

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
SAN JOAQUÍN – CHILE



**“DESARROLLO Y VALIDACIÓN DE UN ENTORNO
EVALUATIVO CON INTELIGENCIA ARTIFICIAL PARA
MEDIR EL ÁREA DE SEGURIDAD SEGÚN EL MARCO
DIGCOMP 2.2”**

JOSEFA PÍA FLORES JIL

**MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA**

Profesor Guía: Liubov Dombrovskaia
Profesor Correferente: Dayana Carrillo

Noviembre – 2025



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título ☐ Tesis de Postgrado

Título del trabajo: Desarrollo y validación de un entorno evaluativo con inteligencia artificial para medir el área de seguridad según el marco Digcomp 2.2

Nombre del candidato(a): Josefa Pía Flores Jil

Carrera / Grado: Ingeniería civil en informática

Campus: San Joaquín **Departamento:** Informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Liubov Dombrovskaya, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por (**marcar una opción**):

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 10-11-2025

Firma: 

Estudiante o Candidato(a):

Fecha: 10-11-2025

Firma: 

RESUMEN

Resumen— Chile presenta un bajo desarrollo de competencias digitales, lo que impacta negativamente en la productividad laboral y en la adaptación tecnológica de su población. Frente a la limitada precisión de los instrumentos basados en autopercepción, esta investigación propone Ladico, un entorno digital que evalúa el desempeño real de los usuarios mediante preguntas adaptadas por inteligencia artificial generativa, alineadas al marco europeo DigComp 2.2 en el área de Seguridad. La validación empírica, aplicada a 30 participantes, comparó los resultados de desempeño con un cuestionario de autopercepción, obteniendo altas correlaciones ($r = 0,78$ a $0,87$) que evidencian validez convergente y consistencia estadística. En consecuencia, Ladico se consolida como una herramienta válida y contextualizada para medir competencias digitales basadas en evidencia.

Palabras Clave—Competencia digital, DigComp 2.2, Inteligencia Artificial, Ladico, Evaluación.

ABSTRACT

Abstract— Chile shows low levels of digital competence development, which negatively affects labor productivity and technological adaptation. To address the limited accuracy of self-perception instruments, this research proposes Ladico, a digital environment that evaluates users' actual performance through generative AI-adapted questions aligned with the European DigComp 2.2 framework, specifically in the Security area. The empirical validation, applied to 30 participants, compared performance results with a self-perception questionnaire, obtaining high correlations ($r = 0.78$ to 0.87) that demonstrate convergent validity and statistical consistency. Consequently, Ladico is established as a valid and context-aware tool for evidence-based measurement of digital competences.

Keywords—Digital Competence, DigComp 2.2, Artificial Intelligence, Ladico, Evaluation.

ÍNDICE DE CONTENIDO

RESUMEN.....	3
ABSTRACT	4
INDICE DE FIGURAS.....	5
CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA	7
1.1 BRECHAS EN COMPETENCIAS DIGITALES EN CHILE	8
1.2 LIMITACIONES DE LOS INSTRUMENTOS DE EVALUCIÓN ACTUALES.....	10
1.3 PROPUESTA DE SOLUCIÓN: LADICO	11
1.4 OBJETIVOS DEL ESTUDIO.....	12
1.5 ESTRUCTURA DE LA MEMORIA	12
CAPÍTULO 2: MARCO CONCEPTUAL	13
2.1 COMPETENCIAS DIGITALES: DEFINICIÓN Y MARCO DIGCOMP 2.2.....	14
2.2 ÁREA DE SEGURIDAD DIGITAL EN EL MARCO DIGCOMP 2.2	15
2.2.1 PROTECCIÓN DE DISPOSITIVOS	15
2.2.2 PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD	16
2.2.3 PROTECCIÓN DE LA SALUD Y DEL BIENESTAR.....	16
2.2.4 PROTECCIÓN MEDIOAMBIENTAL	16
2.3 PROBLEMAS ASOCIADOS A LA MEDICIÓN DEL ÁREA DE SEGURIDAD	17
2.4 EVALUACIÓN DEL ÁREA DE SEGURIDAD MEDIANTE TECNOLOGÍAS EMERGENTES ...	18
2.5 INSTRUMENTOS EXISTENTES RELACIONADOS CON EL ÁREA DE SEGURIDAD	19
2.6 RELACIÓN DEL MARCO CONCEPTUAL CON LA PROPUESTA DE SOLUCIÓN	20
CAPÍTULO 3: PROPUESTA DE SOLUCION	21
3.1 DESCRIPCIÓN GENERAL DE LA PLATAFORMA WEB	22
3.2 ARQUITECTURA E IMPLEMENTACIÓN DEL SISTEMA	24

3.2.1 CAPA DE SOLUCIÓN	24
3.2.2 FLUJO GENERAL DEL SISTEMA	26
3.2.3 FLUJO DE NAVEGACIÓN Y AUTENTICACIÓN	26
3.2.4 LÓGICA INTERNA DEL PROCESO DE EVALUACIÓN	28
3.3 METODOLOGÍA DE FUNCIONAMIENTO	29
3.4 CARACTERÍSTICAS DIFERENCIALES	32
CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN	33
4.1 DESCRIPCIÓN GENERAL DE LA MUESTRA	34
4.2 RESULTADOS DEL CUESTIONARIO DE PERCEPCIÓN	34
4.3 RESULTADOS DE DESEMPEÑO EN LADICO	37
4.4 RESULTADOS DE CORRELACIÓN PERCEPCIÓN-DESEMPEÑO	39
4.4.1 PROCEDIMIENTO DEL ANÁLISIS CORRELACIONAL	40
4.4.2 COMPETENCIA 4.1 – PROTECCIÓN DE DISPOSITIVOS	40
4.4.3 COMPETENCIA 4.2 – PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD	41
4.4.4 COMPETENCIA 4.3 – PROTECCIÓN DE LA SALUD Y DEL BIENESTAR	42
4.4.5 COMPETENCIA 4.4 – PROTECCIÓN MEDIOAMBIENTAL	43
CAPÍTULO 5: CONCLUSIONES	45
5.1 PRINCIPALES HALLAZGOS DEL PROCESO DE VALIDACIÓN	46
5.2 EVALUACIÓN DEL CUMPLIMIENTO DE LOS OBJETIVOS PLANTEADOS	47
5.3 APORTES METODOLÓGICOS Y TECNOLÓGICOS DEL ENTORNO LADICO	48
5.4 LIMITACIONES DEL ESTUDIO	49
5.5 RECOMENDACIONES Y PROYECCIONES FUTURAS	50
REFERENCIAS BIBLIOGRÁFICAS	52
ANEXOS	55

INDICE DE FIGURAS

Figura 1. Proporción de población con desempeño deficiente en las tres dimensiones analizadas [OECD, 2024].....	10
Figura 2. Resultados de estudio ICILS [Agencia de Calidad de Educación, 2024].	10
Figura 3. Áreas de competencia del marco DigComp [Vuorikari, Kluzer & Punie, 2022]	15
Figura 4. Página de inicio de Ladico.....	23
Figura 5. Características principales destacadas de Ladico.	24
Figura 6. Áreas de competencia digital evaluadas en Ladico según DigComp 2.2.	24
Figura 7. Capa de solución y flujo general de datos en Ladico.....	26
Figura 8. Flujo general del sistema Ladico.....	28
Figura 9. Flujo de navegación y autenticación inicial en Ladico.....	29
Figura 10. Lógica interna del proceso de evaluación en Ladico.	30
Figura 11. Interfaz de selección de competencias en Ladico para el área de Seguridad.....	31
Figura 12. Ejemplo de pregunta de nivel básico en la competencia 4.4 Protección medioambiental.	32
Figura 13. Ejemplo de pregunta de nivel intermedio en la competencia 4.4 Protección medioambiental.	32
Figura 14. Ejemplo de pregunta de nivel avanzado en la competencia 4.4: Protección medioambiental.	33
Figura 15. Distribución de respuestas del cuestionario de percepción en el área de Seguridad.....	38
Figura 16. Niveles de desempeño alcanzados por competencia en la plataforma Ladico. .	40
Figura 17. Relación entre autopercepción y el desempeño en la competencia 4.1.	42
Figura 18. Relación entre autopercepción y el desempeño en la competencia 4.2.	43
Figura 19. Relación entre autopercepción y el desempeño en la competencia 4.3.	44

Figura 20. Relación entre autopercepción y el desempeño en la competencia 4.4. 45

INDICE DE TABLAS

Tabla 1. Preguntas del cuestionario de autopercepción para el área de seguridad.....	37
Tabla 2. Distribución general de participantes según nivel de desempeño alcanzado en la plataforma Ladico.	39
Tabla 3. Porcentaje de participantes que alcanzaron cada nivel de desempeño por competencia del área de Seguridad.	40
Tabla 4. Coeficientes de correlación entre percepción y desempeño por competencia del área de Seguridad.	41

CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA

La creciente importancia de la competencia digital en la sociedad actual exige una comprensión clara de las habilidades que las personas deben poseer para participar activamente en entornos digitales. En una era en la que las tecnologías digitales sustentan la educación, el empleo, las interacciones sociales y el compromiso cívico, el uso eficaz y responsable de estas tecnologías es esencial. Esto va más allá de las meras habilidades operativas e incluye un desempeño informado, crítico, creativo y ético [IEA, 2023].

1.1 BRECHAS EN COMPETENCIAS DIGITALES EN CHILE

En el panorama educativo, la competencia digital desempeña un papel fundamental en el éxito académico de los estudiantes. A medida que la tecnología se integra cada vez más en las actividades del aula, las tareas de resolución de problemas y el acceso a los recursos de aprendizaje, los estudiantes con una sólida competencia digital están mejor posicionados para prosperar académicamente. Además, comprender la interacción entre la competencia digital de los estudiantes y su aprendizaje digital informal puede proporcionar información valiosa para mejorar su rendimiento académico [Mehrvarz et al., 2021].

Algunos estudios internacionales en los que participa Chile dan cuenta de la brecha existente en el desarrollo de la competencia digital en la comparación con los países de la OCDE. Según el estudio PIACC, los adultos chilenos entre 16 a 65 años son los menos preparados que sus pares de OCDE según el informe de Evaluación de Competencias de la Población Adulta 2023 Figura 1. Proporción de población con desempeño deficiente en las tres dimensiones analizadas [OECD, 2024]. [Figura 1], el 44% de ellos mostró resultados bajos en las tres áreas evaluadas: alfabetización digital (*literacy*), razonamiento matemático (*numeracy*) y resolución adaptativa de problemas [OECD, 2024]. Este indicador más que duplica el promedio general de todos los países evaluados (18%).

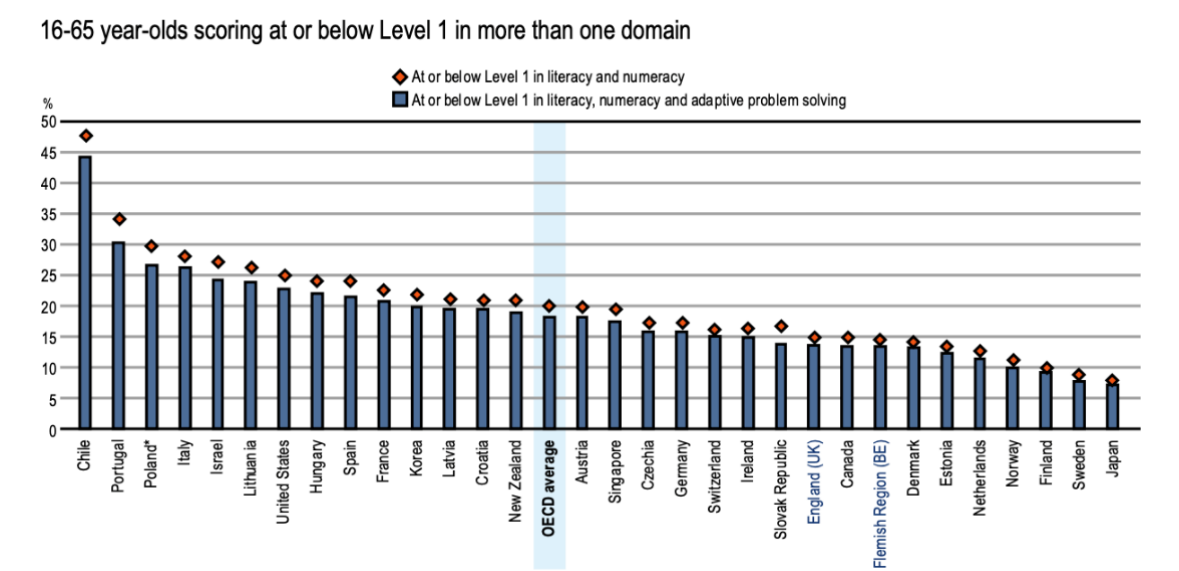


Figura 1. Proporción de población con desempeño deficiente en las tres dimensiones analizadas [OECD, 2024].

A su vez, los escolares chilenos también presentan una importante brecha en habilidades digitales según el estudio ICILS: cerca de 70% de los estudiantes de 8° básico tiene el manejo básico o rudimentario de las tecnologías actuales, o sea, necesitan instrucciones paso a paso al llevar a cabo las tareas [Agencia de Calidad de Educación, 2024]. En la FFigura 2. Resultados de estudio ICILS [Agencia de Calidad de Educación, 2024].igura 2 se puede apreciar los 44 puntos menos que el promedio de los países OCDE, y, Además, Chile muestra la mayor disminución con 55 puntos menos que el año 2013 y 44 puntos menos que el 2018.

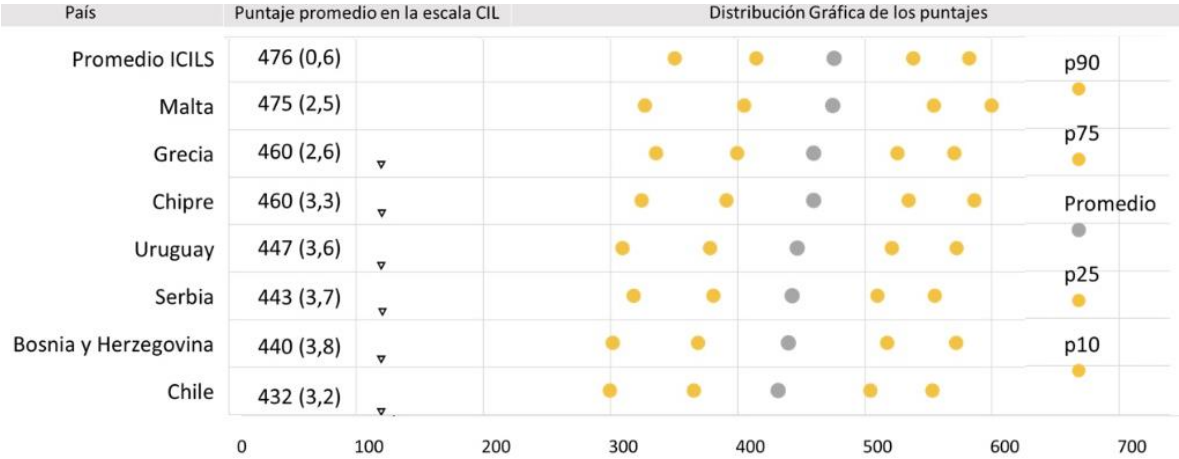


Figura 2. Resultados de estudio ICILS [Agencia de Calidad de Educación, 2024].

Aunque el estudio ICILS da algunas luces sobre el estado general de la competencia digital en la educación media, persiste la falta de conocimiento preciso sobre los niveles de competencia digital, agravado por la escasez de herramientas de evaluación eficaces

adaptadas a esta etapa educativa. Aunque el término «nativos digitales» se utiliza a menudo para describir a los jóvenes que crecen con la tecnología, esta familiaridad no se traduce automáticamente en la competencia digital integral necesaria para el éxito académico y profesional futuro. De hecho, las personas suelen sobreestimar sus habilidades digitales [Usart-Rodríguez et al., 2021] [Aesaert et al., 2017].

1.2 LIMITACIONES DE LOS INSTRUMENTOS DE EVALUACIÓN ACTUALES

La ausencia de un sistema de evaluación aplicable a contextos diversos en Latinoamérica genera varios problemas:

- **Dificultad para identificar fortalezas y debilidades reales:** Sin una herramienta confiable, las personas —ya sean estudiantes, trabajadores o ciudadanos— no pueden conocer con claridad en qué aspectos de su competencia digital destacan o necesitan mejorar. Esta falta de diagnóstico impide planificar procesos de formación personalizada, acompañamiento efectivo o políticas públicas basadas en evidencia.
- **Limitaciones para el diseño de programas de formación y políticas públicas:** Tanto instituciones educativas como organizaciones laborales y gobiernos requieren información precisa sobre el nivel de competencia digital de sus públicos para diseñar planes de acción pertinentes. Sin datos objetivos, muchas iniciativas pueden quedar desalineadas con las necesidades reales de la población.
- **Comprensión limitada del impacto de las intervenciones:** Cuando se implementan programas para cerrar la brecha digital, la falta de una herramienta sólida y validada impide evaluar si estos esfuerzos realmente mejoran las habilidades digitales o los resultados asociados, como la empleabilidad, la productividad o la participación cívica.
- **Dificultades para enfrentar los desafíos del mundo digital:** En un entorno donde el acceso a servicios, oportunidades laborales, educación en línea y participación social ocurre cada vez más en entornos digitales, las personas con baja competencia digital enfrentan barreras que limitan su inclusión y desarrollo.
- **Dependencia de la autoevaluación con sesgo:** Las herramientas disponibles actualmente en la región se basan, en su mayoría, en la autoevaluación. Estas son útiles como diagnóstico inicial, pero tienden a sobrestimar o subestimar las capacidades reales de los usuarios, especialmente cuando hay brechas educativas o tecnológicas. Esto puede llevar a decisiones mal fundamentadas.

