tic

Cuadernos de desarrollo aplicados a las TIC

Ed. 37_Vol. 10_N.º 2
Junio _ Septiembre 2021

Publicación trimestral
ISSN: 2254 – 6529

3C TIC. Cuadernos de desarrollo aplicados a las TIC.

Periodicidad trimestral. *Quarterly periodicity.*

Edición 37, Volumen 10, Número 2 (Junio - Septiembre 2021).

Edition 37, Volume 10, Issue 2 (June - September 2021).

Tirada nacional e internacional. *National and internacional circulation.*

Artículos revisados por el método de evaluación de pares de doble ciego.

Articles reviewed by the double blind peer evaluation method.

ISSN: 2254 – 6529

Nº de Depósito Legal: A 268 – 2012

DOI: <https://doi.org/10.17993/3ctic.2021.102>

Edita:

Área de Innovación y Desarrollo, S.L.

C/Alzamora 17, Alcoy, Alicante (España)

Tel: 965030572

info@3ciencias.com _ www.3ciencias.com

Todos los derechos reservados. Se autoriza la reproducción total o parcial de los artículos citando la fuente y el autor.

This publication may be reproduced by mentioning the source and the authors.

Copyright © Área de Innovación y Desarrollo, S.L.

CONSEJO EDITORIAL EDITORIAL BOARD

Director	Víctor Gisbert Soler
Editores adjuntos	María J. Vilaplana Aparicio Maria Vela Garcia
Editores asociados	David Juárez Varón F. Javier Cárcel Carrasco

CONSEJO DE REDACCIÓN DRAFTING BOARD

Dr. David Juárez Varón. *Universitat Politècnica de València (España)*
Dra. Úrsula Faura Martínez. *Universidad de Murcia (España)*
Dr. Martín León Santiesteban. *Universidad Autónoma de Occidente (México)*
Dra. Inmaculada Bel Oms. *Universitat de València (España)*
Dr. F. Javier Cárcel Carrasco. *Universitat Politècnica de València (España)*
Dra. Ivonne Burguet Lago. *Universidad de las Ciencias Informáticas (La Habana, Cuba)*
Dr. Alberto Rodríguez Rodríguez. *Universidad Estatal del Sur de Manabí (Ecuador)*

CONSEJO ASESOR ADVISORY BOARD

Dra. Ana Isabel Pérez Molina. *Universitat Politècnica de València (España)*
Dr. Julio C. Pino Tarragó. *Universidad Estatal del Sur de Manabí (Ecuador)*
Dra. Irene Belmonte Martín. *Universidad Miguel Hernández (España)*
Dr. Jorge Francisco Bernal Peralta. *Universidad de Tarapacá (Chile)*
Dra. Mariana Alfaro Cendejas. *Instituto Tecnológico de Monterrey (México)*
Dr. Roberth O. Zambrano Santos. *Instituto Tecnológico Superior de Portoviejo (Ecuador)*
Dra. Nilda Delgado Yanes. *Universidad de las Ciencias Informáticas (La Habana, Cuba)*
Dr. Sebastián Sánchez Castillo. *Universitat de València (España)*
Dra. Sonia P. Ubillús Saltos. *Instituto Tecnológico Superior de Portoviejo (Ecuador)*
Dr. Jorge Alejandro Silva Rodríguez de San Miguel. *Instituto Politécnico Nacional (México)*

CONSEJO EDITORIAL EDITORIAL BOARD

Área financiera	Dr. Juan Ángel Lafuente Luengo <i>Universidad Jaime I (España)</i>
Área textil	Dr. Josep Valdeperas Morell <i>Universitat Politècnica de Catalunya (España)</i>
Ciencias de la Salud	Dra. Mar Arlandis Domingo <i>Hospital San Juan de Alicante (España)</i>
Derecho	Dra. María del Carmen Pastor Sempere <i>Universidad de Alicante (España)</i>
Economía y empresariales	Dr. José Joaquín García Gómez <i>Universidad de Almería (España)</i>
Estadística y Investigación operativa	Dra. Elena Pérez Bernabeu <i>Universitat Politècnica de València (España)</i>
Ingeniería y Tecnología	Dr. David Juárez Varón <i>Universitat Politècnica de València (España)</i>
Organización de empresas y RRHH	Dr. Francisco Llopis Vañó <i>Universidad de Alicante (España)</i>
Sinología	Dr. Gabriel Terol Rojo <i>Universitat de València (España)</i>
Sociología y Ciencias Políticas	Dr. Rodrigo Martínez Béjar <i>Universidad de Murcia (España)</i>
Tecnologías de la Información y la Comunicación	Dr. Manuel Llorca Alcón <i>Universitat Politècnica de València (España)</i>

POLÍTICA EDITORIAL

OBJETIVO EDITORIAL

La Editorial científica 3Ciencias pretende transmitir a la sociedad ideas y proyectos innovadores, plasmados, o bien en artículos originales sometidos a revisión por expertos, o bien en los libros publicados con la más alta calidad científica y técnica.

COBERTURA TEMÁTICA

3C TIC es una revista de carácter científico-social en la que se difunden trabajos originales que tratan sobre la aplicación de las Tecnologías de la Información y Comunicación (TIC) y las Telecomunicaciones a la Sociedad, la Educación y la Gestión Empresarial.

NUESTRO PÚBLICO

- Personal investigador.
- Doctorandos.
- Profesores de universidad.
- Oficinas de transferencia de resultados de investigación (OTRI).
- Empresas que desarrollan labor investigadora y quieran publicar alguno de sus estudios.

AIMS AND SCOPE

PUBLISHING GOAL

3C Ciencias wants to transmit to society innovative projects and ideas. This goal is reached through the publication of original articles which are subject to peer review or through the publication of scientific books.

THEMATIC COVERAGE

3C TIC is a scientific-social journal that spreads original works related with the application of Information and Communication Technologies (ICT) and Telecommunications to Society, Education and Business Management.

OUR TARGET

- Research staff.
- PhD students.
- Professors.
- Research Results Transfer Office.
- Companies that develop research and want to publish some of their works.

NORMAS DE PUBLICACIÓN

3C TIC es una revista arbitrada que utiliza el sistema de revisión por pares de doble ciego (*double-blind peer review*), donde expertos externos en la materia sobre la que trata un trabajo lo evalúan, siempre manteniendo el anonimato, tanto de los autores como de los revisores. La revista sigue las normas de publicación de la APA (American Psychological Association) para su indización en las principales bases de datos internacionales.

Cada número de la revista se edita en versión electrónica (e-ISSN: 2254 – 6529), identificándose cada trabajo con su respectivo código DOI (Digital Object Identifier System).

PRESENTACIÓN TRABAJOS

Los artículos se presentarán en tipo de letra Baskerville, cuerpo 11, justificados y sin tabuladores. Han de tener formato Word. La extensión será de no más de 6.000 palabras de texto, incluidas referencias.

Los trabajos deben ser enviados exclusivamente por plataforma de gestión de manuscritos OJS:

<https://ojs.3ciencias.com/>

Toda la información, así como las plantillas a las que deben ceñirse los trabajos se encuentran en:

<https://www.3ciencias.com/revista/informacion-para-autores/>

<https://www.3ciencias.com/normas-de-publicacion/plantillas/>

SUBMISSION GUIDELINES

3C TIC is an arbitrated journal that uses the double-blind peer review system, where external experts in the field on which a paper deals evaluate it, always maintaining the anonymity of both the authors and of the reviewers. The journal follows the standards of publication of the APA (American Psychological Association) for indexing in the main international databases.

Each issue of the journal is published in electronic version (e-ISSN: 2254 – 6529), each work being identified with its respective DOI (Digital Object Identifier System) code.

PRESENTATION WORK

The papers will be presented in Baskerville typeface, body 11, justified and without tabs. They must have Word format. The extension will be no more than 6.000 words of text, including references. Papers must be submitted exclusively by OJS manuscript management platform:

<https://ojs.3ciencias.com/>

All the information, as well as the templates to which the works must adhere, can be found at:

<https://www.3ciencias.com/en/journals/information-for-authors/>

<https://www.3ciencias.com/en/regulations/templates/>

ESTRUCTURA

Los trabajos originales tenderán a respetar la siguiente estructura: introducción, métodos, resultados, discusión/conclusiones, notas, agradecimientos y referencias bibliográficas.

Es obligatoria la inclusión de referencias, mientras que notas y agradecimientos son opcionales. Se valorará la correcta citación conforme a la 7.^a edición de las normas APA.

RESPONSABILIDADES ÉTICAS

No se acepta material previamente publicado (deben ser trabajos inéditos). En la lista de autores firmantes deben figurar única y exclusivamente aquellas personas que hayan contribuido intelectualmente (autoría), con un máximo de 4 autores por trabajo. No se aceptan artículos que no cumplan estrictamente las normas.

INFORMACIÓN ESTADÍSTICA SOBRE TASAS DE ACEPTACIÓN E INTERNACIONALIZACIÓN

- Número de trabajos aceptados publicados: 5.
- Nivel de aceptación de manuscritos en este número: 41,7%.
- Nivel de rechazo de manuscritos: 58,3%.
- Internacionalización de autores: 5 países (Perú, Brasil, Ecuador, España y Pakistán).

Normas de publicación: <https://www.3ciencias.com/normas-de-publicacion/instrucciones/>

STRUCTURE

The original works will tend to respect the following structure: introduction, methods, results, discussion/ conclusions, notes, acknowledgments and bibliographical references.

The inclusion of references is mandatory, while notes and acknowledgments are optional. The correct citation will be assessed according to the 7th edition of the APA standards.

ETHICAL RESPONSIBILITIES

Previously published material is not accepted (they must be unpublished works). The list of signatory authors should include only and exclusively those who have contributed intellectually (authorship), with a maximum of 4 authors per work. Articles that do not strictly comply with the standards are not accepted.

STATISTICAL INFORMATION ON ACCEPTANCE AND INTERNATIONALIZATION FEES

- Number of accepted papers published: 5.
- Level of acceptance of manuscripts in this number: 41,7%.
- Level of rejection of manuscripts: 58,3%.
- Internationalization of authors: 5 countries (Peru, Brazil, Ecuador, Spain and Pakistan).

Guidelines for authors: <https://www.3ciencias.com/en/regulations/instructions/>

INDEXACIONES INDEXATIONS

INDEXACIONES INDEXATIONS

/SUMARIO/ /SUMMARY/

Revisión sistemática sobre aprendizaje autónomo universitario a través de la virtualidad

Systematic review on university autonomous learning through virtuality

Josefina Amanda Suyo-Vega, Ana da Costa Polonia y Angélica Inês Miotto

17

Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador

Cybersecurity for learning platforms in higher education institutions in Tungurahua province of Ecuador

Pablo Israel Morales-Paredes y Patricio Medina-Chicaiza

49

Gamificación y aprendizaje activo con Kahoot!: creación de exámenes por parte del alumnado

Gamification and active learning with Kahoot!: student creation of exams

Cecile Meier y Alejandro Bonnet de León

77

Development of computational linguistic resources for automated detection of textual cyberbullying threats in Roman Urdu language

Amirita Dewani, Mohsin Ali Memon y Sania Bhatti

101

Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations

Maurice Frayssinet Delgado, Doris Esenarro, Francisco Fernando Juárez Regalado y Mónica Díaz Reátegu

123

/01/

REVISIÓN SISTEMÁTICA SOBRE APRENDIZAJE AUTÓNOMO UNIVERSITARIO A TRAVÉS DE LA VIRTUALIDAD

SYSTEMATIC REVIEW ON UNIVERSITY AUTONOMOUS LEARNING THROUGH VIRTUALITY

Josefina Amanda Suyo-Vega

Docente investigadora, Universidad César Vallejo, (Perú).

E-mail: Jsuyov1@ucv.edu.pe ORCID: <https://orcid.org/0000-0002-2954-5771>

Ana da Costa Polonia

Docente, Centro Universitario Euro-Americano Unieuro DF, (Brasil).

E-mail: ana.polonia@unieuro.edu.br ORCID: <https://orcid.org/0000-0002-5089-0254>

Angélica Inês Miotto

Docente, Centro Universitario Euro-Americano Unieuro DF, (Brasil).

E-mail: angelica.miotto@unieuro.edu.br ORCID: <https://orcid.org/0000-0002-3655-2136>

Recepción: 28/04/2021 **Aceptación:** 02/06/2021 **Publicación:** 29/06/2021

Citación sugerida:

Suyo-Vega, J. A., Polonia, A. da C., y Miotto, A. I. (2021). Revisión sistemática sobre aprendizaje autónomo universitario a través de la virtualidad. *3C TIC. Cuadernos de desarrollo aplicados a las TIC*, 10(2), 17-47. <https://doi.org/10.17993/3ctic.2021.102.17-47>

RESUMEN

El aprendizaje autónomo universitario es aquella capacidad que logra el estudiantado fuera de las condiciones establecidas, logrando autorregular el aprendizaje. La enseñanza virtual ha fortalecido el aprendizaje autónomo del estudiantado en todas las modalidades y niveles. El objetivo fue sistematizar las evidencias científicas sobre la autonomía de los estudiantes universitarios, empleando el diagrama de Flujo PRISMA. Se analizó la base de datos Scopus, Scielo, Eric y Ebsco Host. A través de los operadores booleanos “AND” y “OR”, y las operaciones de búsqueda en los idiomas, español, inglés y portugués. Se utilizaron criterios de inclusión y exclusión entre ellos los años, desde el 2011 hasta el 2021, publicaciones en etapa final, países de Iberoamérica, temática en educación y ciencias sociales. A través de la sistematización se obtuvo 11,271,889 artículos, pero se llegaron a analizar 21 artículos, que respondieron a la pregunta de investigación ¿Cuáles son las estrategias que utilizan los estudiantes universitarios para lograr la autonomía en el aprendizaje?, incluyendo instrumentos, enfoques y países de mayor evidencia en publicación sobre la temática. Los resultados indican que la experticia, el conocimiento y la disposición del profesorado, facilitan el aprendizaje autónomo. Concluyendo que la concentración y planeamiento son claves para lograr la autonomía del aprendizaje.

PALABRAS CLAVE

Iberoamérica, Aprendizaje, Autonomía, Universitario, Medios Virtuales, Revisión Sistemática.

ABSTRACT

Autonomous university learning is the capacity that students achieve outside the established conditions, achieving self-regulated learning. Virtual teaching has strengthened the autonomous learning of students in all modalities and levels. The objective was to systematize the scientific evidence on the autonomy of university students, using the PRISMA Flowchart. The Scopus, Scielo, Eric, and Ebsco Host databases were analyzed. Through the Boolean operators "AND" and "OR", and search operations in Spanish, English, and Portuguese. Inclusion and exclusion criteria were used, including the years from 2011 to 2021, publications in the final stage, Ibero-American countries, and topics in education and social sciences. Through systematization, 11,271,889 articles were obtained, but 21 articles were analyzed, which responded to the research question "What are the strategies used by university students to achieve autonomy in learning?", including instruments, approaches, and countries with the most evidence in publications on the subject. The results indicate that the expertise, knowledge, and disposition of the teaching staff facilitate autonomous learning. Concluding that concentration and planning are key to achieve learning autonomy.

KEYWORDS

Ibero- America, Learning, Learning, Autonomy, University, Virtual Media, Systematic Review.

1. INTRODUCCIÓN

El proceso de enseñanza aprendizaje del estudiantado universitario, comprende, estrategias, técnicas, instrumentos, herramientas tecnológicas, ritmos, estilos y evaluación. Todo el proceso recae en un binomio estudiantado y profesorado, que de acuerdo a la realidad del Covid-19, se agrega el aprendizaje autónomo. Diversas investigaciones muestran resultados a tomar en cuenta sobre la autonomía en contexto universitario.

Sáez *et al.* (2018a) desarrollaron una revisión sistemática de la literatura en la base de datos Web of Science Scopus y Scielo, sobre competencias de autorregulación del aprendizaje en estudiantes universitarios y programas intracurriculares para su promoción. El objetivo fue caracterizar las investigaciones sobre autorregulación. Concluyendo que es necesario desarrollar programas de tipo intracurricular para la promoción de competencias de autorregulación del aprendizaje en estudiantes universitarios y orientar nuevas investigaciones centradas en la implicación del profesorado en este proceso.

Resultados similares se encontraron en la revisión sistemática de Lima y Santiba (2020) destacando la tendencia de los estudios cualitativos, señalando que los estudiantes que regulan su aprendizaje tienen un mayor repertorio de estrategias cognitivas y están más motivados académicamente.

Asimismo, Enríquez y Hernández (2021) investigaron sobre el nivel de autonomía que tiene el estudiantado. Analizando las dimensiones afectivas, sociales, cognitivas, metacognitivas y orientadas a la acción. Concluyendo que en el contexto de pandemia es necesario el acompañamiento del profesorado.

En Brasil, varios investigadores Boruchovitch (2014); Polydoro y Azzi, (2009); Silva y Simão, (2016); Ganda y Boruchovitch (2018) han investigado la autorregulación del aprendizaje con el propósito de identificar las dinámicas relacionadas con la autonomía, la autogestión y las estrategias de estudio. Las definiciones destacan que es un proceso a través del cual los estudiantes son capaces de controlar y articular el conocimiento, el pensamiento, la emoción y la motivación, empleando las estrategias necesarias para mejorar el aprendizaje. Entre los factores comunes asociados están la autonomía y la

proactividad para maximizar el aprendizaje y el desarrollo de estrategias asertivas que se emplean en diversos contextos relacionados con la adquisición de conocimientos.

Es fundamental que el espacio universitario, en el escenario pandémico, y a través de los recursos tecnológicos, el estudiantado reconozca y cree estrategias pedagógicas para promover procesos de autorregulación con el fin de consolidar el aprender a aprender. En esta dirección, Polydoro *et al.*, (2019), con el propósito de realizar una adaptación transcultural para la población universitaria brasileña, utilizaron tres instrumentos que exploran la autorregulación del aprendizaje en estudiantes de educación superior: Inventario de Procesos de Autorregulación del Aprendizaje (IPAA), Cuestionario de Instrumentalidad de la Autorregulación del Aprendizaje (QIAR) y Cuestionario de Autoeficacia para la Autorregulación del Aprendizaje (QAEAR).

Los resultados psicométricos indicaron que las versiones para Brasil mostraron validez de constructo, reflejando que los ítems son sensibles y captaron los procesos de autorregulación del aprendizaje, además de las condiciones de instrumentalidad y creencias de autoeficacia para la autorregulación del aprendizaje en la educación superior. Sobre todo, los investigadores insisten en la necesidad de explorar instrumentos que contribuyan a profundizar en la comprensión del tema. Ampliando las investigaciones, Monnerat, Pessoa y Ferreira (2016) analizaron las investigaciones sobre el aprendizaje autorregulado en la educación a distancia en Brasil y Portugal. Identificaron cuatro instrumentos utilizados con un papel importante en la autorregulación: el portafolio, las estrategias de aprendizaje adoptadas para el desarrollo de los contenidos, así como las utilizadas por el tutor que promueven la autorregulación y el uso de hipermedia. En resumen, los autores sugieren que se lleven a cabo más estudios con diversas plataformas para identificar los procesos y las estrategias utilizadas para buscar la autonomía e independencia del estudiantado.

Zoltowski y Teixeira (2020) realizaron un estudio de caso colectivo con tres estudiantes de grado, con el objetivo de investigar las competencias de autorregulación. El análisis de contenido se basó en las categorías teóricas, considerando el ciclo de autorregulación: fase de anticipación, fase de actuación

y fase de autorreflexión. Las conclusiones señalan que la cuestión de la autorregulación estaba bajo la influencia de los reguladores externos, revelando así el papel de la retroalimentación pedagógica, no restringida a los resultados académicos, sin embargo, revelando la promoción de los estudios. Además, señalando factores esenciales para activar aspectos relacionados con la independencia, la criticidad, la reflexión y la propia autorregulación.

Otra investigación promovida por Boruchovitch y Santos (2015) tuvo como objetivo realizar el análisis psicométrico de una escala diseñada para evaluar las estrategias de aprendizaje considerando los componentes cognitivos y metacognitivos: Escala de Estrategias de Aprendizaje para Alumnos universitarios (EEA-U). El instrumento se aplicó a 1490 estudiantes universitarios brasileños de instituciones públicas y privadas. Los análisis señalaron tres factores principales, a saber: (1) autorregulación cognitiva y metacognitiva: planificación, seguimiento y regulación del aprendizaje; (2) autorregulación de los recursos internos y contextuales: cómo se activan y ponen en práctica para realizar el aprendizaje autorregulado; y (3) autorregulación social: gestión del entorno social en apoyo de la organización y del propio proceso de autorregulación. Los autores aluden a que los resultados pueden ayudar significativamente a los investigadores, estudiantes y profesores en el aumento de los procesos de autorregulación.

Salgado, Polydoro y Rosario (2018) desarrollaron una investigación dirigida a evaluar la efectividad de un programa para promover el aprendizaje autorregulado en estudiantes de pregrado. Se aplicó al estudiantado de primer año de una universidad pública. El enfoque cuali-cuantitativo indicó que las competencias instrumentales, interpersonales y sistémicas surgieron al final del programa. Se evidenció que el desarrollo de la competencia de autorregulación ocurre en etapas, además de estar bajo la influencia de factores como el curso y el semestre de graduación del estudiante, vinculados a los aspectos personales, sociales y contextuales.

Teniendo en cuenta la importancia de vislumbrar la panorámica sobre el fenómeno, la propuesta de una revisión bibliográfica sistemática permite analizar las tendencias, los marcos teóricos, los autores

que estudian el fenómeno y la diversidad de enfoques e instrumentos que se utilizan, contribuyendo significativamente a los avances en el área de conocimiento, permitiendo configurar el estado del arte en un período determinado. En este sentido, se señalan lagunas y problemas teórico-metodológicos y se sugieren nuevas líneas de investigación para profundizar y diversificar el estudio sobre el tema.

Hitos de la investigación sobre la autorregulación del aprendizaje: aspectos teóricos y aportaciones

Un referente teórico y metodológico sobre la autonomía en el aprendizaje es Zimmerman (2008), él destaca que las discusiones sobre el aprendizaje autorregulado se vienen dando desde hace décadas, explorando estudios por medio de selectos y diversos instrumentos de investigación para captar el proceso y sus dimensiones, apoyándose en cuestionarios y entrevistas. El autor destaca que en la segunda oleada de investigaciones se ha invertido en captar los matices del aprendizaje de la autorregulación, con nuevas metodologías como las medidas online, los protocolos, los diarios, la observación directa y el microanálisis para implementar el estudio sobre el fenómeno. Cabe mencionar que los estudios de Zimmerman se basaron en la teoría social cognitiva de Bandura. Retomando la propuesta de Bandura, Ganda y Boruchovitch, (2018) postulan que fue el pionero en investigar la autorregulación de la conducta, caracterizando los procesos intrínsecos a la autogestión: autoobservación, juicio y autorreacción. En resumen, la autoobservación se refiere al seguimiento del sujeto en relación con su objetivo, lo que implica calidad, ritmo, cantidad, originalidad, consecuencias, desviación y moralidad. El proceso de juicio refleja la evaluación del propio rendimiento y permite la comparación con el rendimiento de los compañeros, teniendo como referencias los valores personales, las experiencias, las normas sociales y las expectativas.

En esta dirección, Boruchovitch (2014) y Ganda y Boruchovitch (2018), dedicándose a una revisión de los modelos de aprendizaje autorregulado, reportan que inicialmente las preocupaciones recayeron en las estrategias de aprendizaje, posteriormente, se incorporaron otras dimensiones: motivación, metas, atribuciones, autoeficacia, valores y aspectos afectivo-motivacionales en un enfoque integrado de estos procesos. Describen cuatro modelos, resumidos brevemente: a) modelo de McCaslin y Good (1996)

denominado "modelo de corregulación del aprendizaje", basado en el aspecto sociocultural, en el que la unidad de análisis es la interacción entre personas, escenarios y objetos, sobre todo, estructurado en los aspectos motivacionales, de impulso y de evaluación; (b) modelo de Winne y Hadwin (1998) abarca la metacognición, las estrategias de aprendizaje y la supervisión; (c) modelo propuesto por Zimmerman (2000) se centra en los tipos de autorregulación, conductual, ambiental y de comportamiento que se detallarán más adelante; (d) modelo de Pintrich (2000) comprende factores como: la cognición, la motivación, el afecto y el contexto, identificando cuatro momentos: en el primero, la predicción, la planificación y la activación; en el segundo, predomina la monitorización; en el tercero, el control; y el cuarto implica esencialmente la reacción y la reflexión.

Zimmerman (2008), postula que la autorregulación del aprendizaje refleja el grado en que los estudiantes se implican activamente en su propio proceso de aprendizaje mediante la comprensión de las múltiples facetas metacognitivas, motivacionales y conductuales, como ya se ha mencionado. La independencia y la proactividad son un diferencial para el desarrollo académico. Por lo tanto, identificar y caracterizar cómo los estudiantes utilizan la autorregulación en el espacio de aprendizaje se ha convertido en el foco de la investigación y también en el desarrollo de instrumentos que puedan captar este proceso. Este conocimiento puede orientar las dinámicas pedagógicas programadas por los profesores para aumentar y promover el aprendizaje autorregulado.

El propio Zimmerman (2013) señaló que, al iniciar los estudios sobre autorregulación, fueron básicas tres grandes definiciones, las nociones de habilidad, comportamiento y creencias personales. El autor destaca que el aprendizaje autorregulado implica un conjunto de procesos específicos que provocan transformaciones en las habilidades ya adquiridas al realizar nuevas tareas. Así, Zimmerman (1998) alerta de que la autorregulación no puede concebirse como un elemento estático, sobre todo, hay que entender las interrelaciones que la configuran. Principalmente que, el grado y la calidad del proceso de autorregulación están imbricados a factores como la motivación, el método educativo y el tiempo.

Panadero (2017) afirmó que el modelo de aprendizaje autorregulado abarca aspectos cognitivos, motivacionales y emocionales, siendo actualmente uno de los intereses del área de la Psicología Educativa. El autor registra que Zimmerman, en 1989, hizo una primera incursión en la dirección de construir un modelo ilustrativo del aprendizaje autorregulado, con la singular colaboración de dos exponentes del área: Bandura y Rosenthal. Este primer modelo, basado en la perspectiva triádica de la cognición social de Bandura, revela las dimensiones: ambiental, conductual y personal.

Continuando con sus investigaciones, Zimmerman (2013 como se cita en Panadero, 2017), amplía e introduce un segundo modelo de carácter cíclico, caracterizado como multinivel que incluye las etapas de planificación, actuación y autorreflexión. Esencialmente, en la fase de planificación, el alumno analiza la tarea, establece los objetivos, identifica los pasos que permiten la consecución y, paralelamente, moviliza sus energías y se implica, demostrando el nivel de motivación y las creencias para lograr su objetivo. La actuación ilustra el escenario para la realización de la tarea, evaluando el progreso y los obstáculos, buscando herramientas que puedan aumentar eficazmente el proceso, supervisando su compromiso y motivación. Y por último, la autorreflexión, momento en el que se evalúa todo el proceso de autorregulación, analizando los puntos que les permitieron avanzar o las barreras que impidieron su realización. Además, el éxito o el fracaso en la realización de una tarea puede influir en las reacciones del alumno cuando se enfrenta a nuevas situaciones de aprendizaje.

