Año 28
No. Especial 9, 2023
ENERO-JUNIO

Año 28
No. Especial 9, 2023
Enero-Junio

Revista Venezolana de Gerencia

UNIVERSIDAD DEL ZULIA (LUZ)
Facultad de Ciencias Económicas y Sociales
Centro de Estudios de la Empresa

ISSN 1315-9984

Cómo citar: Tenesaca Guamán, G. V., Mejía Quizhpe, L., Jara Obregón, L. S., y Tigre Sánchez, M. A. (2023). Sistema de información integrado en instituciones de educación superior en Ecuador. *Revista Venezolana De Gerencia*, *28*(No. Especial 9), 777-795. https://doi.org/10.52080/rvgluz.28.e9.48

Universidad del Zulia (LUZ)
Revista Venezolana de Gerencia (RVG)
Año 28 No. Especial 9, 2023, 777-795
ENERO-JUNIO
ISSN 1315-9984 / e-ISSN 2477-9423

Sistema de información integrado en instituciones de educación superior en Ecuador

Tenesaca Guamán, Gladiz Verónica*
Mejía Quizhpe, Lorena Del Carmen**
Jara Obregón, Luis Stalin***
Tigre Sánchez, Mayra Alejandra****

Resumen

Las Instituciones de Educación Superior del Ecuador se encuentran en proceso de implementación de Sistemas de Información Integrados, lo que permite influir en toma de decisiones importantes, por eso es esencial analizar factores que permitan brindar seguridad y restricciones al acceder a estos sistemas. En tal sentido, el objetivo de estudio se centró en identificar las principales amenazas de la Seguridad en el acceso a los Sistemas de Información Integrados en las Instituciones de Educación Superior; se estableció una metodología de tipo cualitativa que permitió la revisión sistemática del contenido de 47 artículos, a partir de los cuales se establecen los dominios a utilizarse para establecer la propuesta de los indicadores: personas, control de acceso y criptografía. Así mismo se utilizó el Modelo Goal Question Metric, el método cuantitativo estadístico Kappa de Fleiss y coeficiente V de Aiken. Esto permitió recolectar y analizar datos, con el fin de identificar las variables que se plasman en los seis indicadores propuestos para controlar del acceso a los Sistemas de Información Integrados en las Instituciones de Educación Superior, enfatizado en tres ejes: responsabilidad del personal, cifrado y acceso.

Palabras clave: Indicadores; seguridad de la información, sistemas de información integrado, instituciones de educación superior.

Recibido: 27.11.22 **Aceptado:** 31.03.23

* Magíster en Auditoría de Tecnologías de la Información - Universidad de Especialidades Espíritu Santo. Ecuador. Técnico de Investigación Científica de la Universidad Católica de Cuenca. (Cuenca, Ecuador); Email: gtenesaca@uacue.edu.ec ORCID:https://orcid.org/0000-0003-3592-6244

** Magíster en Auditoría de Tecnologías de la Información - Universidad de Especialidades Espíritu Santo - Ecuador. Técnico de Auditoría Académica de la Universidad Católica de Cuenca. (Cuenca, Ecuador); Email: lmejiaq@ucacue.edu.ec ORCID: https://orcid.org/0000-0002-0451-563X

*** Magister en Gerencias de Tecnologías de la Información - Universidad Estatal de Milagro. Ecuador; Docente titular auxiliar 2 de la Universidad Católica de Cuenca. (Cuenca, Ecuador); Email: lsjaraob@ucacue.edu.ec ORCID: https://orcid.org/0000-0003-4958-5698

**** Magister en Sistemas de Información Gerencial – Universidad Tecnológica Empresarial de Guayaquil. Ecuador; Ingeniera de Sistemas por la Universidad Católica de Cuenca. (Cuenca, Ecuador); Email: Mayratigre@live.com ORCID: https://orcid.org/0000-0003-2018-7362

Integrated information system in higher education institutions in Ecuador

Abstract

The Institutions of Higher Education in Ecuador are currently in the process of implementing Integrated Information Systems, which allows influencing important decision-making, which is why it is essential to analyze important factors that allow providing security and restrictions when accessing these systems. In this sense, the objective of the study focused on identifying the main Security threats in access to Integrated Information Systems in Higher Education Institutions; A qualitative methodology was established that allowed the systematic review of the content of 47 articles, which allowed establishing the domains to be used to establish the proposal of the indicators: people, access control and cryptography. Likewise, the Goal Question Metric Model, the Fleiss Kappa statistical quantitative method and Aiken's V coefficient were used, which allowed the collection and analysis of data, in order to identify the variables that were reflected in the six indicators proposed to control access to Integrated Information Systems in Higher Education Institutions, emphasized on three axes: staff responsibility, encryption and access.

Keywords: Indicators; information security; integrated information systems; higher. Education Institutions.

1. Introducción

A lo largo de la historia, las Instituciones de Educación Superior han sufrido múltiples cambios; esto ha dado lugar a un proceso evolutivo condicionado por las demandas propias de su entorno. Las distintas maneras de vinculación con la sociedad a través de factores económicos, políticos, sociales, ambientales, entre otros, han sido concluyentes en la formación integral y acelerada de los diferentes modelos de gestión (Barajas y Orduz, 2019).

Carrizo, Sauvageot y Bellainer (2003) afirman que la información es la base de la planificación, la evaluación y la gestión de todo sistema educativo, así como su mayor vulnerabilidad. Por ello, surge la necesidad de registrar, almacenar, procesar, recuperar, comunicar y centralizar los grandes volúmenes de datos, mediante Sistemas de Información Integrados (SII) (Torres y Lamenta, 2015). Las grandes organizaciones, principalmente las transaccionales, empezaron a utilizar estos sistemas, con el propósito de integrar en una sola base de datos común toda la información de las diferentes jurisdicciones y sucursales de las organizaciones (Zabala et al, 2021).

Las Instituciones de Educación Superior tienen estructuras y procesos para la toma de decisiones únicas, y no pueden ser comparadas con otras organizaciones (Fontalvo y De la

Hoz, 2018); por lo tanto, los Sistemas de Información Integrados para la Institución de Educación Superior (SII-IES), desempeñan un rol importante, que permiten el perfeccionamiento de los procesos educativos, brindando una solución completa en aspectos de gestión e integración de las diferentes áreas que conforman una Universidad, permitiendo la recopilación de la información, comunicación y la toma de decisiones oportunas (Cornford y Shaikh, 1992).

En el mundo actual, y particularmente en las Universidades, a medida que crece la información sobre notas, evaluaciones, asistencia, títulos, y demás datos estudiantiles, los sistemas de información se encuentran en una constante amenaza mediante técnicas sofisticadas de ataques informáticos, por ello, es indiscutible recurrir a medidas de seguridad de la información, haciendo de este, un tema crítico y aún más complejo de gestionar (Leguizamón et al, 2020).