Las investigaciones existentes subrayan la necesidad de instrumentos de evaluación eficaces en el ámbito de la competencia digital. Aunque se han realizado esfuerzos para desarrollar y validar tales herramientas para estudiantes universitarios [Tzafilkou et al., 2022] y profesores [Usart-Rodríguez et al., 2021], destaca la falta de un enfoque correspondiente a las necesidades del público general. Marcos como DigComp [Vuorikari et al., 2022] proporcionan una valiosa base conceptual para definir las dimensiones clave de la competencia digital

desde un enfoque ciudadano y transversal. Si bien en Europa existen iniciativas como pix.fr, que permiten a los usuarios medir sus competencias digitales de forma automática y objetiva en relación con el marco DigComp, en América Latina predominan aún las herramientas de autoevaluación, centradas en la percepción subjetiva de los usuarios. Este tipo de instrumentos, aunque útiles como aproximación inicial, se basan en la opinión y no siempre reflejan el desempeño real. En contraste, la evaluación por desempeño, que implica observar y analizar la evidencia de las acciones del usuario en tareas auténticas, ofrece un diagnóstico más preciso y válido. La ausencia de este tipo de herramientas adaptadas a los contextos sociales, culturales y tecnológicos de la región genera una brecha significativa en la medición de la competencia digital.

1.3 PROPUESTA DE SOLUCIÓN: LADICO

En respuesta a esta brecha, nace Ladico, que constituye un entorno innovador de evaluación automática de las competencias digitales reales, que mediante inteligencia artificial y otros elementos de software, genera actividades en los cuales los usuarios desarrollan actividades y resuelven preguntas prácticas, permitiendo una evaluación precisa y objetiva del desempeño y nivel de competencia digital logrado. La evaluación del nivel de competencia digital se realiza en cinco ejes de competencia digital definidos por DigComp 2.2 [Vuorikari et al., 2022] compuesta por preguntas que representan distintos niveles de dominio de la competencia: básico, intermedio y avanzado. Al acceder a una prueba de nivel, el usuario debe completar tres preguntas según el eje y nivel seleccionado, y sólo después de completarlo puede pasar al siguiente. Para garantizar una experiencia dinámica y personalizada, una inteligencia artificial genera el contenido de las preguntas en cada intento y califica el desempeño del usuario.

Ladico propone una solución innovadora y contextualizada, que busca replicar y mejorar este enfoque, permitiendo una evaluación más personalizada, inclusiva y alineada a las necesidades reales de los distintos sectores de la población latinoamericana.

Los beneficios que provee el entorno Ladico descrito son las siguientes:

- Se alinea con el marco establecido de la Unión Europea DigComp 2.2 [Vuorikari et al., 2022] para proporcionar una evaluación estructurada y completa de 5 competencias digitales: búsqueda y gestión de información, comunicación y colaboración, creación de contenidos digitales, seguridad y resolución de problemas.
- Evalúa el grado de desarrollo de la competencia digital en base a evidencia, utilizando actividades de desempeño y registros observables del usuario (ejercicios prácticos, trazabilidad de acciones, portafolios digitales). Este enfoque evita depender de la opinión propia o percepción subjetiva del participante, y se centra en datos objetivos que reflejan realmente su nivel de competencia, respondiendo a una necesidad ampliamente reconocida en el campo.

- Personaliza las preguntas, lo cual permite rendir la evaluación varias veces sin repetirlas, gracias al uso de Inteligencia Artificial (IA) para crear las preguntas y evaluar las respuestas.
- Permite medir los factores personales y contextuales que influyen en la competencia digital y calcular el impacto de las intervenciones destinadas a mejorar las habilidades digitales.
- Habilita la posibilidad de medición de las competencias real, escalable, masiva y económica.

1.4 OBJETIVOS DEL ESTUDIO

El objetivo general del presente trabajo es diseñar e implementar un entorno de evaluación automatizada basado en el marco DigComp 2.2, que permita medir de manera objetiva, contextualizada y fiable la competencia digital en el área “Seguridad”, utilizando inteligencia artificial para la generación dinámica de ítems. Este objetivo general se logra con los siguientes objetivos específicos:

- Analizar los principales marcos internacionales de evaluación de competencia digital y su aplicabilidad al contexto latinoamericano.
- Diseñar la arquitectura técnica y funcional del entorno Ladico, garantizando escalabilidad, seguridad y usabilidad.
- Diseñar y estructurar un banco de preguntas generado a partir de prompts predefinidos, que permita adaptar los ítems de evaluación al nivel y contexto del usuario.
- Validar la fiabilidad y pertinencia de los instrumentos de evaluación mediante pruebas piloto con usuarios reales.
- Evaluar la correlación entre la autopercepción digital y el desempeño medido en la plataforma, identificando brechas y oportunidades de mejora.

1.5 ESTRUCTURA DE LA MEMORIA

La presente memoria se organiza en cinco capítulos principales que abordan, de forma progresiva, el desarrollo del proyecto, desde la identificación del problema hasta la validación de la solución propuesta.

El Capítulo 1, denominado Definición del problema, expone el contexto general del estudio, destacando la relevancia de las competencias digitales en el área de seguridad y la justificación de la propuesta desarrollada.

El Capítulo 2, correspondiente al Marco conceptual, revisa los principales referentes teóricos y empíricos vinculados con la competencia digital y la seguridad en línea. En este

apartado se analizan los marcos DigComp 2.2, ICILS [IEA, 2023] y PIAAC [OECD, 2024], además de estudios recientes sobre evaluación basada en desempeño.

El Capítulo 3, titulado Propuesta de solución, describe la arquitectura, los componentes funcionales y la metodología de funcionamiento del entorno Ladico. Asimismo, se detalla la integración de inteligencia artificial para la generación dinámica de ítems y los mecanismos implementados para la evaluación automatizada.

El Capítulo 4, dedicado a la Validación de la solución, presenta el proceso de desarrollo técnico, las pruebas de usabilidad realizadas y los procedimientos de validación empírica, junto con los resultados obtenidos en la aplicación del entorno con usuarios reales.

Finalmente, el Capítulo 5, correspondiente a las Conclusiones, sintetiza los principales hallazgos de la investigación, discute las implicancias del modelo propuesto y propone líneas futuras de mejora y de investigación.

CAPÍTULO 2: MARCO CONCEPTUAL

Este capítulo establece los fundamentos teóricos y conceptuales que sustentan la presente investigación. Se presenta el marco de competencias digitales DigComp 2.2, se profundiza en su área de seguridad, se analizan los problemas asociados a su medición y se exploran las oportunidades que ofrecen las tecnologías emergentes para una evaluación más objetiva y formativa. Finalmente, se revisan instrumentos existentes y se concluye explicitando cómo este marco conceptual fundamenta la propuesta de solución.

2.1 COMPETENCIAS DIGITALES: DEFINICIÓN Y MARCO DIGCOMP 2.2

El concepto de competencia digital ha transitado desde una visión puramente instrumental, centrada en la alfabetización tecnológica y el manejo de herramientas, hacia una concepción holística que integra conocimientos, habilidades y actitudes necesarias para participar de manera crítica y responsable en la sociedad digital. En este contexto, DigComp se ha consolidado como el estándar de referencia internacional.

Desde su primera versión en 2013 hasta la actual versión 2.2 (2022), el marco ha evolucionado incorporando nuevos ejemplos de aplicación y contemplando problemáticas emergentes como la inteligencia artificial, la desinformación y la sostenibilidad [Vuorikari et al., 2022]. DigComp organiza las competencias digitales en cinco áreas: alfabetización en información y datos, comunicación y colaboración, creación de contenido digital, seguridad y resolución de problemas [Figura 3]. Estas se desglosan en 21 competencias específicas, cada una con niveles progresivos que van del básico al altamente especializado.



Figura 3. Áreas de competencia del marco DigComp [Vuorikari, Kluzer & Punie, 2022]

Aunque surgido en Europa, DigComp se ha convertido en un referente global. En Latinoamérica diversos estudios y políticas educativas lo han tomado como marco para evaluar competencias digitales, adaptándolo a los desafíos locales: desigualdad en el acceso

a dispositivos, bajo nivel de alfabetización digital en docentes, y carencias en la formación en seguridad [Cepal, 2025].

En este sentido, existe una relación directa y complementaria entre competencia y ciudadanía digitales. La primera entrega los conocimientos, habilidades y actitudes necesarias para interactuar de manera eficaz con las tecnologías: desde buscar información y comunicarse hasta proteger los datos personales o gestionar la identidad digital. Sin embargo, estas capacidades técnicas por sí solas no garantizan un uso responsable de la tecnología. Es en la ciudadanía digital donde dichas competencias se traducen en el ejercicio activo, crítico y ético de los derechos y deberes en la sociedad digital [Zhao, 2021].

La ciudadanía digital implica no solo protegerse de riesgos, sino también participar activamente en entornos democráticos en línea, respetar normas de convivencia digital, contribuir a comunidades seguras e inclusivas, y tomar decisiones informadas respecto al uso de datos, contenidos y tecnologías. De este modo, la competencia digital se convierte en la base instrumental, mientras que la ciudadanía digital representa su proyección cívica y social, vinculando las habilidades individuales con el bienestar colectivo. En contextos como el latinoamericano, donde la brecha digital no se limita al acceso, sino también al uso seguro, crítico y significativo de la tecnología, fortalecer esta relación es clave. Formar ciudadanos digitales no solo implica enseñarles a usar herramientas, sino también a ejercer sus derechos digitales, proteger su privacidad, respetar a otros en entornos en línea y participar activamente en la construcción de sociedades más equitativas e inclusivas.

2.2 ÁREA DE SEGURIDAD DIGITAL EN EL MARCO DIGCOMP 2.2

El área 4 del marco DigComp se centra en la Seguridad Digital, entendida como la capacidad de proteger dispositivos, datos, salud, bienestar y el entorno en el uso de tecnologías digitales. Este ámbito va más allá de la protección técnica: integra la dimensión individual, social y ambiental del uso seguro de la tecnología, garantizando que los ciudadanos puedan desenvolverse en entornos digitales de forma segura, ética y sostenible [Vuorikari et al., 2022].

2.2.1 PROTECCIÓN DE DISPOSITIVOS

Esta competencia se refiere a la capacidad de los usuarios para proteger dispositivos, aplicaciones y contenidos digitales frente a riesgos de seguridad. Incluye acciones como instalar y actualizar programas de seguridad (antivirus, antimalware, cortafuegos), realizar copias de seguridad, gestionar contraseñas robustas y reconocer amenazas comunes como malware, phishing o ransomware [Vuorikari et al., 2022].

La importancia radica en que constituye la primera línea de defensa frente a incidentes de ciberseguridad. No se limita al aspecto técnico, sino que promueve la conciencia preventiva, la actualización constante y la adopción de buenas prácticas de seguridad.

Estudios muestran que los usuarios suelen tener confianza en su capacidad para proteger dispositivos, pero en la práctica demuestran carencias, como la reutilización de contraseñas o la falta de actualización de software [Skantz, 2022].

2.2.2 PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD

Esta competencia se centra en la gestión de la identidad y de la huella digital. Implica que el ciudadano conozca cómo se recolectan, procesan y utilizan sus datos personales; configure opciones de privacidad en plataformas digitales; y sea capaz de ejercer sus derechos en relación con la protección de datos, como el Reglamento General de Protección de Datos (GDPR) en Europa [Vuorikari et al., 2022] o la Ley N.º 19.628 sobre Protección de la Vida Privada en Chile [Chile, 1999].

Según DigComp, esta competencia abarca desde habilidades básicas, como entender qué es una contraseña segura, hasta capacidades avanzadas, como evaluar la seguridad de las aplicaciones, identificar cláusulas abusivas en términos y condiciones o ejercer derechos ARCO sobre los propios datos [Vuorikari et al., 2022].

Investigaciones empíricas demuestran que estudiantes y docentes suelen sobreestimar su nivel de privacidad digital, configurando perfiles inseguros en redes sociales y compartiendo datos personales sin valorar los riesgos. Esto revela la necesidad de intervenciones educativas y evaluativas que midan no solo el conocimiento, sino el desempeño real [Tzafilkou et al., 2022] [Rioseco-Pais et al., 2023].

2.2.3 PROTECCIÓN DE LA SALUD Y DEL BIENESTAR

Esta competencia amplía el concepto de seguridad hacia la dimensión psicológica, física y social. Implica identificar y prevenir riesgos como el tecnoestrés, la adicción a dispositivos, los problemas de ergonomía por el uso prolongado de pantallas, y las consecuencias del ciberacoso o del discurso de odio en línea [Vuorikari et al., 2022].

La seguridad digital no puede limitarse a lo técnico: también debe garantizar un uso equilibrado y saludable de la tecnología. Por ejemplo, promover hábitos como descansar la vista, mantener posturas ergonómicas, o gestionar el tiempo frente a pantallas.

La OCDE advierte que las generaciones más jóvenes son particularmente vulnerables a problemas de bienestar digital, ya que combinan un alto uso de dispositivos con baja conciencia de sus efectos en la salud mental y social. En América Latina, este tema se vuelve crítico en entornos educativos, donde la pandemia aceleró la exposición prolongada a pantallas sin estrategias claras de autocuidado [OECD, 2024].

2.2.4 PROTECCIÓN MEDIOAMBIENTAL

Esta competencia conecta la seguridad digital con la sostenibilidad ambiental y social. Se refiere a la capacidad de los ciudadanos para comprender el impacto ambiental del uso de tecnologías digitales (consumo energético, huella de carbono de los centros de datos, residuos electrónicos) y adoptar prácticas responsables, como el reciclaje de dispositivos o el uso consciente de recursos digitales [Vuorikari et al., 2022]. Asimismo, involucra la responsabilidad ciudadana en entornos digitales, lo que significa participar de manera ética y solidaria en la sociedad digital, respetando normas, contribuyendo a comunidades seguras e inclusivas y apoyando el bienestar colectivo [Zhao, 2021].

En Latinoamérica, donde aún existe rezago en políticas de reciclaje electrónico y educación ambiental vinculada a lo digital, esta competencia adquiere una importancia estratégica. Favorece la visión de la seguridad no solo como un asunto individual, sino como un bien común que impacta a la sociedad y al planeta.

La seguridad digital es fundamental para el ejercicio pleno de la ciudadanía digital. Permite proteger la integridad personal, garantizar la privacidad, prevenir daños a la salud y fomentar prácticas sostenibles. En sociedades hiperconectadas como las actuales, donde la vida cotidiana, el trabajo y la educación dependen cada vez más de entornos digitales, estas competencias son esenciales para el bienestar individual y colectivo. Su relevancia se acentúa en regiones como América Latina, donde la rápida expansión de la conectividad no siempre ha sido acompañada por formación en competencias de seguridad, lo que aumenta la vulnerabilidad de estudiantes, docentes y ciudadanos en general [Cepal, 2025].

2.3 PROBLEMAS ASOCIADOS A LA MEDICIÓN DEL ÁREA DE SEGURIDAD

La evaluación de la competencia de seguridad digital enfrenta una serie de desafíos que limitan la validez y la confiabilidad de los diagnósticos obtenidos en distintos contextos educativos y sociales. Entre los principales problemas identificados en la literatura destacan el predominio de instrumentos de autoevaluación, la desalineación entre percepción y desempeño real, la escasez de evaluaciones basadas en desempeño, y la necesidad de contar con estudios comparativos y revisiones metodológicas más profundas.

La gran mayoría de las investigaciones y diagnósticos realizados hasta ahora se basan en cuestionarios de autopercepción (escalas Likert o encuestas). Estos instrumentos, aunque de bajo costo y fáciles de aplicar en grandes poblaciones, presentan limitaciones críticas: dependen de la honestidad del encuestado, de su autoconciencia, y son susceptibles al sesgo de deseabilidad social [Aesaert et al., 2017]. Como resultado, suelen ofrecer una imagen sobrestimada del nivel real de competencia, especialmente en áreas sensibles como la seguridad digital.

La literatura muestra de manera consistente una brecha entre lo que los individuos creen saber y lo que realmente saben hacer en contextos prácticos. Sillat y Stemberger evidencian que los estudiantes y profesionales que afirman poseer un alto nivel de competencia en seguridad digital, en la práctica, tienen dificultades para realizar tareas básicas como identificar un intento de phishing, configurar contraseñas seguras o manejar adecuadamente la privacidad en redes sociales [Sillat et al., 2021][Stemberger, 2021]. Åberg refuerzan este hallazgo mostrando que la sobreconfianza en habilidades de seguridad puede aumentar la exposición a riesgos, pues los usuarios confían en conductas que no son realmente seguras [Skantz Åberg et al., 2022].

A diferencia de otros ámbitos de DigComp, como la alfabetización informacional o la creación de contenidos digitales, en el área de seguridad digital existen pocas experiencias de evaluación basadas en desempeño real. Es decir, instrumentos que observen directamente cómo actúa el usuario frente a una situación simulada o real de riesgo

[Aesaert et al., 2017]. La mayoría de los estudios se queda en el nivel declarativo (lo que los usuarios dicen que harían), en lugar de observar la conducta efectiva (lo que realmente hacen). Esto genera un vacío metodológico que limita el diseño de intervenciones educativas y políticas públicas.

Las revisiones recientes coinciden en que existe una necesidad urgente de mejorar los métodos de evaluación de la seguridad digital. Sillat destaca que incluso en países con políticas avanzadas en educación digital, los instrumentos tienden a fragmentarse y carecen de un marco metodológico robusto para medir desempeño [Sillat et al., 2021]. Stemberger añade que las pruebas de autoevaluación no logran identificar a los grupos más vulnerables, ya que son precisamente estos quienes suelen sobrestimar más sus competencias [Stemberger, 2021]. Finalmente, Skantz sugieren que los nuevos instrumentos deben incluir tareas prácticas y contextuales, capaces de medir el comportamiento real de los usuarios frente a escenarios de seguridad digital [Skantz Åberg et al., 2022].

