuro, recomenda-se a ampliação da coleta de dados em colaboração com ONGs e instituições de acolhimento, de modo a diversificar as fontes e melhorar a validade externa dos achados, também como sugestão o rotulamento dos tópicos com apoio de especialistas e a integração de modelos supervisionados de aprendizado profundo para análises de sentimentos e predição de risco mais precisas. Tais avanços poderão consolidar o papel da IA e do PLN como instrumentos científicos e sociais na compreensão e prevenção da violência doméstica e familiar contra a mulher.

Referências

- Acosta, D. F., Gomes, V. L. de O., De Oliveira, D. C., Gomes, G. C., & Da Fonseca, A. D. (2017). Aspectos éticos e legais no cuidado de enfermagem às vítimas de violência doméstica. *Texto & Contexto - Enfermagem*, 26.
- Al-Garadi, M. A., Kim, S., Guo, Y., Warren, E., Yang, Y. C., Lakamana, S., & Sarker, A. (2022). Natural language model for automatic identification of intimate partner violence reports from Twitter. *Array*, 15, 100217.
- Bafna, P., Pramod, D., & Vaidya, A. (2016). Document clustering: TF-IDF approach. In *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 61–66). Institute of Electrical and Electronics Engineers Inc.
- Blei, D. M. (2012). Probabilistic topic models. *Communications of the ACM*, 55, 77–84.
- Boyd, D., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society*, 15, 662–679.
- Brasil. (1994). *Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher*. Convenção de Belém do Pará.
- Brasil. (2006). *Lei nº 11.340*. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/11340.htm
- Brasil. (2022). *Política Nacional de Enfrentamento à Violência contra as Mulheres*.
- Campos, E. A. V., & Andrêo, A. C. O. P. (2024). *Violência doméstica: utilização de IA para quantificação das ocorrências noticiadas na internet*. *Revista Camalotes – RECAM*. Faculdade Insted.
- Campello, R. J. G. B., Moulavi, D., & Sander, J. (2013). *Density-based clustering based on hierarchical density estimates*. In *Advances in Knowledge Discovery and Data Mining* (pp. 160–172).
- Chen, N. C., Drouhard, M., Kocielnik, R., Suh, J., & Aragon, C. R. (2018). Using machine learning to support qualitative coding in social science. *ACM Transactions on Interactive Intelligent Systems (TiiS)*, 8(2), 1–20.

- De Lucca, J. L., & Nunes, M. G. V. (2002). *Lematização versus stemming*. Universidade de São Paulo (USP), Universidade Federal de São Carlos (UFSCar) e Universidade Estadual Paulista (UNESP).
- Dong, W., Charikar, M., & Li, K. (2011). *Efficient k-nearest neighbor graph construction for generic similarity measures*. Proceedings of the 20th International Conference on World Wide Web.
- Egger, R., & Yu, J. (2022). A topic modeling comparison between LDA, NMF, Top2Vec, and BERTopic to demystify Twitter posts. *Frontiers in Sociology*, 7, 6.
- Elsayed, M., Abdelwahab, A., & Ahdelkader, H. (2019). A proposed framework for improving analysis of big unstructured data in social media. In *2019 14th International Conference on Computer Engineering and Systems (ICCES)* (pp. 61–65). Institute of Electrical and Electronics Engineers Inc.
- Estroff, S. E., Penn, D. L., & Topor, A. (1994). The influence of social networks and social support on violence by persons with serious mental illness. *Psychiatric Services*, 45(7), 669–679.
- Ferreira, Í. A., & Moraes, S. S. (2020). Subnotificação e Lei Maria da Penha: o registro como instrumento para o enfrentamento dos casos de violência doméstica contra a mulher considerando o anuário brasileiro de segurança pública (2019). *O Público e o Privado*, 18(37), 1–20.
- Fox, C. (1989). A stop list for general text. *ACM SIGIR Forum*, 24(1–2), 19–35. <https://doi.org/10.1145/378881.378888>
- Fornari, L. F., Lourenço, R. G., Oliveira, R. N. G. de, Santos, D. L. A. dos, Menegatti, M. S., & Fonseca, R. M. G. S. da. (2021). Domestic violence against women amidst the pandemic: Coping strategies disseminated by digital media. *Revista Brasileira de Enfermagem*, 74(29).
- Ghani, N. A., Hamid, S., Hashem, I. A. T., & Ahmed, E. (2019). Social media big data analytics: A survey. *Computers in Human Behavior*, 101, 417–428.
- Giglietto, F., Rossi, L., & Bennato, D. (2012). The open laboratory: Limits and possibilities of using Facebook, Twitter, and YouTube as a research data source. *Journal of Technology in Human Services*, 30, 145–159.
- Gil, A. C. (2022). *Como elaborar projetos de pesquisa* (7ª ed.). Atlas.
- Grootendorst, M. (2022). BERTopic: Neural topic modeling with a class-based TF-IDF procedure. *arXiv preprint arXiv:2203.05794*.
- Guan, S., Hui, V., Stiglic, G., Constantino, R. E., Lee, Y. J., & Wong, A. K. C. (2025). *Classifying the information needs of survivors of domestic violence in online health communities using large language models: Prediction model development and evaluation study*. *Journal of Medical Internet Research*, 27(1), e65397. <https://doi.org/10.2196/65397>
- Kepios. (2022). *Global social media statistics – DataReportal – Global Digital Insights*. Disponível em <https://datareportal.com/social-media-users>

- Khurana, D., Koli, A., Khatter, K., & Singh, S. (2022). Natural language processing: State of the art, current trends and challenges. *Multimedia Tools and Applications*, 1–32.
- Kouzani, A. Z., & Nouman, M. (2025). *Detecting indicators of violence in digital text using deep learning*. *Natural Language Processing Journal*, 12, 100175. <https://doi.org/10.1016/j.nlp.2025.100175>
- Levendosky, A. A., Huth-Bocks, A. C., Semel, M. A., & Shapiro, D. L. (2004). The social networks of women experiencing domestic violence. *American Journal of Community Psychology*, 34(1–2), 95–109.
- Lisboa, T. K., & Zucco, L. P. (2022). Os 15 anos da Lei Maria da Penha. *Revista Estudos Feministas*, 30(29).
- Liu, T., Yang, Y., Huang, G. B., Yeo, Y. K., & Lin, Z. (2015). Driver distraction detection using semi-supervised machine learning. *IEEE Transactions on Intelligent Transportation Systems*, 17, 1108–1120. <https://doi.org/10.1109/TITS.2015.2477470>
- McInnes, L., Healy, J., & Astels, S. (2016). *hdbscan: Hierarchical density based clustering*. *Journal of Open Source Software*, 2(11), 205.
- McInnes, L., & Healy, J. (2017). Accelerated hierarchical density clustering. In *2017 IEEE International Conference on Data Mining Workshops (ICDMW)* (pp. 33–42). IEEE Computer Society. <https://doi.org/10.1109/ICDMW.2017.12>
- McInnes, L., Healy, J., & Melville, J. (2018). *UMAP: Uniform manifold approximation and projection for dimension reduction*. arXiv preprint arXiv:1802.03426.
- Michalski, R. S., Carbonell, J. G., & Mitchell, T. M. (1983). *Machine learning: An artificial intelligence approach*. Springer Berlin Heidelberg. <https://doi.org/10.1007/978-3-662-12405-5>
- Mitchell, T. M. (1997). *Machine learning*. McGraw-Hill Science/Engineering/Math.
- Mouton, J. P., Ferreira, M., & Helberg, A. S. J. (2020). A comparison of clustering algorithms for automatic modulation classification. *Expert Systems with Applications*, 151, 113317. <https://doi.org/10.1016/j.eswa.2020.113317>
- Mullah, N. S., & Zainon, W. M. N. W. (2021). Advances in machine learning algorithms for hate speech detection in social media: A review. *IEEE Access*, 9, 88364–88376.
- Mustak, M., Salminen, J., Plé, L., & Wirtz, J. (2021). Artificial intelligence in marketing: Topic modeling, scientometric analysis, and research agenda. *Journal of Business Research*, 124, 389–404.
- Ni, Y., Barzman, D., Bachtel, A., Griffey, M., Osborn, A., & Sorter, M. (2020). Finding warning markers: Leveraging natural language processing and machine learning technologies to detect risk of school violence. *International Journal of Medical Informatics*, 139.
- Pandove, D., Goel, S., & Rani, R. (2018). *Dimensionality reduction of text data: A comparative study*. *International Journal of Computer Applications*, 179(16), 6–11.

- Previatti, J. F., & Milani, M. L. (2016). Violência contra a mulher no território da 25ª Agência de Desenvolvimento Regional (ADR) catarinense: Realidade social, políticas públicas e implicações para o desenvolvimento. *Colóquio - Revista do Desenvolvimento Regional*, 13, 179–197.
- Radford, A., Kim, J. W., Xu, T., Brockman, G., McLeavey, C., & Sutskever, I. (2022). *Robust speech recognition via large-scale weak supervision*. *arXiv preprint arXiv:2212.04356*. <https://doi.org/10.48550/arXiv.2212.04356>
- Rao, P., & Taboada, M. (2021). Gender bias in the news: A scalable topic modelling and visualization framework. *Frontiers in Artificial Intelligence*, 4, 82.
- Reshamwala, A., Mishra, D., & Pawar, P. (2013). Review on natural language processing. *IRACST Engineering Science and Technology: An International Journal (ESTIJ)*, 3, 113–116.
- Russell, S., & Norvig, P. (2010). *Inteligência artificial* (2ª ed.). Elsevier.
- Samuel, A. L. (1959). Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development*, 3, 210–229.
- Santos, W. de P. (2025). *Combate à violência doméstica contra a mulher: possíveis avanços a partir da inteligência artificial*. *Brazilian Journal of Development*, 11(2), 1–17. <https://doi.org/10.34117/bjdv11n2-004>
- Saravanan, R., & Sujatha, P. (2018). A state of art techniques on machine learning algorithms: A perspective of supervised learning approaches in data classification. In *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 945–949). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/ICCONS.2018.8663155>
- Schraiber, L. B., D'Oliveira, A. F. P. L., França-Junior, I., & Diniz, C. S. G. (2007). Violência contra mulheres entre usuárias de serviços públicos de saúde da Grande São Paulo. *Revista de Saúde Pública*, 41, 359–367.
- Sinaga, K. P., & Yang, M. S. (2020). Unsupervised K-means clustering algorithm. *IEEE Access*, 8, 80716–80727. <https://doi.org/10.1109/ACCESS.2020.2988796>
- Sinoara, R. A., Camacho-Collados, J., Rossi, R. G., Navigli, R., & Rezende, S. O. (2019). Knowledge-enhanced document embeddings for text classification. *Knowledge-Based Systems*, 163, 955–971.
- Souza, A. P. de, Marin, M. J. S., & Rodrigues, P. S. (2021). O mundo sombrio das mulheres vítimas de violência: Uma análise qualitativa dos boletins de ocorrência. *New Trends in Qualitative Research*, 8, 97–105.
- Van der Maaten, L., & Hinton, G. (2008). Visualizing data using t-SNE. *Journal of Machine Learning Research*, 11, 2579–2605.
- Vieira, P. R., Garcia, L. P., & Maciel, E. L. N. (2020). Isolamento social e o aumento da violência doméstica: O que isso nos revela? *Revista Brasileira de Epidemiologia*, 23.

Walker, L. (1979). *The battered woman*. Harper and Row.

World Health Organization. (2022). *Violence against women*. Disponível em <https://www.who.int/news-room/fact-sheets/detail/violence-against-women>

Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., Wang, C., & Liu, Y. (2018). A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21, 393–430. <https://doi.org/10.1109/COMST.2018.2866942>

Zaldívar-Colado, A., Tripp-Barba, C., & Aguilar-Calderón, J. A. (2025). *Inteligencia artificial y creatividad cinematográfica: Revisión sobre el impacto de ChatGPT en la evolución de la escritura de guiones*. RISTI – Revista Ibérica de Sistemas e Tecnologia de Informação. (58), 30-35. <https://doi.org/10.17013/risti.58.20-35>.

Transformación digital sostenible: la convergencia de la innovación tecnológica y la sostenibilidad

Díaz González de Mendoza, Pável¹, Fuentes Prieto Mayda Juana²,
Díaz Manresa Karel³

pdgmendoza@gmail.com; mfp24660@gmail.com; kdm90vr46@gmail.com

¹ Empresa de Aplicaciones Informáticas (Desoft), 10400 La Habana, Cuba.

² Empresa de Aplicaciones Informáticas (Desoft), 10400 La Habana, Cuba.

³ Centro Universitario Interamericano (INTER), 97302 Mérida, Yucatán, México.

DOI: [10.17013/risti.60.96-111](https://doi.org/10.17013/risti.60.96-111)

Resumen: La transformación digital constituye un cambio organizacional profundo habilitado por tecnologías digitales. Sobre esta base emergen dos enfoques complementarios: la transformación digital verde, que orienta la digitalización a objetivos ambientales y la transformación digital sostenible, que incorpora además dimensiones sociales y económicas en alineación con los ODS. Este artículo sintetiza conceptos, delimita alcances y propone un hilo articulador entre la transformación digital, verde y sostenible. Asimismo, compara su adopción en Europa—donde, desde 2019, la “doble transición” digital-verde se integra en políticas y financiamiento y en América Latina y el Caribe, con avances desiguales, pero crecientes. Se incluye el estado del arte en Cuba y una herramienta de autoevaluación verde para mipymes, alineada con el marco normativo ambiental nacional. Se concluye con lineamientos para escalar la transformación digital sostenible con métricas verificables, gobernanza inclusiva y cooperación birregional.

Palabras-clave: Transformación digital; transformación digital verde; transformación digital sostenible; sostenibilidad ambiental y tecnologías digitales.

Sustainable digital transformation: the convergence of technological innovation and sustainability

Abstract: Digital transformation is a profound organizational change enabled by digital technologies. Two complementary approaches emerge from this foundation: green digital transformation, which orients digitalization toward environmental objectives and sustainable digital transformation, which also incorporates social and economic dimensions in alignment with the SDGs. This article synthesizes concepts, defines scope, and proposes a common thread between digital, green, and sustainable transformation. It also compares their adoption in Europe—where, since 2019, the digital-green “double transition” has been integrated into policies and financing—and in Latin America and the Caribbean, with uneven but growing progress. It includes the state of the art in Cuba and a green self-assessment tool

for MSMEs, aligned with the national environmental regulatory framework. It concludes with guidelines for scaling sustainable digital transformation with verifiable metrics, inclusive governance, and bi-regional cooperation.

Keywords: Digital transformation; green digital transformation; sustainable digital transformation; environmental sustainability and digital technologies.

1. Introducción

La transformación digital ha sido uno de los procesos más importantes y disruptivos en la evolución empresarial y social de los últimos años. Su propósito ha sido modificar los modelos de negocio tradicionales, optimizando procesos, mejorando la eficiencia y habilitando nuevas formas de interacción con clientes, proveedores y otros actores del ecosistema empresarial. A partir de 2019, el debate se ancló en la convergencia ineludible entre la digitalización y la transición ecológica con el surgimiento del Pacto Verde Europeo (*European Green Deal*), consolidando la transformación digital con los objetivos de sostenibilidad ambiental dando paso a un nuevo fenómeno: la transformación digital verde.

Este concepto no solo busca mejorar la eficiencia empresarial mediante tecnologías digitales, sino que también pretende contribuir a la sostenibilidad global mediante la reducción de la huella ambiental y el uso eficiente de los recursos naturales. La transformación digital sostenible amplía este enfoque al integrar los aspectos sociales y económicos de la sostenibilidad, alineándose con los objetivos de desarrollo sostenible. Este artículo explora las relaciones entre la transformación digital, verde y sostenible, y su aplicabilidad en diferentes contextos regionales, con énfasis en Europa y América Latina, y el caso específico de Cuba.

Los objetivos de la revisión fueron analizar la evolución conceptual y práctica de la transformación digital hacia sus variantes verde y sostenible, diferenciando sus alcances, características y aportes en relación con los objetivos de desarrollo sostenible, comparar el grado de adopción, las brechas y las oportunidades de la transformación digital verde y sostenible en Europa, América Latina y el Caribe (ALC), con énfasis en el contexto cubano y diseñar y presentar una herramienta de autodiagnóstico verde para las micro, pequeñas y medianas empresas (mipymes) cubanas, contextualizada al marco normativo nacional, que facilite la medición de su madurez ambiental-digital y promueva procesos de mejora continua.

