Fecha de presentación: agosto, 2024 **Fecha de Aceptación**: septiembre, 2024 **Fecha de publicación**: octubre, 2024

33

SEGURIDAD DE LA INFORMACIÓN EN UNA PLATAFORMA DE GESTIÓN DEL APRENDIZAJE (LMS) A NIVEL UNIVERSITARIO: ESTUDIO DE CASO ECUADOR

INFORMATION SECURITY IN A LEARNING MANAGEMENT PLATFORM (LMS) AT THE UNIVERSITY LEVEL: CASE STUDY IN ECUADOR

Janeth Mora Secaira[1]
E-mail: jmora@uteq.edu.ec
ORCID: https://orcid.org/0000-0001-9405-2028
Raúl Díaz Ocampo[1]
E-mail: rdiaz@uteq.edu.ec
ORCID: https://orcid.org/0000-0002-8264-8614
Eduardo Samaniego Mena[1]
E-mail: esamaniego@uteq.edu.ec
ORCID: https://orcid.org/0000-0002-6196-2014
Francisco de Paula Rodríguez Miranda[2]
E-mail: francisco.paula@dedu.uhu.es
ORCID: https://orcid.org/0000-0002-8167-8811
[1] Universidad Técnica Estatal de Quevedo. Ecuador.
[2] Universidad de Huelva. España.
*Autor para correspondencia

Cita sugerida (APA, séptima edición)

Mora Secaira, J., Díaz Ocampo, R., Samaniego Mena, E., y Rodríguez Miranda, F. P. de. (2024). Information Security in a Learning Management Platform (LMS) at the University Level: Case Study in Ecuador. ***Revista Conrado, 20***(S1), 276-286.

RESUMEN

El avance de la tecnología ha puesto al servicio de la educación las plataformas virtuales LMS, basadas en un software para gestionar el aprendizaje, que se constituyen en espacios virtuales para la mejora de los procesos académicos en las instituciones educativas, incluidas las de educación superior. El objetivo principal de la presente investigación es analizar la seguridad de la información en la plataforma LMS, implementada en la carrera de Telemática de la Universidad Técnica Estatal de Quevedo (Ecuador), en función de los principios de disponibilidad, integridad y confidencialidad. Para llevar a cabo este análisis, se aplicaron los principios de la seguridad de la información, se recopiló un conjunto de datos relevantes a partir de fuentes primarias y secundarias, incluyendo encuestas, entrevistas y revisiones documentales. Se realizó un análisis de confiabilidad de las preguntas formuladas a los usuarios de la plataforma. En términos de disponibilidad, la plataforma LMS analizada cumple con las expectativas de los usuarios, asegurando que los sistemas estén operativos y accesibles cuando se necesiten. La evaluación de la integridad de los datos en la plataforma LMS muestra resultados relativamente positivos. Uno de los hallazgos más preocupantes del estudio es la percepción de baja confidencialidad entre los estudiantes. Este aspecto se refiere a la protección de la información contra accesos no autorizados y es esencial para garantizar que los datos sensibles de los usuarios, tales como calificaciones, información personal y actividades académicas, se mantengan privados. Otro hallazgo relevante es la percepción generalizada de la falta de capacitación en seguridad informática entre los usuarios de la plataforma LMS. Esta carencia puede tener un impacto directo en todos los principios de seguridad de la información. Los resultados de este estudio subrayan la necesidad de mejorar la confidencialidad y la capacitación en seguridad informática dentro de la plataforma LMS universitaria. Se recomienda mejorar la capacitación en seguridad informática, implementar y comunicar políticas de privacidad más robustas y fortalecer las medidas de integridad y disponibilidad. La implementación de las recomendaciones propuestas y el compromiso continuo con la mejora de la seguridad de la información serán fundamentales para asegurar que la plataforma continúe apoyando de manera efectiva las necesidades educativas y administrativas de la institución.

Palabras clave:

Plataforma LMS, educación superior, seguridad de la información, vulnerabilidades.

ABSTRACT

The advancement of technology has put LMS virtual platforms at the service of education, based on software to manage learning, which constitute virtual spaces for the improvement of academic processes in educational institutions, including higher education institutions. The main objective of this research is to analyze the security of information in the LMS platform, implemented in the Telematics degree at the State Technical University of Quevedo (Ecuador), based on the principles of availability, integrity and confidentiality. To carry out this analysis, the principles of information security were applied, a set of relevant data was collected from primary and secondary sources, including surveys, interviews and documentary reviews. A reliability analysis was carried out on the questions asked to the users of the platform. In terms of availability, the analyzed LMS platform meets user expectations, ensuring that the systems are operational and accessible when needed. The evaluation of data integrity in the LMS platform shows relatively positive results. One of the most worrying findings of the study is the perception of low confidentiality among students. This aspect refers to the protection of information from unauthorized access and is essential to ensure that sensitive user data, such as grades, personal information and academic activities, is kept private. Another relevant finding is the widespread perception of the lack of computer security training among users of the LMS platform. This lack can have a direct impact on all information security principales. The results of this study highlight the need to improve confidentiality and cybersecurity training within the university LMS platform. t is recommended to improve computer security training, implement and communicate more robust privacy policies, and strengthen integrity and availability measures. Implementation of the proposed recommendations and continued commitment to improving information security will be critical to ensuring that the platform continues to effectively support the educational and administrative needs of the institution

Keywords:

LMS platform, higher education, computer security, vulnerabilities.