2.4 EVALUACIÓN DEL ÁREA DE SEGURIDAD MEDIANTE TECNOLOGÍAS EMERGENTES

En los últimos años, las tecnologías emergentes, y en particular, la inteligencia artificial (IA), han abierto nuevas posibilidades para abordar la medición de competencias digitales desde enfoques más objetivos y situados. A diferencia de los cuestionarios de autopercepción, la IA permite construir entornos adaptativos e interactivos que simulan situaciones reales de riesgo digital, como fraudes, ciberacoso, filtración de datos o configuración de privacidad, registrando no solo el resultado final del desempeño del usuario, sino también el proceso seguido para alcanzarlo [Blanc et al., 2025]. Esto representa un cambio significativo en la forma de evaluar, ya que permite capturar la conducta observable y no únicamente la autopercepción declarada.

Este enfoque posibilita además una evaluación formativa y automatizada, con retroalimentación inmediata y personalizada que se ajusta al nivel de cada usuario. Para contextos como los de Latinoamérica, donde las limitaciones en recursos humanos y financieros dificultan la implementación de evaluaciones presenciales a gran escala, la IA ofrece un potencial particularmente relevante [Martín-Párraga et al., 2022]. Con ello, se puede escalar la evaluación de la seguridad digital sin perder pertinencia ni adaptabilidad a las características individuales.

Sin embargo, la incorporación de IA en procesos educativos y evaluativos requiere un marco ético y normativo claro. En Europa, el Reglamento General de Protección de Datos (GDPR) establece estándares estrictos para el manejo de información personal, mientras que en Chile la próxima Ley de Protección de Datos Personales plantea lineamientos semejantes. En el ámbito educativo, el documento PotenciA el Aprendizaje del Ministerio de Educación [Mineduc, 2025] refuerza la necesidad de utilizar estas tecnologías de manera pedagógicamente pertinente, asegurando la protección de datos estudiantiles. Asimismo, organismos internacionales como la CEPAL y el World Economic Forum han advertido que el uso de IA en educación debe estar orientado a principios de inclusión, equidad y

transparencia, de manera que su potencial no amplíe las brechas existentes, sino que contribuya a reducirlas [CEPAL, 2023][WEF, 2025].

En este escenario, la aplicación de tecnologías emergentes para evaluar la competencia de seguridad digital se presenta como una oportunidad estratégica para avanzar hacia instrumentos que no solo diagnostiquen con mayor precisión, sino que también ofrezcan retroalimentación formativa y adaptada al contexto, potenciando así tanto la alfabetización digital como la ciudadanía digital en Latinoamérica.

2.5 INSTRUMENTOS EXISTENTES RELACIONADOS CON EL ÁREA DE SEGURIDAD

En la literatura se han desarrollado diversos instrumentos para medir las competencias digitales, algunos de los cuales incluyen el área de seguridad como componente central. Estos instrumentos han sido aplicados en distintos contextos y poblaciones, aportando evidencia valiosa sobre el estado de las competencias digitales. Sin embargo, la mayoría de ellos presentan limitaciones, especialmente porque dependen de autopercepción o carecen de entornos adaptativos, lo que restringe su capacidad para capturar el desempeño real del usuario. A continuación, se describen los principales instrumentos identificados:

CompDig-PedEs un instrumento desarrollado y aplicado en Chile que se distingue por ser una de las primeras experiencias de evaluación basada en desempeño dentro del marco DigComp. Fue implementado en estudiantes universitarios de primer año, incluyendo específicamente la medición de las cuatro competencias del área de seguridad digital. Los resultados mostraron diferencias significativas por género, nivel socioeconómico y tipo de institución, evidenciando brechas en el dominio de la seguridad digital [Rioseco-Pais et al., 2023]. Su principal fortaleza radica en que no se limita a la autopercepción, aunque su alcance sigue siendo local y limitado en cobertura.

DigComp-Ped constituye una extensión más amplia, aplicada a más de 4000 estudiantes en contextos latinoamericanos. A diferencia del COMPDIG-PED, este instrumento busca evaluar a gran escala el marco DigComp, manteniendo su enfoque en desempeño, lo que representa un avance significativo frente a los cuestionarios tradicionales. Sus resultados permitieron identificar perfiles de competencia digital y mapear debilidades específicas en el área de seguridad, con énfasis en la protección de datos personales y la sostenibilidad [Rioseco-Pais et al., 2024]. Su principal limitación es que, al ser una prueba estandarizada, todavía carece de componentes adaptativos que permitan personalizar la evaluación.

El Students' Digital Competence Scale (SDiCoS) es un instrumento europeo desarrollado por Tzafilkou. Se basa en autopercepción y está validado estadísticamente, incluyendo un factor específico para la competencia de seguridad digital. Evalúa aspectos como la conciencia sobre riesgos, las prácticas de protección de datos y la percepción de vulnerabilidad frente a amenazas digitales. Aunque es un instrumento robusto en términos psicométricos, su limitación principal es que mide lo que los estudiantes creen saber hacer, y no lo que efectivamente demuestran en entornos prácticos [Tzafilkou et al., 2022].

INCOTIC 2.0 es un instrumento iberoamericano diseñado para evaluar competencias digitales en contextos universitarios. Incluye una dimensión relacionada con la seguridad digital, evaluada mediante cuestionarios de autopercepción [González-Martínez et al., 2018]. Aunque su aplicación ha sido amplia en varios países de la región, comparte las limitaciones de los instrumentos de percepción: no permite observar el comportamiento real del usuario frente a escenarios de riesgo y, por tanto, ofrece diagnósticos parciales.

Aunque todos estos instrumentos han aportado información relevante, presentan una limitación común: ninguno incorpora tecnologías de inteligencia artificial ni entornos adaptativos capaces de ofrecer retroalimentación personalizada. En consecuencia, generan diagnósticos útiles pero incompletos, que dificultan el diseño de intervenciones formativas personalizadas y limitan su aplicabilidad en contextos diversos como los latinoamericanos. La propuesta de esta memoria busca precisamente superar estas limitaciones, ofreciendo un entorno evaluativo innovador y contextualizado.

2.6 RELACIÓN DEL MARCO CONCEPTUAL CON LA PROPUESTA DE SOLUCIÓN

El marco conceptual presentado en este capítulo establece los cimientos que sustentan la propuesta de solución de esta memoria. En primer lugar, DigComp ofrece el marco de referencia más actualizado y ampliamente validado para definir y evaluar las competencias digitales. Estas entregan la estructura de contenidos y habilidades que el entorno evaluativo debe abordar para garantizar la validez de constructo y la coherencia con estándares internacionales.

En segundo lugar, la revisión de la literatura y de los instrumentos existentes muestra que la principal brecha en la evaluación de la seguridad digital radica en la dependencia de instrumentos de autopercepción, los cuales no capturan el desempeño real de los usuarios y tienden a sobreestimar sus habilidades. Estudios recientes confirman la existencia de una desalineación entre percepción y práctica y evidencian que incluso en contextos con alta penetración tecnológica, los usuarios no logran aplicar conductas seguras de manera efectiva. En el caso latinoamericano, esta brecha se profundiza debido a desigualdades en el acceso, carencias en la formación docente y ausencia de instrumentos contextualizados.

Sobre esta base, la propuesta de solución busca cubrir tres brechas principales:

- Superar la dependencia de la autopercepción, implementando un entorno de evaluación basado en tareas situadas que observen el comportamiento real del usuario frente a escenarios de seguridad digital.
- Incorporar adaptabilidad en la evaluación, de manera que las pruebas no sean estáticas, sino que ajusten el nivel de dificultad y los tipos de tareas según el desempeño del participante, favoreciendo así un diagnóstico más preciso.
- Entregar retroalimentación formativa y personalizada, utilizando inteligencia artificial para analizar las trazas de interacción de los usuarios y ofrecer recomendaciones inmediatas que promuevan el aprendizaje continuo.

En conclusión, el marco conceptual presentado no solo expone el problema y sus antecedentes, sino que también sustenta la relevancia y originalidad de la propuesta de esta memoria: el desarrollo de un entorno evaluativo apoyado en inteligencia artificial, alineado con el marco DigComp y contextualizado a la realidad latinoamericana. Esta solución busca ofrecer una evaluación más objetiva y basada en desempeño, al mismo tiempo que proporciona retroalimentación formativa y adaptativa, contribuyendo así al fortalecimiento de la competencia de seguridad digital de manera pertinente y contextualizada.

CAPÍTULO 3: PROPUESTA DE SOLUCION

Se enmarca en la necesidad de contar con herramientas innovadoras, escalables y alineadas a principios éticos y normativos, capaces de generar valor tanto en contextos educativos como laborales y ciudadanos.

En las siguientes secciones se describen en detalle la arquitectura, funcionamiento, componentes y casos de uso de la plataforma, así como sus características diferenciales y beneficios esperados.

3.1 DESCRIPCIÓN GENERAL DE LA PLATAFORMA WEB

Es una plataforma digital diseñada para evaluar y desarrollar competencias digitales alineadas al marco DigComp 2.2, con un enfoque en el área de seguridad. Su propósito principal es ofrecer un entorno evaluativo auténtico, adaptativo y contextualizado a la realidad latinoamericana, que permita medir el desempeño real de los usuarios en tareas vinculadas a la protección de dispositivos, datos personales, salud y bienestar digital, así como sostenibilidad en el uso de las tecnologías.



Figura 4. Página de inicio de Ladico.

La interfaz de la plataforma fue desarrollada bajo criterios de usabilidad y accesibilidad, de manera que cualquier usuario —estudiante, trabajador o ciudadano— pueda navegar con facilidad. En la Figura 4 se muestra la página de inicio de Ladico, donde se invita a evaluar y certificar competencias digitales en las cinco áreas fundamentales del marco europeo DigComp 2.2. Esta presentación inicial enfatiza la propuesta de valor: una evaluación profesional, objetiva y contextualizada.

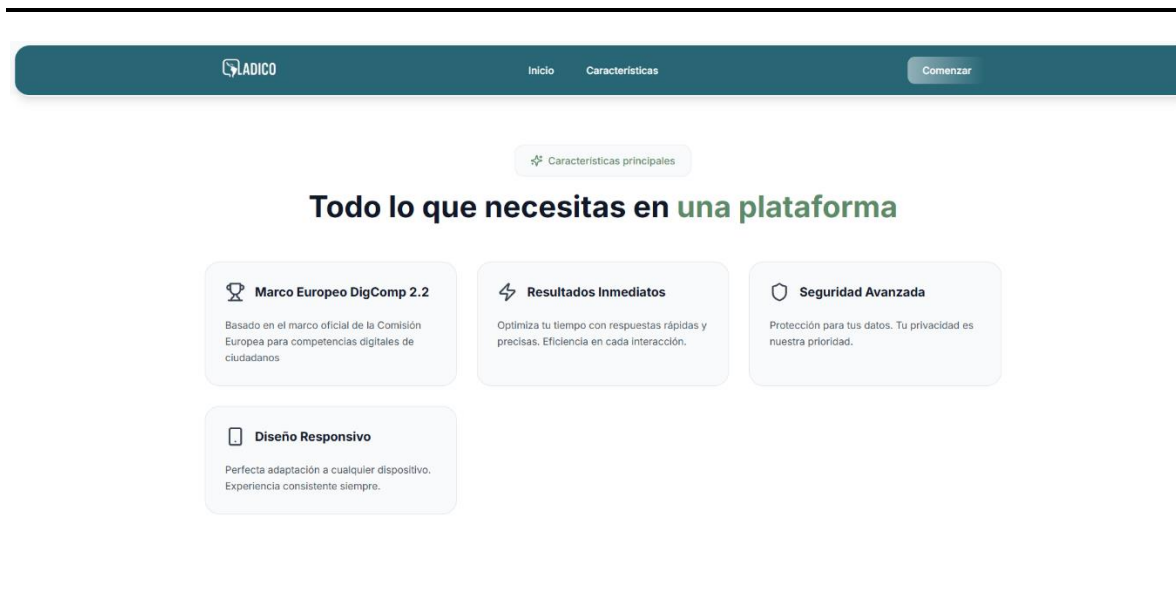


Figura 5. Características principales destacadas de Ladico.

En la sección de características principales, Ladico resalta sus pilares metodológicos: alineación con el marco DigComp 2.2, entrega de resultados inmediatos, seguridad avanzada en la gestión de datos y diseño responsivo que asegura un acceso desde cualquier dispositivo. Estos aspectos se ilustran en la Figura 5, donde se destacan las funciones centrales de la plataforma.

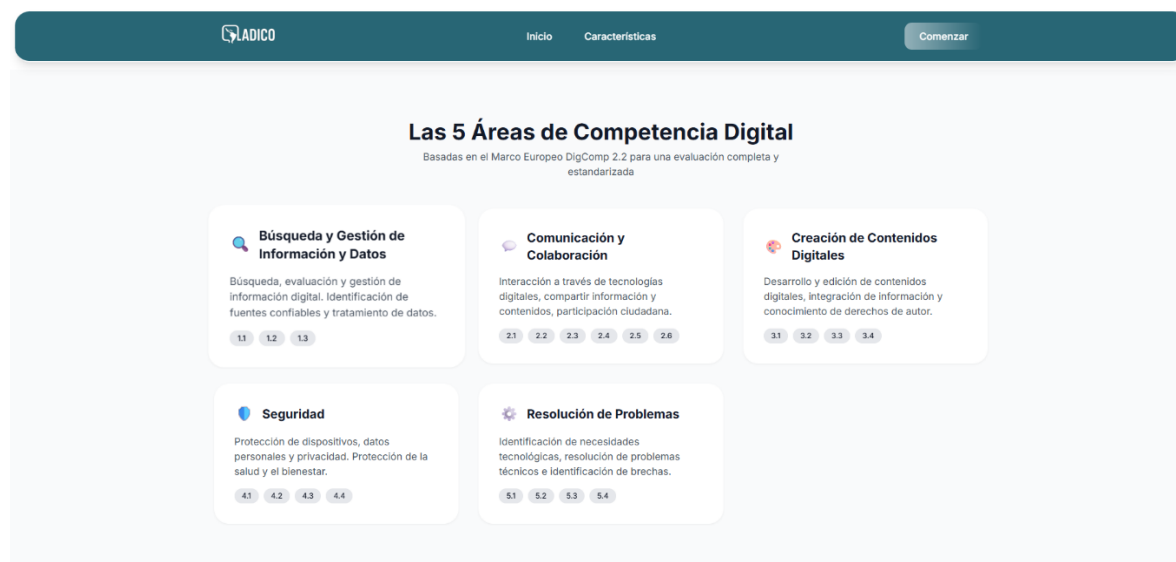


Figura 6. Áreas de competencia digital evaluadas en Ladico según DigComp 2.2.

Asimismo, la Figura 6 muestra las cinco áreas de competencia digital evaluadas en Ladico: Búsqueda y gestión de información y datos, Comunicación y colaboración, Creación de contenidos digitales, Seguridad, y Resolución de problemas. Cada área se organiza en

competencias, siguiendo la taxonomía propuesta por DigComp 2.2, lo que garantiza una cobertura integral y estructurada de las habilidades digitales.

Gracias a esta combinación de adaptabilidad, contextualización y tecnología, Ladico se posiciona como una solución innovadora que supera las limitaciones de los métodos tradicionales y contribuye a cerrar la brecha en la medición de competencias digitales en América Latina.

3.2 ARQUITECTURA E IMPLEMENTACIÓN DEL SISTEMA

La arquitectura de Ladico se diseñó con el objetivo de garantizar escalabilidad, seguridad y flexibilidad en la entrega de evaluaciones digitales adaptativas. Para ello, se adoptó un modelo de arquitectura multicapa complementado con módulos de inteligencia artificial y análisis de comportamiento del usuario, permitiendo integrar, en un mismo ecosistema, la experiencia evaluativa, la lógica de negocio y el almacenamiento seguro de datos.

3.2.1 CAPA DE SOLUCIÓN

La arquitectura general se organiza en tres capas principales y un módulo transversal de inteligencia artificial (ver Figura 7):

1. Capa de Presentación (**Front-End**): Desarrollada en **React/Next.js**, ofrece una interfaz accesible y responsiva que se adapta a distintos dispositivos. En esta capa se ubican los componentes visuales de la *landing page*, el *dashboard* de usuario y la interfaz de evaluación. Se prioriza la usabilidad mediante un diseño intuitivo y accesible, de modo que cualquier usuario —estudiante, trabajador o ciudadano— pueda navegar fácilmente.
2. Capa de Lógica de Negocio (Servicios): Implementada en *Node.js* bajo un esquema de *API REST*, gestiona los procesos internos de la plataforma. Aquí residen los servicios que controlan la autenticación, la gestión de sesiones de evaluación, la generación adaptativa de ítems, y el cálculo de resultados.

Entre sus principales componentes destacan:

- *questionsService*: carga o genera ítems en función de la competencia y el nivel del usuario, conectándose con los modelos de IA externos (*OpenAI*).
 - *resultsManager*: calcula el puntaje y actualiza las estadísticas de desempeño en tiempo real.
 - *AuthContext*: administra los permisos y la navegación según roles (usuario, administrador, profesor).
3. Capa de Persistencia de Datos: Se apoya en *Firebase/Firestore*, una base de datos NoSQL en la nube que permite almacenamiento seguro, sincronización en tiempo real y escalabilidad global. En esta capa se organizan las colecciones principales: *users*, *testSessions*, *questions* y *userResults*.
 4. Módulo de Inteligencia Artificial y Analítica: Actúa de forma transversal sobre las tres capas anteriores. Este módulo permite generar ítems dinámicos adaptados al contexto cultural y nivel en base a *prompts*.