2. Metodología

Se aplicó una revisión narrativa de alcance (*narrative scoping review*) con transparencia metodológica tipo PRISMA adaptada (Moher et al., 2009 y Codina, 2020). Criterios: horizonte 2021–2025 para políticas y reportes clave; fuentes académicas y oficiales (CEPAL, PNUD, UE, ISO, Gaceta Oficial de Cuba). Para cada documento se extrajeron año, tipo de iniciativa, actores, enfoque (digital/verde/sostenible) e indicadores. La síntesis agrupó hallazgos por: infraestructura y conectividad; gobierno y servicios digitales; iniciativas ambientales; brechas e inclusión (género/territorio). Se realizó una síntesis crítica y comparativa de diferentes contextos (Europa, ALC, Cuba),

incluyendo el marco conceptual y propuestas metodológicas propias (la herramienta de autodiagnóstico). Incluyó un amplio análisis contextual y conceptual, característico de la revisión narrativa, pero con organización por dimensiones y categorías propias de una revisión exploratoria.

La pregunta de investigación general empleada: ¿Qué avances, brechas y oportunidades presentan Europa, América Latina y el Caribe en la implementación de la transformación digital verde y sostenible?

3. Desarrollo

3.1. Definición de términos

La Transformación Digital (TD) se refiere al proceso de cambio organizacional fundamental apoyado en tecnologías digitales, con el fin de mejorar significativamente el desempeño, los procesos y modelos de negocio de una entidad. Gong y Ribiere (2021), tras analizar más de 130 definiciones, la describen como “los procesos de cambio fundamental utilizando tecnologías digitales para acelerar la transformación de negocios, procesos y competencias, aprovechando estratégicamente los recursos tecnológicos y capacidades, con impacto en la organización y la sociedad”.

Este concepto evolucionó de la mera digitalización (adopción de herramientas digitales) hacia una reconversión integral de las empresas en la era digital. El término TD cobró popularidad a partir de 2011, cuando Capgemini Consulting y el Instituto Tecnológico de Massachusetts (MIT, por sus siglas en inglés) lo acuñaron formalmente definiéndolo como “el uso de la tecnología para mejorar radicalmente el desempeño y el alcance de las empresas” (Almaguer y Malleuve, 2023; Westerman et al., 2011).

Desde entonces, la literatura académica ha enfatizado que la TD no solo implica incorporar software o hardware, sino replantear la estrategia, la cultura y los modelos operativos para aprovechar plenamente las posibilidades de las tecnologías de información, comunicación y conectividad (Aguirre y Gayá (2024), AlphaBeta, 2022; CEPAL, 2020; GorjianKhanzad y Gooyabadi, 2022; Miranda-Torrez, 2023 y Ruiz et. al., 2022 a y b).

En síntesis, la TD supone una reinención estratégica de las organizaciones apalancada en tecnologías digitales (big data, inteligencia artificial, IoT, etc.), con miras a ganar ventajas competitivas sostenibles en un entorno cada vez más digital (Alvarez, 2024; Baier et. al., 2021; Cruz y Delgado, 2024; Díaz y Fuentes, 2024; González-Varona et al., 2024; World Bank, 2023 y Ruiz et al., 2022 a y b).

La transformación digital verde (TDV) alude a la convergencia de la TD con objetivos de sostenibilidad ambiental. En términos precisos, implica aplicar las tecnologías digitales de forma estratégica para facilitar la sostenibilidad ecológica y avanzar en la acción climática. Consiste en aprovechar la digitalización para medir y reducir la huella ambiental de procesos y productos, a la vez que se cierra la brecha digital de manera sostenible (Machado-García et al., 2023 y Yan, 2018).

En la literatura académica emergente se concibe la TDV como catalizador de la “doble transición” (digital y verde) para dirigir sectores económicos hacia la neutralidad

de carbono: reducción de emisiones de gases de efecto invernadero, sin sacrificar innovación. Aunque no existe un “acuñador” único del término, su uso se ha extendido al calor de iniciativas como el Pacto Verde Europeo (*European Green Deal*) de 2019 y la noción de transformación gemela (*twin transformation*) en la Unión Europea, que enfatiza que las transiciones digital y verde deben avanzar de la mano fijando la meta de ser el primer continente climáticamente neutro para el 2050 (AIT, 2025).

Por ejemplo, la TDV abarca iniciativas como la optimización energética mediante IoT, ciudades inteligentes bajas en la emisión de carbono, agricultura de precisión que reduce insumos, entre otros, todo articulado en tecnología digital para lograr resultados “verdes”. Organismos internacionales lo han comenzado a emplear en los últimos años; el Banco Mundial lo define como “combinar el enfoque de transformación digital e inclusión con un uso estratégico y sostenible de tecnologías digitales para abordar el cambio climático”, habilitando un desarrollo bajo en emisiones. (Kocaman, 2024).

La transformación digital sostenible (TDS) es un concepto aún más integrador que busca que la transformación digital verde se planifique y ejecute incorporada plenamente a los objetivos de desarrollo sostenible (ODS) adoptados por la Organización de las Naciones Unidas que integran los aspectos relacionados el cambio climático, el desarrollo económico sostenible y el progreso social (CAF, 2022 y CEEI, 2021).

La alianza European DIGITAL SME define a la TDS como “el proceso de digitalizar la economía de manera duradera, verde y orgánica”, de forma tal que apoye la doble transición verde y digital. En otras palabras, significa orientar la TD con una mentalidad de sostenibilidad, asegurando que las innovaciones digitales no solo generen eficiencia y crecimiento, sino que también minimicen impactos ambientales, promuevan la inclusión social y creen valor a largo plazo. Este término engloba aspectos como: reducir la huella de carbono de las tecnologías de la informática y las comunicaciones (TIC) (p.ej., centros de datos alimentados con energías renovables, “Green IT”), garantizar la accesibilidad digital y la reducción de brechas sociales, y alinear las estrategias digitales corporativas con los ODS (CEPAL, 2022 y 2024). Su formulación explícita como TDS ha ganado fuerza en los últimos tres años, conforme a que empresas y gobiernos buscan conciliar la transformación tecnológica con los compromisos de sostenibilidad que vienen desarrollo con el objetivo de concentrar esfuerzos y ganar tiempo (Bonet, 2021).

La TDS enfatiza que la TD debe “durar” en el tiempo (evitando soluciones digitales efímeras o no escalables, evaluándose solamente desde perfil económico), ser verde (incidir en el control del impacto ambiental y ser en sí propia, tecnologías respetuosas con el medio ambiente) y aportar beneficios sociales.

3.2. Articulación conceptual

La TDV y la TDS ganan protagonismo entre 2019 y 2025 por su contribución a la obtención de metas medibles en la emisión de carbono (2030–2050) y por el reconocimiento de que la digitalización sin intencionalidad puede ampliar desigualdades (CEPAL, 2024). Técnica y conceptualmente, estos términos están entrelazados como partes de un mismo panorama de cambio hacia la sostenibilidad en la era digital. Cada concepto posee un énfasis particular, pero comparten fronteras comunes. La TD es principalmente un proceso habilitador transversal – la digitalización puede impulsar o acelerar otros tipos de transformación (verde y sostenible). La TDV surge precisamente en la intersección de

lo digital y lo ambiental: aprovecha la digitalización para lograr objetivos ecológicos (por ejemplo, el uso de big data para monitorear emisiones, o la inteligencia artificial para optimizar redes energéticas renovables) (World Bank, 2023). A su vez, la TDS se ubica en la intersección de la TD con la agenda amplia de sostenibilidad (ambiental y social), buscando que la digitalización sea congruente con los ODS (p. ej., usar tecnología para inclusión educativa, gobierno digital transparente, reducción de desigualdades, además de impactos verdes).

Estas relaciones pueden entenderse mediante el concepto europeo de “doble transición o transición gemela” (*twin transition*), que destaca la sinergia entre la TD y la verde como motores conjuntos de un futuro sostenible (AIT, 2025). Autores como Kocaman (2024) señalan que la intersección de la TD y la transformación verde “apunta a apoyar un crecimiento sostenible mediante la digitalización”, integrando innovación tecnológica con objetivos de sostenibilidad ambiental.

En la práctica, significa que las políticas públicas y estrategias corporativas tienden a abordar simultáneamente la digitalización y la descarbonización, reconociendo que pueden reforzarse mutuamente: las tecnologías digitales hacen más eficiente la transición ecológica, y la agenda verde le da orientación y propósito a la digitalización (por ejemplo, digitalizar para monitorear la huella de carbono, o emplear IoT para la gestión inteligente de residuos) (Haarstad y Rusten, 2018).

Asimismo, varios investigadores han tratado conjuntamente estos conceptos desarrollando marcos integrados. Por ejemplo, la literatura de Green IT/IS, también conocida como informática verde o computación sostenible, ya desde la década de 2000 exploraba cómo los sistemas de información podían usarse para la sostenibilidad ambiental, prefigurando la idea de TDV. Se refiere a un conjunto de prácticas y tecnologías diseñadas para minimizar el impacto ambiental de las operaciones de tecnologías de la información (TI). Implica el uso eficiente de los recursos, la reducción del consumo de energía y la minimización de residuos electrónicos (Fahimi, 2021).

Entre 2020 y 2025, se han publicado trabajos que abordan la TDS apoyada en lo digital en sectores pertenecientes a la industria 5.0, las ciudades inteligentes o la agricultura climáticamente inteligente. Todos ellos confirman que la digitalización puede ser un catalizador para alcanzar metas verdes y sociales, siempre que se incorpore intencionalmente a tiempo en esa dirección (Aguilar et al., 2023, Díaz y Macía, 2024 y AIT, 2025).

En la literatura académica y sobre políticas se reconoce cada vez más esta interdependencia. La Unión Europea, por ejemplo, ha adoptado explícitamente la agenda de transformaciones gemelas: su estrategia pospandemia condicionó gran parte de los fondos de recuperación a que los proyectos contribuyan simultáneamente a la TD y verde (Kocaman, 2024). Esto refleja que, en la práctica, resulta beneficioso impulsar ambas transformaciones en conjunto –no como vías separadas– para lograr un impacto más profundo.

La Figura 1 ilustra esquemáticamente estas interrelaciones. La TD es un proceso transversal que puede solaparse tanto con la transformación verde (orientado a la implementación de la política ambiental), como con los objetivos de transformación

sostenible (que engloba las políticas gubernamentales asociadas a los elementos ambientales y sociales).

La zona de superposición entre las transformaciones digital y verde (1), corresponde a la TDV, donde las iniciativas digitales se orientan explícitamente a objetivos ecológicos. La intersección entre la esfera de la TD y toda la agenda gubernamental sostenible (2), corresponde a la TDS, que implica alinear la transformación digital con todos los pilares de la sostenibilidad. De este modo, puede verse que los términos no compiten entre sí, sino que se complementan: la TD provee herramientas y cambios tecnológicos; articulan esfuerzos híbridos necesarios para materializar la visión de un desarrollo sostenible apoyado en la tecnología.

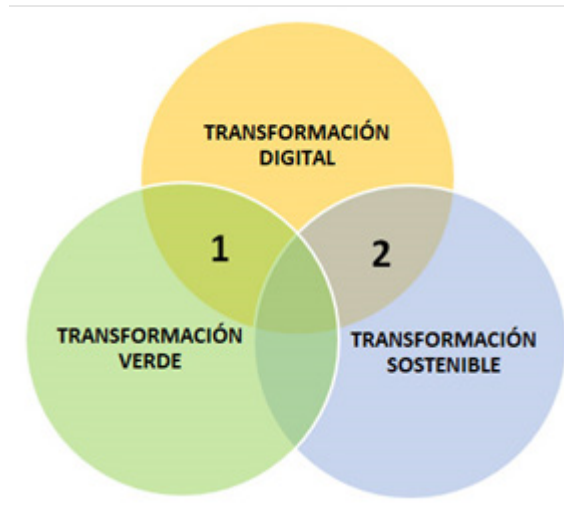


Figura 1 – Representación conceptual de la interrelación entre los términos transformación digital, verde y sostenible.

Para una organización empresarial, independientemente de su dimensión, la estrategia debe desarrollarse por etapas para poder ir adoptando las herramientas digitales más adecuadas a su modelo de negocio, la disponibilidad de financiamiento y las normativas sobre la gestión ambiental globales, nacionales y locales donde se encuentre, así como del destino de sus productos y servicios (Figura 2).



Figura 2 – Transición entre digitalización, transformación digital, transformación digital verde y transformación sostenible.

3.2.1. Valoración de la novedad de los conceptos

La TDV ha cobrado relevancia conforme las empresas y gobiernos se plantean metas de neutralidad para la emisión de carbono en el periodo 2030-2050, reconociendo que sin herramientas digitales (p.ej. redes inteligentes, sensores ambientales, algoritmos de eficiencia) será difícil lograrlas (Miranda-Torrez, 2023 y Abdulhadi et al., 2024).

Por su parte, TDS expande aún más el alcance e introduce una visión innovadora: propone que la TD debe diseñarse con un mandato de sostenibilidad desde el inicio, en vez de corregir externamente sus efectos. Este énfasis relativamente nuevo en “digital con propósito sostenible” está siendo impulsado por iniciativas globales recientes, como la Alianza Digital Inclusiva y Sostenible UE–ALC de 2023 (EDSA, 2020) y por la creciente atención a aspectos como la huella ambiental de la industria tecnológica (pensemos en los *data centers* y el consumo energético de las criptomonedas) y la brecha digital como problema de equidad (Aguilar et al., 2023).

Es importante conceptualizar independientemente estos nuevos términos –TDV y TDS– porque aportan matices que no estaban presentes en las nociones originales. La TD “genérica” suele orientarse a eficiencia y competitividad, pero al incorporarle el adjetivo verde o sostenible se introducen criterios cualitativos distintos: bajas emisiones, uso responsable de recursos, inclusión social, etc. y vincularlos a indicadores de desempeño de las empresas. Separarlos conceptualmente ayuda a establecer metas claras y métricas propias. Por ejemplo, una iniciativa de TDS deberá medirse no solo en términos de ganancias de productividad, sino también en su contribución a los ODS (reducción de desigualdades, mejora ambiental, etc.). En cambio, una TD tradicional podría medirse únicamente en retorno de la inversión (ROI) o crecimiento digital. Así, distinguir estos términos evita que la sostenibilidad quede diluida como mera consecuencia deseable y, en cambio, la posiciona como objetivo explícito de ciertas transformaciones. Autores en el ámbito de la gestión ambiental enfatizan que integrar la sostenibilidad en la TD requiere cambios de mentalidad y enfoques diferentes, lo cual justifica un marco conceptual propio.

En cuanto a la relevancia actual de cada término: todos son altamente pertinentes, pero en contextos algo distintos. La TD sigue siendo un imperativo estratégico para empresas y gobiernos –aún más tras la pandemia de COVID-19, que aceleró la digitalización–, dado que está asociada con innovación, eficiencia y nueva creación de valor (CEPAL, 2024).

Ahora bien, los términos híbridos muestran su relevancia en agendas específicas: TDV es vital en sectores donde la digitalización puede generar saltos cualitativos en sostenibilidad (energía, agricultura, transporte). Por ejemplo, sin digitalización (redes eléctricas inteligentes, sensores, IA) la incorporación masiva de renovables y la eficiencia energética a gran escala sería mucho más lenta –de ahí que la TDV sea un habilitador clave para cumplir el Acuerdo de París (Kocaman, 2024).

A su vez, la TDS refleja preocupaciones actuales sobre el impacto social de la digitalización: hoy reconocemos que la tecnología digital no es neutra, puede amplificar brechas sociales si no se gestiona bien. Por ende, se habla de TDS al diseñar estrategias nacionales de digitalización que incluyan capacitación laboral, accesibilidad, ética en

inteligencia artificial, etc., asegurando que la TD “no deje a nadie atrás”, principio central de la Agenda 2030 (CEPAL, 2024).

En suma, en el contexto contemporáneo estos conceptos son complementarios y cada uno aborda un desafío de nuestra triple transición global (tecnológica, ambiental y socioeconómica). La novedad de TDV y TDS radica en su enfoque integrado, lo cual responde a la convicción creciente de que los grandes desafíos (digitalización, cambio climático, desarrollo sostenible) deben encararse simultáneamente y de forma articulada para obtener soluciones efectivas y sinérgicas.

3.2.2. Desarrollo regional: Europa vs. América Latina y el Caribe

La dinámica empresarial contemporánea, tanto en países desarrollados como en aquellos en vías de desarrollo, revela una integración creciente entre la TD y los sistemas de gestión ambiental (SGA). Dos factores están acelerando esta sinergia: en primer lugar, la obligación de implementar SGA en las organizaciones, una exigencia ya vigente en grandes empresas y que se extenderá a las pymes de manera gradual a nivel internacional. En segundo lugar, la creciente demanda del mercado por productos y servicios respaldados por procesos respetuosos con el entorno, lo que otorga valor añadido a la oferta empresarial. Este escenario en el sistema empresarial, impone un reto particular a los productores y proveedores de herramientas y servicios informáticos.