Consustanciando las discusiones, Wigfield, Klauda y Cambria (2011) destacaron que la fase de previsión y planificación abarca aspectos motivacionales, así como creencias y valores que impulsan a la persona a trazar pasos, momentos o etapas para alcanzar una meta, en relación con una tarea predeterminada. A continuación, se produce el seguimiento con el fin de investigar las estrategias que facilitan o dificultan el rendimiento académico y, en consecuencia, interfieren en el nivel de motivación. También añaden la subdivisión propuesta por Pintrich y Zusho (2002) como se cita en Wigfield *et al.* (2011) que incluyó, el seguimiento y el control. Otra tarea, corresponde a la reflexión sobre la actuación que tiene lugar una vez finalizada la actividad o tarea. En ella, se puede comprobar por qué se obtuvo un determinado resultado

u otro diferente al esperado, también es posible gestionar las emociones o sentimientos que surgen en relación a las expectativas en relación a lo obtenido. Siendo necesario, repensar lo que debe modificarse o mejorarse, indicando su carácter evaluativo. Aun así, en esta fase retoman los desarrollos, identificando los factores que deben ser regulados como: la cognición, la motivación, los efectos o influencias sobre el sujeto y la conducta.

La visión general del ciclo de aprendizaje autorregulado registra que su estructura está construida por etapas los momentos que son cruciales para ayudar al estudiantado y al profesorado en la sistematización de la actividad y la organización privilegiada para asegurar la planificación, el rendimiento y la autorreflexión. Esta noción integrada no separa los aspectos cognitivos, motivacionales y ambientales que pueden ser facilitadores o pueden ser barreras para el aprendizaje autónomo, crítico, proactivo y reflexivo. Así, se caracteriza el papel activo, proactivo y autónomo que debe fomentarse continuamente en el espacio universitario, con el profesorado y el estudiantado como interlocutores, mediados por propuestas pedagógicas. Resaltan las guías de orientación, que se pueden utilizar para estudios posteriores, para prepararse en los exámenes siguientes y en la elaboración de resúmenes, aunque conlleve mayor trabajo y dedicación, que finalmente se refleja en la reflexión de los nuevos conocimientos del estudiantado (López y Moya, 2012). Asimismo, el uso del portafolio digital en el ámbito universitario es importante, en el cual se reconoce la participación, aprendizaje autónomo y motivación del estudiantado (Gámiz-Sánchez, Gallego-Arrufat y Cristo-Moya, 2016).

De lo expuesto, se evidencia vacíos en las investigaciones como la descripción de las estrategias de aprendizaje por parte del estudiantado universitario. Por ello, es necesario contestar a las siguientes interrogantes ¿Cuáles son las evidencias científicas sobre estrategias que se han desarrollado para lograr el aprendizaje autónomo?, ¿Qué instrumentos se han aplicado para identificar procesos de aprendizaje autónomo? Asimismo, es necesario conocer por parte del profesorado ¿Qué estrategias metodológicas utiliza para promover el aprendizaje autónomo en el estudiantado?

2. METODOLOGÍA

Para desarrollar la revisión sistemática se eligieron las siguientes bases de datos: Scopus, Scielo, Eric y Ebsco Host. Se eligieron estas bases de datos porque reúnen revistas que adoptan criterios reconocidos por la comunidad científica, así como publicaciones de diferentes países e idiomas. Los artículos seleccionados en español, portugués e inglés que produjeron las siguientes ecuaciones de búsqueda en los tres idiomas, así como el uso de sinónimos que produjeron dichas ecuaciones (Tabla 1 y 2). Retomando los descriptores booleanos considerando la proposición de su empleo en cada base, en este caso: "AND", "or", "OR". La encuesta inicial generó un total de 11,271,889 artículos que, al aplicar los criterios de inclusión y exclusión, quedaron 21 artículos, siguiendo el diagrama de flujo denominado PRISMA (Donato y Donato, 2019).

Tabla 1. Palabras clave y sinónimos.

Palabras clave	Sinónimos
Aprendizaje autónomo	Aprendizaje independiente OR autoaprendizaje OR aprendizaje autónomo OR autorregulación OR aprendizaje autorregulado
Estudiante universitario	"Universitario" OR "graduado" OR "graduación"

Fuente: elaboración propia.

Tabla 2. Ecuaciones de búsqueda en las bases de datos Scopus, Ebsco, Scielo y Eric.

Base de datos	Ecuación de búsqueda (español, inglés y portugués)	Total	Tiempo	Idioma, año, país, materia	Análisis
SCOPUS	(aprendizaje independiente OR autoaprendizaje OR aprendizaje autónomo OR autorregulación OR aprendizaje autorregulado) and (Universitario OR graduado OR graduación)	2	2	2	1
	(Independent learning OR self-learning OR autonomous learning OR self-regulation OR self-regulated learning OR self-regulated learning) and (University OR graduate OR graduation OR graduation)	4 706	1 420	21	7
	(aprendizagem independente OU auto-aprendizagem OU aprendizagem autônoma OU aprendizagem auto-regulada OU aprendizagem auto-regulada OU aprendizagem auto-regulada) e (Universidade OU pós-graduação OU graduação OU graduação)	0	0	0	0
EBSCO	(Aprendizaje independiente OR autoaprendizaje OR aprendizaje autónomo OR autorregulación OR aprendizaje autorregulado) and (Universitario OR graduado OR graduación)	62 526	17 607	18	1
	(Independent learning OR self-learning OR autonomous learning OR self-regulation OR self-regulated learning OR self-regulated learning) and (University OR graduate OR graduation OR graduation)	11 109 746	1 246 839	8	3
	(aprendizagem independente OU auto-aprendizagem OU aprendizagem autônoma OU aprendizagem auto-regulada OU aprendizagem auto-regulada OU aprendizagem auto-regulada) e (Universidade OU pós-graduação OU graduação OU graduação)	1	0	0	0

SCIELO	(Aprendizaje independiente OR autoaprendizaje OR aprendizaje autónomo OR autorregulación OR aprendizaje autorregulado) and (Universitario OR graduado OR graduación)	29	8	8	8
	(Independent learning OR self-learning OR autonomous learning OR self-regulation OR self-regulated learning OR self-regulated learning) and (University OR graduate OR graduation OR graduation)	0	0	0	0
	(aprendizagem independente OU auto-aprendizagem OU aprendizagem autônoma OU aprendizagem auto-regulada OU aprendizagem auto-regulada OU aprendizagem auto-regulada) e (Universidade OU pós-graduação OU graduação OU graduação)	0	0	0	0
ERIC	(Aprendizaje independiente OR autoaprendizaje OR aprendizaje autónomo OR autorregulación OR aprendizaje autorregulado) and (Universitario OR graduado OR graduación)	5	2	1	1
	(Independent learning OR self-learning OR autonomous learning OR self-regulation OR self-regulated learning OR self-regulated learning) and (University OR graduate OR graduation OR graduation)	94 807	40 893	8	0
	(aprendizagem independente OU auto-aprendizagem OU aprendizagem autônoma OU aprendizagem auto-regulada OU aprendizagem auto-regulada OU aprendizagem auto-regulada) e (Universidade OU pós-graduação OU graduação OU graduação)	67	27	10	0
Total		11 271 889	1 306 790	76	21

Fuente: elaboración propia.

Los criterios de inclusión y exclusión se configuraron teniendo en cuenta los siguientes requisitos: (a) artículos completos sobre el tema aprendizaje autónomo, autorregulado o independiente; (b) textos de acceso abierto; (c) publicaciones en español, inglés y portugués; (d) publicación con revisión por pares; (e) periodo de publicación entre 2011 y 2021; (f) revistas con publicaciones de países iberoamericanos, excepto España; ya que la realidad de la región es muy diferente a un país que pertenece al continente europeo; (g) investigaciones centradas en el público universitario; (h) temas vinculados a la educación y las ciencias sociales; (i) producciones empíricas, excluyendo artículos teóricos, de reflexión y resúmenes de libros. La sistematización del material recogido generó la matriz que caracteriza (a) autor y año; (b)

país de la publicación; (c) palabras clave; (d) dimensiones descritas; (e) instrumentos utilizados; (f) enfoque de la investigación; (g) estrategias; (h) conclusiones. Se excluyeron las disertaciones, tesis, monografías y libros.

Observándose en la Figura 1.

Figura 1. Diagrama de Flujo: Prisma.

Fuente: elaboración propia.

3. RESULTADOS

Los resultados referidos a los 21 artículos encontrados se organizan en dos grandes conjuntos: Evidencias científicas sobre el aprendizaje autónomo identificando autores, país y dimensiones (Tabla 3) y Evidencias

científicas sobre aprendizaje autónomo identificando instrumentos, enfoque, estrategias y conclusiones (Tabla 4), de acuerdo con las preguntas que guían la investigación

Tabla 3. Evidencias científicas sobre el aprendizaje autónomo identificando autores, país y dimensiones.

	Autor/año	País	Palabras clave	Dimensiones
1.	(Daura, 2011)	Argentina	University teaching methodology; teaching strategies; self-regulated learning	Motivacional, Estrategias de aprendizaje, Personalización de los aprendizajes
2.	(Gaxiola y González, 2019)	México	Learning methods; high school students; student adjustment	Actitud positiva, sentido del humor, perseverancia, religiosidad, autoeficacia, optimismo y orientación a la meta
3.	(Ventura <i>et al.</i> , 2017)	Argentina	Estrategias de aprendizaje; patrones de motivación; MSLQe; estudiantado universitario	dimensiones personales (frías y cálidas), dimensiones contextuales (niveles de formación académica)
4.	(Martínez-Sarmiento y Gaeta, 2019)	Colombia y México	Enseñanza superior; autogestión; estrategias de aprendizaje; motivación; tecnologías de la información y de la comunicación	Cognitiva, Motivacional, Estrategias de apoyo, Contextual
5.	(Zambrano, 2016)	Chile	Estrategias de aprendizaje; estrategias metacognitivas; aprendizaje autorregulado; autoeficacia genera	Prácticas de planificación de estudio Prácticas de monitoreo de estudio Prácticas de evaluación de estudio
6.	(Morales-Martínez <i>et al.</i> , 2019)	México	Propensity for academic cheating; learning evaluation; online; face-to-face evaluation; cognitive algebra	El estilo de enseñanza del profesor, el tipo de examen, modalidad de evaluación
7.	(Ríos-Rodríguez <i>et al.</i> , 2021)	Cuba	Trabajo independiente; enseñanza asistida por computadora; sistemas adaptativos; ambiente virtual; sistema multiagente	Planificación, orientación, ejecución y control-evaluación
8.	(Carbonero <i>et al.</i> , 2017)	Brasil	Enseñanza superior; estilo de enseñanza; habilidades docentes; profesor; género	Organización, Comunicación, Habilidades sociales, Resolución de conflictos, Procesos de enseñanza
9.	(Padilla, 2017)	México	Estudiantes de primer ingreso; educación superior; orientación educativa.	Percepción de las preocupaciones de los estudiantes, Identificación de estrategias, Percepción de involucramiento y valoración de la efectividad
10.	(Melo <i>et al.</i> , 2020)	Colombia	ICT; Education; Universities; Colombia	Explorador, Integrador, Innovador
11.	(Cajiao y Burke, 2016)	Colombia	No figura	Método de instrucción, seguridad psicológica, autoeficacia para el rendimiento en clase, demostración de habilidades
12.	(Velasco y Cardeñoso, 2020)	Ecuador	Aprendizaje autorregulado; MSLQ; Género; Niveles educativos; Carreras administrativa	Nivel educativo, motivación y estrategias de aprendizaje

13.	(Naffah <i>et al.</i> , 2016)	Colombia	Aprendizaje virtual; educación superior; percepción; adaptación tecnológica; relación estudiante-profesor	Facilidad de uso (FU), la percepción de utilidad (UP), la actitud frente al uso (ACT) y la intención de uso (INT), la auto eficiencia percibida (PA), la preparación del estudiante (Pest), la disposición a innovar –Personal Innovativeness (PI)– y la percepción de los docentes para utilizar las plataformas virtuales como herramientas de e-learning
14.	(Zambrano-Matamala <i>et al.</i> , 2020)	Chile	Estrategias de autorregulación; aprendizaje autorregulado; enseñanza superior; segmentación social	Hábitos inadecuados de regulación; organización del entorno; búsqueda de información; y organización de la tarea
15.	(González Moreno, 2011)	Colombia	ALEX Virtual English program; blended learning; discussion forums	Interacción a través de los foros de discusión, Práctica de la destreza de escritura en los tableros de discusión
16.	(Chan-Martín y León, 2017)	México	Aprendizaje autorregulado; autorregulación; estudiantes universitarios mayas	Planificación, ejecución y autorregulación
17.	(Valencia <i>et al.</i> , 2013)	Colombia	Metas académicas; autorregulación del aprendizaje; evaluación; rendimiento; estudiantes universitarios	Metas académicas (Metas de dominio por evitación, Metas de dominio por aproximación, Metas de ejecución por evitación, Metas de ejecución por aproximación). Niveles de regulación
18.	(Pool-Cibrián y Martínez-Guerrero, 2013)	México	Autoeficacia percibida; Estrategias de aprendizaje; Educación superior; Análisis de senderos; Teoría de Respuesta al Ítem	Metas de aprendizaje, autoeficacia percibida, problemas de concentración y estrategias de aprendizaje
19.	(Elvira-Valdés y Pujol, 2012)	Venezuela	Autorregulación académica; rendimiento académico; educación superior	Autorregulación académica: planeamiento, control y reflexión
20.	(Sáez <i>et al.</i> , 2018b)	Chile	Aprendizaje autorregulado; disposición al estudio; autoeficacia; atribuciones causales; educación Superior.	Disposición al estudio, atribuciones causales y autoeficacia para la disposición al estudio.
21.	(Mujica <i>et al.</i> , 2017)	Chile	Entrenamiento; Aprendizaje; Universidad; Estrategia; Autorregulado; Autoeficacia; Impacto	Motivación (Aratex), Planificación (Aratex), Gestión del contexto (Aratex), Cognición (Aratex), Evaluación (Aratex), Disposición (IPA), Cognición (IPA), Metacognitivo (IPA), Procesos de autorregulación del aprendizaje, Utilidad de estrategias de Autorregulación, Percepción de autoeficacia autorregulatoria

Fuente: elaboración propia.

Tabla 4. Evidencias científicas sobre aprendizaje autónomo identificando instrumentos, enfoque, estrategias y conclusiones.

	Instrumento	Enfoque	Estrategias	Conclusiones
1.	Cuestionario MSLQ (Motivated Strategies Learning Questionnaire)	Cuantitativo	Se aplicó la Escala MSLQ, en cuyos componentes organización, la regulación del tiempo-entorno de aprendizaje y el repaso, resalta significativo el uso de la estrategia del repaso.	Existen factores que obstaculizan el aprendizaje como la escasa duración de los espacios curriculares, la presencia de varios docentes invitados y una gran carga de contenidos por dictar en cada materia.

2.	Cuestionario MSLQ	Cuantitativo	Se aplicó la Escala MSLQ, en el aspecto aprendizaje autorregulado destacó el componente social y académico, en el desarrollo de estrategias la concentración es muy importante ya que entiende, hace preguntas y se mantiene al tanto.	El apoyo social y académico percibido influye indirectamente en el aprendizaje autorregulado, por lo tanto, es recomendable promover los apoyos sociales y académicos, de la familia y amigos de los adolescentes para incidir en el aprendizaje autorregulado.
3.	Cuestionario MSLQe	Cuantitativo	Se aplicó la Escala MSLQ. En los resultados se observó que la estrategia cognitiva de menor uso por estudiantes es la estrategia de manejo de recursos vinculada a la regulación del esfuerzo y la de mayor uso es la organización. Asimismo, una frecuencia medio-baja en el uso de estrategias de repaso, seguido del pensamiento crítico y manejo del tiempo/elección del ambiente adecuado para estudiar. Finalmente, se obtuvo una frecuencia medio-alta de uso de estrategias de aprendizaje con pares, seguido de búsqueda de ayuda, autorregulación metacognitiva y elaboración.	La formación académica favorece el desarrollo de estrategias de aprendizaje y patrones de motivación en el sentido de una integración jerárquica
4.	MSLQ, Escala de orientación a metas de Skaalvik, inventario de procesos de autorregulación del aprendizaje	Cuantitativo	Se aplicó programa virtual de acompañamiento a través de la Plataforma Moodle, el proceso cuasi experimental consistió en brindar además de contenidos adicionales y diferentes, la interacción en los foros a través del chat, tres veces a la semana. El papel del profesorado fue de mediador.	La eficacia del programa de acompañamiento, ya que el estudiantado que participó en el grupo experimental presentó un aumento significativo en los procesos de autorregulación del aprendizaje en general y, de manera más concreta, en la orientación a metas de adquisición de conocimientos, el gusto por la asignatura, las estrategias de aprendizaje, la utilización de herramientas tecnológicas y el tiempo de estudio, las estrategias de autorregulación del aprendizaje y la percepción del apoyo docente en tareas de formación
5.	Escala de la autoeficacia general	Cuantitativo	Se diseñaron 8 talleres en todos los casos se aplicó una herramienta para planificar, organizar y reflexionar sobre el estudio. Un cuadro que contenía que conoce (C), que quiere (Q) que aprende (A). El estudiantado lee un capítulo del libro o un artículo o resolver un caso práctico preparado por el profesorado. Al inicio completaban la columna C y Q. En el desarrollo (70 minutos) desarrollaban una guía de estudio completando y finalmente al concluir la clase (10 minutos), completaban la columna A del cuadro. El estudiantado trabajaba en equipo y/o en forma individual para obtener un producto. No hubo tareas fuera del aula. De esta forma se trabajó en modalidad de aprendizaje activo y no de forma tradicional por la exposición de diapositivas.	El estudiantado no planifica, ni monitorea su proceso de aprendizaje. Sin embargo, son capaces de evaluar y reflexionar sobre las causas del por qué no realizan una planificación y monitoreo.

6.	El instrumento de álgebra cognitiva, Escala de comportamiento orientado a la meta, Escala de Levenson de Intimidad	Cuantitativo	A todos los participantes del estudio se les proporcionaron descripciones escritas de 12 escenarios relacionados con los criterios de evaluación académica y se les pidió que calificaran la probabilidad de que hicieran trampa en tales circunstancias. Los 12 escenarios reflejaban la manipulación experimental de tres factores ortogonales: el estilo de enseñanza del profesor, el tipo de examen y la modalidad de evaluación.	Se hallaron cuatro actitudes distintas hacia las trampas entre los estudiantes, dos de las cuales eran independientes del contexto (bajo y alto deseo de hacer trampas) mientras que las dos restantes dependían del contexto (bajo y moderado deseo de hacer trampas).
7.	APA-Prolog, Cuestionario elaborado sobre la base teórica del PDTI	Cuantitativo	Se desarrolló una investigación cuasiexperimental en el espacio denominado APA-Prolog. En ella se aloja un conjunto de mapas conceptuales relacionados entre sí, sobre los cuales navega el estudiantado, que encuentra en su travesía disímiles recursos informáticos entre los que se hallan textos explicativos, entrenadores, tutoriales, simuladores y evaluadores. Asimismo, este espacio se desarrolló en cuatro fases: Planificación y determinación del tipo de trabajo independiente, Orientación, Ejecución o participación activa del estudiantado en el trabajo independiente y Control y evaluación. La metodología consistió en la retroalimentación por vía electrónica, mediante correos, foros o chat, también disponibles en el ambiente y la participación en debates propiciado por el profesorado en el aula, tomando como base alguno de los recursos disponibles en el ambiente.	El estudiantado valora positivamente el uso de APA-Prolog como herramienta de apoyo al PDTI, pues ofrece una dinámica de estudio interactiva y participativa.
8.	El Cuestionario de Evaluación Superior (CEVES), El Cuestionario de Evaluación de la Metodología Docente y Evaluativa (CEMEDEPU)	Cuantitativo	El rol del profesorado es primordial para que el estudiantado logre metas académicas ajustadas, autonomía, uso de estrategias de aprendizaje; afectivas, aumentando la motivación y atribuciones; y sociales, mejorando las habilidades sociales, en especial, en la petición de apoyo social. Siendo una estrategia importante el contacto visual en la comunicación con el estudiantado. Y para lograr para el desarrollo integral de un estilo de enseñanza universitaria eficaz, se parte del estilo de enseñar, la personalidad y del pensamiento del profesorado.	El profesorado universitario brasileño enfatiza en mayor grado el contacto visual cuando se comunica con su alumnado, expresando una competencia psico instruccional.
9.	Entrevista simultánea	Cualitativo	Investigación que plantea la presencia del profesorado y del tutor, ambos son piezas que trabajan conjuntamente, se aplicaron exámenes psicométricos que aportan información sobre personalidad, hábitos de estudio, la información se entrega a coordinadores de carrera y a los tutores. Reciben una hora de tutoría semanal, luego una evaluación para encontrar focos rojos que abarca diferentes áreas; académica, o psicosocial. Se usó las redes sociales, como el Facebook, para interactuar con el estudiantado.	Involucrar al estudiantado de manera activa, sin saturarlos de información ni paternalismo; más bien, orientarlos hacia su desarrollo social y académico autónomo

10.	Cuestionario	Cuantitativo	Para lograr una formación permanente es necesario el conocimiento del profesorado, tiempo dedicado por el profesorado, importancia profesional y científica, Innovación tecnológica y didáctica y la accesibilidad para el estudiantado.	Diseñar e impartir una formación permanente y continuada sobre las TIC y su aplicación en el contexto educativo.
11.	Cuestionario de seguridad psicológica	Cuantitativo	Las clases magistrales con tareas de lectura como modo principal de enseñanza, esta instrucción era principalmente teórica y conceptual, y se caracterizaba por el uso regular de vídeos, el control del profesor y la asunción de un papel pasivo por parte del estudiantado, el desarrolló contó con tareas de lectura, uso periódico de vídeos y casos, proyectos en grupos pequeños, debates en grupos pequeños y reflexión guiada sobre las actividades de clase.	Los educadores y formadores deben promover el desarrollo de comportamientos de aprendizaje que mejoren la capacidad de los individuos para afrontar y adaptarse eficazmente a un entorno que cambia rápidamente.
12.	Cuestionario	Cuantitativo	El género femenino puso en práctica más estrategias de aprendizaje ya que son más organizadas al momento de llevar a cabo sus estudios, repasan más y regulan su tiempo y entorno de trabajo.	Disminución de la motivación intrínseca a medida que va concluyendo la carrera universitaria.
13.	Cuestionario	Cuantitativo	Se desarrolló el Modelo de Aceptación a la Tecnología, si bien el estudiantado reconoce que la preparación del profesorado es positiva, tiene una tendencia hacia la neutralidad. El autoaprendizaje y la autonomía son dos condiciones que motivan al estudiante hacia a la innovación pedagógica y didáctica.	Las herramientas virtuales y capacidades del profesorado que los incentivan a utilizarlas, desarrollan estrategias de seguimiento y evaluación en la implementación de estrategias pedagógicas y didácticas para la medicación del proceso de enseñanza-aprendizaje.
14.	Cuestionario, Escala SRSI-SR	Cuantitativo	Al aplicarse el Cuestionario se encontró diferencias para la dimensión hábitos inadecuados de regulación.	El uso de estrategias de autorregulación del aprendizaje depende mayoritariamente de la capacidad percibida y variables personales como el interés por aprender y la utilidad percibida del uso de dichas estrategias.
15.	Entrevistas semiestructuradas	Cualitativo	Se entrevistaron a los estudiantes sobre la percepción de los tableros de discusión como herramienta de comunicación, de acuerdo a las respuestas, se revisaron y corrigieron cada uno de los fragmentos del tablero. Existió una compensación con notas por la interacción en el foro. La actividad en el foro estuvo diseñada en cuatro momentos. El primero el profesorado publica una tarea en el tablero. Segundo, el estudiantado lee las tareas. Tercero, trabajan en ella individualmente antes de publicar sus soluciones completas en el foro de debate. Cuarto, el profesorado corrige todas las intervenciones.	Dos componentes principales: la interacción y la práctica de las habilidades de escritura. La retroalimentación de las actividades fue permanente y exigente, identificando características de un estudiante con aprendizaje autónomo, cuanto más rápida sea la retroalimentación mayor será el aprendizaje y la satisfacción.

16.	Escala interactiva del proceso de enseñanza-aprendizaje (EIPEA)	Cuantitativo	El 45% de los alumnos universitarios, del presente estudio, hacen uso de estrategias de aprendizaje reproductor.	No es el género, ni el idioma de los aprendices, ni bilingües que determina el buen aprendizaje o el aprendizaje eficaz; es la práctica de establecer objetivos, metas, ejecución efectiva de las metas y actividades, la motivación sostenida, el establecimiento de estrategias de aprendizaje y la autorreflexión los que conducen al desarrollo de un nivel de autorregulación de aprendizaje.
17.	Entrevista semiestructurada, Observación directa Protocolos verbales y Evaluación académica y rendimiento	Cuantitativo	Respecto al aprendizaje autorregulado, se encontraron estudiantes con bajos y altos niveles. Aquellos que presentan altos niveles se caracterizan por establecer metas de dominio por aproximación y desplegar esfuerzos cognitivos y metacognitivos.	El abordaje procedimental del aprendizaje autorregulado, en función de las metas académicas, permitió obtener información relevante para la comprensión de este proceso, por lo que se recomienda seguir realizando este tipo de estudios para dar cuenta de los diferentes funcionamientos de las estudiantes universitarias en tiempo real, de sus variaciones y relación con otros aspectos motivacionales involucrados en sus procesos de aprendizaje
18.	Cuestionario de Autoeficacia para el Aprendizaje, SELF-A; Cuestionario de Estrategias para el Aprendizaje Autorregulado, CEPAA	Cuantitativo	El efecto directo de la variable problemas de concentración en las estrategias metacognitivas y de dominio, sugiere que el estudiantado necesita generar un ambiente interno y externo adecuado para lograr concentrarse en sus estudios, así como reflexionar y monitorear las estrategias utilizadas con el fin de adecuarlas a exigencias del contexto.	Existe una interacción de procesos psicológicos en donde varían conjuntamente las metas para el aprendizaje, la autoeficacia percibida y los problemas de concentración. Dichas variables predicen y tienen efectos directos e indirectos sobre otras estrategias de aprendizaje autorregulado.
19.	Escala de Aprendizaje Autorregulado; Encuesta de Datos Sociodemográficos	Cuantitativo	Al obtener ligeras diferencias en el uso de estrategias autorregulatorias del estudiantado del sector privado, en la selección y uso de estrategias relacionadas con la regulación de tiempo, esfuerzo, tareas académicas y ambiente de estudio.	El estudiantado mostró un mejor desempeño en cuanto a la planificación y, en cuanto a las diferencias entre las instituciones públicas y privadas, el grupo de esta investigación se diferenció en el uso de estrategias de control efectivas.

