

UNIVERSIDAD PERUANA UNIÓN
FACULTAD DE INGENIERIA Y ARQUITECTURA
Escuela Profesional de Ingeniería de Sistemas



**Evaluación de la calidad de plataformas e-learning: Un modelo
basado en las normas ISO/IEC 25000**

Tesis para obtener el Título Profesional de Ingeniero de Sistemas

Autor:

Jose Luis Cardenas Garcia
Robinson Genaro Espinal Asenjo
Jesus Alberto Abanto Cruz

Asesor:

MG. Jose Bustamante Romero

Lima, Febrero 2026

DECLARACIÓN JURADA DE ORIGINALIDAD DE TESIS

Yo Jose Bustamante Romero docente de la Facultad de Ingeniería y Arquitectura, Escuela Profesional de Ingeniería de Sistemas, de la Universidad Peruana Unión.

DECLARO:

Que la presente investigación titulada: **“EVALUACION DE LA CALIDAD DE PLATAFORMAS E-LEARNING: UN MODELO BASADO EN LAS NORMAS ISO/IEC 25000”** del (los) autor (autores) Jose Luis Cardenas Garcia, Robinson Genaro Espinal Asenjo, Jesus Alberto Abanto Cruz tiene un índice de similitud de 8 % verificable en el informe del programa Turnitin, y fue realizada en la Universidad Peruana Unión bajo mi dirección.

En tal sentido asumo la responsabilidad que corresponde ante cualquier falsedad u omisión de los documentos como de la información aportada, firmo la presente declaración en la ciudad de lima a los 15 días del mes de diciembre del año 2025.



MG Jose Bustamante Romero

ACTA DE SUSTENTACIÓN DE TESIS

En Lima, Naña, Villa Unión, a 26 día(s) del mes de febrero del año 2026, siendo las 9:00 horas, se reunieron los miembros del jurado en la Universidad Peruana Unión Campus Lima, bajo la dirección del (de la) presidente(a):

Mg. Immer Elías Cuellar Rodríguez, el (la) secretario(a): Mg. Lennin Henry Centurión Julca y los demás miembros: Mg. Nemias Saboya Ríos Mg. Daniel Levano Rodríguez y el (la) asesor(a) Mg. Jose Bustamante Romero

con el propósito de administrar el acto académico de sustentación de la tesis titulado: "Evaluación de la Calidad de Plataformas e-learning: Un modelo basado en las normas ISO/IEC 25000"

del(los) bachiller(es): a) Jesús Alberto Abanto Cruz b) Jose Luis Cardenas Garcia c) Robinson Genaro Espinal Asenjo

conducente a la obtención del título profesional de: Ingeniero de Sistemas

El Presidente inició el acto académico de sustentación invitando al (a la) / a (los) (las) candidato(a)s hacer uso del tiempo determinado para su exposición. Concluida la exposición, el Presidente invitó a los demás miembros del jurado a efectuar las preguntas, y aclaraciones pertinentes, las cuales fueron absueltas por al (a la) / a (los) (las) candidato(a)s. Luego, se produjo un receso para las deliberaciones y la emisión del dictamen del jurado.

Posteriormente, el jurado procedió a dejar constancia escrita sobre la evaluación en la presente acta, con el dictamen siguiente:

Bachiller (a): Jesús Alberto Abanto Cruz

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literar	Cualitativa	
Aprobado	17	B+	Muy bueno	Sobresaliente

Bachiller (b): Jose Luis Cardenas Garcia

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literar	Cualitativa	
Aprobado	17	B+	Muy bueno	Sobresaliente

Bachiller (c): Robinson Genaro Espinal Asenjo

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literar	Cualitativa	
Aprobado	17	B+	Muy bueno	Sobresaliente

(*) Ver parte posterior

Finalmente, el Presidente del jurado invitó al (a la) / a (los) (las) candidato(a)s a ponerse de pie, para recibir la evaluación final y concluir el acto académico de sustentación procediéndose a registrar las firmas respectivas.

Presidente/a
Asesor/a
Bachiller (a)
Miembro
Miembro
Bachiller (b)
Bachiller (c)
Secretario/a

Esta sustentación fue realizada de manera virtual u online sincrónica según conforme al Reglamento General de Grados y Títulos.

CONTENIDO

RESUMEN.....	5
ABSTRACT.....	5
1. INTRODUCCION	6
2. METODOLOGIA.....	8
2.1. Fase 1: Análisis de características funcionales en plataformas e-learning	9
2.2. Fase 2: Revisión de Normas Internacionales	9
2.3. Fase 3: Modelo de evaluación de la calidad en seguridad del software	11
2.4. Fase 4: Validación del modelo de evaluación de la calidad del software ..	14
2.5. Fase 5: Aplicación del modelo de evaluación de la calidad en seguridad del software	15
3. RESULTADOS.....	15
4. DISCUSIÓN	19
5. CONCLUSIÓN	20
6. REFERENCIAS	20

Evaluación de la calidad de las plataformas E-learning: un modelo basado en las normas ISO/IEC 25000

Evaluation of the Quality of e-learning Platforms: A model based on ISO/IEC 25000 standards

RESUMEN

El rápido crecimiento del e-learning puso de manifiesto las debilidades en la seguridad de las plataformas educativas digitales. En este contexto, se desarrolló, validó y aplicó un modelo de evaluación de la calidad de la seguridad del software de e-learning. El modelo se basa en las normas internacionales ISO/IEC 25010, 25023 y 25040, y considera cinco aspectos clave de seguridad: confidencialidad, integridad, no repudio, responsabilidad y autenticidad. Para su construcción, se elaboró un catálogo estructurado de métricas y una escala de aceptación, lo que facilitó la medición objetiva de cada aspecto. El instrumento se validó mediante el método Delphi, con la participación de expertos en evaluación de software, quienes confirmaron la coherencia y relevancia del modelo. Posteriormente, se aplicó en tres plataformas e-learning, en colaboración con evaluadores internos y externos, lo que permitió verificar su capacidad para diferenciar la implementación de medidas de seguridad entre sistemas. Los resultados mostraron que la confidencialidad alcanzó valores aceptables, superando el 70 % de media, mientras que la autenticidad fue el aspecto más crítico, con valores inferiores al 40 % en todas las plataformas. Los atributos de integridad, responsabilidad y no repudio fueron calificados como mínimamente aceptables, lo que indica una cobertura de control limitada. En resumen, el modelo propuesto constituye un método riguroso y replicable.

ABSTRACT

The accelerated growth of e-learning exposed weaknesses in the security of digital educational platforms. In this context, a software security quality assessment model for e-learning was developed, validated, and applied. The model is based on the international standards ISO/IEC 25010, 25023, and 25040, and considers five key security aspects: confidentiality, integrity, non-repudiation, responsibility, and authenticity. For its construction, a structured catalog of metrics and an acceptance scale were developed, facilitating the objective measurement of each aspect. The instrument was validated using the Delphi method, with the participation of software evaluation experts, who confirmed the model's coherence and relevance. Subsequently, it was applied in three e-learning platforms, in collaboration with internal and external evaluators, which enabled verification of its ability to differentiate the implementation of security measures across systems. The results showed that confidentiality reached acceptable values, exceeding 70% on average, while authenticity was the most critical aspect, with values below 40% on all platforms. The attributes of integrity, responsibility, and non-repudiation were

rated as only minimally acceptable, indicating limited coverage of control. In summary, the proposed model constitutes a rigorous and replicable tool to support strategic decisions, thereby contributing to the protection of sensitive information for students and teachers.

Palabras clave: E-learning, Seguridad, ISO/IEC 25010, ISO/IEC 25023, ISO/IEC 25040

Keywords: E-learning, Security, ISO/IEC 25010, ISO/IEC 25023, ISO/IEC 25040

1. INTRODUCCION

La crisis de la COVID-19, que comenzó a finales de 2019, trastocó la vida cotidiana, la economía y las interacciones sociales en todo el mundo [1]. Como parte de los esfuerzos para detener la propagación del virus, la mayoría de los gobiernos optaron por suspender temporalmente las instituciones educativas, priorizando la salud de los estudiantes, los profesores y el personal [2]. En este contexto, se produjo una aceleración en la adopción de nuevas tecnologías digitales en el ámbito educativo, y el e-learning alcanzó la madurez como principal medio de enseñanza [3]. Las entidades educativas adoptaron plataformas e-learning como Blackboard, Moodle y Google Classroom, además de plataformas de apoyo como Zoom y Microsoft Teams [4], [5]. Estas plataformas se han vuelto esenciales para la educación en línea, facilitando no solo el aprendizaje a distancia sino también la introducción de nuevas metodologías pedagógicas. Sin embargo, se han descubierto vulnerabilidades en las plataformas e-learning, lo que subraya la necesidad urgente de implementar estrategias de mitigación para hacer frente a los riesgos digitales [6], [7].