Introducción

En la era digital contemporánea, el ámbito educativo universitario ha experimentado una transformación profunda impulsada por el uso de tecnologías de la información y la comunicación (TIC) (Cedeño et al., 2023). Uno de los pilares fundamentales de esta transformación es la adopción generalizada de los LMS, en instituciones educativas de todo el mundo (Gil-Jaurena y Domínguez Figaredo, 2012). La seguridad en las plataformas LMS a nivel universitario es un tema de creciente importancia en la era digital, según la ISO/IEC (2016), la SI se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada (Valencia-Duque y Orozco-Alzate, 2017).

Las plataformas LMS son herramientas clave en la ES, pero deben proteger la información de docentes y estudiantes, y funcionar sin interrupciones, la seguridad, la privacidad y la continuidad del servicio son pilares fundamentales para la efectividad de las LMS en la ES (Ñustes-Bermudez y Orjuela-Supelano, 2021).

La transformación tecnológica en la ES ha traído consigo una serie de beneficios, pero también ha presentado desafíos importantes. Uno de los más relevantes es la seguridad de las plataformas LMS. Es fundamental comprender y abordar este tema, ya que afecta directamente a la integridad de los recursos educativos, la disponibilidad de los servicios y la confidencialidad de la información de estudiantes y docentes (Tejena, 2018). En este sentido, este trabajo se propone explorar los fundamentos teóricos y la importancia práctica de abordar la seguridad en las plataformas LMS, en consonancia con los principios de integralidad, disponibilidad y confidencialidad.

La evaluación de la seguridad de una plataforma de LMS a nivel universitario es un tema de gran relevancia en la ES, sin embargo, este entorno digital también presenta riesgos importantes para la seguridad de la información, la privacidad de los usuarios y la continuidad del servicio.

En la literatura científica, se han propuesto diversos enfoques y autores que abordan este tema de manera exhaustiva. Es necesaria la generación de instrumentos para validación de los criterios de evaluación de la seguridad a los diferentes usuarios principales del LMS: estudiantes, profesores de la carrera de Telemática y administradores de la plataforma. Los criterios de valoración son diferentes según el perfil del usuario que se consulte.

Por otra parte, se han realizado estudios con diversos enfoques que consideran la seguridad de las plataformas LMS, centrados en la identificación de amenazas, la evaluación de vulnerabilidades y la implementación de contramedidas efectivas.

Para las plataformas educativas existen riesgos y amenazas (Tabla 1) a los que se han expuesto en los últimos años, las principales amenazas y la descripción que esta tiene son: violación de confidencialidad y de integridad,

denegación de servicio, uso ilegítimo, repudio, enmascaramiento, análisis de tráfico, ataque de fuerza bruta (Pillajo y Avila, 2023).

Tabla 1. Principales amenazas en plataformas educativas LMS.

Principales Amenazas	Descripción
Violación de Confidencialidad	Una parte no autorizada que obtiene acceso a los activos alojados en el sistema de e-learning.
Violación de integridad	Una parte no autorizada que accede y se apropia de un activo utilizado en el sistema de e-learning.
Denegación de Servicio	Prevención de derechos de acceso legítimos al interrumpir el tráfico durante Transacciones entre los usuarios del sistema E-Learning.
Uso ilegítimo	Explotación de privilegios por parte de usuarios legítimos.
Programa malicioso	Líneas de código para dañar otros programas.
Repudio	Negación de la participación de uno de los participantes en la plataforma E-Learning en cualquier transacción de documentos.
Enmascaramiento	Una forma de comportamiento que esconde la identidad de los hackers.
Análisis de tráfico	Fuga de información al abusar del canal de comunicación.
Ataque de fuerza bruta	Un intento con todas las combinaciones posibles para descubrir lo correcto, en este caso las claves de acceso a la plataforma E-Learning.

Fuente: Guzmán et al. (2018).

La evaluación de la seguridad en plataformas LMS a nivel universitario es un campo multidisciplinario que abarca la identificación de amenazas, la evaluación de vulnerabilidades, la gestión de riesgos, el cumplimiento normativo y la implementación de prácticas de seguridad efectivas.

Los LMS, albergan una amplia gama de funciones que van desde la facilidad de uso y la experiencia del usuario hasta la eficacia pedagógica y la seguridad. Evaluar la seguridad en estas plataformas implica considerar todas estas dimensiones de manera integral. Al comprender y aplicar teorías relacionadas con cada una de estas dimensiones, podemos mejorar continuamente los LMS y optimizar su papel en el proceso de enseñanza-aprendizaje (Ramírez León, 2016).

La relevancia de la seguridad en los LMS a nivel universitario es multifacética y se la aborda en términos de los principios de seguridad de la información: disponibilidad, integridad y confidencialidad en dichas plataformas.

Tres de los conceptos principales en seguridad de la información son precisamente la confidencialidad, integridad y disponibilidad, comúnmente conocida como la tríada de la seguridad de la información. La tríada de la CIA, que ha sido utilizada por más de 20 años, brinda un modelo mediante el cual podemos pensar y discutir conceptos de seguridad, y tiende a centrarse mucho en la seguridad de los datos (Vega Briceño, 2021).

