Propuesta metodológica para la evaluación de la seguridad de información en software de gestión académica

Cesar Leonel Zambrano Delgado[1]
Universidad Técnica de Manabí
Email: czambrano7942@utm.edu.ec
Portoviejo, Ecuador

Alex Gregorio Mendoza-Arteaga[2]
Universidad Técnica de Manabí,
Email: alex.mendoza@utm.edu.ec
Portoviejo, Ecuador.

DOI: https://doi.org/10.56124/encriptar.v8i15.002

Resumen

La investigación surge de la necesidad de brindar una metodología que utilice una herramienta para la evaluación de la seguridad de la información en software de gestión académica. Para ello, mediante la revisión de la literatura, se realizó un análisis de metodologías, herramientas, políticas o estándares y normativas locales, con el fin de evaluar y obtener un mayor grado de madurez en la seguridad de la información, considerando todos estos estándares y normativas locales se diseñó la propuesta antes mencionada. Dicha propuesta metodológica fue sometida a validación por expertos utilizando el método Delphi. Los resultados que se obtuvieron en base a dos rondas de consultas evidencian una estabilidad, fiabilidad y consistencia de los juicios emitidos, por lo que se concluyó que la propuesta metodológica para la evaluación de la seguridad de la información en software de gestión académica es teóricamente factible para su aplicación.

Palabras clave: Seguridad de información, Software de Gestión Académica, Estándares, Grado de madurez, Método Delphi.

Methodological proposal for the evaluation of information security in academic management software

Abstract

The research arises from the need to provide a methodology that uses a tool for the evaluation of information security in academic management software. To do this, through the review of the literature, an analysis of methodologies, tools, policies or local standards and regulations was carried out, in order to evaluate and obtain a higher degree of maturity in information security, considering all these standards and local regulations the aforementioned proposal was designed. This methodological proposal was subjected to validation by experts using the Delphi method. The results obtained based on two rounds of consultations show stability, reliability and consistency of the judgments issued, so it was concluded that the methodological proposal for the evaluation of information security in academic management software is theoretically feasible. For your application.

Keywords: Information security, Academic Management Software, Standards, Degree of maturity, Delphi Method.

1. Introducción

En la vida de las personas, la inclusión de las Tecnologías de Información y Comunicación (TIC) han generado un cambio radical, la gran mayoría de la humanidad utiliza las TIC para sus propósitos personales, sin embargo, existen retos también asociados a su adopción, como por ejemplo garantizar la confidencialidad, disponibilidad e integridad de los datos cuando exista un ataque informático o cibernético, como lo indica la ISO/IEC 27001:2013 con relación a la seguridad de la información.

La seguridad de la información es un campo de estudio y práctica que se centra en proteger la confidencialidad, integridad, disponibilidad de la información. Es esencial en un mundo cada vez más digitalizado, donde la información se encuentra expuesta a amenazas constantes, como el robo de

datos, el acceso no autorizado y el sabotaje. La introducción a la seguridad de la información implica comprender los principios fundamentales y las mejores prácticas para garantizar la protección de la información sensible. Esto implica la identificación y evaluación de riesgos, la implementación de controles de seguridad, la gestión de incidentes y la concientización de los usuarios.

Gladden afirma que, la seguridad de la información, también conocida como InfoSec, está definida como la protección de la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para brindar confidencialidad, integridad y disponibilidad (Gladden, 2017).

Hoy en día con el fin de evaluar y obtener un mayor grado de madurez en la seguridad de la información, se aplican herramientas, políticas o estándares o metodologías como Manual de metodología de pruebas de seguridad de código abierto (OSSTMM), los sistemas de la Organización Internacional de Normalización Security Engineering Capability Maturity Model, la tecnología de seguridad de la información federal marco de evaluación y los Objetivos de Control para la Tecnología de la Información – COBIT que se basan en tener un punto de referencia para la comparación y como una herramienta para comprender las mejores prácticas y lograr el cumplimiento de un conjunto de requisitos con respecto a los pilares fundamentales de la seguridad de la información (Guijarro & Guerra, 2018).