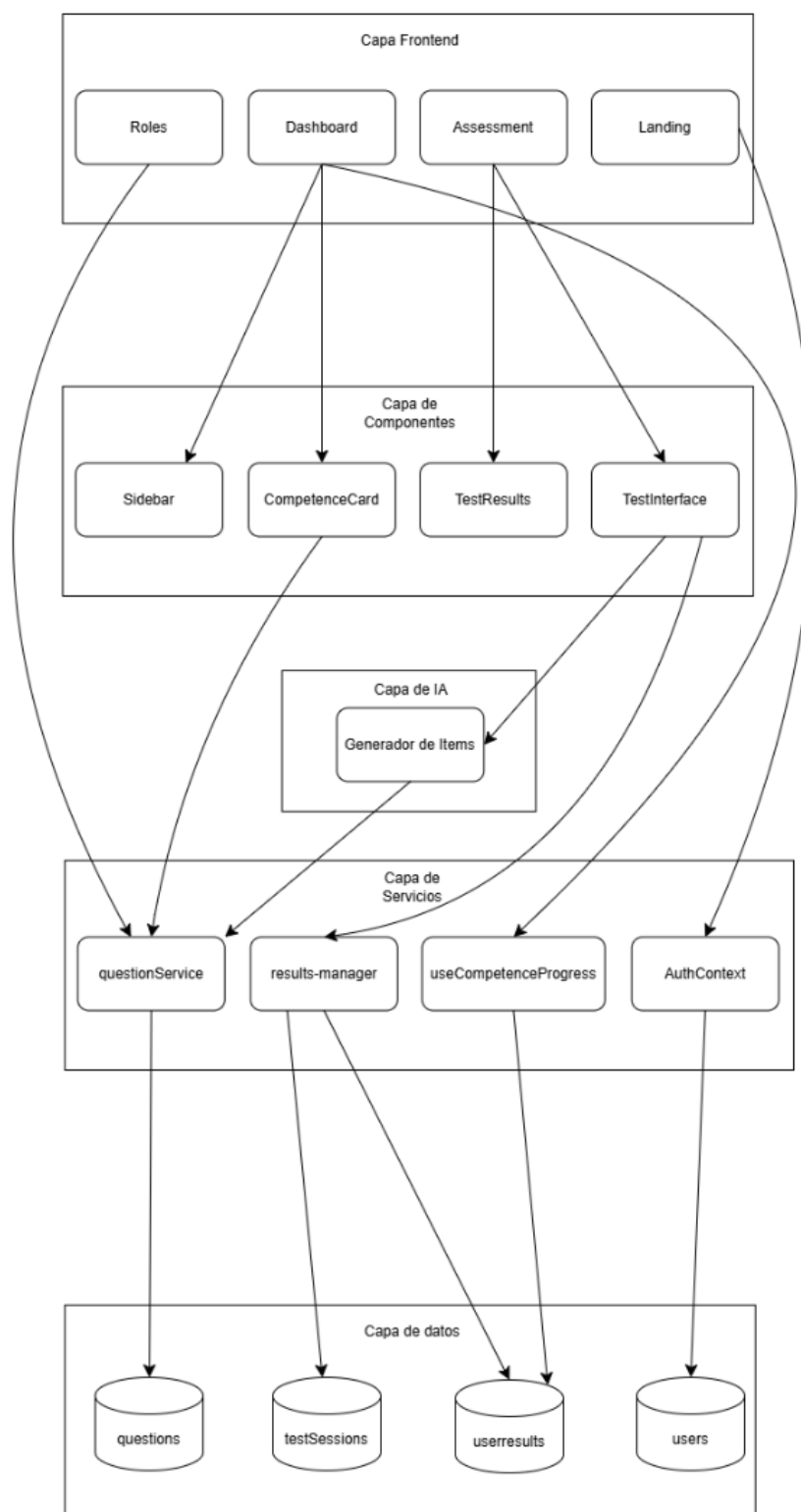


Figura 7. Capa de solución y flujo general de datos en Ladico.

3.2.2 FLUJO GENERAL DEL SISTEMA

La Figura 8 muestra el flujo general del sistema Ladico, que representa la secuencia de interacción entre las distintas rutas, componentes y servicios desde el momento en que el usuario accede a la aplicación hasta la obtención de los resultados finales. Este modelo unifica la navegación, la gestión de roles y la lógica de persistencia de datos, describiendo el comportamiento del sistema para tres perfiles principales: usuario, profesor y administrador.

El flujo comienza con el componente *Authentication*, que determina si el usuario está autenticado. En caso contrario, se redirige al Formulario de *Login*. Una vez autenticado, el sistema lo dirige al *Dashboard*, donde se habilitan distintas rutas según su rol:

- Los usuarios estándar acceden a la sección de Selección de Competencias (*CompetenceCard*), desde donde pueden iniciar una evaluación específica a través de la ruta */test/[competenceId]*.
- Los profesores son redirigidos al módulo */profesor*, donde pueden revisar resultados de sus estudiantes y analizar el progreso.
- Los administradores ingresan al panel */admin*, que permite la gestión de ítems, usuarios y configuraciones del sistema.

Durante la evaluación, el componente *TestInterface* controla la lógica de la sesión, permitiendo la carga de ítems mediante el servicio *loadQuestionsByCompetence()* y registrando las respuestas del usuario. Al finalizar, la plataforma ejecuta los procesos *saveUserResult()* y *updateQuestionStats()*, encargados de almacenar los resultados individuales y actualizar las estadísticas globales en la **lógica de datos**.

Finalmente, los resultados se presentan en la vista */test/[competenceId]/results*, donde el usuario puede consultar su puntaje y nivel alcanzado. Este flujo garantiza una experiencia coherente para todos los perfiles de usuario, manteniendo la trazabilidad y consistencia entre las distintas capas de la aplicación.

3.2.3 FLUJO DE NAVEGACIÓN Y AUTENTICACIÓN

La Figura 9 muestra el flujo de navegación inicial y autenticación de la plataforma Ladico, el cual define la forma en que los usuarios acceden y se orientan dentro del sistema. Este proceso se gestiona principalmente desde el componente *LandingPage* y el contexto de autenticación (*AuthContext*) en el *front-end*.

El flujo comienza cuando el usuario accede a la *landing page*, donde el componente *LadicoLanding* carga las secciones principales: *Hero*, Características y *Footer*. En esta vista inicial no se requiere autenticación, y su propósito es presentar el objetivo de la plataforma y permitir un acceso rápido mediante el botón “Comenzar”.

El *Header* del sitio es dinámico y se renderiza según el estado de autenticación del usuario:

- Si el usuario no está autenticado, el encabezado muestra el botón “Comenzar”, que redirige al formulario de inicio de sesión (*/login*).
- Si el usuario ya está autenticado, el *Header* muestra su nombre y un enlace directo al *Dashboard*, permitiéndole continuar con su sesión activa sin necesidad de reingresar credenciales.

Una vez autenticado, el usuario puede navegar hacia el *Dashboard*, donde se despliegan las competencias disponibles y el progreso personal. Este flujo está diseñado para ser simple, fluido y seguro, reduciendo los pasos de acceso e integrando los mecanismos de control de sesión proporcionados por *AuthContext* y *Firebase Authentication*.

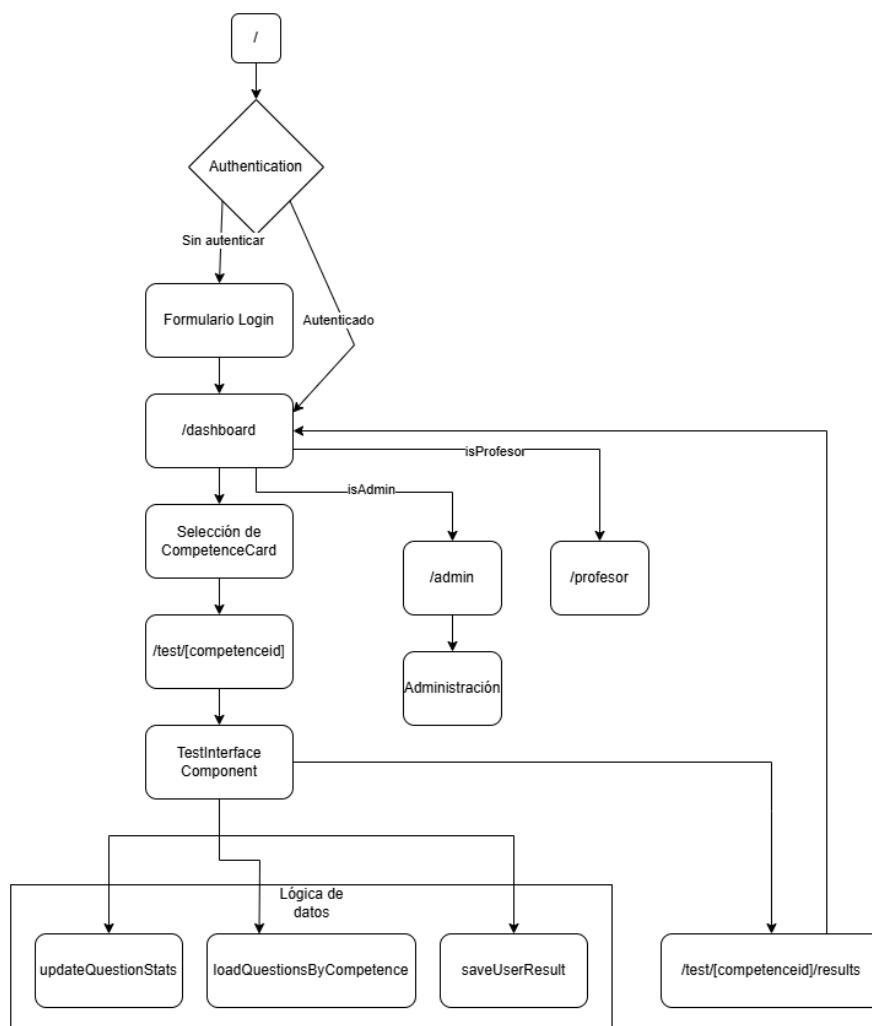


Figura 8. Flujo general del sistema Ladico.

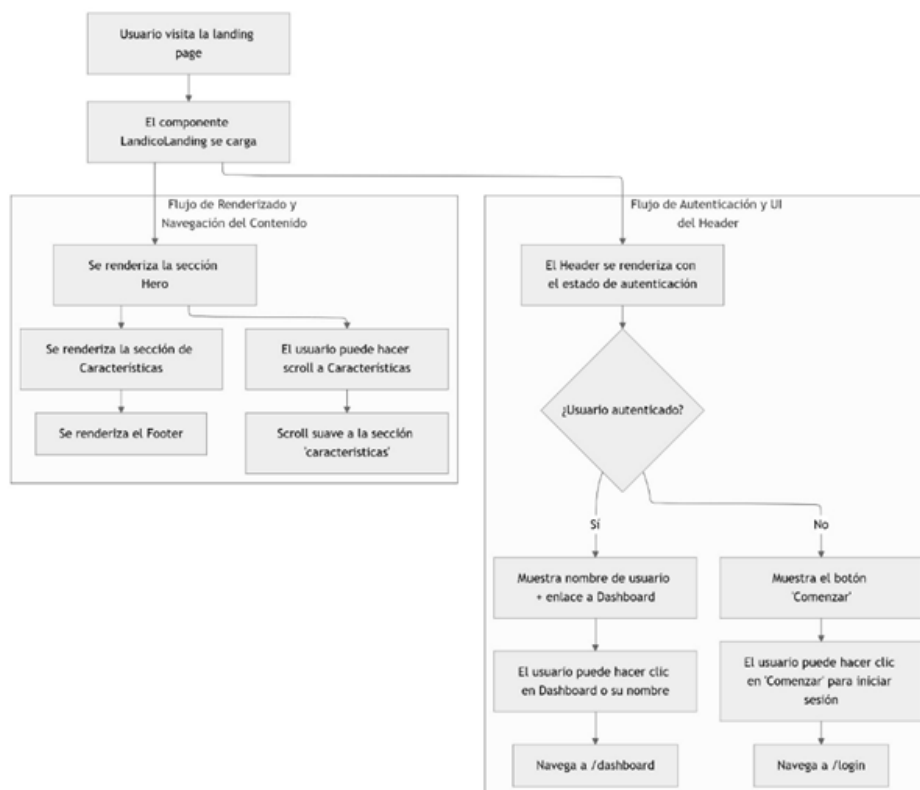


Figura 9. Flujo de navegación y autenticación inicial en Ladico.

3.2.4 LÓGICA INTERNA DEL PROCESO DE EVALUACIÓN

La Figura 10 representa la lógica interna del proceso de evaluación en Ladico, donde se modela el flujo completo que ocurre desde la carga de preguntas hasta el registro final de resultados. Este proceso combina la gestión de estado en el *front-end* con operaciones asincrónicas de lectura y escritura en la base de datos *Firestore*. El componente principal del sistema es *TestInterface*, encargado de renderizar dinámicamente cada pregunta y mantener el estado de la sesión (*TestSession State*).

Dentro de este estado se registran variables clave como:

- *currentQuestionIndex*: posición de la pregunta actual.
- *answers*: arreglo que almacena las respuestas seleccionadas por el usuario.

Durante la ejecución de la prueba, *questionsService* realiza la carga de ítems a través de la función *loadQuestionsByCompetence()*, la cual consulta la colección *questions* en la base de datos. Estos ítems han sido previamente generados por el módulo de inteligencia artificial, que crea preguntas alineadas con la competencia y el nivel del usuario mediante *prompts* parametrizados.

Una vez que el usuario completa la evaluación, se activa el proceso de finalización controlado por la función *handleTestComplete()*, la cual:

1. Calcula el puntaje total y determina si el usuario aprueba (*passed: boolean*).
2. Actualiza las estadísticas globales mediante *updateQuestionStats()*, registrando aciertos y errores por pregunta.
3. Persiste los resultados en las colecciones *testSessions* y *userResults*, garantizando trazabilidad de cada sesión.

Esta estructura modular asegura la separación entre la capa lógica y la persistencia, lo que facilita la escalabilidad y la integración futura con modelos de evaluación adaptativa.

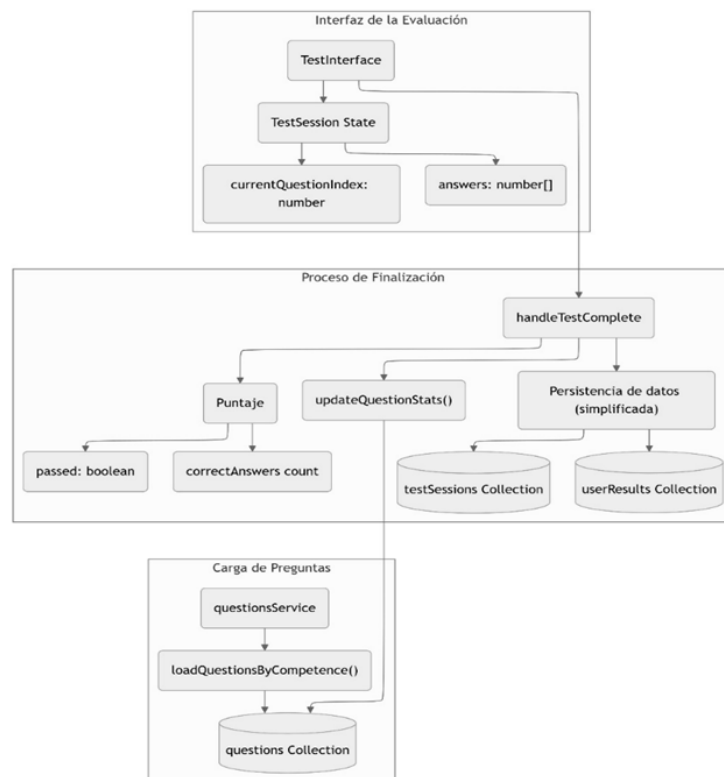


Figura 10. Lógica interna del proceso de evaluación en Ladico.

3.3 METODOLOGÍA DE FUNCIONAMIENTO

Ladico se articula en un flujo sencillo e intuitivo que guía al usuario desde su ingreso hasta la realización de ejercicios personalizados. La investigación adopta un enfoque exploratorio-aplicado, al proponer y validar un nuevo entorno tecnológico de evaluación basado en inteligencia artificial, con el propósito de verificar su viabilidad técnica y conceptual.

Para asegurar la validez de contenido del banco de preguntas y ejercicios generados mediante inteligencia artificial, se realizaron revisiones expertas con académicos del área de tecnología educativa y competencias digitales. Los especialistas evaluaron la correspondencia de los ítems con los descriptores del marco DigComp 2.2, así como su claridad, pertinencia cultural y nivel de dificultad. Las observaciones obtenidas fueron incorporadas en los prompts que guían la generación automatizada de los ejercicios.

En cuanto a su funcionamiento, en primer lugar, el usuario accede a la plataforma mediante un inicio de sesión y completa un breve perfil que permite contextualizar la evaluación según su edad, país y género. Una vez autenticado, se presenta la pantalla de selección de competencias, donde puede elegir el área y competencias específicas a evaluar. En la Figura 11 se muestra la interfaz correspondiente al área 4 (Seguridad), que incluye sus cuatro competencias.



Figura 11. Interfaz de selección de competencias en Ladico para el área de Seguridad.

Posteriormente, el sistema despliega la interfaz de evaluación, en la que se presentan preguntas y simulaciones generadas dinámicamente mediante inteligencia artificial. Estas preguntas están adaptadas al contexto latinoamericano y diseñadas para medir las competencias del DigComp 2.2 en distintos niveles de dificultad. La Figura 12 muestra un ejemplo de una pregunta de nivel básico en la competencia 4.4 Protección medioambiental, donde el usuario debe identificar la acción que reduce el impacto ambiental asociado al uso de dispositivos y la transmisión de video en alta resolución. Este tipo de ejercicio permite evaluar si el participante reconoce prácticas sostenibles en el consumo digital, como el uso eficiente de la energía y de los datos móviles, contribuyendo al desarrollo de una conciencia ambiental en el uso responsable de la tecnología.

La generación de este tipo de preguntas se apoya en prompts predefinidos que guían a la IA en la construcción de ítems coherentes con el marco de competencias. Este enfoque asegura que las evaluaciones no solo midan conocimientos técnicos sobre protección digital, sino también habilidades críticas como la identificación de riesgos, la toma de decisiones seguras en entornos digitales y la aplicación responsable de buenas prácticas de ciberseguridad y sostenibilidad tecnológica.