20.	Cuestionario, Escala de Estrategias de Disposición al Estudio	Cuantitativo	La autoeficacia presenta correlaciones fuertes y positivas con las distintas estrategias de disposición al estudio (GTA: Gestión del tiempo académico, ORMA: Organización de recursos materiales y ambientales, AEE: Atribuciones causales de éxito al esfuerzo, AEH: Atribuciones causales de éxito a la habilidad, AEFE: Atribuciones causales de éxito a factores externos, AFE: Atribuciones causales de fracaso al esfuerzo, AFH: Atribuciones causales de fracaso a la habilidad, AFFE: Atribuciones causales de fracaso a factores externos, AE: Autoeficacia en la autorregulación de la disposición al estudio).	El estudiantado con altos niveles de estrategias de disposición al estudio presenta creencias positivas acerca de la propia capacidad para autorregular sus procesos de disposición al estudio, realizan atribuciones causales de sus éxitos principalmente al esfuerzo y disminuyen las explicaciones de fracasos académicos a su esfuerzo, su capacidad y a causas externas.
21.	Escala de utilización de estrategias de autorregulación del aprendizaje, Inventario de procesos de autorregulación del aprendizaje (IPA), Inventario de auto eficacia en autorregulación del aprendizaje	Cuantitativo	La estrategia consistió en ver un video de aproximadamente tres minutos de duración en el que conversan dos estudiantes universitarios acerca de situaciones académicas cotidianas; luego se presenta un cuestionario de auto aplicación; y finalmente se presenta una propuesta de actividad para ordenar y planificar tiempos de estudio o para aplicar procedimientos de estudio. Desarrollado en 10 sesiones, cada una centrada en un punto específico de estrategias de planificación del estudio, estrategias cognitivas o estrategias metacognitivas de aprendizaje, presentadas en la plataforma virtual Moodle.	Las condiciones para mejorar la autorregulación del aprendizaje, son: 1) considerar un conjunto específico de procedimientos; 2) observar evidencias de sus resultados; 3) situarlo en el contexto del aula, en función de los objetivos y condiciones particulares de una determinada asignatura; 4) utilizar las TIC con apoyo del docente de asignatura; y 5) ser propiciado por el docente de la asignatura.

Fuente: elaboración propia.

3.1. EVIDENCIAS CIENTÍFICAS SOBRE EL APRENDIZAJE AUTÓNOMO IDENTIFICANDO AUTORES, PAÍSES Y DIMENSIONES

Los países que presentan evidencias científicas sobre la autonomía universitaria son Colombia (n=6), México(n=5), Chile(n=4), Argentina (n=2), Ecuador, Cuba, Venezuela y Brasil con una sola publicación, siendo necesario una reflexión acerca de la baja producción científica sobre esta temática relevante en el espacio educativo. El número de palabras claves oscilan entre tres y siete, que guardan relación con la temática investigada. Las palabras claves se pueden ubicar en el Tesauro de la Unesco, que hace fácil la ubicación de publicaciones. Asimismo, los autores de las publicaciones aportaron información relevante sobre la temática autonomía del estudiantado universitario, siendo necesario el reconocimiento.

3.2. EVIDENCIAS CIENTÍFICAS SOBRE APRENDIZAJE AUTÓNOMO IDENTIFICANDO INSTRUMENTOS, ENFOQUE, ESTRATEGIAS Y CONCLUSIONES

Estrategias de Planificación

Para lograr el aprendizaje autorregulado es necesario concentrarse (Romero y González, 2019), así como generar ambientes internos y externos adecuados (Pool-Cibrián y Martínez-Guerrero, 2013). Asimismo, otras investigaciones detallan que las estrategias de aprendizaje con pares tiene una alta frecuencia (Ventura *et al.*, 2017). Sin dejar de lado al profesionalismo que cuenta el profesorado que incluye didáctica, conocimientos, tiempo, innovación y accesibilidad (Melo *et al.*, 2020).

Monitoreo

Estrategias del repaso que comprende uso del tiempo y el entorno donde se desarrolla el estudiantado (Daura, 2011). Siendo necesario la interacción con el estudiantado a través de medios digitales, siendo el profesorado el intermediario, resaltando que el acompañamiento es vital en el proceso de aprendizaje (Martínez-Sarmiento y Gaeta, 2019). La retroalimentación es un factor importante en la interacción profesorado y estudiantado, la utilización de foros, chat y medios electrónicos facilita el aprendizaje. La presencia del profesorado es vital en esta metodología APA-Prolog (Ríos-Rodríguez *et al.*, 2021). Esta presencia se evidencia cuando existe el contacto visual en la comunicación de esta manera se desarrolla la competencia psicoinstruccional (Ríos-Rodríguez *et al.*, 2021). En esta etapa se puede identificar focos rojos en el área académica o psicosocial utilizando redes sociales que facilitan la interacción (Padilla, 2017). La reproducción permanente es otra estrategia de lograr la autonomía (González, 2011).

Evaluación

La actividad de leer y resolver un caso, para luego completar la guía propuesta de manera individual o colectiva, refleja un proceso de aprendizaje autónomo. Si no se logra el desarrollo de estos procesos entonces se evidenciará que el estudiando no planifica ni monitorea (Zambrano, 2016). Es evidente

que todo proceso de aprendizaje pasa por la evaluación, pero hacer trampas revela inseguridad. Siendo necesario el estilo de enseñanza del profesorado, el tipo de evaluación y modalidad (Morales-Martínez *et al.*, 2019). El corregir todas las participaciones y brindar un puntaje o puntuación por hacerlo es parte de la evaluación que cada vez se vuelve más exigente, de esta manera se logra el aprendizaje autónomo, cuando más rápido se atiende al estudiante mayor será su aprendizaje (González, 2011).

Enfoque e Instrumentos

Los instrumentos utilizados en las investigaciones sobre autonomía desde el año 2011 al 6 de abril 2021, son variados al igual que los enfoques. Destaca el cuestionario Motivated (M), Strategies (S), Learning (L), Questionnaire (Q), por sus siglas en inglés MSLQ, aplicados a investigaciones con enfoque cuantitativo (Daura, 2011; Gaxiola y González, 2019; Ventura *et al.*, 2017; Martínez-Sarmiento y Gaeta, 2019). Asimismo, la Escala SRSI-SR (Zambrano-Matamala *et al.*, 2020), Escala de orientación a metas de Skaalvik, donde se identifica los procesos de autorregulación del aprendizaje (Gaeta, 2019), Escala de autoeficacia (Zambrano, 2016), Escala de comportamiento orientado a la meta (Morales-Martínez *et al.*, 2019), El Cuestionario de Evaluación de las Variables de los estilos de enseñanza en la Educación Superior (CEVES) (Carbonero *et al.*, 2017), Escala interactiva del proceso de enseñanza-aprendizaje, por sus siglas EIPEA (Chan-Martín y León, 2017), Cuestionario de Autoeficacia para el aprendizaje SELF-A y cuestionario de estrategias para el aprendizaje autorregulado, por sus siglas CEPAA (Pool-Cibrián y Martínez-Guerrero, 2013; Mujica *et al.*, 2017), Escala de estrategias de disposición al estudio (Sáez *et al.*, 2018b), y finalmente entrevistas semiestructuradas para los enfoques cualitativos (González, 2011) o entrevistas simultáneas (Padilla, 2017).

Respecto a los enfoques e instrumentos, a pesar de la riqueza y variedad existe el predominio del enfoque cuantitativo. Respecto a los instrumentos se evidencian escalas, cuestionarios y/o entrevistas. Asimismo, se observa investigaciones cualitativas que profundizan la dinámica del aprendizaje autorregulado, categorías o dimensiones como la planificación, el seguimiento consciente y la autoevaluación que implican y están presentes en los procesos educativos.

4. DISCUSIÓN Y CONCLUSIONES

El objetivo de este estudio fue sistematizar la evidencia científica sobre la autonomía de los estudiantes universitarios, considerando las estrategias metodológicas y los instrumentos utilizados. Las estrategias de autorregulación o autonomía a nivel universitario se logran a través de varios factores como la experticia, el conocimiento y la disposición del profesorado, que facilitan el aprendizaje del estudiantado (Melo *et al.*, 2020), de esta manera obtiene seguridad. Si el profesorado se involucra en el desarrollo de las competencias entonces logra en el estudiantado la autorrealización posición que coincide con Sáez *et al.* (2018a). El acompañamiento permanente o la disposición que tenga el profesorado se observa en las conclusiones que coinciden con Enríquez y Hernández (2021).

La literatura apunta a favorecer los procesos de intervención propuestos por el profesor como organizador del aprendizaje y mediador del conocimiento y, sobre todo, a promover aspectos pedagógicos que impliquen la autorregulación del aprendizaje en los alumnos. Así, el profesor que conoce las dinámicas implicadas en el aprendizaje autónomo fortalece en el escenario educativo, la adopción de la planificación, el seguimiento y la autoevaluación o autorreflexión de los procesos de adquisición de conocimientos en sus alumnos.

Para lograr el aprendizaje autónomo, no solo es necesario el apoyo del profesorado también es necesario la presencia de la familia, amigos (Gaxiola y González, 2019), posición que coincide con de Carbonero *et al.* (2017) quienes destacan el papel diferenciado del profesorado en la calidad del aprendizaje y las interacciones sociales proporcionadas, destinadas al apoyo social y la posición de Padilla (2017) quien además del profesorado, menciona la acción diferenciada del tutor en el proceso autorregulado en la perspectiva psicosocial.

Entre las dificultades que tiene el estudiantado para lograr el aprendizaje de manera virtual son la presencia profesorado invitado, carga de contenidos (Daura, 2011) aunado a la conectividad, por ello es necesario que desarrolle el aprendizaje autónomo, resultado que coincide con Bravo y Quesada (2021).

Zambrano (2016), identificó que los académicos no planifican ni monitorean el proceso de aprendizaje, por lo que tienen dificultades para caracterizar los factores que influyen en el proceso de autorregulación. Estas situaciones señalan la importancia de que los profesores conozcan el proceso de aprendizaje autorregulado y empleen estrategias pedagógicas y metodológicas para promover la autonomía del aprendizaje, posiciones que coinciden con Boruchovitch (2014) y Ganda y Boruchovitch (2018).

Respecto a la metodología, la revisión sistemática identificó que hay un predominio de estudios cuantitativos y Zimmerman (2008), destacó la necesidad de utilizar enfoques diversificados y en lo posible promover la triangulación de las informaciones para ampliar la investigación sobre un fenómeno. Finalmente, el papel del aprendizaje autorregulado posibilita la mejora de las estrategias pedagógicas que fomentan la organización de contextos de aprendizaje en el estudiantado y el profesorado que experimentan la proactividad, el trabajo en grupo, la motivación y la autorreflexión.

De acuerdo al planteamiento de los diversos autores sobre estrategias para lograr la autonomía, se concluye que es necesario la presencia de dos actores: el profesorado y el estudiantado. El profesorado que brinda su experiencia, su formación académica y acompañamiento sistemático. Y el estudiantado desarrolla habilidades de planificación, concentración, motivación y reflexión sobre el aprendizaje. A pesar que el estudiantado no siente la presencia física del profesorado desarrolla diversas estrategias que fomentan el aprendizaje autónomo.

Los resultados sobre los instrumentos utilizados en las investigaciones desde el año 2011 hasta el 2021, indican que la mayoría de investigadores utilizaron el cuestionario de Motivated Strategies Learning Questionnaire (MSLQ), cuestionario que fue diseñado por Pintrich *et al.*, en 1988. Pero, el objetivo de usar este instrumento fue evaluar las motivaciones y estrategias de aprendizaje. Siendo necesario caracterizar las estrategias más utilizadas por el estudiantado universitario, de acuerdo a la carrera o disciplina de estudio, ya que cada área del conocimiento tiene diversas formas de desarrollarse. En ella se identifica aciertos y desaciertos logrando la independencia en sus estudios, siendo necesario utilizar todas las herramientas tecnológicas, que presenta la virtualidad.

AGRADECIMIENTOS

Las autoras agradecen a la Universidad César Vallejo del Perú, por el apoyo constante al fomento de las investigaciones. Esta investigación se desarrolló bajo el marco de pertenecer al Grupo de Investigación Educación Virtual que desarrolla investigaciones que fortalecen el ámbito educativo.

REFERENCIAS BIBLIOGRÁFICAS

- Boruchovitch, E.** (2014). Autorregulação da aprendizagem: Contribuições da psicologia educacional para a formação de professores. *Psicologia Escolar e Educacional*, 18(3), 401–409. <https://doi.org/10.1590/2175-3539/2014/0183759>
- Boruchovitch, E., y Santos, A. A. A.** (2015). Psychometric Studies of the Learning Strategies Scale for University Students. *Paidéia (Ribeirão Preto)*, 25(60), 19-27. <https://doi.org/10.1590/1982-43272560201504>
- Bravo, F., y Quezada, T.** (2021). Educación virtual en la universidad en tiempos de Covid-19. *Espíritu Emprendedor TES*, 5(1), 154–166. <https://doi.org/10.33970/cetes.v5.n1.2021.238>
- Cajiao, J., y Burke, M. J.** (2016). How instructional methods influence skill development in management education. *Academy of Management Learning and Education*, 15(3), 508–524. <https://doi.org/10.5465/amle.2013.0354>
- Carbonero, M. A., Martín-Antón, L. J., Flores, V., y Freitas, A.** (2017). Estudio comparado de los estilos de enseñanza del profesorado universitario de ciencias sociales de España y Brasil. *Revista Complutense de Educación*, 28(2), 631–647. https://doi.org/10.5209/rev_RCED.2017.v28.n2.50711
- Chan-Martín, E. D., y León, E. E.** (2017). Exploración del proceso de aprendizaje autorregulado de estudiantes universitarios mayahablantes. *IE Revista de Investigación Educativa de La REDIECH*, 8(14), 91–110. https://doi.org/10.33010/ie_rie_rediech.v8i14.37

- Donato, H., y Donato, M.** (2019). Etapas na condução de uma revisão sistemática. *Acta Médica Portuguesa*, 32(3), 227-235. <https://doi.org/10.20344/amp.11923>
- Daura, F.** (2011). Las estrategias docentes al servicio del desarrollo del aprendizaje autorregulado. *Estudios Pedagógicos (Valdivia)*, 37(2), 77–88. <https://doi.org/10.4067/s0718-07052011000200004>
- Elvira-Valdés, M. A., y Pujol, L.** (2012). Autorregulación y rendimiento académico en la transición secundaria-universidad. *Latinoamericana, Revista Sociales*, 10(1), 367–378. <http://www.scielo.org.co/pdf/pepsi/v11n2/v11n2a04.pdf>
- Enríquez, L., y Hernández, M.** (2021). Alumnos en pandemia: una mirada desde el aprendizaje autónomo. *Digital Universitaria*, 22(2). <https://doi.org/10.22201/cuaieed.16076079e.2021.22.2.11> Universidad
- Gámiz-Sánchez, V-M., Gallego-Arrufat, M-J., y Crisol-Moya, E.** (2016). Impact of electronic portfolios on prospective teachers' participation, motivation and autonomous learning. *Journal of Information Technology Education: Research*, 15, 517-533. <http://www.informingscience.org/Publications/3575>
- Ganda, D. R. y Boruchovitch, E.** (2018). A autorregulação da aprendizagem: principais conceitos e modelos teóricos. *Psicologia da Educação*, 46, 331-340. <https://doi.org/10.5935/2175-3520.20180008>
- Gaxiola, J. C., y González, S.** (2019). Perceived support, resilience, goals, and self-regulated learning in high school students. *Revista Electrónica de Investigación Educativa*, 21(1), 1–10. <https://doi.org/10.24320/REDIE.2019.21.E08.1983>
- González, R. I.** (2011). The Role of Discussion Boards in a University Blended Learning Program. *Profile Issues in Teachers' Professional Development*, 13(1), 157-174. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1657-07902011000100010&lng=en&tylng=en

- Lima, C. S., y Santiba, C.** (2020). Analysis of the scientific production of academic self-regulation learning in the educational context. *Eccos*, (55), 1–17. <https://doi.org/10.5585/eccos.n55.8210>
- López M. A., y Moya, E.C.** (2012). Las guías de aprendizaje au tónomo como herramienta didáctica de apoyo a la docencia. *Escuela Abierta*, 15, 9-31. <https://dialnet.unirioja.es/servlet/articulo?codigo=4078711>
- Maciel, A. G., y Alliprandini, P. M. Z.** (2017). Estratégias de autorregulação no ensino superior brasileiro: análise da produção científica de pesquisas interventivas. *Anais do XVII SEDU, Semana de Educação da UEL*, Londrina, PR, Brasil, 1817-1823.
- Martínez-Sarmiento, L. F., y Gaeta, M. L.** (2019). Utilización de la plataforma virtual Moodle para el desarrollo del aprendizaje autorregulado en estudiantes universitarios. *Educar*, 55(2), 479–498. <https://www.raco.cat/index.php/Educar/article/view/v55-n2-martinez-sarmiento-gaeta>
- Monnerat, J. C. Q., Pessoa, M. T. R., y Ferreira, J. A. G. A.** (2016). Autorregulação da Aprendizagem na Educação a Distância: Análise das Produções Científicas Realizadas em Brasil e Portugal no Período de 2010 a 2015. *EaD Em Foco*, 6(2). <https://doi.org/10.18264/eadf.v6i2.377>
- Melo, E., Llopis, J., Gascó, J., y González, R.** (2020). Integration of ICT into the higher education process: The case of Colombia. *Journal of Small Business Strategy*, 30(1), 58-67. <https://libjournals.mtsu.edu/index.php/jsbs/article/view/1665>
- Morales-Martinez, G. E., Lopez-Ramirez, E. O., Mezquita-Hoyos, Y. N., Lopez-Perez, R., y Lara, A. Y.** (2019). Cognitive mechanisms underlying the engineering students' desire to cheat during online and onsite statistics exams. *European Journal of Educational Research*, 8(4), 1145–1158. <https://doi.org/10.12973/eu-jer.8.4.1145>

- Mujica, A. D., Villalobos, M. V. P., González-Pienda, J. A., y Núñez, J. C.** (2017). Impacto de un entrenamiento en aprendizaje autorregulado en estudiantes universitarios. *Perfiles Educativos*, 39(157), 87–104. <https://doi.org/10.22201/iisuc.24486167e.2017.157.58442>
- Naffah, S. C., Arias, A. V., Hernández, J. B., y Ortega, C. M.** (2016). Percepciones estudiantiles acerca del uso de nuevas tecnologías en instituciones de Educación Superior en Medellín. *Revista Lasallista de Investigación*, 13(2), 151–162. <https://doi.org/10.22507/rli.v13n2a14>
- Padilla, L. E.** (2017). La incorporación a la universidad de los estudiantes en Aguascalientes. La perspectiva del orientador educativo. *Revista Electrónica de Educación*, 1(19), 1–19. <http://search.ebsco-host.com/login.aspx?direct=true&db=a9hy&AN=122475701&lang=es&site=eds-live>
- Panadero, E.** (2017) A Review of Self-regulated Learning: Six Models and Four Directions for Research. *Frontier in Psychology*, 8(422), 1-28. <https://doi.org/10.3389/fpsyg.2017.00422>
- Polydoro, S. A. J., y Azzi, R. G.** (2009). Autorregulação da aprendizagem na perspectiva da teoria sociocognitiva: introduzindo modelos de investigação e intervenção. *Psicologia Da Educação*, 29, 75–94. <https://doi.org/1414-6975>
- Polydoro, S. A. J., Fior, C. A., Pelissoni, A. M. S., y Rosário, P. S. L.** (2019). Autorregulação da aprendizagem: adaptação e evidências de validade de instrumentos para universitários brasileiros. *Educação em Análise*, 4(1), 21-42. <https://doi.org/10.5433/1984-7939.2019v4n1p21>
- Pool-Cibrián, W.J., y Martínez-Guerrero, J. I.** (2013). Autoeficacia y uso de estrategias para el aprendizaje autorregulado en estudiantes universitarios. *Revista electrónica de investigación educativa*, 15(3), 21-36. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1607-40412013000300002&lng=es&lng=

- Ríos-Rodríguez, L. R., Román-Cao, E., y Pérez-Medinilla, Y. T.** (2021). La dirección del trabajo independiente mediante el ambiente de enseñanza-aprendizaje adaptativo APA-Prolog. *Revista Electrónica Educare*, 25(1), 1–22. <https://doi.org/10.15359/rec.25-1.11>
- Sáez, F. M., Bustos, C. E., Pérez, M. V., Mella, J. A., Lobos, K. A., y Díaz, A. E.** (2018a). Disposición al estudio, autoeficacia y atribuciones causales en estudiantes universitarios chilenos. *Propósitos y Representaciones*, 6(1), 199–221. <https://doi.org/10.20511/pyr2018.v6n1.179>
- Sáez, F. M., Díaz, A. E., Panadero, E., y Bruna, D. V.** (2018b). Revisión sistemática sobre competencias de autorregulación del aprendizaje en estudiantes universitarios y programas intracurriculares para su promoción. *Formación Universitaria*, 11(6), 83–98. <https://doi.org/10.4067/S0718-50062018000600083>
- Salgado, F. A. F., Polydoro, S. A. J., y Rosário, P.** (2018). Programa de promoção da aprendizagem autorregulada em alunos calouros do ensino superior. *Psico-USF*, 23(4), 667-679. <https://dx.doi.org/10.1590/1413-82712018230407>
- Silva, J., y Simão, A. M. V.** (2016). Entrevista com tarefa na identificação de processos na aprendizagem autorregulada. *Psicologia Escolar e Educacional*, 20(1), 89-100. <https://doi.org/10.1590/2175-3539/2015/0201932>
- Valencia, M., Duarte, J., y Caicedo, A. M.** (2013). Aprendizaje autorregulador metas académicas y rendimiento en evaluaciones de estudiantes universitarios. *Aprendizaje Autorregulado, Metas Académicas y Rendimiento En Evaluaciones de Estudiantes Universitarios*, 11(2), 53–70. <https://doi.org/10.111144/428>
- Velasco, C., y Cardeñoso, O.** (2020). Evaluación de la competencia de aprendizaje autorregulado en función del nivel educativo y el género de alumnado de carreras administrativas. *Perfiles Educativos*, 42(169), 8–20. <https://doi.org/10.22201/iisue.24486167e.2020.169.58687>

- Ventura, A. C., Cattoni, M. S., y Borgobello, A.** (2017). Aprendizaje autorregulado en el nivel universitario: Un estudio situado con estudiantes de psicopedagogía de diferentes ciclos académicos. *Revista Electrónica Educare*, 21(2), 1–20. <https://doi.org/10.15359/rec.21-2.15>
- Wigfield, A., Klauda, S. L., y Cambria, J.** (2011). Influences on the development of academic self-regulatory processes. In B. J. Zimmerman y D. H. Schunk (Eds.), *Educational psychology handbook series. Handbook of self-regulation of learning and performance* (p. 33–48). Routledge/Taylor y Francis Group.
- Zambrano-Matamala, C. M., Díaz-Mujica, A. M., Pérez-Villalobos, M. V., y Rojas-Díaz, D.** (2020). Analysis of self-regulation strategies in pedagogy students from a Chilean university. *Formación Universitaria*, 13(5), 223–232. <https://doi.org/10.4067/S0718-50062020000500223>
- Zambrano, C.** (2016). Autoeficacia, prácticas de aprendizaje autorregulado y docencia para fomentar el aprendizaje autorregulado en un curso de ingeniería de software. *Formación Universitaria*, 9(3), 51–60. <https://doi.org/10.4067/S0718-50062016000300007>
- Zimmerman, B. J.** (1998). Academic Studing and the Development of Personal Skill: A self-regulatory perspective. *Educational Psychologist*, 33(2/3), 73-86. https://doi.org/10.1207/s15326985ep3302y3_3
- Zimmerman, B. J.** (2008). Investigating self-regulation and motivation: Historical background, methodological developments, and future prospects. *American Educational Research Journal*, 45(1), 166-183. <https://doi.org/10.3102/0002831207312909>
- Zimmerman, B. J.** (2013). From Cognitive Modeling to Self-Regulation: A Social Cognitive Career Path. *Educational Psychologist*, 48(3), 135-147. <https://doi.org/10.1080/00461520.2013.794676>
- Zoltowski, A. P. C., y Teixeira, M. A. P.** (2020). Desenvolvimento da autorregulação da aprendizagem em estudantes universitários: um estudo qualitativo. *Psicologia em Estudo*, 25, e47501. <https://doi.org/10.4025/psicolestud.v25i0.47501>

/02/

CIBERSEGURIDAD EN PLATAFORMAS EDUCATIVAS INSTITUCIONALES DE EDUCACIÓN SUPERIOR DE LA PROVINCIA DE TUNGURAHUA - ECUADOR

CYBERSECURITY FOR LEARNING PLATFORMS IN HIGHER EDUCATION INSTITUTIONS IN TUNGURAHUA PROVINCE OF ECUADOR

Pablo Israel Morales-Paredes

Coordinador de Carrera de Desarrollo de Software Instituto Superior Tecnológico Pelileo, (Ecuador).

E-mail: pimorales@institutos.gob.ec ORCID: <https://orcid.org/0000-0003-2150-4585>

Patricio Medina-Chicaiza

Docente de la Escuela de Ingeniería de Sistemas, Pontificia Universidad Católica del Ecuador Sede Ambato.

Grupo de Investigación de Desarrollo Territorial, Empresa e Innovación (DeTEI),

Facultad de Ciencias Administrativas de la Universidad Técnica de Ambato, (Ecuador).

E-mail: pmolina@pucesa.edu.ec / ricardopmedina@uta.edu.ec ORCID: <https://orcid.org/0000-0002-2736-8214>

Recepción: 02/05/2021 **Aceptación:** 31/05/2021 **Publicación:** 29/06/2021

Citación sugerida:

Morales-Paredes, P. I., y Medina-Chicaiza, P. (2021). Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador. *3C TIC. Cuadernos de desarrollo aplicados a las TIC*, 10(2), 49-75. <https://doi.org/10.17993/3ctic.2021.102.49-75>

RESUMEN

El objetivo de esta investigación es desarrollar un procedimiento de gestión de seguridad para las plataformas educativas de los Institutos Tecnológicos Superiores públicos de la provincia de Tungurahua, el cual ayude a identificar las vulnerabilidades y riesgos de ciberseguridad a fin de brindar protección a sus plataformas educativas. En el desarrollo de la presente investigación se determinó que los ITS no cuentan con una designación exclusiva de un docente a tiempo completo para el manejo y gestión de ciberseguridad de las plataformas educativas. Por lo tanto, para el desarrollo de esta propuesta se aplicó la metodología de investigación documental a fin de seleccionar las mejores normas y metodologías como soluciones en materia de ciberseguridad. Mediante la combinación del marco de control en ciberseguridad de la norma ISO27032:2012 y la metodología MAGERIT v3.0, se estableció tres áreas de afectación que implican directamente a las aplicaciones web educativas: 1. Administración del Sistema, 2. Aplicaciones Web, 3. Usuarios. Una vez identificadas estas áreas se plantean salvaguardas necesarias para mitigar los riesgos de seguridad.