En el área educativa, el Ministerio de Educación del Ecuador (MINEDUC) asocia la tecnología y el uso distintas herramientas que utilizan el internet para sus transacciones diarias, por ejemplo, se implementa Carmenta - Educar (Sistema de Gestión de Control Escolar – Educar Ecuador | Ministerio de Educación, n.d.), los sistemas web o sistemas de gestión académica (SGA)

en instituciones particulares, que responda a las normas técnicas ecuatorianas (NTE) y la Ley Orgánica de Protección de Datos vigente en nuestro país, y que en muchos establecimientos educativos son herramientas fundamentales, tanto de autoridades, docentes, representantes o padres de familia, así como de estudiantes; pero que han generado la necesidad de atender aspectos importantes como por ejemplo implementación de políticas de seguridad informática o seguridad de la información, aspectos transcendentales para evitar que puedan ser blanco de innumerables ataques informáticos o cibernéticos (Vega et al., 2022).

Según Ponemon Institute (2018), los ataques cibernéticos a las empresas son cada vez más frecuentes y difíciles de detener en todo el mundo, la extorsión cibernética o los ataques de ransomware aumentarán en frecuencia, por lo que se vuelve fundamental comprometer al personal y obtener los recursos necesarios para proteger la información como un medio de apoyo para el logro de los objetivos estratégicos de la organización (Ponemon Institute LLC, 2018).

Con respecto a dichos ataques y en lo referente a la vulneración de la seguridad de los datos personales, la Ley Orgánica de Protección de Datos Personales del Ecuador menciona que es el incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos y que las personas responsables de los bancos o archivos de datos podrán difundir la información con autorización de su titular o de la ley (LOPDP, 2021).

La confidencialidad, disponibilidad o integridad de los datos personales es parte del presente proyecto, el cual tiene como propuesta metodológica la creación de una herramienta para la evaluación de la seguridad de la información en software de gestión académica , que en la actualidad no se evidencia en nuestro país, basado en la Ley Orgánica de Datos Personales

del Ecuador y métricas que se adapten a la seguridad de la información establecidas en los tres pilares fundamentales según la ISO/IEC 27001:2013 a través de la lente del marco de seguridad cibernética (CF) del Instituto Nacional de Estándares y Tecnología (NIST) para la protección de infraestructura crítica, versión 1.1 y que el 25 de octubre de 2022, se publicó la tercera edición de la norma con cambios referenciales para abordar los desafíos de ciberseguridad global, mejorar la confianza digital y la protección de los servicios de computación en la nube debido a la tendencia del uso de esta tecnología.

Con estos antecedentes, la finalidad de este proyecto, es establecer una metodología de evaluación de los sistemas de gestión académica, basada en marcos referenciales internaciones y normativas locales, que permita conocer el estado de madurez de la seguridad de información e identificar vulnerabilidades con la finalidad de aplicar controles que permitan reducir las brechas de seguridad en los sistemas de gestión académicos en el Ecuador, debido que información que almacenan dichos sistemas es considerada como sensible por la Ley de Protección de Datos vigente en el Ecuador por tratarse de niños, jóvenes y adolescentes que se considera una categoría especial de datos.

2. Materiales y métodos

Metodológicamente este trabajo presentará una investigación descriptiva siendo el enfoque metodológico mixto. Para cumplir con la propuesta de una metodología de evaluación de seguridad de la información para los softwares de gestión académica (SGA) se definió el siguiente diseño de investigación compuesto por las fases de revisión de literatura relevante relacionada, revisión de normativas legales con privación de datos,

construcción de la metodología de evaluación de la seguridad de la información, validación de la propuesta metodología mediante juicio de expertos (Método Delphi) el cual se fundamenta en los criterios de voces autorizadas y de gran experiencia sobre el objeto de estudio en cuestión, que parte de la selección de los mejores especialistas según las competencias demostradas (Cedeño & Mena, 2022), análisis, discusión y presentación de los resultados.