Al respecto, Altamirano (2019) señala que problemáticas como el abuso de confianza, la inadecuada asignación de roles, el uso inapropiado de privilegios en cuanto al acceso de la información, generan riesgos de seguridad en los SII, provocando que la información almacenada en estos sistemas no sea confiable, y arrastres inconvenientes a la hora de tomar de decisiones (Govea, 2021).

Frente a la problemática planteada, Ventura-León, Arancibia & Madrid (2017) sugieren velar por el uso de privilegios útiles que permitan proteger, controlar y auditar tanto accesos indeseados, como la manipulación de los datos, sosegando la propagación de información, y asegurando la confiabilidad y precisión de los datos. Por su parte, Arevalo et al, (2020) recalcan la necesidad de implementar medidas de seguridad, para que los SII no tengan pérdidas de información y/o datos alterados.

Para poder obtener la información, la investigación es de tipo cualitativa, basada en Okoli y Schabram (2010), esto permite establecer los dominios de los indicadores. Se empleó el método Goal-Question-Metric (GQM) y los métodos cuantitativos Kappa de Fleiss y V de Aike, métodos importantes que analiza y mide los datos obtenidos, tomando en cuenta aquellos relevantes por el impacto propio del análisis.

El desarrollo de esta investigación resulta ser de gran ayuda para las IES, siendo una estrategia que proporcionará una visión general a través de la identificación de las principales amenazas de la problemática planteada en relación con el control de acceso de la información, lo que establece una propuesta de indicadores de cumplimiento y gestión para la seguridad para controlar el acceso, que buscan caracterizar el grado de cumplimiento de estos sistemas en materia de seguridad y otorgar instrumentos para hacer frente a un ataque o un incidente en el acceso de la información de acuerdo a las necesidades que una IES posee.

2. Sistemas Integrados: concepciones teóricas

Los Sistemas Integrados y los datos están robustamente conexos, pero la frágil cultura de seguridad de la información en las IES que se mantiene sobre los recursos institucionales, ha dado paso a un sistema de seguridad enfocado al comportamiento del personal y a controles técnicos (Quinteros et al, 2023). Adicionalmente, dentro de las deficiencias y amenazas de seguridad de la información de los SII en las IES,

existe la falta de normas y políticas de seguridad descrita, esto influye en el comportamiento del personal interno entre docentes y estudiantes, que por negligencia o mala intención dan paso a accesos no autorizados y robo de información confidencial.

Actualmente, en Ecuador existen iniciativas, que consideran tanto la protección de los datos personales y financieros, que asegura el acceso a la información en función de los requisitos de negocio y de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información (Muyón et al, 2019). Pero a pesar de múltiples esfuerzos, todavía no se trabaja en seguridad de manera metódica con políticas concretas para el sector de las IES, y de acuerdo con la encuesta efectuada por la red nacional de educación e investigación (CEDIA), el 82% de las IES no cuenta con un presupuesto destinado solamente para la gestión de la seguridad, sin embargo, existe un 36% de las IES que tiene un área reservada para gestionar las amenazas y riesgos concernientes. Así mismo, el 64% de las IES están trabajando en la gestión de acceso, para tener roles definidos y privilegios en sus sistemas (CEDIA, 2014).

De acuerdo con Lapiedra et al, (2021) los Sistemas de Información Integrados, son conjuntos de elementos encaminados al proceso y gestión de volúmenes de datos e información, que en un principio fueron creados para enfocarse al ámbito empresarial, integrando todas las unidades de la organización, pero en esta última década han desempeñado un papel importante en la educación superior.

Quirumbay et al, (2022) mencionan que la seguridad de la información combina sistemas, operaciones y controles internos para garantizar la integridad, disponibilidad y confidencialidad de los datos en las IES; por esto, es evidente la necesidad de mecanismos para reducir los riesgos de la información digital en sus principales dimensiones de seguridad como confidencialidad, integridad, disponibilidad, pero además autenticidad y trazabilidad; estos pilares permiten levantar una estructura firme para controlar el acceso en los sistemas de Información Integrados.

3. Consideraciones metodológicas de la investigación

En este apartado se especifican las fases de desarrollo de la investigación y las dimensiones relevantes del presente estudio. En primera instancia, se utiliza la metodología propuesta por Okoli y Schabram (2010), que como primer aspecto se acentúa en la “planificación” que es identificar las principales amenazas a la seguridad de la información; en cuanto al segundo aspecto “la selección”, se realizó a una búsqueda en bases de datos con contenido científico – técnico. En lo relacionado con el tercer aspecto, “la extracción”, se intensificó la búsqueda por palabras clave, vinculación por autores sobre el campo del conocimiento.

En cuanto al último aspecto, “ejecución”, los hallazgos sobre el objetivo de estudio, donde se establece que el 43% del estudio es sobre las amenazas internas y se relaciona con el comportamiento del personal o usuarios finales, el 32% es referente a los deficientes controles de acceso a la información tratada diariamente, y un 25% hacen referencia a limitados

esfuerzos por la implementación de controles que permitan asegurar los datos ante intrusos. Por consiguiente, este análisis y la obtención de resultados da origen a tres criterios, control de acceso, responsabilidad del trabajador y criptografía.

Ahora bien, en cuanto al enfoque cuantitativo, bajo los aspectos ya descritos, se trabaja con el Método GQM que es una propuesta de Calabrese et al, (2017), que comprende básicamente tres niveles con seis pasos: a) Nivel conceptual, aquí se define el objetivo, el plan, el proceso, el panorama y un hecho de calidad y es considerada como la raíz (Solingen, 1999); b) Nivel operativo, conforme a las metas establecidas se define una serie de preguntas que permiten identificar la evaluación de un objetivo específico; c) Nivel cuantitativo, a cada pregunta se la relaciona con datos que faciliten una respuesta cuantitativa a los objetivos, dichos atributos pueden ser cuantificados dependiendo del criterio que será empleado para medir.

Dicho de otra manera, la metodología GQM no proporciona objetivos, refina el objetivo en preguntas y delimita métricas, proporciona datos para responder a estas preguntas, las mismas que ayudarán a medir si se está alcanzando el objetivo principal (Rainho y Barreiros, 2019). Si bien, el proceso de GQM se describe en seis pasos, este modelo no es empleado para efectuar las mediciones, sino únicamente para alcanzar la estructura, puesto que permiten la identificación de métricas efectivas.

4. Sistema de indicadores de control de acceso a la información: Propuesta

Para estructurar los indicadores, se enfatiza en los pasos del método GQM, que como como primer paso “Establecer Metas”, identifican lo que deseamos lograr; por esta razón se desarrolla un conjunto de objetivos para los criterios obtenidos en la revisión literaria: control de acceso, responsabilidad del trabajador y criptografía a los cuales se denomina dominios (cuadro 1).