The screenshot shows a quiz interface for '4.4 Protección Medioambiental - Nivel Básico'. It is 'Pregunta 1 de 3'. The question is 'Impacto de la transmisión en video' and asks what action reduces environmental impact when watching 4K videos on a mobile phone. There are four radio button options: 'Bajar la resolución a calidad estándar cuando no es necesario 4K', 'Usar siempre datos móviles para aprovechar la velocidad', 'Mantener el brillo al máximo durante todo el partido', and 'Dejar el video en pausa con la pantalla encendida'. A 'Siguiente' button is at the bottom right, and a feedback message says 'Por favor, selecciona una respuesta para continuar'.

39

Impacto de la transmisión en video

Usted ve partidos de fútbol en su celular usando datos móviles en resolución 4K. Nota que la batería se descarga más rápido y la cuenta de datos se eleva. ¿Qué acción reduce el impacto ambiental?

☐ Bajar la resolución a calidad estándar cuando no es necesario 4K

☐ Usar siempre datos móviles para aprovechar la velocidad

☐ Mantener el brillo al máximo durante todo el partido

☐ Dejar el video en pausa con la pantalla encendida

Siguiente

Por favor, selecciona una respuesta para continuar

Figura 12. Pregunta de nivel básico en la competencia 4.4 Protección medioambiental.

The screenshot shows a quiz interface for '4.4 Protección medioambiental - Nivel Intermedio'. It is 'Pregunta 2 de 3'. The question is 'Configurar el dispositivo para reducir su consumo energético' and asks the user to configure a mobile phone to reduce energy consumption. It includes a visual representation of a 'Centro de control' (Control Center) with eight toggle switches: Wi-Fi, Datos móviles, Modo avión, Brillo automático, Bluetooth, Localización (GPS), Ahorro de batería, and Modo oscuro. The 'Wi-Fi', 'Datos móviles', 'Modo avión', and 'Modo oscuro' toggles are currently off, while 'Bluetooth', 'Localización (GPS)', and 'Ahorro de batería' are on. A 'Siguiente' button is at the bottom right.

Configurar el dispositivo para reducir su consumo energético

Se le presenta un menú de configuraciones rápidas de un teléfono móvil donde aparecen los iconos que permiten activar o desactivar distintas funciones. Configure el teléfono de modo que ayude a reducir el consumo energético.

9:41 | Centro de control

Wi-Fi

Datos móviles

Modo avión

Brillo automático

Bluetooth

Localización (GPS)

Ahorro de batería

Modo oscuro

Siguiente

Figura 13. Pregunta de nivel intermedio en la competencia 4.4 Protección medioambiental.

En los niveles siguientes, la complejidad de las tareas aumenta progresivamente. La Figura 13 corresponde al nivel intermedio, donde se solicita al usuario configurar un dispositivo

móvil para optimizar su consumo energético, seleccionando las opciones adecuadas dentro de un menú de configuraciones rápidas. Este tipo de ejercicio permite evaluar la capacidad del participante para aplicar conocimientos prácticos orientados a la sostenibilidad digital, identificando las acciones que contribuyen a reducir el impacto ambiental y el uso innecesario de recursos energéticos.

Finalmente, la Figura 14 presenta un ejemplo correspondiente al nivel avanzado de la competencia 4.4 Protección medioambiental, enfocado en la aplicación autónoma de configuraciones digitales sostenibles. En este nivel, el usuario debe navegar por las opciones del sistema y seleccionar los ajustes que reduzcan al máximo el consumo energético y el impacto ambiental del teléfono, sin comprometer las funciones esenciales del dispositivo. El ejercicio busca evaluar la toma de decisiones informadas y la autonomía digital al equilibrar la eficiencia tecnológica con la sostenibilidad, fomentando una comprensión más profunda sobre el uso responsable de la energía y los recursos digitales.

Este tipo de tareas permite observar la capacidad del participante para integrar criterios ambientales en la gestión cotidiana de la tecnología, en concordancia con los descriptores del nivel avanzado del marco DigComp 2.2.

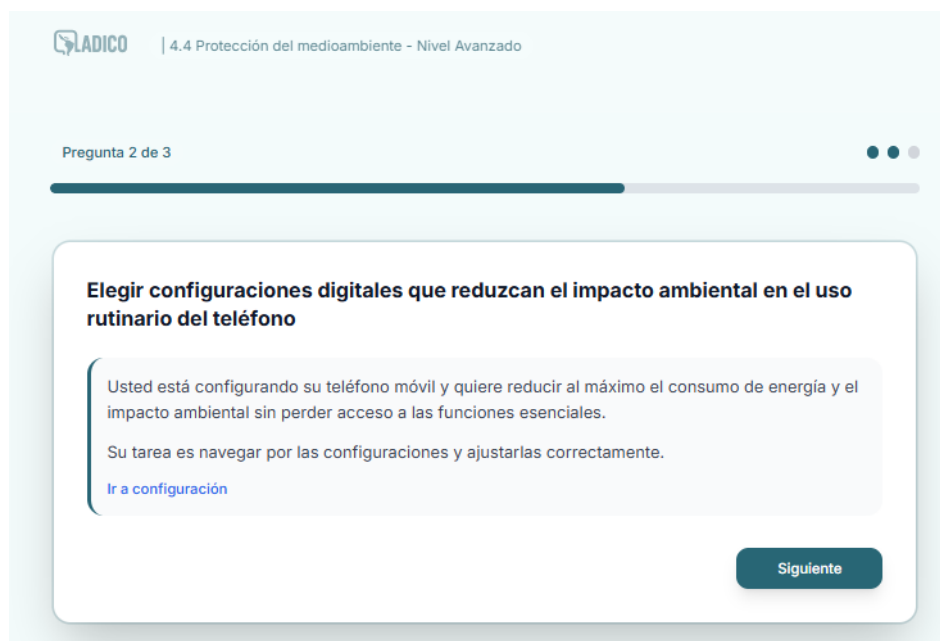


Figura 14. Ejemplo de pregunta de nivel avanzado en la competencia 4.4: Protección medioambiental.

3.4 CARACTERÍSTICAS DIFERENCIALES

Ladico se distingue de otras plataformas e instrumentos de evaluación de competencias digitales gracias a un conjunto de características que combinan innovación tecnológica, pertinencia cultural y enfoque general de usuarios:

- **Contextualización al entorno latinoamericano:** todos los escenarios y preguntas se diseñan considerando situaciones, servicios y herramientas comunes en países de América Latina, lo que aumenta la relevancia y validez de la evaluación.
- **Generación dinámica de ítems mediante IA:** el uso de inteligencia artificial permite crear preguntas y simulaciones únicas en cada sesión, evitando la memorización mecánica y asegurando la variabilidad del contenido evaluativo.
- **Escalabilidad y modularidad:** la arquitectura permite incorporar nuevas áreas del DigComp 2.2 y expandir la cobertura a otros contextos y marcos de competencias.

CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN

El presente capítulo expone el análisis de los resultados obtenidos durante el proceso de validación de la plataforma Ladico, cuyo propósito fue comprobar su eficacia como entorno de evaluación digital basado en el marco DigComp 2.2, específicamente en el área de Búsqueda y gestión de información y datos.

La validación tuvo como objetivo principal determinar la **correspondencia entre la autopercepción de los usuarios sobre sus competencias digitales**, medida mediante un cuestionario previo, y su desempeño real evaluado en Ladico, a través de tareas de búsqueda, evaluación y gestión de información. Este contraste permite analizar en qué medida la percepción subjetiva de los participantes refleja su competencia digital efectiva, un aspecto ampliamente discutido en la literatura [Aesaert et al., 2017], [Sillat, 2021], [Mehrvarez et al., 2021].

4.1 DESCRIPCIÓN GENERAL DE LA MUESTRA

La muestra considerada en el proceso de validación estuvo compuesta por 30 participantes pertenecientes a la Universidad Técnica Federico Santa María (USM), quienes participaron voluntariamente en las actividades de evaluación. Todos cursaban el último año de la carrera de Ingeniería Civil Informática, lo que permitió aplicar el entorno en un grupo con sólida experiencia en el uso de tecnologías digitales y con alta familiaridad con entornos virtuales de aprendizaje.

El procedimiento contempló dos etapas consecutivas: primero, la aplicación del cuestionario de autopercepción de competencias digitales, adaptado del instrumento DigCompSAT (A Self-reflection Tool for DigComp) desarrollado por JRC de la Comisión Europea [¡Error! No se encuentra el origen de la referencia.]; y posteriormente, la realización de las evaluaciones prácticas en la plataforma Ladico. Esta secuencia permitió comparar la percepción subjetiva de los participantes con su desempeño real en tareas vinculadas al marco DigComp 2.2.

La composición por género fue predominantemente masculina, con 27 hombres (90%) y 3 mujeres (10%), tendencia consistente con la distribución habitual en programas de ingeniería civil informática. En cuanto a la edad, los participantes se concentraron principalmente en el rango de 22 a 25 años, correspondiente a estudiantes de los cursos superiores de pregrado.

En síntesis, la muestra utilizada en esta etapa constituye un grupo homogéneo, joven y tecnológicamente competente, idóneo para verificar el desempeño técnico y la validez inicial del sistema. Debido a esta homogeneidad en edad, nivel académico y dominio tecnológico, no se realizará un análisis de diferencias significativas entre grupos (por género u otras variables), ya que la falta de variabilidad en estos factores impedirá obtener resultados comparativos con validez estadística.

4.2 RESULTADOS DEL CUESTIONARIO DE PERCEPCIÓN

Antes de acceder a la plataforma Ladico, los participantes completaron un cuestionario de percepción inicial diseñado para medir su autovaloración respecto a las competencias del área de Seguridad del marco DigComp 2.2 como muestra la Tabla 1. Este instrumento tuvo como propósito identificar la confianza percibida por los usuarios en su capacidad para proteger sus dispositivos, datos personales, bienestar y entorno digital, sirviendo como línea base para contrastarla con su desempeño real dentro de la plataforma.

Preguntas
P1. Comprendo las ventajas y los riesgos de seguridad cuando se utilizan dispositivos o sistemas conectados a internet (por ejemplo, relojes o dispositivos domésticos inteligentes).
P2. Conozco la importancia de mantener actualizados el sistema operativo, el antivirus y otros programas informáticos para evitar problemas de seguridad.
P3. Sé cómo configurar los parámetros de un firewall en diferentes dispositivos.
P4. Sé cómo recuperar datos, información y contenido digital (por ejemplo, fotos, contactos) a partir de una copia de seguridad.
P5. Sé cómo restringir o denegar el acceso a mi ubicación geográfica.
P6. Sé cómo identificar los mensajes de correo electrónico sospechosos que tratan de obtener mis datos personales.
P7. Sé cómo comprobar que un sitio web en el que se me pide que facilite datos personales es seguro (por ejemplo, sitios https, logotipo o certificado de seguridad).
P8. Sé qué datos personales no debo compartir y mostrar en internet (por ejemplo, en redes sociales).
P9. Tengo cuidado al comprobar las políticas de privacidad de los servicios digitales que utilizo.
P10. Soy consciente de que debo administrar el tiempo que paso utilizando mis dispositivos digitales.
P11. Sé cómo protegerme de encuentros y materiales no deseados y maliciosos en internet (p.ej. mensajes de spam, correos para robar mi identidad).
P12. Sé que hay herramientas digitales que pueden ayudar a las personas mayores o con necesidades especiales.
P13. Busco formas en las que las tecnologías digitales puedan ayudarme a vivir y consumir de forma más respetuosa con el medio ambiente.
P14. Sé que los dispositivos y consumibles digitales (por ejemplo, computadoras, teléfonos, baterías) deben ser eliminados de manera adecuada para reducir al mínimo su impacto ambiental.
P15. Sé cómo reducir el consumo de energía de mis dispositivos (por ejemplo, cambiar la configuración, cerrar aplicaciones, apagar el wifi).
P16. Conozco los comportamientos "verdes" que debo seguir al comprar o utilizar dispositivos digitales (por ejemplo, comprar dispositivos con etiqueta ecológica, evitar imprimir innecesariamente, no dejar conectados los cargadores sin el dispositivo).

Tabla 1. Preguntas del cuestionario de autopercepción para el área de seguridad.

El cuestionario fue aplicado mediante Google Forms y estructurado con ítems en escala Likert de 1 a 5 puntos, donde 1 representaba un nivel “muy bajo” y 5 un nivel “muy alto” de autopercepción. Cada competencia del área fue evaluada a través de un conjunto de afirmaciones que abordaban situaciones cotidianas relacionadas con la seguridad y el uso responsable de la tecnología, considerando tanto aspectos conductuales como de conciencia digital.

En total, el instrumento incluyó 16 ítems, distribuidos de la siguiente manera:

- **Competencia 4.1 (P1 – P4): Protección de dispositivos**
Evalúa la capacidad para aplicar medidas básicas de seguridad, como contraseñas seguras, antivirus y actualizaciones del sistema.
- **Competencia 4.2 (P5 – P9): Protección de datos personales y privacidad**
Explora el conocimiento y las prácticas sobre gestión de información personal, configuración de privacidad y protección frente a riesgos en línea.
- **Competencia 4.3 (P9 – P12): Protección de la salud y del bienestar**
Analiza la conciencia del usuario respecto al uso equilibrado y seguro de la tecnología, incluyendo hábitos saludables y prevención de riesgos digitales.
- **Competencia 4.4 (P13 – P16): Protección medioambiental**
Evalúa el grado de responsabilidad digital en el uso sostenible de los recursos tecnológicos y la gestión de residuos electrónicos.

Los resultados generales del cuestionario muestran que los participantes presentan una autopercepción elevada en las cuatro competencias del área, con una concentración mayoritaria de respuestas en los niveles 4 y 5 de la escala.

- En la **competencia 4.1**, el 42 % de las respuestas correspondió al nivel 5 y el 26 % al nivel 4, lo que refleja una alta confianza en la capacidad para mantener la seguridad de los equipos y aplicar medidas preventivas básicas como contraseñas seguras o actualizaciones de software.
- En la **competencia 4.2**, el 47 % de los participantes se calificó en el nivel 5 y el 35 % en el nivel 4, evidenciando una percepción positiva y consistente sobre sus habilidades para resguardar información personal, configurar la privacidad y prevenir riesgos en línea.
- En la **competencia 4.3**, el 46 % alcanzó el nivel 5 y el 31 % el nivel 4, lo que indica una autopercepción alta pero más dispersa, con algunos participantes que aún se sitúan en niveles intermedios (17 % en nivel 3), lo que podría reflejar diferencias en la conciencia sobre el impacto del uso intensivo de las tecnologías.

- Finalmente, en la **competencia 4.4**, el 56 % de los participantes se ubicó en el nivel 5 y el 19 % en el nivel 4, mostrando una mayor confianza en la aplicación de prácticas responsables y sostenibles relacionadas con el uso y descarte de dispositivos tecnológicos.

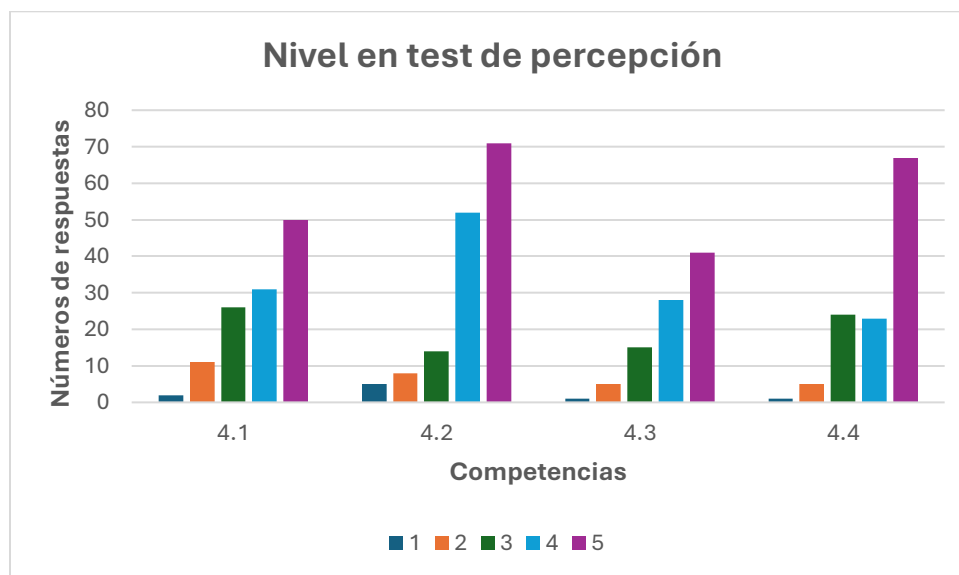


Figura 15. Distribución de respuestas del cuestionario de percepción en el área de Seguridad.

En conjunto, estos resultados reflejan una autopercepción sólida y homogénea respecto de las competencias de seguridad digital. La mayoría de los participantes se considera capaz de proteger sus dispositivos, datos personales y entorno digital, aunque se observa una leve variabilidad en los aspectos vinculados al bienestar digital.

4.3 RESULTADOS DE DESEMPEÑO EN LADICO

Una vez completado el cuestionario de percepción inicial, los participantes accedieron a la plataforma Ladico para realizar la evaluación práctica correspondiente al área de Seguridad del marco DigComp 2.2. El entorno evaluativo se estructuró en cuatro competencias —4.1 Protección de dispositivos, 4.2 Protección de datos personales y privacidad, 4.3 Protección de la salud y el bienestar y 4.4 Protección medioambiental—, cada una compuesta por actividades interactivas generadas mediante inteligencia artificial, diseñadas para observar la aplicación práctica de los conocimientos y habilidades digitales de los usuarios.

Durante la validación, la plataforma registró automáticamente el nivel alcanzado por cada participante (básico, intermedio o avanzado), permitiendo obtener evidencia objetiva y cuantificable de su desempeño real. Esta información fue posteriormente utilizada para comparar los resultados prácticos con la autopercepción inicial, a fin de analizar la coherencia entre ambos instrumentos y aportar evidencia a la validez del entorno evaluativo.