2.1. Validación de la metodología

Se formaron los grupos coordinador y expertos, delegados a realizar la validación teórica de la propuesta metodológica, el grupo coordinador estuvo conformado por un PhD docente de la Universidad Técnica de Manabí, y el autor postulante a Máster de la Universidad de Técnica de Manabí. Para su conformación se tuvieron en cuenta las siguientes características: conocimiento del método Delphi, ser investigadores académicos relacionados con el tema a estudiar y tener facilidad de comunicación al trabajar conjuntamente en otros estudios. El grupo coordinador tomó la responsabilidad de escoger a los expertos, interpretar los resultados, realizar los ajustes y correcciones necesarias.

Para la selección de expertos se fijó como criterio de selección el conocimiento de los candidatos en el área de la investigación. Se identificaron veinte candidatos, de los cuales se descartaron seis por no disponer con el tiempo para la participación quedando catorce expertos a los cuales se les aplicó la metodología propuesta por el Comité Estatal para la Ciencia y la Técnica de Rusia, elaborado en 1971 y expuesta por Oñate, Ramos, y Díaz (1988), donde se determinó el coeficiente de competencia relacionado al tema de la investigación. Se aplicó la siguiente fórmula para cálculo del coeficiente de competencia: $K=½(kc+ka)$

En donde Kc es el coeficiente de conocimiento o información del experto acerca del problema, calculado sobre la autoevaluación del experto en una escala del 0 al 10 y multiplicado por 0,1. Y Ka es el coeficiente de argumentación o fundamentación de los criterios del experto, obtenido como resultado de la suma de los puntos alcanzados a partir de una tabla patrón.

Posterior a ello, se realizaron tres rondas para la validación del modelo. La ronda número uno se realizó al interior del grupo coordinador, donde se obtuvo como resultado la primera versión del cuestionario, estableciendo una escala de Likert (1932) con cinco categorías para las evaluaciones cuantitativas de cinco componentes y para la evaluación cualitativa se incluyó una pregunta abierta, donde cada experto evalúa el modelo en términos de inclusión, modificación y eliminación. Además, se incluyó una pregunta para recoger la valoración de la Relevancia, Pertinencia y Coherencia.

Con el objetivo de obtener los criterios cuantitativos y cualitativos estables, el cuestionario fue sometido a dos rondas de valoración por los expertos, para lo cual fue necesario implementar el cuestionario en un formulario de Google para luego ser enviado por correo electrónico a los expertos, estableciendo un plazo máximo de respuesta de 10 días, para que se garantice el anonimato de los expertos se le asignaron códigos.

Los resultados obtenidos en las dos primeras rondas, se analizaron a nivel cualitativo mediante la metodología descrita por Green en 1954 y adaptada para su método estadístico matemático por Oñate, Ramos, y Díaz (1988), los cuales fueron tabulados mediante el sistema automático para el procesamiento de la técnica de consulta a expertos versión 1.0 expuesto por Hurtado y Méndez (2007).

La consistencia y fiabilidad de los resultados se analizaron aplicando el coeficiente de ANOCHI (Domínguez, 2023) determinado como el índice de concordancia de los datos obtenidos relacionados con el acuerdo máximo posible. La aplicación de la estadística no paramétrica consistió en determinar la asociación entre el número de expertos, el número de ítems y las valoraciones entre los criterios contribuidos y fue calculada mediante los siguientes pasos:

1. Se determinan las diferencias de los rangos (DR) asignados para cada ítem a partir de todas las combinaciones de pares de jueces, utilizando la expresión n!/2! (n-2!).

2. Se calcula la fracción de discrepancia (FD) de cada ítem y el promedio de los n ítems, utilizando la expresión FD= DR/ DRM. El valor de la diferencia de rangos máximos (DRM) se toma de la tabla de diferencia de rango máxima de las evaluaciones de n jueces propuestas.