Cuadro 1
Metas Establecidas SII-IES

Dominio	Objetivo
Control de Acceso	Identificar la existencia de lineamientos, normas o estándares para un control de acceso seguro a SII-IES
Responsabilidad del trabajador	Medir el nivel de capacitación al recurso humano y su adjudicación en relación a la seguridad de la información para SII-IES
Criptografía	Identificar la existencia de lineamientos, normas o estándares en cuanto a la preservación de la confidencialidad tanto en la información como en su almacenamiento en SII-IES

Fuente: Elaboración propia.

En cuanto al segundo paso “generación de preguntas”, una vez establecidos los objetivos, se procede a elaborar preguntas fundamentadas en la Normativa ISO/IEC 27002:2022, así como en leyes ecuatorianas en temas de seguridad de la información y encuestas realizadas a personal que día a día

está involucrado en el manejo de SII. Adicionalmente, se toma la propuesta de Escobar y Cuervo (2008) y se establece para cada pregunta criterios, para cada pregunta con una escala de adecuación del 1 al 4, para los criterios suficiencia, relevancia, claridad y coherencia, con la diferencia que el criterio de suficiencia es validado por dimensión y no por ítem, donde las observaciones emitidas por los jueces que estimaron oportunas, permiten ajustar la encuesta a lo requerido.

Para estimar el grado de acuerdo de los jueces se utiliza el método estadístico Kappa de Fleiss, que brinda una perspectiva más avanzada sobre la concordancia de los expertos y la confiabilidad del acuerdo, se utiliza la escala de estimación para k de seis niveles, conforme tabla 1, que enuncia cualitativamente la fuerza de la concordancia y puede ser calculado en tablas de cualquier dimensión, tomando como referencia valores entre -1 y +1; mientras más próximo a +1 mayor es el grado de correlación entre los jueces expertos (Fleiss et al, 2003).

Tabla 1
Estimación del coeficiente Kappa de Fleiss

K	Interpretación
<0	Pobre Acuerdo
0.01 - 0.20	Ligero Acuerdo
0.21 - 0.40	Acuerdo Justo
0.41 - 0.60	Acuerdo Moderado
0.61 - 0.80	Acuerdo Sustancial
0.81 - 1.00	Acuerdo Casi Perfecto

Nota: Etiquetas de rango correspondiente a Kappa

Fuente: elaboración propia con base en Landis y Koch (1977).

De ello, el grado de fiabilidad de los observadores o jueces expertos utilizando el coeficiente Kappa de Fleiss a partir de los índices estimados para la concordancia, se obtiene que para la encuesta Control de Acceso se estimaron valores de entre 0.231 - 0.338 (tabla 2);

Tabla 2
Validez Acuerdo de los Jueces Expertos - Control de Acceso

	Total	Bajo Nivel (2)	Moderado (3)	Alto Nivel (4)
Relevancia	0.231	0.018	0.187	0.310
Claridad	0.354	-0.008	0.353	0.367
Coherencia	0.338	-0.004	0.336	0.347

Fuente: elaboración propia con base al Juicio de Expertos.

Mientras que, para la encuesta de Responsabilidad del Personal las estimaciones oscilan entre 0.21 - 0.25 (tabla 3).

Tabla 3
Validez Acuerdo de los Jueces Expertos – Responsabilidad del Personal

	Total	Bajo Nivel (2)	Moderado (3)	Alto Nivel (4)
Relevancia	0.253	0.000	0.253	0.253
Claridad	0.210	0.050	0.208	0.208
Coherencia	0.210	0.050	0.206	0.206

Fuente: elaboración propia con base al Juicio de Expertos.

Y finalmente para la encuesta denominada Criptografía aplicando el coeficiente de kappa Fleiss se obtuvo una concordancia que oscila entre 0.211-0.356 (tabla 4).

Tabla 4
Validez Acuerdo de los Jueces Expertos Criptografía

	Total	Bajo Nivel (2)	Moderado (3)	Alto Nivel (4)
Relevancia	0.240	-0.013	0.243	0.260
Claridad	0.356	-0.013	0.316	0.421
Coherencia	0.211	-0.013	0.229	0.214

Fuente: elaboración propia con base al Juicio de Expertos.

Todas las estimaciones denotan como resultado: Acuerdo justo entre los expertos; soportándose este resultado en las directrices de kappa de Flesiss que sugiere que los valores de 0.21 a 0.40 indican una concordancia justa, lo que es válido para este estudio (Fleiss et al, 2000).

Para una valoración adecuada del contenido de las encuestas por el criterio de los expertos, se emplea el cálculo de promedios por dimensión con la ayuda de la prueba de V de Aiken; este método permitió cuantificar la eficacia o relevancia de los ítems con relación a N jueces (Penfield y Giancobbi, 2009).

Según los expertos el coeficiente V de Aiken posee distintos valores, derivando en dos niveles, Vo igual a 0.50 que indica nivel liberal (Cicchetti, 1994), mientras que Vo igual a 0.70, revela nivel conservador o más.

Luego de obtener el juicio de los expertos se procede a realizar la estimación de cada ítem que contendrán los indicadores, según los ítems que tengan la valoración de Vo ≥ 0.63, manteniendo como prioridad las categorías de relevancia y coherencia; en su defecto la categoría suficiencia será valorada por dimensión de cada encuesta, y con respecto a la categoría claridad, si el promedio es bajo, se buscará reformular o eliminar el ítem.

Una vez realizada la valoración estadística de la encuesta Control de

Acceso con el método V de Aiken, se determina que del total de los ítems planteados solamente los que mantienen valores óptimos son considerados (tabla 5).