Las plataformas e-learning deben evaluarse en aspectos como la funcionalidad, la eficiencia, la usabilidad y la seguridad. [8], [9]. Para llevar a cabo esta evaluación, la familia de normas ISO/IEC 25000 proporciona un marco sólido que permite la medición objetiva de estas características, en particular la seguridad, a través de métricas estandarizadas [10]. Su correcta aplicación contribuye a proteger la información sensible, reducir los riesgos de ciberataques y fortalecer la reputación de las instituciones educativas. [11], [12].

En el contexto del rápido crecimiento del e-learning, han surgido importantes desafíos de seguridad. Muchas instituciones educativas aún carecen de un modelo claro y estandarizado para evaluar la calidad de la seguridad en las plataformas e-learning. Aunque existen estándares internacionales como ISO/IEC 25010, ISO/IEC 25023 e ISO/IEC 25040 [13], [14] Si bien ofrecen marcos para evaluar la calidad del software, su implementación específica en el contexto de la seguridad de la plataforma sigue siendo bastante limitada [15].

La falta de un marco adecuado para la evaluación de la seguridad ha generado vulnerabilidades y deficiencias, poniendo en grave riesgo la protección de la información sensible y la continuidad de los procesos educativos. Por lo

tanto, es esencial desarrollar un modelo de evaluación de la calidad de la seguridad específicamente adaptado a las plataformas e-learning, basado en la norma internacional ISO/IEC pertinente [16], [17]. Sin embargo, es fundamental tener en cuenta que los modelos de calidad de software, como ISO/IEC 25010, McCall, Boehm y Dromey, son más generales y no abordan específicamente las vulnerabilidades de seguridad típicas de los entornos educativos en línea [18].

Varios estudios han investigado la importancia de la seguridad del software, y los investigadores [19] enfatizar la necesidad de incorporar la seguridad desde las primeras etapas del desarrollo, utilizando la norma internacional ISO/IEC 25010. Por su parte [12], demuestra que la aplicación de estos estándares en plataformas e-learning mejora la seguridad, aunque enfrentan desafíos en términos de integridad. Otros investigadores, como [20], Han abordado la brecha entre la enseñanza académica y las demandas industriales en materia de seguridad, proponiendo un enfoque de madurez que integra la seguridad desde la fase de diseño. [21] Analizaron la seguridad del almacenamiento de datos personales en los sistemas de gestión del aprendizaje, identificando vulnerabilidades significativas y proponiendo soluciones para mejorar la confidencialidad y la seguridad de los datos. Por otro lado [22], Se centró en el uso de tecnologías emergentes para mejorar la autenticidad de los estudiantes en las evaluaciones en línea, abordando aspectos de seguridad de la autenticación y previniendo el uso compartido de cuentas.

A nivel mundial, el sector educativo ha sido un objetivo ideal para los ciberdelincuentes. Según un informe de SOCRadar, en 2024, varias plataformas e-learning experimentaron un aumento significativo de ciberataques, incluidos ataques de ransomware, filtraciones de datos y ataques de phishing, que afectaron a instituciones educativas de todo el mundo, incluidas escuelas y universidades. [23]. Un informe de IBM reveló que las universidades y escuelas han sido blanco de un 25 % más de ataques de ransomware en comparación con el año anterior, lo que pone de manifiesto la creciente amenaza para las plataformas educativas [24].

En Perú, aunque no existen cifras exactas sobre ciberataques dirigidos específicamente a plataformas e-learning, se ha observado un aumento significativo de incidentes cibernéticos en todo el país. En 2024, Perú experimentó más de 45.500 millones de ciberataques, incluidos ransomware, phishing y ataques automatizados [25]. Durante la Cumbre APEC 2024 en Lima, se mitigaron más de medio millón de ciberataques, lo que demuestra la creciente amenaza que representan los eventos internacionales a gran escala [26].

Plataformas e-learning como Google, Moodle y Blackboard han sufrido brechas de seguridad debido a diferentes fallos, lo que demuestra la vulnerabilidad de los datos de profesores y alumnos.:

- Blackboard: En 2019, Bill Demirkapi descubrió fallos de seguridad críticos que permitieron el acceso no autorizado a información confidencial de más de 5 millones de registros, afectando a más de 5.000 escuelas [27].
- Moodle: Se ha identificado una vulnerabilidad en el módulo de autenticación Shibboleth de Moodle, que permite la ejecución remota de código y podría comprometer millones de cuentas. Estos incidentes ponen de manifiesto la gravedad de las brechas de seguridad en las plataformas educativas [28].

Este estudio contribuye al desarrollo y validación de un modelo de evaluación de la calidad de seguridad para plataformas e-learning, guiado por estándares de calidad como ISO/IEC 25010, ISO/IEC 25040 e ISO/IEC 25023. Este modelo cuantifica la calidad de seguridad en las plataformas e-learning e identifica vulnerabilidades específicas utilizando métricas basadas en los estándares ISO.

2. METODOLOGIA

Este estudio se fundamenta en los principios de la investigación aplicada, tal como lo plantean [30], en la cual propone un modelo de evaluación enfocado en entender los diferentes enfoques relacionados con la calidad del software. Para facilitar la comprensión y el uso del modelo propuesto, se diseñó un diagrama siguiendo las recomendaciones de las normas internacionales ISO/IEC 25000. En la Figura 1 se detallan las distintas fases que componen la investigación.

Para ello, se emplea un enfoque cuantitativo, siguiendo las pautas de [31], que se distingue por un proceso ordenado y validado, apoyado en herramientas confiables para la recopilación de datos. Mediante análisis numéricos y técnicas estadísticas, el estudio garantiza la precisión de los resultados y su aplicabilidad en distintos escenarios, respaldando la efectividad del modelo con datos evaluados por expertos, según lo señalado por [32].

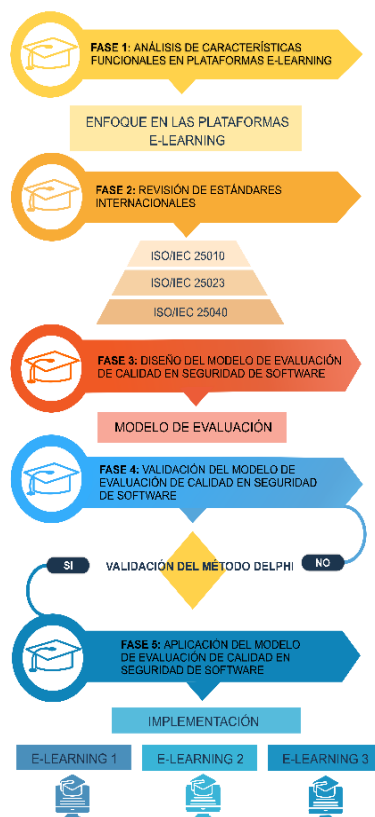


Figura 1. Fases de la investigación del modelo de evaluación propuesto

El desarrollo metodológico del modelo se estructura en cinco fases, las cuales se describen a continuación de manera resumida.

2.1. Fase 1: Análisis de características funcionales en plataformas e-learning

En esta fase se realizó una revisión de literatura sobre distintas plataformas de e-learning y sus características funcionales, poniendo especial atención en los aspectos relacionados con la calidad y la seguridad. A partir de este análisis se identificaron las funcionalidades más comunes y se agruparon en tres niveles de criticidad: alto, medio y bajo, según la frecuencia con la que fueron reportadas en los estudios [1], [6], [11], [12], [33]. La Tabla 1 muestra esta clasificación, donde se aprecia que funciones como la autenticación, la gestión de contenidos, la administración de cursos, la gestión de evaluación y los foros resultan las más críticas; mientras que la recuperación de contraseñas, el chat y la videoconferencia tienen una criticidad media, y la realidad virtual junto con el perfil del usuario se consideran de menor impacto.