3. Se calcula la fracción de coincidencia (FC) de cada ítem y la del promedio como coeficiente de ANOCHI a partir del complemento del valor 1, utilizando la expresión FC= (1-FD).

Para el análisis estadístico matemático se aplicó estadística descriptiva mediante análisis de frecuencias de las respuestas de los ítems del modelo propuesto y las relaciones que se establecen entre sus componentes en la representación esquemática, así como la relevancia, pertinencia y coherencia. Además, se realizó un análisis cualitativo de las opiniones expresadas por los expertos en la pregunta abierta. Por último, se tabularon los resultados de la modelación estadístico-matemática empleando la validación mediante el Método Delphi como modelo cualitativo de validación teórica, dando lugar a la

versión definitiva de la propuesta metodología para la evaluación de la seguridad de la información de software de gestión académica.

3. Resultados y discusión

En el desarrollo de este artículo se planteó la propuesta metodológica para la evaluación de la seguridad de la información del Software de Gestión Académica (SGA), la cual está basada la metodología de OSSTMM para la gestión de auditorías de seguridad de la información (Miranda Silva, 2019), donde lo que desea es definir, controlar e implementar acciones, decisiones con respecto a la identificación de vulnerabilidades, amenazas y reducir brechas para mejorar la seguridad de la información en software de gestión académica, mediante el uso de un instrumento para apreciar la postura de seguridad en el SGA, el cumplimiento de métricas y controles relacionados con la ISO 27001 – 27002, normativas locales vigentes aplicables a software de gestión académico, Ley de Protección de Datos vigente en el Ecuador por tratarse de niños, jóvenes y adolescentes que se considera una categoría especial de datos en dicha ley, detallando finalmente un reporte del análisis de la madurez de estado de cumplimiento, su porcentaje correspondiente.

La realización de la auditoría se basa en las 4 fases descritas en OSSTMM mostradas a continuación.

Figura 1. Fases de la propuesta metodológica.

Fuente: César Zambrano Delgado, 2024

3.1 Fase de inducción.

Donde se define el alcance y se elabora el cronograma de la auditoría. Así como también se realiza la recopilación de información sobre el objetivo del análisis. Este proceso es crítico para entender el entorno, identificar y evaluar la postura de seguridad en el SGA, así como también entender los requisitos, alcance y las limitaciones del mismo.

3.2 Fase de Indagación.

Aquí se recopila información del SGA, tanto de forma interna como externa, llevando a cabo una enumeración detallada de sistemas, servicios y recursos. La evaluación de configuraciones y la identificación de vulnerabilidades potenciales forman parte de este proceso. En esta fase se obtienen los datos principalmente documentales o por observación, entrevistas con los usuarios de los distintos perfiles que interactúan con el SGA, y se realiza la solicitud de documentos e información a los responsables gerentes o jefes del proyecto. En esta fase se utilizó la ficha para obtener los datos (principalmente documentales o por observación) del SGA.

3.3 Fase de Interacción.

En esta fase se evalúa la seguridad de la información y su protección. Se considera la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, y se determinan los controles y procesos asociados en la aplicación de la seguridad de la información, se debe establecer la política, objetivos, procesos y procedimientos de seguridad en marcos referenciales internaciones y normativas locales.

A partir de la información obtenida se consideraron métricas y estándares relacionados con la familia ISO 27000, entre los que se utilizaron tres como son 27001:2013, 27002:2013, 27001:2022, adicionalmente la Ley de Protección de Datos Personales vigente Ecuador, para elaborar preguntas y así la construcción del instrumento de validación de seguridad de la información en SGA, clasificándolas de acuerdo a 5 pilares de seguridad de la información.