- Disponibilidad: Asegurando que los usuarios autorizados tienen el acceso debido a la información es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones (Chilán y Pionce, 2017).
- Integridad: Se refiere a los datos que sean consistentes con lo que se ha registrado o provisto por los dueños de ellos. Cuando hay una alteración o modificación por personas o procesos no autorizados se ha perdido la integridad, esto tiende a ser lo más grave (Tejenas, 2018).
- Confidencialidad: Asegurando que sólo quienes estén autorizados, pueden acceder a la información, es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados (Chilán y Pionce, 2017).

La confidencialidad puede verse comprometida por la pérdida de una computadora portátil que contiene datos confidenciales, una persona que mira por encima del hombro mientras escribimos una contraseña, envío de archivos adjuntos de correo electrónico a la persona equivocada, un atacante que penetra en nuestros sistemas o infraestructura por medio de aplicaciones MITM (Man in The Middle) (Tchernykh et al., 2019).

Autores como Alarcón et al. (2016), han subrayado la importancia de implementar políticas de privacidad y mecanismos de anonimización de datos para para solucionar de manera segura las amenazas o fallos informáticos que perjudican la integridad de la información y que no se altere la confidencialidad de los datos en el sistema.

A pesar de su potencial para mejorar la ES, las plataformas LMS también presentan vulnerabilidades considerables que pueden ser explotadas por actores maliciosos, estas vulnerabilidades van desde ataques dirigidos a la integridad de los contenidos académicos hasta la exposición de datos confidenciales de estudiantes y docentes. En este sentido, resulta crucial destacar algunos de los riesgos y desafíos específicos que enfrentan las instituciones universitarias: Ataques de integridad, amenazas a la disponibilidad y violación de la confidencialidad.

Para abordar eficazmente estos riesgos y desafíos, es fundamental comprender los fundamentos teóricos de la seguridad de las plataformas LMS.

Autenticación y Autorización: La autenticación se refiere a la verificación de la identidad de un usuario **«¿Eres quien dices ser?»**, mientras que la autorización **«¿Qué puedes hacer una vez que estás dentro?», ósea se** determina qué acciones o recursos específicos tiene permiso para realizar o acceder (Castillo Gutiérrez, 2018). Estos conceptos son esenciales para garantizar que solo usuarios autorizados tengan acceso a determinadas funciones y datos en el LMS.

Cifrado de Datos: El cifrado es una técnica que protege la confidencialidad de la información mediante la conversión de datos en un formato ilegible que solo puede descifrarse con la clave correcta (Stallings, 1994).

Gestión de Identidad y Acceso: La gestión de identidad y acceso se refiere a los procesos y tecnologías utilizados para administrar y controlar las identidades de los usuarios y su acceso a los recursos en línea (Pineda Guerrero, 2019). Esto incluye la gestión de contraseñas, la autenticación de dos factores y la revisión periódica de privilegios.

Monitoreo y Detección de Amenazas: El monitoreo constante de la plataforma LMS es esencial para detectar y responder rápidamente a amenazas y anomalías (Carriazo Regino, 2021). Las técnicas de análisis de registros (logs) y la implementación de sistemas de detección de intrusiones son prácticas recomendadas en este contexto.

Los profesores son actores fundamentales en el contexto de la seguridad de la información en un LMS universitario. Su rol abarca la creación y gestión de contenidos educativos, la evaluación de los estudiantes y la interacción pedagógica en línea. Desde una perspectiva de seguridad, los profesores deben ser conscientes de las políticas y procedimientos de seguridad establecidos por la institución y seguir buenas prácticas al crear y compartir materiales didácticos. Esto incluye el uso responsable de contraseñas seguras y la protección de su propia cuenta, ya que su compromiso con la seguridad puede influir en la integridad de los recursos educativos.

Los estudiantes, como usuarios finales de la plataforma LMS, desempeñan un papel central en la seguridad de la información. Su interacción con la plataforma implica el acceso a contenidos educativos, la presentación de trabajos, la realización de exámenes y la comunicación con profesores y compañeros. Para garantizar la seguridad de la información, los estudiantes deben cumplir con las políticas de seguridad establecidas por la institución, lo que incluye el uso adecuado de contraseñas y la protección de sus credenciales de acceso.

Los administradores del sistema desempeñan un papel crítico en la implementación y gestión de la seguridad de la plataforma LMS. Son responsables de configurar y mantener la infraestructura tecnológica subyacente, lo que incluye servidores, bases de datos y sistemas de autenticación. Su conocimiento en seguridad informática es esencial para garantizar que la plataforma esté protegida contra vulnerabilidades técnicas y ataques cibernéticos.

La relación entre estos actores en el contexto de la seguridad de la información en un LMS es interdependiente. Los profesores y estudiantes dependen de la infraestructura segura proporcionada por los administradores del sistema para acceder y utilizar la plataforma de manera confiable. A su vez, los profesores y estudiantes tienen la responsabilidad de seguir las prácticas de seguridad recomendadas y reportar cualquier actividad sospechosa, contribuyendo así a la protección de la información académica y la continuidad de la educación en línea.