PALABRAS CLAVE

Ciberseguridad, Plataforma Educativa, Entorno Virtual, Aplicaciones Web.

ABSTRACT

The main objective of this investigation is to develop a security management procedure for educational platforms of the public Higher Technological Institutes (HTI) of the Tungurahua province. This investigation can help to identify vulnerabilities and cybersecurity risks in order to provide protection to their educational platforms. During this study, the results determined that HTIs do not have full-time teachers, who are in charged for the management of the cybersecurity of their educational platforms. Therefore, this proposal applied desk-based research in order to select the best standards and methodologies as solutions for cybersecurity. Through the combination of the cybersecurity control framework of the ISO27032:2012 standard and the MAGERIT v3.0 methodology, this study established three areas of impact which directly involve educational web applications: 1. System Management, 2. Web Applications, 3. Users. After the identification of these areas, it is necessary to establish safeguards to mitigate security risks.

KEYWORDS

Cybersecurity, Educational Platform, Virtual Environment, Web Applications.

1. INTRODUCCIÓN

En el Ecuador el Consejo de Educación Superior (CES) es el organismo encargado de planificar, regular y coordinar el sistema de Educación Superior mediante la Ley Orgánica de Educación Superior (LOES) la cual garantiza una Educación de calidad. Estas garantías se detallan claramente en su Art. 8, literal a) correspondiente a los fines de la Educación Superior, en donde se aportará al desarrollo del pensamiento universal, al despliegue de la producción científica, de las artes y de la cultura y a la promoción de las transferencias e innovaciones tecnológicas. Por su parte la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) es la responsable de velar que los fines de la Educación Superior se cumplan a través de la elaboración, ejecución y evaluación de políticas, programas y proyectos que deben verse plasmados para garantizar la educación de calidad.

Los Institutos Tecnológicos son parte del Sistema de Educación Superior conforme a lo establecido en el artículo 352 de la Constitución de la República del Ecuador, siendo regulados por el CES. En la Provincia de Tungurahua existen 13 Institutos Superiores Tecnológicos (IST), de los cuales 9 son de carácter público, de un total de 200 Institutos a nivel nacional, según datos recogidos en la página del CES. Estas instituciones han tenido un crecimiento significativo en los últimos años ya que según el Art. 118 literal b) de la LOES habilita a los Institutos Tecnológicos a otorgar títulos de tercer nivel. Esto implica que las Instituciones de Educación Superior deben promover la creación, desarrollo, transmisión y difusión de la ciencia, la técnica, la tecnología y la cultura claramente detallado en el Art 12. Literal b) de la LOES. Para su ejecución es determinante la transferencia e innovación tecnológica mediante la utilización de las Tecnologías de la Información y la Comunicación (TIC), fundamentales dentro la educación superior ecuatoriana.

La infraestructura digital actual permite la conectividad en línea mediante las aplicaciones móviles, en donde los estudiantes se integran hacia las nuevas experiencias del estudio remoto mediante plataformas educativas disponibles para gestión y conexión académica en cualquier parte del mundo, lo cual brinda una oportunidad para que los profesores implementen nuevas estrategias de enseñanza – aprendizaje

enmarcadas en las limitaciones del contexto virtual. Esta realidad es la puerta de la educación remota fortalecida a raíz de la pandemia del COVID-19; a pesar de que aún existen problemas conectividad a internet en las áreas rurales (Lockee, 2021). Sin embargo, Abrigo-Córdova, Granados-Gómez, Donald Sánchez-Sulú, y Celi-Vivanco (2019) mencionan que la mayoría de las instituciones educativas de nivel superior usan las plataformas de manera exclusiva para la preparación académica; de tal manera que incrementa la posibilidad de los ataques informáticos y violaciones de seguridad en las plataformas web educativas.

El estudio realizado por Chhetri y Motti (2020) indica que entre los medios electrónicos más vulnerables en una red doméstica son las tablets, teléfonos inteligentes, computadoras de escritorio, portátiles y routers; debido a los siguientes factores: fuga de información, manipulación de datos, fallas en la interfaz de voz, detección del comportamiento del usuario, interrupción y las más relevante de todas, la autenticación de las cuentas de usuario, ya que no disponen con medidas de seguridad apropiadas y utilizan mecanismos simples tales como contraseñas débiles, credenciales predeterminadas como sus nombres o año de nacimiento; esto puede ser un error muy grave por parte del usuario, al momento de precautelar su información confidencial.

En el Ecuador no se ha desarrollado aún una estrategia nacional de ciberseguridad, que permita establecer los lineamientos, objetivos y plan de acción necesario para proteger los servicios, la información, las infraestructuras críticas y a los usuarios frente a ciber amenazas en el ciberespacio (Zambrano y Zambrano, 2019). Esta consideración también abarca a las Instituciones de Educación Superior a pesar de haber sido declarada en el Ecuador a la Ciberseguridad como política pública. Por lo tanto, existen aspectos que deben ser tomados en cuenta para proteger nuestros datos en la web. Con base al estudio de Redrován *et al.* (2018), el cual identifica a la accesibilidad, confiabilidad, seguridad y eficiencia como parte de las características de calidad que deben tener aplicaciones web, dado que en los últimos cinco años se ha experimentado un crecimiento en el uso de diferentes aplicaciones web y móviles en los Institutos Tecnológicos Superiores (ITS) dentro de la Provincia de Tungurahua.

La problemática se ha identificado mediante una entrevista realizada a los docentes encargados de TIC de los IST públicos de las ciudades de Ambato, Pelileo, Patate y Baños pertenecientes a la provincia del Tungurahua, en donde se evidencia que no cuentan con una designación exclusiva de un docente a tiempo completo para el manejo de las plataformas educativas, lo cual conlleva a tener riesgos de ciberseguridad en sus plataformas. Adicionalmente el personal no está capacitado y preparado para proponer un plan de respuesta a incidentes informáticos. Por tanto, los beneficiarios directos son los encargados de TIC de los ITS Públicos de la Provincia de Tungurahua, con estrategias para la administración segura de sus plataformas. En cambio, los beneficiarios indirectos son sus docentes y estudiantes, quienes accederán a las plataformas web educativas de manera segura y confiable por que se garantiza la integridad de su información.

El objetivo de esta investigación es desarrollar un procedimiento de gestión de seguridad para las plataformas educativas, la cual reduzca vulnerabilidades y riesgos de ciberseguridad en los Institutos Tecnológicos Superiores públicos de la provincia de Tungurahua.

2. METODOLOGÍA

La revisión empírica de los elementos teóricos se realizó mediante una búsqueda bibliográfica en Scielo, Scopus, Google Scholar y Microsoft Academic Search, en donde se pudo recopilar la información de la Ciberseguridad en aplicaciones educativas web, mediante la utilización del software Perish (Harzing, 2020). Para la búsqueda se consideró las siguientes palabras clave en los idiomas español e inglés como: ciberseguridad en aplicaciones web (cybersecurity in web applications), ciberseguridad en la educación Superior (cybersecurity in higher education), seguridad en plataformas educativas (security in educational platforms) dentro de los últimos diez años, tiempo en que la ciberseguridad ha tomado más fuerza y significancia. A continuación, se detalla en el cuadro resumen las métricas de la investigación que fueron encontradas:

Tabla 1. Métricas de la búsqueda realizada.

	Español	Inglés
Años de publicación	2010-2020	2010-2020
Años de las citas	10(2010-2020)	10(2010-2020)
Cantidad de documentos	999	1000
Citas	610	106153
Citas/Año	61.10	10615.30
Citas/Documentos	0.61	106.15
Autores/	1.51	2.81

Fuente: a partir de Perish (Harzing, 2020).

Cabe mencionar que del total de 1999 publicaciones encontradas sobre la temática de estudios se identifica que existe una mínima diferencia en el desarrollo de artículos y libros en español que en inglés. Pero se evidencia que existe un número mayor de publicaciones citadas en el idioma inglés, lo cual indica el nivel de desarrollo y madurez en términos de ciberseguridad en esa lengua.

Figura 1. Citas en Español vs Citas en Inglés.
Fuente: a partir de Perish (Harzing, 2020).

El estudio de la Ciberseguridad y su aplicación en los ITS de la Provincia de Tungurahua tiene el propósito de determinar el nivel de Seguridad con el que cuenta el acceso a la información Institucional

además de conocer los riesgos, amenazas y vulnerabilidades de los sistemas de aprendizaje virtual. Mediante la utilización de la metodología MAGERIT V3.0 propuesta en el estudio de la Seguridad en entornos virtuales de Santiso, Koller, y Bisaro (2016), se pretende definir los incidentes más comunes en ciberseguridad en las aplicaciones web de los ITS. Esto permite plantear medidas de corrección en base a los controles sugeridos en la Norma ISO 27032 para proteger los sistemas en su integridad, disponibilidad y confiabilidad en el manejo de la información.

3. RESULTADOS

3.1. ESTADO DEL ARTE

Es importante analizar los principales aportes teóricos sobre la ciberseguridad y su campo de desarrollo a lo largo de su historia. A continuación, se detallan cuatro apartados relevantes como son: 1.- Estudio de la Ciberseguridad; 2.- Aplicaciones web educativas; 3.- Ciberseguridad educativa en el Ecuador; 4.- Normas y Metodologías para la prevención y respuesta a incidentes de ciberseguridad en plataformas web educativas. Este estudio abre un camino importante para definir un procedimiento metodológico basado en una norma de calidad, en donde se define controles de ciberseguridad para salvaguardar los sistemas y aplicaciones web dentro de los IST de la provincia de Tungurahua.

3.2. ESTUDIO DE LA CIBERSEGURIDAD

La Ciberseguridad a lo largo de su evolución ha tenido diferentes áreas de estudio, de las cuales se ha identificado tres con más relevancia en investigaciones a nivel mundial con una relación respecto al estudio específico de las ciber amenazas y soluciones de ciberseguridad.

Tabla 2. Áreas de Estudios en Ciberseguridad.

Áreas de Estudio en Ciberseguridad	Estudio de amenazas (autores)	t	Soluciones de Ciberseguridad (autores)	t
------------------------------------	-------------------------------	---	--	---

Aplicaciones Web	(Hernández Moreno, 2017) ; (Jang-Jaccard y Nepal, 2014) ; (Mulligan y Schneider, 2011) ; (Juarez, 2019) ; (ENISA, 2020)	4	(Crescenzi-Lanna, Valente, y Suárez-Gómez, 2019) ; (Romero Moreno, 2010) (Barea <i>et al.</i> , s.f.) ; (Santiso <i>et al.</i> , 2016) ; (Zambrano y Zambrano, 2019) ; (MAGERIT, 2012) ; (Li <i>et al.</i> , 2019)	7
			Aplicaciones Educativas	
			(Zambrano y Zambrano, 2019) ; (Santiso <i>et al.</i> , 2016) ; (Haz <i>et al.</i> , 2019) ; (Congacha y García, 2017)	4
Infraestructura Redes	(Lewis, 2006) ; (Roldán-Molina, Almache-Cueva, Silva-Rabadão, Yevseyeva y Basto-Fernandes, 2017)	2	(Vega Villacís y Ramos Morocho, 2017) ; (Zambrano y Zambrano, 2019) ; (Carlini, 2016) ; (Vargas, Recalde, y Reyes, 2017) ; (Mirkovic y Benzel, 2012) ; (Grossman <i>et al.</i> , 2015) ; (Arango, 2020) ; (Ramirez y Venkataramanan, 2019)	8
			Aplicaciones Educativas	
			(Mirkovic y Benzel, 2012)	1
Seguridad en la nube	(Carlini, 2016) ; (Aguilar, 2011) (Seefeldt y Tadoro, 2019) ; (Antonio <i>et al.</i> , 2016)	4	(Juarez, 2019)	1

Fuente: elaboración propia.

Se ha identificado que la mayor parte de estudios en ciberseguridad están enmarcados en brindar soluciones a las aplicaciones web e infraestructura de redes, las cuales son las más afectadas por los ciber ataques. Estos estudios abren una puerta para continuar con el desarrollo de procedimientos que permitan estar preparados a los continuos y futuros ataques de los cuales los sistemas e infraestructuras sufren todos los días. Además, existen muy pocos estudios con procedimientos que ofrezcan mitigar los riesgos de ciberseguridad en aplicaciones web o entornos educativos.

3.2.1. APLICACIONES WEB EDUCATIVAS

BENEFICIOS

Las aplicaciones web educativas o e-learning, se pueden definir como una forma de enseñanza-aprendizaje que hace uso de las nuevas tecnologías disponibles para vincular la planificación académica con un entorno educativo que generalmente está fuera del aula física. Estas aplicaciones educativas según Sánchez (2009) han permitido dar apoyo a las asignaturas presenciales, lo cual ha dado paso al concepto educativo blended learning que consiste en mezclar la formación presencial con la formación a través de las TIC. Gracias a las aplicaciones web educativas podemos tener los siguientes beneficios:

- Acceder a la plataforma educativa desde cualquier parte del mundo gracias al acceso y disponibilidad de internet.
- Brindan igualdad de oportunidades a todas las personas de cualquier edad sin restricciones.
- Registro de actividad, acceso y entrega de tareas, lo cual permite una evidencia de participación de los estudiantes.

CIBER AMENAZAS

Las ciber amenazas a las plataformas educativas a raíz de la pandemia del COVID-19 se han incrementado considerablemente en este año según el Reporte de Ciberseguridad (BID-OEA, 2020, p. 16). Los organismos European Union Agency for Cybersecurity (ENISA), ESET Security y EcuCert del Ecuador realizaron estudio actualizado sobre los riesgos latentes que pueden afectar a las infraestructuras tecnológicas y aplicaciones web a nivel mundial.

Tabla 3. Top 5 de ciber amenazas 2020.

Nº	ENISA (2020)	ESET Security Report (2020)	ECUCERT (2020)
1	Malware	Malware	Click Fraud
2	Ataques vía Web	Ransomware	DDoS
3	Phishing	Criptominería	Keylogging
4	Ataques a aplicaciones Web	Phishing	Warez
5	Spam	Exploits	Spam

Fuente: elaboración propia.

En base a la referencia anterior las aplicaciones web educativas pueden ser un blanco fácil para los ciberataques. Por lo tanto, es importante identificar cómo estas amenazas afectan a las aplicaciones dentro de las siguientes etapas de seguridad:

Tabla 4. Clasificación de las ciber amenazas de las aplicaciones web.

Etapas de Seguridad en aplicaciones web	Ciber amenaza
Autenticación	Phishing Comunicación insegura
Disponibilidad	DDoS (denegación de servicios)
Confidencialidad	Manejo incorrecto de errores Fuga de Información
Integridad	SQLi (Inyección SQL) XSS (secuencia de comandos en sitios cruzados) PHPi (Inyección PHP) RFI (Remote File Inclusion) CMDi (Inyección de Comandos)

Fuente: elaboración propia.

Existe una percepción generalizada de que los ataques a las aplicaciones web son bastante diversos, sin embargo, los datos de la investigación de seguridad sugieren que la mayoría de los ataques a aplicaciones se limitan a: Inyecciones SQL, Directory Transversal o Inclusión local de archivos (Local File Inclusion), secuencia de comandos en sitios cruzados o (XSS), pérdida de autenticación y gestión de sesiones, (ENISA, 2020).

Figura 2. Ataques más comunes a aplicaciones web.

Fuente: (ENISA, 2020).

3.2.2. CIBERSEGURIDAD EDUCATIVA EN EL ECUADOR

En lo que se refiere a la educación, en el año 2020, el uso de las aplicaciones de educación virtual y aplicaciones para video llamadas o conferencias se han incrementado sustancialmente debido a la pandemia del COVID-19. Esta realidad aceleró la migración de la educación presencial a la virtual, por lo tanto, la SENESCYT puso en funcionamiento las plataformas tecnológicas (IES) y el acceso de equipos tecnológicos para los estudiantes, en base al informe de evaluación de los efectos e impactos de la pandemia en la educación superior.

Esta nueva realidad lleva consigo riesgos al momento de acceder a recursos virtuales en línea, por tal motivo la Asociación Ecuatoriana de Ciberseguridad (AECI), realizó un estudio en el primer semestre del año 2020, en donde se identificó que en el Ecuador uno de los principales riesgos es la falta de gestión y dedicación exclusiva de ciberseguridad en las empresas o instituciones educativas; a pesar de aquello, el Ecuador ha logrado obtener a una cierta madurez en materia de seguridad informática, ya que se ha entendido que unos de los recursos más valiosos que pueden tener las empresas es el personal capacitado en materia de ciberseguridad. Cabe indicar, además, que el gobierno ecuatoriano también contribuye a la seguridad de las redes de telecomunicaciones y el uso de Internet a nivel nacional, mediante el Centro de Respuesta a Incidentes Informáticos (EcuCERT) perteneciente a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). De esta manera el Ecuador pretende correlacionar a los usuarios con el acceso a los servicios, información y participación por medios electrónicos con calidad y seguridad, lo cual está contemplado dentro del Plan Nacional de Gobierno Electrónico 2018-2021 (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2018).

3.2.3. NORMAS Y METODOLOGÍAS PARA LA PREVENCIÓN Y RESPUESTA A INCIDENTES DE CIBERSEGURIDAD EN PLATAFORMAS WEB

Se considera necesario realizar una revisión de las normativas y metodologías para la gestión de seguridad y riesgo informático más utilizados en el ámbito de la ciberseguridad:

Tabla 5. Normas y metodologías más utilizadas en Ciberseguridad.

Soluciones de Ciberseguridad	Estudios/artículos (autores)	Utilización			Total
Metodologías	(Santiso <i>et al.</i> , 2016) ; (Guzman, 2019) ; (Santos <i>et al.</i> , 2016) ; (Zambrano y Zambrano, 2019) ; (Morales <i>et al.</i> , 2020)	MAGERITv3.0	AMFE		
		4	1		5
Normas	(Toapanta <i>et al.</i> , 2020) ; (Juarez, 2019) ; (Danilo <i>et al.</i> , 2015) ; (Santos <i>et al.</i> , 2016) ; (Morales <i>et al.</i> , 2020)	ISO27001	ISO27032	ISO15408	
		1	2	1	4

Fuente: elaboración propia.

Se concluye que una de las metodologías más utilizadas para el análisis y gestión de riesgos en seguridad de la Información es la MAGERITv3.0, desarrollada por el Consejo de Administración Electrónica de España, enfocada principalmente a entidades de Administración Pública. Esta metodología ofrece un método sistemático para analizar los riesgos derivados del uso de las TIC, para luego definir las medidas de mitigación más apropiadas. Dentro de las normas más utilizadas para la protección de la ciberseguridad es la ISO27032:2012 la cual ofrece un marco de gestión con controles específicos para los sistemas, infraestructura y usuarios finales, adaptados a las necesidades internas de los IST para el manejo y prevención de ataques. Este marco de seguridad, se complementa con el plan de contingencia planteado en el estudio de Padilla y Freire (2019) donde propone tres fases de respuesta a los ciberataques como son: Alerta, Transición y Recuperación de las infraestructura física o virtual que tiene cada institución.

3.2.4. PROCEDIMIENTOS Y ESTRATEGIAS DE CIBERSEGURIDAD

Existen varios procedimientos y estrategias que se han desarrollado en materia de ciberseguridad. A continuación, se ha identificado cuales son las normas y metodologías más utilizadas en el desarrollo de soluciones de ciberseguridad en las aplicaciones web.

Tabla 6. Procedimientos y estrategias de Ciberseguridad.

Respuestas a incidentes de Ciberseguridad	Estudios/artículos (autores)	Normas		Metodologías		Total
		ISO27001	ISO27032	MAGERIT V3.0	AMFE	
Procedimientos	(Santiso <i>et al.</i> , 2016) ; (Guzman, 2019) (López, 2019) ; (Arango, 2020) ; (Morales <i>et al.</i> , 2020)	1	2	2	1	6
Estrategias	(Vargas <i>et al.</i> , 2017) ; (Meriño <i>et al.</i> , 2019)		2			2

Fuente: elaboración propia.

Los procedimientos y estrategias estudiadas, en su mayoría utilizan la Norma ISO27032; la cual se encarga específicamente de la gestión y buenas prácticas de seguridad considerando todo el Ciberespacio (Equipamiento de red, Software, Interconexión de redes, personas, servicios de internet). Esta norma abarca los siguientes controles: Aplicaciones (Validación, Autenticación), Servidores (guías de instalación, monitoreo), usuario final (Antivirus, seguridad web, firewall) y Personas (educación continua, campañas de security awareness). De igual manera MAGERIT v3.0 es una de las metodologías más implementadas ya que gestiona de manera prudente las medidas de seguridad y confianza de los usuarios con sus servicios e infraestructura. Esta metodología se divide en tres partes: 1. Gestión de riesgos, 2. Tipifica criterios mediante la valoración de activos, 3. Brinda un conjunto de técnicas para el análisis de riesgos.

3.3. PROCEDIMIENTO METODOLÓGICO DE GESTIÓN DE CIBERSEGURIDAD PARA LAS PLATAFORMAS WEB EDUCATIVAS EN LOS ITS DE LA PROVINCIA DE TUNGURAHUA

Para alcanzar el objetivo planteado, se propone el siguiente procedimiento para la Gestión de riesgos de ciberseguridad dentro de los ITS de la Provincia de Tungurahua.

Figura 3. Fases del Procedimiento de Gestión.

Fuente: elaboración propia.

3.3.1. FASE 1: DEFINIR OBJETIVOS DE CIBERSEGURIDAD

Para establecer objetivos de Ciberseguridad en los ITS es necesario crear una conciencia en términos de precautelar la ciberseguridad por parte de las autoridades. Hoy en día los datos más sensibles son gestionados por las TIC, por lo tanto, definir los procesos internos de seguridad se hace indispensable. Por tal motivo, se ha visto necesario establecer objetivos institucionales en términos de ciberseguridad para brindar protección a toda la comunidad educativa.

- Implementar la Unidad de Gestión de Ciberseguridad dentro del Departamento de TIC Institucional.
- Crear una Normativa de Ciberseguridad Institucional.
- Alinear los procesos de gestión de seguridad dentro del Plan Operativo Anual.
- Permitir procesos de autogestión para solventar problemas de seguridad en las infraestructuras tecnológicas.

Con estos objetivos se pretende mitigar los riesgos y vulnerabilidades de las aplicaciones educativas.

3.3.2. FASE 2: IDENTIFICAR INFRAESTRUCTURA TECNOLÓGICA A PROTEGER

Para identificar las infraestructuras de hardware y software que se pretende proteger es necesario tomar como referencia las áreas definidas en el estado del arte como las más vulnerables para los ciberataques.

- Plataformas Web: Plataformas educativas e-learning, Sistemas de gestión educativa, Repositorios Digitales, página web institucional.
- Infraestructura: Servidor Web, Servidor de aplicaciones.
- Redes: Red interna Institucional.
- La Nube: Aplicaciones Web alojadas en servidores externos.

3.3.3. FASE 3: SELECCIONAR INCIDENTES DE SEGURIDAD MÁS COMUNES EN LAS APLICACIONES WEB

En esta fase se ha tomado una referencia al “Catálogo de Amenazas” definido en la metodología MAGERIT V3.0 para seleccionar las amenazas o riesgos que pueden afectar a la infraestructura y las aplicaciones web educativas. Los riesgos de ciberseguridad se las ha dividido en tres áreas de afectación: Administración del Sistema, Plataforma y Usuarios. A partir de esta referencia cada ITS debe seleccionar cuales son los incidentes más comunes que afecten a sus aplicaciones.

Tabla 7. Cuadro de selección de Amenazas comunes en aplicaciones web.

✓	Administración del Sistema	✓	Plataforma Web	✓	Usuarios
	Error de operación y mantenimiento del sistema		DDoS (denegación de servicios)		Errores en la utilización de la plataforma
	Error de supervisión y monitoreo		SQLi (Inyección SQL)		Ingeniería social
	Publicación accidental de información		XSS (secuencia de comandos en sitios cruzados)		Fuga de información

	Manipulación y destrucción accidental de la información		PHPi (Inyección PHP)		Suplantación de acceso
	Falta de procesos de seguridad de la información		RFI (Remote File Inclusion)		
	Fuga de información		CMDi (Inyección de Comandos)		
	Acceso de usuarios no autorizados		Phishing		
	Mal uso de privilegios del sistema				
	Poca preparación del personal				
	Manejo incorrecto de errores				

Fuente: a partir de (MAGERIT, 2012).

3.3.4. FASE 4: IDENTIFICAR LAS VULNERABILIDADES DEL ITS

Para identificar las vulnerabilidades en las aplicaciones web es necesario realizar pruebas de penetración basados en el hacking ético, las cuales se resumen a continuación en 4 etapas basadas en el estudio de Páez (2014):

- Reconocimiento:** Establecer el objetivo estudiar (aplicaciones web, sistemas de gestión educativa, página web), para buscar las posibles vulnerabilidades que pueda tener.
- Exploración:** Usar la información obtenida en la etapa de reconocimiento con el fin de detectar vulnerabilidades definidas en la Fase 3.
- Enumeración:** Recopilar la información vital, como puertos abiertos, servicios, usuarios de la red activos que puedan afectar al sistema.
- Informes:** Registrar las vulnerabilidades encontradas en el test de penetración y sobre estas generar recomendaciones o salvaguardas para evitar posibles ataques externos que afecten a la autenticación, disponibilidad, Integridad y confidencialidad.

Es necesario relacionar las vulnerabilidades encontradas con los incidentes más comunes en las aplicaciones web para definir una referencia al momento de encontrar las soluciones definidas en la siguiente fase.

3.3.5. FASE 5: DEFINIR CONTROLES DE CIBERSEGURIDAD

Una vez definidos los riesgos, es necesario realizar un cruce con los controles de la norma ISO 27032, con el objetivo de determinar las mejores soluciones de seguridad para las aplicaciones web enmarcadas en los incidentes y riesgos más comunes.