Tabla 5
Validez Contenido Control de Acceso

Pregunta	Suficiencia		Coherencia		Relevancia		Claridad		Media	V Aiken
	Media	V Aiken	Media	V Aiken	Media	V Aiken	Media	V Aiken		
1	3.14	0.54	3.57	0.64	3.57	0.64	3.29	0.57	3.39	0.60
2	3.14	0.54	3.43	0.61	3.43	0.61	3.43	0.61	3.36	0.59
3	3.14	0.54	3.57	0.64	3.43	0.61	3.71	0.68	3.46	0.62
4	3.14	0.54	3.43	0.61	3.57	0.64	3.57	0.64	3.43	0.61
5	3.14	0.54	3.71	0.68	3.71	0.68	3.29	0.57	3.46	0.62
6	3.14	0.54	3	0.50	3	0.50	3	0.50	3.04	0.51
7	3.14	0.54	3.14	0.54	2.86	0.46	3.43	0.61	3.14	0.54
8	3.14	0.71	3.43	0.61	3.43	0.61	3	0.50	3.25	0.61
9	3.14	0.71	3.71	0.68	3.71	0.68	3.71	0.68	3.57	0.69
1	3.14	0.71	3.86	0.71	3.86	0.71	3.86	0.71	3.68	0.71
11	3.14	0.71	3.71	0.68	3.71	0.68	4	0.75	3.64	0.71
12	3.14	0.71	3.86	0.71	3.57	0.64	3.43	0.61	3.50	0.67
13	3.14	0.71	3.71	0.68	3.57	0.64	3	0.50	3.36	0.63
14	3.14	0.75	3.14	0.54	2.86	0.46	3.14	0.54	3.07	0.57
15	3.14	0.75	4	0.75	3.86	0.71	3.86	0.71	3.71	0.73
16	3.14	0.75	4	0.75	3.71	0.68	4	0.75	3.71	0.73
17	3.14	0.75	4	0.75	3.71	0.68	3.86	0.71	3.68	0.72
18	3.14	0.75	4	0.75	3.71	0.68	3.71	0.68	3.64	0.71
19	3.14	0.75	3.86	0.71	3.71	0.68	3.71	0.68	3.61	0.71
2	3.14	0.75	3.57	0.64	3.71	0.68	3.57	0.64	3.50	0.68
21	3.14	0.75	3.43	0.61	3	0.50	3.29	0.57	3.21	0.61
22	3.14	0.75	4	0.75	4	0.75	4	0.75	3.79	0.75
23	3.14	0.75	4	0.75	4	0.75	4	0.75	3.79	0.75
24	3.14	0.75	4	0.75	4	0.75	4	0.75	3.79	0.75
25	3.14	0.75	3.43	0.61	3.14	0.54	3.43	0.61	3.29	0.63
26	3.14	0.75	3.86	0.71	3.57	0.64	3.71	0.68	3.57	0.70
27	3.14	0.75	4	0.75	3	0.50	4	0.75	3.54	0.69
28	3.14	0.75	4	0.75	4	0.75	4	0.75	3.79	0.75
29	3.14	0.75	3.57	0.64	3.43	0.61	3.71	0.68	3.46	0.67
3	3.14	0.75	3.29	0.57	3.14	0.54	3.57	0.64	3.29	0.63
31	3.14	0.68	4	0.75	4	0.75	4	0.75	3.79	0.73
32	3.14	0.68	3	0.50	2.71	0.43	3.29	0.57	3.04	0.54
33	3.14	0.68	3.71	0.68	3.71	0.68	4	0.75	3.64	0.70
34	3.14	0.68	4	0.75	4	0.75	4	0.75	3.79	0.73
35	3.14	0.68	4	0.75	4	0.75	4	0.75	3.79	0.73
36	3.14	.68	4	0.75	4	0.75	4	0.75	3.79	0.73

Fuente: elaboración propia con base al Juicio de Expertos.

Por otra parte, para la encuesta Responsabilidad del Personal según V Aiken del total de los ítems planteados todos como pertinentes del estudio, sin embargo, se reformuló de manera clara, sin perder la coherencia y relevancia del mismo. Así mismo, el resultado por dimensión de responsabilidad de personal refleja promedios ≥ 0.63, en donde los jueces expertos señalan que los valores son aceptables para validar el contenido de tres dimensiones (tabla 6).

Tabla 6
Validez Contenido Responsabilidad del Personal

Pregunta	Suficiencia		Coherencia		Relevancia		Claridad		Media	V Aiken
	Media	V Aiken	Media	V Aiken	Media	V Aiken	Media	V Aiken		
1	4	0.75	4	0.75	3,57	0.64	3,43	0.61	3,75	0.69
2	4	0.75	3,57	0.75	4	0.75	3,86	0.71	3,86	0.74
3	4	0.75	4	0.75	4	0.75	4	0.75	4	0.75
4	4	0.75	3,57	0.64	4	0.75	4	0.75	3,89	0.72
5	4	0.75	4	0.75	4	0.75	3,86	0.71	3,96	0.74
6	4	0.75	3,57	0.64	4	0.75	3,86	0.71	3,86	0.71
7	4	0.75	4	0.75	4	0.75	4	0.75	4	0.75
8	4	0.75	4	0.75	3,57	0.64	3,43	0.61	3,75	0.69

Fuente: elaboración propia con base al Juicio de Expertos.

Finalmente, para la encuesta Criptografía con V Aiken, de los ítems trazados se ha considerado en su totalidad como ítems pertinentes para el estudio, sin embargo, se modificó varios ítems para obtener la claridad necesaria, dando importancia a coherencia y relevancia de los mismos; además, en relación a las dimensiones, se obtiene un promedio ≥ 0.63, siendo una estimación aceptable para validar el contenido de dos dimensiones (tabla 7).

Tabla 7
Validez Contenido Criptografía con el Método V Aiken

Pregunta	Suficiencia		Coherencia		Relevancia		Claridad		Media	V Aiken
	Media	V Aiken	Media	V Aiken	Media	V Aiken	Media	V Aiken		
1	3.86	0.71	3.57	0.64	4	0.75	4	0.75	3.86	0.71
2	3.86	0.71	3.43	0.71	4	0.75	4	0.75	3.82	0.73
3	3.86	0.71	4	0.75	3.43	0.61	3.57	0.64	3.71	0.68
4	3.86	0.71	3.71	0.68	4	0.75	3.57	0.64	3.79	0.70
5	3.86	0.71	3.43	0.61	3.57	0.64	4	0.75	3.71	0.68
6	3.86	0.71	4	0.75	3.57	0.64	4	0.75	3.86	0.71
7	3.86	0.71	3.71	0.68	4	0.75	3.71	0.68	3.82	0.71
8	3.14	0.75	4	0.75	4	0.75	3.86	0.71	3.75	0.74
9	3.14	0.75	4	0.75	4	0.75	3.86	0.71	3.75	0.74
10	3.14	0.75	4	0.75	3.43	0.61	4	0.75	3.64	0.71
11	3.14	0.75	4	0.75	4	0.75	2.86	0.46	3.50	0.68

Fuente: elaboración propia con base al Juicio de Expertos.

En lo relacionado al tercer paso del Método GQM "especificación de medidas", tras revisar los criterios de calidad de cada pregunta establecida en el paso anterior, se plantea dos preferencias elementales que corresponde al grado de seguridad de cada indicador que se va a proponer. De ello, se obtiene una preferencia elemental para las preguntas que indican cumplimiento con el atributo de si evidencia o no véase en la ecuación 1;

$$v=1 \text{ (si se evidencia)}$$
$$v=0 \text{ (no se evidencia)}$$

(Ecuación 1)

Mientras que para las preguntas que indican control existe atributos de satisfactorio o sobresaliente conforme ecuación 2;

$$\sum = \frac{v_0}{v_1} * 100$$

(Ecuación 2)

A continuación, se realiza una plantilla, que servirá como referencia para constituir la propuesta de indicadores de gestión y/o indicador de cumplimiento , que pueden ser utilizados en las IES, para medir la efectividad, eficacia y eficiencia de la seguridad en el acceso a la información de los SII, esta plantilla está conformada por: a) cabecera, la misma que contendrá nombre del indicador, numero, definición y objetivo; b) Cuerpo, aquí se definirá número y descripción de las N variables, y las fórmulas para la especificación de medidas; c) pie, se verificará si se cumple las metas, estableciendo una valoración, así también se precisa el campo para observaciones y una para fuente de información, en la que se puede describir los nombres de los diversos documentos que ayudaron a satisfacer la demanda de información contenida en las variables.