Sobre la base de lo expuesto, se justifica plenamente para evaluar y analizar la seguridad de una plataforma LMS utilizada por una institución universitaria en Ecuador, con un enfoque en los principios de confidencialidad, integridad y disponibilidad, con el fin de identificar las vulnerabilidades existentes y proponer mejoras en las medidas de seguridad, con un enfoque en los principios de seguridad de la información.

MATERIALES Y MÉTODOS

La metodología se basa en un enfoque exploratorio, se utilizan técnicas de muestreo por relación con la temática del estudio, para analizar la seguridad de una plataforma LMS, considerando los aspectos de integridad,

confidencialidad y disponibilidad, con el objetivo de abordar los criterios de seguridad d la información de un sistema LMS, en el contexto universitario. La muestra quedó constituida por 265 estudiantes y 22 profesores de la carrera de Telemática de la UTEQ y 6 administradores de la plataforma SGA.

Se diseñaron cuestionarios específicos para recopilar datos cuantitativos de usuarios de la plataforma LMS, evaluando aspectos relacionados con los principios de integridad, confidencialidad y disponibilidad. Se aplicaron pruebas de confiabilidad mediante el estadístico Alfa de Cronbach (Tabla 2).

Tabla 2. Preguntas sobre seguridad de la información LMS.

Principios de seguridad	Preguntas
Integridad	20
Confidencialidad	10
Disponibilidad	23
Total de Preguntas	52

Fuente: Elaboración de autores

Se realizaron entrevistas en profundidad con los administradores de la plataforma SGA - UTEQ y expertos en tecnología educativa de la UTEQ, para obtener datos cualitativos sobre el soporte técnico y principios de seguridad en la plataforma LMS.

Se examinaron documentos relevantes, como políticas institucionales y datos de desempeño de la plataforma LMS, para complementar la recopilación de datos. Los datos recopilados se sometieron a un análisis exhaustivo utilizando técnicas estadísticas y análisis de contenido para valorar la percepción de los usuarios en relación a la aplicación de los principios de la seguridad de la información (Tabla 3).

Tabla 3. Preguntas planteadas a los usuarios de la plataforma SGA sobre la aplicación de los principios de la seguridad de la información.

Pri.	Enunciado de pregunta	Preg.	Usu.
INTEGRIDAD	¿Se implementa un proceso de verificación de la identidad de los alumnos durante el registro?	IPE2	ESTUDIANTES
	¿Existen políticas de contraseñas seguras y su renovación es periódica?	IPE3	
	¿La plataforma registra y audita las actividades de inicio de sesión de los alumnos?	IPE4	
	¿Existen restricciones de acceso a los datos y recursos de los alumnos basadas en roles?	IPE10	
	¿La plataforma notifica a los alumnos de cualquier violación de seguridad que afecte sus datos personales?	IPE13	
	¿Considera que su información personal, como datos de contacto y registros académicos, está segura en la plataforma?	IPE15	
	¿La plataforma realiza evaluaciones de seguridad periódicas y auditorías externas por terceros independientes?	IPE16	
	¿Existen políticas de contraseñas seguras y su renovación periódica para las cuentas de los profesores?	IPP4	PROFESORES
	¿La plataforma registra y audita las actividades de inicio de sesión de los profesores?	IPP5	
	¿Existe un protocolo para la gestión segura de archivos y documentos compartidos por los profesores?	IPP7	
	¿La plataforma cuenta con un sistema de alerta temprana para detectar actividades inusuales en las cuentas de los profesores?	IPP10	
	¿Se lleva un registro de cambios en los cursos y contenidos creados por los profesores?	IPP11	
	¿Existe una política de retención de datos para los contenidos de los cursos, y se cumple de manera consistente?	IPP13	
	¿La plataforma ofrece herramientas de cifrado para proteger la integridad de los datos de los cursos?	IPP14	
	¿Se aplican políticas de acceso basado en roles para los administradores del sistema?	IPA2	ADMINISTRADOR SGA
	¿Se realizan auditorías de seguridad regulares en la infraestructura de la plataforma?	IPA3	
	¿Existe un proceso para gestionar de manera segura las credenciales de administración?	IPA7	
	¿La plataforma tiene una política de gestión de contraseñas fuertes y requiere su cambio periódico?	IPA11	
	¿Se realizan análisis de riesgos y evaluaciones de seguridad regulares?	IPA13	
	¿La plataforma realiza revisiones periódicas de cumplimiento con normalidad?	IPA19	