Los resultados obtenidos en la plataforma Ladico evidencian que la mayoría de los participantes logró completar satisfactoriamente los niveles básico e intermedio, mientras que un grupo menor alcanzó el nivel avanzado en todas las competencias. Tal como se presenta en la Tabla 2, la totalidad de los participantes consiguió finalizar el nivel básico, el 60 % avanzó hasta el nivel intermedio y un 27 % alcanzó el nivel avanzado. Esta distribución refleja una progresión esperada en el desempeño, donde la complejidad de las tareas y los criterios de evaluación aumentan progresivamente en cada nivel. En conjunto, los resultados muestran un rendimiento positivo y consistente en las competencias del área de Seguridad, confirmando que los participantes fueron capaces de aplicar medidas de protección digital, privacidad, bienestar y sostenibilidad tecnológica de manera efectiva en distintos contextos de evaluación.

Nivel	Cantidad de participantes que alcanzaron el nivel	Porcentaje de logro
Nivel 1	30	100%
Nivel 2	18	60%
Nivel 3	8	27%

Tabla 2. Participantes según nivel de desempeño alcanzado en la plataforma Ladico.

El análisis por competencia muestra un comportamiento homogéneo y positivo en el desempeño general del área de Seguridad. Tal como se observa en la Tabla 3 y en el Figura 16, todos los participantes lograron completar el nivel 1 en las cuatro competencias, lo que confirma que las habilidades fundamentales de protección digital están sólidamente adquiridas en el grupo evaluado. La mayoría también alcanzó el nivel 2, con porcentajes de logro superiores al 75 %, lo que evidencia la capacidad de aplicar medidas de seguridad de manera funcional y autónoma en situaciones de complejidad media. En cuanto al nivel 3, se aprecia una disminución esperada en la proporción de participantes, coherente con el incremento de exigencia cognitiva y práctica de las tareas.

Las competencias 4.3 y 4.4 presentan los porcentajes más altos en este nivel (63 %), lo que sugiere un mayor dominio en la adopción de hábitos digitales responsables y sostenibles. En contraste, las competencias 4.1 y 4.2 alcanzan un 37 % de logro avanzado, indicando que las acciones más técnicas de seguridad y gestión de datos representan un desafío mayor para parte de los participantes. El promedio general de logro por competencia oscila entre 76 % y 87 %, reflejando un rendimiento estable y consistente en todo el conjunto del área. Estos resultados permiten concluir que los participantes demostraron una apropiación efectiva de las competencias de seguridad digital, con un dominio sólido en las prácticas esenciales y un avance progresivo hacia los niveles más complejos de autonomía y conciencia digital, en concordancia con los descriptores del marco DigComp 2.2.

Competencia	Nivel 1	Nivel 2	Nivel 3	Promedio Niveles
4.1	100%	90%	37%	76%

4.2	100%	100%	37%	79%
4.3	100%	77%	63%	80%
4.4	100%	97%	63%	87%

Tabla 3. Porcentaje de participantes que alcanzaron cada nivel de desempeño por competencia del área de Seguridad.

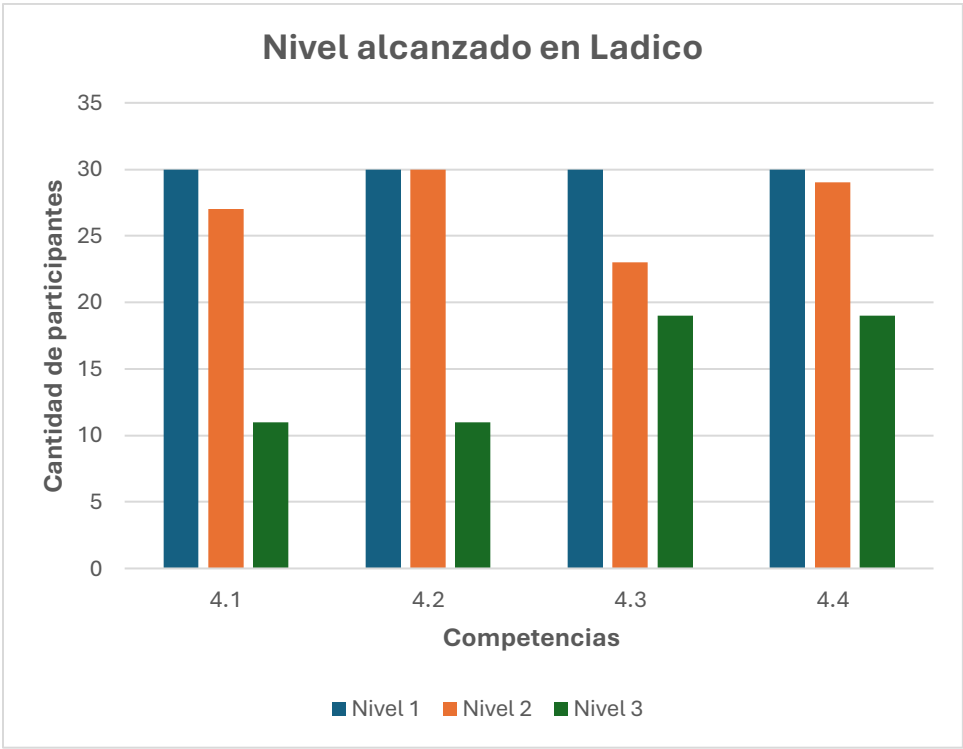


Figura 16. Niveles de desempeño alcanzados por competencia en la plataforma Ladico.

En conjunto, los datos de desempeño permiten afirmar que la plataforma Ladico ofrece resultados consistentes y diferenciados por nivel, lo que respalda su capacidad para evaluar de manera válida y gradual las competencias digitales del área de Seguridad.

Estos hallazgos proporcionan la base para el análisis comparativo posterior entre la autopercepción declarada por los participantes y el nivel de desempeño efectivamente alcanzado, con el fin de validar la coherencia y fiabilidad del sistema de evaluación.

4.4 RESULTADOS DE CORRELACIÓN PERCEPCIÓN-DESEMPEÑO

Con el propósito de evaluar la validez del entorno Ladico como instrumento de medición objetiva de las competencias digitales del área de Seguridad, se realizó un análisis correlacional entre los resultados del cuestionario de percepción inicial y los niveles de desempeño alcanzados en la plataforma. Este análisis tuvo como finalidad determinar si existe coherencia entre la autopercepción declarada por los participantes —respecto a sus capacidades para proteger dispositivos, datos personales, bienestar y entorno digital— y su

desempeño real al resolver tareas prácticas asociadas a estas competencias. La relación entre ambas medidas permite obtener evidencia empírica sobre la fiabilidad y validez del entorno Ladico como herramienta de evaluación, verificando su capacidad para medir de manera consistente y alineada con el marco DigComp 2.2 los distintos niveles de competencia en materia de seguridad digital.

4.4.1 PROCEDIMIENTO DEL ANÁLISIS CORRELACIONAL

Los resultados de la Tabla 4 muestran una correlación positiva en todas las competencias del área de Seguridad, indicando que los participantes que se perciben con un mayor nivel de dominio tienden efectivamente a alcanzar mejores resultados en las evaluaciones prácticas.

Competencias	R	R ²
4.1	0,78	0,61
4.2	0,80	0,64
4.3	0,80	0,64
4.4	0,87	0,75

Tabla 4. Correlación entre percepción y desempeño por competencia del área de Seguridad.

Los valores de R se sitúan entre 0,78 y 0,87, lo que representa una relación fuerte y consistente según los criterios de Cohen, mientras que los coeficientes R², comprendidos entre 0,61 y 0,75, indican que entre un 41 % y un 75 % de la variabilidad del desempeño real puede explicarse a partir de la autopercepción inicial.

La correlación más alta se observa en la competencia 4.4, con un R = 0,87 y R² = 0,75, lo que evidencia una coherencia muy fuerte entre la autopercepción y el desempeño práctico en prácticas de sostenibilidad y uso responsable de recursos digitales. Por su parte, las competencias 4.2 y 4.3 presentan valores similares (R = 0,80; R² = 0,64), reflejando una correspondencia sólida y equilibrada entre la confianza declarada y la ejecución efectiva en tareas vinculadas a la privacidad, el bienestar y la seguridad digital. Finalmente, la competencia 4.1 muestra un R = 0,78 y R² = 0,61, manteniendo una relación fuerte pero ligeramente inferior, posiblemente debido a diferencias en la aplicación práctica de medidas técnicas de protección.

En conjunto, estos resultados respaldan la validez del entorno Ladico como herramienta de evaluación, al mostrar una correspondencia sólida entre las medidas subjetivas (percepción) y las objetivas (desempeño), en plena coherencia con los principios del marco DigComp 2.2 para el área de Seguridad digital.

4.4.2 COMPETENCIA 4.1 – PROTECCIÓN DE DISPOSITIVOS

La Figura 17 muestra la relación entre la autopercepción declarada por los participantes y el nivel real de desempeño alcanzado en la competencia 4.1. Esta competencia evalúa la capacidad de los usuarios para mantener la seguridad de sus equipos y contenidos digitales,

aplicando medidas preventivas como contraseñas seguras, actualizaciones de software, uso de antivirus y configuración de redes seguras.

El gráfico de dispersión evidencia una correlación positiva fuerte entre el nivel percibido y el nivel efectivamente alcanzado en la plataforma, con un coeficiente de $R = 0,78$ y un $R^2 = 0,61$. Esto significa que el 61 % de la variabilidad del desempeño real puede explicarse por la autopercepción inicial, lo que indica una coherencia alta entre la confianza declarada y las habilidades demostradas por los participantes. La tendencia ascendente de la línea de regresión muestra que, a medida que los usuarios se perciben más competentes, tienden a obtener mejores resultados en la resolución de tareas prácticas, especialmente en acciones relacionadas con la protección de dispositivos frente a amenazas comunes.

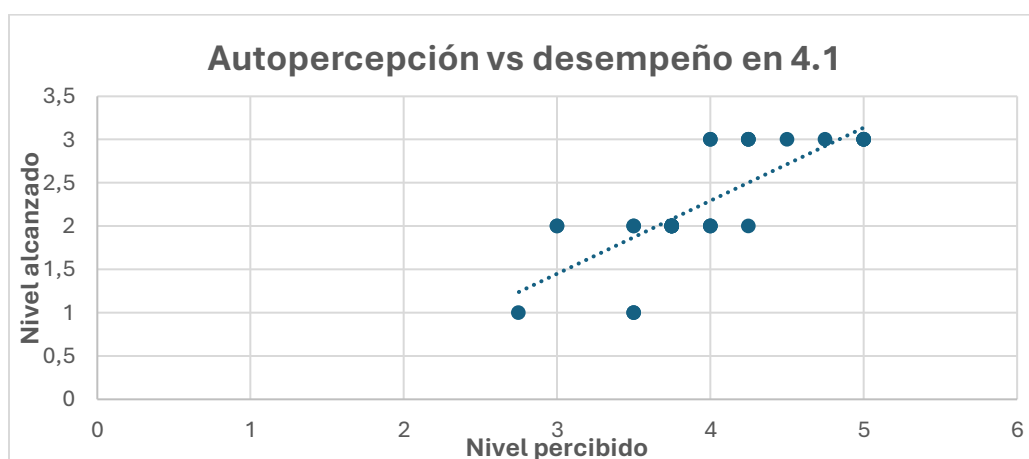


Figura 17. Relación entre autopercepción y el desempeño en la competencia 4.1.

Estos resultados respaldan la validez del entorno Ladico en la medición objetiva de esta competencia, demostrando que el instrumento es capaz de reflejar de forma consistente el nivel real de conocimiento y aplicación de medidas básicas de seguridad digital.

4.4.3 COMPETENCIA 4.2 – PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD

La Figura 18 muestra la relación entre la autopercepción de los participantes y el nivel real de desempeño obtenido en la competencia 4.2. Esta competencia evalúa la capacidad de los usuarios para identificar riesgos asociados al manejo de información personal, configurar adecuadamente la privacidad en entornos digitales y aplicar prácticas seguras frente a amenazas como el robo de datos o la exposición de información sensible.

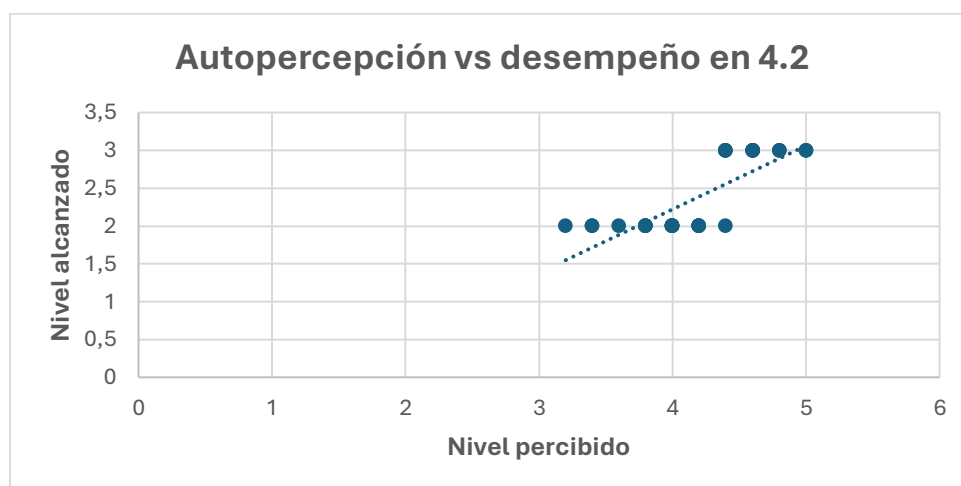


Figura 18. Relación entre autopercepción y el desempeño en la competencia 4.2.

El gráfico de dispersión evidencia una correlación positiva fuerte, con un coeficiente $R = 0,80$ y un $R^2 = 0,64$, lo que significa que un 64 % de la variabilidad en el desempeño real puede explicarse por la autopercepción inicial de los participantes. Esta relación indica una consistencia destacable entre la percepción de competencia y la ejecución práctica en tareas que implican el reconocimiento y la gestión de la privacidad digital. La línea de tendencia ascendente muestra que los participantes que se perciben más competentes tienden efectivamente a obtener mejores resultados en la evaluación, lo que refleja una comprensión sólida de los principios de protección de datos y su aplicación en contextos cotidianos.

Estos resultados refuerzan la validez del entorno Ladico como instrumento de medición en el área de Seguridad, al demostrar que la plataforma es capaz de distinguir adecuadamente los niveles de dominio en materia de privacidad y gestión de información personal.

4.4.4 COMPETENCIA 4.3 – PROTECCIÓN DE LA SALUD Y DEL BIENESTAR

La Figura 19 presenta la relación entre la autopercepción inicial de los participantes y el nivel real de desempeño alcanzado en la competencia 4.3. Esta competencia aborda la capacidad de los usuarios para mantener un equilibrio saludable en el uso de las tecnologías digitales, considerando aspectos como la gestión del tiempo en línea, la prevención de la fatiga digital y la protección frente a riesgos psicológicos o sociales derivados del uso intensivo de dispositivos.

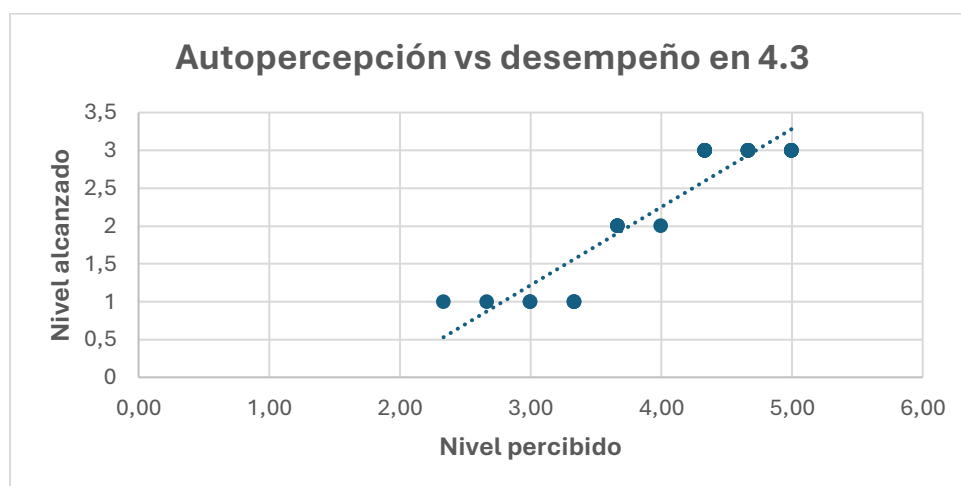


Figura 19. Relación entre autopercepción y el desempeño en la competencia 4.3.

El gráfico de dispersión evidencia una correlación positiva fuerte, con un coeficiente $R = 0,80$ y un $R^2 = 0,64$, lo que indica que aproximadamente un 64 % de la variabilidad del desempeño real puede explicarse por la autopercepción inicial. Estos resultados reflejan una consistencia notable entre la percepción de competencia y la ejecución práctica, sugiriendo que quienes se consideran capaces de mantener hábitos digitales saludables tienden efectivamente a demostrar un buen desempeño en las tareas asociadas.

La tendencia ascendente del gráfico confirma esta relación directa, mostrando que los participantes con una mayor autopercepción obtienen niveles de logro más altos en la evaluación. No obstante, se observa cierta dispersión entre los casos individuales, lo que puede atribuirse a la naturaleza multidimensional de esta competencia, que combina aspectos conductuales, actitudinales y de conciencia personal.

En conjunto, la correlación observada respalda la capacidad del entorno Ladico para evaluar esta competencia de forma coherente con el marco DigComp 2.2, aportando evidencia de validez también en los ámbitos vinculados al bienestar y la sostenibilidad del uso tecnológico.

4.4.5 COMPETENCIA 4.4 – PROTECCIÓN MEDIOAMBIENTAL

La Figura 20 muestra la relación entre la autopercepción declarada por los participantes y el nivel real de desempeño alcanzado en la competencia 4.4. Esta competencia aborda la capacidad para adoptar comportamientos sostenibles en el uso de las tecnologías digitales, como la gestión responsable de los dispositivos, el ahorro energético, la reducción del impacto ambiental y el uso eficiente de los recursos tecnológicos.