En la actualidad, estas exigencias representan una oportunidad para acceder a los mercados más competitivos. Sin embargo, en un futuro próximo, constituirán verdaderas barreras de entrada. Una TD orientada estratégicamente a las nuevas tendencias sostenibles puede marcar una diferencia significativa en el desempeño de una organización y en la aceptación de sus productos y servicios.

El grado de avance y la forma de adopción de estos conceptos presentan diferencias notables entre Europa y América Latina y el Caribe (ALC), aunque también algunas tendencias convergen (Unión Europea, 2022). En Europa, la TD y la transformación verde/sostenible se abordan de manera intencionalmente integrada, reflejándose en estrategias de alto nivel. La Unión Europea ha sido pionera en declarar la meta de una “transición gemela” digital y verde –por ejemplo, condicionando su fondo de recuperación NextGenerationEU (750.000 M€) a que los proyectos apoyen simultáneamente la TD y la ecológica (Kocaman, 2024).

Europa exhibe altos niveles de digitalización: más del 90% de su población usa internet. Las empresas y gobiernos tienen índices elevados de adopción tecnológica, y existe un ecosistema robusto de innovación digital. Esto ha permitido que la TD europea esté relativamente madura, pasando de una mera digitalización de procesos hacia la reconfiguración digital de sectores enteros (industria 5.0 en manufactura, fintech en banca, gobierno digital, etc.) (Fahimi, 2021).

Por contraste, en ALC la adopción de estos conceptos ha sido más heterogénea y con ritmos diferentes, aunque en años recientes la brecha comienza a cerrarse parcialmente. En materia de TD, ALC ha avanzado en la conectividad y digitalización, pero persisten importantes brechas. Alrededor del 80% de la población urbana latinoamericana tiene acceso a internet, cifra comparable a regiones desarrolladas, pero en las zonas rurales y

entre los estratos de menores ingresos el acceso cae drásticamente, con brechas de hasta 50 puntos porcentuales (NU-CEPAL, 2025).

La investigación muestra que la región aún enfrenta un desafío de inclusión digital (infraestructura deficiente en áreas remotas, costos elevados y desigualdad socio-digital). No obstante, la pandemia actuó como catalizador: se aceleró el comercio electrónico, la banca digital, el teletrabajo y educación virtual, forzando a muchos actores a transformarse digitalmente. Organismos como CEPAL sostienen que una TD real y efectiva podría ser el puente para que ALC supere sus trampas estructurales de bajo crecimiento y alta desigualdad, siempre y cuando se cierre la brecha digital y se oriente hacia la productividad e inclusión (CEPAL, 2024).

En este sentido, varios países latinoamericanos han lanzado agendas de TD (ej. Colombia y Chile con estrategias nacionales “Industria 4.0” o “Gobierno Digital”). Sin embargo, en general la madurez digital corporativa y estatal en ALC es menor que en Europa. Muchas pymes aún están en etapas básicas de digitalización y la inversión en investigación y desarrollo tecnológico es reducida (en promedio ~0.5% del PIB, muy por debajo de la UE) (CEPAL, 2022).

Otro contraste está en el enfoque estratégico regional: Europa ha adoptado una aproximación normativa y proactiva (imponiendo objetivos legales, estándares –por ejemplo, exigencias de eco- diseño, digitalización de servicios públicos obligatoria– y destinando fondos cuantiosos a innovación verde-digital). ALC, en cambio, tiende a avanzar mediante proyectos piloto y cooperación internacional. Por ejemplo, la reciente Alianza Digital UE-ALC y el programa Global Gateway destinarán inversiones para infraestructura digital y energías limpias en la región, reflejando un enfoque de asociación para impulsar la doble transformación digital-verde en Latinoamérica. Esto evidencia la convergencia de intereses: tanto Europa como ALC reconocen la importancia de la transformación digital y verde, y buscan colaborar (Europa aportando tecnología y financiamiento, ALC aprovechando la oportunidad para modernizarse sosteniblemente).

La CEPAL en 2022 subrayó que la coordinación birregional puede ayudar a ALC a recuperarse mejor tras la pandemia, invirtiendo en sectores verdes con apoyo de herramientas digitales, a la vez que reduce brechas sociales (CEPAL, 2024).

Lo avanzado evidencia que Europa exhibe un mayor grado de avance en la TDV y su integración sostenible: alta penetración digital, marcos regulatorios verdes robustos, y vinculación explícita de ambas (*twin transition*). ALC, aunque rezagada en indicadores (menor productividad digital, mayores brechas socio-digitales, y desafíos socioeconómicos que compiten con prioridades ambientales), está adoptando gradualmente estos conceptos en su agenda de desarrollo.

La similitud principal es que ambas regiones conciben ya la TD y la TDV como elementos clave para un desarrollo futuro sostenible, con énfasis en la inclusión. La diferencia estriba en la velocidad y profundidad: Europa avanza con pasos firmes hacia la neutralidad de carbono y la sociedad digital del conocimiento, mientras ALC aún se esfuerza por sentar las bases (conectividad universal, instituciones sólidas) para poder emprender esas transformaciones plenamente (CEPAL, 2022 y NU-CEPAL, 2025).

No obstante, la cooperación reciente y el aprendizaje mutuo, compartiendo regulación digital o tecnologías limpias europeas adaptadas a contextos latinoamericanos, auguran que la brecha podría acortarse.

En cualquier caso, tanto en Europa como en ALC la triple transformación –digital, verde y sostenible– se reconoce como la vía obligada para afrontar los desafíos del siglo XXI, desde la cuarta revolución industrial hasta la crisis climática y la necesidad de un desarrollo más humano, sientan las bases para el desarrollo regional de la Industria 5.0 (Díaz y Maciá, 2024).

3.3. Estado del arte en Cuba (2021–2025)

3.3.1. Transformación digital y sostenibilidad en la política pública cubana

Durante el período 2021–2025, Cuba ha experimentado un proceso de reconfiguración digital que, aunque desigual y con limitaciones tecnológicas, ha estado acompañado de avances normativos, institucionales y experimentales hacia una TD más inclusiva y sosteniblemente orientada (Ruiz *et. al.*, 2022 a y b). En este contexto, aunque aún incipiente, es posible identificar la presencia de elementos asociados a la TDV y a una TDS en determinadas políticas, proyectos y estudios nacionales.

Un punto de inflexión clave en este quinquenio ha sido la aprobación de la política para la TD y la Agenda Digital Cubana 2030, adoptadas en 2022 bajo el liderazgo del Ministerio de Comunicaciones (MINCOM) y del grupo temporal para la informatización. Esta política establece cinco pilares estratégicos: infraestructura digital, economía digital, gobierno digital, desarrollo de capacidades y ciberseguridad. Aunque el enfoque central de esta agenda es económico y gubernamental, la inclusión social y la sostenibilidad ambiental comienzan a perfilarse como dimensiones transversales. En su artículo sobre esta política, Arevich (2022) destaca que la Agenda Digital Cubana se alinea con los ODS, pero advierte que aún es necesario desarrollar mecanismos concretos para evaluar el impacto ambiental y social de la digitalización.

La visión oficial cubana considera a la TD como palanca para el desarrollo socioeconómico, el cierre de brechas territoriales y la eficiencia en la gestión pública. No obstante, el marco normativo no explicita aún métricas ambientales asociadas a procesos digitales, ni criterios de sostenibilidad ecológica en la expansión de infraestructuras TIC. Aun así, esta política representa el andamiaje sobre el cual podrían desarrollarse acciones futuras vinculadas a la TDV y la TDS, al menos en términos programáticos (Arevich, 2022).

3.3.2. Iniciativas locales, proyectos científicos y sostenibilidad tecnológica

Un segundo enfoque emergente dentro del estado del arte cubano es la articulación entre digitalización, desarrollo territorial y sostenibilidad, en parte impulsado por experiencias de cooperación internacional. En este sentido, el trabajo de Ruiz y Amoroso (2023) analiza cómo algunos gobiernos locales, apoyados por la Plataforma Articulada para el Desarrollo Integral Territorial (PADIT) —una iniciativa conjunta entre el Gobierno cubano, el PNUD y otros socios— están adoptando modelos de gobernanza digital local. Estos modelos permiten la incorporación de herramientas tecnológicas en procesos

de planificación, participación y servicios públicos, integrando criterios de inclusión (especialmente de género) y eficiencia administrativa (Méndez y Torres, 2023).

Uno de los aportes centrales de esta línea de investigación es que la TD en el contexto cubano debe ser entendida desde una lógica territorial, participativa y adaptada a los recursos disponibles. En experiencias documentadas en provincias como Holguín y Villa Clara, la digitalización se vincula con la gestión local del desarrollo, la administración electrónica y los servicios sensibles al género. Aunque no se emplea el término TDV de manera explícita, se observan elementos que la prefiguran, tales como la optimización del uso energético en oficinas públicas mediante herramientas de monitoreo, o la digitalización de procesos de planificación urbana con enfoque ambiental (Ruiz *et. al*, 2023 a).

Esta dimensión sugiere que la sostenibilidad digital en Cuba puede no provenir exclusivamente del estado a nivel central, sino también de experiencias locales contextualizadas, apoyadas en sinergias con organismos internacionales y la academia cubana.

3.3.3. Innovación científica y transformación digital verde

Una tercera área incipiente, pero prometedora, dentro del ecosistema cubano es la convergencia entre investigación científica, infraestructura digital y sostenibilidad energética. El desarrollo del proyecto Humboldt Highway II, consiste en un clúster de alto rendimiento para la computación científica, ubicado en el Instituto Superior de Tecnologías y Ciencias Aplicadas (InSTEC) de la Universidad de La Habana. Esta instalación está diseñada para funcionar exclusivamente con energías renovables, como parte de un modelo de soberanía tecnológica verde.

Este caso es particularmente relevante como ejemplo cubano de TDV en el ámbito científico-académico, donde se integran consideraciones de eficiencia energética, reducción de huella de carbono y computación distribuida. A diferencia de muchas implementaciones tecnológicas convencionales, esta propuesta parte de una visión “eco-digital” desde su diseño: cada módulo del clúster se alimenta de fuentes limpias y busca reducir el impacto ambiental de los procesos de cálculo intensivo. Además, el proyecto contempla la colaboración abierta con universidades latinoamericanas para escalar este modelo en el sur global.

Este tipo de experiencia, aunque aún aislada, evidencia que existen capacidades científicas y técnicas en Cuba para desarrollar proyectos de TDV, siempre que cuenten con el apoyo institucional y financiero necesario.

3.3.4. Brechas, desafíos y oportunidades

A pesar de los avances mencionados, Cuba enfrenta importantes desafíos tecnológicos para consolidar una verdadera TDS. En términos de infraestructura, persiste una notable brecha digital territorial y económica, especialmente entre zonas urbanas y rurales. Según datos oficiales, la cobertura de internet móvil ronda el 86 % de la población, pero con importantes disparidades en velocidad, asequibilidad y calidad del servicio.

Asimismo, se requieren indicadores ambientales asociados a la expansión digital —como el consumo energético de centros de datos, la generación de residuos electrónicos o el uso eficiente del espectro digital— limita la capacidad de monitorear impactos ecológicos. A esto se suma la necesidad de incorporar enfoques de derechos digitales, accesibilidad universal y ética tecnológica, dimensiones fundamentales para una TDS plena, y que en el caso cubano requieren aún desarrollo regulatorio.

3.4. Las mipymes cubanas ante la TDV: una herramienta de autodiagnóstico contextualizada

Las mipymes cubanas operan en un entorno complejo, caracterizado por limitaciones tecnológicas, problemas de conectividad y crecientes exigencias regulatorias ambientales, lo que hace prioritaria una transformación digital con enfoque verde. No obstante, hasta recientemente el país carecía de instrumentos contextualizados y alineados con la legislación nacional para evaluar la madurez ambiental-digital de estas organizaciones.

Para atender esta brecha, se desarrolló la herramienta **TDV-Cuba**, un autodiagnóstico verde diseñado específicamente para mipymes cubanas, basado en una adaptación del modelo TETR4DIG (De Armas et al., 2022). El instrumento evalúa de forma integral y formativa la incorporación de la transformación digital verde mediante 22 preguntas organizadas en tres dimensiones: cumplimiento normativo ambiental, gestión digital ambiental y cultura organizacional e innovación ambiental digital, todas vinculadas a la normativa vigente.

La herramienta permite identificar riesgos regulatorios, valorar el uso de tecnologías digitales para la sostenibilidad y analizar el grado de apropiación organizacional del enfoque TDV. Su escala pedagógica de cinco niveles de madurez orienta planes de mejora continua sin fines punitivos.

A diferencia de diagnósticos internacionales, TDV-Cuba se distingue por su alineación normativa, adaptación al contexto cubano y aplicabilidad tanto en espacios formativos como en procesos reales de asesoría y autodiagnóstico. En conjunto, constituye una innovación metodológica coherente con la Agenda Ambiental y la estrategia de transformación digital del país, facilitando que las mipymes avancen de manera viable y responsable hacia la sostenibilidad digital.

4. Conclusiones

La convergencia entre transformación digital, digital verde y digital sostenible es hoy imprescindible para responder a los desafíos del desarrollo, al integrar innovación, sostenibilidad ambiental e inclusión social. La experiencia europea evidencia avances sólidos en esta doble transición, mientras que América Latina y el Caribe, y en particular Cuba, enfrentan brechas estructurales, pero también oportunidades de adaptación y escalamiento de soluciones propias.

En este contexto, la Agenda Digital Cubana 2030 y experiencias nacionales emergentes muestran un punto de partida relevante, aunque aún insuficiente sin instrumentos operativos y métricas claras. La herramienta TDV-Cuba constituye un aporte concreto

al ofrecer un autodiagnóstico normativamente alineado y formativo para impulsar la madurez ambiental-digital de las mipymes.

Avanzar hacia una transformación digital verdaderamente sostenible exige integrar criterios ambientales y sociales desde el diseño, medir impactos, fortalecer capacidades y consolidar alianzas. Este trabajo aporta fundamentos conceptuales y una herramienta aplicable para orientar políticas públicas, investigación y gestión organizacional hacia una digitalización innovadora, verde y socialmente justa.

Agradecimientos

A AS@I Informatika, Orío, Gipuzkoa, País Vasco, España (<https://www.asaiinformatik.es>) por el soporte técnico y financiamiento para la realización de las investigaciones en España.

Al Dr. C. Gotzon Bernaola Ariño, Coordinador General de Innovación Empresarial de la Agencia Vasca de Innovación, País Vasco, España (<https://www.innobasque.eus>), por las sugerencias brindadas para encausar la investigación y la información técnica aportada.

Al M.Sc. Ricardo Castro Armas, Director de Infocomunicaciones, del Centro de Investigaciones y Desarrollo de Medicamentos (CIDEM) (www.cidem.cu) por las orientaciones metodológicas aportadas.

A la Dra. Marta Negrillo Damas, Consultora Medio Ambiente, Formadora, Técnico en Servicios Ambientales, Universidad de Valladolid y Universidad de Jaén, Andalucía, España por los conocimientos aportados sobre los sistemas de gestión ambiental en el marco de la UE y específicamente España.