Por tal razón, de los resultados antes expuestos se reúnen los valores recomendables y pasan a ser parte de la propuesta de los indicadores:

Para el indicador de cumplimiento de control de acceso con las variables entre VSII01 y VSII24 (tabla 8).

Tabla 8
Indicador de cumplimiento - Control de Acceso

INDICADOR- REVISIÓN DEL CONTROL DE ACCESO	
Indicador	**INSII01**
Definición	Nivel de control de acceso en Sistemas de Información Integrados
Objetivo	Identificar la existencia de lineamientos, normas o estándares para un control de acceso seguro a Sistemas de información Integrados, para realizar un levantamiento de la información inexistente.
TIPO DE INDICADOR	
Indicador de Cumplimiento	

Cont... Tabla 8

DESCRIPCIÓN DE VARIABLES		FÓRMULA
VSII01:	¿Las IES tienen definidos políticas de control de acceso de los usuarios a los SII?	
VSII02:	¿Las IES han determinado procedimientos, normas y/o políticas para gestionar las cuentas de usuario de los SII?	
VSII03:	¿Las IES han determinado políticas, procedimientos y/o normas para la entrega y recepción de cuentas digitales que permitan el acceso en los SII?	
VSII04:	¿Los usuarios tienen el conocimiento que deben asegurar las contraseñas de acceso a los SII?	
VSII5:	¿Existe validación del login y contraseña para acceder a los SII-IES?	
VSII6:	¿Existe la gestión de contraseñas en los SII-IES?	
VSII7:	¿Los SII-IES ejecutan procesos de concienciación a los usuarios para que puedan cambiar su contraseña utilizando caracteres alfabéticos y numéricos?	
VSII8:	¿Los SII-IES gestionan el cambio de contraseña en el inicio de sesión para que la contraseña del usuario caduque en un tiempo determinado	
VSII9:	¿Los usuarios acceden a los SII-IES solamente por tareas definidas en su puesto de trabajo?	
VSII10:	¿Existe un control para que no todos los usuarios (trabajador, estudiante y/o proveedor) tengan accesos a la misma información de los SII?	
VSII11:	¿Los SII-IES realizan una verificación constante de los derechos de accesos de los usuarios (trabajador, estudiante y/o proveedor)?	
VSII12:	¿Existen controles para restringir y limpiar, suspender o habilitar el acceso de los usuarios en los SII-IES?	
VSII13:	¿Los SII-IES mantiene la limitación de los recursos accesibles por el usuario, así como el acceso en tiempo permitido?	VSIIX=1 (**SI** se Evidencia)
VSII14:	¿Los SII-IES controla el determinado número de intentos para acceder al sistema?	VSIIX=0 (**NO** se Evidencia)
VSII15:	¿Los SII-IES gestiona la suspensión de la cuenta de usuario (trabajador, estudiante y/o proveedor) después de haber ejecutado los intentos fallidos?	
VSII16:	¿Los SII-IES permiten gestionar, guardar y controlar el inicio y fin de la relación académica de cada estudiante?	
VSII17:	¿Los SII-IES permiten guardar bitácoras de las direcciones IP que accedieron a los SII?	
VSII18:	¿Los SII-IES permiten administrar la identidad en cada sesión configurando el tiempo de inactividad de la cuenta de usuario?	
VSII19:	¿Los SII-IES permiten el acceso solo a los datos académicos que se son necesarios para el desempeño del trabajo de cada usuario? es decir si el usuario profesor solo tendrá acceso a los datos académicos de sus estudiantes y las asignaturas.	
VSII20:	¿Los SII-IES gestionan alertas de seguridad cuando existen intentos de instrucción a los SII?	
VSII21:	¿Los SII-IES gestionan técnicas de control de acceso, tales como Control de acceso discrecional (DAC), Control de acceso mandatorio (MAC) y/o Control de acceso basado en roles (RBAC) así como la asignación de privilegios de acceso?	
VSII22:	¿Están claramente definidos los perfiles de usuarios (estudiantes, administrativos, docentes, proveedores) en los SII-IES?	
VSII23:	¿Los SII-IES establecen grupos de usuarios utilizando las técnicas de control de acceso (RBAC), (DAC) y/o (MAC)?	
VSII24:	¿Los SII-IES controlan la creación de usuarios genéricos?	
METAS	CUMPLE 1	
	NO CUMPLE 0	
OBSERVACIONES		
Fuente de Información	Normas COBIT, Normas ISO, Leyes Ecuatorianas	

Fuente: elaboración propia (2022)

Para el indicador de gestión de control de acceso se plasma las variables VSII25 a la VSII44 (tabla 9).

Tabla 9
Indicador de gestión - Control de Acceso

INDICADOR- CONTROL DE ACCESO		
Indicador	**INSII02**	
Definición	El indicador permite determinar y hacer un seguimiento, en cuanto a la seguridad en el acceso en Sistemas de Información Integrados, en lo relacionado a la asignación de permisos, contraseñas y responsabilidades.	
Objetivo	Hacer seguimiento a la asignación de recursos y responsabilidades, dentro del marco de seguridad en el acceso a los SII.	
TIPO DE INDICADOR		
Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES		**FÓRMULA**
VSII25:	Número de usuarios que tienen el conocimiento que deben asegurar las contraseñas de acceso a los SII	(VSII25/VSII26) *100
VSII26:	Número de usuarios que tiene permisos para ingresar a los SII	
VSII27:	Número de empleados que validan el login y contraseña para acceder a los SII	(VSII27/VSII28) *100
VSII28:	Número de usuarios que tiene permisos para ingresar a los SII	
VSII29:	Número de capacitaciones implementadas sobre el aseguramiento de las contraseñas de acceso a los SII	(VSII29/VSII30) *100
VSII30:	Número de capacitaciones que se planearon implementar sobre el aseguramiento de las contraseñas de acceso a los SII	
VSII31:	Número de usuarios son su respectivo rol definido para el puesto de trabajo.	(VSII31/VSII32) *100
VSII32:	Número de usuarios con roles definidos después de un tiempo determinado, tomando como referencia permanencia de un año de trabajo.	
VSII33:	Número de usuarios (trabajador, estudiante y/o proveedor)suspendidos después de haber ejecutado los intentos fallidos	(VSII33/VSII34) *100
VSII34:	Número de alertas de seguridad cuando existen intentos de instrucción a los SII	
VSII35:	Número de usuarios suspendidos el acceso a los SII	(VSII35/VSII36) *100
VSII36:	Número de usuarios que terminan la relación laboral y/o termina relación académica, tomando como referencia un año	
VSII37:	Número de usuarios por perfil definido (estudiantes, administrativos, docentes, proveedores)	(VSII37/VSII38) *100
VSII38:	Número de usuarios de estudiantes, administrativos, docentes, proveedores)	
VSII39:	Número de veces que se realiza una verificación constante de los derechos de accesos de los usuarios (trabajador, estudiante y/o proveedor).	(VSII39/VSII40) *100
VSII40:	Número de veces que se propuso realizar una verificación sobre los derechos de acceso de los usuarios trabajador, estudiante y/o proveedor)	
VSII41:	Número de grupos de usuarios utilizando las técnicas de control	VSII41/VSII42) *100
VSII42:	Número de técnicas de control	
VSII43:	Número de accesos a los SII, con usuario genérico	VSII43/VSII44) *100
VSII44:	Número de usuarios genéricos creados.	
METAS		
MÍNIMA 75-80%	**SATISFACTORIA** 80-90%	**SOBRESALIENTE** 100%
OBSERVACIONES		
Fuente de Información		
Normas COBIT, Normas ISO, Leyes Ecuatorianas		