Tabla 1. Clasificación de criticidad de características funcionales

<i>Nivel de criticidad</i>	<i>Características funcionales</i>	<i>Estudios</i>
Alto	Autenticación	[1], [6], [11], [12], [13]
	Gestión de contenidos	
	Administración de cursos	
	Gestión de evaluación	
Medio	Foros	[1], [6], [12], [33]
	Recuperación de contraseña	
	Chat	
	Video conferencia	
Bajo	Realidad virtual	[11]
	Perfil	

2.2. Fase 2: Revisión de Normas Internacionales

En esta fase, se establece las bases para desarrollar un modelo de evaluación confiable. Para ello se realizó un análisis exhaustivo de los estándares y marcos internacionales de calidad de software, con un enfoque especial en la seguridad de las plataformas de e-learning. La Tabla 2 mostró una comparación entre diferentes modelos de calidad, resaltando sus características más importantes y citando estudios relevantes. Esta comparación permitió clarificar cómo cada modelo integra la seguridad, la mejora continua, la facilidad de mantenimiento y su aceptación en el mercado.

Tabla 2. Comparación de modelos de Calidad de software

<i>Características</i>	<i>McCall</i>	<i>ISO 25010</i>	<i>Boehm</i>	<i>Dromey</i>	<i>ISO 9126</i>
Seguridad como atributo clave	[34]	[35]		[36]	[37]
Orientado a mejora continua		[38]	[37]	[37]	
Evaluación de mantenibilidad		[39]			
Uso generalizado en la industria	[40], [41]	[8]			

En la Tabla 3 se comparó varios estándares internacionales relacionados con métricas de seguridad. Esta comparación fue clave para entender cómo cada estándar aborda aspectos fundamentales como la confidencialidad, integridad y disponibilidad de la información. Este análisis facilitó la identificación de los estándares más adecuados para evaluar plataformas e-learning, asegurando que se cubrieran de manera efectiva las amenazas y vulnerabilidades propias de estos entornos.

Tabla 3. Comparación de estándares internacionales sobre métricas de seguridad

<i>Características</i>	<i>ISO 25023</i>	<i>Owasp metrics</i>	<i>ISO 15408</i>	<i>ISO 27005</i>
Confidencialidad, integridad, disponibilidad	[42], [43]		[44]	[45]
Normas Internacionales	[42]		[46]	[46]
Métricas cuantitativas	[42]	[43]		
Aplicabilidad en TI				[45]

Por otro lado, la Tabla 4 presenta un análisis detallado de las características de los modelos de evaluación, estos procesos resultaron especialmente valiosos para las plataformas e-learning porque ofrecen una descripción clara y accesible de cada una de las etapas, sirviendo como una guía práctica para los equipos técnicos y administradores educativos. De esta manera, se buscó asegurar que los sistemas mantuvieran de forma continua los

estándares de calidad necesarios para el correcto funcionamiento de las plataformas e-learning.

Tabla 4. Comparación de modelos de evaluación de software

<i>Características</i>	<i>ISO 25040</i>	<i>ISO 15939</i>	<i>ISO 33063</i>	<i>ISO 29119</i>
Evaluación continua	[46]	[47]		[48]
Estandarización internacional	[49]		[50]	
Focalización en la calidad global del software.	[46]			[51]
Definición clara de etapas	[52]	[47]	[50]	
Orientado a Procesos	[49]			

2.3. Fase 3: Modelo de evaluación de la calidad en seguridad del software

En esta fase se diseñó un modelo de evaluación orientado a medir el nivel de seguridad en plataformas e-learning, tomando como base la información recopilada en la Fase 1 y la Fase 2. El diseño se centró en cinco aspectos fundamentales definidas por la norma ISO/IEC 25010 [53]: Confidencialidad, Integridad, No Repudio, Responsabilidad y Autenticidad.

Para la evaluación de estos aspectos se escogió a la norma ISO/IEC 25040 [49] que garantiza un proceso de evaluación estructurado dado que incluye entradas y salidas de proceso, limitaciones y recursos, de esta manera se asegura que el modelo de evaluación sea técnico y confiable.

Por otro lado, se consideró las 10 métricas de seguridad definidas en la ISO/IEC 25023 [42], Considerando las características o funcionalidades de las plataformas e-learning descritas en la Tabla 6, se desarrolló un instrumento para servir como base y herramienta de evaluación. Este instrumento se estructura en torno a los 5 aspectos de seguridad y las 10 métricas correspondientes. El aspecto de confidencialidad consta de 21 ítems, la integridad de 18, la no repudiación de 9, la responsabilidad de 13 y la autenticidad de 36; cada ítem tiene tres alternativas (Sí, No y No aplica). Según los resultados, se aplica la fórmula de la métrica y se calcula el promedio para cada aspecto evaluado. Para el resultado final, el valor del aspecto se multiplica por un peso determinado (Confidencialidad = 0,4, Integridad = 0,15, No repudio = 0,05, Responsabilidad = 0,10 y Autenticidad = 0,30), y finalmente, los resultados se suman y se verifica en qué escala se encuentra según la Tabla V, donde se define una escala de aceptación considerando las puntuaciones obtenidas por la plataforma evaluada: "Inaceptable", "Mínimamente aceptable", "Rango objetivo" y "Supera los requisitos". Dichas escalas se presentan en la Tabla 5.

Table 5. Escala de aceptación para la evaluación de seguridad

<i>Nivel de aceptación</i>	<i>Escala de medición</i>
Inaceptable (I)	$0 \leq X < 40$
Mínimamente aceptable (MA)	$40 \leq X < 60$
Rango objetivo (RO)	$60 \leq X < 90$
Excede los requerimientos (ER)	$90 \leq X < 100$

El diseño final del modelo articula aspectos, métricas y escala en un proceso evaluativo estructurado en cinco etapas, tal como se presenta en la Figura 2. En la Etapa 1 (Establecer) se identifican los aspectos de seguridad más relevantes que serán utilizados para la evaluación de la plataforma e-learning. La Etapa 2 (Especificar) consiste en seleccionar y ponderar las métricas más adecuadas para evaluar los aspectos seleccionados en la etapa 1, tomando como referencia la norma ISO/IEC 25023. En la Etapa 3 (Diseñar) se personaliza el instrumento de evaluación en función de las particularidades del contexto de la plataforma e-learning. La Etapa 4 (Ejecutar) corresponde a la aplicación del instrumento en la práctica, desarrollando el proceso de evaluación

de manera estructurada y controlada, de acuerdo con lo establecido en la norma ISO/IEC 25040. Finalmente, en la Etapa 5 (Concluir) se procesan y analizan los resultados obtenidos, generando un informe que determina el nivel de aceptación.

Tabla 6. Métricas de seguridad basadas en ISO/IEC 25023

<i>Aspectos Claves</i>	<i>Métrica</i>	<i>Descripción</i>	<i>Formula</i>
Confidencialidad	1. Control de acceso	¿Qué proporción de datos confidenciales están protegidos de accesos no autorizados?	$X = 1 - (A / B)$ A = Número de datos confidenciales que pueden ser accedidos sin autorización B = Número de datos que requieren control de acceso
	2. Encriptación de datos	¿Qué tan correctamente se implementa la encriptación/desencriptación de los elementos de datos según lo especificado en los requisitos?	$X = A / B$ A= Número de datos cifrados/descifrados correctamente B= Número de datos que requieren cifrado/descifrado
	3. Algoritmos criptográficos	¿Qué proporción de algoritmos criptográficos han sido bien evaluados?	$X = 1 - A/B$ A= Número de algoritmos criptográficos rotos o inaceptablemente riesgosos en uso B= Número de algoritmos criptográficos utilizados
Integridad	4. Integridad de datos	¿Hasta qué punto se ha prevenido la corrupción o modificación de datos por acceso no autorizado?	$X = 1 - A/B$ A= Número de elementos de datos que han sido efectivamente corrompidos por acceso no autorizado B= Número de elementos de datos para los cuales debe prevenirse la corrupción o modificación
	5. Prevención de corrupción de datos interna	¿Hasta qué punto se ha prevenido la corrupción o modificación de datos por acceso no autorizado?	$X = A / B$ A= Número de métodos de prevención de corrupción de datos realmente implementados B= Número de métodos de prevención de corrupción de datos disponibles y recomendados
No Repudio	6. Uso de firma digital	¿Cuál es la proporción de eventos que requieren no repudio se procesa usando firmas digitales?	$X = A/B$ A= Número de eventos que aseguran no repudio utilizando firma digital B= Numero de accesos al sistema y los datos registrados en el log del sistema
Responsabilidad	7. Integridad del registro de auditoría de usuarios	¿Cuán completo es el registro de auditoria con respecto al acceso de los usuarios al sistema o los datos?	$X = A/B$ A= Número de accesos registrados en todos los registros (logs) B= Número de accesos al sistema o a los datos realmente verificados
	8. Retención de registros del sistema	¿Por cuánto tiempo se retiene el registro del sistema en almacenamiento estable en porcentaje?	$X=A/B$ A= Duración durante la cual el registro del sistema se conserva efectivamente en almacenamiento estable B= Período de retención especificado para mantener el registro del sistema en almacenamiento estable
Autenticidad	9. Suficiencia del mecanismo de autenticación	¿Cuán bien autentica el sistema la identidad de un sujeto?	$X=A/B$ A= Número de mecanismos de autenticación proporcionados (por ejemplo, ID de usuario/contraseña o tarjeta IC) B= Número de mecanismos de autenticación especificados