CONFIDENCIALIDAD	¿Se realizan pruebas de vulnerabilidades y análisis de seguridad de manera regular en la plataforma?	CPE7	ESTUDIANTES
	¿Los alumnos pueden reportar incidentes de seguridad de forma anónima?	CPE8	
	¿Los alumnos pueden revisar un registro de acceso a sus propios datos y actividades?	CPE11	
	¿Los profesores pueden denunciar problemas de seguridad de manera confidencial?	CPP9	PROFESORES
	¿Se realiza una revisión periódica de las cuentas de los profesores para eliminar el acceso no autorizado?	CPP17	
	¿Se realizan pruebas de penetración de manera periódica en la plataforma?	CPA5	ADMINISTRADOR SGA
	¿Se establecen y siguen políticas de optimización de la información para garantizar la privacidad y seguridad de la información almacenada en la plataforma?	CPA10	
	¿Los administradores del sistema reciben notificaciones de intentos de acceso no autorizados?	CPA15	
	¿Se ha establecido una comunicación y coordinación efectiva con las autoridades de seguridad cibernética locales o nacionales?	CPA16	
	¿Se documentan y evalúan los incidentes de seguridad para mejorar la postura de seguridad?	CPA17	
DISPONIBILIDAD	¿La plataforma educativa requiere autenticación para el acceso de los alumnos?	DPE1	ESTUDIANTES
	¿La plataforma educa a los alumnos sobre la importancia de proteger su información personal?	DPE6	
	¿La plataforma educa a los alumnos sobre el phishing y cómo identificar correos electrónicos maliciosos?	DPE9	
	¿Se realizan copias de seguridad regulares y pruebas de restauración de datos en la plataforma?	DPE12	
	¿La plataforma le permite exportar sus datos personales y académicos en un formato legible y transferible?	DPE14	
	¿Los profesores tienen acceso seguro a funciones de administración y gestión de cursos?	DPP1	PRFESORES
	¿La plataforma educativa requiere autenticación para el acceso de los profesores?	DPP2	
	¿La plataforma limita el acceso de los profesores a datos sensibles de los alumnos?	DPP3	
	¿Se proporciona capacitación en seguridad de datos a los profesores?	DPP6	
	¿La plataforma permite a los profesores realizar copias de seguridad de los datos de sus cursos?	DPP8	
	¿Los profesores tienen la capacidad de revocar el acceso a su contenido compartido con otros usuarios?	DPP12	
	¿Los profesores reciben notificaciones de cualquier actividad sospechosa en sus cuentas?	DPP15	
	¿La plataforma impone límites de ancho de banda y almacenamiento para evitar abusos o ataques DDoS?	DPP16	
	¿El equipo de administración del sistema tiene un proceso de autenticación segura?	DPA1	ADMINISTRADOR SGA
	¿Existe un plan de respuesta a incidentes de seguridad claramente definido y probado?	DPA4	
	¿Se mantienen actualizados y se aplican parches de seguridad en todos los componentes del sistema?	DPA6	
	¿Se implementa un control de acceso riguroso a los servidores y sistemas críticos?	DPA8	
	¿El equipo de administración recibe formación en seguridad de la información?	DPA9	
	¿Se utilizan sistemas de monitoreo de seguridad para detectar amenazas en tiempo real?	DPA12	
	¿La plataforma tiene una política de acceso mínimo necesario para limitar los privilegios de administración?	DPA14	
	¿Existe un plan de continuidad del negocio y recuperación ante desastres?	DPA18	
	¿Se realizan actualizaciones periódicas a nivel de infraestructura y aplicativos?	DPA20	

Fuente: Elaboración de autores

RESULTADOS Y DISCUSIÓN

La fiabilidad de la consistencia interna de las puntuaciones de la encuesta de satisfacción de los usuarios con la plataforma SGA, se estimó mediante el coeficiente Alfa de Cronbach, basado en el promedio de la correlación entre los ítems, habiéndose obtenido un valor de 0,90, lo que refleja la confiabilidad de las preguntas planteadas (Tabla 4).

Tabla 4: Alfa Cronbach.

Estadísticas de fiabilidad		
Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de preguntas
0,90	0,90	52

Fuente: Elaboración de autores

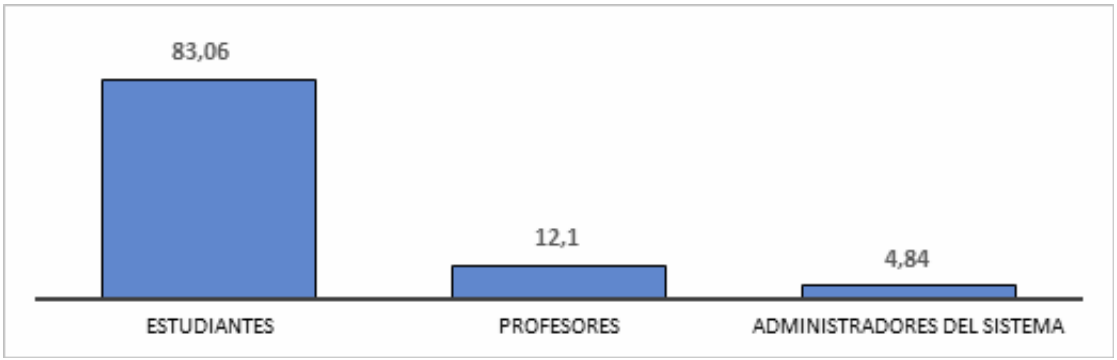
Tabla 5: Estadística descriptiva.