Fuente: elaboración propia (2022)

De igual forma, se obtiene las variables comprendidas entre VSII45 y VSII52 para el Indicador de cumplimiento-responsabilidad del personal (tabla 10) y para el indicador de gestión -responsabilidad del Personal la tabla 11.

Tabla 10
Indicador de Cumplimiento- Responsabilidad del Personal

INDICADOR- REVISIÓN RESPONSABILIDAD DEL PERSONAL		
Indicador	**INSII03**	
Definición	Nivel de responsabilidad del personal que manipula Sistemas Integrados de Información	
Objetivo	Medir el nivel de capacitación al Recurso humano y su adjudicación en relación a la seguridad de la información para Sistemas de información Integrados.	
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES		**FÓRMULA**
VSII45:	¿Las IES dan a conocer a los empleados, estudiantes o proveedores políticas y procedimientos apropiados para la manipulación de la información y de los SII?	VSIIX=1 (**SI** se Evidencia) VSIIX=0 (**NO** se Evidencia)
VSII46:	¿En las IES existen planes que enseñen o concienticen sobre la necesidad de proteger la información de los SII, entregada y encomendada a los usuarios (empleados, estudiantes o proveedores)?	
VSII47:	¿Cuándo la información que reposa en los SII es quebrantada o existe fuga de información, las IES tienen reglamentos, procedimientos y/o normas disciplinarias para sancionar a los usuarios?	
VSII48:	¿Las IES evalúan periódicamente el cumplimiento de los reglamentos, normas y/o procedimientos de responsabilidad de seguridad de los usuarios en cuanto a sus funciones en los SII?	
VSII49:	¿Las IES definen entes responsables en distintos grados de seguridad de los SII?	
VSII50:	¿En las IES existen controles para garantizar el cumplimiento de estándares de seguridad en los SII?	
VSII51:	¿Los SII-IES permite guardar, gestionar y controlar las altas y bajas de los usuarios?	
VSII52:	¿Los SII-IES permiten gestionar y controlar los permisos en el cese o cambio de cargos y puestos de trabajo?	
METAS		
MÍNIMA 75-80%	**SATISFACTORIA** 80-90%	**SOBRESALIENTE** 100%
OBSERVACIONES		
Fuente de Información		
Normas COBIT, Normas ISO, Leyes Ecuatorianas		

Fuente: elaboración propia (2022)

Tabla 11
Indicador de Gestión- Responsabilidad del Personal

INDICADOR- REVISIÓN RESPONSABILIDAD DEL PERSONAL		
Indicador	**INSII04**	
Definición	El indicador permite medir la aplicación de temas de sensibilización en seguridad al acceso de la información en SII de las IES por parte de los usuarios finales.	
Objetivo	Establecer la garantía de un plan de formación y sensibilización preliminarmente definido como canal para el control de incidentes de seguridad en el acceso a la información de los SII en las IES.	
TIPO DE INDICADOR		
Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES		**FÓRMULA**
VSII53:	Número de capacitaciones implementadas sobre políticas y procedimientos apropiados para la manipulación de la información y de los SII en las IES	(VSII53/VSII54) *100
VSII54:	Número de capacitaciones que estaban planificadas sobre políticas y procedimientos apropiados para la manipulación de la información y de los SII en las IES	
VSII55:	Número de incidentes por fuga de información	(VSII55/VSII56) *100
VSII56:	Número de sanciones y/0 normas disciplinarias después de encontrar incidentes por fuga de información	
VSII57:	Número de evaluaciones a los usuarios sobre la responsabilidad de la seguridad en las funciones en los SII	(VSII57/VSII58) *100
VSII58:	Total, de evaluaciones planificadas	
VSII59:	Número de controles implementados para garantizar el cumplimiento de estándares de seguridad en los SII.	(VSII59/VSII60) *100
VSII60:	Número de controles que se plantearon para garantizar el cumplimiento de estándares de seguridad en los SII.	
VSII61:	Número de veces que los SII han gestionado las altas y bajas de los usuarios automáticamente en el último año	(VSII61/VSII62) *100
VSII62:	Número de altas y bajas en el último año	
VSII63:	Número de veces que los SII han gestionado automáticamente los permisos de usuario por cese, cambio de cargo y/0 puesto de trabajo en el último año.	(VSII63/VSII64) *100
VSII64:	Número de permisos de usuario por cese, cambio de cargo y/0 puesto de trabajo en el último año	
METAS		
MÍNIMA 75-80%	**SATISFACTORIA** 80-90%	**SOBRESALIENTE** 100%
OBSERVACIONES		
Fuente de Información		
Normas COBIT, Normas ISO, Leyes Ecuatorianas		

Fuente: elaboración propia (2022)

Finalmente, el Indicador de cumplimento contiene 8 ítems, entre las variables VSII65 y VSII72 (tabla 13) y para el indicador de gestión de Control Criptográfico resultan las variables VSII73 - VSII82 (tabla 14).