Riesgos de Ciberseguridad en las Plataformas Web	Controles de Ciberseguridad ISO27032:2012															
	1. Control de Aplicaciones				2. Control de Servidores				3. Usuarios Finales				4. Ingeniería Social (Personas)			
	- Gestión de Sesiones	- Validación de Datos	- Protección de ataques	- Procesos de autenticación	- Configuraciones seguras	- Gestión de parches	- Monitorización	- Respaldos	- Actualizaciones de Sistema Operativo	- Uso de aplicaciones	- Herramientas y configuraciones de seguridad	- Programas de concienciación	- Pruebas regulares	- Controles de seguridad	- Capacitación Constante	
Administración del Sistema																
Error de operación y mantenimiento del sistema	x								x	x					x	
Error de supervisión y monitoreo	x		x	x	x	x	x		x	x	x		x	x		
Publicación accidental de Información	x	x		x	x		x		x						x	
Manipulación y destrucción accidental de la información				x	x	x	x	x			x				x	
Falta de procesos de seguridad de la información			x	x	x	x	x	x	x				x	x		
Fuga de Información	x	x	x	x	x		x	x		x	x		x	x	x	x
Acceso de usuarios no autorizados	x	x	x	x	x	x	x				x		x	x		
Mal uso de privilegios del sistema	x	x		x		x					x		x	x		
Poca preparación del personal				x	x	x	x	x	x	x	x		x	x		x
Manejo incorrecto de errores	x	x	x	x	x	x	x						x	x		
Plataforma Web																
DDoS (denegación de servicios)	x	x	x	x	x		x	x			x		x	x	x	x
SQLi (Inyección SQL)	x	x	x	x		x	x	x					x	x	x	x
XSS (secuencia de comandos en sitios cruzados)	x	x	x	x	x		x	x			x		x	x	x	x
PHPI (Inyección PHP)	x	x	x	x		x	x	x			x		x	x	x	x
RFI (Remote File Inclusion)	x	x	x	x		x	x	x			x		x	x	x	x
CMDi (Inyección de Comandos)	x	x	x	x		x	x	x			x		x	x	x	x
Phishing	x	x	x	x	x		x	x			x		x	x	x	x
Usuarios																
Errores en la utilización de la plataforma						x	x	x	x		x	x	x	x	x	x
Ingeniería social										x	x	x		x	x	x
Fuga de información			x	x	x		x	x	x		x			x	x	x

Figura 4. Matriz de Correlación de Riesgos y Controles de Ciberseguridad ISO 27032:2012.

Fuente: elaboración propia.

La matriz de riesgos se ha definido conforme al estudio realizado por Santiso *et al.* (2016) en donde se realiza un análisis de correlación de las amenazas y controles con respecto a la norma ISO 27001. En cambio, esta propuesta se basa en la norma ISO 27032:2012, la cual establece controles de ciberseguridad para precautelar la información que está enlazada a la web. Este estudio varía conforme la realidad de cada instituto con respecto al tipo de infraestructura que disponen, procesos de gestión implementados, perfiles de usuario, amenazas, entre otras. Por tanto, es necesario que cada Instituto realice su propio análisis de riesgos para identificar sus amenazas y encontrar las mejores soluciones de seguridad que se deben implementar.

3.3.6. FASE 6: GENERACIÓN DE SALVAGUARDAS

Para solventar los problemas de ciberseguridad que afectan a cada institución es necesario implementar salvaguardias que brinden seguridad al entorno de las aplicaciones web. Por tanto, a continuación, se plantean salvaguardias de seguridad en base a los resultados en la matriz de correlación de la Fase 5 con respecto a las áreas de afectación.

SALVAGUARDA 1: ADMINISTRACIÓN DEL SISTEMA

Para la gestión de la ciberseguridad en los ITS es necesario llevar a cabo las siguientes actividades de administración en base a los controles de seguridad de la Norma ISO27032.

- Desarrollar la Normativa interna de Ciberseguridad en base a los siguientes controles:
 - Definición de Roles y Privilegios en los Sistemas (gestión de sesiones).
 - Gestión de Acceso mediante métodos autenticación en la plataforma web.
 - Validación de datos de usuario para definir la integridad de la información (criptografía).
 - Gestión de respaldos de la Información.
 - Capacitación Constante del Personal a Cargo.

SALVAGUARDA 2: PLATAFORMA WEB

Protección de ataques mediante la implementación de:

Arquitectura física:

- Implementación de un Firewall, para auditar y autorizar conexiones permitidas.
- Implementación de un Wireless LAN Controller para los accesos a las aplicaciones web dentro de los Institutos.

Arquitectura lógica:

- Manejo de errores de ejecución de los sistemas.
- Para la protección de ataques en las plataformas web se ha visto necesario tomar ciertas referencias de seguridad en base al estudio realizado por (OWASP, 2019).
- Codificar los datos de requerimientos HTTP con confiables en los campos de salida de HTML (cuerpo atributos, JavaScript, CSS o URL).
- Supervisar bibliotecas y componentes que no poseen mantenimiento o no liberan parches de seguridad.
- Cada instituto debe asegurar la existencia de un plan para monitorizar, evaluar y aplicar actualizaciones o cambios durante el ciclo de vida de las aplicaciones.

SALVAGUARDA 3: USUARIOS

- Capacitación en el uso de las Plataformas Institucionales.
- Definir procesos seguros para el restablecimiento de contraseñas.
- Promover el uso de antivirus para evitar malware en los quipos y dispositivos.

4. CONCLUSIONES

El procedimiento metodológico planteado logra establecer un marco de gestión de ciberseguridad aplicable a la infraestructura física y virtual de las plataformas web educativas de los IST de la provincia de Tungurahua, basado en un estándar y metodología de calidad internacional.

La educación virtual durante el último año se ha incrementado notablemente por el COVID-19, por tanto, el estudio planteado ofrece medios para precautelar la confidencialidad, integridad y disponibilidad de las plataformas web educativas institucionales.

Los principales riesgos de ciberseguridad que sufren las plataformas web educativas tienen que ver directamente con el control inadecuado de las aplicaciones, mala configuración de servidores, falta administración de usuarios e ingeniería social, esto ligado a la falta de designación de un personal exclusivo para el área de seguridad de la información en los IST.

El uso del procedimiento de gestión propuesto brinda una guía para el control y seguimiento de cada una de las áreas que implican riesgos de seguridad como son las aplicaciones, infraestructura y usuarios finales mediante el uso de controles basados en la Norma ISO27032:2012 y la metodología MAGERIT V3.0.

Las salvaguardias planteadas no pretenden ser soluciones absolutas sino más bien son el punto de partida para futuras investigaciones dentro de las Instituciones de educación superior enmarcados en planes de gestión que impliquen nuevos controles a amenazas que se puedan presentar en el futuro dentro de la educación online.

REFERENCIAS BIBLIOGRÁFICAS

- Abrigo-Córdova, I., Granados-Gómez, Donald Sánchez-Sulú, N., y Celi-Vivanco, Y.** (2019). El aula virtual: una experiencia educativa desde diversos ámbitos universitarios latinoamericanos. *Revista Ciencia Matria*, VI(27).
- Aguilar, L. J.** (2011). *Introducción. Estado Del Arte De La Ciberseguridad*. (1697–6924), 35. <http://www.pensamientopenal.com.ar/system/files/2015/01/doctrina38717.pdf>
- Antonio, J., López, A., Rosalba, C., y Rodríguez, R.** (2016). Paakat: Revista de Tecnología y Sociedad Seguridad en internet. *Revista de Tecnología y Sociedad*, 6(11), 2007–3607.
- Arango, L.** (2020). *Diseño y consolidación de un centro de respuesta ante incidentes de seguridad informática en la empresa cybersecurity de colombia ltda*. 117. <http://repositorio.unan.edu.ni/2986/1/5624.pdf>
- Barea, F., Romero, I., Rojo, I., y Villagr, A.** (s.f.). *Plataforma de gestión De Escenarios De Ciberseguridad Para Aprendizaje Y Entrenamiento*. <http://oa.upm.es/55294/>
- Carlini, A.** (2016). *Documento de Opinión. Ciberseguridad Un Nuevo Desafío Para La Comunidad Internacional*, 950–966.
- Chhetri, C., y Motti, V.** (2021) Identifying Vulnerabilities in Security and Privacy of Smart Home Devices. En Choo, K.K.R., Morris, T., Peterson, G.L., y Imsand, E. (eds) *National Cyber Summit (NCS) Research Track 2020*. NCS 2020. Advances in Intelligent Systems and Computing, vol 1271. Springer, Cham. https://doi.org/10.1007/978-3-030-58703-1_13
- Congacha, A., y García, V. J.** (2017). Modelación, simulación y automatización de procesos en la gestión de servicios académicos universitarios. *3C Tecnología. Glosas de innovación aplicadas a la pyme*, 6(2), 32–51. <https://www.3ciencias.com/wp-content/uploads/2017/06/ART-3.pdf>

- Crescenzi-Lanna, L., Valente, R., y Suárez-Gómez, R.** (2019). Safe and inclusive educational apps: Digital protection from an ethical and critical perspective. *Comunicar*, 27(61), 88–97. <https://doi.org/10.3916/C61-2019-08>
- Danilo, H., Cabrera, S. A., Abad, E. M., Torres, V. A., y Verdum, J. C.** (2015). Definition of cybersecurity business framework based on ADM-TOGAF. 1–7. <https://doi.org/10.1109/cis-ti.2015.7170391>
- ENISA.** (2020). Trust Services Security Incidents 2019. <https://doi.org/10.2824/047833>
- Grossman, I. R. L., Forest, R., Heath, J. E., Key, S. L., Us, F. L., Richardson, R. D., ... y Alexander, K. B.** (2015). (12) *United States Patent*. 1(12).
- Guzman, S.** (2019). *Guía para la Implementación de la Norma ISO 27032*. Universidad Católica de Colombia, 69.
- Harzing, A. W.** (2020) *Publish or Perish*. <https://harzing.com/resources/publish-or-perish>
- Haz, L., Flores, M., Ximena, A., Guzman, C., y Espín, L.** (2019). Implementation of IT Security and Risk Management Process for an Academic Platform. En *Advances in Intelligent Systems and Computing*, 379–386. https://doi.org/10.1007/978-3-030-02351-51-5_43
- Hernández, A.** (2017). Ciberseguridad y confianza en el ámbito digital. *Información Comercial Española, ICE: Revista de Economía*, (897), 55–66.
- Jang-Jaccard, J., y Nepal, S.** (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973–993. <https://doi.org/10.1016/j.jcss.2014.02.005>
- Juarez, F. A. B.** (2019). Ciberseguridad en un entorno de Internet de las Cosas Industrial (IIoT). En *8th International Conference on Software Process Improvement, CIMPS 2019 - Applications in Software Engineering*, 1–6. <https://ieeexplore.ieee.org/document/9082437/>

- Lewis, J.** (2006). Cybersecurity and Critical Infrastructure Protection. *Center for Strategic & International Studies*, 1(9), 12. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf
- Li, L., He, W., Xu, L., Ash, I., Anwar, M., y Yuan, X.** (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45(February 2018), 13–24. <https://doi.org/10.1016/j.ijinfomgt.2018.10.017>
- Lockee, B. B.** (2021). Online education in the post-COVID era. *Nature Electronics*, 4(1), 5–6. <https://doi.org/10.1038/s41928-020-00534-0>
- López, C. J.** (2019). *Desarrollo de una guía de controles ciberseguridad para la protección integral de la pyme*. 79. <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/95026/6/cjlopezTFM0619memoria.pdf>
- MAGERIT.** (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Libro I - Método. Ministerio de Hacienda y Administraciones Públicas, 2006(630-12-171–8), 127. <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>
- Meriño, I., Nieto, W., Moreno, S., y Hernández, Y.** (2019). Diseño de un Framework de Arquitectura Empresarial para Instituciones Públicas de Educación Superior. *Revista Ibérica de Sistemas e Tecnologías de Informação*, E17, 742–755. <http://www.risti.xyz/issues/ristie17.pdf>
- Ministerio de Telecomunicaciones y de la Sociedad de la Información.** (2018). *Plan Nacional de Gobierno Electrónico*. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/09/PNGE_2018_2021sv2.pdf
- Mirkovic, J., y Benzel, T.** (2012). Teaching cybersecurity with DeterLab. *IEEE Security and Privacy*, 10(1), 73–76. <https://doi.org/10.1109/MSP.2012.23>

- Morales, J., Zambrano, N., Lectong, T., y Zambrano, M.** (2020). Proceso de Ciberseguridad : Guía Metodológica para su implementación. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (26), 11.
- Mulligan, D. K., y Schneider, F. B.** (2011). Doctrine for cybersecurity. *Daedalus*, 140(4), 70–92. https://doi.org/10.1162/DAED_a_00116
- OWASP.** (2019). *Copyright y Licencia Tabla de Contenidos Sobre OWASP*. <https://github.com/OWASP/Top10/issues>
- Padilla, V. S., y Freire, F. F.** (2019). A Contingency Plan Framework for Cyber-Attacks. *Journal of Information Systems Engineering & Management*, 4(2), 2–7. <https://doi.org/10.29333/jisem/5898>
- Páez, M.** (2014). *Propuesta de Procedimiento para la ejecución de Pentest dentro del esquema de pruebas de las fábricas de software para aplicaciones web*, 7, 69. <http://polux.unipiloto.edu.co:8080/00002027.pdf>
- Ramirez, D., Ramirez, V., y Venkataramanan, G.** (2019). Ciberseguridad En Infraestructuras. Aplicación a Los Elementos De Un Smart Grid. *Dyna Ingeniería E Industria*, 94(1), 518–522. <https://doi.org/10.6036/9041>
- Redrován, F., Loja, N., Correa, K., y Piña, J.** (2018). Comparación de métricas de calidad para el desarrollo de aplicaciones web. *3C Tecnología. Glosas de innovación aplicadas a la pyme*, 7(3), 94–113. <https://ojs.3ciencias.com/index.php/3c-tecnologia/article/view/620>
- Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., y Basto-Fernandes, V.** (2017). A Comparison of Cybersecurity Risk Analysis Tools. *Procedia Computer Science*, 121, 568–575. <https://doi.org/10.1016/j.procs.2017.11.075>
- Romero, L.** (2010). La seguridad informática en el trabajo con la plataforma “Moodle.” *Revista de Humanidades*, (17), 169–190.

- Sánchez, J.** (2009). Plataformas de enseñanza virtual para entornos educativos. *Pixel-Bit: Revista de Medios y Educación*, 34, 217–233. <http://www.sav.us.es/pixelbit/actual/15.pdf>
- Santiso, H., Koller, J., y Bisaro, M.** (2016). Seguridad en Entornos de Educación Virtual. *Security in Virtual Education Environments.*, 14(14), 67–88. <http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=120577699&lang=es&site=ehost-live>
- Santos, A., Sanchez, L. E., Alvarez, E., Huerta, M., y Fernandez, E.** (2016). Methodology for Dynamic Analysis and Risk Management on ISO27001. *IEEE Latin America Transactions*, 14(6), 2897–2911. <https://doi.org/10.1109/TLA.2016.7555273>
- Seefeldt, J., y Tadoro, S.** (2019). *El efecto orwell en la sociedad en red: ciberseguridad, régimen global de vigilancia social y derecho a la privacidad en el siglo xxi*, 85. https://buleria.unileon.es/handle/10612/12563?local-attribute=pt_BR
- Toapanta, S. M. T., Gustavo, E., y Gallegos, L. E. M.** (2020). Analysis of appropriate standards to solve cybersecurity problems in public organizations. En *ACM International Conference Proceeding Series*, (May), 14–19. <https://doi.org/10.1145/3404663.3404678>
- Vargas, R., Recalde, L., y Reyes, R.** (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *Revista Latinoamericana de Estudios de Seguridad*, (20).
- Vega, G., y Ramos, R.** (2017). Vulnerabilidades Y Amenazas a Web. *3C Tecnología. Glosas de innovación aplicadas a la pyme*, 6(1), 53–66. <https://ojs.3ciencias.com/index.php/3c-tecnologia/article/view/53>
- Zambrano, N., y Zambrano, M.** (2019). Ciberseguridad Y Su Aplicación En Las Instituciones De Educación Superior Públicas De Manabí. *Espam*, 199. <http://repositorio.esпам.edu.ec/bitstream/42000/1032/1/TTMTI3.pdf>

/03/

GAMIFICACIÓN Y APRENDIZAJE ACTIVO CON KAHOOT!: CREACIÓN DE EXÁMENES POR PARTE DEL ALUMNADO

GAMIFICATION AND ACTIVE LEARNING WITH KAHOOT!: STUDENT CREATION OF EXAMS

Cecile Meier

Profesora ayudante doctora de la Universidad de La Laguna, departamento de Bellas Artes, área de Escultura.
Miembro del grupo de investigación “Diseño y Fabricación Digital” y profesora de fotografía.
Santa Cruz de Tenerife, (España).

E-mail: cemeier@ull.edu.es ORCID: <https://orcid.org/0000-0001-7160-2154>

Alejandro Bonnet de León

Profesor ayudante doctor de la Universidad de La Laguna, departamento de Bellas Artes,
área Didáctica de la Expresión Plástica. Especialista en la incorporación de nuevas tecnologías en el aula.
Santa Cruz de Tenerife, (España).

E-mail: abonnetl@ull.edu.es ORCID: <https://orcid.org/0000-0001-7992-545X>

Recepción: 01/06/2021 **Aceptación:** 20/06/2021 **Publicación:** 29/06/2021

Citación sugerida:

Meier, C., y Bonnet de León, A. (2021). Gamificación y aprendizaje activo con Kahoot!: creación de exámenes por parte del alumnado. *3C TIC. Cuadernos de desarrollo aplicados a las TIC*, 10(2), 77-99. <https://doi.org/10.17993/3ctic.2021.102.77-99>

RESUMEN

La gamificación y el uso de los nuevos medios tecnológicos, se han convertido en la actualidad, en una nueva forma de aprendizaje y evaluación de contenidos. En este texto se describe el uso de Kahoot! para fomentar el aprendizaje activo, reforzar el conocimiento de conceptos vistos en clase y para crear una prueba evaluativa a modo de juego. Además, es una manera de realizar un examen en igualdad de condiciones para una clase semipresencial, donde la mitad está en la clase y la otra mitad asiste online. Sobre un temario teórico de la clase de fotografía, 42 estudiantes divididos en grupos de dos a cuatro integrantes, crean su propio examen (Conjunto de preguntas sobre la temática propuesta) mediante Kahoot. El día de la prueba, los exámenes elaborados por cada grupo, son planteados al resto de la clase mediante Kahoot!. Al final de la actividad se pasó un test de satisfacción a los alumnos donde valoran el uso de Kahoot! y la posibilidad de ser parte activa en la creación del examen, valoración que ha resultado puntuada como muy positiva.

PALABRAS CLAVE

Kahoot!, Aprendizaje Activo, Gamificación, Mobile Learning, Examen.

ABSTRACT

New technologies and gamification are increasingly being used to facilitate learning and also to carry out evaluative tests at the end of a lesson plans. This text describes the use of Kahoot! to promote active learning, to reinforce the knowledge of the concepts seen in class and to create an evaluative test in the form of a game. It is also a way of conducting a test on equal terms for a semipresential class, where half of the students are in the classroom and the other half attend online. Based on a theoretical lesson plan from the photography class, 42 students, divided into groups of two to four, create their own test using Kahoot!. On the day of the test, the tests created by the students themselves are performed to the rest of the class via Kahoot! The results have been positive, all the students have managed to pass, thanks also to the large number of questions and the constant repetition of them. At the end of the activity, a satisfaction test was given to the students where they evaluated the use of Kahoot! and the possibility of being an active part in the creation of the exam in a very positive way.

KEYWORDS

Kahoot!, Active Learning, Gamification, Mobile Learning, Exam.

1. INTRODUCCIÓN

Kahoot! es una plataforma que ofrece una versión gratuita que permite crear exámenes o cuestionarios online, a modo de concurso de preguntas, en donde los alumnos son los concursantes. Cada participante introduce su nombre en el juego y contesta a una serie de cuestiones por medio de un dispositivo móvil, tableta u ordenador. Las partidas de preguntas, una vez creadas, son accesibles por todos los usuarios de manera que pueden ser reutilizadas e incluso modificadas para garantizar el aprendizaje, además de servir como método de estudio.

Según la página oficial de Kahoot!, la aplicación está diseñada para hacer pruebas rápidas o evaluar previamente el conocimiento de la clase sobre un tema, además de evaluar los resultados del aprendizaje y el progreso de la clase. Puede servir para revisar contenido e identificar los temas que necesitan ser repasados o que requieren refuerzo para que los estudiantes lo dominen. También se usa para practicar las posibles preguntas de un examen y prepararse para la evaluación. Esto potencia el estudio independiente ya que los alumnos puedan estudiar y practicar el temario en casa o en clase desde cualquier dispositivo. Aparte de la evaluación se puede usar para hacer presentaciones interactivas, motivar a la participación en el aula, evaluar opiniones, presentar trabajos, incentivar la asistencia, impulsar la retención, etc. (Kahoot!, 2021).

Kahoot! une varias tendencias emergentes en el uso de tecnologías en el aula, el aprendizaje móvil electrónico (M-learning), la ludificación (Gamification), así como utilizar dispositivos propios (Bring your own device).

Desde 2012 el informe Horizon (Durall *et al.*, 2012; Horizon, 2017), menciona el mobile learning como una tecnología que se está usando en educación. El mobile learnig se refiere al uso de Smartphones, tabletas digitales u ordenadores propios de los alumnos en el aula. En la educación universitaria el uso de móviles está ampliamente aceptado y usado, Chen y deNoyellesen un estudio de 2013 mencionan que dos tercios de los estudiantes buscan el contenido y estudian a través de su Smartphone (Chen y

deNoyelles, 2013). En 2016 un estudio muestra que ya el 81 % de los estudiantes utiliza el móvil para estudiar (Al-Emran, Elsherif, y Shaalan, 2016). Además, este año el mobile learnig se ha convertido en imprescindible debido a la educación online (Naciri *et al.*, 2020).

En el Informe Horizon de 2014 se añade una corriente de aprendizaje basada en juegos (Johnson, y otros, 2014) que se prevé como uso generalizado en los siguientes dos o tres años. Dicha corriente de aprendizaje, en los últimos años se ha denominado con diferentes términos como por ejemplo ludificación, game based learning (GBL), gamificación, etc. (Lee y Hammer, 2011; Deterding *et al.*, 2012). En los últimos años ha terminado por designarse como Gamificación. Esta tendencia educativa trata de fomentar los valores comunes a todos los juegos. En un informe de 2019 consta que, de los españoles que poseen un móvil, el 97,7% lo ha utilizado para los juegos (Ditrendia, 2019).

Por ultimo el término Bring your own device (BYOD), es decir, que los estudiantes lleven su propio dispositivo digital al aula es muy habitual en las aulas universitarias. Hay muchos estudios que han investigado el uso de la tecnología móvil en las aulas con resultados positivos (Gikas y Grant, 2013; Basantes *et al.*, 2017; Sánchez, 2012). Con los alumnos que se realizó la experiencia, el 100% dispone de Smartphone, lo llevan siempre encima y lo utilizan activamente en el aula para consultar temario, estudiar, preparar ejercicios y también chatear o similar.

En este trabajo se utilizan las tendencias mencionadas, los alumnos utilizan sus propios dispositivos, tanto en el aula como en casa, para crear partidas de preguntas sobre un temario visto en el aula mediante la app de Kahoot!. Al ser los propios estudiantes que programan las preguntas que luego serán parte de su examen, participan activamente en el proceso, fomentando el aprendizaje activo y participativo. El aprendizaje activo significa que el alumno participa en el proceso de aprendizaje mediante el desarrollo del conocimiento y la comprensión no solo como sujeto pasivo que recibe información (Cambridge International, 2019). En los años 80 se empieza a investigar sobre el aprendizaje activo y a concebirlo cada vez más importante para que el alumno aprenda de forma significativa. Bonwell (1991) describe el aprendizaje activo como aquel en el que el alumno realiza diversas actividades aparte de escuchar a

una clase magistral de forma pasiva. Kersey (2000) describe el aprendizaje activo como aquel que tiene como objetivo involucrar al alumno, haciéndolo protagonista o hacerlo pensar sobre lo que aprende. El propósito es lograr que los estudiantes pasen a un estado activo en la creación de su propio examen.

Una vez que los alumnos crean sus partidas de preguntas en Kahoot!, éstas se ponen a disposición abierta para cualquier usuario de Kahoot!, por lo tanto los compañeros pueden acceder a ellas y utilizarlas para jugar y estudiar para la evaluación (Figura 1). Los Kahoot! están disponibles en el siguiente enlace: <https://cutt.ly/OnJwnCd>. Por último, estas partidas se juegan luego, a modo gamificación, como preguntas de examen para la evaluación en una clase semipresencial. Esto permite realizar el examen en el mismo momento y en las mismas condiciones para los alumnos presentes en el aula y los que asisten de forma virtual a través de google meet.

Figura 1. Exámenes creados por los alumnos, accesibles online una vez registrado en la página con un usuario.

Fuente: Kahoot!.

1.1. ANTECEDENTES

Un sistema que se podría considerar antecedente al Kahoot!, es el “Personal Response Systems” llamado también “Clickers”. Con ese sistema, el alumno responde a preguntas mediante un dispositivo electrónico. En este caso se entregaba un mando a cada alumno y se presentaban preguntas tipo test en la pantalla del aula y cada uno respondía mediante su mando donde disponía de varios botones para elegir la respuesta. El problema de los Clickers es que necesitan de un software específico, un conocimiento del funcionamiento del sistema por parte del profesor y de material propio que hay que llevar al aula: captador de infrarrojos y un número limitado de mandos específicos para recoger las respuestas (Pintor *et al.*, 2014).

Kahoot! se basa en ese sistema, pero con una tecnología disponible y accesible por todos, además es muy fácil de manejar o programar. Se lanzó al público en septiembre de 2013 y fue fundado por Johan Brand, Jamie Brooker y Morten Versvik en un proyecto realizado en conjunto con la Universidad Noruega de Ciencia y Tecnología en Trondheim, Noruega. El juego funciona a modo de concurso de preguntas (Figura 2 a y b), donde el alumno tiene entre dos y cuatro respuestas posibles. Éstas le aparecen en una pantalla del móvil en botones de diferentes colores (Figura 2c) donde se puede seleccionar la respuesta correcta (Kahoot!, 2021).

Figura 2. a) Vista del juego para la pregunta. b) Vista del juego para la respuesta en el ordenador del profesor. c) Vista del juego para el jugador donde debe elegir el color que corresponde a la respuesta correcta

Fuente: Kahoot!.

Crear el juego, es decir una partida de preguntas, es sencillo y no requiere de un aprendizaje exhaustivo. En el juego, se puede modificar el tiempo del que dispone el alumno para contestar, las posibles preguntas y respuestas, y también se pueden añadir fotos o vídeos. Una vez terminada la batería de preguntas, se puede guardar en la cuenta personal o bien, hacer visible la partida para todo el mundo, de esta manera, otros profesores o alumnos pueden usar las preguntas para jugar, estudiar, repasar contenido o utilizarlo como herramienta de evaluación. En una sola partida se pueden conectar hasta 200 estudiantes lo que permite también, evaluar clases grandes. Además, es posible realizar el juego de forma virtual, presencial o en clases semipresenciales. Una vez que el profesor utiliza una partida de preguntas para realizar un examen o evaluación de ciertos conocimientos, el programa permite descargar un Excel con todos los datos detallados, lo que facilita la calificación y la retroalimentación. Asimismo, nada más responder las preguntas en el aula, el alumno obtiene la información de la respuesta correcta por lo que la retroalimentación a cada pregunta es inmediata (Figura 3). El juego, o la partida de preguntas las gana el jugador que más puntuación obtiene, los puntos son una mezcla entre las respuestas acertadas y la rapidez con que se ha acertado cada respuesta.