Aspectos Claves	Métrica	Descripción	Formula
10. Conformidad con las reglas de autenticación	¿Cuál es la proporción de la regla de autenticación requerida está establecida?	A= Número de reglas de autenticación implementadas B= Número de reglas de autenticación especificadas	$X=A/B$

2.4. Fase 4: Validación del modelo de evaluación de la calidad del software

Durante la cuarta fase, se desarrolló el instrumento para la validación del modelo; dicho instrumento consta de cinco dimensiones: adecuación a las plataformas e-learning y a las normas ISO, con dos ítems; metodología y métricas, con tres ítems; objetividad, con cuatro ítems; eficacia, con dos ítems; y facilidad de uso, con tres ítems. A continuación, se utilizó el método Delphi para validar el modelo. Este método consiste en reunir a un panel de expertos para alcanzar un consenso sobre un problema o tema específico. Para ello, se seleccionó a expertos en ciberseguridad, calidad y evaluación de software para que realizaran una valoración utilizando el instrumento de validación mencionado anteriormente. Se llevó a cabo un proceso de retroalimentación iterativa con los expertos hasta alcanzar un consenso, y posteriormente se validó el modelo, tal y como se ilustra en la Figura 3, que resume el proceso de validación del modelo.

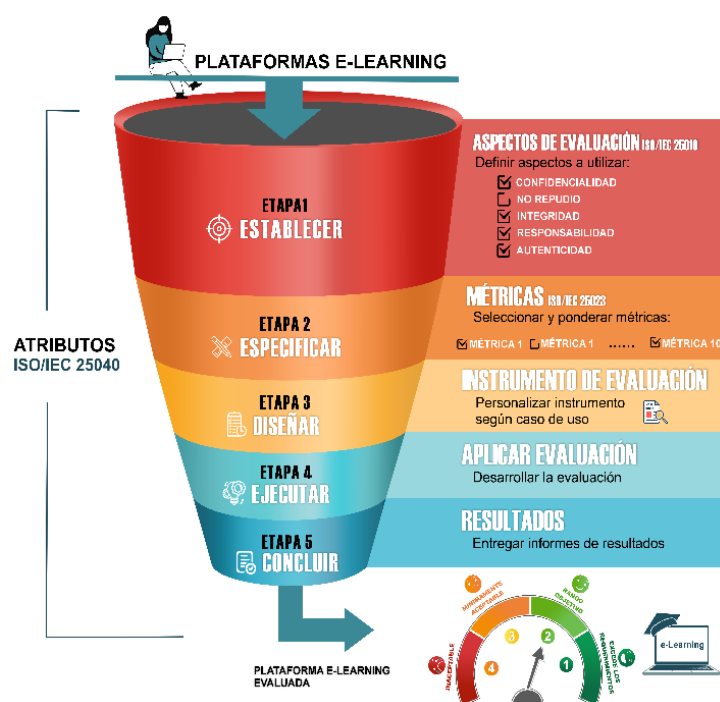


Figura 2. Diseño final del modelo de evaluación de seguridad

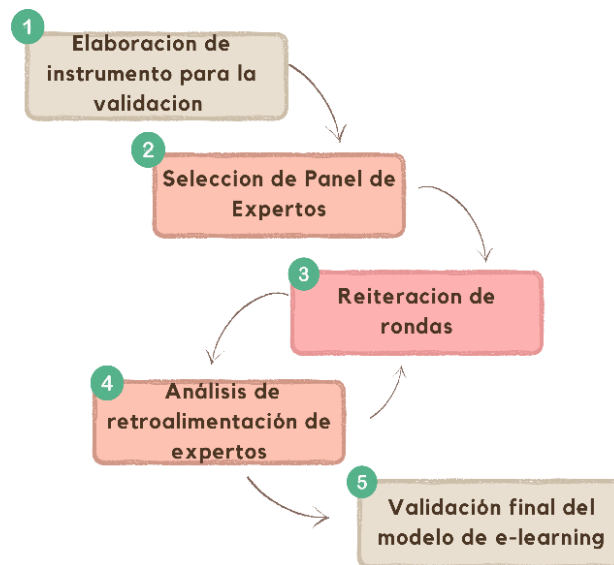


Figura 3. Proceso de validación del modelo propuesto (método Delphi)

2.5. Fase 5: Aplicación del modelo de evaluación de la calidad en seguridad del software

Finalmente, en la Fase 5, se implementó el modelo de evaluación de calidad en seguridad en tres plataformas e-learning distintas. Para ello en primer lugar, se desarrolló un plan detallado que definió las plataformas, los módulos y herramientas a evaluar, así como los métodos y métricas de calidad a aplicar, a continuación, los evaluadores llevaron a cabo las mediciones, se obtuvo por cada plataforma tres evaluaciones de los cuales un resultado fue por un evaluador interno técnico del equipo de desarrollo, un evaluador interno con perfil de auditor y un evaluador externo experto en seguridad. Posteriormente, el adquiriente revisó los resultados para tomar decisiones sobre la adopción o mejora de las plataformas, generando un informe con recomendaciones finales basadas en los atributos de calidad evaluados.

3. RESULTADOS

El modelo de evaluación de la calidad de la seguridad se aplicó a las plataformas educativas de tres instituciones diferentes: la Plataforma A, la Plataforma B y la Plataforma C. En cada una de estas plataformas se asignaron tres evaluadores que utilizaron el instrumento desarrollado y validado en el estudio; las funciones de estos evaluadores eran las siguientes: “Auditor interno (AI)”, “Evaluador externo (EE)” y “responsable técnico (LT)”. En la figura 4 muestra los resultados consolidados de las tres plataformas e-learning en los cinco aspectos de seguridad evaluados. En la Plataforma A, los resultados muestran un rendimiento desigual en los cinco aspectos de seguridad evaluados.

La confidencialidad alcanza el “rango objetivo” con valores superiores al 60 % en las tres evaluaciones (LT: 77 %, AI: 87 % y EE: 68 %), lo que indica que existen mecanismos adecuados para proteger la información sensible de los usuarios. Sin embargo, la autenticidad refleja una clara debilidad, con puntuaciones muy bajas (LT: 38 %, AI: 25 % y EE: 22 %), lo que indica un nivel «inaceptable» y plantea graves riesgos para la validación de las identidades de los usuarios. En cuanto a la integridad, los resultados son heterogéneos: mientras que el responsable técnico informa de un 71 %, los demás evaluadores indican niveles muy bajos (EE: 38 % y AI: 13 %), lo que sugiere una falta de coherencia en los controles implementados. La responsabilidad se divide al 50 % entre el auditor interno y el evaluador externo, clasificada como “Mínimamente aceptable”, y el líder técnico al 75 %, lo que refleja limitaciones en la trazabilidad de las acciones dentro del sistema. Por último, no se contempla la evaluación del aspecto de no repudio, ya que el objetivo de las plataformas e-learning no requiere dicha funcionalidad.

En la Plataforma B, los resultados indican avances en determinados aspectos de seguridad, aunque persisten deficiencias significativas. La confidencialidad obtiene valores relativamente estables (LT: 64 %, AI: 70 % y EE: 70 %), lo que la sitúa dentro de un “rango objetivo”, lo cual indica un buen nivel de protección. En cuanto a la autenticidad, los tres evaluadores coinciden en una puntuación baja (38 %), lo que la sitúa en el nivel «inaceptable». Este hallazgo revela una deficiencia significativa en la validación de la identidad y representa un riesgo crítico para la fiabilidad de la plataforma. La integridad presenta una evaluación mixta: mientras que el auditor interno alcanza el 64 %, los demás evaluadores registran resultados más bajos (LT: 50 % y EE: 48 %), situándose dentro del rango “mínimamente aceptable”. Esto refleja que los controles de consistencia de los datos no están totalmente garantizados. La responsabilidad es el punto más fuerte de la Plataforma B, con valores máximos (AI: 100% y EE: 100%), aunque el responsable técnico solo obtiene una puntuación del 50 %. En general, este aspecto puede considerarse aceptable, ya que destaca la presencia de mecanismos de trazabilidad, aunque existen diferencias en las percepciones de los evaluadores. Por último, la no repudio obtiene una calificación crítica (0 % en EE y AI, y 44 % en LT), lo que sitúa este aspecto en el nivel «inaceptable» y pone de manifiesto la falta de controles que garanticen la verificación de las transacciones, así como la imposibilidad de que un usuario pueda negar su participación en ellas.