Referencias

- Abdulhadi, M., Zafar, M., Reeti, A., Alofaysan, H., & Kumar, A. (2024). Unveiling green digital transformational leadership: Nexus between green digital culture, green digital mindset, and green digital transformation. *Journal of Cleaner Production*, 450, 141670. <https://doi.org/10.1016/j.jclepro.2024.141670>
- Aguilar, A., Melguizo, A., Balmaseda, M., & Muñoz, V. (2023). Digitales, verdes y aliados: Impacto económico, social y medioambiental de la iniciativa Global Gateway y la Alianza Digital UE–América Latina y el Caribe. Fundación Carolina y Telefónica. <https://www.fundacioncarolina.es/catalogo/digitales-verdes-y-aliados-impacto-economico-social-y-medioambiental-de-la-iniciativa-global-gateway-y-la-alianza-digital-ue-america-latina-y-el-caribe/>
- Aguirre, E & Gayá, R. (2024). Programas escalables para la transformación digital de las pymes con miras a la exportación. Documentos de proyectos e investigación (CEPAL). <https://hdl.handle.net/11362/68870>.
- Austrian Institute of Technology (2025). “Twin Transition”: How can we shape the green and digital transformation that is currently taking place in parallels? Discussing Technology. <https://www.ait.ac.at/en/blog/green-and-digital-transformation>

- Almaguer, A. & Malleuve, A. (2023). El proceso de digitalización como una transformación organizacional: Clave de eficiencia y competitividad. *Revista Cubana de Transformación Digital*, 4(2),1–11. <https://rctd.uic.cu/rctd/article/view/197>
- AlphaBeta (2022). Transformación digital. Así es como las tecnologías digitales impulsan las exportaciones en América Latina. <https://connectamericas.com/es/tecnologias-digitales-exportaciones>
- Alvarez, Z. (2024). Alfabetización digital y competencias digitales: Una mirada desde eLAC2024. *Revista Cubana de Transformación Digital*, 5(2),1–9. <https://rctd.uic.cu/rctd/article/view/240>
- Arevich Marín, M. (2022). Política para la transformación digital y la Agenda Digital Cubana 2030. *Revista APyE*, (13), 23–35.
- Baier, H., Walsh, D. & Mulder, N. (2021). La transformación digital de las pymes exportadoras: Perspectiva teórica y práctica. CEPAL. <https://repositorio.cepal.org/handle/11362/47450>
- Bonet, J.L. (2021). Los objetivos de desarrollo sostenible en la estrategia de la cámara de España y de la red cameral. https://empresasostenible.camara.es/sites/default/files/2022-09/ODS%20Ca%CC%81mara%20de%20Espan%CC%83a%20DATOS%202021_o.pdf
- CAF (2022). Guía práctica de sostenibilidad para pymes. Banco de Desarrollo de América Latina. <https://sostenibilidad.caf.com/documentos/guia-pymes.pdf>
- Centro Europeo de Empresas e Innovación de Valencia (2021). Autoevaluación: Madurez digital para pymes. Centro Europeo de Empresas e Innovación. <https://ceeivalencia.emprenemjunts.es/?op=65yn=1076>
- CEPAL (2020). Transformación digital para una recuperación sostenible y con igualdad. <https://www.cepal.org/es/publicaciones/46504-transformacion-digital-una-recuperacion-sostenible-igualdad>
- CEPAL (2022). Un camino digital para el desarrollo sostenible de América Latina y el Caribe (LC/CMSI.8/3). <https://repositorio.cepal.org/handle/11362/48460>
- CEPAL (2024). Una transformación digital real y efectiva puede ayudar a ALC a superar trampas de desarrollo. <https://www.cepal.org/es/comunicados/transformacion-digital-real-efectiva-puede-ayudar-america-latina-caribe-superar-trampas>
- Codina, Ll. (2020). Cómo hacer revisiones bibliográficas tradicionales o sistemáticas utilizando bases de datos académicas. *Revista ORL*, 11(2), 22977. <https://dx.doi.org/10.14201/orl.22977>
- Cruz, J.C. & Delgado, M (2024). Bases del modelo de dirección estratégica de la transformación digital con impacto económico-social en el municipio Baraguá. *Rev. APyE*, 8(3),e322. <https://doi.org/10.5281/zenodo.14606459>
- De Armas, L., Díaz, E. & Reyes, G. (2022). TETR4DIG: Modelo conceptual y evaluación de madurez del cambio organizacional enfocado en la transformación digital. *Revista Cubana de Transformación Digital*, 3(3),177. <https://rctd.uic.cu/rctd/article/view/177>

- Díaz, P. & Fuentes, J. (2025) Transformación digital para la exportación. Enfoque: Revista NUEVA EMPRESA, 12(1).
- Díaz, P. & Maciá, M. E. (2024). Convergencias hacia la Industria 5.0 en Cuba. Revista Cubana de Educación Superior, 43(2), 214-229. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=So257-43142024000200214
- Fahimi, Y. (2021) Europa y América Latina: ¿cómo enfrentar juntos una transformación social y ecológica? NUEVA SOCIEDAD 2021:291. https://static.nuso.org/media/articles/downloads/4.TC_Fahimi_291.pdf
- Gong, C. & Ribiere, V. (2021). Developing a unified definition of digital transformation. Technovation, 102, 102217. <https://doi.org/10.1016/j.technovation.2020.102217>
- González-Varona, J. M., López-Paredes, A., Poza, D., & Acebes, F. (2024). Building and development of an organizational competence for digital transformation in SMEs. Journal of Industrial Engineering and Management, 14(1), 15-24.
- GorjianKhanzad, Z., & Gooyabadi, A. A. (2022). Digital Strategizing: The Role of the Corporate Culture. Open Journal of Business and Management, 10, 2974-2995.
- Haarstad, H., & Rusten, G. (2018). Transformación verde en Noruega. Compilación académica en noruego que analiza la conceptualización de la transformación verde y el cambio verde con énfasis en políticas noruegas. Universidad de Oslo.
- Kocaman, E. (2024). Twin Transformation: Integration of Green and Digital Transformation. CarbonGate Blog, 13 July 2024. <https://www.carbongate.io/en/blog/ikiz-donusum-yesil-donusum-ve-dijital-donusumun-entegrasyonu>
- Machado-García, N., Fernández, A. & Farradas-Machado, C. (2023). Transformación digital del sector agroalimentario en Cuba. Ingeniería Agrícola, 13(2).
- Méndez, M. & Torres, L. M. (2023). Del gobierno electrónico al gobierno digital: transformación integral más allá de la digitalización de servicios. Tono, 19(1), 7-22. <http://www.revistatono.etecsa.cu/tono/article/view/376>
- Miranda-Torrez, J. (2023). La transformación digital. Estrategia generadora de cambios en las organizaciones. Revista Estrategia Organizacional, 12,(2), 109-135.
- Moher, D., Liberati, A., Tetzlaff, J. & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Medicine, 6(7).
- NU-CEPAL. (2025). Superar las trampas del desarrollo de América Latina y el Caribe en la era digital: el potencial transformador de las tecnologías digitales y la inteligencia artificial. <https://repositorio.cepal.org/server/api/core/bitstreams/e4ca636c-2b8a-4138-8c62-b685540d9b99/content>
- Ruiz, A., Delgado, T., Febles, A. & Estévez, S. (2022a). Habilitando la transformación digital. Tomo I. Editorial UH. <https://repositorio.uci.cu/jspui/handle/123456789/10427>.
- Ruiz, A., Delgado, T., Febles, A. & Estévez, S. (2022b). Habilitando la transformación digital. Tomo II. Editorial UH. <https://repositorio.uci.cu/jspui/handle/123456789/10428>.

- Unión Europea (AL-INVEST Verde). (2022). Guía de financiamiento sostenible para pymes en América Latina. <https://eulacfoundation.org/es/guia-financiamiento-sostenible-pymes-al-invest-verde.pdf>
- Westerman, G., Calmédjane, C., Bonnet, D., Ferraris, P., & McAfee, A. (2011). Digital Transformation: A Road-Map for Billion-Dollar Organizations. MIT Center for Digital Business and Capgemini Consulting. https://www.capgemini.com/wp-content/uploads/2017/07/Digital_Transformation__A_Road-Map_for_Billion-dollar_Organizations.pdf
- World Bank (2023). Green Digital Transformation: How to Sustainably Close the Digital Divide and Harness Digital Tools for Climate Action. Climate Change and Development Series. <https://openknowledge.worldbank.org/handle/10986/40653>
- Yan, H. W. (2018). Exploration of Chinese SMEs' export development: The role of managerial determinants based on an adapted innovation-related internationalization model. *Thunderbird International Business Review*, 60(1).

Reconocimiento de emociones en texto de estudiantes de educación secundaria rural utilizando algoritmos de clasificación

Fidel Huanco-Ramos¹, Yesenia Valentin-Ccori², Henry Shuta-Lloclla³,
Martha Yucra-Sotomayor³, Fredy Aparicio Castillo-Suaquita³

**fhuanco@unsa.edu.pe; valentinyesenia2@gmail.com; henryshuta@unap.edu.pe;
myucras@unap.edu.pe; fcastillo@unap.edu.pe**

¹ Universidad Nacional de San Agustín de Arequipa, Arequipa, 04001, Perú.

² Universidad Nacional de San Antonio Abad del Cusco, Puno, 21001, Perú.

³ Universidad Nacional del Altiplano, Puno, 21001, Perú.

DOI: 10.17013/risti.60.112-126

Resumen: Este estudio se centra en la aplicación de algoritmos de inteligencia artificial para el reconocimiento automático de emociones a partir de textos. El objetivo es identificar el algoritmo de clasificación más adecuado para detectar emociones en los textos que comúnmente se expresan en las instituciones de educación secundaria rural de Puno. Se recopiló una encuesta de autoevaluación emocional, los cuales fueron etiquetados manualmente por evaluadores capacitados y validados mediante consenso. Tras un preprocesamiento que incluyó tokenización, eliminación de stopwords y vectorización TF-IDF, los modelos fueron entrenados y evaluados utilizando Google Colab y la biblioteca scikit-learn. Los resultados revelaron que el algoritmo Random Forest destacó con una precisión del 73.81% y un AUC de 88.67%, superando a otros algoritmos en la identificación de emociones críticas. En conclusión, los hallazgos resaltan la importancia de detectar emociones negativas para mejorar el bienestar estudiantil y sugieren que la inteligencia artificial puede enriquecer la educación rural al identificar grupos de estudiantes con emociones similares, promoviendo así un ambiente escolar positivo y un mejor rendimiento académico.

Palabras-clave: Algoritmos de clasificación; Educación secundaria; Inteligencia artificial; Reconocimiento de emociones.

Emotion recognition in the text of rural secondary school students using classification algorithms

Abstract: This study focuses on the application of artificial intelligence algorithms for the automatic recognition of emotions from textual data. The objective is to identify the most suitable classification algorithm for detecting emotions in texts commonly expressed in rural secondary education institutions in Puno. A total

of 1,150 textual comments were collected through an emotional self-assessment survey, manually labeled by trained evaluators and validated through consensus. After preprocessing steps including tokenization, stopword removal, and TF-IDF vectorization, the models were trained and evaluated using Google Colab and the *scikit-learn* library. The results indicate that the Random Forest algorithm achieved the best performance, with a precision of 73.81% and an AUC of 88.67%, outperforming other algorithms in the identification of critical emotions. In conclusion, the findings highlight the importance of detecting negative emotions to improve student well-being and suggest that artificial intelligence can enhance rural education by identifying groups of students with similar emotional profiles, thereby promoting a positive school environment and improved academic performance.

Keywords: Artificial intelligence; Classification algorithms; Emotion recognition; Secondary education.

1. Introducción

Durante la última década, el interés por comprender las emociones ha ido en aumento dentro del ámbito educativo, en particular en aquellos espacios donde el bienestar emocional de los estudiantes se refleja directamente en su rendimiento académico (Alcocer-Sánchez et al., 2023). La habilidad para identificar y entender las emociones de los estudiantes se ha vuelto fundamental para crear entornos de aprendizaje efectivos y fomentar el desarrollo integral de los alumnos (Sagredo-Lillo et al., 2024). En las zonas rurales, esta necesidad es aún más importante debido a los retos específicos que enfrentan estas comunidades, como el aislamiento geográfico, el acceso limitado a servicios de apoyo psicológico, la escasez de recursos educativos y los factores culturales únicos que influyen en la forma en que se expresan las emociones (U. Alzubaidi, 2025).

En la región de Puno, Perú, ubicada a más de 3800 metros sobre el nivel del mar (m s.n. m.), es fundamental comprender cómo las emociones impactan en el aprendizaje y disponer de estrategias efectivas para detectarlas a tiempo (Vilca, 2016). Esta región presenta características particulares del contexto rural andino, donde factores culturales, socioeconómicos y de aislamiento geográfico influyen significativamente en las manifestaciones emocionales de los estudiantes (Zela Payi et al., 2022a). El uso de algoritmos de clasificación para el reconocimiento automático de emociones se plantea como una herramienta innovadora que puede ayudar a mejorar la interacción educativa y fortalecer el clima escolar en estas comunidades (Zhou, 2012).

Las tecnologías de inteligencia artificial (IA) y los algoritmos de aprendizaje automático abarcan un conjunto diverso de técnicas y aplicaciones orientadas a crear sistemas capaces de llevar a cabo tareas que, por lo general, requieren de la inteligencia humana (Segura Zúñiga, 2022). La inteligencia artificial está cambiando distintos sectores, como el reconocimiento de voz, el procesamiento del lenguaje natural, la visión por computadora y la robótica (Huanco-Ramos & Apaza-Tarqui, 2024). Gracias a su capacidad para aprender a partir de grandes volúmenes de datos, estos sistemas pueden mejorar de manera constante su rendimiento (Apaza-Tarqui & Huanco-Ramos, 2025). En el campo educativo, se han creado distintas tecnologías que buscan incorporar el análisis de las emociones dentro del proceso de enseñanza-aprendizaje (López et al., 2016).

A pesar de ello, son pocos los estudios que se centran específicamente en el reconocimiento de emociones en contextos educativos rurales, incorporando los factores culturales propios que influyen en las expresiones emocionales de los estudiantes en estas regiones (Cordero García et al., 2019a). Este vacío en la literatura evidencia la necesidad de explorar cómo los algoritmos de clasificación basados en aprendizaje automático pueden ajustarse y utilizarse de forma eficaz para detectar emociones en entornos educativos rurales de gran altitud, especialmente en la región de Puno (Patiño et al., 2024; Zela Payi et al., 2022b).

Las instituciones educativas en estos contextos se enfrentan a retos importantes debido a la presencia de conductas desadaptativas en algunos estudiantes. (Velázquez-Jurado et al., 2019). Estas conductas surgen de una interacción compleja de factores, entre los que se encuentran las disfunciones familiares, las dificultades socioemocionales, los elementos propios de la cultura viva de las comunidades rurales andinas y las limitaciones en las estrategias de prevención y manejo de conflictos (Richaud & Mesurado, 2016). La identificación temprana de emociones negativas, como la tristeza y la angustia, resulta fundamental para prevenir tanto el deterioro del rendimiento académico como posibles problemas de salud mental. Esto evidencia la necesidad de implementar programas integrales que atiendan de manera holística las necesidades emocionales de los estudiantes, involucrando de manera coordinada a la familia, la escuela y la comunidad (Ruales Jurado et al., 2022a).

La investigación se centra en responder la siguiente interrogante: ¿Qué algoritmo de clasificación de aprendizaje automático es el más efectivo para identificar automáticamente las emociones en los textos escritos por estudiantes de secundaria rural en Puno? Esta cuestión resulta relevante porque, aunque se dispone de diversos algoritmos de clasificación como KNN, Random Forest, SVM y GBM, no existe un consenso definido respecto a cuál de ellos proporciona el mejor equilibrio entre precisión, capacidad de generalización y facilidad de implementación, particularmente en contextos educativos que operan con recursos tecnológicos limitados (L. Alzubaidi et al., 2021).

Elegir el algoritmo adecuado no solo implica mirar métricas de efectividad como la precisión, el recall, el F1-score y el AUC (Mehta et al., 2019). También es importante tener en cuenta cuán interpretables son los resultados y si el algoritmo puede funcionar en tiempo real con recursos computacionales limitados. Los algoritmos tradicionales de aprendizaje automático son especialmente útiles en situaciones donde hay pocos datos y requieren menos potencia de cálculo que los modelos más complejos de deep learning (Janiesch et al., 2021). Esto los convierte en una opción para entornos educativos rurales, donde los recursos tecnológicos pueden ser bastante limitados.

Se plantea la hipótesis de que existe un algoritmo de clasificación que presenta un desempeño significativamente superior a los demás en la detección de emociones a partir de los textos expresados por estudiantes de instituciones de educación secundaria rural de la región Puno, facilitando la definición de perfiles estudiantiles diferenciados. En ese sentido, el objetivo del estudio es identificar el algoritmo de clasificación más adecuado para detectar emociones en los textos que comúnmente se expresan en las instituciones de educación secundaria rural de Puno, con el fin de seleccionar un modelo que pueda

implementarse como módulo base de un sistema de monitoreo emocional educativo, aportando evidencia empírica a la inteligencia artificial aplicada a la educación y una base metodológica orientada al fortalecimiento del bienestar emocional y el rendimiento académico en contextos rurales.

2. Revision de literatura

2.1. Las emociones y la educación

Definir las emociones es un verdadero desafío conceptual, ya que son tan complejas y multidimensionales. Involucran una mezcla de procesos neurobiológicos, fisiológicos, cognitivos y socioculturales. Desde un enfoque más moderno, podemos ver las emociones como sistemas adaptativos intrincados que ayudan a las personas a interpretar su entorno, regular su comportamiento y tomar decisiones basadas en estímulos tanto internos como externos (Ekman, 1992). En este sentido, sentir significa que la persona se involucra activamente con su entorno, donde la emoción juega un papel crucial en la regulación y adaptación a las exigencias del contexto educativo y social (Pennebaker, 2004).

La emoción y la educación están interrelacionadas, ya que las emociones tienen un impacto significativo en el proceso de aprendizaje y en el entorno educativo (Gao, 2022). La investigación científica ha demostrado que las emociones afectan aspectos fundamentales como la motivación, la atención y la memoria, los cuales son esenciales para un aprendizaje efectivo. Según John D. Mayer, las emociones juegan un papel crucial en la manera en que los estudiantes procesan la información y se involucran en el aula. Además, la capacidad de los estudiantes para regular sus propias emociones influye notablemente en el éxito académico (Mayer, 2001). Además, **Daniel Goleman** sostiene que la inteligencia emocional, que incluye la capacidad para entender y manejar las propias emociones y las de los demás, es esencial para el éxito tanto académico como personal (Goleman, 1995).