Tabla 13
Indicador de cumplimiento- Control Criptográfico

INDICADOR- CONTROL CRIPTOGRÁFICO		
Indicador	**INSII05**	
Definición	Nivel de seguridad de un archivo mediante la codificación del contenido en Sistemas Integrados de información	
Objetivo	Identificar la existencia de lineamientos, normas o estándares en cuanto a la preservación de la confidencialidad tanto en la información como en su almacenamiento	
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES		**FÓRMULA**
VSII65:	¿Las IES han determinado políticas, normas y/o procedimientos para cifrar documentos que contengan datos personales de nivel alto o datos sensibles almacenados en los SII?	VSIIX=1 (**S**I se Evidencia) VSIIX=0 (**NO** se Evidencia)
VSII66:	¿Las IES han determinado políticas, normas y/o procedimientos en particular para cifrar la información con un nivel alto de confidencialidad, o con datos personales de nivel alto, durante su almacenamiento como durante su distribución o transmisión a través del SII?	
VSII67:	¿Las IES han determinado políticas, normas y/o procedimientos para gestiona el nivel de seguridad, cifrar todos los soportes de información que pueden extraerse del ordenador, tales como discos, llaves de memoria USB y dispositivos análogos, y la información de nivel alto que se contenga en ordenadores portátiles, con el fin de evitar fuga de información contenida en los SII?	
VSII68:	¿Las IES han determinado políticas, normas y/o procedimientos para cifrar los documentos digitales utilizados para la comunicación en los SII?	
VSII69:	¿Las IES han determinado políticas, normas y/o procedimientos para enviar correos electrónicos con información confidencial que manejan los SII?	
VSII70:	¿Los SII-IES permiten cifrar los datos personales?	
VSII71:	¿Los SII-IES permiten la gestión de llaves para cifrar la información que contiene?	
VSII72:	¿Los SII-IES permiten el cifrado de la contraseña del usuario desde la base de datos?	
METAS	CUMPLE 1	
	NO CUMPLE 0	
OBSERVACIONES		
Fuente de Información	Normas COBIT, Normas ISO, Leyes Ecuatorianas	

Fuente: elaboración propia (2022)

Tabla 14
Indicador de gestión- Control Criptográfico

INDICADOR- CONTROL CRIPTOGRÁFICO	
Indicador	**INSII06**
Definición	El indicador permitirá establecer y hacer seguimiento al compromiso de la necesidad de la codificación del contenido en Sistemas Integrados de información en las IES
Objetivo	Hacer el seguimiento a la inclusión de la necesidad de codificar la información en cuanto a la preservación de la confidencialidad a través de los SII, dentro del marco de seguridad y privacidad en el acceso en los SII de las IES.

Cont... Tabla 14

TIPO DE INDICADOR		
Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES		**FÓRMULA**
VSII73:	Número de capacitaciones sobre procedimientos para cifrar documentos que contengan datos personales de nivel alto o datos sensibles almacenados en los SII	(VSII73/VSII74) *100
VSII74:	Número de capacitaciones programadas	
VSII75:	Número de capacitaciones sobre procedimientos para cifrar la información con un nivel alto de confidencialidad, o con datos personales de nivel alto, durante su almacenamiento como durante su distribución o transmisión a través del SII	(VSII75/VSII76) *100
VSII76:	Número de capacitaciones planificadas	
VSII77:	Número de capacitaciones sobre los procedimientos para gestionar el nivel de seguridad, cifrar todos los soportes de información que pueden extraerse del ordenador, tales como discos, llaves de memoria USB y dispositivos análogos, y la información de nivel alto que se contenga en ordenadores portátiles, con el fin de evitar fuga de información contenida en los SII.	(VSII77/VSII78) *100
VSII78:	Número de capacitaciones programadas	
VSII79:	Número de requisitos atendidos para cifrar datos personales	(VSII79/VSII80) *100
VSII80:	Número de requisitos solicitados para cifrar datos personales	
VSII81:	Número de password ingresados	(VSII81/VSII82) *100
VSII82:	Número de paswword cifrados guardados	
METAS		
MÍNIMA 75-80%	**SATISFACTORIA** 80-90%	**SOBRESALIENTE** 100%
OBSERVACIONES		
Fuente de Información		
Normas COBIT, Normas ISO, Leyes Ecuatorianas		

Fuente: elaboración propia (2022)

Por consiguiente, tras definir los dominios, asentar en metas y someter los cuestionarios a juicio de expertos, se plantean los indicadores de cumplimiento y gestión para control de acceso, responsabilidad del Personal y control Criptográfico, los mismos que pretenden ser una guía práctica para identificar las falencias que impiden el cumplimiento de los objetivos de estos procesos (Marchand y Vega, 2020), analizando el grado de ejecución de las políticas a seguir para los procesos de Acceso de a la Información, Responsabilidad del Personal y Lineamientos para cifrado en los SII-IES.

Por lo tanto, el objetivo de cada indicador es tener un mayor control sobre el proceso, permitiendo visualizar oportunidades de mejora y estrategias en respuesta a la protección integral, aumento de la eficiencia y adecuado desempeño de los SII en las IES (Contreras et al, 2017).

Además, la propuesta de indicadores de cumplimiento, pretenden ser una ayuda para conocer el grado de cumplimiento de seguridad en la SII-IES (Schroeder y Trinh, 2022); mientras que los indicadores de gestión, son una propuesta como base para que las IES administren de forma adecuada los procesos del SII.

5. Conclusiones

Los criterios de seguridad de la información expuestos en este documento plasman la problemática de seguridad que existente en los SII en la educación superior de la región y del país, considerando a estos sistemas un blanco directo para robo de información. En definitiva, se evidencia la resistencia y desgaste ante el compromiso que significa invertir esfuerzos en seguridad en el acceso a la información; ante ello, las IES del Ecuador deben tomar conciencia que no son tan diferentes entre sí y que es necesario la colaboración mutua en investigaciones pertinentes sobre la definición de un SII bajo criterios de seguridad, lo cual permitirá enfrentar los desafíos y problemas de acceso a la información a las que se afrontan actualmente.

Además, las IES deben mejorar los procedimientos interinstitucionales y redefinir métodos que comprometan al personal docente, administrativo y estudiantil a asumir la gran misión de apoderarse responsablemente de los planes, programas, políticas, normas y herramientas para el acceso, la manipulación y la seguridad de los sistemas de información, siempre con el respaldo de expertos del área que creen estrategias de seguridad proactiva y mantengan actualizados los criterios seguridad para el control de acceso y manipulación de la información. No se trata de que tan seguro sea el control de ingreso a los sistemas de información integrados, sino de que tan comprometidos estén los empleados con la seguridad para no dejar perceptiblemente información que esté al alcance de hackers.

Los indicadores de control y de gestión son una alternativa de seguridad de información, puesto que concentran variables de fácil entendimiento tanto para directivos como para los docentes y administrativos de una Institución de educación Superior, además son una opción de control para que el área de Tecnologías de la Información pueda prever alguna eventualidad.