En la Plataforma C, los resultados indican un rendimiento aceptable en determinados aspectos de seguridad, aunque persisten deficiencias críticas que afectan a la confianza general en el sistema. La confidencialidad muestra valores consistentes (LT: 65%, AI: 75% y EE: 76%), alcanzando el «rango objetivo» y poniendo de manifiesto un nivel óptimo de protección de la información. En cuanto a la autenticidad, los tres evaluadores coinciden en puntuaciones muy bajas (LT: 31%, AI: 22% y EE: 22%), lo que indica un nivel claramente «inaceptable». Esta deficiencia es el punto más crítico de la plataforma, ya que pone en riesgo la veracidad de la identidad de los usuarios. La integridad obtiene resultados dispares: mientras que el auditor interno registra un 38% de “inaceptable”, el responsable técnico alcanza el 71% y el evaluador externo el 33%, este último se sitúa dentro del rango “inaceptable”. Esta variabilidad refleja

la falta de uniformidad en los mecanismos que garantizan la coherencia y la integridad de los datos. En cuanto a la responsabilidad, los tres evaluadores otorgan un 50 %, lo que sitúa este aspecto en el nivel “Mínimamente aceptable”. Aunque existe trazabilidad en las acciones, no hay indicios de un control sólido que permita un seguimiento detallado de las operaciones. Por último, el no repudio presenta una situación heterogénea: el responsable técnico y el auditor interno reportan valores bajos (67% y 44%, respectivamente), mientras que el evaluador externo reporta un valor más alto, del 33%. Esto sitúa este aspecto entre lo “Inaceptable” y lo “Mínimamente aceptable”, lo que pone en duda la capacidad del sistema para garantizar la validación de las transacciones y la no negación de responsabilidades.

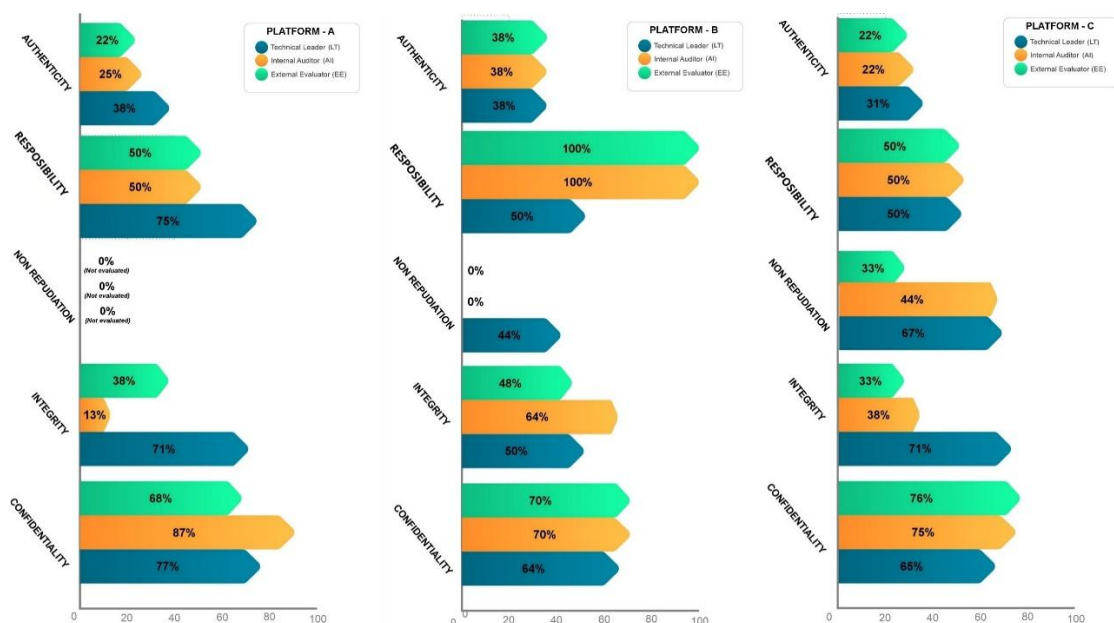


Figura 4. Resultado de evaluación de la calidad en seguridad de las plataformas e-learning

Por último, los resultados se han sintetizado en la figura 5 teniendo en cuenta los cinco aspectos clave de seguridad de las tres plataformas; todas ellas se sitúan dentro de la escala “Mínimamente aceptable”; aunque el aspecto de la confidencialidad alcanza el nivel esperado en todas las plataformas, el panorama general es preocupante, ya que el aspecto de la autenticidad es el eslabón más débil, puesto que sus evaluaciones alcanzan un nivel “Inaceptable” en las tres plataformas analizadas, lo que suscita serias dudas sobre la identidad de los usuarios y la veracidad de los datos. Otros aspectos, como la integridad, la responsabilidad y el no repudio, también presentan deficiencias, lo que deja a los sistemas de información en un estado “Mínimamente aceptable”. Estos hallazgos subrayan la necesidad de reforzar los controles de acceso, las políticas de autenticación y las normas de seguridad en las plataformas e-learning.

Todas las plataformas presentan puntos débiles señalados por los tres evaluadores de cada una de ellas; sin embargo, en la Tabla 7 se recogen algunas vulnerabilidades como las principales, ya que aparecen en todas las evaluaciones. Esto pone de manifiesto que es necesario establecer normas para reforzar su mecanismo de autenticación e implementar políticas de seguridad claras y conformes, al tiempo que se recomienda invertir en la actualización de las tecnologías de autenticación y cifrado, con el fin de garantizar el cumplimiento de los aspectos de autenticidad, confidencialidad e integridad definidos en la norma ISO/IEC 25010.

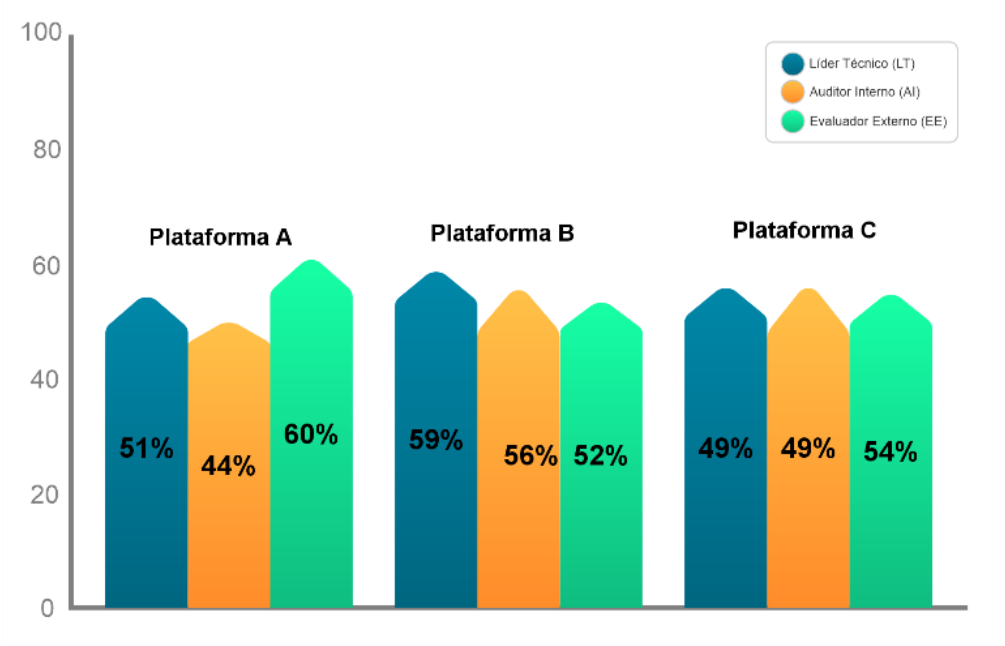


Figura 5. Resultados consolidados de las tres plataformas e-learning

Tabla 7. Principales vulnerabilidades detectadas en las plataformas evaluadas

Aspecto	Criterio Evaluado	Vulnerabilidad identificada
Autenticidad	Conformidad con las reglas de autenticación	Contraseñas temporales sin periodo de validez definido
		Mensajes de error no genéricos en el login (pueden filtrar información)
		No cambio obligatorio de contraseña tras un período definido
		No MFA o reautenticación para funciones críticas
		No integración con aplicación de autenticación de un solo uso (OTP)