¿Qué es una emoción?

El término *emoción* proviene del latín *emotio*, derivado de *motio* (movimiento), lo que remite a la idea de impulso o activación hacia la acción. Esta raíz etimológica, compartida con el concepto de *motivación*, refuerza la concepción de la emoción como un proceso dinámico que orienta la conducta del individuo frente a su entorno (Villegas, 2020). Desde esta perspectiva, las emociones no se limitan a estados subjetivos, sino que constituyen respuestas organizadas del organismo que integran componentes afectivos, cognitivos y conductuales.

Uno de los primeros enfoques científicos sobre la naturaleza de las emociones fue propuesto por Darwin, (1873). Él las vio como mecanismos adaptativos universales que compartimos tanto los humanos como otros animales, y que funcionan de manera independiente del aprendizaje cultural. Esta perspectiva evolutiva sentó las bases para investigaciones posteriores que revelaron la existencia de patrones emocionales reconocibles a través de diferentes culturas. Este enfoque es especialmente importante para los estudios actuales en la detección automática de emociones, ya que respalda la

idea de que es posible identificar regularidades emocionales a partir de manifestaciones observables, como el lenguaje escrito, incluso en contextos socioculturales específicos.

2.2. Modelos de clasificación de emociones

Son modelos teóricos que organizan y analizan las emociones humanas desde diferentes perspectivas. Los modelos empleados para la clasificación de emociones suelen ser “Categorías Emocionales” y “Dimensiones Emocionales” (Canales & Martínez-Barco, 2015). Según Scherer (2000), los modelos dimensionales se centran en los sentimientos subjetivos y se diferencian según el grado de similitud entre dimensiones. En contraste, las categorías emocionales se enfocan en la expresión motora o en patrones de comportamiento. A continuación, se presenta las principales modelos de clasificación de emociones:

Modelo de las Emociones Básicas: Paul Ekman propuso que existen seis emociones básicas universales: alegría, tristeza, ira, miedo, sorpresa y disgusto. Estas emociones son reconocidas a través de expresiones faciales universales (Ekman, 1992). Básicamente consistía en que personas de distintas nacionalidades se reconocen y se identifican de manera particular.

Modelo de las Emociones Primarias: Según Plutchik (1982) menciona que, para determinar cuáles son las emociones primarias y poder etiquetarlas, es necesario entenderlas en un marco evolutivo, aplicable tanto a animales como a humanos. Asimismo, sugiere ocho emociones: Miedo, Ira, Alegría, Tristeza, Confianza, Disgusto, Sorpresa y Anticipación.

2.3. Detección de emociones en texto

La detección de emociones en textos se apoya en técnicas de análisis de sentimientos y en el procesamiento del lenguaje natural (PLN)(Malagi et al., 2023). De manera histórica, esta tarea ha utilizado métodos de análisis léxico-semántico junto con algoritmos de aprendizaje automático para identificar y comprender las emociones que se manifiestan a través de la escritura(Pang & Lee, 2008). Las herramientas como los lexicones emocionales y el análisis semántico han hecho posible vincular palabras y expresiones con categorías emocionales específicas. (Mohammad & Turney, 2013).

En los últimos años, la detección de emociones en textos ha evolucionado gracias a modelos de aprendizaje automático y redes neuronales. Estas herramientas son capaces de captar el contexto y las relaciones semánticas del lenguaje de una manera mucho más precisa. Han demostrado ser especialmente útiles en entornos educativos digitales, donde los estudiantes comparten sus emociones a través de comentarios, mensajes o publicaciones en plataformas virtuales.

2.4. Algoritmos de clasificación

Estos son la base de los sistemas de inteligencia artificial, ya que permiten a las máquinas aprender de la experiencia (Oviedo et al., 2021). Los algoritmos de clasificación se utilizan en casos en los que el resultado es un conjunto infinito de resultados (Cruz Guerrero et al., 2017). Actualmente se utilizan diversas técnicas de aprendizaje automático para problemas de clasificación. Entre ellas, encontramos:

1. El algoritmo k-Nearest Neighbors (k-NN o k-vecinos más próximos) es un método de Machine Learning simple. En clasificación, asigna una etiqueta de clase a un punto de datos basándose en las etiquetas de clase de los k vecinos más cercanos en el conjunto de entrenamiento. Los vecinos se seleccionan según la distancia euclidiana u otra medida de distancia, y el valor de k se especifica previamente (Cunningham & Delany, 2021).
2. Random Forest es un algoritmo de aprendizaje supervisado que se utiliza tanto para clasificación y regresión (Dayananda et al., 2023a). Se basa en la creación de múltiples árboles de decisión durante el entrenamiento y realiza predicciones a partir de la votación o el promedio de las predicciones de todos los árboles individuales. Este enfoque ayuda a mejorar la precisión y a reducir el riesgo de sobreajuste (Schonlau & Zou, 2020).
3. Support Vector Machines (SVM) es un algoritmo de aprendizaje supervisado utilizado principalmente para problemas de clasificación, aunque también se adapta para regresión. SVM busca encontrar el hiperplano óptimo que separa las diferentes clases en el espacio de características, maximizando el margen entre las clases más cercanas (Breerton & Lloyd, 2010).
4. Gradient Boosting Machines (GBM) es un algoritmo de aprendizaje supervisado utilizado para problemas de clasificación y regresión. Se basa en el principio del “boosting”, que combina múltiples modelos débiles (como árboles de decisión) para crear un modelo fuerte (Biau et al., 2019). GBM ajusta los árboles de decisión de manera secuencial, corrigiendo los errores de los árboles anteriores.

2.5. Evaluación de los clasificadores

La evaluación de clasificadores es el proceso mediante el cual se mide el rendimiento de un modelo de clasificación, utiliza diversas métricas que permiten cuantificar su capacidad para predecir correctamente las categorías de datos no vistos. Este proceso es crucial para garantizar que el modelo sea robusto, generalice bien a nuevos datos y cumpla con los requisitos del problema que se está abordando.

1. **Matriz de confusión:** La matriz de confusión permite visualizar el desempeño de un algoritmo utilizado en aprendizaje supervisado. Las columnas representan el número de predicciones para cada clase, mientras que cada fila representa las instancias de la clase real.
2. **Exactitud (Accuracy):** Esta métrica indica el porcentaje de predicciones correctas respecto al total de predicciones realizadas. Es una medida general que proporciona una visión rápida del rendimiento del modelo (Friedman, 2001).

$$Exactitud = \frac{VP + VP + VP}{VP + VP + VP + FP + FP + FP + FN + FN + FN}$$

3. **Precisión (Precision):** La precisión se refiere a la proporción de verdaderos positivos entre el total de predicciones positivas realizadas. Es crucial en contextos donde es importante minimizar los falsos positivos (Pang & Lee, 2008).

$$Precision_{A,F,T} = \frac{VP}{VP + FP}$$

4. **Recall (Sensibilidad o Tasa de Verdaderos Positivos):** El recall indica la capacidad del modelo para identificar correctamente las emociones verdaderas. Un alto valor de recall es esencial en escenarios donde la detección de emociones es crítica, minimizando los falsos negativos (Bishop, 2006).

$$Recall_{A,F,T} = \frac{VP}{VP + FN}$$

5. **F1-Score:** Esta métrica combina precisión y recall en un solo valor, proporcionando un equilibrio entre ambas. Es particularmente útil cuando se busca un compromiso entre la exactitud y la exhaustividad (Goodfellow et al., 2016).

$$F1-Score_{A,F,T} = 2 * \frac{Precision * Recall}{Precision + Recall}$$

6. **AUC (Área bajo la curva ROC):** El AUC proporciona una medida del rendimiento del modelo en función de la tasa de verdaderos positivos frente a la tasa de falsos positivos. Un AUC cercano a 1 indica un modelo altamente efectivo, mientras que un AUC de 0.5 sugiere un rendimiento aleatorio (Hanley & McNeil, 1982).

3. Metodología

El estudio se llevó a cabo con un diseño de investigación no experimental, de tipo transversal y con un enfoque cuantitativo. Su objetivo fue evaluar de manera comparativa el rendimiento de varios algoritmos clásicos de aprendizaje automático en la detección de emociones a partir de textos escritos por estudiantes de educación secundaria en áreas rurales (Sampieri, 2014).

Desde una perspectiva computacional, el experimento se llevó a cabo en Google Colab, utilizando Python y algunas bibliotecas especializadas como scikit-learn, pandas y numpy. Esto no solo aseguró que los experimentos fueran reproducibles, sino que también facilitó el acceso a recursos en la nube y mantuvo la consistencia en los resultados. El proceso metodológico se dividió en cuatro etapas: recolección de datos, preprocesamiento del texto, entrenamiento de modelos y evaluación del rendimiento. El proceso se dividió en cuatro etapas:

3.1. Recolección de datos y muestra

La población objetivo estuvo compuesta por estudiantes de secundaria de escuelas rurales en la región de Puno, Perú, que se encuentra a más de 4,000 metros sobre el nivel

del mar. Este entorno geográfico y sociocultural presenta desafíos únicos que afectan el bienestar emocional de los estudiantes.

La muestra fue seleccionada mediante un muestreo no probabilístico por conveniencia y estuvo conformada por 1 150 textos escritos recolectados a lo largo del año académico. Dichos textos fueron producidos por estudiantes que participaron de manera voluntaria en el estudio. Como criterios de inclusión se consideraron: estar matriculados en educación secundaria, pertenecer a instituciones educativas de contexto rural y presentar respuestas textuales completas y legibles.

Se excluyeron aquellos textos incompletos, irrelevantes o que no presentaban un contenido emocional claramente identificable.

Para la recolección de datos se diseñó una encuesta de autoevaluación emocional, mediante la cual se solicitó a los estudiantes que describieran libremente sus estados emocionales frente a situaciones escolares cotidianas. Las emociones analizadas fueron tristeza, angustia y felicidad, seleccionadas debido a su alta prevalencia en contextos educativos y a su relevancia en la literatura científica sobre bienestar emocional en adolescentes. Se observa en la Tabla 1.

Emoción	Características	Palabras o Frases representativas	Textos escritos (%)	Textos escritos(n)
<i>Tristeza</i>	Sensación de pérdida, desánimo, melancolía.	“Me siento vacío”, “Estoy muy desilusionado”, “No tengo ganas de nada.”	24.43	281
<i>Angustia</i>	Ansiedad, tensión, preocupación intensa	“Siento un nudo en el estómago”, “No puedo dejar de pensar en eso”, “Estoy abrumado.”	44.43	511
<i>Felicidad</i>	Alegría, satisfacción, bienestar emocional.	“Estoy muy contento”, “Me siento pleno”, “Todo me parece maravilloso.”	31.13	358
Total			100 %	1150

Tabla 1 – Emociones expresadas por estudiantes en textos escritos

Dado que el estudio incluye datos de menores, se aplicaron principios éticos fundamentales. La participación fue completamente voluntaria, los textos se anonimizaron antes del análisis y no se recogió información personal identificable. Los datos se usaron únicamente con fines académicos y de investigación, respetando las normas de privacidad y protección de datos, de acuerdo con las recomendaciones éticas para investigaciones educativas que utilizan inteligencia artificial.

3.2. Preprocesamiento de texto

El preprocesamiento es una etapa fundamental en las tareas de detección de emociones en texto, ya que tiene un impacto directo en el rendimiento de los modelos de clasificación. En este estudio, se llevaron a cabo los siguientes pasos estandarizados de procesamiento de lenguaje natural:

- Cambia todas las letras del texto a minúsculas, para evitar duplicidad semántica.
- Elimina dígitos y signos de puntuación
- Elimina caracteres como comas, puntos, signos de interrogación.
- Tokenización, divide los textos en palabras o frases.
- Eliminación de stopwords en español, con el fin de reducir ruido lingüístico.

Posteriormente, los textos fueron transformados en representaciones numéricas mediante técnicas de vectorización TF-IDF, ampliamente utilizadas en tareas de clasificación textual por su capacidad para ponderar términos relevantes en función de su frecuencia e importancia contextual.

3.3. Entrenamiento de algoritmos de clasificación

El conjunto de datos que se preprocesó se dividió en dos partes: un 80 % se destinó al entrenamiento y un 20 % a la prueba, utilizando la función `train_test_split` de la biblioteca `scikit-learn`. Esta estrategia es útil porque permite evaluar cómo se desempeñan los modelos con datos que no han visto durante el entrenamiento, lo que ayuda a disminuir el riesgo de sobreajuste.

Se entrenaron y compararon cuatro algoritmos clásicos de aprendizaje supervisado:

- k-Nearest Neighbors (KNN)
- Random Forest
- Support Vector Machines (SVM)
- Gradient Boosting Machines (GBM).

Cada modelo fue entrenado con el mismo conjunto de datos y las tres clases emocionales: tristeza, angustia y felicidad. Los hiperparámetros se ajustaron a través de validación cruzada, con el fin de optimizar el rendimiento de cada algoritmo y garantizar una comparación justa entre ellos.

3.4. Evaluación de modelos

El rendimiento de los modelos se evaluó utilizando el conjunto de prueba, mediante métricas estándar propias de la clasificación multiclase, tales como:

- Exactitud (*accuracy*)
- Precisión (*precision*)
- Exhaustividad (*recall*)
- F1-score
- Área bajo la curva ROC (AUC)

Además, se crearon matrices de confusión y reportes detallados de clasificación utilizando la función `classification_report` de `scikit-learn`. Esto nos permitió examinar cómo se comportaba cada algoritmo, tanto en términos generales como por cada clase emocional.

Esta evaluación completa ayudó a identificar cuál modelo tenía el mejor rendimiento y a entender las dificultades que surgen al clasificar automáticamente emociones a partir de textos breves en contextos educativos rurales.

4. Resultados y discusion

4.1. Resultados

4.1.1. Evaluación de algoritmos de clasificación según las métricas

En la Figura 1 se presenta la evaluación de los algoritmos de clasificación mediante una matriz de confusión multiclase, a partir de métricas como accuracy, precision, recall y F1-score. Tras el entrenamiento de KNN, Random Forest, SVM y GBM con datos de estudiantes rurales de Puno, el modelo Random Forest mostró el mejor desempeño, destacando especialmente en la detección de la emoción de angustia, seguido de felicidad y tristeza.

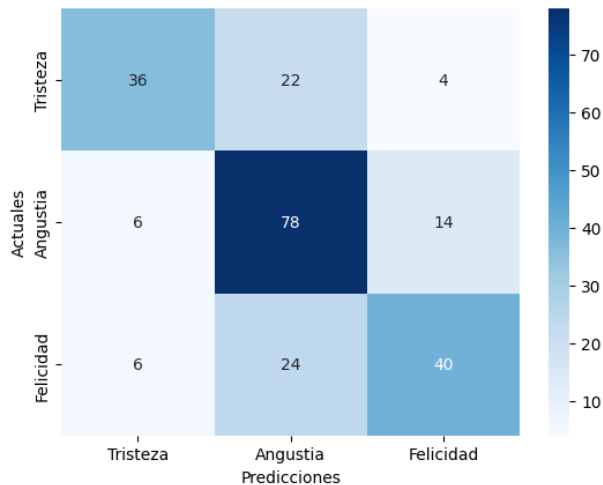


Figura 1 – Matriz de Confusión multi-clase para tres (03) emociones del Modelo Random Forest para la Detección de Emociones.

Algoritmos	Accuracy	Precision	Recall	F1-Score	AUC
KNN	66.9565%	67.4368%	66.9565%	66.8495%	82.2629%
Random Forest	72.6087%	73.8145%	72.6087%	72.5735%	88.6749%
SVM	71.3043%	72.4236%	71.3043%	70.8757%	84.0898%
GBM	66.9565%	68.0091%	66.9565%	66.6073%	85.9492%

Tabla 2 – Rendimiento de Modelos: Exactitud, Precisión, Recall, F1-Score y AUC

El algoritmo Random Forest presenta el mejor desempeño en la detección de emociones en textos estudiantiles, alcanzando un Accuracy de 72.61%, Precision de 73.81% y un AUC de 88.67%. Su equilibrio entre precisión y recall lo posiciona como la opción más

robusta frente a SVM, KNN y GBM, recomendándose su optimización y validación en conjuntos de datos más amplios.

En la Figura 2 se visualiza el desempeño de diversos algoritmos de clasificación (KNN, Random Forest, SVM, GBM), utilizando métricas como accuracy, precisión, recall, F1-score y AUC. En consecuencia, el modelo de Random Forest demostró el mejor rendimiento en las métricas claves como el F1-score y AUC.