3.4 Fase de intervención.

Finalmente, en esta la última fase de la metodología propuesta se establece el nivel de seguridad de los canales, así como el detalle de cumplimiento de métricas y controles asociados en los pilares correspondiente de seguridad de información obtenidos en la aplicación de instrumentos creado e ingresados para el cálculo correspondiente del estado de madurez de cumplimiento.

Para la asignación y cálculo de madurez de cumplimiento se utilizó un análisis de brechas GAP (Groups, Algorithms and Programming) o análisis de

deficiencias, el cual consiste en un análisis de cumplimiento tanto con los requisitos de la norma 27001:2013, 27002:2013 o 27001:2022 como de sus controles (Triana Osorio, 2024). Asignamos valores según los niveles de madurez de 0 a 5 para cada control, y obtendremos un nivel medio de madurez que vendrá determinado por:

Nivel Medio Cumplimiento = Puntuación total de cada Control / Número de controles totales.

Esta fórmula nos entregara un valor medio para cada control entre 0 y 5, con lo que podríamos clasificar los controles y su cumplimiento entre los siguientes valores:

Puntaje de madurez por debajo de 1.65: No cumple. Puntaje de madurez entre 1.66 y 3.25: Cumple parcialmente.

Puntaje de madurez por encima de 3.26: Cumplimiento con requisitos de la Norma.

En esta fase finalmente se presenta el informe de madurez de cumplimiento mediante un resumen de las fases de la auditoria aplicadas, evidencia las métricas y controles agrupados por los pilares de seguridad de la información considerados, cantidad y porcentaje de cumplimiento, así como el semáforo se madurez como resultado final de la auditoria efectuada.

Figura 2: Informe de madurez de cumplimiento

Métricas y controles de seguridad

OSSTMM- ISO 27001

Detalle de cumplimiento de métricas y controles agrupados por los 5 pilares de seguridad de información considerados en esta auditoría.

Pilares		Cumplimiento	Porcentaje	Nivel medio
Autenticidad		13	100%	3.154
Integridad		9	100%	3.222
Confidencialidad		4	80%	3.200
Disponibilidad		6	100%	5.000
Trazabilidad		6	100%	5.000
Todos los Pilares		0	0%	0.000
Total	0	38	95%	

Madurez de estado de cumplimiento	3.65
Porcentaje de Nivel medio de cumplimiento:	73%

Cumple con requisitos de la Norma

Fuente: César Zambrano Delgado, 2024

Resultado de la validación

Experto	Kc	Ka	K	Valoración
E1	0.8	0.8	0.8	Alto
E2	1	1	1	Alto
E3	0.8	1	0.9	Alto
E4	1	1	1	Alto
E5	0.5	0.6	0.55	Medio
E6	0.8	0.9	0.85	Alto
E7	0.8	1	0.9	Alto
E8	0.3	0.7	0.5	Medio
E9	0.6	0.8	0.7	Medio
E10	0.6	0.9	0.75	Medio
E11	0.9	1	0.95	Alto
E12	1	1	1	Alto
E13	0.7	1	0.85	Alto
E14	0.8	0.8	0.8	Alto

Tabla 1. Resultado del coeficiente de competencia

La encuesta realizada a los expertos se obtuvo como resultado que diez alcanzaron un coeficiente de competencia alto y cuatro un coeficiente de competencia medio valoración aceptable para dar criterios confiables y valido sobre la metodología propuesta (Tabla 1), resultados que se concierne con la cantidad de expertos aceptables que debe estar entre 7 y 30 para obtener del 1% al 5% de margen de error. Además, se consideraron características adicionales de los expertos, como que el 71% poseen curato nivel académico y el 86% tienen relación directa en trabajos basados en la seguridad de información y conocen sobre software de gestión de académica, contemplada en la propuesta metodológica con 8 años de experiencias promedio en tecnologías y desarrollo de sistemas.

Se contó de 2 rondas para la validación de la propuesta metodológica. Como etapa inicial el grupo coordinador valoró la primera versión del cuestionario, analizando cada uno de sus ítems, donde se realizaron consideraciones que ayudaron a la corrección y ajustes de la versión final del cuestionario y sus ítems.