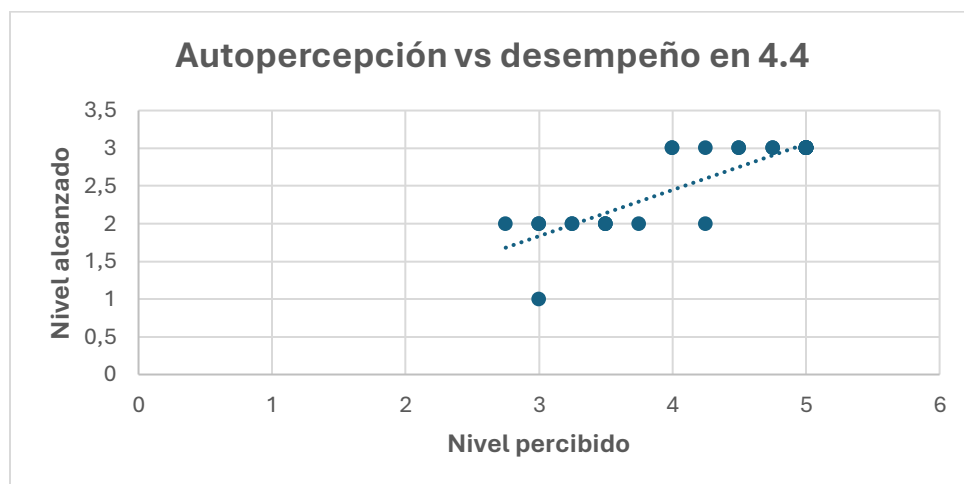


Figura 20. Relación entre autopercepción y el desempeño en la competencia 4.4.

El gráfico de dispersión evidencia una correlación positiva muy fuerte, con un coeficiente $R = 0,87$ y un $R^2 = 0,75$, lo que significa que el 75 % de la variabilidad del desempeño real puede explicarse por la autopercepción inicial. Estos valores representan la mayor coherencia observada entre las cuatro competencias del área de Seguridad, evidenciando que los participantes que se perciben con un mayor nivel de conciencia ambiental y digital tienden a demostrar un desempeño igualmente alto en las actividades prácticas. La línea de tendencia ascendente refuerza esta relación directa y consistente, indicando que la autopercepción en esta competencia se alinea fuertemente con la conducta observada en la plataforma. Esto sugiere que las prácticas vinculadas a la sostenibilidad digital y la eficiencia energética son bien comprendidas y aplicadas de manera consciente por los usuarios evaluados.

En conjunto, los resultados de esta competencia reflejan que Ladico logra evaluar de manera efectiva la dimensión ambiental de la seguridad digital, permitiendo identificar niveles diferenciados de desempeño y consolidando la validez del entorno como herramienta de medición integral dentro del marco DigComp 2.2.

En conclusión, los resultados del análisis correlacional entre la autopercepción y el desempeño real evidencian una coherencia sólida y consistente en las cuatro competencias del área de Seguridad del marco DigComp 2.2. Los valores de correlación obtenidos reflejan que los participantes que se perciben con un mayor dominio en materia de seguridad digital tienden, efectivamente, a alcanzar mejores niveles de desempeño en la plataforma Ladico. Esta correspondencia indica que el entorno es capaz de distinguir con precisión los distintos grados de competencia, mostrando una relación directa entre la percepción subjetiva y la evidencia objetiva de desempeño.

Las correlaciones más altas se observaron en las competencias 4.4 (Protección del entorno) y 4.2 (Protección de datos personales y privacidad), donde la coincidencia entre percepción y desempeño fue particularmente fuerte. Por su parte, las competencias 4.1 (Protección de

dispositivos) y 4.3 (Protección de la salud y el bienestar) también presentaron relaciones positivas elevadas, lo que demuestra la consistencia general del modelo evaluativo en todos los ámbitos de la seguridad digital.

Estos hallazgos permiten concluir que la plataforma Ladico constituye un instrumento válido y fiable para la evaluación de competencias digitales, al generar resultados coherentes con las autoevaluaciones de los usuarios y alineados con la estructura y los descriptores del marco DigComp 2.2. De este modo, se confirma la validez del entorno como sistema de medición integral, capaz de reflejar con objetividad tanto el nivel percibido como el nivel real de competencia en seguridad digital.

Los resultados obtenidos también tienen implicancias prácticas relevantes para instituciones educativas y organismos de formación. La alta correlación entre percepción y desempeño valida a Ladico como una herramienta confiable para evaluar competencias digitales de seguridad de manera objetiva, escalable y automatizada. Esto permite reemplazar o complementar los tradicionales instrumentos de autoevaluación con evaluaciones basadas en evidencia, más allá de la percepción del usuario, facilitando diagnósticos más certeros, planes de formación personalizados y decisiones fundamentadas en políticas públicas sobre alfabetización digital. Asimismo, su capacidad adaptativa lo hace pertinente y aplicable a una amplia variedad de contextos educativos y poblaciones, aportando un valor concreto a los procesos de enseñanza, aprendizaje y certificación de competencias digitales.

CAPÍTULO 5: CONCLUSIONES

El presente trabajo tuvo como propósito diseñar, implementar y validar un entorno de evaluación automatizada denominado Ladico, orientado a medir el nivel real de competencia digital en el área de Seguridad, según los lineamientos del marco europeo DigComp 2.2. Este desarrollo surgió como respuesta a la necesidad de contar con instrumentos objetivos, contextualizados y confiables que permitan diagnosticar las habilidades digitales basadas en desempeño, superando las limitaciones de las evaluaciones de autopercepción predominantes en América Latina.

La propuesta tecnológica consistió en el desarrollo del entorno Ladico, una plataforma digital que permite evaluar la competencia en seguridad a través de actividades interactivas, simulaciones y un banco de preguntas construido mediante prompts predefinidos, los cuales generan ítems adaptados a distintos niveles de dominio: básico, intermedio y avanzado. Este enfoque posibilita que la evaluación sea dinámica, contextual y escalable, manteniendo la coherencia con los principios de equidad, inclusión y pertinencia cultural.

El proceso de validación empírica demostró que el entorno Ladico es capaz de medir de manera fiable, objetiva y contextualizada el nivel de competencia digital de los usuarios. Los resultados evidenciaron correlaciones positivas entre la autopercepción y el desempeño real, confirmando la validez del instrumento y su potencial como herramienta de diagnóstico educativo y formativo. Asimismo, se observó un impacto favorable en la comprensión y aplicación de prácticas seguras en línea por parte de los participantes.

En síntesis, este estudio integró dimensiones teóricas, tecnológicas y metodológicas para construir una propuesta innovadora que contribuye al fortalecimiento de la competencia digital en el ámbito de la seguridad. El entorno Ladico representa un avance significativo en la evaluación basada en desempeño, constituyendo un modelo replicable para otros contextos y áreas del marco DigComp 2.2.

5.1 PRINCIPALES HALLAZGOS DEL PROCESO DE VALIDACIÓN

El proceso de validación del entorno Ladico permitió obtener resultados relevantes tanto en el plano técnico como en el pedagógico y metodológico, confirmando la pertinencia del modelo de evaluación propuesto para medir la competencia digital en el área de Seguridad. La validación se realizó mediante pruebas piloto con usuarios reales, aplicando instrumentos complementarios que evaluaron tanto la autopercepción de las habilidades digitales como el desempeño efectivo dentro del entorno.

En primer lugar, los resultados evidenciaron una correlación positiva entre la autopercepción y el desempeño real, aunque con diferencias significativas en determinados indicadores. Esto permitió constatar que muchos usuarios tienden a sobrestimar sus habilidades en materia de protección de datos personales, uso de contraseñas seguras y gestión de la privacidad en línea. Este hallazgo refuerza la necesidad de utilizar

instrumentos basados en desempeño, capaces de revelar las brechas reales entre lo que las personas creen saber y lo que efectivamente demuestran en la práctica.

En el plano técnico, se comprobó que el entorno Ladico presenta estabilidad operativa, escalabilidad y facilidad de uso, características clave para su futura implementación masiva. La interfaz resultó intuitiva para los participantes, lo que facilitó el desarrollo de las actividades sin requerir asistencia externa. Además, la estructura modular del sistema permite incorporar nuevas competencias o niveles de dificultad sin alterar la arquitectura base.

Desde una perspectiva pedagógica, los hallazgos mostraron que los usuarios lograron mayor conciencia sobre la importancia de las prácticas seguras en entornos digitales después de realizar la evaluación. Las simulaciones y actividades interactivas fueron percibidas como más representativas de situaciones reales que los cuestionarios tradicionales, lo que aumentó la motivación y la autenticidad de las respuestas.

Finalmente, la validación evidenció que Ladico puede constituirse en una herramienta útil para instituciones educativas, programas de formación y organismos públicos, ya que permite obtener datos objetivos sobre el nivel de competencia digital en seguridad de distintos grupos poblacionales. Estos resultados sientan las bases para escalar la plataforma y adaptar su uso a contextos educativos, laborales y ciudadanos, contribuyendo al fortalecimiento de una cultura digital segura y responsable.

5.2 EVALUACIÓN DEL CUMPLIMIENTO DE LOS OBJETIVOS PLANTEADOS

El desarrollo de esta investigación permitió cumplir satisfactoriamente los objetivos formulados, tanto en el ámbito general como en los específicos, evidenciando la coherencia entre la fundamentación teórica, el diseño metodológico y los resultados obtenidos durante la validación del entorno Ladico.

En cuanto al **objetivo general**, se logró **diseñar e implementar un entorno de evaluación automatizada basado en el marco DigComp 2.2**, enfocado en el área de Seguridad, que mide de manera objetiva, contextualizada y fiable el nivel de competencia digital de los usuarios. El entorno demostró su eficacia al ofrecer una experiencia de evaluación dinámica, con tareas auténticas y resultados cuantificables, permitiendo obtener diagnósticos precisos del nivel de desempeño.

Respecto a los **objetivos específicos**, los resultados se pueden sintetizar del siguiente modo:

- **Análisis de marcos internacionales:** se efectuó una revisión exhaustiva de los principales referentes conceptuales de competencia digital —entre ellos DigComp 2.2, ICILS (IEA, 2023) y PIAAC (OECD, 2024)—, identificando su aplicabilidad al contexto latinoamericano y sus limitaciones en cuanto a medición de desempeño. Este análisis permitió definir criterios de evaluación coherentes y transferibles al diseño del entorno.

- **Diseño de la arquitectura técnica y funcional:** se construyó una arquitectura modular, segura y escalable, que permite incorporar distintas áreas de competencia y niveles de dificultad. La interfaz fue validada con usuarios reales, quienes destacaron su facilidad de uso, estabilidad y claridad en las instrucciones, confirmando su pertinencia técnica y pedagógica.
- **Banco de preguntas generado mediante *prompts* predefinidos:** se logró estructurar un banco de ítems adaptativo, alineado a los descriptores del área de seguridad del DigComp 2.2, que permite ajustar las preguntas según el nivel y contexto del usuario. Este enfoque asegura la validez de contenido y la posibilidad de actualización continua sin alterar la estructura del sistema.
- **Validación del instrumento:** la aplicación piloto con usuarios permitió comprobar la fiabilidad del entorno y su capacidad para distinguir distintos niveles de dominio. Los resultados mostraron correlaciones positivas entre autopercepción y desempeño real, evidenciando la validez de constructo del instrumento y su capacidad para medir la competencia en seguridad de forma objetiva.
- **Evaluación de correlación percepción–desempeño:** el análisis estadístico confirmó que, aunque los usuarios suelen sobreestimar sus habilidades de seguridad digital, existe una tendencia general coherente entre lo que declaran y lo que efectivamente logran en las tareas prácticas. Este hallazgo refuerza la pertinencia de combinar mediciones de percepción con evaluaciones de desempeño.

En conjunto, estos resultados demuestran que los objetivos planteados fueron alcanzados plenamente, cumpliendo la finalidad central de esta memoria: disponer de una herramienta tecnológica validada que contribuya a la evaluación objetiva de la competencia digital en el área de seguridad, con proyección de aplicación en contextos educativos, laborales y ciudadanos.

5.3 APORTES METODOLÓGICOS Y TECNOLÓGICOS DEL ENTORNO LADICO

El desarrollo del entorno Ladico representa un avance significativo tanto desde el punto de vista metodológico como tecnológico en la evaluación de la competencia digital, particularmente en el área de Seguridad. La propuesta integra principios de evaluación basada en desempeño, usabilidad, inteligencia adaptativa y contextualización cultural, aportando un modelo replicable y escalable para futuras aplicaciones en otras áreas del marco DigComp 2.2.

Desde la perspectiva metodológica, Ladico aporta una nueva forma de comprender y medir la competencia digital en seguridad, centrada en la observación de la acción y la evidencia del desempeño más que en la autopercepción declarada. Este enfoque permite valorar cómo las personas aplican sus conocimientos y criterios frente a situaciones reales o simuladas que involucren la protección de datos, la privacidad, el uso seguro de dispositivos y la gestión ética de la información.

A diferencia de los instrumentos tradicionales, Ladico incorpora actividades auténticas que requieren la toma de decisiones, el razonamiento ético y la aplicación práctica de estrategias de seguridad digital, lo que incrementa la validez y profundidad del diagnóstico.

Otro aporte metodológico relevante es la adaptación de los descriptores del DigComp 2.2 al contexto latinoamericano, lo cual permitió traducir estándares europeos en tareas y ejemplos pertinentes a las realidades tecnológicas y socioculturales de los usuarios de la región. Esta adecuación favorece una medición más inclusiva y significativa, considerando factores de acceso, experiencia previa y brecha digital.

En el ámbito tecnológico, Ladico introduce innovaciones orientadas a la automatización y personalización del proceso de evaluación. El entorno combina un banco de preguntas estructurado a partir de prompts predefinidos con una arquitectura escalable, que posibilita la generación de ítems variados, coherentes con los niveles de dominio (básico, intermedio y avanzado). Esto permite mantener la calidad y diversidad de las evaluaciones sin requerir una intervención manual constante.

Asimismo, la plataforma fue diseñada bajo criterios de seguridad, estabilidad y accesibilidad, garantizando la protección de la información de los usuarios y la integridad de los resultados. La implementación modular de la arquitectura facilita futuras ampliaciones, permitiendo incorporar nuevas áreas o adaptar las existentes a distintos públicos, como docentes, estudiantes o trabajadores.

Finalmente, Ladico contribuye al fortalecimiento de la investigación aplicada en evaluación de competencias digitales al demostrar que es posible integrar herramientas digitales, bases de datos estructuradas y análisis estadístico en un sistema coherente, eficiente y pedagógicamente válido. Su diseño proporciona una base sólida para futuras investigaciones que busquen explorar el impacto de la alfabetización en seguridad digital sobre la autonomía tecnológica, la ciudadanía digital y la protección de datos personales.

En síntesis, el entorno Ladico se consolida como una propuesta metodológica innovadora y tecnológicamente robusta, que combina la precisión de la medición automatizada con la pertinencia pedagógica del aprendizaje contextualizado, aportando una alternativa real para evaluar la competencia digital en seguridad de forma fiable, ética y escalable. En el ámbito educativo, Ladico puede integrarse como herramienta diagnóstica en programas de formación docente, planes de mejora institucional o procesos de acreditación digital, permitiendo identificar con mayor detalle las brechas específicas de competencia y orientar estrategias formativas más efectivas. Desde una perspectiva institucional, el entorno ofrece un soporte técnico y metodológico para fortalecer los procesos de enseñanza y evaluación en competencias digitales, al proporcionar información basada en evidencia y resultados estandarizados. Finalmente, en el ámbito de las políticas públicas, los datos generados por Ladico pueden contribuir al diseño de estrategias nacionales de alfabetización digital, diferenciadas por contexto socioeconómico, género o edad, promoviendo decisiones más informadas y equitativas en materia de desarrollo digital y ciudadanía digital responsable.

5.4 LIMITACIONES DEL ESTUDIO

Si bien los resultados obtenidos en la validación del entorno Ladico fueron positivos y evidencian su potencial como herramienta de evaluación objetiva de la competencia digital en el área de Seguridad, es necesario reconocer una serie de limitaciones que condicionaron el alcance y la generalización de los hallazgos de esta investigación.

En primer lugar, una limitación relevante corresponde al tamaño y composición de la muestra utilizada en la validación empírica. Si bien permitió obtener datos consistentes y significativos, su extensión fue limitada a un grupo acotado de usuarios, por lo que los resultados no pueden generalizarse a toda la población. Será necesario ampliar el número de participantes y diversificar los perfiles (por edad, nivel educativo y contexto laboral) para fortalecer la validez externa del instrumento.

En segundo lugar, se identifican restricciones técnicas propias del desarrollo del entorno. Aunque Ladico mostró estabilidad y funcionalidad durante las pruebas, su rendimiento puede variar dependiendo de la capacidad del servidor, la conexión a internet o las características de los dispositivos utilizados por los participantes. Estos factores externos pueden incidir en la experiencia de uso y en la percepción de la dificultad de las actividades.

Otra limitación se relaciona con el alcance temático del estudio, centrado exclusivamente en el área 4 del marco DigComp 2.2 (Seguridad). Si bien esta focalización permitió profundizar en la validez de los ítems y en la pertinencia de las actividades interactivas, el modelo no aborda las otras áreas del marco, como la información, la comunicación o la creación de contenido digital. Por tanto, futuras investigaciones deberán ampliar la cobertura del entorno para abarcar de forma integral las cinco áreas de competencia digital. Asimismo, la dependencia del banco de preguntas basado en prompts predefinidos implica que la calidad de la evaluación depende de la precisión y diversidad de dichos prompts. Aunque el sistema permite generar múltiples variantes de preguntas, la riqueza de los ítems sigue sujeta a la calidad de los diseños iniciales y a la constante revisión pedagógica del banco de contenidos.