Aspecto	Criterio Evaluado	Vulnerabilidad identificada
	Suficiencia del mecanismo de autenticación	No integración con múltiples aplicaciones de autenticación
		No límite de intentos fallidos con apps de autenticación
		No límite de intentos para recuperación de contraseña
		No prevención de uso de información personal como contraseña
Confidencialidad	Control de acceso	Acceso sin autorización a credenciales
	Encriptación de datos	Certificados, diplomas y calificaciones sin cifrado
	Algoritmos criptográficos	Uso de MD5 para hashing (vulnerable a colisiones)

4. DISCUSIÓN

Los resultados obtenidos permiten validar el modelo de evaluación propuesto como una herramienta eficaz para diagnosticar el nivel de seguridad en plataformas e-learning. A diferencia del enfoque planteado en [12] centrado exclusivamente en la usabilidad y experiencia del usuario, el modelo desarrollado en este estudio aborda específicamente la calidad en seguridad del software, incorporando cinco aspectos críticos definidos por la norma ISO/IEC 25010. Esto permite una evaluación más técnica y estructurada, considerando elementos como autenticidad, no repudio y responsabilidad, esenciales en entornos donde se gestionan datos sensibles de estudiantes y docentes.

Por su parte, la propuesta presentada en [18] se basa en un conjunto de indicadores generales de calidad aplicables a sistemas de gestión del aprendizaje. No obstante, dicho enfoque carece de una estructura fundamentada en normas técnicas específicas como ISO/IEC 25023 y no incluye un catálogo validado de métricas aplicables directamente al análisis de seguridad del software. En contraste, el presente estudio incorpora métricas normativas integradas en un instrumento diseñado y validado mediante juicio de expertos.

Además, los resultados diferenciados entre las plataformas evaluadas evidencian la capacidad discriminativa del modelo, al identificar con claridad fortalezas y debilidades particulares. Por ejemplo, las diferencias observadas en confidencialidad y autenticidad entre las plataformas B y C reflejan variaciones sustanciales en la implementación de controles de acceso, cifrado y mecanismos de autenticación. Estas distinciones permiten a los responsables tecnológicos tomar decisiones informadas para mitigar riesgos y mejorar la protección de los datos institucionales.

Finalmente, aunque el modelo mostró resultados sólidos en su validación y aplicación inicial, se reconoce como limitación el tamaño reducido de la muestra.

Por ello, se recomienda su aplicación en un número mayor de plataformas y contextos institucionales diversos, con el fin de fortalecer su validez externa y ampliar su aplicabilidad práctica en el ámbito educativo digital.

5. CONCLUSIÓN

Este estudio presentó un modelo de evaluación de la calidad en seguridad del software para plataformas e-learning, basado en las normas ISO/IEC 25010, 25023 y 25040. El modelo fue desarrollado en cinco fases, e integra cinco aspectos de seguridad, un catálogo estructurado de métricas técnicas y una escala de aceptación validada mediante juicio de expertos.

La aplicación del modelo en tres plataformas educativas permitió identificar diferencias significativas en el nivel de cumplimiento de criterios de seguridad. Los resultados demostraron que el instrumento es capaz de discriminar con precisión entre plataformas con distintos niveles de madurez técnica en aspectos clave como confidencialidad, autenticidad y responsabilidad.

A diferencia de propuestas previas [12], [18], el modelo presentado se fundamenta en estándares internacionales y ofrece una estructura cuantitativa que facilita la evaluación reproducible de sistemas educativos digitales. Esto lo convierte en una herramienta útil tanto para procesos de auditoría como para la mejora continua de plataformas tecnológicas en entornos académicos.

Como trabajo futuro, se plantea ampliar la aplicación del modelo a una muestra mayor de plataformas, así como explorar su integración en entornos híbridos o móviles, donde la seguridad sigue siendo un desafío relevante. Asimismo, se sugiere evaluar la adaptabilidad del modelo a otros dominios de software más allá del ámbito educativo.

6. REFERENCIAS

- [1]. Alkabaa, A. S. (2022). Effectiveness of using E-learning systems during COVID-19 in Saudi Arabia: Experiences and perceptions analysis of engineering students. *Education and Information Technologies*, 27(8), 10625–10645. [Doi: 10.1007/s10639-022-11054-z](https://doi.org/10.1007/s10639-022-11054-z)
- [2]. Kaur, J., & Kumar, P. (2022). Teachers' perception of online teaching and its effects on learning outcome during Covid-19: an India based mixed method study. *Journal of E-Learning and Knowledge Society*, 18(2), 11–21. Doi: 10.20368/1971-8829/1135450
- [3]. Saloom, R. H., Elameer, A. S., & Jalal, A. S. (2018). A new style of an academic institutions in Iraq: E-University. *Proceedings of the 1st Annual International Conference on Information and Sciences (AiCIS 2018)*, 187–192. Doi: 10.1109/AiCIS.2018.00044
- [4]. Turnbull, D., Chugh, R., & Luck, J. (2021). Transitioning to E-Learning during the COVID-19 pandemic: How have Higher Education Institutions responded to the challenge? *Education and Information Technologies*, 26(5), 6401–6419. Doi: 10.1007/s10639-021-10633-w

- [5]. Chatti, H., & Hadoussa, S. (2021). Factors Affecting the Adoption of E-Learning Technology by Students during the COVID-19 Quarantine Period: The Application of the UTAUT Model. *Engineering, Technology & Applied Science Research*, 11(2), 6993–7000. Doi: 10.48084/etasr.3985
- [6]. Akacha, S. A. L., & Awad, A. I. (2023). Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders. *Sustainability*, 15(19), 14132. Doi: 10.3390/su151914132
- [7]. Rathgeb, C., Poppelmann, K., & Busch, C. (2021). Face morphing attacks: A threat to eLearning? *Proceedings of the IEEE Global Engineering Education Conference (EDUCON 2021)*, 1149–1154. Doi: 10.1109/EDUCON46332.2021.9454128
- [8]. Thamilarasan, Y., Raja Ikram, R. R., Osman, M., Salahuddin, L., Wan Bujeri, W. Y., & Kanchymalay, K. (2023). Enhanced System Usability Scale using the Software Quality Standard Approach. *Engineering, Technology and Applied Science Research*, 13(5), 11779–11784. Doi: [10.48084/etasr.5971](https://doi.org/10.48084/etasr.5971)
- [9]. Awangditama, B. R., Mardhatillah, L., & Rochimah, S. (2023). Quality Conformity Analysis Functional and Usability in Academic Information Systems Using ISO/IEC 25010. *Proceedings of the 14th International Conference on Information and Communication Technology and System (ICTS 2023)*, 24–28. Doi: [10.1109/ICTS58770.2023.10330881](https://doi.org/10.1109/ICTS58770.2023.10330881)
- [10]. Schaffernak, H., Moesl, B., Url, P., Victoria Koglbauer, I., & Vorraber, W. (2025). Towards sustainable software quality in use: a review of measures. *Next Research*, 2(3), 100680. Doi: [10.1016/j.nexres.2025.100680](https://doi.org/10.1016/j.nexres.2025.100680)
- [11]. Manglapuz, S. J. R., & Lacatan, L. L. (2019). Academic management android application for student performance analytics: A comprehensive evaluation using ISO 25010:2011. *International Journal of Innovative Technology and Exploring Engineering*, 8(12), 5085–5089. Doi: 10.35940/ijitee.L2735.1081219
- [12]. Sekarini, D., Alfiani, F. S., & Rochimah, S. (2020). Security Characteristic Evaluation of New Students Admission Information System Based on ISO/IEC 25010 Quality Standard. *Proceedings of the 12th International Conference on Information Technology and Electrical Engineering (ICITEE 2020)*, 120–124. Doi: [10.1109/ICITEE49829.2020.9271756](https://doi.org/10.1109/ICITEE49829.2020.9271756)
- [13]. Aziz, M. N., Sapta, I. M., & Rochimah, S. (2018). Security Characteristic Evaluation Based on ISO/IEC 25023 Quality Model, Case Study: Laboratory Management Information System. *Proceedings of the Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS 2018)*, 332–336. Doi: [10.1109/EECCIS.2018.8692982](https://doi.org/10.1109/EECCIS.2018.8692982)
- [14]. Yenny Milagritos Sifuentes Díaz, & José Luis Peralta Luján. (2022). Modelo de medición y evaluación de calidad del software basado en la norma ISO/IEC 25000 para medir la usabilidad en productos de software académicos universitarios. *Tecnohumanismo*, 2(1), 181–204. Doi: [10.53673/th.v2i4.125](https://doi.org/10.53673/th.v2i4.125)
- [15]. Purbaratri, W., Hartomo, K. D., Hendry, & Tambotih, J. J. C. (2023). The New Smart Government Software Quality Framework Uses Modifications to ISO/IEC 25010. *Proceedings of the 8th International Conference on*