Una vez lista la versión final del instrumento a partir de las consideraciones obtenidas, en la primera ronda se envió el cuestionario al grupo de expertos seleccionados donde se obtuvieron resultados de las valoraciones cuantitativas y fueron procesados mediante análisis matemático estadístico aplicando el proceder descrito en los métodos.

En la Tabla 2 se aprecia el análisis efectuado por parte de los expertos acerca de la propuesta metodológica para la evaluación de la seguridad de la información en software de gestión académica, resultó que, de los 12 aspectos sometidos a valoración, 10 (83,3%) fueron considerados como Muy Adecuados (MA) y 2 (16,7%) fueron considerados como Bastante Adecuados (BA).

Tabla 2. Análisis de las respuestas en la primera ronda de la consulta a expertos.

C1	C2	C3	C4	C5	C1	C2	C3	C4	C1	C2	C3	C4	Sumas	Promedio
8	13	14	14	14	0.571	0.929	1.000	1.000	0.180	1.465	3.090	3.090	7.830	1.960
8	14	14	14	14	0.571	1.000	1.000	1.000	0.180	3.090	3.090	3.090	9.450	2.360
7	13	14	14	14	0.500	0.929	1.000	1.000	0.000	1.465	3.090	3.090	7.650	1.910
5	12	14	14	14	0.357	0.857	1.000	1.000	-0.366	1.067	3.090	3.090	6.880	1.720
5	13	14	14	14	0.357	0.929	1.000	1.000	-0.366	1.465	3.090	3.090	7.280	1.820
7	13	14	14	14	0.500	0.929	1.000	1.000	0.000	1.465	3.090	3.090	7.650	1.910
7	14	14	14	14	0.500	1.000	1.000	1.000	0.000	3.090	3.090	3.090	9.270	2.320
4	13	14	14	14	0.286	0.929	1.000	1.000	-0.566	1.465	3.090	3.090	7.080	1.770
4	12	14	14	14	0.286	0.857	1.000	1.000	-0.566	1.067	3.090	3.090	6.680	1.670
7	14	14	14	14	0.500	1.000	1.000	1.000	0.000	3.090	3.090	3.090	9.270	2.320
8	14	14	14	14	0.571	1.000	1.000	1.000	0.180	3.090	3.090	3.090	9.450	2.360
8	14	14	14	14	0.571	1.000	1.000	1.000	0.180	3.090	3.090	3.090	9.450	2.360

Fuente: César Zambrano Delgado, 2024

Para el análisis de la consistencia y fiabilidad de estos resultados, se aplicó el Coeficiente de ANOCHI, definido por Domínguez (2023) como el índice de la concordancia del acuerdo efectivo mostrado en los datos en relación con el acuerdo máximo posible. Esta aplicación estadística no paramétrica permite la determinación de la asociación entre el número de expertos, el número de ítems y las valoraciones entre los criterios aportados.

Permite establecer un rango cuantitativo según una escala numérica que oscila entre 0 y 1, donde el valor 1 significa la concordancia perfecta y el valor 0 ausencia total de concordancia. En la presente investigación, el mismo para un valor de diferencia de rango máxima de las evaluaciones de n jueces (DRM) de 196, dio un valor de 0,71, lo que indica una Aceptable o una buena fiabilidad de los criterios de los expertos

Tabla 3. Resultados del Coeficiente de ANOCHI en la primera ronda de la consulta a expertos.

Aspectos a evaluar del modelo	Discrepancia (FD)	Coincidencia (FC)
1.1	0,31	0,69
1.2	0,24	0,76
2.1	0,32	0,68
2.2	0,35	0,65
2.3	0,30	0,70
2.4	0,32	0,68
3.1	0.25	0.75
3.2	0,27	0,73
4.1	0,33	0,67
4.2	0,25	0,75
5.1	0,24	0,76
5.2	0,24	0,76

Coeficiente de ANOCHI	**0,71**

Fuente: César Zambrano Delgado, 2024

En cuanto a la Relevancia, Pertinencia y Coherencia de la propuesta metodológica para la evaluación de la seguridad de la información en software de gestión académica, las evaluaciones mostraron que el 100% de los expertos consideran a la propuesta metodológica para la evaluación de la seguridad de la información en software de gestión académica en los rangos muy relevante y relevante (Tabla 4).