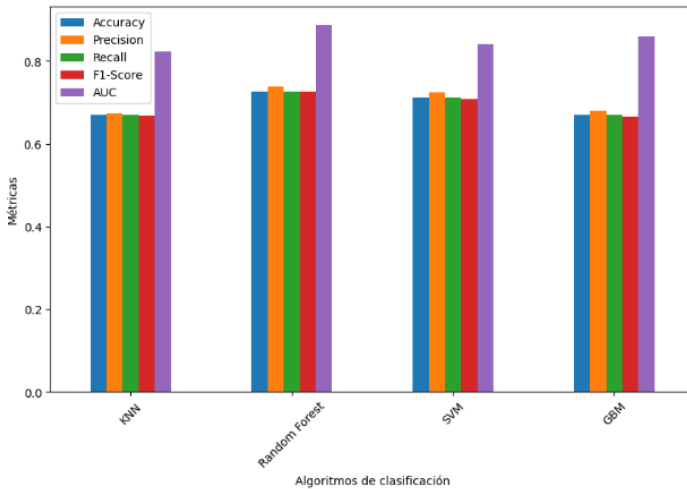


Figura 2 – Matriz de confusión para la clasificación de las emociones: KNN, Random Forest, SMV, GBM

4.1.2. Reconocimiento de emociones en texto por categoría

En la Tabla 3 se muestran las métricas de desempeño del modelo (precision, recall, F1-score y support). Los resultados indican que la clase **tristeza** presenta la mayor precisión (83%), lo que sugiere que el modelo identifica de manera adecuada la mayoría de los textos asociados con esta emoción. Por otro lado, la clase **angustia** sobresale por alcanzar un recall del 80% y un F1-score del 75%, lo que refleja una buena capacidad para detectar correctamente los casos positivos.

Emociones	Precision	Recall	F1-Score	support
Tristeza	83%	65%	73%	62
Angustia	70%	80%	75%	98
Felicidad	68%	69%	68%	70

Tabla 3 – Resultados de clasificación de emociones

De forma general, el algoritmo tiene un mejor desempeño al identificar emociones negativas, como la tristeza y la angustia, en comparación con emociones positivas

como la felicidad. Este comportamiento podría estar relacionado con el contexto de los estudiantes de educación secundaria en zonas rurales, donde aspectos como las limitaciones educativas, la falta de apoyo psicológico y el aislamiento social influyen de manera significativa en su estado emocional y, en consecuencia, en su rendimiento académico.

4.2. Discusion

Este estudio ha demostrado que el uso de algoritmos de clasificación como KNN, Random Forest, SVM y GBM resultan apropiados para el reconocimiento automático de emociones en textos producidos por estudiantes de educación secundaria del sector rural. Estos hallazgos coinciden con investigaciones previas que destacan la efectividad del aprendizaje automático en tareas de clasificación textual (Dayananda et al., 2023), particularmente cuando se trabaja con datos limitados y recursos tecnológicos restringidos, condiciones características de los entornos educativos rurales.

El análisis de sentimientos y emociones permite identificar tanto emociones positivas como negativas, aunque con diferentes niveles de efectividad. La identificación precisa de emociones, especialmente emociones negativas como la tristeza y la angustia, resulta esencial para comprender el estado emocional de los estudiantes y desarrollar estrategias de intervención que promuevan su bienestar (Ruales Jurado et al., 2022b). Esto subraya la importancia de aplicar modelos de clasificación adaptados a entornos educativos rurales, contribuyendo así a un aprendizaje más inclusivo y emocionalmente consciente, tal como sugieren (Sagredo-Lillo et al., 2024) al enfatizar la necesidad de considerar las particularidades contextuales en las intervenciones educativas.

Entre los algoritmos evaluados, Random Forest se destacó por obtener los mejores resultados, presentando un balance óptimo en términos de exactitud (72.61%), precisión (73.81%), recall (72.61%), F1-score (72.57%) y AUC (88.67%). Este hallazgo es consistente con estudios previos que han demostrado la superioridad de Random Forest en tareas de clasificación complejas debido a su capacidad para manejar datos multidimensionales y reducir el sobreajuste (Schonlau & Zou, 2020). La robustez de este algoritmo sugiere que es el más adecuado para la detección de emociones en textos dentro de contextos educativos rurales específicos, donde factores culturales y sociolingüísticos particulares influyen en las expresiones emocionales. (Berné Manero et al., 2013; Cordero García et al., 2019b)

Los resultados obtenidos revelan que las emociones negativas, particularmente la angustia (recall del 80%), fueron detectadas con mayor efectividad que las emociones positivas como la felicidad (F1-Score del 68%). Este patrón puede estar relacionado con la mayor intensidad expresiva de las emociones negativas en el lenguaje escrito, como han señalado Canales y Martínez-Barco (2015), así como con el contexto socioemocional de los estudiantes rurales de Puno, quienes enfrentan desafíos particulares relacionados con el aislamiento geográfico, la limitada disponibilidad de apoyo psicológico y las condiciones socioeconómicas adversas (Zela Payi et al., 2022a).

La detección temprana de emociones negativas en estudiantes rurales adquiere especial relevancia considerando que la región de Puno presenta características únicas del contexto andino, donde factores de altitud (más de 3,800 m.s.n.m.), culturales y de

aislamiento geográfico influyen significativamente en las manifestaciones emocionales (Vilca, 2016). La implementación de sistemas automatizados de monitoreo emocional puede compensar parcialmente la escasez de recursos de apoyo psicológico en estas comunidades, permitiendo identificar estudiantes en riesgo de manera oportuna.

5. Conclusion

Este estudio demuestra que algoritmos de clasificación como KNN, Random Forest, SVM y GBM pueden convertirse en aliados valiosos para comprender las emociones de estudiantes de educación secundaria en contextos rurales. A través del análisis de sentimientos y emociones, fue posible reconocer tanto estados emocionales positivos como negativos, aunque con distintos niveles de efectividad. En particular, la identificación de emociones negativas —como la tristeza y la angustia— cobra especial relevancia, ya que permite entender mejor el estado emocional de los estudiantes y orientar acciones de apoyo que contribuyan a su bienestar integral.

Entre los modelos evaluados, Random Forest destacó por su mejor desempeño, alcanzando una exactitud del 72.61%, una precisión del 73.81%, un recall del 72.61%, un F1-score del 72.57% y un AUC del 88.67%. Estos resultados indican que este algoritmo es especialmente eficaz para detectar emociones a partir de textos en entornos educativos rurales, donde comprender la realidad emocional de los estudiantes resulta clave.

Sin embargo, el estudio presenta algunas limitaciones que deben considerarse. La muestra analizada proviene de un contexto geográfico específico, se enfocó únicamente en tres emociones y utilizó una sola plataforma social como fuente de datos. Por ello, los hallazgos deben interpretarse con cautela y no pueden generalizarse de manera automática a otros escenarios educativos o regiones.

De cara al futuro, se sugiere ampliar el tamaño y la diversidad de la muestra, incorporar un mayor número de categorías emocionales y comparar el desempeño de los algoritmos en distintas plataformas digitales. La aplicación de herramientas de inteligencia artificial en contextos educativos rurales ofrece un gran potencial para detectar de manera temprana las necesidades emocionales de los estudiantes, mejorar el clima escolar y favorecer su rendimiento académico, promoviendo así un aprendizaje más inclusivo y sensible a la dimensión socioemocional

Referencias

- Apaza-Tarqui, A., & Huanco-Ramos, F. (2025). Models of automatic recognition of collaborative emotions in rural secondary education institutions in Puno, 2024. *Journal of International Crisis and Risk Communication Research*, 3306–3325. <https://doi.org/10.63278/JICRCR.VI.2615>
- Canales, L., & Martínez-Barco, P. (2015). *Emotion Detection from text: A Survey*. <https://doi.org/10.3115/v1/w14-6905>

- Cordero García, S. P., Chinome Alba, C. P., & Garzón Bautista, A. del P. (2019). Emociones y habilidades comunicativas en la convivencia escolar en la IE Rural del Sur de Tunja. *Educación y Ciencia*, 22. <https://doi.org/10.19053/0120-7105.eyc.2019.22.e10047>
- Cruz Guerrero, R., Alonso Lavernia, Ma. de los Á., Franco Arcega, A., & Simón Marmolejo, I. (2017). Estudio del comportamiento de algoritmos de clasificación según la naturaleza de los datos. *Revista de Tecnología Informática*, 1(2), 9-18.
- Darwin, C. (1873). The Expression of the Emotions in Man and Animals. *The Journal of the Anthropological Institute of Great Britain and Ireland*, 2(2), 444-446. <https://doi.org/10.2307/2841467>
- Ekman, P. (1992). Facial expressions of emotion: an old controversy and new findings. *Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences*, 335(1273), 63-69. <https://doi.org/10.1098/RSTB.1992.0008>
- Huanco-Ramos, F., & Apaza-Tarqui, A. (2024). Covid 19 identification model using Deep Learning techniques from thorax of lung X-ray images. *Proceedings of the LACCEI International Multi-Conference for Engineering, Education and Technology*. <https://doi.org/10.18687/LACCEI2024.1.1.1491>
- López, M. B., Montes, A. J. H., Ramírez, R. V., Hernández, G. A., Cabada, R. Z., & Estrada, M. L. B. (2016). EmoRemSys: Sistema de recomendación de recursos educativos basado en detección de emociones. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, (17), 80-95. <https://doi.org/10.17013/risti.17.80-95>
- Mohammad, S. M., & Turney, P. D. (2013). Crowdsourcing a word-emotion association lexicon. *Computational Intelligence*, 29(3), 436-465. <https://doi.org/10.1111/j.1467-8640.2012.00460.x>
- Oviedo, B., Jorge, B., Fajardo, G., & Gómez-Gómez, J. (2021). Utilización de algoritmos de clasificación para la predicción de los delitos que afectan la seguridad ciudadana. *Centro Sur*.
- Pang, B., & Lee, L. (2008). Opinion mining and sentiment analysis. *Foundations and Trends in Information Retrieval*, 2(1-2), 1-135. <https://doi.org/10.1561/15000000011>
- Patiño, M. M., Pérez, E. C., & Sanchez, S. S. (2024). Detección temprana de cáncer de mama: clasificación de mastografías mediante un modelo de aprendizaje profundo. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (55), 21-37. <https://doi.org/10.17013/risti.55.21-37>
- Plutchik, R. (1982). A psychoevolutionary theory of emotions. *Social Science Information*, 21(4-5), 529-553. <https://doi.org/10.1177/053901882021004003>
- Richaud, M. C., & Mesurado, B. (2016). Las emociones positivas y la empatía como promotores de las conductas prosociales e inhibidores de las conductas agresivas. *Acción Psicológica*, 13(2), 31-42. <https://doi.org/10.5944/ap.13.2.17808>

- Ruales Jurado, R. E., Lucero Revelo, S. E., & Gómez Rosero, Á. H. (2022). La autorregulación emocional desde una perspectiva educativa. *Fedumar Pedagogía y Educación*, 9(1), 64–73. <https://doi.org/10.31948/rev.fedumar9-1.art-4>
- Sagredo-Lillo, E., Zapata, J., & Salamanca-Garay, I. (2024). Inclusión de estudiantes con altas capacidades en la escuela: centrándose en el aprendizaje de la matemática, la docencia universitaria y el trabajo colaborativo tanto en entornos presenciales como virtuales. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (56), 21-34. <https://doi.org/10.17013/risti.56.21-34>
- Sampieri, undefined H. (2014). *Metodología de la investigación*. 6 (metodologia de la investigacion). <https://www.mendeley.com/catalogue/41b023b1-ca08-3166-a338-3b2d45e3b313/>
- Scherer, K. R. (2000). Psychological Models of Emotion. In *The Neuropsychology of Emotion*.
- Segura Zúñiga, L. (2022). Inteligencia artificial en las organizaciones. *InvestigaTEC*.
- Velázquez-Jurado, H., Niño-Tamayo, D., Castro, C. G., Flores Torres, A., & Briseño González, O. (2019). Identification of emotional schemes and their association with symptoms of anxiety and depression in Mexican adults. *Revista Latinoamericana de Medicina Conductual/Latin American Journal of Behavioral Medicine*, 9(2).
- Vilca, A. (2016). Clima socio familiar y habilidades sociales de los estudiantes de la institución educativa secundaria San Andrés del distrito de Atuncolla - Puno, 2015. *Universidad Nacional Del Altiplano*.
- Zela Payí, N. O., Chambi Condori, N., Ticona Arapa, H. C., & Barrionuevo Valero, J. F. (2022b). Nivel de inteligencia emocional en niños y niñas del II ciclo de instituciones educativas de la zona rural durante la pandemia-Puno 2021. *Horizontes. Revista de Investigación En Ciencias de La Educación*, 6(22), 35–47. <https://doi.org/10.33996/revistahorizontes.v6i22.312>
- Zhou, Z. H. (2012). Ensemble methods: Foundations and algorithms. In *Ensemble Methods: Foundations and Algorithms*. <https://doi.org/10.1201/b12207>

Madurez en ciberseguridad y resiliencia digital en PYMEs iberoamericanas: diagnóstico y desafíos estratégicos

Hernán Cornejo

mghcornejo@gmail.com

¹ Universidad Tecnológica Nacional, Zeballos 1341, 2000, Rosario, Argentina.

DOI: [10.17013/risti.60.127-141](https://doi.org/10.17013/risti.60.127-141)

Resumen: Este artículo analiza el nivel de madurez en ciberseguridad y resiliencia digital de las pequeñas y medianas empresas (PYMEs) iberoamericanas, un sector especialmente vulnerable ante el aumento de ciberamenazas globales. A partir de un enfoque exploratorio-descriptivo, se propone un modelo de diagnóstico basado en el marco NIST Cybersecurity Framework, complementado con indicadores de gestión organizativa y cultura de seguridad. Los resultados evidencian brechas significativas en la adopción de políticas formales, formación del personal y continuidad operativa ante incidentes. Asimismo, se identifican factores determinantes que influyen en la capacidad de respuesta y recuperación de las organizaciones. El estudio aporta un conjunto de lineamientos estratégicos adaptados al contexto regional, orientados a fortalecer la resiliencia digital con recursos limitados. Se concluye que la madurez en ciberseguridad constituye un componente esencial para la sostenibilidad tecnológica y competitiva de las PYMEs en Iberoamérica.

Palabras-clave: Ciberseguridad; Resiliencia digital; Madurez tecnológica; Pequeñas y medianas empresas; Gestión de la información.

Cybersecurity Maturity and Digital Resilience in Ibero-American SMEs: Diagnosis and strategies challenges

Abstract: This article analyzes the level of cybersecurity maturity and digital resilience of Ibero-American small and medium-sized enterprises (SMEs), a sector particularly vulnerable to the rise of global cyberthreats. Using an exploratory-descriptive approach, we propose a diagnostic model based on the NIST Cybersecurity Framework, complemented by organizational management and security culture indicators. The results reveal significant gaps in the adoption of formal policies, staff training, and operational continuity in the event of incidents. Furthermore, determining factors that influence organizations' response and recovery capacity are identified. The study provides a set of strategic guidelines adapted to the regional context, aimed at strengthening digital resilience with limited resources. It concludes that cybersecurity maturity is an essential component for the technological and competitive sustainability of SMEs in Ibero-America.

Keywords: Cybersecurity; Digital Resilience; Technological Maturity; Small and Medium-Sized Enterprises; Information Management.

1. Introducción

En los últimos diez años, la rápida digitalización ha transformado la forma en que las pequeñas y medianas empresas (PYMEs) operan, producen y compiten. Las herramientas digitales han mejorado la eficiencia y el acceso a los mercados globales, pero también han incrementado la exposición a amenazas cibernéticas. En el entorno digital actual, las PYMEs de América Latina y España enfrentan riesgos cada vez más complejos, lo que convierte a la ciberseguridad en una cuestión estratégica para los negocios y no solo en un problema técnico. La Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) informaron en 2023 que el 80 % de las empresas latinoamericanas sufrió al menos un ciberataque en los últimos dos años, y que más del 60 % de los casos afectó a PYMEs (OEA & BID, 2023).

A diferencia de las grandes empresas, que cuentan con sistemas sólidos de ciberseguridad, las PYMEs suelen operar con presupuestos reducidos, capacidades técnicas limitadas y escaso conocimiento de las normativas en materia de seguridad digital. Esta situación resulta especialmente problemática si se considera que las PYMEs representan más del 95 % de las empresas en América Latina y España y generan aproximadamente el 67 % del empleo total (CEPAL, 2022). Diversos estudios señalan que el 58 % de las PYMEs latinoamericanas no dispone de planes formales de ciberseguridad y que solo el 25 % cuenta con capacidades de recuperación ante ataques, lo que incrementa el riesgo operativo y debilita la confianza de clientes y socios comerciales (Kaspersky, 2024).