Figura 3. Retroalimentación después de responder a una pregunta en el test.

Fuente: elaboración propia a partir de Kahoot!.

Este juego se ha utilizado en gran variedad de situaciones y en su mayoría con resultados positivos, aunque también afirman que no es tan efectivo como se esperaba y algunos denotan problemas con la conexión a internet (Wang y Tahir, 2020; Zhang y Yu, 2021). En una asignatura de anatomía se ha utilizado Kahoot! para que los estudiantes repasen el contenido visto en clase. Como es una materia donde es necesario aprender una gran cantidad de nombres y nuevos conceptos, este juego proporciona a los estudiantes una manera de revisar lo que han aprendido de forma interactiva y competitiva. Se ha observado una mayor asistencia y participación, así como un mayor número de estudiantes enfocados y comprometidos en clase. Los resultados sugieren que este juego se puede usar como una actividad de cierre de un temario (Aktekin, Çelebi, y Aktekin, 2018).

En otro estudio se utiliza Kahoot! como una herramienta participativa para mejorar el aprendizaje e incrementar la competencia en el aula (Rodríguez-Fernández, 2017), los resultados arrojan que Kahoot! es altamente valorado por el alumnado. Los autores afirman que la repetición y frecuencia de utilización de la aplicación contribuye directamente en la efectividad del mismo, aunque también afirman que no es tan efectivo como se esperaba.

Cárdenas, Véliz y Véliz (2020) y Llerena y Rodríguez (2017) utilizan la app para facilitar el aprendizaje de vocabulario de inglés. Los resultados de su trabajo corroboran que mejora el compromiso y la interacción de los alumnos, además aumenta la motivación y mejora la adquisición de vocabulario para los exámenes posteriores. Los resultados de su encuesta de satisfacción indican que los alumnos disfrutaron jugando a Kahoot! y que les resultaba fácil de usar. Martínez (2017), concluye que, aun con limitaciones, la combinación de tecnología, juego y aprendizaje resulta más eficaz que las metodologías tradicionales. Moya *et al.* (2016) concluyen que este juego permite hacer clases más dinámicas y entretenidas, además, de realizar evaluaciones interactivas del rendimiento y también fomentar la participación y aprendizaje en el aula. Rojas-Viteri, Álvarez-Zurita y Bracero-Huertas (2021) utilizan Kahoot como elemento motivador en el aula, los resultados muestran alumnos más motivados en el aprendizaje y en la evaluación.

En el caso descrito en este artículo, los propios alumnos, por grupo, crean sus preguntas de examen y el papel del profesor pasa a un segundo plano, siendo los mismos alumnos los protagonistas de la sesión educativa. Con ello se pretende involucrar al alumnado en el proceso de evaluación, creando un aprendizaje activo. Las funciones del docente se reducen a ser un mero presentador del juego, presentar y explicar el funcionamiento del mismo; así como leer las preguntas de los exámenes creados por los alumnos y justificar las respuestas en caso necesario con la meta de aclarar posibles dudas.

2. MATERIALES Y MÉTODOS

Se ha utilizado Kahoot! para realizar la evaluación del tema teórico impartido en la asignatura de Fotografía del grado universitario de Restauración y Conservación de Bienes Culturales de la Facultad de Bellas Artes de la Universidad de La Laguna. Esta asignatura es eminentemente práctica, ya que se trata principalmente de aprender a manejar la cámara fotográfica profesional y realizar proyectos de fotografía. Sin embargo, al principio de la asignatura se imparte un temario sobre la historia de la fotografía y la composición de la luz. Este temario incluye una serie de conceptos nuevos así como bastantes nombres y fechas de los hitos durante la historia de la fotografía.

Para fomentar el aprendizaje activo y hacer el aprendizaje del temario más ameno y participativo, se han decidido incorporar nuevas tendencias como m-learning, gamificación y BYOD en esta asignatura, a partir de la utilización de la aplicación Kahoot!. Para ello son los propios estudiantes los que crean los exámenes online, y el día de la evaluación, se utilizan esos exámenes para evaluar a toda la clase.

2.1. DESARROLLO DE LA ACTIVIDAD

Se ha seguido un método cuasiexperimental con los 42 alumnos matriculados en la asignatura durante el presente curso. La actividad se ha desarrollado en todo momento de forma semipresencial, es decir, solo asiste la mitad de los alumnos al aula y la otra mitad sigue la clase en formato online a través de Google

Meet, para mantener los ratios en un aula con las distancias de seguridad y las medidas necesarias durante el curso 2020/2021.

Para empezar, el docente imparte dos clases lectivas, cuatro horas en total, de teoría en método expositivo a la clase. Dicha teoría está disponible para el alumnado en el aula virtual y contiene explicaciones, esquemas, videos, imágenes y enlaces a información ampliada. Una vez que se ha presentado toda la información al alumnado se procede a explicar la actividad y el tipo de examen que se realizará con Kahoot! y cómo se deben involucrar los estudiantes en la creación de la prueba. La clase se imparte en dos horarios diferentes, con dos grupos de 18 y 24 alumnos. Se dividen ambos grupos en 7 y 8 subgrupos respectivamente. De esta manera colaboran entre dos y cuatro alumnos para crear un test con preguntas que eligen entre ellos.

Durante el resto de la clase y la semana, los alumnos trabajan con sus compañeros asignados, para crear una batería de preguntas en Kahoot!. Cada grupo debe hacer 15 preguntas y es libre de añadir imágenes, vídeos y formular las cuestiones como estimen oportuno.

Cada test en Kahoot! con las preguntas creadas además está disponible online para el resto de compañeros. Esto se consigue al dar un nombre fácil de buscar e identificar (Figura 4a). En este caso cada grupo debe marcar la pestaña de “visibility-everyone” (Figura 4b) y añadir exactamente el nombre de “C&R 2021 grupo x”. En el nombre, al final se añade el número de grupo asignado a cada uno, para así poder encontrar uno específico, saber cuál de los exámenes toca realizar, y poder añadir además, una nota de la elaboración del Kahoot!.

Figura 4. a) Ajustes, importante para poder encontrar y compartir el examen. b) Detalles de los ajustes que se deben hacer para que sea visible para todos.

Fuente: elaboración propia a partir de Kahoot!.

En una de las clases, también se realiza una demostración activa del funcionamiento de Kahoot!, el docente selecciona un test previamente creado a modo ejemplo con solo cuatro preguntas. Este test se realiza con los alumnos para comprobar que todos entiendan el funcionamiento de la aplicación, asegurarse de la conexión de sus dispositivos a internet y prepararlos para el examen del siguiente día. En la siguiente tabla se detalla a modo esquemático las actividades y su temporalización.

Tabla 1. Esquema de la temporalización.

1º	4 horas	Explicación del temario
2º	½ hora	División de grupos y explicación de la actividad con Kahoot!
3º	1 semana	Trabajo autónomo del alumnado
4º	½ hora	Tutorización y demostración activa del examen.
5º	1 hora	Examen
6º	1 hora	Corrección y notas

Fuente: elaboración propia.

Para el día del examen se cuenta con 7 y 8 test creados por los grupos de 15 preguntas cada uno, es decir en total 105 y 120 preguntas para cada grupo. Esto evidentemente provoca una gran cantidad de preguntas repetidas o muy similares ya que el tema a tratar es reducido. Sin embargo, la repetición

constante de preguntas, formuladas de distinta forma, es clave para retener el contenido y afianzar el conocimiento.

Al final de cada juego, es decir, una vez que los estudiantes hayan respondido a cada batería de preguntas, se descarga un Excel con las respuestas. Al haber realizado la prueba con 17 grupos, divididos en dos horas diferentes, se obtienen 17 archivos Excel diferentes con las notas. Concretamente 7 archivos del grupo A y 8 archivos del grupo B.

Si trabajamos la información de forma correcta se tarda menos de una hora en obtener las calificaciones detalladas de cada alumno y con una nota justa. Para ello primero se ordena cada Excel por orden alfabético de los nombres de los alumnos. En segundo lugar se cogen los datos, en este caso la puntuación final de cada alumno que es un conjunto de respuestas acertadas, falsas y el tiempo que ha tardado en responder. Se toma esta puntuación ya que se quiere tener en cuenta el tiempo en la respuesta para penalizar alumnos que tardan 30 segundos o más en responder y les pudiera haber dado tiempo en buscar la respuesta correcta. Una vez ordenado los resultados de los diferentes test, se suman las puntuaciones y se realiza una regla de tres, en la que se adjudica la nota máxima, un 10, al alumno que mayor puntuación haya sacado. Y el resto recibe una nota según el cálculo. Por otro lado se aplica un 10 % de la nota de la puntuación que se ha puesto en la propia creación del Kahoot! En la evaluación de la creación de las cuestiones, se restan puntos por preguntas mal formuladas, faltas de ortografía, respuestas ambiguas, etc.

Al finalizar, también se pasa un test de satisfacción a los alumnos para obtener una valoración sobre esta forma de realizar la evaluación del temario.

3. RESULTADOS

Cada grupo de alumnos creó un test con la aplicación Kahoot! con las indicaciones expuestas en clase. La mayoría de preguntas fueron apropiadas y acordes al temario impartido en las sesiones. Los test pueden encontrarse en el siguiente enlace después de registrarse: <https://cutt.ly/OnJwnCd>.

El día del examen, el trabajo se desarrolló sin dificultades. Todos pudieron responder a las preguntas con sus dispositivos personales, tanto Smartphone, ordenadores y tabletas. Los alumnos se conectaron simultáneamente desde casa y desde clase al test y respondieron en el tiempo indicado.

Después de pasar los diferentes test, se pudo descargar un Excel con todos los resultados detallados. De esta manera el profesor no necesita corregir test, pero si tiene que dedicar un rato a cruzar todos los datos, es decir la puntuación final de cada alumno en cada test y en este caso también se añadió la cantidad de respuestas correctas e incorrectas. Con todo esto se obtuvo una tabla donde se asignó una nota del 1-10 a las puntuaciones y la cantidad de respuestas correctas obtenidas por el alumno. En este caso se adjudicó la nota máxima (10) a la mejor puntuación y a continuación se calculó mediante una regla de 3 el resto de las notas. Por último se añadió un 10% al cálculo, de la nota que obtuvo cada alumno en la creación del Kahoot. El cálculo completo de las notas está disponible en el siguiente enlace: <https://cutt.ly/Mn8Bcw6>.

Por otro lado, durante la prueba, o al corregir los Kahoot! antes del día del examen, el profesor debe seleccionar las preguntas inadecuadas o mal formuladas y eliminarlas de la ecuación final. Este trabajo requiere un tiempo de dedicación, sin embargo se considera que es menos tiempo que corregir todos los exámenes con sus 105 y 120 preguntas respectivamente. En la siguiente tabla se muestran las notas finales y como se organizaron las puntuaciones.

Tabla 2. Resultados y notas finales del grupo A.

	Final score	Correct answer	Incorrct answer	Nota Kahoot!	Create Kahoot!	Total
a1	91284	94	4	10	8	9,80
a2	90923	96	2	9,96	7	9,66
a3	89693	98	0	9,83	7	9,54
a4	88779	92	6	9,73	8	9,55
a5	88354	93	5	9,68	7	9,41
a6	86628	93	5	9,49	8	9,34
a7	85857	89	9	9,41	8	9,26
a8	84642	87	11	9,27	8	9,14
a9	84635	87	11	9,27	9,5	9,29
a10	84475	94	4	9,25	8	9,13
a11	82737	85	13	9,06	9	9,06
a12	80951	84	14	8,87	9,5	8,93
a13	78758	83	15	8,63	8	8,56
a14	77977	80	18	8,54	9,5	8,64
a15	77191	79	19	8,46	9	8,51
a16	67610	71	27	7,41	9,5	7,62
a17	66353	75	23	7,27	8	7,34
a18	63194	67	31	6,92	9	7,13

Fuente: elaboración propia.

Tabla 3. Resultados y notas finales del grupo B.

	Final score	Correct answer	Incorrct answer	Nota Kahoot!	Create Kahoot!	Total
b1	114499	115	0	10	10	10,00
b2	114225	115	0	9,98	10	9,98
b3	112664	115	0	9,84	10	9,86
b4	112091	113	2	9,79	10	9,81
b5	111137	113	2	9,71	10	9,74
b6	108817	111	4	9,50	10	9,55
b7	108267	112	3	9,46	10	9,51
b8	108179	110	5	9,45	10	9,50

b9	107422	112	3	9,38	10	9,44
b10	107109	109	6	9,35	10	9,42
b11	104608	106	9	9,14	10	9,22
b12	104604	110	5	9,14	10	9,22
b13	103989	107	8	9,08	10	9,17
b14	103523	105	10	9,04	10	9,14
b15	103445	112	3	9,03	10	9,13
b16	103024	109	6	9,00	10	9,10
b17	102953	107	8	8,99	8	8,89
b18	101327	107	8	8,85	8	8,76
b19	100925	106	9	8,81	10	8,93
b20	99137	105	10	8,66	10	8,79
b21	80164	90	25	7,00	10	7,30
b22	69155	72	43	6,04	10	6,44
b23	64468	70	30	5,63	10	6,07
b24	63660	67	48	5,56	10	6,00

Fuente: elaboración propia.

En la siguiente tabla se muestra el resultado del cuestionario de satisfacción realizado mediante una escala Likert. Con una posibilidad de seleccionar una puntuación del 1-5, que es acorde a nada de acuerdo a totalmente de acuerdo. Dicho cuestionario fue realizado con la opción de formulario disponible en Google Drive, aplicando la opción de escala lineal. Antes de pasar el cuestionario a los alumnos, fue validado por un grupo de expertos en tecnología educativa. Está disponible en el siguiente enlace: <https://forms.gle/9SSGRB4D2q5VgBrM6>.

Tabla 4. Resultados del cuestionario de satisfacción.

Pregunta	Media (1-5)	Desv. Est.
Prefiero realizar un examen en Kahoot frente a un tipo test normal.	4,34	1,52
Creo que al participar en la creación del examen he aprendido el contenido de forma activa	4,72	0,89
Me ha gustado poder crear las preguntas del examen	4,52	0,55
Creo que he obtenido una nota justa	4,45	0,55
Pienso que he sacado mejor nota que en un examen normal	4,10	1,00

Todo el proceso ha sido muy complicado para mi	2,38	0,71
Al repetir varias veces las mismas preguntas durante el examen he aprendido el contenido un poco más	4,66	0,89
Me parece útil poder tener acceso a los exámenes creados por los compañeros.	4,83	0,45
Me parece muy favorable poder consultar y estudiar todas las preguntas antes del examen.	4,55	1,30
He utilizado los Kahoot creado por los compañeros para estudiar.	4,55	1,79
Es la primera vez que realizo un examen con esta dinámica.	3,76	2,00
He afrontado este examen con menos nervios que un examen normal	3,90	1,48

Fuente: elaboración propia.

4. CONCLUSIÓN Y DISCUSIÓN

En un escenario de docencia online o semipresencial como ha sido en este caso, realizar una evaluación mediante la herramienta Kahoot! es muy favorable. Permite contestar a todos los participantes en igualdad de condiciones, estén presentes en el aula o de forma online. En el caso de esta Universidad, prácticamente el 100% de los alumnos dispone de dispositivos móviles u ordenadores para realizar el trabajo o contestar al examen. Además disponen de internet en sus domicilios o hay conexión gratuita en todas las instalaciones universitarias. Por lo tanto la tecnología favorece este tipo de iniciativas.

Por otro lado, está demostrado que de cuantas más formas diferentes se enfrenta un alumno a la información que debe aprender, más fácil le será recordar los temarios y menos debe disponer de pura memoria (Bonwell y James, 1991). Los alumnos necesitan tiempo suficiente para procesar información nueva. Según Nuthall (2007), generalmente los alumnos requieren que los contenidos les sean explicados en su totalidad al menos tres veces y de diferentes maneras (no por mera repetición), antes de poder recordarlos. En el caso descrito en este artículo, los estudiantes se han enfrentado de cuatro maneras diferentes a la información.

- 1º Recibe la clase magistral con todo el temario a estudiar. Esto incluye diapositivas, texto escrito a modo esquemático en las diapositivas, videos de refuerzo e imágenes.

2º Al realizar las preguntas de examen debe desgranar todo la información recibida y seleccionar de ahí las preguntas relevantes así como las respuestas de manera adecuada. En este caso, como Kahoot permite integrar imágenes o vídeos en la app también se apoyen en la búsqueda del material gráfico.

3º Estudian en casa o junto con otros compañeros el material y repasan las preguntas que saldrán en el examen. Esto es posible al disponer de los Kahoot! realizados por los compañeros.

4º En el día del examen, aparte de contestar a las preguntas, también se adquiere conocimiento. Debido a que hay preguntas que se repiten con frecuencia, el alumno vuelve a incidir en esos conocimientos reforzándolos, además de recibir un feedback inmediato después de cada pregunta.

Este proceso les lleva a estudiar el material teórico de forma diferente a la usualmente empleada, contribuyendo a una participación activa, en la elaboración de sus propios exámenes. Con ello se pretende fomentar la participación del alumno en todo el proceso de evaluación y prepararlo para la prueba de forma distinta. Por otro lado, como es un temario relativamente corto, realizar esta actividad tiene sentido ya que se repiten con frecuencia las preguntas lo que conlleva a una mayor consolidación del conocimiento adquirido. Se pretende de esta manera que el estudiante a través de todo el proceso se enfrente al material de diferentes maneras y consolide así su conocimiento de manera más profunda que en un examen normal donde solo estudia a su manera en casa y luego aplica el conocimiento en el examen.

En los resultados se observa que las notas generalmente son muy buenas y no ha suspendido ningún alumno. También se puede deber a que el temario era relativamente sencillo y al repetirse las preguntas, al final todos se sabían la respuesta. Además la corrección de los exámenes se hace de forma automática y requiere mucho menos tiempo que hacerlo a mano.

Por otro lado, los resultados del cuestionario de satisfacción son positivos. Los alumnos prefieren hacer un examen con Kahoot! frente a un test normal (4,34 sobre 5) y opinan que su nota es justa (4,45 sobre 5), incluso que han sacado mejor nota que en un test normal.

Además son conscientes que al repetir varias veces las mismas preguntas han aprendido un poco más (4,66 sobre 5). Todos han utilizado los test creados por los compañeros para estudiar, y además les parece muy útil y favorable poder disponer de los test para ello (4,55 y 4,83 sobre 5).

Para la mayoría ha sido la primera vez que realizan un test con esta dinámica de juego y aproximadamente la mitad afirma que ha afrontado el examen con menos nervios que una prueba ordinaria.

Para futuros trabajos, se pretenden seguir implementando estas estrategias de gamificación, ya no solamente para la realización de evaluaciones, sino sobre todo, para involucrar al alumnado de forma activa en todo el proceso de aprendizaje. Por otro lado se comprobará si hay diferencia en las notas y satisfacción de los participantes en comparación con un test normal, realizando un ensayo doble ciego con un grupo de control que hará una prueba de evaluación tradicional en papel.

REFERENCIAS BIBLIOGRÁFICAS

- Aktekin, N., Çelebi, H., y Aktekin, M.** (2018). Let's Kahoot! Anatomy. *International Journal of Morphology*, 36(2), 716-721. <https://scielo.conicyt.cl/pdf/ijmorphol/v36n2/0717-9502-ijmorphol-36-02-00716.pdf>
- Al-Emran, M., Elsherif, H. M., y Shaalan, K.** (2016). Investigating attitudes towards the use of mobile learning in higher education. *Computers in Human behavior*, 56, 93-102. <https://doi.org/10.1016/j.chb.2015.11.033>

- Basantes, A. V., Naranjo, M. E., Gallegos, M. C., y Benítez, N. M.** (2017). Mobile Devices in the Learning Process of the Faculty of Education Science and Technology of the Technical University of the North in Ecuador. *Formación universitaria*, 10(2). <http://dx.doi.org/10.4067/S0718-50062017000200009>
- Bonwell, C. C., y James, A. E.** (1991). *Active Learning: Creating Excitement in the Classroom*. ASHE-ERIC HigherEducation Report No. 1. The George Washington University, School of Education and Human Development.
- Cambridge International.** (2019). *Aprendizaje Activo*. Cambridge assessment International Education/ UCLES.
- Cánovas, G., García, A., Oliaga, A., y Aboy, I.** (2014). *Menores de edad y conectividad móvil en España: Tablets y Smartphones*. Centro de Seguridad en Internet para los Menores en España: PROTEGELES, dependiente del Safer Internet Programme de la Comisión Europea.
- Cárdenas, C., Véliz, M., y Veliz, L.** (2020). Game-Based Student Response Systems: The Impact of Kahoot in a Chilean Vocational Higher Education EFL Classroom. *CALL-Ej*, 21(1), 64-78.
- Chen, B., y deNoyelles, A.** (2013). Exploring Students' Mobile Learning Practices in Higher Education. *Educause Review*, 7(1), 36-43. <https://er.educause.edu/articles/2013/10/exploring-students-mobile-learning-practices-in-higher-education>
- Deterding, S., Dixon, D., Khaled, R., y Nacke, L.** (2011). From game design elements to gamefulness: defining gamification. *15th International Academic MindTrek Conference: Envisioning Future Media Environments* (pp. 9-15). ACM.
- Ditrendia.** (2019). *Informe ditrendia: Mobile en España y en el mundo*. Ditrendia.

- Durall, E., Gros, B., Maina, M., Johnson, L., y Adams, S.** (2012). *Perspectivas tecnológicas: educación superior en Iberoamérica 2012-2017*. The New Media Consortium.
- Gikas, J., y Grant, M. M.** (2013). Mobile computing devices in higher education: Student perspectives on learning with cellphones, smartphones & social media. *The internet and Higher Education*, 19, 18-26.
- Horizon.** (2017). *Horizon Report: 2017 Higher Education Edition*. The new Media Consortium. <https://library.educause.edu/-/media/files/library/2017/2/2017horizonreporthe.pdf>
- Institute of International Education.** (2014). *Annual Report*. Institute of International education.
- Johnson, L., Adams Becker, S., Estrada, V., Freeman, A., Kampylis, P., Vuorikari, R., y Punie, Y.** (2014). *NMC Horizon Report Europe: 2014 Schools Edition*. The New Media Consortium.
- Kahoot!.** (2021, 2 de junio). *¡Kahoot! para escuelas: Evaluación*. Opgehaald van. <https://kahoot.com/schools/assessment/>
- Kapp, K. M.** (2012). *The gamification of learning and instruction: game-based methods and strategies for training and education*. John Wiley & Sons.
- Keyser, M. W.** (2000). Active Learning and Cooperative Learning: Understanding the Difference and Using Both Styles Effectively. *Research Strategies*, 17(1), 35-40.
- Lee, J. J., y Hammer, J.** (2011). Gamification in Education: What, How, Why Bother? *Academic exchange quarterly*, 15(2), 146.
- Llerena, E., y Rodríguez, C.** (2017). Kahoot! A Digital Tool for Learning Vocabulary in a language classroom. *Revista Publicando*, 4(12), 441-449. <https://revistapublicando.org/revista/index.php/crv/article/view/673>

- Martín, A. M., Herranz, P., y Segovia, M. M.** (2015). Gamificación en la educación, una aplicación práctica con la plataforma Kahoot. *XXV Jornadas ASEPUMA – XIII Encuentro Internacional*. 25. Anales de ASEPUMA.
- Martínez, G.** (2017). Tecnologías y nuevas tendencias en educación, aprender jugando. El caso de Kahoot. *Opción, Revista de Ciencias Humanas y Sociales*, (83), 252-277. <https://dialnet.unirioja.es/servlet/articulo?codigo=6228338>
- Moya, M. d., Carrasco, M. d., Jiménez, A., Ramón, A., Soler, C., y Vaello, T.** (2016). El aprendizaje basado en juegos: experiencias docentes en la aplicación de la plataforma virtual “Kahoot”. *XIV Jornades de Xarxes d’Investigació en Docència Universitària. Investigació, innovació i ensenyament universitari: enfocaments pluridisciplinaris* (pp. 1241-1254). Universitat d’Alacant, Institut de Ciències de l’Educació.
- Naciri, A., Baba, M. A., Achbani, A., y Kharbach, A.** (2020). Mobile learning in Higher education: Unavoidable alternative during COVID-19. *Aquademia*, 4(1), 1-2. <https://www.aquademia-journal.com/article/mobile-learning-in-higher-education-unavoidable-alternative-during-covid-19-8227>
- Nuthall, G.** (2007). *The Hidden Lives of Learners*. NZCER Press.
- OECD.** (2020). *Education at a Glance 2020*. OECD.
- Pintor, E., Gargantilla, P., Herreros, B., y López, M.** (2014). Kahoot en docencia: una alternativa practica a los clickers. *XI Jornadas Internacionales de Innovación Universitaria, Educar para transformar*, (pp. 322-329). Villaviciosa de Odón.
- Rodríguez-Fernández, L.** (2017). Smartphones y aprendizaje: el uso de Kahoot en el aula universitaria. *Revista Mediterránea de Comunicación*, 8(1), 181-190. <https://doi.org/10.14198/MED-COM2017.8.1.13>

- Rojas-Viteri, J., Álvarez-Zurita, A., y Bracero-Huertas, D.** (2021). Uso de Kahoot como elemento motivador en el proceso enseñanza-aprendizaje. *Revista Cátedra*, 4(1), 98–114. <https://revistadigital.uce.edu.ec/index.php/CATEDRA/article/view/2815>
- Sánchez, M. L.** (2012). Uso del dispositivo móvil como recurso digital. *Didáctica, innovación y multimedia*, 1-10. <https://raco.cat/index.php/DIM/article/view/252453>
- UNESCO.** (2015). *La Educación para Todos, 2000 - 2015, Logros y Desafíos*.
- Wang, A., y Tahir, R.** (2020). The effect of using Kahoot! for learning – A literature review. *Computers & Education*, 149, 103818. <https://doi.org/10.1016/j.compedu.2020.103818>
- Zhang, Q., y Yu, Z.** (2021). *A literature review on the influence of Kahoot! On learning outcomes, interaction, and collaboration*. Education and Information Technologies.