Desde el punto de vista metodológico, la investigación se concentró en la fase de validación inicial, sin incluir un seguimiento longitudinal que permitiera observar la evolución de la competencia digital de los usuarios a lo largo del tiempo. La incorporación de mediciones repetidas o comparativas entre distintos grupos de usuarios podría aportar información adicional sobre la eficacia del entorno en contextos formativos.

Finalmente, debe considerarse que la dimensión ética y de privacidad en la recolección de datos constituye un aspecto sensible y prioritario. Si bien se aplicaron medidas de resguardo para proteger la información de los participantes, futuras versiones del entorno deberán integrar mecanismos más avanzados de anonimización y control de acceso para cumplir con estándares internacionales de protección de datos personales.

En síntesis, estas limitaciones no invalidan los resultados alcanzados, sino que establecen los márgenes y oportunidades de mejora para el perfeccionamiento de Ladico como

herramienta de evaluación digital. Reconocerlas permite proyectar nuevas líneas de trabajo orientadas a consolidar su fiabilidad, escalabilidad y aplicabilidad en distintos contextos educativos y sociales.

5.5 RECOMENDACIONES Y PROYECCIONES FUTURAS

A partir de los resultados obtenidos y de las limitaciones identificadas, se formulan una serie de recomendaciones y proyecciones orientadas a fortalecer la continuidad del proyecto Ladico y su aplicación en contextos educativos, laborales y ciudadanos.

En primer lugar, se recomienda ampliar la muestra de validación para incluir participantes de diferentes edades, niveles educativos, ocupaciones y contextos socioculturales. Esto permitirá obtener resultados más representativos y establecer comparaciones entre grupos, favoreciendo la generalización de los hallazgos y la identificación de patrones de competencia digital en materia de seguridad.

En segundo lugar, se sugiere expandir el alcance del entorno hacia las demás áreas del marco DigComp 2.2, de modo que Ladico evolucione hacia una plataforma integral de evaluación de competencias digitales. La ampliación a las áreas de información, comunicación, creación de contenido y resolución de problemas permitiría ofrecer un diagnóstico completo del perfil digital del usuario.

Desde el punto de vista técnico, se recomienda fortalecer la infraestructura y el almacenamiento del sistema, garantizando mayor estabilidad, capacidad de respuesta y escalabilidad. Asimismo, la incorporación de mecanismos de analítica avanzada y visualización de resultados podría facilitar el seguimiento del progreso de los usuarios y generar reportes automáticos útiles para instituciones educativas o entidades formadoras. En cuanto al componente evaluativo, se plantea continuar el perfeccionamiento del banco de preguntas basado en prompts, incrementando la variedad, el nivel de complejidad y la contextualización cultural de los ítems. Para ello, sería conveniente conformar un comité interdisciplinario que integre especialistas en educación digital, ciberseguridad, lingüística y desarrollo de software, garantizando la pertinencia y calidad de los contenidos generados.

Desde una perspectiva pedagógica, se recomienda incorporar el entorno Ladico como herramienta formativa, no solo evaluativa, integrando retroalimentaciones automáticas, recursos de aprendizaje personalizados y rutas de mejora según el nivel alcanzado. Esto permitiría que los usuarios no solo conozcan su nivel de competencia, sino que también desarrollen habilidades para fortalecer su seguridad digital de manera autónoma. Asimismo, se proyecta la posibilidad de establecer alianzas con instituciones educativas, organismos públicos y empresas tecnológicas que promuevan la alfabetización en seguridad digital a nivel regional. La implementación de Ladico en programas de formación docente, capacitación laboral o ciudadanía digital podría contribuir a reducir la brecha de habilidades y fomentar una cultura tecnológica más segura y consciente.

Finalmente, se sugiere dar continuidad a la línea de investigación mediante estudios longitudinales que evalúen el impacto de la herramienta en la evolución de las

competencias digitales de los usuarios a lo largo del tiempo. Esta proyección permitiría medir no solo la efectividad inmediata del entorno, sino también su capacidad para generar aprendizajes sostenibles y transferibles.

En conclusión, las proyecciones de esta investigación apuntan a consolidar Ladico como un referente en la evaluación y fortalecimiento de las competencias digitales en seguridad, articulando innovación tecnológica, validez pedagógica y compromiso ético con la protección de los datos y la privacidad de los usuarios. Su desarrollo futuro permitirá avanzar hacia una sociedad más informada, crítica y resiliente frente a los desafíos de la era digital.

REFERENCIAS BIBLIOGRÁFICAS

[Aesaert et al., 2017] Aesaert Koen, Voogt Joke, Kuiper Els, van Braak Johan (2017) Accuracy and bias of ICT self-efficacy: An empirical study into students' over- and underestimation of their ICT competences, *Computers in Human Behavior*, Volume 75, Pages 92-102, ISSN 0747-5632, <https://doi.org/10.1016/j.chb.2017.05.010>

[Agencia de Calidad de Educación, 2024] Agencia de Calidad de Educación (2024). Estudio internacional de alfabetización computacional y manejo de información (icils) 2023, https://s3.us-east-1.amazonaws.com/archivos-web.agenciaeducacion.cl/archivos_web/Entrega+de+resultados+ICILS+2023.pdf

[Blanc et al., 2025] Blanc, S., Conchado, A., Benlloch-Dualde, J. V., Monteiro, A., & Grindei, L. (2025). Digital competence development in schools: A study on the association of problem-solving with autonomy and digital attitudes. *International Journal of STEM Education*, 12(1), Article 13. <https://doi.org/10.1186/s40594-025-00534-6>

[Cepal, 2025] CEPAL. (2025). Education and the Development of Digital Competences in Latin America and the Caribbean. United Nations Economic Commission for Latin America and the Caribbean.

[González-Martínez et al., 2018] González-Martínez, J., Estebanell, M., & Rostan, C. (2018). Digital competence assessment in higher education: The INCOTIC-HE instrument. *RED. Revista de Educación a Distancia*, 56, 1–29. <https://doi.org/10.6018/red/56/6>

[IEA, 2023] International Computer and Information Literacy Study. (2023) : Assessment Framework, Editors: Julian Fraillon, Mojca Rožman, Springer Cham, <https://doi.org/10.1007/978-3-031-61194-0>

[Martín-Párraga et al., 2022] MartínPárraga, L., LlorenteCejudo, C., & CaberoAlmenara, J. (2022). *Análisis de las competencias digitales docentes desde los marcos e instrumentos de evaluación*. *International Journal of Educational Research and Innovation*, 18, 62–79. <https://doi.org/10.46661/ijeri.7444>

[Mehrvarz et al., 2021] Mehrvarz, M., Heidari, E., Farrokhnia, M., Noroozi, O. (2021) The mediating role of digital informal learning in the relationship between students' digital competence and their academic performance, *Computers & Education*, 167, 104184. <https://doi.org/10.1016/j.compedu.2021.104184>

[Mineduc, 2025] Centro de Innovación del Ministerio de Educación (MINEDUC). (2025, marzo). Potencia el aprendizaje: Preguntas para la reflexión y práctica de la inteligencia artificial generativa en contextos educativos. Ministerio de Educación, Chile. Disponible en <https://ciudadaniadigital.mineduc.cl/wp-content/uploads/2025/03/Potencia-el-aprendizaje-IA-en-educacion.pdf>

[OECD, 2024] OECD. (2024). Do Adults Have the Skills They Need to Thrive in a Changing World? Survey of Adult Skills 2023, OECD Skills Studies, OECD Publishing, Paris, <https://doi.org/10.1787/b263dc5d-en>

[OECD, 2024] OECD. (2024). Evaluación de Competencias de la Población Adulta 2023: Chile, Organización para la Cooperación y el Desarrollo Económicos. https://www.oecd.org/es/publications/evaluacion-de-competencias-de-la-poblacion-adulta-2023_f79f56e3-es/chile_dbf64059-es.html

[Rioseco-Pais et al., 2023] Rioseco-Pais, C., Fernández-Mellizo, M., & Muñoz-Carril, P. C. (2023). Assessing digital competence: A systematic review of instruments and frameworks in higher education. *Education and Information Technologies*, 28(9), 9849–9880. <https://doi.org/10.1007/s10639-023-11634-3>

[Rioseco-Pais et al., 2023] Rioseco Pais, M., Silva Quiroz, J., & Carrasco-Manríquez, C. (2023). Development of Digital Competences in Students of a Public State-Owned Chilean University Considering the Safety Area. *Education Sciences*, 13(7), Article 710. <https://doi.org/10.3390/educsci13070710>

[Rioseco-Pais et al., 2024] Rioseco-Pais, M., Silva-Quiroz, J., & Vargas-Vitoria, R. (2024). Digital Competences and Years of Access to Technologies Among Chilean University Students: An Analysis Based on the DIGCOMP Framework. *Sustainability*, 16(22), Article 9876. <https://doi.org/10.3390/su16229876>

[Sillat et al., 2021] Sillat, H., Tammets, K., & Laanpere, M. (2021). Measuring digital competence: The case of Estonia. *Education and Information Technologies*, 26(1), 121–138.

[Skantz, 2022] Skantz Åberg, E., Hatakka, M., & Grönlund, Å. (2022). *Digital competence and online safety: Self-perceptions versus actual behaviors*. *Computers & Education*, 179, 104413. <https://doi.org/10.1016/j.compedu.2021.104413>

[Stemberger et al., 2021] Stemberger, T., & Cotic, M. (2021). Assessing students' digital skills: Self-perception vs. performance. *Journal of Information Technology Education: Research*, 20(1), 1–15.

[Tzafilkou et al., 2022] Tzafilkou, K., Magoulas, G. D., & Papanastasiou, G. (2022). Validation of the student digital competence scale (SDiCoS) using confirmatory factor analysis. *International Journal of Educational Technology in Higher Education*, 19(1), 30.7 ...

[Tzafilkou et al., 2022] Tzafilkou, K., Perifanou, M. & Economides, A.A. (2022) Development and validation of students' digital competence scale (SDiCoS). *Int J Educ Technol High Educ* 19, 30 . <https://doi.org/10.1186/s41239-022-00330-0>

[Tzafilkou et al., 2022] Tzafilkou, K., Perifanou, M., & Economides, A. A. (2022). Exploring the relationship between digital competence and online safety: A structural equation modeling approach. *Education and Information Technologies*, 27(8), 11221–11244. <https://doi.org/10.1007/s10639-022-11064-2>

[Usart-Rodríguez et al., 2021] Usart Rodríguez, Mireia; Lázaro Cantabrana, José Luis; Gisbert Cervera, Mercè (2021) VALIDATION OF A TOOL FOR SELF-EVALUATING TEACHER DIGITAL COMPETENCE, *Educación XX1*, vol. 24, no. 1, 2021, -June, pp. 353-373, DOI: <https://doi.org/10.5944/educXX1.27080>

[Vuorikari et al., 2022] Vuorikari, R., Kluzer, S. and Punie, Y., (2022) DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes, EUR 31006 EN, Publications Office of the European Union, Luxembourg, doi:10.2760/490274, JRC128415

[WEF, 2025] World Economic Forum. (2025). 7 principles on responsible AI use in education. World Economic Forum. <https://www.weforum.org/stories/2024/01/ai-guidance-school-responsible-use-in-education>

[Zhao, 2021] Zhao, Y., Pinto, M., & Escobar, C. (2021). *Digital competence and digital citizenship: A systematic review of the framework and implementation*. *Journal of e-Learning and Knowledge Society*, 17(3), 47–59.

[Chile, 1999] Ley N.º 19.628 sobre protección de la vida privada. Diario Oficial de la República de Chile, 28 de agosto de 1999. <https://www.bcn.cl/leychile/n?i=141599>

ANEXOS

ANEXO A

N°	Edad	Género	Carrera	Año de carrera	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
1	21	Masculino	ICI	4to año	3	5	3	4	3	2	4	5
2	22	Masculino	ICI	4to año	5	5	5	5	4	5	5	5
3	21	Femenino	ICI	4to año	5	5	2	3	4	5	4	5
4	23	Masculino	ICI	5to año	3	5	3	4	4	5	4	5
5	23	Masculino	ICI	> 5to año	4	5	1	2	4	4	3	5
6	23	Femenino	ICI	5to año	4	4	3	4	4	5	4	5
7	24	Masculino	ICI	> 5to año	5	5	5	5	5	5	5	5
8	23	Masculino	ICI	5to año	4	5	3	4	5	5	4	4
9	24	Masculino	ICI	> 5to año	5	5	5	5	5	5	5	5
10	23	Masculino	ICI	> 5to año	5	5	2	4	4	3	4	4
11	24	Masculino	ICI	> 5to año	4	4	5	5	4	5	4	5
12	24	Masculino	ICI	> 5to año	5	5	4	5	5	5	5	5
13	24	Masculino	ICI	4to año	4	5	3	5	4	4	4	5
14	23	Masculino	ICI	> 5to año	5	3	3	5	3	4	5	5
15	24	Masculino	ICI	> 5to año	5	5	5	5	5	5	5	5
16	23	Masculino	ICI	> 5to año	4	4	3	4	4	4	3	4
17	22	Masculino	ICI	4to año	4	5	4	4	3	4	4	5
18	22	Masculino	ICI	5to año	4	4	3	3	3	5	5	5
19	23	Masculino	ICI	5to año	3	4	3	5	4	4	5	5
20	23	Masculino	ICI	5to año	4	5	4	2	4	4	5	5
21	22	Masculino	ICI	5to año	5	5	4	3	5	5	5	3
22	23	Masculino	ICI	> 5to año	5	5	1	5	4	5	3	5
23	23	Masculino	ICI	> 5to año	5	5	2	5	4	5	4	5
24	24	Masculino	ICI	5to año	5	5	3	3	4	4	5	4
25	22	Masculino	ICI	4to año	5	3	4	2	4	4	4	5
26	24	Femenino	ICI	5to año	4	4	2	4	4	4	4	4
27	21	Masculino	ICI	4to año	3	5	3	3	2	5	4	5
28	23	Masculino	ICI	> 5to año	3	3	2	3	5	4	4	5
29	24	Masculino	ICI	> 5to año	2	5	3	2	5	5	5	5
30	24	Masculino	ICI	> 5to año	4	5	2	4	4	5	4	5

N°	Edad	Género	Carrera	Año de carrera	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16
1	21	Masculino	ICI	4to año	2	5	5	5	5	5	5	5
2	22	Masculino	ICI	4to año	5	4	5	5	5	5	4	3
3	21	Femenino	ICI	4to año	2	3	3	3	3	4	4	3
4	23	Masculino	ICI	5to año	5	5	5	4	5	5	5	5
5	23	Masculino	ICI	> 5to año	4	5	5	5	5	4	5	2
6	23	Femenino	ICI	5to año	2	4	4	1	2	4	2	4
7	24	Masculino	ICI	> 5to año	2	5	5	3	4	5	4	3
8	23	Masculino	ICI	5to año	5	5	5	5	5	5	5	5
9	24	Masculino	ICI	> 5to año	5	5	5	5	5	5	5	5
10	23	Masculino	ICI	> 5to año	5	5	5	3	5	5	5	5
11	24	Masculino	ICI	> 5to año	4	5	4	4	5	5	5	5
12	24	Masculino	ICI	> 5to año	4	5	5	5	4	5	5	5
13	24	Masculino	ICI	4to año	3	4	4	5	5	5	5	5
14	23	Masculino	ICI	> 5to año	5	4	5	4	5	5	5	5
15	24	Masculino	ICI	> 5to año	5	5	5	5	5	5	5	5
16	23	Masculino	ICI	> 5to año	4	3	2	2	3	4	3	2
17	22	Masculino	ICI	4to año	1	4	4	5	5	5	5	4
18	22	Masculino	ICI	5to año	1	3	3	5	4	3	3	3
19	23	Masculino	ICI	5to año	3	4	4	3	3	3	3	3
20	23	Masculino	ICI	5to año	5	4	5	5	3	5	5	5
21	22	Masculino	ICI	5to año	3	2	3	3	3	4	4	3
22	23	Masculino	ICI	> 5to año	2	5	4	5	5	4	5	4
23	23	Masculino	ICI	> 5to año	5	5	5	4	5	5	5	5
24	24	Masculino	ICI	5to año	5	4	2	4	4	3	3	3
25	22	Masculino	ICI	4to año	1	4	5	4	5	5	5	5
26	24	Femenino	ICI	5to año	1	4	4	4	3	5	2	1
27	21	Masculino	ICI	4to año	3	3	5	2	4	5	5	3
28	23	Masculino	ICI	> 5to año	3	3	4	4	3	4	3	4
29	24	Masculino	ICI	> 5to año	1	5	5	4	5	5	5	5
30	24	Masculino	ICI	> 5to año	2	3	4	3	4	3	4	4

ANEXO B

N°	Nivel 4.1	Nivel 4.2	Nivel 4.3	Nivel 4.4	Competencias falladas	Nivel actual
1	2	2	3	3	4.1 A, 4.2 A	2
2	3	3	3	3	-	3
3	2	2	1	2	4.3 I	1
4	2	3	3	3	4.1 A	2
5	2	2	3	3	4.1 A, 4.2 A	2
6	2	2	1	2	4.3 I	1
7	3	3	3	3	-	3
8	3	3	3	3	-	3
9	3	3	3	3	-	3
10	2	2	3	3	4.1 A, 4.2 A	2
11	3	3	3	3	-	3
12	3	3	3	3	-	3
13	3	2	3	3	4.2 A	2
14	2	3	3	3	4.1 A	2
15	3	3	3	3	-	3
16	2	2	1	2	4.3 I	1
17	3	2	3	3	4.2 A	2
18	1	2	2	2	4.1 I	1
19	2	2	2	1	4.4 I	1
20	2	3	3	3	4.1 A	2
21	2	2	1	2	4.3 I	1
22	3	2	3	3	4.2 A	2
23	3	3	3	3	-	3
24	2	2	1	2	4.3 I	1
25	2	2	3	3	4.1 A, 4.2 A	2
26	1	2	2	2	4.1 I	1
27	2	2	1	2	4.3 I	1
28	1	2	2	2	4.1 I	1
29	2	2	3	3	4.1 A, 4.2 A	2
30	2	2	1	2	4.3 I	1