La ciberseguridad comprende el conjunto de acciones, herramientas y normativas destinadas a proteger los sistemas de información y los activos digitales frente a ataques (NIST, 2022). En la actualidad, este concepto trasciende el ámbito puramente tecnológico e incorpora dimensiones organizacionales, culturales y humanas. De forma complementaria, la resiliencia digital se refiere a la capacidad de una organización para resistir, adaptarse y recuperarse de incidentes cibernéticos, garantizando la continuidad de sus operaciones (ENISA, 2023). Ambas dimensiones confluyen en el concepto de madurez en ciberseguridad, entendido como el grado en que las prácticas de seguridad están formalizadas, supervisadas y sujetas a procesos de mejora continua (Bada et al., 2021).

Para hacer frente al aumento de las amenazas digitales, se han desarrollado diversos modelos de madurez. El NIST Cybersecurity Framework (NIST CSF) es uno de los más utilizados y se estructura en las funciones de identificar, proteger, detectar, responder y recuperar. Otros enfoques, como el Cybersecurity Capability Maturity Model (C2M2) y la norma ISO/IEC 27001:2022, persiguen objetivos similares. No obstante, estos modelos fueron concebidos principalmente para organizaciones con elevados recursos tecnológicos y financieros, lo que limita su adecuación a las PYMEs de América Latina y España (Silva & Costa, 2023).

Los desafíos de la ciberseguridad en la región se ven agravados por deficiencias de infraestructura, debilidades en la gobernanza digital, escasa cooperación entre los sectores público y privado y una limitada disponibilidad de capital humano especializado.

La Estrategia Iberoamericana de Transformación Digital 2022–2025 reconoce que estas carencias reducen la competitividad regional y aumentan la dependencia tecnológica externa (SEGIB, 2022). Asimismo, la falta de una cultura preventiva y la percepción de la ciberseguridad como una prioridad secundaria por parte de la gestión empresarial constituyen obstáculos relevantes para la implementación de políticas efectivas (Gutiérrez & Hernández, 2021; Molina et al., 2023).

Desde una perspectiva operativa, las PYMEs tienden a priorizar la productividad de corto plazo, postergando las inversiones en ciberseguridad ante la dificultad de estimar sus beneficios. Como resultado, muchas operan en lo que el *ENISA Threat Landscape 2024* denomina una “zona de riesgo latente”, caracterizada por niveles de protección insuficientes, ausencia de planes de contingencia, monitoreo limitado y escasa capacitación del personal. Entre las amenazas más frecuentes se encuentran los ataques de ransomware, el phishing avanzado, la filtración de datos, la explotación de vulnerabilidades en software desactualizado y los riesgos asociados a la cadena de suministro digital (ENISA, 2024).

Si bien la literatura reciente ha comenzado a vincular la ciberseguridad con el aprendizaje organizacional y la resiliencia estratégica (Teece, 2018; Radanliev et al., 2022), la investigación empírica sobre la madurez en ciberseguridad de las PYMEs en América Latina y España sigue siendo limitada. La mayoría de los estudios se concentra en Europa, Norteamérica o en grandes organizaciones, dejando a las PYMEs subrepresentadas (Hernández et al., 2021). Esta brecha limita el diseño de estrategias contextualizadas y debilita la efectividad de las políticas públicas.

Este estudio aborda dicha laguna mediante un análisis de la madurez en ciberseguridad y la resiliencia digital en PYMEs de América Latina y España. A partir de un enfoque metodológico mixto, basado en el NIST Cybersecurity Framework adaptado a las PYMEs, se analizan las prácticas de seguridad, las capacidades de respuesta ante incidentes y la cultura organizacional en relación con el riesgo digital.

El objetivo de la investigación es evaluar el nivel de madurez en ciberseguridad de las PYMEs latinoamericanas y españolas, identificar brechas clave y proponer lineamientos adecuados al contexto regional. En particular, se busca responder a las siguientes preguntas: (1) ¿Cuál es el nivel actual de preparación en ciberseguridad de las PYMEs? (2) ¿Qué factores internos y externos explican las debilidades en resiliencia digital? y (3) ¿Qué acciones pueden fortalecer la capacidad de respuesta y recuperación de las PYMEs?

El artículo se organiza de la siguiente manera. En primer lugar, se presenta la metodología de investigación y el modelo de madurez utilizado. A continuación, se exponen los resultados del análisis empírico, seguidos de una discusión que los vincula con la literatura reciente. Finalmente, se formulan recomendaciones estratégicas y se reflexiona sobre los desafíos futuros de la ciberseguridad en las PYMEs de América Latina y España.

2. Materiales y métodos

El presente estudio adoptó un enfoque mixto de carácter exploratorio-descriptivo y transversal, con el propósito de diagnosticar los niveles de madurez en ciberseguridad

y resiliencia digital en pequeñas y medianas empresas (PYMEs) de distintos países iberoamericanos. Se combinó el análisis cuantitativo mediante encuestas estructuradas con el análisis cualitativo a partir de entrevistas semiestructuradas, lo que permitió obtener una comprensión integral de las prácticas, vulnerabilidades y estrategias de respuesta adoptadas por las organizaciones ante amenazas digitales.

Este enfoque se seleccionó debido a que la ciberseguridad en las PYMEs es un fenómeno multidimensional, donde interactúan factores tecnológicos, humanos, organizacionales y regulatorios (ENISA, 2023; OEA & BID, 2022). El diseño transversal facilitó captar una fotografía representativa del estado actual de la madurez digital y de los mecanismos de resiliencia implementados en el ecosistema empresarial iberoamericano.

2.1. Diseño de la investigación

El estudio se estructuró en tres fases principales:

- Revisión documental: se realizó una revisión sistemática de literatura reciente (2020–2024) en bases de datos académicas como Scopus, Web of Science, Scielo y Google Scholar. Los términos de búsqueda incluyeron: “maturity model”, “cybersecurity in SMEs”, “digital resilience”, “Ibero-America”, y “risk management”. Esta fase permitió identificar marcos de referencia y estudios previos sobre niveles de madurez cibernética y resiliencia organizacional en PYMEs.
- Aplicación de encuesta estructurada: se diseñó un instrumento basado en el NIST Cybersecurity Framework (CSF) y en el modelo de madurez de la ENISA (2022). El cuestionario evaluó cinco funciones clave —Identify, Protect, Detect, Respond y Recover—, con escalas Likert de 1 a 5 para medir el grado de implementación de controles y prácticas de seguridad.
- Entrevistas cualitativas: se efectuaron entrevistas a 20 responsables de TI y gerentes generales de PYMEs en sectores manufacturero, tecnológico y de servicios de Argentina, Chile, España, México y Colombia. Las entrevistas, realizadas por videoconferencia, exploraron percepciones sobre riesgos, cultura organizacional y obstáculos a la adopción de políticas de ciberseguridad.

2.2. Población y muestra

La población objetivo estuvo conformada por PYMEs iberoamericanas con entre 10 y 250 empleados y operaciones digitales activas (e-commerce, gestión en la nube o servicios basados en TIC). La selección de un muestreo no probabilístico intencional se debió a que el estudio era exploratorio. También hubo dificultades para encontrar marcos muestrales completos y similares de pequeñas y medianas empresas (PYMEs) con capacidades digitales parecidas en Iberoamérica. En estudios diagnósticos y comparativos como este, el muestreo intencional es útil cuando se quiere analizar a fondo organizaciones que tienen riesgos cibernéticos y una gestión tecnológica básica (Patton, 2015; Hair et al., 2022).

El criterio de incluir empresas con al menos cinco años de actividad digital sirvió para confirmar que la madurez observada reflejaba prácticas establecidas y no procesos de digitalización recientes. La distribución por país buscó captar la variabilidad contextual

sin favorecer a ningún país en particular, lo que mejoró la capacidad de comparar el modelo en la región.

2.3. Procedimiento de recolección y análisis de datos

La recolección de datos se llevó a cabo entre abril y julio de 2024. Las encuestas fueron administradas en línea mediante formularios seguros con autenticación de usuario. Los datos cuantitativos se procesaron con SPSS v.28, aplicando análisis descriptivos, índices de madurez ponderados y comparaciones interregionales. El análisis cualitativo se realizó con NVivo 14, codificando las entrevistas en torno a tres categorías: cultura de seguridad, gestión de incidentes y aprendizaje organizacional.

Para evaluar la madurez en ciberseguridad, se aplicó un índice compuesto adaptado del modelo CMMI (Capability Maturity Model Integration), clasificando las empresas en cinco niveles: Inicial, Gestionado, Definido, Cuantitativamente Gestionado y Optimizado. La resiliencia digital se midió según la capacidad de recuperación operativa posterior a incidentes, siguiendo los lineamientos del Digital Operational Resilience Act (DORA, 2022).

Índice de madurez en ciberseguridad

El índice de madurez se creó con un modelo jerárquico de suma ponderada. Cada una de las cinco funciones del NIST CSF (Identificar, Proteger, Detectar, Responder y Recuperar) se midió con elementos específicos, basados en las prácticas recomendadas por NIST y ENISA. Los puntajes se estandarizaron en una escala de 0 a 100 y se sumaron con el mismo peso, ya que no había datos previos que justificaran darles pesos diferentes en las PYMEs iberoamericanas.

El puntaje total de madurez se calculó como el promedio ponderado de las cinco funciones y se ubicó en uno de los cinco niveles del modelo CMMI adaptado, usando puntos de corte teóricos definidos (0–20 Inicial; 21–40 Gestionado; 41–60 Definido; 61–80 Cuantitativamente Gestionado; 81–100). Esto aseguró que el índice fuera transparente, reproducible y consistente.

Además de los análisis descriptivos, se calcularon intervalos de confianza del 95 % para los puntajes promedio de madurez y resiliencia digital por país y sector, para estimar la precisión de los resultados. Se reportaron tamaños del para evaluar la magnitud de las diferencias entre grupos, evitando basarse solo en la estadística.

Se estimaron modelos de regresión multivariada para ver la relación entre la madurez en ciberseguridad (variable dependiente) y factores de la organización como tamaño, sector, país, políticas de seguridad formales y capacitación del personal (variables independientes). Estos modelos ayudaron a controlar factores externos y aportaron datos más sólidos sobre qué determina la madurez digital en PYMEs iberoamericanas.

Modelo de madurez iberoamericano propuesto

El modelo de madurez iberoamericano propuesto es un marco que une estándares internacionales (NIST CSF, ENISA y CMMI) con características de Iberoamérica. Funciona con una progresión secuencial, donde cada nivel de madurez implica

incorporar controles técnicos y desarrollar capacidades organizacionales, culturales y de aprendizaje.

2.4. Consideraciones éticas y validez

El estudio cumplió con los principios éticos de confidencialidad y consentimiento informado. Se garantizó el anonimato de las empresas participantes y se utilizó la información únicamente con fines académicos. Para asegurar la validez y fiabilidad, el cuestionario fue sometido a una prueba piloto en 10 empresas, alcanzando un coeficiente de consistencia interna $\alpha = 0,86$ (alta confiabilidad).

2.5. Limitaciones del estudio

Los resultados deben interpretarse como indicativos de tendencias observadas en PYMEs de los países analizados y no como representativos del conjunto de PYMEs iberoamericanas.

Entre las principales limitaciones se reconoce la disparidad en los niveles de digitalización entre países y sectores, así como la posible autoselección de empresas más sensibilizadas con el tema de ciberseguridad. No obstante, la combinación metodológica y el enfoque comparativo proporcionan una base sólida para la interpretación de resultados y la elaboración de políticas de fortalecimiento digital para el tejido empresarial iberoamericano.

3. Resultados

Los resultados obtenidos permiten caracterizar el estado actual de la madurez en ciberseguridad y resiliencia digital de las PYMEs iberoamericanas, así como identificar los factores que condicionan su desarrollo y las brechas existentes entre países y sectores. En términos generales, los hallazgos muestran que las PYMEs de la región presentan niveles medios o bajos de madurez, con un predominio de enfoques reactivos frente a las amenazas digitales.

3.1. Nivel de madurez en ciberseguridad

A partir del modelo de referencia del NIST Cybersecurity Framework (CSF), se calcularon los niveles promedio de madurez en las cinco funciones clave. La Tabla 1 resume los resultados agregados para los cinco países analizados.

Función NIST	Argentina	Chile	México	Colombia	España	Promedio regional
Identify	2,8	3,0	2,7	2,6	3,4	2,9
Protect	2,6	2,9	2,5	2,4	3,2	2,7
Detect	2,3	2,7	2,2	2,1	3,0	2,5
Respond	2,1	2,5	2,3	2,0	2,8	2,3
Recover	2,4	2,8	2,5	2,2	3,1	2,6

Tabla 1 – Niveles promedio de madurez en ciberseguridad por función y país (escala 1–5)

Los resultados evidencian que España presenta el mayor nivel promedio de madurez (3,1), seguido por Chile (2,8), mientras que Colombia y México registran los niveles más bajos (2,3–2,4). Las funciones más desarrolladas corresponden a Identify y Protect, mientras que Respond y Detect muestran las mayores debilidades, reflejando una tendencia a la reacción tardía ante incidentes más que a la prevención proactiva.

En el análisis por sector, las PYMEs tecnológicas y de servicios financieros alcanzaron los niveles más altos de madurez (promedios de 3,2 y 3,0 respectivamente), en contraste con las empresas manufactureras y de comercio minorista, que no superan el 2,5. Estos datos concuerdan con estudios previos que señalan que las organizaciones más digitalizadas tienden a adoptar mejores prácticas de seguridad (ENISA, 2023; OEA & BID, 2022).

3.2. Factores que influyen en la madurez

El análisis de regresión simple reveló una correlación positiva significativa ($r = 0,67$, $p < 0,01$) entre la madurez cibernética y la existencia de políticas formales de gestión de riesgos digitales. Asimismo, se encontró una asociación moderada ($r = 0,54$, $p < 0,05$) entre el nivel de madurez y la formación del personal en seguridad de la información.

Las entrevistas cualitativas destacaron tres obstáculos principales:

1. Limitaciones presupuestarias, que dificultan la inversión en herramientas y auditorías.
2. Escasa cultura organizacional orientada a la ciberseguridad, percibida como un asunto técnico y no estratégico.
3. Dependencia de proveedores externos sin criterios homogéneos de seguridad.

Un gerente de TI de una PYME chilena señaló: **“La seguridad se atiende cuando ocurre un incidente; antes de eso, no se le asigna prioridad”**. Este patrón se repitió en la mayoría de las entrevistas, reforzando la necesidad de un enfoque sistémico.

3.3. Resiliencia digital y recuperación operativa

En cuanto a resiliencia digital, el 62% de las empresas indicó haber sufrido al menos un incidente de seguridad en los últimos 24 meses. Sin embargo, solo el 27% disponía de un plan formal de continuidad de negocio y un 19% había realizado simulacros de recuperación.

Las organizaciones españolas y chilenas mostraron mayor preparación, con tiempos medios de recuperación (MTTR) inferiores a 24 horas, mientras que en México y Colombia superaron las 48 horas. Estos resultados reflejan una brecha significativa en la capacidad de respuesta y recuperación, lo cual impacta directamente en la sostenibilidad del negocio y la confianza de los clientes (BID, 2023).

3.4. Comparación con estudios previos

Para situar los resultados en un contexto más amplio, la Tabla 2 resume los principales aportes de investigaciones relevantes sobre ciberseguridad en PYMEs publicadas entre 2015 y 2024.

Como se observa, la literatura muestra una evolución gradual desde el reconocimiento de la vulnerabilidad estructural (Cisco, 2015) hasta la incorporación de la resiliencia como pilar estratégico (ENISA, 2023). Este estudio amplía esa línea al ofrecer un diagnóstico empírico comparativo que integra las dimensiones técnicas y culturales de la seguridad digital.

Autor(es)	Año	Alcance	Principales hallazgos	Relevancia para este estudio
Cisco & IDC	2015	Global	Las PYMEs representan el 43% de los objetivos de ciberataques.	Evidencia temprana de vulnerabilidad estructural.
OEA & Symantec	2016	América Latina	Falta de políticas regionales coordinadas en ciberseguridad.	Base para políticas públicas actuales.
ENISA	2018	Europa	Modelos de madurez adaptados al tamaño de las empresas.	Referencia para escalas de medición.
CISA	2020	EE. UU.	Enfoque en resiliencia digital post-pandemia.	Inspiró el componente de recuperación.
OEA & BID	2022	Iberoamérica	Brechas formativas y baja adopción del enfoque preventivo.	Comparación directa con resultados actuales.
ENISA	2023	Europa	Promueve cultura de ciberseguridad como factor clave de resiliencia.	Refuerza la importancia del componente humano.
Torres & Calderón	2024	Chile y Colombia	Niveles medios-bajos de madurez tecnológica en PYMEs.	Corroboración empírica de los hallazgos.