Tabla 4. Resultado de Relevancia, Pertinencia y coherencia en la primera ronda de la consulta a expertos

Aspecto	Muy Relevante	Relevante	Total
5.1. Relevancia	42,86%	57,14%	100%
5.2. Pertinencia	42,86%	57,14%	100%
5.3. Coherencia	35,71%	64,29%	100%

Fuente: César Zambrano Delgado, 2024

Una vez modificada la propuesta metodológica para la evaluación de la seguridad de la información en software de gestión académica, considerando las recomendaciones realizadas por los expertos, fue remitido el cuestionario modificado y los resultados estadísticos tabulados a los expertos para una

segunda ronda de consulta, para que reconsiderara sus criterios si fuese necesario o los mantuviera. Luego de recibir los resultados de la segunda ronda se realizó la modelación estadística matemática definida por el Método Delphi lo cual evidenció que los 12 aspectos que componen la propuesta metodológica para la evaluación de la seguridad de la información en software de gestión académica fueron considerados como muy adecuados por el grupo de expertos (Tabla 5), el Coeficiente de ANOCHI para un valor de diferencia de rango máxima de las evaluaciones de n jueces (DRM) de 196, dio un valor de 0,81, lo que indica una elevada o muy buena fiabilidad de los criterios de los expertos.

Tabla 5. Resultados del Coeficiente de ANOCHI en la segunda ronda de la consulta a expertos.

Aspectos a evaluar del modelo	Discrepancia (FD)	Coincidencia (FC)
1.1	0.12	0,88
1.2	0,07	0.93
2.1	0,12	0,88
2.2	0,20	0,80
2.3	0,12	0,88
2.4	0,25	0,75
3.1	0,25	0,75
3.2	0,24	0,76
4.1	0,25	0,75
4.2	0,25	0,75

5.1	0,12	0,88
5.2	0,23	0,77
Coeficiente de ANOCHI		**0,81**

Fuente: César Zambrano Delgado, 2024

De igual forma los resultados de Relevancia, Pertinencia y Coherencia cambiaron en la segunda ronda de consulta, obteniendo un aumento significativo en la valoración muy relevante (Tabla 6).

Tabla 6. Resultado de Relevancia, Pertinencia y Coherencia en la segunda ronda de la consulta a expertos

Aspecto	Muy Relevante	Relevante	Total
5.1. Relevancia	85,71%	14,29%	100%
5.2. Pertinencia	78,57%	21,43%	100%
5.3. Coherencia	71.43%	28,57%	100%

Fuente: César Zambrano Delgado, 2024

Los resultados definidos evidencian una estabilidad, fiabilidad y consistencia de los juicios emitidos por los expertos, por lo que se consideró que la propuesta metodológica para la evaluación de la seguridad de la información en software de gestión académica, en la forma que se exhibe en el presente artículo, cumple su validación aceptable para la investigación, motivo por el cual no se realiza una ronda nueva coincidiendo con lo expresado por otros autores en sus investigaciones (Fernández de Castro & López, 2013; Domínguez, 2023).

4. CONCLUSIONES

La propuesta metodológica para la evaluación de la seguridad de la información en software de gestión académica como base para el modelo propuesto. Se utilizó el Método Delphi para la validación teórica y juicio de expertos para la validación de la factibilidad teórica de la propuesta metodológica.