	Media	Desviación Típica
Total	4,11	0,96

Fuente: Elaboración de autores

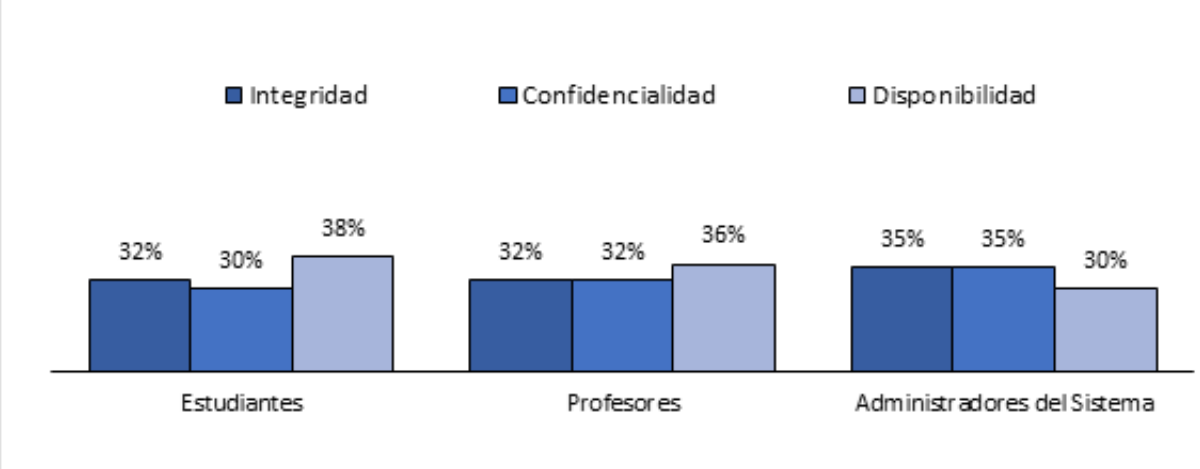
En la Tabla 5, se observa el resumen descriptivo sobre la percepción de los usuarios (estudiantes, profesores y administradores del sistema) sobre la plataforma SGA, en donde la valoración media es de 4,11, que refleja un alto de nivel de satisfacción de los usuarios, mientras que la desviación típica es 0,96, que indica que las respuestas están agrupadas cerca de la media (Figura 1).

Figura 1. Usuarios involucrados (porcentaje) en la evaluación de la seguridad de la información en la plataforma SGA.



Fuente: Elaboración de autores

Fig. 2. Percepción de los usuarios sobre los principios de seguridad de la información en la plataforma SGA



Fuente: Elaboración de autores

En la Figura 2, se observa la percepción promedio de los diferentes usuarios al utilizar la plataforma del SGA. Todos los usuarios perciben como muy satisfactoria la aplicación del principio de disponibilidad, mientras que la integridad

es considerada satisfactoria para estudiantes y profesores y los administradores la perciben como altamente satisfactoria. Por otra parte, los estudiantes muestran su preocupación por la confidencialidad con una baja valoración a este principio.

Fig. 3. Percepción de los estudiantes sobre la seguridad de la información de la plataforma SGA.

Fuente: Elaboración de autores

En la Figura 3, se observa que los estudiantes en relación al principio de disponibilidad, asignan una alta valoración al proceso de autenticación en la plataforma del SGA (DPE1), seguido por la exportación de datos personales y académicos en un formato legible y transferible (DPE14), mientras que se muestra una baja valoración de los procesos de capacitación sobre phishing y correos

) y una valoración electrónicos maliciosos (DPE9).

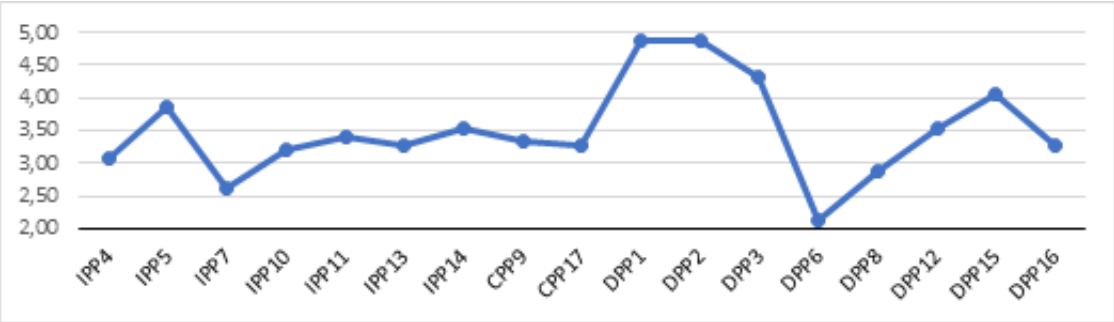
En el caso del principio de integridad, se asigna una alta valoración al proceso de verificación de la identidad durante el registro (IPE2media a la recepción por los usuarios de notificaciones de eventos que podrían afectar la seguridad de los datos personales (IPE13).

Por otra parte, los estudiantes asignan una valoración baja a la confidencialidad de la plataforma, en el registro de acceso a sus propios datos y actividades (CPE11).

Los usuarios que no están bien informados sobre las mejores prácticas de seguridad, como la gestión de contraseñas y el reconocimiento de intentos de phishing, son más propensos a comprometer la confidencialidad de sus datos (Caputo et al., 2013).

La carencia de comunicación efectiva sobre cómo se gestionan y protegen los datos puede llevar a los estudiantes a dudar de la seguridad de la plataforma (Brown y Klein, 2020).

Fig. 4. Percepción de los profesores sobre la seguridad de la información del SGA.



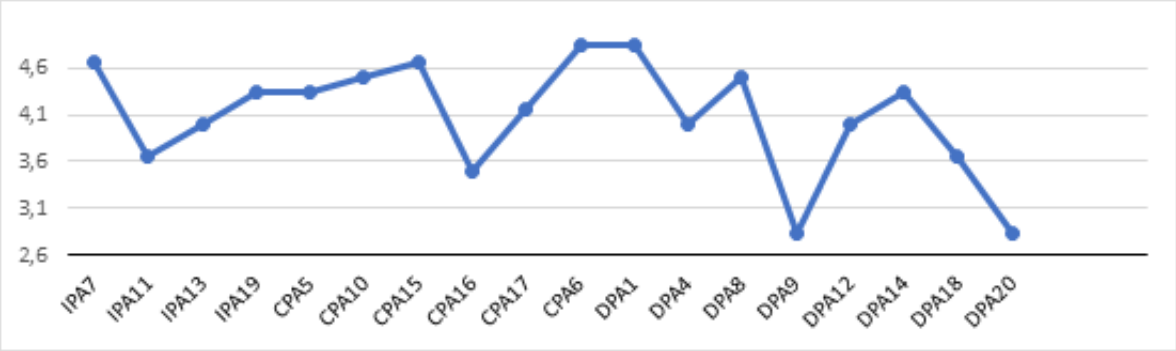
Fuente: Elaboración de autores

En la Figura 4, en el caso del principio de disponibilidad, se muestra que los profesores asignan una alta valoración, al acceso seguro a funciones de administración, gestión de cursos y procesos de autenticación en la plataforma del SGA (DPP1 y DPP2), respectivamente. Por otra parte, enfatiza en la falta de capacitación en seguridad de la información (DPP6).

En relación al principio de integridad, tiene una alta valoración el registro y auditoria de actividades de inicio de sesión (IPP5), pero se le asigna un valor bajo a la gestión de archivos y documentos compartidos (IPP7); Además, se observa una limitada confidencialidad en la documentación y evaluación de los incidentes de seguridad informática (CPP17).

La seguridad, la protección de datos y la privacidad son cuestiones para valorar seriamente; especialmente en el caso de aplicaciones externas no implementadas en la universidad (Grande de Prado et al., 2021).

Fig. 5. Percepción de los administradores del sistema sobre la seguridad de la información del SGA.



Fuente: Elaboración de autores

En la Figura 5, los administradores en relación al principio de disponibilidad, asignan una alta valoración al proceso de autenticación (DPA1 y DPA14), pero le conceden un valor muy bajo a la política de acceso mínimo necesario (DPA9 y DPA20), lo cual refleja una escasa capacitación en seguridad de la información y poca actualización a nivel de infraestructura y aplicativos. La falta de capacitación puede resultar en una manipulación accidental o maliciosa de los datos. La integridad asegura que la información se mantenga completa y sin alteraciones no autorizadas (Stallings y Brown, 2015).

Por otra parte, la falta de políticas claras y estrictas puede generar desconfianza entre los usuarios. Estudios recientes señalan que las plataformas educativas deben implementar políticas robustas y transparentes para manejar los datos personales de manera adecuada (Chang, 2021).

En el caso del principio de integridad, los administradores atribuyen una alta valoración al proceso para gestionar las credenciales de manera segura, con una política de gestión de contraseñas fuertes, pero con limitados cambios periódicos (IPA7).

Por otra parte, los administradores en relación al principio de confidencialidad, valoran como baja la coordinación con los organismos de seguridad de la información a nivel local y nacional (CPA16).

CONCLUSIONES

El presente estudio exploratorio ha permitido analizar la seguridad de la información en la plataforma virtual de gestión académica de la UTEQ (Ecuador), considerando los principios fundamentales de confidencialidad, integridad y disponibilidad. Mediante encuestas dirigidas a profesores, estudiantes y administradores de la plataforma, se han obtenido datos valiosos que arrojan luz sobre el estado actual de la seguridad en el sistema y proporcionan una base sólida para futuras mejoras.

La percepción de los estudiantes sobre la confidencialidad es la más baja, lo que sugiere la necesidad de mejorar las políticas de acceso y autenticación, así como la educación y concienciación sobre buenas prácticas de seguridad.

Mientras que la mayoría de los administradores confían en los mecanismos de integridad del sistema, los estudiantes y profesores expresaron ciertas preocupaciones.

Las preocupaciones principales incluyen la posible manipulación de notas y registros académicos. Reforzar los controles de acceso y auditorías regulares puede aumentar la confianza en la integridad del sistema.

La mayoría de los usuarios expresaron confianza en la disponibilidad del sistema, pero señalaron que las interrupciones ocasionales impactan negativamente en la

experiencia educativa. Mejorar la infraestructura técnica e implementar y establecer planes de contingencia sólidos son recomendaciones clave para aumentar la disponibilidad. Por otra parte, es necesario implementar programas de formación para estudiantes y profesores sobre buenas prácticas de seguridad puede mejorar significativamente la percepción y realidad de la confidencialidad y la integridad.

Por otra parte, es crucial revisar y actualizar las políticas de seguridad regularmente para asegurarse de que estén alineadas con las mejores prácticas y los estándares internacionales. Aunque la plataforma virtual sistema de gestión académica SGA de la UTEQ, presenta un nivel adecuado de seguridad en términos de confidencialidad, integridad y disponibilidad, existen áreas clave que requieren atención y mejora.

REFERENCIAS BIBLIOGRÁFICAS

Alarcón Salvatierra, P., Barriga Díaz, R., Picón Fara, C., y Alarcón, J. (2016). La importancia de la seguridad informática en las instituciones gubernamentales (Ecuador). Revista Caribeña de Ciencias Sociales**.** https://www.eumed.net/rev/caribe/2016/11/seguridad.html

Brown, M. y Klein, C. (2020). Whose data? Which rights? Whose power? A policy discourse analysis of student privacy policy documents. ***The Journal of Higher Education, 91***(7), 1149-1178. https://ideas.repec.org/a/taf/uhejxx/v91y2020i7p1149-1178.html

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., y Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. ***Journals & Magazines, 12***(1), 28-38. https://www.cybsafe.com/research-library/going-spear-phishing-exploring-embedded-training-and-awareness/

Carriazo Regino, Y. P. (2021). ***Sistema de monitoreo de la calidad del agua basado en IOT, utilizando técnicas de analítica de datos para la detección de anomalías, en los acueductos ejecutados por el plan departamental de aguas (PDA) de Córdoba***. [Tesis de maestría. Universidad Autónoma de Bucaramanga].

Castillo Gutiérrez, M. A. (2018). ***Diseño e implementación de una estrategia de seguridad mediante políticas de autenticación y autorización para una empresa de seguros***. [Tesis de maestría. Universidad de Chile].

Cedeño, R. J., Vásquez, P., y Maldonado, I. (2023). Impacto de las Tecnologías de la Información y la Comunicación (TIC) en el Rendimiento Académico: Una Revisión Sistemática de la Literatura. ***Revista Multidisciplinar Ciencia Latina, 7***(4), 10297-10316. https://cienciala tina.org/index.php/cienciala/article/view/7732

Chang, B. (2021). Student privacy issues in online learning environments. ***Distance Education, 42***(1). https://www.tandfonline.com/doi/full/10.1080/01587919.2020.1869527

Chilán-Santana, E. I. y Pionce-Pico, W. F. (2017). Apuntes teóricos introductorios sobre la seguridad de la información. ***Dominio De Las Ciencias***, ***3***(4), 284–295. https://doi.org/10.23857/dc.v3i4.686

Gil-Jaurena, I. y Domínguez Figaredo, D. D. (2012). Open Social Learning y Educación Superior: Oportunidades y Retos (Open Social Learning and Higher Education; Opportunities and Challenges. ***Revista Iberoamericana de Educación, 60***(1), 191-203**.** https://rieoei.org/historico/documentos/rie60a12.htm

Grande de Prado, M., García-Peñalvo, F. J., Corell, A., & Abella García, V. (2021). Evaluación en Educación Superior durante la pandemia de la COVID-19. ***Campus Vituales, 1***(10), 49-58. http://uajournals.com/ojs/index.php/campusvirtuales/article/view/747/

Guzmán Duque, A. P., Oliveros Contreras, D., y Mendoza García, E. M. (2018). La gestión del conocimiento, las TIC y la educación superior en el desarrollo de competencias**.** En, R Roig ***El compromiso académico y social a través de la investigación e innovación educativas en la Enseñanza Superior***. (pp. 1240-1247). Octaedro.

Ñustes-Bermúdez, C. A. y Orjuela-Supelano, E. C. (2021). ***Análisis de los riesgos y vulnerabilidades de un data center en Colombia para crear una matriz de riesgo acorde lo establecido en la norma ISO 27001: 2013***. [Trabajo de grado. Universitaria Agustiniana].

Pillajo Garcia, P. A. y Avila Pesantez, D. (2023). Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura. ***Revista Perspectivas***, ***5***(1), 19–29. https://doi.org/10.47187/perspectivas.5.1.179

Pineda Guerrero, R. D. (2019). ***Diseño de un modelo para la creación de políticas para el control de acceso basado en gobierno TI y gestión de identidades digitales en las instituciones de educación superior públicas caso de estudio Universidad del Magdalena***. [Tesis de maestría. Universidad del Norte].

Ramírez León, Y. (2016). ***Adaptación del diseño de unidades didácticas a estilos de aprendizaje en entornos virtuales de enseñanza-aprendizaje***. [Tesis doctoral. Universidad de Granada].

Stallings, W. (1994). ***Fundamentos de seguridad en redes: aplicaciones y estándares***. Pearson Educación.

Stallings, W. y Brown, L. (2015). ***Computer security: principles and practice***. Pearson.

Tchernykh, A., Schwiegelsohn, U., Talbi, E., y Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. ***Journal of Computational Science, 36,*** 100581. https://hal.science/hal-02304771/

Tejena-Macías, M. (2018). Análisis de riesgos en seguridad de la información. ***Polo del Conocimiento, 3***(4), 230-244. https://doi.org/10.23857/pc.v3i4.809

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI: ***Revista Ibérica de Sistemas e Tecnologias de Informação, 22***, 73-88. https://dialnet.unirioja.es/servlet/articulo?codigo=6672188&orden=0&info=link

Vega Briceño, E. (2021). ***Seguridad de la información***. 3 Ciencias.