Tabla 2 – Principales estudios sobre ciberseguridad y resiliencia digital en PYMEs (2015–2024)

4. Discusión

Los resultados obtenidos indican que la madurez en ciberseguridad y la resiliencia digital en las PYMEs iberoamericanas siguen siendo dimensiones en construcción, caracterizadas por estrategias fragmentadas y dependientes del contexto económico y regulatorio. Esta situación coincide con tendencias globales descritas en la literatura de la última década, que señalan la creciente brecha entre la sofisticación tecnológica de las amenazas y la capacidad de respuesta de las organizaciones de menor tamaño (ENISA, 2018; OEA & BID, 2022).

4.1. Interpretación general de los hallazgos

La evidencia empírica sugiere que, si bien la digitalización ha avanzado rápidamente en la región, la gestión del riesgo cibernético no ha evolucionado al mismo ritmo. Las funciones del marco NIST mejor valoradas —Identify y Protect— corresponden a acciones reactivas o de cumplimiento mínimo, mientras que las más débiles —

Respond y Recover— demandan una planificación estratégica que pocas empresas han institucionalizado. Este patrón coincide con lo identificado por OEA & Symantec (2016) y Torres & Calderón (2024), quienes advierten que el enfoque predominante en América Latina continúa siendo reactivo y centrado en la corrección posterior al incidente.

Los resultados también sugieren que la madurez cibernética no depende exclusivamente de la infraestructura tecnológica, sino de factores organizacionales, culturales y formativos, en línea con la visión de Von Solms & Van Niekerk (2018) sobre la necesidad de integrar la cultura de seguridad dentro del comportamiento corporativo. Esta relación se refleja en la correlación positiva entre la formación del personal y el nivel de madurez alcanzado.

4.2. Comparación con la literatura internacional

El panorama iberoamericano guarda similitudes con experiencias internacionales en cuanto a las dificultades de las PYMEs para desarrollar ecosistemas digitales resilientes. Sin embargo, existen diferencias marcadas en la disponibilidad de políticas públicas y programas de apoyo.

La Tabla 3 sintetiza los aportes más relevantes de autores y organismos internacionales en el período 2015–2024, que permiten contextualizar y contrastar los resultados obtenidos.

Autor(es) / Fuente	Año	Contexto geográfico	Aporte principal	Coincidencia con este estudio
Cisco & IDC	2015	Global	Identifican que el 43 % de los ciberataques se dirigen a PYMEs.	Confirma la exposición estructural del sector.
ENISA	2018	Europa	Propone modelos de madurez ajustados al tamaño de empresa.	Base metodológica del índice aplicado.
Von Solms & Van Niekerk	2018	Sudáfrica	Introducen el concepto de cultura de ciberseguridad organizacional.	Refuerza el vínculo entre cultura y resiliencia.
CISA	2020	EE. UU.	Define lineamientos de resiliencia digital post-COVID-19.	Apoya la incorporación de indicadores de recuperación.
OEA & BID	2022	Iberoamérica	Diagnostican brechas formativas y bajo nivel de preparación.	Coincide plenamente con los resultados regionales.
ENISA	2023	Europa	Destaca la formación continua y el liderazgo como ejes de resiliencia.	Reflejado en la correlación hallada entre formación y madurez.
Torres & Calderón	2024	Chile-Colombia	Reportan niveles medios-bajos de madurez digital.	Confirma los patrones detectados en este estudio.

Tabla 3 – Estudios internacionales relevantes sobre ciberseguridad y resiliencia en PYMEs (2015–2024)

Estos antecedentes muestran una evolución conceptual hacia la integración de la cultura organizacional y la resiliencia digital como dimensiones críticas de la seguridad. La presente investigación amplía esa tendencia al ofrecer datos empíricos comparativos de cinco países, algo escasamente documentado en la región.

4.3. Factores estructurales y culturales

El análisis comparativo sugiere que los países con políticas nacionales de ciberseguridad consolidadas —como España y Chile— presentan mejores indicadores de madurez. Este hallazgo respalda la hipótesis de González & Ramos (2021), quienes sostienen que la presencia de marcos regulatorios estables y programas estatales de capacitación correlaciona con mayores niveles de preparación digital.

Por el contrario, en países donde las políticas son incipientes o desarticuladas, las PYMEs dependen casi exclusivamente de su capacidad interna, lo que genera disparidades incluso dentro de un mismo sector. La falta de incentivos fiscales o de certificaciones adaptadas al tamaño empresarial limita la adopción de medidas preventivas sostenibles.

A nivel organizacional, se observa que la percepción de la ciberseguridad como un gasto y no como una inversión estratégica continúa siendo una barrera, tal como señalan Calder & Moody (2019). En las entrevistas, la mayoría de los gerentes asoció la seguridad digital a la tecnología de hardware, sin reconocer su dimensión humana o de procesos.

Dimensión	Factor determinante	Evidencia empírica	Referencia
Organizacional	Liderazgo comprometido con la seguridad	Correlación $r = 0,61$ con madurez	ENISA (2023)
Cultural	Conciencia del personal sobre riesgos digitales	68 % de las PYMEs sin capacitación anual	Torres & Calderón (2024)
Estructural	Disponibilidad presupuestaria	72 % reporta limitaciones	BID (2023)
Institucional	Existencia de marco normativo nacional	Mejores índices en España y Chile	González & Ramos (2021)

Tabla 4 – Factores internos y externos que influyen en la madurez cibernética

La evidencia demuestra que la madurez tecnológica no garantiza resiliencia digital si no se acompaña de liderazgo directivo, cultura preventiva y políticas públicas coherentes.

4.4. Hacia un modelo iberoamericano de madurez y resiliencia

Los resultados y la literatura convergen en la necesidad de desarrollar un modelo regional de madurez cibernética que considere la heterogeneidad económica y cultural de las PYMEs iberoamericanas. Tal enfoque debería combinar tres niveles:

- Técnico, basado en los marcos NIST y ENISA.
- Organizacional, que incorpore prácticas de gestión del conocimiento y cultura de seguridad.
- Ecosistémico, que articule políticas estatales, cámaras empresarias y universidades.

Nivel	Características principales	Enfoque dominante
Inicial	Ausencia de políticas formales; acciones reactivas.	Técnico-correctivo.
Gestionado	Procedimientos básicos y responsable designado.	Cumplimiento normativo.
Definido	Procesos documentados y capacitación regular.	Gestión integral del riesgo.
Cuantitativamente gestionado	Indicadores de desempeño y monitoreo continuo.	Prevención sistemática.
Optimizado	Cultura de resiliencia y mejora continua.	Estrategia corporativa.

Tabla 5 – Propuesta sintética de niveles de madurez adaptados al contexto iberoamericano

Este modelo, derivado de los hallazgos empíricos y de la revisión de marcos internacionales, busca ofrecer una herramienta adaptable a la realidad de las PYMEs de la región, facilitando diagnósticos periódicos y la implementación gradual de capacidades de ciberresiliencia.

El modelo propuesto tiene un carácter exploratorio y heurístico, y requiere validación empírica adicional en un mayor número de países y sectores.

4.5. Implicaciones teóricas y prácticas

Desde el punto de vista teórico, este estudio refuerza la necesidad de integrar la teoría de capacidades dinámicas (Teece, 2018) en el análisis de la ciberseguridad organizacional, entendiendo la resiliencia como una competencia estratégica que se aprende y evoluciona. En el plano práctico, aporta evidencias útiles para diseñar políticas públicas de apoyo, programas de certificación adaptados al tamaño empresarial y estrategias formativas sectoriales.

La madurez en ciberseguridad deja de ser un atributo técnico para convertirse en un indicador de sostenibilidad empresarial, estrechamente vinculado con la continuidad operativa y la confianza digital. Los resultados sugieren que fortalecer la resiliencia de las PYMEs no solo mejora su protección, sino que también incrementa su competitividad y su capacidad de integrarse en cadenas globales de valor digital.

5. Conclusiones

Este artículo ha demostrado que la madurez en ciberseguridad y la resiliencia digital constituyen factores estratégicos determinantes para la sostenibilidad de las PYMEs iberoamericanas en un entorno de creciente digitalización y riesgo. A partir del diagnóstico realizado en cinco países de la región, se evidenció que, aunque la adopción tecnológica ha avanzado de manera significativa, la gestión de la ciberseguridad continúa anclada en enfoques reactivos, dependientes de la infraestructura técnica y poco integrados en la cultura organizacional.

Los resultados han permitido confirmar el cumplimiento de los objetivos de la investigación: (1) caracterizar el nivel de madurez en ciberseguridad de las PYMEs analizadas de los distintos países a partir del modelo NIST, (2) identificar los factores estructurales, culturales y de liderazgo que condicionan la resiliencia digital, y (3) establecer lineamientos estratégicos para la evolución hacia modelos más integrales y sostenibles de gestión del riesgo digital. La evidencia empírica recogida, junto con la revisión de la literatura internacional, confirma que la madurez cibernética no puede comprenderse sin integrar dimensiones humanas, cognitivas y culturales en el análisis.

En cuanto a la pregunta de investigación —¿cuál es el nivel de madurez en ciberseguridad y resiliencia digital de las PYMEs iberoamericanas, y qué factores estratégicos determinan su desarrollo?— los hallazgos indican que la región se encuentra, en las empresas analizadas, en un estadio medio-bajo de preparación. Las capacidades más desarrolladas se concentran en la identificación y protección, mientras que las relacionadas con la respuesta y recuperación ante incidentes muestran una clara debilidad. Estos resultados concuerdan con diagnósticos previos realizados por organismos como la OEA y el BID, y evidencian una brecha creciente entre el ritmo de digitalización y la madurez en la gestión de riesgos tecnológicos.

Asimismo, se ha comprobado que las variables más influyentes en la madurez organizacional son el liderazgo comprometido, la capacitación continua y la existencia de políticas públicas de apoyo. Las empresas que incorporan la ciberseguridad como parte de su estrategia de negocio y que promueven una cultura de conciencia digital alcanzan niveles significativamente más altos de resiliencia. Por el contrario, aquellas que perciben la seguridad como un gasto operativo presentan respuestas reactivas, vulnerabilidades recurrentes y menor capacidad de recuperación post-incidente.

Esta investigación también aporta implicaciones prácticas relevantes. En primer lugar, resalta la necesidad de diseñar modelos de madurez adaptados al contexto iberoamericano, que combinen estándares internacionales (NIST, ENISA) con particularidades culturales y económicas de la región. En segundo lugar, sugiere la urgencia de articular políticas públicas, cámaras empresariales y universidades para desarrollar programas de formación y certificación que fortalezcan el capital humano en ciberseguridad. En tercer lugar, plantea la conveniencia de promover ecosistemas colaborativos de intercambio de información sobre incidentes, que incrementen la capacidad de respuesta sectorial.

Finalmente, este estudio contribuye a la literatura sobre gestión de la ciberseguridad al proponer una visión integral y evolutiva de la madurez digital, entendida no solo como un estado técnico, sino como una competencia dinámica y estratégica que se construye colectivamente. La resiliencia digital emerge, así, como un nuevo indicador de sostenibilidad empresarial, clave para la competitividad en mercados globalizados.

En consecuencia, se recomienda:

(1) consolidar un observatorio regional de madurez cibernética que monitoree avances y brechas;

(2) fomentar la formación continua de líderes y empleados en competencias digitales críticas;

(3) promover incentivos fiscales y certificaciones para las PYMEs que implementen buenas prácticas de seguridad;

y (4) realizar investigaciones longitudinales que evalúen la evolución de la madurez y la resiliencia digital en función de políticas nacionales y sectoriales.

El camino hacia una región digitalmente segura y resiliente no depende únicamente de la tecnología, sino de la capacidad colectiva para construir confianza, conocimiento y cultura de seguridad como ejes del desarrollo sostenible y competitivo iberoamericano.

Referencias

- Banco Interamericano de Desarrollo. (2023). *Ciberseguridad: Avances y desafíos en América Latina y el Caribe*. BID. <https://publications.iadb.org>
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2021). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.
- Calder, A., & Moody, S. (2019). *Information security risk management for ISO/IEC 27001*. IT Governance Publishing.
- Cano, J. J. & Rocha, A. (2019). *Ciberseguridad y ciberdefensa: Retos y perspectivas en un mundo digital*. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (32). <https://doi.org/10.17013/risti.32.0>
- Cisco & IDC. (2015). *Small business security: Threats are real, protection is critical*. Cisco Systems.
- Comisión Económica para América Latina y el Caribe. (2022). *Transformación digital y seguridad de la información en las PYMEs de América Latina*. CEPAL. <https://www.cepal.org>
- Cybersecurity and Infrastructure Security Agency. (2020). *Cyber resilience review*. U.S. Department of Homeland Security. <https://www.cisa.gov>
- European Union Agency for Cybersecurity. (2018). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu>
- European Union Agency for Cybersecurity. (2023). *National cybersecurity strategies evaluation framework*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu>
- European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu>
- González, A., & Ramos, J. (2021). Políticas públicas y preparación digital en América Latina. *Revista de Administración Pública*, 55(2), 89–108.
- Gutiérrez, L., & Hernández, P. (2021). Cultura organizacional y percepción del riesgo digital en PYMEs. *Revista Latinoamericana de Gestión*, 14(1), 33–49.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage.

- Hernández, R., Fernández, C., & Baptista, P. (2021). *Metodología de la investigación* (7.^a ed.). McGraw-Hill.
- ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection*. International Organization for Standardization.
- Kaspersky. (2024). *Cybersecurity risks for SMEs in Latin America*. Kaspersky Lab. <https://www.kaspersky.com>
- Molina, F., Pérez, J., & Suárez, R. (2023). Madurez digital y gestión del riesgo en PYMEs iberoamericanas. *Revista Iberoamericana de Sistemas y Tecnologías de Información*, 54(1), 19–34.
- National Institute of Standards and Technology. (2023). *Cybersecurity framework (Version 2.0)*. <https://www.nist.gov/cyberframework>
- Organization of American States & Inter-American Development Bank. (2022). *Cybersecurity: Risks, progress, and the way forward in Latin America and the Caribbean*. OAS–IDB.
- Organization of American States & Inter-American Development Bank. (2023). *Cybersecurity report 2023*. OAS–IDB.
- Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). Sage.
- Radanliev, P., De Roure, D., Nurse, J. R. C., & Burnap, P. (2022). Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence. *Journal of Cybersecurity*, 8(1), 1–14. <https://doi.org/10.1093/cybsec/tyac006>
- Sánchez-García, I. D., Rea-Guamán, A. M., San Feliu, T., & Calvo-Manzano, J. A. (2024). *Cybersecurity risk audit: Literature review, proposal, and application*. RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação, (53), 69–87. <https://doi.org/10.17013/risti.53.69-87>
- Secretaría General Iberoamericana. (2022). *Estrategia iberoamericana de transformación digital 2022–2025*. Secretaría General Iberoamericana.
- Silva, R., & Costa, E. (2023). Cybersecurity maturity models and SMEs: A systematic review. *Computers & Security*, 122, 102900. <https://doi.org/10.1016/j.cose.2022.102900>
- Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning*, 51(1), 40–49. <https://doi.org/10.1016/j.lrp.2017.06.007>
- Torres, J., & Calderón, M. (2024). Niveles de madurez digital en PYMEs de Chile y Colombia. *Revista Latinoamericana de Administración*, 20(2), 55–72.
- Von Solms, R., & Van Niekerk, J. (2018). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- World Economic Forum. (2024). *Global cybersecurity outlook 2024*. <https://www.weforum.org/reports/global-cybersecurity-outlook-2024>

Crítérios Editoriais

A RISTI (Revista Ibérica de Sistemas e Tecnologias de Informação) é um periódico científico, que foca a investigação e a aplicação prática inovadora no domínio dos sistemas e tecnologias de informação.

O Conselho Editorial da RISTI incentiva potenciais autores a submeterem artigos originais e inovadores para avaliação pelo Conselho Científico.

A submissão de artigos para publicação na RISTI deve realizar-se de acordo com as chamadas de artigos e as instruções e normas disponibilizadas no sítio Web da revista (<http://www.risti.xyz/>).

Todos os artigos submetidos são avaliados por um conjunto de membros do Conselho Científico, não inferior a três elementos.

Em cada número da revista são publicados entre cinco a oito dos melhores artigos submetidos.

Críterios Editoriales

La RISTI (Revista Ibérica de Sistemas y Tecnologías de la Información) es un periódico científico, centrado en la investigación y en la aplicación práctica innovadora en el dominio de los sistemas y tecnologías de la información.

El Consejo Editorial de la RISTI incentiva autores potenciales a enviar sus artículos originales e innovadores para evaluación por el Consejo Científico.

El envío de artículos para publicación en la RISTI debe hacerse de conformidad con las llamadas de los artículos y las instrucciones y normas establecidas en el sitio Web de la revista (<http://www.risti.xyz/>).

Todos los trabajos enviados son evaluados por un número de miembros del Consejo Científico de no menos de tres elementos.

En cada número de la revista se publican cinco a ocho de los mejores artículos enviados.



Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

©ITMA 2025 <http://www.risti.xyz>