En el aspecto técnico, la propuesta metodológica estará enfocada únicamente a la evaluación de la seguridad de la información en software de gestión académica de unidades educativas de educación general básica y bachillerato del Ecuador, mediante el uso un instrumento de ayuda para realizar auditorías de seguridad de información en SGA, basándose en la propuesta metodológica la cual es una adaptación de la metodología OSSTMM, para entender el entorno, identificar, evaluar la seguridad de la información en el SGA, el cumplimiento de métricas y controles relacionados con la ISO 27001 – 27002.

Esta herramienta busca ser una guía al momento de cuantificar el nivel de seguridad de este tipo software de gestión académica, mediante un análisis de brechas de cumplimiento tanto con los requisitos de la norma ISO 27001:2013 como de sus controles mediante el cálculo de madurez de cumplimiento de la ISO/IEC 27001:2013.

La herramienta dispone de tres componentes: Una ficha para la obtención de datos, y una hoja electrónica para ingresar los valores correspondientes de cada pregunta y otra hoja para realizar el cálculo de análisis de brechas y reportar el estado medio de cumplimiento y el porcentaje de seguridad correspondiente. La aplicación de esta herramienta en la auditoría realizada, permitió determinar de forma rápida la valoración cuantitativa de seguridad del SGA.

5. Referencia

Cedeño, E. L. C., & Mena, K. E. S. (2022). El Método Delphi Cualitativo y su Rigor Científico: Una revisión argumentativa. Sociedad & Tecnología, 5(3), 530-540.

Domínguez, F. J. A. (2023). Optimización de la planificación a través del método de expertos: Una perspectiva metodológica. Ciencia y Educación, 62-73.

Guijarro, E. G. L., & Guerra, F. A. C. (2018). Comparación de modelos tradicionales de seguridad de la información para centros de educación. Tierra Infinita, 4(1), 22-33.

Gladden, M. E. (2017). The Handbook of Information Security for Advanced Neuroprosthetics. Synthypnion Academic.

ISO 27001. (2013). ISO 27001. Recuperado 28 de enero de 2023, de https://normaiso27001.es/referencias-normativas-iso-27000/

ISO/IEC 27000. (2013). ISO/IEC 27000:2013. Normas ISO. https://www.iso.org/standard/73906.html

ISO/IEC 27001. (2023) Implementar ISO 27001 paso a paso—1 como hacer un Analisis Previo [Https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/]. ISO 27001. Recuperado 6 de agosto de 2023, de https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis/

Miranda Silva, C. P. (2019). Auditoría de redes, aplicando la metodología OSSTMM V3, para el Ministerio de Inclusión Económica y Social. Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas.

Likert, R. (1932). A technique for the measurement of attitudes. Archives of Psychology,
140, 1-55. Retrieved from https://psycnet.apa.org/record/1933-01885-001

LOPDP. (2021). Ley de Protección de Datos Personales [Registros publicos]. Dirección Nacional de Registros Públicos. https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/

Oñate, N., Ramos, L., & Díaz, A. (1988). Utilización del Método Delphi en la pronosticación: Una experiencia inicial. Cuba: Economía Planificada, 3(4), 9-48.

Ponemon Institute. (2018). Global_Cyber_Megatrends Cybersecurity. https://edge.spiceworksstatic.com/service.client-interactive/2018/hpi/toolkit%20lp/Secur ity-toolkit-assets/2018_Global_Cyber_Megatrends.pdf

Sistema de Gestión de Control Escolar – Educar Ecuador | Ministerio de Educación. (2023) Retrieved May 4, 2023, from https://educarecuador.gob.ec/sistema-de-gestion-de-control-escolar/

Triana Osorio, J. S. (2024). Desarrollo de una aplicación para análisis GAP que permita la verificación del cumplimiento en la implementación de la norma ISO 27001-2022.

Vega, E. M. D. G., Deza, J. R. D., & de los Santos, A. C. M. (2022). Importancia de la gestión de seguridad de la información en instituciones educativas

con ITIL e ISO 27001. Revista de investigación de Sistemas e Informática, 15(1), 113-123.