/04/

DEVELOPMENT OF COMPUTATIONAL LINGUISTIC RESOURCES FOR AUTOMATED DETECTION OF TEXTUAL CYBERBULLYING THREATS IN ROMAN URDU LANGUAGE

Amirita Dewani

Mehran University of Engineering & Technology, Jamshoro, Sindh, (Pakistan).
E-mail: amirita@faculty.muett.edu.pk ORCID: <https://orcid.org/0000-0002-3816-3644>

Mohsin Ali Memon

Mehran University of Engineering & Technology, Jamshoro, Sindh, (Pakistan).
E-mail: mohsin.memon@faculty.muett.edu.pk ORCID: <https://orcid.org/0000-0003-2638-4252>

Sania Bhatti

Mehran University of Engineering & Technology, Jamshoro, Sindh, (Pakistan).
E-mail: sania.bhatti@faculty.muett.edu.pk ORCID: <https://orcid.org/0000-0002-0887-8083>

Recepción: 20/04/2021 **Aceptación:** 10/06/2021 **Publicación:** 29/06/2021

Citación sugerida:

Dewani, A., Memon, M. A., y Bhatti, S. (2021). Development of computational linguistic resources for automated detection of textual cyberbullying threats in Roman Urdu language. *3C TIC. Cuadernos de desarrollo aplicados a las TIC*, 10(2), 101-121. <https://doi.org/10.17993/3ctic.2021.102.101-121>

ABSTRACT

Automatic Cyberbullying detection has remained very challenging task since social media content and conversations are usually posted in unstructured free-text form leaving behind the language norms. The major concern and gap in formulating cyberbullying detection strategies is scarcity of available linguistic resources typically for newly evolved languages. Roman Urdu has recently emerged and hence is a resource poor language. Urdu has been widely known as the national language of Pakistan. However, because of socio-cultural and multilingual aspects, Roman Urdu is used widely on the Internet by Asians and more specifically Pakistanis.

To fulfil the above stated gap, this research work presents guidelines for data annotation process and developed two linguistic resources: (i) Annotated corpus in Roman Urdu Language for cyberaggression and offensive language detection. The process of data annotation involved bilingual annotators instead of crowdsourcing. It has the benefit of correctly annotating instances that constitute clear cases of cyberbullying without compromising data quality. The developed corpus is highly balanced (with almost negligible skew) unlike most of the existing corpuses even in mature languages. (ii) Processing textual information for NLP tasks involves Stop-word elimination as a sub phase. Stop words carry least semantic information and increase feature space as compared to the other tokens and index terms in corpora. We have developed domain specific stop words for Roman Urdu Language considering all the lexical variants and typically in the context of aggression detection and collected data. The work has been carried out using python programming language and Pycharm IDE.

KEYWORDS

Linguistic Resources, Cyberaggression, Cyberbullying, Hate Speech Detection. Abusive Language Automated Detection.

1. INTRODUCTION

The rapid advancement in technology and compelling needs of users have made internet and typically SNS's an integral part of everyone's life, resulting in huge amount of user generated content aka Big social media data. Escalation in Social media has completely shifted the way in which people view, create or share information and ideas (Namdeo *et al.*, 2017).

Undeniably, Web 2.0 has a vital role in the communication, relationships, and collaboration in today's society. The communities belonging to different age groups (children, youngsters, and adults) interact with each other anytime, anywhere in diverse ways (e.g. via laptops, smartphones, tablets etc.) and using wide number of social networking platforms. Even though the perks and positive edges of digital communication are evident since most of the user's internet usage is harmless but the anonymity preservation and freedom of speech often makes young people to be offensive and vulnerable leading towards one of the alarming threat i-e cyberbullying/Cyberaggression or hate speech (Van Hee *et al.*, 2018). People, typically youngsters have reported life disturbing and annoying experiences thus drawing the attention of researchers/scholars and making cyberbullying and its automatic detection a growing community need and a promising area of Natural Language Processing (NLP) (Huang *et al.*, 2018).

Several studies contributed by different researchers are evident that computational formation of cyberaggression detection strategies is extremely challenging. One of the major challenges is posed by the scarcity of the required resources typically for newly emerged languages. Moreover, most of the datasets used for cyberbullying detection, even in mature languages, exhibit an extreme skew between hate speech and non-hate speech textual contents (Emmery *et al.*, 2020). This leads to formation of inappropriate strategies, unreliable predictive performance (specifically for the minority class) and more sensitivity towards classification errors.

With advent of Unicode encoding, Urdu language content, written using roman script, is escalating rapidly on social networking sites. Roman Urdu is a nonnormative language. The written script of

this language does not follow any rigid set of grammatical rules or standards of spellings. A survey statistics in (Shahroz *et al.*, 2020) affirms that about 300 million people are speaking Urdu language and approximately 11 million speakers are in Pakistan from which maximum users switched to Roman Urdu language for the textual communication, typically on social media (Shahroz *et al.*, 2020). It is linguistically rich and morphologically complex language (Mehmood *et al.*, 2020).

Urdu orthography (aka imla) bears a resemblance to Trukish, Arabic and Persian languages. Moreover, cursive Arabic and Nastaliques writing style is used (Syed *et al.*, 2010). Roman Urdu uses Roman script. An example instance of Roman Urdu script and its equivalent Urdu and English scripts are depicted in Figure 1.

Figure 1. Script and Morphological variability in Roman Urdu, Urdu, and English Language.

Source: own elaboration.

Regardless of its huge prevalence worldwide (and more specifically in South Asia), Roman Urdu is an under-resource language. Linguistic resources for Asian languages are typically focused by some of the conferences and journals such as ACM Transactions on Asian and Low-Resource Language Information Processing (“ACM Transactions on Asian and Low-Resource Language Information Processing”, n.d.), International Joint Conference of Natural Language Processing (“First Task for Automatic Cyberbullying Detection for the Polish Language | ACL Member Portal”, 2019), Conference

of Central Asian Language and Linguistics (“Central Asian Languages and Linguistics”, n.d.) etc. for supporting vast number of NLP tasks related to phonology, morphology, name entity recognition (NER), language parsing and word segmentation.

To support the development of NLP applications for Roman Urdu typically in the field of cyberaggression and hate speech, this paper presents annotation guidelines, the first-ever highly balanced Roman Urdu dataset and development of domain specific stop words using python language.

Rest of this paper is organized as follows: Cyberaggression and existing resources are conferred in section II. Section III puts light on Data extraction from Twitter social media platform. Data annotation guidelines preparation and kappas weighing scheme are given in section VI & V respectively. Section VI discusses Stop word development. Finally, Section VII conclude the research work.

2. RELATED WORK

Even though the researchers have widely used Natural Language Processing (NLP) and realized Machine Learning (ML) techniques to uncover solutions for variety of tasks based on unstructured text data (e.g. topic identification, opinion mining, document summarization, text translation etc.), but it’s applicability for resolving automatic detection of cyber-crime related problems is relatively new and has encountered so many challenges (Rosa *et al.*, 2019).

The availability of appropriate data, huge data skew because of natural uneven distribution of hate speech content on social media and NLP resources scarcity represents one amongst many significant issues in research on cyberbullying detection (Mahlangu *et al.*, 2018; Gencoglu, 2020). A handful of studies are contributed by scholars to develop resources and cyberbullying detection strategies in different languages worldwide. Most studies have hateful instances ranging from 2 to 5% (Emmery *et al.*, 2020).

The study by Sprugnoli *et al.* (2018), developed a WhatsApp dataset from WhatsApp chats to study offensive language among Italian students. They also presented annotation scheme and user roles.

Research work accomplished in Fersini *et al.* (2018) collected misogynous and hateful tweets data using a combined approach. They monitored prospective victims of hate accounts, downloading the history of identified haters and filtered twitter stream contents via keywords.

The study conducted in Fišer *et al.* (2017) extracted data from an online platform that collects impulsive reports by internet users of any material having Child sex abuse; a special category of cyber-aggressiveness, to develop a corpus. The validation of corpus by experts revealed that only 3% was illegal content and more than 40% in non-disturbing content. Indonesian language hateful corpus was contributed in Ibrohim and Budi (2018). The research work used twitter platform, crowdsourcing annotation, and a multi-level scheme to identify Hate speech and non-hate speech categories along with their intensity levels. Work carried out in Bohra *et al.* (2018) presents a dataset comprising of Hindi-English code-mixed data. The tweets are annotated with the language at word level and the class they belong to (Hate Speech or Normal Speech).

The study in Van Bruwaene *et al.* (2020) formed a dataset using multiple platforms in English language from SafeToNet's VISR-branded child safety app for adolescents. In collaboration with expert annotators, they utilized crowd sourcing and machine learning techniques to enlarge the corpus and handle skew in iterative manner. The work by Özel *et al.* (2017) is the first study performed in Turkish Language. The research has contributed corpus in Turkish language prepared using Instagram and twitter social media platforms. Experimentation is also conducted using machine learning techniques.

Undeniably, English is the de facto common language among researchers at international level, hence greater number of computational resources, as highlighted by a review study (Poletto *et al.*, 2020) are English corpora and datasets. Nevertheless, several other languages are represented too, and this certainly is immensely significant for international community that seeks to address a worldwide social issue of cyberbullying and hate speech spread in many languages.

Roman Urdu has become a contemporary trend these days as a language of communication for Pakistani or more generally Asian youth. To the best of knowledge, this is the first ever study that has developed computational linguistic resource of Roman Urdu for Cyberaggression. This research study presents our approach for collecting and annotating social media data to develop a cyberbullying corpus in Roman Urdu language and domain specific stop words. The extraction of data was a multi-phase process to ensure high quality data with minimum skew. It encompasses vast range of content inciting hatred. The content is also based on wide bullying tactics like race, ethnic origin, religious affiliation, sexual orientation, caste, gender, identity and serious disease or disability Intelligence. Since a natural distribution of social media data is heavily skewed which results in a scarcity of bullying instances to be used in training, So we did extraction in phases. Moreover, this work used different weighing schemes for automatic identification and bilingual expert annotators manual input to develop stop words related to cyberbullying detection problem in Roman Urdu.

3. METHODOLOGY

3.1. DATA EXTRACTION

Twitter is one of the most popular microblogging service having 316 million monthly active users. As compared to other social media platforms, twitter has attracted more to the academic researchers as it makes its data available for research purposes via Application Programming Interface (API) (Ahmed *et al.*, 2017). To develop cyberbullying corpus, data was scrapped from twitter using python language, tweepy and twitter streaming API in multiple phases over the duration of 3 months as depicted in Figure 2. The reasons were twofold: (i) Restrictions on data access imposed on standard API (ii) The natural distribution of content is highly skewed.

Figure 2. Data Extraction- Tweet Count.
Source: own elaboration.

Currently, no language code is available for Roman Urdu in API, So the queries for data collection were formed based on geo-location information; taking coordinates from google maps of the areas in Pakistan where high saturation of Roman Urdu content was expected. Secondly, we extracted tweets based on insulting seeds or curse words typically used in Roman Urdu language for bullying. Thirdly we used hash values for aggression and trash talking on recent topics from the regions in Pakistan. Substantial number of tweets were in English Language and such content was filtered out leaving behind 3K tweets. In order to retain writing patterns of Roman Urdu users on social media, data with inherent English words (*such as batting, topic, character, bowling, follow, design, ok, yes, no, music, video, free, hope, player, code, development, etc.*) was preserved. Some examples of such data instances are depicted in Figure 3.

2021-01-02 15:03:03 ,b' Yakeen karen Follow back milnay kay bad unfollow karny waly log kisi ky sagge nahe ho saky ..., "b'Karachi, Pakistan"
 2020-12-15 18:44:06,b' Acha atleast tell me boards k papers postpone hone ki koi probability hai?', "b' Faisalabad, Pakistan"

Figure 3. Natural writing patterns of users on social media in Roman Urdu Language.

Source: own elaboration.

3.2. DATA ANNOTATION PROCESS

Data annotation is indeed a Human Intelligence Task (HIT). Undeniably, crowdsourcing has obvious organizational advantages, especially for a time consuming task as the annotation of textual data, but annotation quality might get compromised from employing non-expert annotators typically for recently evolved languages and challenging task like cyberaggression (Schmidt & Wiegand, 2017). Moreover, many studies have uncovered that a non-trivial percentage of the data collected on MTurk is “doubtous”, annotated either by “non-respondents” (bots instead of humans) or non-serious respondents (Dreyfuss *et al.*, 2018; Ahler *et al.*, 2019).

Instead of crowdsourcing, data was annotated by linguistic experts having bilingual expertise (having good knowledge of Nastaliq scripting and Roman Urdu patterns). Annotators were provided with guidelines on how to label social media documents for bullying. The main task of each annotator was to label each sample with one of three possible labels:

- 0 – text certainly does not contain any form of online violence, hate speech or abusive language.
- 1 – text certainly contains any form of online violence, hate speech or abusive language
- 2 – Indeterminate case(doubtful) when text cannot be identified with good certainty to either contain or do not contain any form of online violence, hate speech or abusive language.

To provide the annotators with some context and preserve original writing intentions, all posts were presented in their original form i-e before applying major text preprocessing techniques, wherever possible. Social Media data is considered as Microtext (Mehmood *et al.*, 2020). Microtext is extremely noisy. Deep comprehension of microtext is immensely important for effective understanding and further processing. Hence preliminary Text preprocessing was applied to handle Unicodes, punctuations, hashtags, emojis, URLs, case conversion, date and time data, insignificant string literals, and @ user mentions. The preprocessing results are given in Figure 4.

Figure 4. Preliminary Text preprocessing on Roman Urdu Data.

Source: own elaboration.

To avoid any incorrect annotation, the linguistic experts were encouraged to use “2” whenever they have doubts if an instance contains any form of aggressive speech or not. The example of such doubtful instances is given in Figure 5.

2020-12-18 09:42:05,b' Inse acha to aj kal gali cricket match me ache catch hote hai', b"
2020-12-18 01:31:55,"b""iska jab dosri larki kay sath affair tha he to sara ki zinadgi tabah ki
2020-12-18 09:25:42,b' Ziyada Free Na Ho dono main interest the hai,b"

Figure 5. Examples of instance might be tagged as 2 by annotators.

Source: own elaboration.

Because of the huge size of dataset, the whole annotation process was split into multiple phases. The entire annotation process was conducted by linguistic experts as per developed guidelines and categories.

Based on these phases, the final labels were determined using weighting scheme described in section 5. The main concern of annotators was to analyze which types of phenomena in Roman Urdu can be considered as cyberbullying/hate speech (e.g. attack on personality characteristics, threats, curse, blackmails) or profanity/ abusive language and aggressiveness that might harm an individual's physical or mental health, lower self-esteem or hurt feelings. The sample data instances for each category are given in Table 1.

Table 1. Cyberbullying categories and Roman Urdu Instances.

S. No	Category	Example Instances
1	Threat or blackmail	beta Himat hai na to mujhse milnay aajana batata hon phr' Main tumhaun choron ga nahe tum bas dekhti jao.
2	Racism	Bhai extra bounce jidr ho hum Acha ni krte, remember World Cup main West Indies shediyon ne kiya kia tha Humare saath African jaise hogaye ho shakal dekho apni, jutt zameendaar log hain ye to phir dimag bhi to utna chalay ga
3	Insult	Ji uncle ap chaly jayein please twitter suit nahe krta ap pay Subha subha mazaq acha nai lgta shaista ko bolo apna talak karwaya ab doosron ka karwao:/'
4	Sexual Talk	kapray kam hote ja rahe hain, Oh babs, shayad sex education topic nahe parha main parha doon baby
5	Curse or exclusion	yes, you are the only one jo itna bura hy. dua kar raha hoon k tum mar jao. Allah karay tum hamesha aziyat main raho takleef main raho kabhi khush na raho
6	Defamation	don't expect ye jhooti aurat acha acha sach bolegi Hhhhhhhh acha mazak hai lanat ho tm par aur tumhary channel pr'
7	Encouragements to the harasser	Sahi kah raha hai tum mar kiyon neh jati itni badnami kafi neh hai kiya
8	Personality characteristics	Ary ry ry tum to pooray aalo ban gaye ho ek hota hai kaala aur phir aata hai daambar ka tukra

Source: own elaboration.

3.3. WEIGHING SCHEME

Since the process of annotation is a subjective phenomenon, hence different annotators might have a bit different judgment for the same textual comments. To eliminate dubious data and to ensure data quality

and for further scrutiny and validation of dataset, Inter-Rater Reliability (IRR/IRA) was estimated using Cohen's kappa coefficient (κ) (definition 5.1). for measurement of inter-annotator agreement, Cohen's kappa coefficient has been accepted as the de facto standard. Empirically, based on kappa score the threshold value or cut off value is set. Usually, kappa score of 0.67 is used as a cutoff in computational linguistics (Wang *et al.*, 2019).

3.3.1. DEFINITION AND COMPUTATION OF COHEN' S KAPPA

Cohen's kappa is a function of p_o , the relative observed agreement, and p_e , the expected hypothetical agreement by chance. Mathematically it can be stated as in equation 1.

$$\kappa = \frac{p_o - p_e}{1 - p_e} \quad \dots\dots (1)$$

Where p_o i-e observed agreement can be computed using Equation (2).

$$p_o = \frac{\text{count of agreements}}{\text{ount of agreements} + \text{count of disagreements}} \quad \dots\dots (2)$$

and p_e i-e the expected agreement by chance can be computed using Equation (3).

$$p_e = \frac{1}{N^2} \sum_k n_{k1} n_{k2} \quad \dots\dots (3)$$

Where N indicates the number of items, k is the number of categories, n_{k1} is the number of times rater 1 selected category k , and n_{k2} is the number of times rater 2 selected category k .

The kappa score was computed using Statistical Software (n.d.). The standard error and 95% confidence interval are calculated according to Fleiss *et al.* (2013). The weighted kappa score as shown in Table 2 is significantly higher than the cutoff value.

Table 2. Weighted Kappa Score.

Weighted Kappa	0.81818
Standard Error	0.12730
95% CI	0.56868 to 1.00000

Source: own elaboration.

4. RESULTS

4.1. IDENTIFICATION OF DOMAIN SPECIFIC STOP WORDS

In this era of big data and information retrieval, process optimization for Text and Data Analytic systems becomes immensely significant. Therefore, to achieve accuracy, identification & filtration of terms with minimal or no semantic meaning is significant. Stop words has been developed in so many languages like English, Italian, Chinese, Arabic, Punjabi, Hindi, etc. (Kaur & Saini, 2015, 2016; Hao & Hao, 2008; Alajmi *et al.*, 2012) and are also part of NLTK, spaCy, and gensim.

Stop words not only vary from corpora to corpora, language to language, they also vary from one problem domain to another. For example, in a corpus of news articles, comprising of crucial information that is time-sensitive and location-sensitive, eliminating terms like “here”, “today”, etc. would affect results of related NLP application. This is because news articles link and relate current event to the similar events that had happened in the past or on another location.

In this work, we have identified stop-words from developed corpora, specific to the domain of cyberbullying and hate speech using statistical methods and human evaluation i-e direct Term Frequency (TF), Inverse-Document Frequency (IDF), Term-Frequency-Inverse-Document-Frequency (TFIDF) weighting model and human evaluation by bilingual experts. The methods are described below.

Let $tf(t,d)$ denotes direct frequency of term t in document d . Mathematically, it can be defined as:

$$tf(t, d) = fd(t) / \max_{w \in d} fd(w)$$

where $fd(w)$ indicates the total number of words in a document. The metric term frequency highlights commonality of a term within a collection of documents. Semantically least significant terms are expected to have high term frequency. 30 samples, based on term frequencies are depicted in Figure 6.

Figure 6. Samples based on term frequencies (n=30).

Source: own elaboration.

Inverse document frequency, idf can be defined mathematically as:

$$Idf(t, D) = \ln \left[\frac{|D|}{|\{d \in D: t \in d\}|} \right]$$

Where, D is the collection of documents in the corpus.

This metric is very significant since it penalizes the more frequently occurring terms and favors the ones occurring in a few documents only. The lower bound of this metric is 0 and refers to the terms that appear in every single document in the corpus 40. Feature names sorted by their idf weights in ascending order are given in Figure 7.

Figure 7. Feature names by idf weights (Sorted in ascending order).

Source: own elaboration.

```
[ 'aap' 'ab' 'abhi' 'acha' 'ache' 'achi' 'agar' 'aise' 'ajeeb' 'allah'
  'and' 'ap' 'apko' 'apna' 'apni' 'aur' 'aye' 'baad' 'baat' 'bahut' 'ban'
  'bana' 'bas' 'bat' 'bhai' 'bhi' 'bht' 'bilkul' 'birthday' 'but' 'chaiye'
  'chal' 'chor' 'de' 'dekh' 'dekha' 'dekho' 'dil' 'dimag' 'din' 'diya' 'do'
  'dono' 'dont' 'dost' 'ek' 'ga' 'gay' 'gaya' 'gaye' 'ghar' 'gi' 'good'
  'ha' 'hai' 'hain' 'hamesha' 'har' 'he' 'hi' 'ho' 'hoga' 'hogaye' 'hon'
  'hona' 'hoon' 'hota' 'hoti' 'hu' 'hua' 'hum' 'hun' 'hy' 'in' 'insan' 'is'
  'itna' 'itne' 'itni' 'ja' 'jab' 'jaisay' 'jao' 'jaye' 'jo' 'ka' 'kaam'
  'kabhi' 'kahin' 'kam' 'kar' 'karay' 'karen' 'karna' 'karo' 'karta'
  'karte' 'kay' 'ke' 'khud' 'khush' 'ki' 'kia' 'kisi' 'kiya' 'kiyon' 'ko'
  'koi' 'kr' 'krna' 'kro' 'kuch' 'kya' 'lag' 'laga' 'lagta' 'larki' 'le'
  'liye' 'lo' 'log' 'lolz' 'love' 'mai' 'main' 'maine' 'mar' 'mat' 'me'
  'mein' 'mera' 'meray' 'mere' 'mujhay' 'mujhe' 'my' 'na' 'nahe' 'nahen'
  'nahi' 'ne' 'nhi' 'of' 'oh' 'or' 'par' 'pass' 'pata' 'pe' 'pehle' 'phir'
  'phr' 'please' 'raha' 'rahay' 'rahe' 'raho' 'rha' 'sab' 'sachi' 'sahi'
  'sath' 'say' 'se' 'shakal' 'sirf' 'so' 'sorry' 'sy' 'tak' 'tarah' 'tha'
  'the' 'theek' 'thi' 'time' 'to' 'toh' 'tou' 'tu' 'tum' 'tumhain'
  'tumhara' 'tumhare' 'tweet' 'us' 'use' 'wah' 'wala' 'warna' 'wo' 'woh'
  'ya' 'yaar' 'yahan' 'yar' 'ye' 'yeh' 'you' 'ziada' ]
```

Figure 8. Terms sorted by low Tfidf scores (max-features= 200).

Source: own elaboration.

Figure 9. Cloud Representation of Corpus. (a) Prior to removal of stop words. (b) After removal of stop words.
Source: own elaboration.

7. CONCLUSIONS

Social networking sites has become a communal breeding ground for youth to aggress one another. During the pandemic, the traffic in cyberspace increased significantly. Recent studies and published news reports highlight that there is great surge in the number of cyberbullying and harassment cases during the pandemic. This paper made novel contributions and achieved important landmark in regard of NLP on Roman Urdu language which has been embraced recently on social media by youth. The corpus was developed for cyberbullying and hate speech by collecting data for over 3 months to have high quality data with less skew. A well-defined set of data annotation guidelines were prepared and provided to experts for annotation. Since the process of annotation was a subjective phenomenon, hence, for further scrutiny and validation of corpus, Inter-Rater Reliability (IRR) based on Cohen's kappa coefficient(κ) was identified using statistical software Medcalc. Finally, the work rigorously developed an automatic stop word identification strategy using statistical methods and weighing model. Moreover, manual input

of linguistic experts was also taken to form comprehensive list specific to cyberbullying corpus. In future we plan to conduct experiments using deep learning approaches and hand engineered feature sets. As the field of cyberaggression and cyberbullying is at its emergence so this research would greatly benefit NLP and machine learning research community.

ACKNOWLEDGEMENTS

This research has been performed at Institute of information Technology, Mehran University of Engineering and Technology, Pakistan and is Funded under MUET funds for postgraduate students. We would like to thank bilingual experts Ms. Irum Parvaiz (Lecturer Dawood University of Engineering & Technology) and Mariyam Bughio (Assistant Professor, Zubaida Degree Girls college) for huge support through data annotation process.

REFERENCES

- ACM Transactions on Asian and Low-Resource Language Information Processing* (n.d.). <https://dl.acm.org/journal/tallip>
- Ahler, D. J., Roush, C. E., & Sood, G.** (2019). *The micro-task market for lemons: Data quality on Amazon's Mechanical Turk*. Meeting of the Midwest Political Science Association.
- Ahmed, W., Bath, P. A., & Demartini, G.** (2017). *Using Twitter as a Data Source: An Overview of Ethical, Legal, and Methodological Challenges*. In *The Ethics of Online Research* (pp. 79–107). Emerald Publishing Limited.
- Alajmi, A., Saad, E. M., & Darwish, R. R.** (2012). Toward an ARABIC stop-words list generation. *International Journal of Computer Applications*, 46(8), 8–13. https://www.researchgate.net/publication/306364790_Toward_an_ARABIC_Stop-Words_List_Generation

- Bohra, A., Vijay, D., Singh, V., Akhtar, S. S., & Shrivastava, M.** (2018). A Dataset of Hindi-English Code-Mixed Social Media Text for Hate Speech Detection. *Proceedings of the Second Workshop on Computational Modeling of People's Opinions, Personality, and Emotions in Social Media*, 36–41.
- Central Asian Languages and Linguistics*. (n.d.). <https://concall.indiana.edu/papers.html>
- Dreyfuss, E., Barrett, B., & Newman, L. H.** (2018). *A bot panic hits Amazon's Mechanical Turk*. *Wired*. <https://www.wired.com/story/amazon-mechanical-turk-bot-panic/>
- Emmery, C., Verhoeven, B., De Pauw, G., Jacobs, G., Van Hee, C., Lefever, E., Desmet, B., Hoste, V., & Daelemans, W.** (2020). Current limitations in cyberbullying detection: On evaluation criteria, reproducibility, and data scarcity. *Language Resources and Evaluation*, 1–37. https://www.researchgate.net/publication/336869277_Current_Limitations_in_Cyberbullying_Detection_on_Evaluation_Criteria_Reproducibility_and_Data_Scarcity
- Fersini, E., Nozza, D., & Rosso, P.** (2018). Overview of the evalita 2018 task on automatic misogyny identification (ami). *Evalita Evaluation of NLP and Speech Tools for Italian*, 12, 59. http://personales.upv.es/prosso/resources/FersiniEtAl_Evalita18.pdf
- First Task for Automatic Cyberbullying Detection for the Polish Language | ACL Member Portal*. (2019). <https://www.aclweb.org/portal/content/deadline-extension-first-task-automatic-cyberbullying-detection-polish-language>
- Fišer, D., Erjavec, T., & Ljubešić, N.** (2017). Legal framework, dataset and annotation schema for socially unacceptable online discourse practices in Slovene. *Proceedings of the First Workshop on Abusive Language Online*, 46–51. <https://www.aclweb.org/anthology/W17-3007/>
- Fleiss, J. L., Levin, B., & Paik, M. C.** (2013). *Statistical methods for rates and proportions*. John Wiley & Sons.