Referencias bibliográficas

Altamirano Di Luca, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Avances, 21*(2), 248-263. http://www.ciget.pinar.cu/ojs/index.php/publicaciones/article/view/440/1653

Amón, J. P., y Zhindón Mora, M. (2020). Modelo de Gobierno y Gestión de TI, basado en COBIT 2019 e ITIL 4, para la Universidad Católica de Cuenca. *Revista Científica FIPCAEC, 5*(16), 219-239. https://doi.org/10.23857/fipcaec.v5i14.168

Arevalo, F., Ingrid, O., Peñaherrera, M., y Suarez, V. (2020). Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información. *Dominio de las Ciencias, 6*(2). SearchDataCenter en Español: https://dominiodelasciencias.com/ojs/index.php/es/article/view/1197

Barajas, C., y Orduz, A. (2019). Gestión del cambio: el nuevo desafío para mejorar la calidad de la educación superior. *Revista de Investigación, 43*(98). https://www.redalyc.org/articulo.oa?id=376168604012

Calabrese, J., Muñoz, R., Pasini, A., Esponda, S., Boracchia, M., y Pesado, P. (2017). Asistente para la evaluación de características de calidad de producto de software propuestas por ISO/IEC 25010 basado en métricas definidas

usando el enfoque GQM. *XXIII Congreso Argentino de Ciencias de la Computación*, 660-671.

Carrizo, L., Sauvageot, C., y Bella, N. (2003). Information tools for the preparation and monitoring of education plans. *Unesco*, 117. https://unesdoc.unesco.org/ark:/48223/pf0000132306

CEDIA. (2014). *Informe de Resultados de la "1° encuesta de Seguridad de la Información en Universidades Ecuatorianas miembros de CEDIA*. La Universidad Particular de Loja y la Red Nacional de Educación e Investigación del Ecuaador , Loja. https://csirt.cedia.edu.ec/wp-content/uploads/2014/05/Informe-de-Resultados-2014.pdf

Cicchetti, D. (1994). Guidelines, Criteria, and Rules of Thumb for Evaluating Normed and Standardized Assessment Instrument in Psychology. *Psychological Assessment*, 284-290.

Contreras, F., Olaya, J., y Matos, F. (2017). *Gestión por procesos, indicadores y estándares para unidades de información* (Primera edición ed.). F. F. Uribe, Ed.

Cornford, T., y Shaikh, M. (1992). *Introduction to information systems.* University of London. https://www.studocu.com/row/document/kenyatta-university/library-and-information-science/introduction-to-information-systems/9072537

Escobar Pérez, J., y Cuervo Martínez, Á. (2008). Validez de Contenido y Juicio de Expertos:Una Aproximacion a su Utilizacion. *Avances en Medición, 6*(1), 27-36. http://www.humanas.unal.edu.co/psicometria/files/7113/8574/5708/Articulo3_Juicio_de_expertos_27-36.pdf

Fleiss, J., Levin, B., y Paik, M. C. (2003). *Statistical methods for rates and proportions.* New York: John Wiley & Sons. https://doi.org/10.1002/0471445428

Fontalvo, T., y De la Hoz, E. (2018). Diseño e Implementación de un Sistema de Gestión de la Calidad ISO 9001:2015 en una Universidad Colombiana. *Formación universitaria, 11*(1). https://doi.org/10.4067/S0718-50062018000100035

Govea, J. (2021). Sistema de planificación de recursos empresariales (ERP) y su influencia en los procesos de negocio de empresas distribuidoras de productos de consumo masivo en Lima Metropolitana en el 2019. *Industrial Data, 24*(1). https://doi.org/0000-0003-1043-709X

Landis, R., y Koch, G. (1977). The measurement of observer agreement for categorical data. *International Biometric Society33, 33*(1), 159-174. https://www.jstor.org/stable/2529310

Lapiedra, R., Julian, B., Puig, A., y Martinez, L. (2021). *Introducción a la gestión de sistemas de información en las empresas.* https://doi.org/10.6035/Sapientia178

Leguizamón, M., María, B., y León, C. (2020). Análisis de ataques informáticos mediante Honeypots en la Universidad Distrital Francisco José de Caldas. *Ingeniería y competitividad, 22*(2). https://doi.org/10.25100/iyc.v22i2.8483

Marchand, W., y Vega, E. (2020). Modelo Balanced Scorecard para los controles críticos de seguridad informática según el Center for Internet Security (CIS) . *Interfases* (013). https://doi.org/10.26439/interfases2020.n013.4876

Muyón, C., Guaranda, T., Vargas, G., y Quiña, G. (septiembre de 2019). Esquema Gubernamental de Seguridad de la Información EGSI

y su aplicación en las entidades públicas del Ecuador. *Revista Ibérica de Sistemas e Tecnologias de Informação*(E18), 310-317. https://www.risti.xyz/issues/ristie18.pdf

Okoli, C., y Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Social Science Research Network, 10*(26). https://doi.org/https://doi.org/10.2139/ssrn.1954824

Penfield, R., y Giacobbi, P. (2004). Applying a score confidence interval to Aiken's item content-relevance index. *Measurement in Physical Education and Exercise Science*, 213-225.

Quinteros, B., Godoy, M., y Gómez, M. (2023). Aportes Bibliográficos sobre la realción entre Gbernanza ,planeación Universitaria y Desempeño Institucional. *Journal of the Academy, 8*, 148-163. https://doi.org/10.47058/joa8.8

Quirumbay, D., Castillo, C., y Coronel, I. (2022). Una revisión del Aprendizaje profundo aplicado a la ciberseguridad. *Revista CTU, 9*(1). https://doi.org/10.26423/rctu.v9i1.671

Rainho, F., y Barreiros, J. (2019). Agile Process Optimization: An Approach Using the CMMI and GQM. *14th Iberian Conference on Information Systems and Technologies (CISTI)*, (pp. 1-6). Coimbra. https://doi.org/10.23919/CISTI.2019.8760924

Schroeder, K., y Trinh, H. (2022). Performance Measurement Guide for Information Security. *Computer security resourse center*, 55-80. https://doi.org/10.6028/NIST.SP.800-55r2.iwd

Solingen, R. (1999). *The Goal/Question/Metric Method:a practical guide for quality improvement of software development.* London: McGraw-Hill.

Torres, K., y Lamenta, P. (2015). La gestión del conocimiento y los sistemas de información en las organizaciones. *Revista Científica Electrónica de Ciencias Gerenciales, 11*(32), 3-20. http://www.redalyc.org/articulo.oa?id=78246590001

Ventura-León, J. L., Arancibia, M. & Madrid, E. (2017). La importancia de reportar la validez y confiabilidad en los instrumentos de medición: Comentarios a Arancibia et al. *Revista médica de Chile*, *145*(7), 955-956. https://dx.doi.org/10.4067/s0034-98872017000700955

Zabala, R., Granja, L., Calderón, H., y Velastegui, L. (2021). Enterprise resource planning (ERP) effect on organizational management and user satisfaction in Riobamba, Ecuador. *Información tecnológica*, *32*(5), 101-110. https://dx.doi.org/10.4067/S0718-07642021000500101