Informatics and Computing (ICIC 2023), 1-6 [Doi: 10.1109/ICIC60109.2023.10382109](https://doi.org/10.1109/ICIC60109.2023.10382109)

- [16]. Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information (Switzerland)*, 13(4). [Doi: 10.3390/info13040192](https://doi.org/10.3390/info13040192)
- [17]. Ivanova, M., Trifonova, I., & Bogdanova, G. (2022). Privacy Preservation in eLearning: Exploration and Analysis. *Proceedings of the 20th International Conference on Information Technology Based Higher Education and Training (ITHET 2022)*, 1-8 [Doi: 10.1109/ITHET56107.2022.10031904](https://doi.org/10.1109/ITHET56107.2022.10031904)
- [18]. Peters, E., & Aggrey, G. K. (2020). An ISO 25010 based quality model for ERP systems. *Advances in Science, Technology and Engineering Systems*, 5(2), 578–583. [Doi: 10.25046/aj050272](https://doi.org/10.25046/aj050272)
- [19]. Haoues, M., Sellami, A., Ben-Abdallah, H., & Demirors, O. (2019). Evaluating Software Security Change Requests: A COSMIC-Based Quantification Approach. *Proceedings of the 45th Euromicro Conference on Software Engineering and Advanced Applications (SEAA 2019)*, 268–275. [Doi: 10.1109/SEAA.2019.00049](https://doi.org/10.1109/SEAA.2019.00049)
- [20]. Al-Matouq, H., Mahmood, S., Alshayeb, M., & Niazi, M. (2020). A Maturity Model for Secure Software Design: A Multivocal Study. *IEEE Access*, 8, 215758–215776. [Doi: 10.1109/ACCESS.2020.3040220](https://doi.org/10.1109/ACCESS.2020.3040220)
- [21]. Amo, D., Alier, M., García-Péalvo, F. J., Fonseca, D., & Casany, M. J. (2019). GDPR security and confidentiality compliance in LMS' a problem analysis and engineering solution proposal. *Proceedings of the ACM International Conference Proceeding Series*, 253–259. [Doi: 10.1145/3362789.3362823](https://doi.org/10.1145/3362789.3362823)
- [22]. Herrera-Cubides, J. F., Gaona-García, P. A., & Salcedo-Salgado, G. A. (2019). Towards the construction of a user unique authentication mechanism on LMS platforms through model-driven engineering(MDE). *Scientific Programming*, 2019. [Doi: 10.1155/2019/9313571](https://doi.org/10.1155/2019/9313571)
- [23]. SoCRadar. (2024). *Education Industry Biggest Attacks in 2024*. SoCRadar. Retrieved from: <https://socradar.io/biggest-education-industry-attacks-in-2024/> [accessed: 01 October 2024]
- [24]. IBM. (2024). *Reducing ransomware recovery costs in education*. Jennifer Gregory. Retrieved from: <https://www.ibm.com/think/insights/reducing-ransomware-recovery-costs-in-education> [accessed: 01 October 2024]
- [25]. Infobae. (2025). *Perú registró 45 mil millones de ciberataques en 2024: así puedes proteger tu pyme sin ser experto en tecnología*. Infobae. Retrieved from : <https://www.infobae.com/peru/2025/05/22/peru-registro-45-mil-millones-de-ciberataques-en-2024-asi-puedes-proteger-tu-pyme-sin-ser-experto-en-tecnologia/> [accessed: 03 October 2024]
- [26]. APEC Peru 2024. (2024). *APEC Peru 2024 successfully fended off more than half a million cyberattacks*. APEC Perú. Retrieved from: <https://www.apecperu.pe/2024/en/2024/11/22/apec-peru-2024-successfully-fended-off-more-than-half-a-million-cyberattacks/> [accessed: 03 October 2024]
- [27]. Greenberg, A. (2019). *Teen hacker exposes vulnerabilities in Blackboard*. Wired. Retrieved from: <https://www.wired.com/story/teen-hacker-school-software-blackboard-follett> [accessed: 09 October 2024]

- [28]. Paganini, P. (2020). *Moodle account takeover threats*. In *Security Affairs*. Retrieved from: <https://securityaffairs.com/116560/hacking/moodle-account-takeover-threats.html> [accessed: 09 October 2024]
- [29]. Kimery, A. (2024). *Google settles over kids' biometric data collection in schools*. Biometric Update. Retrieved from: <https://www.biometricupdate.com/202408/google-settles-over-kids-biometric-data-collection-in-schools> [accessed: 10 October 2024]
- [30]. Silva Vernier, L., Dartora, J., Herbert, J., Cazella, S. C., & Centenaro Levandowski, D. (2021). *Model for quality analysis of neonatal hearing screening software: theory applied*. *International Journal of Medical Informatics*, 150, 104435.
- [31]. Hernández Sampieri, R., Fernández Collado, C., & María del Pilar Baptista Lucio, M. (2014) *METODOLOGIA DE LA INVESTIGACION SEXTA EDICION*. McGRAW-HILL & INTERAMERICANA.
- [32]. Aponte Figueroa, G., Cardozo Montilla, M. A., & Melo, R. M. (2012). *METODO DELPHI: APLICACIONES Y POSIBILIDADES EN LA GESTION PROSPECTIVA DE LA INVESTIGACION Y DESARROLLO*. *Revista Venezolana de Análisis de Coyuntura*, XVIII(1), 41-52
- [33]. Djeki, E., Degila, J., Bondiombouy, C., & Alhassan, M. H. (2022). *Preventive Measures for Digital Learning Spaces' Security Issues*. 2022 IEEE TEMSCON EUROPE 2022, 48–55. Doi: TEMSCONEUROPE54743.2022.9801945.
- [34]. Budi, S., Gata, W., Noor, M., Pangabea, S., & Rahayu, C. S. (2022). *News Portal Website Measurement Analysis Using ISO/IEC 25010 And McCall Methods*. *Journal of Applied Engineering and Technological Science (JAETS)*, 4(1), 273–285. Doi: 10.37385/jaets.v4i1.1094.
- [35]. Marroquin, J. P., & Rodriguez, C. R. (2023). *Quality Assessment Model Based on ISO/IEC 25010 for E-Learning Platforms in the Cloud and Based on Laravel*. *Proceedings - 2023 15th IEEE International Conference on Computational Intelligence and Communication Networks, CICN 2023*, 751–757. Doi: 10.1109/CICN59264.2023.10402281
- [36]. Raffoul, E., Domínguez, K., Pérez, M., Mendoza, L. E., & Grimán, A. C. (2008). *Quality model for the selection of floss-based issue tracking system*. *Proceedings of the IASTED International Conference on Software Engineering, SE 2008*, 43–49.
- [37]. Ortega, M., Pérez, M., & Rojas, T. (2003). *Construction of a Systemic Quality Model for Evaluating a Software Product*. *Software Quality Journal*, 11(3), 219–242. Doi: 10.1023/A:1025166710988
- [38]. Chand, R., Khan, S. U. R., Hussain, S., Wang, W.-L., Tang, M.-H., & Ibrahim, N. (2024). *Exploring Software Quality Through Data-Driven Approaches and Knowledge Graphs*. *Proceeding of the Good practices and new perspectives in information systems and technologies Lecture Notes in Networks and Systems*, vol 990, 373–382. Doi: 10.1007/978-3-031-60328-0_37
- [39]. Aguirre, A. F., Villareal-Freire, Á., Gil, R., & Collazos, C. A. (2017). *Extending the concept of user satisfaction in e-learning systems from ISO/IEC 25010*. *Proceedings of the Lecture Notes in Computer*, vol 10290, 167–179. Doi: 10.1007/978-3-319-58640-3_13

- [40]. Wang, S.-H., Samadhiya, D., & Chen, D. (2011). *Software quality: Role and value of quality models*. International Journal of Advancements in Computing Technology, 3(6), 65–74. Doi: 10.4156/ijact.vol3.issue6.9
- [41]. Wolski, M., Walter, B., Kupiński, S., & Chojnacki, J. (2018). *Software quality model for a research-driven organization—An experience report*. Journal of Software: Evolution and Process, 30(5). Doi: 10.1002/smr.1911
- [42]. Falco, M., Scott, E., & Robiolo, G. (2020). Overview of an automated framework to measure and track the quality level of a product. *Proceedings of the 2020 IEEE Congreso Bienal de Argentina, ARGENCON 2020*. Doi: 10.1109/ARGENCON49523.2020.9505405
- [43]. Sonmez, F. O., & Kilic, B. G. (2021). *Holistic Web Application Security Visualization for Multi-Project and Multi-Phase Dynamic Application Security Test Results*. IEEE Access, 9, 25858–25884. Doi: 10.1109/ACCESS.2021.3057044
- [44]. Nakai, H., Tsuda, N., Honda, K., Washizaki, H., & Fukazawa, Y. (2016). Initial Framework for Software Quality Evaluation Based on ISO/IEC 25022 and ISO/IEC 25023. *Proceedings of the 2016 IEEE International Conference on Software Quality, Reliability and Security-Companion, QRS-C 2016*, 410–411. Doi: 10.1109/QRS-C.2016.66
- [45]. Taylor, S., Surridge, M., & Pickering, B. (2021). Regulatory Compliance Modelling Using Risk Management Techniques. *Proceedings of the IEEE World AI IoT Congress*, 474–481. Doi: 10.1109/AlIoT52608.2021.9454188
- [46]. Dhouib, A., Trabelsi, A., Kolski, C., & Neji, M. (2017). *Prioritizing the usability criteria of adaptive user interfaces of information systems based on ISO/IEC 25040 standard*. Ingenierie Des Systemes d'Information, 22(4), 107–128. Doi: 10.3166/ISI.22.4.107-128
- [47]. Monla, Z., Assila, A., Beladjine, D., & Zghal, M. (2024). Maturity Measurement Framework for Evaluating BIM-Based AR/VR Systems Adapted from ISO/IEC 15939 Standard. *Proceeding of the Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 14721 LNCS, 79–95. Doi: 10.1007/978-3-031-61318-0_7
- [48]. Patrício, C., Pinto, R., & Marques, G. (2021). *A Study on Software Testing Standard Using ISO/IEC/IEEE 29119-2: 2013*. Studies in Systems, Decision and Control, 295, 43–62. Doi: 10.1007/978-3-030-47411-9_3
- [49]. Calabrese, J., Esponda, S., Pasini, A., & Pesado, P. (2021). *Data Evaluation Model Using GQM Approach*. Communications in Computer and Information Science, 1409 CCIS, 141–154. Doi: 10.1007/978-3-030-75836-3_10
- [50]. Carpio, A. F. Del. (2018). *Visualizing composition and behavior of the ISO/IEC 33000 assessment framework through a multi-layer model*. Computer Standards and Interfaces, 60, 3–12. Doi: 10.1016/j.csi.2018.04.008
- [51]. Buchalcevova, A. (2021). *Towards higher software quality in very small entities: ISO/IEC 29110 software basic profile mapping to testing standards*. International Journal of Information Technologies and Systems Approach, 14(1), 1–16. Doi: 10.4018/IJITSA.2021010105

- [52]. Yuan, Y., Wu, X., Lu, Y., Esaki, K., Azuma, M., & Komiyama, T. (2013). Introduction of Quality Requirement and Evaluation Based on ISO/IEC SQuaRE Series of Standard. *Proceedings of the Communications in Computer and Information Science*, vol 320, 94–101. Doi: 10.1007/978-3-642-35795-4_12
- [53]. Rojas, H., Renteria, R., Duran, V. M., Gutiérrez, Y. T., Cabrera, M. J. I., & Aminuddin, A. (2025). *Mapping the Evolution and Future Directions of ISO/IEC 25010: A Bibliometric and Thematic Analysis*. *Engineering, Technology & Applied Science Research*, 15(5), 27530–27541. Doi: 10.48084/etasr.11772

EVIDENCIAS DE SUMISION



 **TEM Journal** a través de gmail.com
para mí ▼

vie, 23 ene, 2:01 ☆ 😊 ↩ ⋮

 Parece que este mensaje está en inglés 
[Traducir al español](#)

Dear Nemias Saboya,

We would like to inform you that we have received your manuscript and forwarded it to the reviewers.
Thank you for sending.

If your paper passes review processes and meets our standards it is necessary to fulfill the payment.

Publication fee - covers: publishing, review and databases indexing costs: 1200 USD
<https://www.temjournal.com/oa/oa.html>

Please confirm that you will meet the payment APC., if your paper got accepted.

*The authors should ensure that they have written entirely original papers, and if the authors have used the work and/or words of other authors/references then this has to be appropriately cited or quoted.
Manuscripts submitted must not have been published as copyrighted material elsewhere. Manuscripts under review by the Journal should not be submitted for consideration by other publications or conferences as copyrighted material.
Plagiarism in all its forms constitutes unethical publishing behavior and is unacceptable.
We are using professional tools to prevent plagiarism.*



"AÑO DEL BICENTENARIO, DE LA CONSOLIDACIÓN DE NUESTRA INDEPENDENCIA, Y DE LA CONMEMORACIÓN DE LAS HEROICAS BATALLAS DE JUNÍN Y AYACUCHO"

RESOLUCIÓN N° 0065-2024/UPeU-FIA-CF-T

Lima, Ñaña 20 de febrero de 2024

VISTO:

El expediente de **Jesús Alberto Abanto Cruz**, identificado(a) con Código Universitario N° 201323408, **Jose Luis Cardenas Garcia**, identificado(a) con Código Universitario N° 201420299 y **Robinsón Genaro Espinal Asenjo**, identificado(a) con Código Universitario N° 200610079, de la Escuela Profesional de Ingeniería de Sistemas de la Facultad de Ingeniería y Arquitectura de la Universidad Peruana Unión;

CONSIDERANDO

Que la Universidad Peruana Unión tiene autonomía académica, administrativa y normativa, dentro del ámbito establecido por la Ley Universitaria N° 30220 y el Estatuto de la Universidad;

Que la Facultad de Ingeniería y Arquitectura de la Universidad Peruana Unión, mediante sus reglamentos académicos y administrativos, ha establecido las formas y procedimientos para la aprobación e inscripción del perfil de proyecto de tesis en formato artículo y la designación o nombramiento del asesor para la obtención del título profesional;

Que **Jesús Alberto Abanto Cruz**, **Jose Luis Cardenas Garcia** y **Robinsón Genaro Espinal Asenjo**, han solicitado: la inscripción del perfil de proyecto de tesis titulado "Evaluación de la calidad de plataformas e-learning: un modelo basado en las normas ISO/IEC 25000" y la designación del Asesor, encargado de orientar y asesorar la ejecución del perfil de proyecto de tesis en formato artículo;

Estando a lo acordado en la sesión del Consejo de la Facultad de Ingeniería y Arquitectura de la Universidad Peruana Unión, celebrada el 20 de febrero de 2024, y en aplicación del Estatuto y el Reglamento General de Investigación de la Universidad;

SE RESUELVE:

Aprobar el perfil de proyecto de tesis en formato artículo titulado "**Evaluación de la calidad de plataformas e-learning: un modelo basado en las normas ISO/IEC 25000**" y disponer su inscripción en el registro correspondiente, designar al (a la) **Mg. Jose Bustamante Romero** como ASESOR para que oriente y asesore la ejecución del perfil de proyecto de tesis en formato artículo el cual fue dictaminado por: **Mg. Nemias Saboya Rios** y **Mg. Danny Lévano Rodriguez**, otorgándoles un plazo máximo de doce (12) meses para la ejecución.

Regístrese, comuníquese y archívese.




Dra. Erika Inés Acuña Salinas
DECANA




Mg. Ketty Magaly Arellano Lino
SECRETARIA ACADÉMICA

cc:

- Interesado
- Asesor
- Dirección General de Investigación
- Archivo