- Gencoglu, O.** (2020). *Cyberbullying detection with fairness constraints*. IEEE Internet Computing.
- Hao, L., & Hao, L.** (2008). Automatic identification of stop words in chinese text classification. In *2008 International Conference on Computer Science and Software Engineering*, 1, 718–722. <https://www.semanticscholar.org/paper/Automatic-Identification-of-Stop-Words-in-Chinese-Hao-Hao/cd7d1fdf-3b3eec1ebc9378065279442bacbf6fa5>
- Huang, Q., Inkpen, D., Zhang, J., & Van Bruwaene, D.** (2018). Cyberbullying Intervention Interface Based on Convolutional Neural Networks. *Proceedings of the First Workshop on Trolling, Aggression and Cyberbullying*, 42. <https://www.aclweb.org/anthology/W18-4405/>
- Ibrohim, M. O., & Budi, I.** (2018). A dataset and preliminaries study for abusive language detection in Indonesian social media. *Procedia Computer Science*, 135, 222–229. <https://doi.org/10.1016/j.procs.2018.08.169>
- Kaur, J., & Saini, J.** (2016). Stop-Word Removal Algorithm and its Implementation for Sanskrit Language. *International Journal of Computer Applications*, 150, 15–17. <https://doi.org/10.5120/ijca2016911462>
- Kaur, J., & Saini, J. R.** (2015). A Natural Language Processing Approach for Identification of Stop Words in Punjabi Language. *Annals of Health and Health Sciences-Indian Journals*, 5(2), 114-120. <https://doi.org/10.5958/2249-3220.2015.00015.4>
- Mahlangu, T., Tu, C., & Owolawi, P.** (2018). A review of automated detection methods for cyberbullying. In *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, 1–5. <https://www.semanticscholar.org/paper/A-Review-of-Automated-Detection-Methods-for-Mahlangu-Tu/fc86a8bab87e3cdb6cc1f35bf38094aa373d88de>

- Mehmood, F., Ghani, M. U., Ibrahim, M. A., Shahzadi, R., Mahmood, W., & Asim, M. N.** (2020). A precisely xtreme-multi channel hybrid approach for roman urdu sentiment analysis. *IEEE Access*, 8, 192740–192759. <https://ieeexplore.ieee.org/document/9223633>
- Namdeo, P., Pateriya, R. K., & Shrivastava, S.** (2017). A Review of Cyber bullying Detection in Social Networking. *Proceedings of ICICCT*, 162–170.
- Özel, S. A., Saraç, E., Akdemir, S., & Aksu, H.** (2017). Detection of cyberbullying on social media messages in Turkish. In *2017 International Conference on Computer Science and Engineering (UBMK)*, 366–370.
- Poletto, F., Basile, V., Sanguinetti, M., Bosco, C., & Patti, V.** (2020). Resources and benchmark corpora for hate speech detection: a systematic review. *Language Resources and Evaluation*, 1–47. <https://doi.org/10.1007/s10579-020-09502-8>
- Rosa, H., Pereira, N., Ribeiro, R., Ferreira, P. C., Carvalho, J. P., Oliveira, S., Coheur, L., Paulino, P., Simão, A. M. V., & Trancoso, I.** (2019). Automatic cyberbullying detection: A systematic review. *Computers in Human Behavior*, 93, 333–345. <https://doi.org/10.1016/j.chb.2018.12.021>
- Schmidt, A., & Wiegand, M.** (2017). A survey on hate speech detection using natural language processing. *Proceedings of the Fifth International Workshop on Natural Language Processing for Social Media*, 1–10. <https://www.aclweb.org/anthology/W17-1101/>
- Shahroz, M., Mushtaq, M. F., Mehmood, A., Ullah, S., & Choi, G. S.** (2020). RUTUT: Roman Urdu to Urdu Translator Based on Character Substitution Rules and Unicode Mapping. *IEEE Access*, 8, 189823–189841.
- Sprugnoli, R., Menini, S., Tonelli, S., Oncini, F., & Piras, E.** (2018). Creating a whatsapp dataset to study pre-teen cyberbullying. *Proceedings of the 2nd Workshop on Abusive Language Online (ALW2)*, 51–59.

Statistical Software. (n.d.). <https://www.medcalc.org/>

Syed, A. Z., Aslam, M., & Martinez-Enriquez, A. M. (2010). Lexicon Based Sentiment Analysis of Urdu Text Using SentiUnits. In Sidorov, G., Hernández, A., Reyes, C. A. (eds) *Advances in Artificial Intelligence*. MICAI 2010. Lecture Notes in Computer Science, vol 6437. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-16761-4_4

Van Bruwaene, D., Huang, Q., & Inkpen, D. (2020). A multi-platform dataset for detecting cyberbullying in social media. *Language Resources and Evaluation*, 54(4), 851–874. <https://doi.org/10.1007/s10579-020-09488-3>

Van Hee, C., Jacobs, G., Emmery, C., Desmet, B., Lefever, E., Verhoeven, B., De Pauw, G., Daelemans, W., & Hoste, V. (2018). Automatic detection of cyberbullying in social media text. *PloS One*, 13(10), e0203794. <https://doi.org/10.1371/journal.pone.0203794>

Wang, J., Yang, Y., & Xia, B. (2019). A Simplified Cohen's Kappa for Use in Binary Classification Data Annotation Tasks. *IEEE Access*, 7, 164386–164397.

/05/

METHODOLOGY BASED ON THE NIST CYBERSECURITY FRAMEWORK AS A PROPOSAL FOR CYBERSECURITY MANAGEMENT IN GOVERNMENT ORGANIZATIONS

Maurice Frayssinet Delgado

Graduate University School - EUPG - Federico Villarreal National University, (Peru).

E-mail: mfrayssinet@gmail.com ORCID: <https://orcid.org/0000-0001-6223-2577>

Doris Esenarro

Specialized Institute for Ecosystems and Natural Resources Research (INERN).

Graduate University School - EUPG - Federico Villarreal National University, (Peru).

E-mail: desenarro@unfv.edu.pe ORCID: <https://orcid.org/0000-0002-7186-9614>

Francisco Fernando Juárez Regalado

Graduate University School - EUPG - Federico Villarreal National University,

Universidad Tecnológica del Perú-UTP, (Peru).

E-mail: fjuarezr@hotmail.com ORCID: <https://orcid.org/0000-0002-3942-7832>

Mónica Díaz Reátegui

Graduate University School - EUPG - Federico Villarreal National University.

Universidad Norbert Wiener, (Peru).

E-mail: monicdre@yahoo.com ORCID: <https://orcid.org/0000-0003-4506-7383>

Recepción: 29/04/2021 **Aceptación:** 18/06/2021 **Publicación:** 29/06/2021

Citación sugerida:

Frayssinet, M., Esenarro, D., Juárez, F. F., y Díaz, M. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. *3C TIC. Cuadernos de desarrollo aplicados a las TIC*, 10(2), 123-141. <https://doi.org/10.17993/3ctic.2021.102.123-141>

ABSTRACT

This research aims to propose the use of the methodology based on the NIST Framework for adequate management of cybersecurity in government organizations within the framework of the delivery of digital services. Many government organizations have been managing cybersecurity without a defined process; this generates that the management is deficient and without indicators. Concerning whether they are implementing the methodology based on the NIST cybersecurity framework”, shows that 36.8% of respondents present a level in disagreement, 31.6% (6) an undecided level, 15.8% (3) a level of agreement, 10.5% (2) a level totally in disagreement and 5.3% (1) a level totally in agreement. Meanwhile, the variable “The management of cybersecurity” shows that 36.8% (7) of the Ministries surveyed present a level in disagreement; 36.8% (7) an undecided level, 15.8% (3) a level of agreement, and 10.5% (2) a level totally in disagreement In conclusion: It has been shown that the use of the methodology based on the NIST cybersecurity framework influences cybersecurity management in government organizations and it is clear that they are currently not using it which causes a relatively poor level of leadership in the implementation of security measures concerning cybersecurity management.

KEYWORDS

Methodology, Nist Cybersecurity Framework, Cybersecurity, Management.

1. INTRODUCTION

New information technologies have been developing more and more, giving rise to more significant interaction of the internet the person, which causes a large volume of information within cyberspace, such fact has led to the emergence of digital threats, which cause adverse effects on the lives of people and many institutions, being victims of information theft. Often cybercriminals can not be identified by the authorities, so States have to adapt their structures and use regulatory frameworks, strategies, or cybersecurity policies (Nagurney & Shukla, 2017). In the region, it is possible to highlight that there are already ten countries with a national cybersecurity policy or strategy. Recently, the Dominican Republic and Guatemala joined the list integrated by Colombia, Trinidad and Tobago, Jamaica, Panama, Chile, Costa Rica, Mexico, and Paraguay (Alvarez, 2018). In the case of Peru, it could be said that it is a country with insufficient awareness in terms of digital security, risks, and protection, being one of the countries that have legislated the least in terms of cyber defense and cybersecurity, i.e., there are no national security strategies. Therefore, there is a need to take protective measures against malicious attacks within both the public and private sectors (Montes, 2020).

In a comparison made in the Cybersecurity Report 2020, it can be observed that in Peru, there was no progress since 2016 in terms of Cyber Security Policy and Strategy (National Cyber Security Strategy, Critical Infrastructure Protection). Likewise, there is no difference in Cyber Security Training, Capacity Building, and Skills (Awareness Raising, Framework for Training, Framework for Professional Training). Furthermore, no changes in Legal and Regulatory Frameworks (Criminal Justice System) were visualized. Finally, no progress in Standards, Organizations, and Technologies (Standards Compliance, Internet Infrastructure Resilience, Responsible Disclosure) (Cybersecurity Observatory in Latin America and the Caribbean, 2020).

To date, after the increase of digital processes due to the state of a health emergency, it is worrying the amount of sensitive information that is handled online and see that many of the institutions, both public and private, do not have a policy or strategy to help neutralize the loss or deterioration of information,

also unauthorized access by cybercriminals, which steal the essential knowledge of the institutions (León, 2021). It is worth mentioning that, in these times, all organizations require and demand the use of technologies, but many of them do not know how to handle it; as far as cybersecurity is concerned, this means that they do not have a methodology for the detection of incidents. This is the reason for the great concern about the risks to which government institutions and citizens are exposed (Santos, 2020). Cybersecurity has a value; today, we express it in the concept of digital trust, an approach that allows citizens, in general, to feel confident to use digital technologies and services (Presidency of the Council of Ministers. Government of Peru, 2018).

When the standards or methodologies that exist for adequate protection of technology are not respected and mismanaged, we find its weak point, which causes cybersecurity breaches to be created that compromise the confidentiality, integrity, or availability of technological assets.

NIST framework methodology

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk for internal and external stakeholders. It can help identify and prioritize actions to reduce cybersecurity risk and align policy, business, and technology approaches to manage cybersecurity risk. It can also be used to manage cybersecurity risk across all parts of an organization or can be focused on the delivery of critical services within one part of the organization. Different types of entities, including sector coordination structures, associations, and organizations, can use the Framework for other purposes, including the creation of Common Profiles. The NIST framework, a set of activities and deliverables for a guide to assess organizational IT security, consists of 3 parts:

- 05 High-level functions.
- 23 Categories, which cover technical aspects, people and processes, with a focus on results.
- 108 Subcategories, which are based on results, to create or improve a cybersecurity program.

It is worth mentioning that it is a tool for cybersecurity risk management, which fits any type of organization. In addition, it can be used as a key part of your systematic process, which does not replace existing processes. Rather, it determines gaps and improves them, optimizing costs and results (National Institute of Standards and Technology, 2018; Wallis, 2018; Almagro, 2019).

Table 1. NIST Framework methodology categories.

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Source: own elaboration.

The NIST Framework has five functions: Identify, Protect, Detect, Detect, Respond, and Recover; in each of these functions, you can see the framework categories that group strategies for managing cybersecurity in an organization (Gomez, 2019).

Cybersecurity

In essence, cybersecurity is dedicated to protecting everything that is safeguarded in the intangible medium of cyberspace, sensitive information concerning operating systems, media, national plans, innovations, and strategic infrastructure. For example, for criminals and terrorists, the connectivity of industrial control systems presents windows of opportunity for the attack at points where the impact on a nation's power is most significant, highlighting the dangers posed by cyber-attacks on critical infrastructure for public welfare economic development. Therefore, achieving cybersecurity is a joint work between government, private initiative, and citizens (García, 2019).

Cybersecurity is effective when cyberspace is considered reliable, secure, and flexible. Its primary objective was to prevent an attack from being carried out successfully. Currently, its goals are to prevent, detect, respond and recover. Most security professionals consider that it is impossible to avoid all attacks; that is why there must be planning and preparation that involves methods of detection and prevention of seizures (Leiva, 2015; ITU, 2018; Watson, 2019).

Figure 1. Three components of Cybersecurity.

Source: own elaboration.

Cybersecurity must contemplate the three components for its proper management, the focus on people that must be trained, the processes that must be written, defined, and implemented, and finally, the

necessary technology to implement the technical controls. All three are interrelated and must be managed (Fadrell Grupo Tecnológico, 2020; Vilcarromero & Vilchez, 2018).

Defining a digital security strategy is necessary, identifying vulnerabilities and protecting against cyber-attacks. To do so, the following actions are defined:

- Perform backups (backups) of information and confirm the restoration process.
- Update information technology systems.
- Raise employee awareness of the importance of cybersecurity.
- Control the information environment.
- Layered defense to reduce risk (Fadrell Grupo Tecnológico, 2020).

Management

Management is generally defined as a social process and by the actors that embody it (Clegg, 2005; Déry, 2010). As a social process, management brings together the set of management devices that are implemented to make an organization effective and efficient. While effectiveness refers to achieving the objectives set, efficiency refers to optimizing the means about the aim. As many management specialists have shown, this distinction is not neutral in implementing management practices, with some managers favoring effectiveness and others essentially favoring efficiency.

2. METHOD

The Experimental Research design has been selected since it handles variables of the cause-effect type. The independent variable is of interest to the researcher because the hypothesized variable (X) is one of the causes that produce the supposed effect.

3. RESULTS

In this research, a survey was conducted to 19 government organizations, where questions were posed about the current state of cybersecurity management with a scale to be used:

Level 0= Strongly disagree.

Level 1= Disagree.

Level 2= Undecided.

Level 3= Agree.

Level 4= Strongly agree.

The following results were obtained:

Table 2. Dimension: Nist Framework Phases.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Strongly Disagree	2	10,5	10,5	10,5
	Disagree	7	36,8	36,8	47,4
	Undecided	6	31,6	31,6	78,9
	Agree	4	21,1	21,1	100,0
	Total	19	100,0	100,0	

Source: own elaboration.

Table 2 shows the information protection processes and procedures that have been established in the organization.

Figure 2. Dimension: phases of Nist Framework.

Source: own elaboration.

Figure 2 shows that protection processes and procedures were established in the organization.

According to Table 2 and Figure 2, 36.84% of the government organizations present a level of disagreement on establishing processes and procedures for information protection in the organizations. In the Nist Framework Phases dimension, 31.58% of the respondents were undecided, 21.05% agreed, and 10.53% disagreed.

Table 3. Dimension: Nist Framework Phases.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Strongly Disagree	3	15,8	15,8	15,8
	Disagree	4	21,1	21,1	36,8
	Undecided	7	36,8	36,8	73,7
	Agree	4	21,1	21,1	94,7
	Strongly Agree	1	5,3	5,3	100,0
	Total	19	100,0	100,0	

Source: own elaboration.

In Table 3, the procedures have been implemented for intrusion detection in the organization.

Figure 3. Dimension: Phases of Nist Framework.

Source: own elaboration.

From Figure 3, it can be deduced that procedures for intrusion detection have been implemented in the organization.

According to Table 3 and Figure 3, 36.84% of the government organizations present an undecided level about implementing procedures for intrusion detection in the organizations. In the Nist Framework Phases dimension, 21.05% disagreed and agreed; 15.79% disagreed, and 5.26% agreed.

Table 4. Dimension: Incident Level.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Strongly Disagree	1	5,3	5,3	5,3
	Disagree	8	42,1	42,1	47,4
	Undecided	7	36,8	36,8	84,2
	Agree	2	10,5	10,5	94,7
	Strongly Agree	1	5,3	5,3	100,0
	Total	19	100,0	100,0	

Source: own elaboration.

In Table 4, a plan for incident management has been implemented.

Figure 4. Dimension: Incident level.

Source: own elaboration.

In Figure 4, a plan for incident management has been implemented.

According to Table 4 and Figure 4, 42.11% of the government organizations present a level of Disagree on implementing a plan for incident management in the organizations. Incident Level Dimension, 36.84% an undecided level; 10.53% an agreed level and 5.26% a disagree level; decide on the deck.

Table 5. Dimension: Incident Level.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Strongly Disagree	4	21,1	21,1	21,1
	Disagree	4	21,1	21,1	42,1
	Undecided	8	42,1	42,1	84,2
	Agree	2	10,5	10,5	94,7
	Strongly Agree	1	5,3	5,3	100,0
	Total	19	100,0	100,0	

Source: own elaboration.

In Table 5, a plan has been implemented for communication between areas involved in an incident.

Figure 5. Dimension: Incident level.
Source: own elaboration.

In Figure 5, the implementation of a plan for communication between areas involved in an incident.

According to Table 5 and Figure 5, 42.11% of the government organizations present an undecided level on implementing a plan for communication between areas involved before an incident in the organizations. 21.05% disagreed and disagreed; 10.53% agreed, and 5.26% agreed.

Table 6. Capabilities.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Strongly Disagree	5	26,3	26,3	26,3
	Disagree	4	21,1	21,1	47,4
	Undecided	7	36,8	36,8	84,2
	Agree	1	5,3	5,3	89,5
	Strongly Agree	2	10,5	10,5	100,0
	Total	19	100,0	100,0	

Source: own elaboration.

The Table 6 show all personnel are trained and informed.

Figure 6. Capabilities.
Source: own elaboration.

Figure 6 shows that all personnel is informed.

According to Table 6 and Figure 6, 36.84% of the government organizations present an undecided level about the training and education of all personnel in the organizations. In the Capabilities dimension, 26.32% disagree; 21.05% disagree; 10.53% totally agree, and 5.26% agree.

Table 7. Dimension: Capabilities.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Strongly Disagree	6	31,6	31,6	31,6
	Disagree	5	26,3	26,3	57,9
	Undecided	6	31,6	31,6	89,5
	Agree	2	10,5	10,5	100,0
	Total	19	100,0	100,0	

Source: own elaboration.

The Table 7 show there is training in cybersecurity issues.

Figure 7. Dimension: capabilities.

Source: own elaboration.

Figure 7 shows that there is training in cybersecurity issues.

According to Table 7 and Figure 7, 31.58% of government organizations present a disagree and uncertain status on training in cybersecurity issues in organizations. In the Capabilities dimension, 26.32% disagreed, and 10.53% strongly agreed.

Concerning the general statistical hypothesis, we have the following results:

Hi: using the methodology based on the NIST framework does influence cybersecurity management in government organizations.

Ho: using the methodology based on the NIST framework does not influence cybersecurity management in government organizations.

Table 8. Chi-square tests of the methodology based on the NIST framework and the management of cybersecurity in government organizations.

	Value	gl	Asymptotic significance (bilateral)
Pearson's Chi-square	34,392a	12	,433
Likelihood ratio	35,706	12	,303
Linear by linear association	14,651	1	,208
N of Valid cases	19		
a.; four boxes (66.7%) have expected a count of less than 5. The minimum expected count is 54.			

Source: own elaboration.

According to Table 6, when the chi-square statistic was applied, a correlation coefficient value (p) of 0.433 was obtained. As the (p) value is less than the significance level ($\alpha = 0.5$), it allows us to have sufficient evidence to accept the alternative research hypothesis and reject the null hypothesis. Therefore, the use of the methodology based on the NIST framework influences cybersecurity management in government organizations.

4. DISCUSSION

According to Alvarez, in the region, there are already ten countries with a national cybersecurity policy or strategy; however, Peru is not among them; this can be evidenced in the lack of proper cybersecurity management that is evident in this study. Santos (2020) also speaks of the great concern for the risks to which government institutions and citizens are exposed; in this sense, I reaffirm that it is only a concern, but it has not yet been transferred to the implementation of effective measures to manage cybersecurity.

5. CONCLUSIONS

It was observed that most government organizations do not have formalized cybersecurity, since they do not have incident statistics; this is due to poor management by untrained personnel.

It has been shown that there is an influence between the use of the methodology based on the NIST framework and cybersecurity management in government organizations obtaining. As a result, Pearson's chi-square = 0.433.

It is recommended that government organizations adopt the NIST cybersecurity Framework methodology to measure cybersecurity improvement and management.

REFERENCES

- Almagro, L.** (2019). NIST Cybersecurity Framework (CSF) / A comprehensive approach to cybersecurity. *White paper series, Issue 5*. http://www.itsd.gov.vc/itsd/images/pdf_documents/OAS_AWS_NIST_Cybersecurity_Framework_CSF_ENG.pdf
- Alvarez, D.** (2018). Cybersecurity in Latin America and cyber defense in Chile. *Chilean journal of law and technology*, 7(1). <https://rchdt.uchile.cl/index.php/RCHDT/article/view/50416>
- Ayala, C., & Lopez, E.** (2019). *Design and implementation of ISO 27035 (information security incident management) for the service platform area of a Peruvian state entity*. <http://repositorio.utp.edu.pe/handle/UTP/2477>
- Clegg, S. R.** (2005). *Managing and Organizations: an introduction to theory and practice*. SAGE.
- Cybersecurity Observatory in Latin America and the Caribbean.** (2020). *CYBERSECURITY: Risks, progress and the way forward in Latin America and the Caribbean*. USA. <https://observatoriociberseguridad.org/>
- Dammert, L., & Núñez, C.** (2019). Facing cyber threats: national cybersecurity strategies in the Southern Cone. *Security, Science & Defense*, 5(5), 107-129. <http://35.190.156.69/index.php/rscd/article/view/99>

Déry, R. (2010). *Les perspectives de Management*. JFD Éditions.

Dominguez, D. (2020). National cyber security system in the face of cyber attacks as a threat to National Security. *Journal of Defense Science and Research*, 1(2), 43-48. <http://recide.caen.edu.pe/index.php/Recide/article/view/11/18>

Fadrell Grupo Tecnológico. (2020). *Cybersecurity pie chart*. <http://www.fadrell.com/ciberseguridad-defensa-en-capas-para-reducir-el-riesgo/grafica-circular-ciberseguridad/>

Fernández, D., & Martínez, G. (2018). *Cybersecurity, cyberspace and cybercrime*. Thomson Reuters Aranzadi.

García, A. (2019). *Cybersecurity Why is it important for everyone?* Siglo XXI Editores Mexico.

García, O. (2019). *Information Security Governance Model for the Office of the Comptroller General of the Republic of Colombia*. <https://bdigital.uxternado.edu.co/handle/001/1895>

Gómez, Á. (2019). *Designing an enterprise cybersecurity program based on the NIST framework*. <https://hdl.handle.net/10953.1/11905>

Gomez, G. (2019). *What is the U.S. NIST Cybersecurity Framework?* <https://www.esan.edu.pe/conexion/actualidad/2019/04/30/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos/>

International ISO/IEC Standard 27000. (2018). *Information technology-Security techniques-Information security management systems-Information security management systems-Overview and vocabulary*. Switzerland.

ITU. (2018). *Global Cybersecurity Index (GCI)*. ITU Publications. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

- Leiva, E.** (2015). National cybersecurity strategies: comparative study based on top-down approach from a global to a local vision. *Latin American Journal of Software Engineering*, 3(4), 161-17. <https://doi.org/10.18294/relais.2015.161-176>
- León, J.** (2021). Cybersecurity and personal data protection in Peru. *Advocatus*, (039), 15-21.
- Martinez, N.** (2019). *Cybersecurity and operational risk in organizations*. <https://repositorio.comillas.edu/xmlui/handle/11531/42317>
- Montes, J.** (2020). Integrated cybersecurity strategies for strengthening homeland security. *Journal of Defense Science and Research*, 1(4), 36-48. <http://recide.caen.edu.pe/index.php/Recide/article/view/29>
- Nagurney, A., & Shukla, S.** (2017). Multiform models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, 260(2), 588-600. <https://doi.org/10.1016/j.ejor.2016.12.034>
- National Institute of Standards and Technology.** (2018). *Framework for improving cybersecurity in critical infrastructure*. https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmill-rev_20181102mn_clean.pdf
- Poma, A., & Vargas, R.** (2019). Problematic in Cybersecurity as protection of computer systems and social networks in Peru and the World. *Revista SCIENDO*, 22(4), 275-282. <https://revistas.unitru.edu.pe/index.php/SCIENDO/article/view/2692>
- Presidency of the Council of Ministers. Government of Peru.** (2018). *Legislative Decree No. 1412: Legislative Decree approving the Digital Government Law*. <https://www.gob.pe/institucion/pcm/normas-legales/289706-1412>

- Rios, J.** (2018). *Digital certification and efficient administrative management in Peruvian State Institutions*. <http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/2476/RIOS%20BARRIOS%20JUAN%20CARLOS%20HUGO%20-MAESTRIA.pdf?sequence=1&isAllowed=y>
- Santos, Z.** (2020). *From the documented public service to the digital public service*. <https://cader.sunarp.gob.pe/repositorio/cader/cader2019/jornadas/jornada1/docs/01D.pdf>
- Tates, C., & Recalde, L.** (2019). Cybersecurity in Ecuador, a proposal for Organization. *Journal of Security and Defense Sciences*, IV(7), 156-169. <http://geol.espe.edu.ec/wp-content/uploads/2019/03/7art12.pdf>
- Vila, G.** (2019). *Cyberattacks as threats to infrastructures and resources*. Estrategia Magazine. https://www.gub.uy/ministerio-defensa-nacional/sites/ministerio-defensa-nacional/files/2020-03/Revista_Estrategia_6.pdf#page=24
- Vilcarromero, L., & Vilchez, E.** (2018). *Proposal for the implementation of a cybersecurity management model for the security operations center (SOC) of a telecommunications company*. <https://repositorioacademico.upc.edu.pe/handle/10757/624832>
- Villamil, W.** (2019). *Risk management in government entities in Colombia*. <http://35.227.45.16/bitstream/handle/20.500.12277/6351/Gestion%20de%20Riesgos%20en%20Entidades%20del%20Gobierno.pdf?sequence=1&isAllowed=y>
- Wallis, A.** (2018). *What is Information Security? Why it's Important, Job Outlook and More*. <https://www.snhu.edu/about-us/newsroom/2018/06/what-is-information-security>
- Watson, M.** (2019). *The top 4 cybersecurity frameworks*. <https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks>