UNIVERSIDAD TÉCNICA DEL NORTE
Innovation & Development in Engineering and Applied Science
Journal homepage: https://revistasojs.utn.edu.ec/index.php/ideas

Seguridad y privacidad de los datos en la era de la información en el Ecuador

Data security and privacy in the information age in Ecuador

Cristopher Quijije Menendez, Wilmer Moreira Sánchez
Universidad Técnica de Manabí, Av. Universitaria, Portoviejo, Ecuador

Recibido: 10/06/2024, Aceptado: 30/07/2025
Autor de correspondencia: Cristopher Quijije: cquijije8250@utm.edu.ec
Correo adicional: wilmer.moreira@utm.edu.ec
DOI: https://doi.org/10.53358/ideas.v7i2.1287

PALABRAS CLAVE

Seguridad de la información,
protección de datos,
políticas de seguridad,
Ecuador,
vulnerabilidades,
buenas prácticas.

RESUMEN

La digitalización en el Ecuador en los últimos años ha aumentado, y también la exposición de datos, tanto personales como organizacionales; esta exposi-ción incrementa el riesgo a ataques cibernéticos, es necesario tener conoci-miento de los riesgos que pueden existir actualmente y las recomendaciones para evitarlos. Este estudio presenta una revisión sistemática de la literatura con el objetivo de facilitar recomendaciones y reconocer riesgos en un Ecuador cada vez más digitalizado, utilizando la metodología PRISMA, de-mostrando que las princi-pales amenazas son ciberataques sofisticados y una falta de conocimiento por parte de los usuarios hacia la ciberseguridad. Aun-que existe la Ley Orgánica de Protección de Datos Personales (LOPDP, por sus siglas) hay desafíos para una aplicación efectiva. En conclusión, se pre-sentan estrategias importantes, como pueden ser: marcos normativos, capaci-tación continua del personal sobre ciberataques y el uso de nuevas tecnolo-gías para evitar dichos ciberataques. Estas medidas, alineadas con estándares internacionales, son importantes para fortalecer la resiliencia tecnológica de Ecuador frente a las amenazas del entorno digital.

KEYWORDS

Information security,
data protection,
security policies,
Ecuador,
vulnerabilities,
good practices.

ABSTRACT

Digitalization in Ecuador has increased in recent years, and with it the exposure of both personal and organizational data. This exposure increases the risk of cyberattacks. It is necessary to be aware of the risks that currently exist and recommendations for avoiding them. This study presents a systematic literature review with the aim of providing recommendations and recognizing risks in an increasingly digitalized Ecuador, using the PRISMA methodology. It demonstrates that the main threats are sophisticated cyberattacks and a lack of user awareness regarding cybersecurity. Although the Organic Law on Personal Data Protection (LOPDP) exists, there are challenges to its effective implementation. In conclusion, important strategies are presented, such as regulatory frameworks, ongoing staff training on cyberattacks, and the use of new technologies to prevent such cyberattacks. These measures, aligned with international standards, are important for strengthening Ecuador's technological resilience against threats from the digital environment.

1. Introducción

El desarrollo tanto tecnológico como digital en el Ecuador han puesto en un lugar importante a la seguridad y privacidad de datos. Uno de los problemas más gra-ves en ciberseguridad, el cual afecta a muchas naciones, es la falta de reglas o marcos técnicos. En el Ecuador, la integración de servicios digitales y el uso fre-cuente de internet, por parte de las personas y empresas, ha cambiado el panora-ma de los riesgos que enfrentan, lo que representa un desafío para la ciberseguri-dad en el Ecuador. Para hacer que la ciberseguridad avance se requiere hacer esfuerzos en áreas de leyes, educación, y ciberseguridad, en este contexto [1], comparte que la capacitación adecuada de policías, fiscales y jueces es esencial para asegurar que los delitos cibernéticos se investiguen y procesen correctamen-te. Además, el avance tecnológico rápido implica que el COIP debe ser revisado y actualizado periódicamente para mantenerse relevante frente a nuevas formas de cibercrimen.

Algunos estudios señalan que muchos usuarios desconocen sobre temas de se-guridad digital, lo que permite que los delincuentes cibernéticos se aprovechen muy fácilmente. [2]. afirma que, aunque existen numerosos estudios acerca de las estrategias de protección de datos a nivel mundial, la indagación sobre su aplica-ción concreta en las entidades gubernamentales de Ecuador es escasa; junto ello, resultados de encuestas sugieren que los ataques cibernéticos y delitos informá-ticos están siendo un problema que avanza aceleradamente. La poca concientiza-ción que existe en la materia, y aunque exista la Ley Orgánica de Protección de Datos Personales, existen desafíos para una buena aplicación, donde se puede asegurar que, en el sector estatal o privado, control y vigilancia no se ponen mu-chas veces en práctica.

El presente estudio se compone de literatura utilizando la metodología PRISMA, ya que examinando las principales amenazas y puntos débiles que afec-tan la seguridad de la información en el Ecuador, y también las estrategias y su-gerencias para mejorar la protección de los datos. El objetivo es ofrecer un marco de referencia que apoye el desarrollo de políticas y planes alineados con están-dares internacionales, fortaleciendo así la resiliencia digital del país. Además, se espera que los resultados de esta investigación sirvan como guía para tomar deci-siones en tema de ciberseguridad, concientizando así una cultura de protección de datos y estimulando el uso de tecnologías avanzadas para reducir riesgos en un entorno digital que continuamente está cambiando.

2. Metodología

2.1. Materiales utilizados

2.1.1. Bases de datos científicas

Se utilizaron bases de datos científicas reconocidas. Estas plataformas ofrecieron acceso a artículos científicos, documentos técnicos y normativas que fueron con-sideradas importantes respecto a este tema. Al seleccionar las bases de datos, se logró garantizar la calidad de la información obtenida. Las bases utilizadas fue-ron: Scielo, Dialnet, ScienceDirect, IEEE Xplore.

2.2. Tipo de estudio

Este estudio tiene un enfoque cualitativo de tipo descriptivo, por lo que su obje-tivo principal es explorar y detallar el estado actual de la seguridad y privacidad de los datos en Ecuador durante la era de la información. Este enfoque busca identificar y describir las principales amenazas y vulnerabilidades que enfrentan las organizaciones y los usuarios en el Ecuador.

Para obtener los datos, se empleó el método de análisis documental, revisando y evaluando fuentes con normativas, políticas públicas, estudios previos y do-cumentos técnicos relacionados con la seguridad de la información y la privaci-dad de los datos. Este método ayuda a reunir información importante para cons-truir una base sólida de conocimiento.

Con este enfoque metodológico, no se pretende solo ilustrar las características específicas del entorno ecuatoriano, sino también considerar prácticas y estrate-gias exitosas implementadas en otras regiones que podrían ser adaptadas en el Ecuador.

2.3. Metodología PRISMA

La metodología PRISMA 2020 fue empleada como guía para estructurar esta re-visión sistemática. [3] menciona que, es útil en muchos aspectos críticos, ya que pueden proporcionar una síntesis del estado del conocimiento en un área deter-minada, a partir de la cual se pueden identificar futuras prioridades de investiga-ción, abordar preguntas que

de otro modo no podrían ser respondidas por estu-dios individuales, identificar problemas en la investigación primaria que deben ser corregidos en futuros estudios y generar o evaluar teorías sobre cómo o por-que ocurren fenómenos de interés.

El uso de la declaración PRISMA 2020 tiene el potencial de beneficiar a mu-chos grupos de interés. Las publicaciones completas de revisiones sistemáticas permiten a los lectores evaluar la idoneidad de los métodos y, por lo tanto, la fiabilidad de los hallazgos [3].

Se tomó como guía la metodología PRISMA, leyendo el documento detallado por [3], para lo cual se procedió a seguir con los siguientes pasos para la elabora-ción de este articulo:

2.3.1. Identificación de la Pregunta de Investigación

Primero se realizaron las preguntas de investigación, para obtener mejores resul-tados al momento de la investigación; dichas preguntas tenían que ser claras y específicas, ya que en la era de la información, las organizaciones se enfrentan a un panorama cada vez más complicado de amenazas y vulnerabilidades en la seguridad de sus datos.

Los ecuatorianos pueden llegar a tener riesgos si no tienen estrategias claras, provocando perdidas, ya sean económicas o de reputación. Es importante obtener estrategias específicas que puedan ser usadas para reducir riesgos, y hacerles frente a los desafíos que existen en seguridad y privacidad de los datos en el Ecuador. Se intenta abordar este problema y proporcionar información sobre vulnerabilidades y recomendaciones, usando las siguientes preguntas de investigación:

P1: ¿Cuáles son las principales amenazas y vulnerabilidades en la seguridad y privacidad de los datos en el Ecuador?

P2: ¿Cuáles son las estrategias más efectivas para mitigar las vulnerabilidades y desafíos relacionados con la seguridad y privacidad de los datos en el Ecuador?

2.3.2. Desarrollo de la Estrategia de Búsqueda

Los artículos seleccionados fueron utilizados bajo una estrategia de búsqueda sólida utilizando operadores booleanos (AND, OR, NOT) y palabras clave que representan los conceptos importantes para esta investigación. Esta estrategia fue ajustada de acuerdo a las particularidades y funcionalidades de las bases de datos elegidas, asegurando que las búsquedas fueran efectivas.

2.3.3. Selección de fuentes

Las bases de datos empleadas en esta revisión fueron Scielo, Dialnet, ScienceDi-rect e IEEE Xplore, todas ampliamente reconocidas por la calidad de sus publica-ciones científicas en temas como tecnologías de la información, ciberseguridad y protección de datos. La selección de estas plataformas se realizó con el objetivo de garantizar el acceso a literatura relevante, actualizada y diversa, alineada con los objetivos del estudio. Para detallar las fuentes utilizadas, se elaboró la Tabla 1, donde se presentan las bases seleccionadas, palabras clave utilizadas y la cadena de búsqueda.

Tabla 1: Cadena de búsqueda y palabras clave.

Bases de datos	**Palabras clave**	**Cadena de búsqueda**
Scielo	Seguridad de la información; Ciberseguridad; Protección de datos; Privacidad de datos; Políticas de seguridad; Ecuador; Ley de protección de datos; Vulnerabilidades; Buenas prácticas.	(Seguridad de información) AND (Privacidad de datos) OR (Vulnerabilidades) OR (Buenas Prácticas) OR (LEY DE PROTECCION DE DATOS) OR (ECUADOR)
IEEE Xplore		
ScienceDirect		
ZDialnet		

2.3.4. Criterios de inclusión y exclusión

Se establecieron criterios de inclusión y exclusión específicos para garantizar la pertinencia de los estudios seleccionados. La cadena de búsqueda fue diseñada utilizando operadores booleanos y palabras clave relacionadas con los temas de seguridad de la información, privacidad de datos, amenazas digitales, y protec-ción de datos en Ecuador.

La búsqueda se llevó a cabo a través de los diferentes repositorios y bases de datos anexadas, limitándose a publicaciones en español, inglés y portugués, de los últimos 6 años para garantizar la actualidad de los resultados.

Los registros recuperados fueron gestionados a través de la herramienta Mendeley para facili-tar la identificación y eliminación de duplicados.

El proceso de selección incluyó una lectura inicial de títulos y resúmenes para descartar estudios irrelevantes, seguida de una revisión completa de los textos seleccionados según los criterios predefinidos. En la Tabla 2, se detallan los cri-terios de inclusión y exclusión utilizados en esta etapa. Los estudios que cum-plieron con todos los criterios fueron finalmente incluidos en la síntesis cualita-tiva y cuantitativa.

Tabla 2: Términos de inclusión y exclusión.

Inclusión	**Exclusión**
Artículos publicados en los últimos 6 años.	Artículos publicados hace más de 6 años.
Artículos de acceso abierto.	Artículos restringidos.
Artículos con idioma inglés, español o en su defecto portugués.	Artículos con un idioma diferente al español, inglés o portugués.
Publicaciones relacionadas con la seguridad de la información, privacidad de datos y contexto ecuatoriano o latinoamericano.	Estudios que no abordan directamente la temática investigada.
Artículos indexados en las bases de datos revisadas.	Artículos que no están indexados en bases de datos revisadas.

2.3.5. Diagrama de flujo PRISMA

El proceso de selección de estudios fue documentado utilizando un diagrama de flujo PRISMA, que detalló cada etapa: desde la identificación inicial de 203,732 registros, la eliminación de duplicados, la aplicación de criterios de inclusión y exclusión, hasta la selección final de 37 artículos.

Durante la fase de cribado, se eliminaron duplicados y se aplicaron los crite-rios de inclusión y exclusión previamente establecidos. Se descartaron informes por diversas razones, como: falta de acceso al texto completo, publicaciones que no estaban relacionadas directamente con la seguridad y privacidad de los datos, estudios sin revisión por pares o que no abordaban el contexto latinoamericano o ecuatoriano. Como resultado, el número de documentos se redujo a 80 artículos potencialmente relevantes.

En la fase de evaluación de elegibilidad, se realizó una revisión detallada del contenido de estos 80 artículos. Se excluyeron 43 estudios adicionales por no cumplir con los estándares de calidad metodológica requeridos o por presentar información redundante o poco significativa para los objetivos del estudio.

Finalmente, 37 artículos cumplieron con todos los criterios y fueron seleccio-nados para su análisis en la presente investigación. En la Fig 1 se observa el dia-grama detallado para la aplicación de la metodología PRISMA, este diagrama no solo se enfoca en el proceso, sino que también busca proporcionar transparencia al describir cómo se tomaron las decisiones en cada etapa.

2.3.6. Extracción de datos

Después de seleccionar los estudios, se realizó el proceso de extraer datos. Se obtuvo información clave como el país de origen, el año de publicación, la fuente del artículo y los principales descubrimientos relacionados con la seguridad y privacidad de los datos. Estos datos fueron organizados en tablas para así tener más estructurado un análisis, asegurando que la información obtenida fuera coherente y útil para el estudio.

2.3.7. Síntesis de resultados

Los artículos elegidos fueron revisados de forma cualitativa para identificar te-mas emergentes. Se buscó resaltar las estrategias propuestas en otros contextos que podrían ser adaptadas al escenario ecuatoriano.

2.3.8. Evaluación de calidad

Se revisaron los estudios incluidos para evaluar su calidad metodológica y la validez de sus hallazgos. Esto incluyó una evaluación de los métodos utilizados en cada estudio, su relevancia para la pregunta de investigación, y la confia-bilidad de las fuentes. Solo se incluyeron aquellos estudios que cumplieron con criterios estrictos de rigor académico, asegurando que las conclusiones del artículo estuvieran fundamentadas en evidencia sólida.

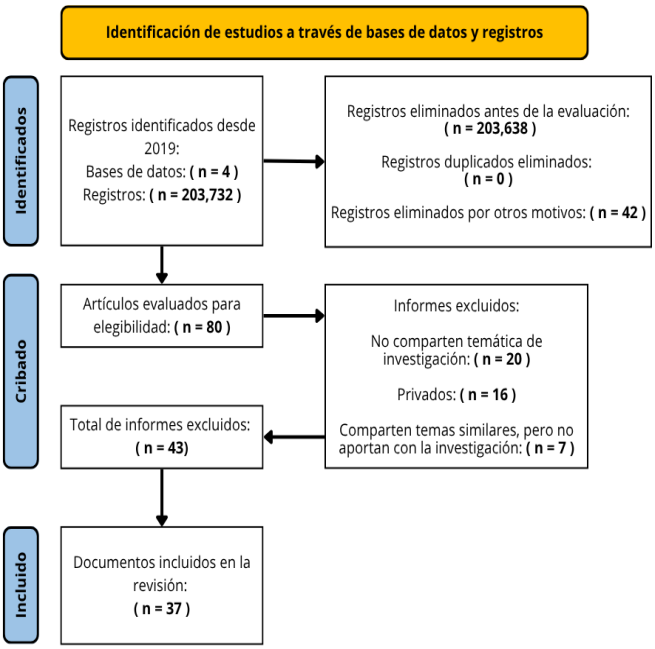

Figura 1: Diagrama de flujo PRISMA en 3 niveles.

3. Resultados

A partir de los 37 documentos seleccionados, se procedió a analizar los datos con el objetivo de identificar la distribución de registros por país relacionados con nuestro tema de estudio. La Fig 2 presenta un resumen detallado de la cantidad de registros obtenidos por cada país, lo que nos permite observar la relevancia y contribución de cada región al análisis.

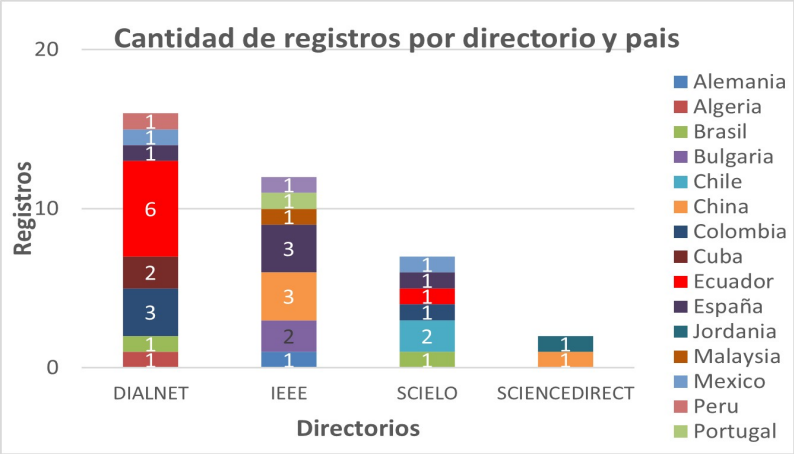

Figura 2: Cantidad de Registros por Directorio y País.

Como se puede observar en la Fig 2, se identificaron artículos provenientes de diversos países, lo que evidencia el interés global en las temáticas de seguridad y privacidad de los datos. Ecuador lidera la lista con 7 artículos, lo cual resalta el enfoque nacional de la investigación. Le siguen España con 5 artículos, poste-riormente Colombia y China, con 4 artículos cada uno. Otros países como Brasil, México, Bulgaria, Chile y Cuba también aportaron al análisis, con 2 artículos cada uno. Finalmente, se encontraron contribuciones individuales de países co-mo Argelia, Malasia, Suecia, Jordania, Portugal, Perú y Alemania, cada uno con un artículo. Esta diversidad geográfica demuestra la relevancia internacional de las amenazas y soluciones relacionadas con la protección de datos.

Por otra parte, la Fig 3 complementa este análisis al mostrar la distribución de los artículos seleccionados por

región. En ella, se observa que América del Sur lidera con un 43 %, seguida por Europa con un 27 %, Asia con un 16 %, América Central y el Caribe 11 % y África con un 3 %. Este desglose regional refuerza la diversidad y representatividad de las investigaciones incluidas, destacando la contribución de diversas partes del mundo en el estudio de seguridad y privacidad de los datos.

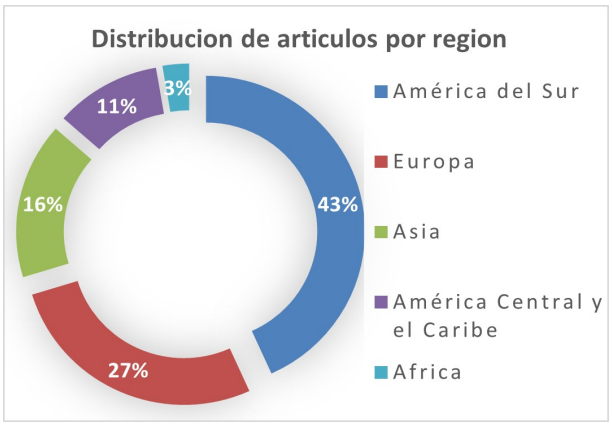

Figura 3: Distribución de artículos por región.

Se puede observar una predominancia de investigaciones provenientes de América del Sur, que concentra un 43 % (16 artículos), lo cual refleja un interés significativo en esta región por abordar los temas de seguridad y privacidad de la información. Europa sigue en relevancia con un 27 % (10 artículos), mientras que Asia aporta con un 16 % (6 artículos). América Central y el Caribe contribuyen con 11 % (4 artículos), y África con un 3 % (1 articulo). Esta diversidad regional pone de manifiesto el alcance global de los desafíos y soluciones relacionados con la protección de datos, aunque con un énfasis notable en las regiones de América del Sur y Europa. Este análisis resalta las diferencias regionales en la investigación sobre seguridad y privacidad de datos, mostrando una fuerte con-centración en regiones con mayor infraestructura tecnológica y recursos acadé-micos.

3.1. Seguridad y privacidad de los datos en el Ecuador

[2] menciona que, la integración y adaptación de tecnologías de vanguardia para fortalecer la seguridad de la información en el sector público de Ecuador es una laguna notable en la literatura especializada, y a pesar del creciente interés en tecnologías como la inteligencia artificial y el blockchain para la seguridad de la información, existe un vacío en cuanto a investigaciones sobre su implementa-ción efectiva en las instituciones públicas ecuatorianas y los desafíos vinculados a su adopción.

En [4] se argumenta que, a nivel ético, el principio de autodeterminación informati-va debe permitir a las personas controlar sus datos, además se deben establecer mecanismos de responsabilidad y transparencia para las entidades que los ges-tionan, evaluando también la perpetuación de sesgos y discriminaciones en el uso de la IA. Por ello, Ecuador debe fortalecer sus capacidades técnicas y opera-tivas, concienciar sobre la relevancia de la reserva de los datos, la instrucción de estructuras de gobernanza y rendición de cuentas que aseguren la utilización ética y responsable de los avances tecnológicos, salvaguardando los derechos fundamentales de los ciudadanos.

En este contexto, [2] propone que la normativa y legislación ecuatoriana sobre seguridad informática revela que, si bien se ha establecido una sólida base legal para la protección de datos en el ámbito público, aún persisten áreas significativas que requieren mejora y alineación con estándares internacionales reconocidos.

[4] indica que la era digital ha traído consigo numerosos beneficios, pero también desafíos en la confidencialidad de los datos. En el Estado ecuatoriano y otros territorios, la adopción creciente de tecnologías como internet, redes socia-les, comercio electrónico, entre otras, ha facilitado la compilación y el manejo de información personal sin que los ciudadanos den su consentimiento.

En [5] se afirma que el Ecuador necesita definitivamente enfrentar el reto de elaborar la ENC, como un acuerdo nacional, no solo en términos de prevención y san-ción del ciberdelito, sino también para disuadir posibles atacantes, identificarlos y perseguirlos con ayuda de la cooperación internacional.

3.2. Principales amenazas y vulnerabilidades

[6] observa que, aunque el sistema de información de las grandes empresas ha logrado avances positivos en la protección de seguridad en gestión y tecnología, todavía existen problemas urgentes y deficiencias basadas en la situación actual, como algunas brechas y deficiencias en la gestión de seguridad, ya que no existen muchas tecnologías y aplicaciones para aumentar la seguridad. Las protecciones tecnológicas se centran principalmente en el cortafuegos, antivirus, detección de intrusiones y tecnología de respaldo de datos.

Por consiguiente, [2] señala que la integración y adaptación de tecnologías avanzadas para aumentar la seguridad de la información en el sector público de Ecuador es una carencia destacada en la literatura especializada, añadiendo que, aunque exista un interés en tecnologías como la inteligencia artificial y el blockchain para la seguridad de la información, existe una falta de investigaciones sobre su implementación en las instituciones públicas ecuatorianas y los retos asociados a su adopción.

Por otra parte, uno de los aspectos negativos identificados en la revisión son vulnerabilidades que comprometen la seguridad y privacidad de la información en múltiples contextos organizacionales. En la Tabla 3 se han seleccionado algunas de estas vulnerabilidades, describiendo vulnerabilidades como el acceso no autorizado, las configuraciones débiles en sistemas y redes, la falta de capacitación del personal y la dependencia de tecnologías. Estas vulnerabilidades reflejan la necesidad de adoptar enfoques más completos para evitar riesgos y fortalecer las estrategias de protección de datos en las organizaciones ecuatorianas.

Tabla 3: Vulnerabilidades más comunes

Vulnerabilidad	Descripción	Autores de referencia
Por comportamiento humano	El rol que desempeñan las personas en el ámbito de seguridad es sumamente importante, teniendo en cuenta que el factor humano es el eslabón más débil en la protección de la información [**?**].	[7]; [8]; [9]
Falta de formación y cultura de ciberseguridad	La ausencia de conocimiento y comportamientos seguros puede exponer a las personas a riesgos, resaltando así la relevancia de la enseñanza sobre seguridad cibernética y la incorporación de hábitos adecuados para resguardarse en el entorno digital actual [10].	[2]; [4]; [6]; [10]; [11]; [12]; [13]; [14]; [15]; [16]
Ciberataques actualizados o más complejos	La evolución de los ciberataques requiere que las instituciones y los individuos inviertan más en ciberseguridad para enfrentar amenazas más sofisticadas [1].	[12]; [17]; [18], [19]; [20]
Falta de control de acceso	Acceso no autorizado a la alteración parcial o total de la información que se almacena estos sistemas [21].	[21]; [2]
Resistencia al cambio	La resistencia al cambio dentro de las instituciones es una vulnerabilidad que afecta la implementación de medidas de seguridad [7].	[7]

Se generó la Fig 4, el cual muestra que la vulnerabilidad más referenciada por los autores es la falta de formación y cultura de ciberseguridad (10 menciones), lo que resalta la necesidad de educar y concienciar a las personas sobre los riesgos cibernéticos y la adopción de hábitos seguros. Le siguen los ciberataques más complejos (5 menciones), que evidencian la creciente sofisticación de las ame-nazas y la urgencia de invertir en tecnologías avanzadas de protección. El com-portamiento humano (3 menciones) se confirma como un eslabón débil, desta-cando la importancia de estrategias educativas. En menor frecuencia se encuen-tran la falta de control de acceso (2 menciones) y la resistencia al cambio (1 mención), aunque estas últimas, pese a su menor relevancia en el análisis, pueden tener impactos significativos en la implementación de medidas de seguridad. Estos hallazgos subrayan la importancia de abordar tanto los factores tecnológi-cos como los humanos para mejorar la seguridad de la información.

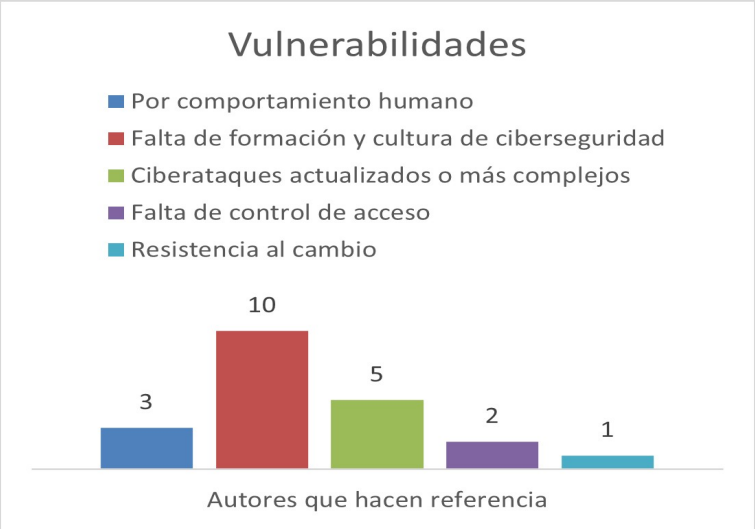

Figura 4: Vulnerabilidades más comunes.

4. Discusión

4.1. 3.3 Recomendaciones sobre políticas y normativas de seguridad aplicables para mejorar la seguridad y privacidad de los datos en el Ecuador

En su investigación, [1] expresa que, el estudio de modelos legislativos interna-cionales es esencial para identificar mejores prácticas y adaptar estrategias efec-tivas en Ecuador. Países como Estados Unidos, la Unión Europea y Japón han desarrollado marcos legales robustos que pueden servir como referencia.

Es en este contexto [22] destaca como normativa importante que, la política estatal debe basarse en estándares nacionales que combatan el cibercrimen, pro-tejan la información y aseguren la seguridad tecnológica. También es fundamen-tal definir las áreas económicas donde se supervisarán las TIC, especialmente en infraestructuras críticas, asegurando la protección de datos y promoviendo un desarrollo digital sostenible, además de que estos principios no pueden imple-mentarse sin priorizar tecnologías nacionales y garantizar la seguridad informati-va a través de una normativa adecuada.

Por otro lado [15] expresa que, las auditorías y metodologías específicas son eficaces para evaluar y fortalecer la seguridad, en donde la capacitación es esen-cial. La implementación de tecnologías avanzadas plantea retos que deben ser abordados adecuadamente, y los planes de gestión basados en normas reconoci-das son estrategias efectivas para mejorar la seguridad.

[2] afirma que, respecto a las políticas y regulaciones, a pesar de los avances en el desarrollo de un marco legal sólido para la protección de datos, se enfrentan dificultades en la eficacia de las sanciones y la aplicación de las leyes.

Haciendo referencia a computación en la nube [23], expresan las políticas de seguridad son la base de una defensa efectiva en la nube. Las organizaciones deben desarrollar y mantener políticas de seguridad claras y detalladas que cu-bran todos los aspectos de la gestión de la seguridad en la nube, desde la configu-ración de los recursos hasta la gestión de identidades y accesos. Estas políticas deben ser revisadas y actualizadas regularmente para abordar nuevas amenazas y cumplir con las regulaciones en evolución.

[5] adjunta que, las soluciones estratégicas al problema de la ciberseguridad han sido impulsadas por países de-sarrollados, sin embargo, el uso globalizado de las TlC, afecta de todas maneras a los sistemas interorganizacionales internacio-nales. Por tanto, es importante ayudar y motivar a los países en desarrollo en la elaboración de sus estrategias nacionales y coadyuvar en su implantación me-diante un ciclo de vida.

Por otro lado, [5] manifiesta que las buenas prácticas desarrolladas hasta el momento, especifican que las ENC tendrán que contemplar aspectos políticos, de gobernanza, estratégicos, operativos, técnicos y jurídicos; que deben ser organi-zados y priorizados con base en modelos y principios generales definidos, con-centrados en la protección del ciberespacio.

La Tabla 4 sintetiza las principales estrategias de ciberseguridad identificadas en diversas investigaciones, descri-biendo brevemente su propósito y citando a los autores que las respaldan. Incluye enfoques como la implementación de SGSI, auditorías, uso de nuevas tecnologías, planes de respuesta ante incidentes, mar-cos normativos, monitoreo

continuo, y programas de capacitación. Cada estrate-gia está acompañada por referencias bibliográficas que validan su efectividad, destacando su relevancia en la protección de la información y en la mitigación de amenazas cibernéticas.

Tabla 4: Estrategias de mitigación y referencias.

Estrategias	Descripción	Autores de referencia
SGSI	El SGSI debe asegurar la selección de procedimientos de control de seguridad de la información adecuados y suficientes para proteger los activos de información y generar confianza en las partes interesadas [8].	[8]; [17]; [24]; [2]
Auditorios	Las auditorías de ciberseguridad realizadas por dominios pueden ser muy efectivas para evaluar los controles y las respuestas a las amenazas cibernéticas [25].	[15]; [7]; [25]
Nuevas tecnologías	Uso de tecnologías de seguridad avanzadas, aunque con retos en recursos y capacitación especializada [2].	[2]; [12]; [26]; [6]; [27]; [20]; [16]; [28]
Planes de respuesta	Establecer planes de respuesta a incidentes que definen los procedimientos a seguir en caso de una brecha de seguridad [12].	[12]
Implementación de marcos normativos	Las organizaciones deben aplicar políticas de seguridad respaldadas por marcos como ISO 27001, COBIT 5 e ITIL para protegerse de ciberataques [9].	[2]; [9]; [13]; [29]; [15]; [17]; [30]; [31]; [27]; [24]; [23], [32]; [25]
Monitoreo continuo	El monitoreo continuo es esencial para detectar y responder a incidentes de seguridad en tiempo real [23].	[12]; [33]; [6]; [23]; [34]; [35]
Capacitación y concienciación del personal	Invertir en programas de educación sobre ciberseguridad para aumentar la conciencia pública y reducir los riesgos de ataques cibernéticos [14].	[2]; [4]; [12]; [17]; [14]; [18]; [15]; [7]; [36]; [6]; [37]; [19]; [27]; [1]; [23]; [10]; [20]; [38]

Sabiendo esto se elaboró la Fig 5, la cual muestra las diversas estrategias utiliza-das para fortalecer la seguridad de la información en las organizaciones y la fre-cuencia con la que se implementan. Las estrategias más frecuentes son la capaci-tación y concienciación del personal, que se ha implementado 19 veces, y la im-plementación de marcos normativos, con una frecuencia de 14. Estas dos estrate-gias reflejan un enfoque claro en el desarrollo de una cultura de seguridad orga-nizacional y en la alineación con las mejores prácticas normativas.

Figura 5: Estrategias de mitigación y frecuencia.

Se puede observar que las estrategias como el monitoreo continuo (6) y las nue-vas tecnologías (8) también son importantes y de mucha ayuda, aportando una adopción de medidas tecnológicas y una vigilancia constante para proteger los activos de información.

Por otro lado, las estrategias menos frecuentes incluyen el SGSI y las audito-rías, ambas con una frecuencia de 3, y los planes de respuesta, con solo 1 aplica-ción. Esto sugiere que, aunque esenciales, estas estrategias pueden no estar tan integradas o ser menos priorizadas en comparación con la formación continua del personal y la adopción de marcos regulatorios.

5. Conclusión

Se demuestra la relevancia de mejorar la seguridad y privacidad de los datos en el contexto ecuatoriano, especialmente en una época donde la digitalización está tomando fuerza y creciendo constantemente. Las principales amenazas identifi-cadas, como ciberataques avanzados, la poca capacitación en ciberseguridad y las vulnerabilidades técnicas, evidencian la necesidad de adoptar estrategias que sean de ayuda. Entre las más destacadas se encuentran la implementación de marcos normativos sólidos, la formación continua del personal y la incorpora-ción de tecnologías avanzadas como el Big data, blockchain e inteligencia artifi-cial.

Aunque Ecuador ha avanzado en el desarrollo de un marco legal, como la Ley de Protección de Datos Personales, aún enfrenta retos significativos en su aplica-ción y alineación con estándares internacionales. Este estudio da como consejo tomar medidas prácticas, como auditorías de seguridad, planes de respuesta ante incidentes y monitoreo continuo, que, junto con una cultura de ciberseguridad fortalecida, permitirían reducir riesgos y garantizar una protección eficaz de la información.

Para sobrellevar estos desafíos, es necesario poner en primer lugar la imple-mentación de políticas claras y sostenibles que refuercen la protección de datos en todos los sectores. De esta manera, Ecuador podrá consolidar su posición frente a las demandas del entorno digital global, promoviendo la confianza en los sistemas tecnológicos y asegurando un desarrollo digital inclusivo y seguro.

Referencias

[1] L. A. Ordóñez Córdova, "El Marco Legal de los Delitos Cibernéticos en Ecuador," Reincisol., vol. 3, no. 5, pp. 1447–1469, Jun. 2024, doi: 10.59282/reincisol.v3(5)1447-1469.

[2] A. A. Ávila Coello, "Seguridad de la información en instituciones públi-cas: desafíos y buenas prácticas en el contexto ecuatoriano.," Journal of Economic and Social Science Research, vol. 4, no. 2, pp. 140–156, Apr. 2024, doi: 10.55813/gaea/jessr/v4/n2/96.

[3] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," Mar. 29, 2021, BMJ Publishing Group. doi: 10.1136/bmj.n71.

[4] G. E. Barahona Martinez, Y. G. Barzola Plúas, and L. V. Peñafiel Muñoz, "El Derecho a la Protección de Datos y el Avance de las Nuevas Tecnolo-gías en Ecuador: Implicaciones Legales y Éticas," Journal of Economic and Social Science Research, vol. 4, no. 3, pp. 46–64, Jul. 2024, doi: 10.55813/gaea/jessr/v4/n3/113.

[5] M. R. Egas, G. Ninahualpa, D. Molina, and J. Diaz, Estrategia Nacional de Ciberseguridad para Paises en Desarrollo National Cybersecurity Stra-tegy for Developing Countries Case study: Ecuador proposal. 2020.

[6] Liu Jia, Research on Information Security of Large Enterprises. IEEE, 2020.

[7] D. Imbaquingo, F. Diaz, T. Saltos, S. Arciniega, D. Leon, and A. Robayo, Problemas de seguridad de la información en Instituciones de Educación Superior. IEEE, 2020.

[8] R. Almeida De Paula and J. Oliveira Castro, "Sistemas de gestão de segu-rança da informação-uma análise comportamental (Information security management systems-a behavioral analysis)," 2023.

[9] Bhaharin Surayahani, Sulaiman Rossilawati, Mokhtar Umi, and Yusof Maryati, Issues and Trends in Information Security Policy Compliance. IEEE, 2019.

[10] N. J. Pinda Román and L. A. Moya Martínez, "Ciberseguridad enfocada en el futuro digital de los estudiantes," LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, vol. 5, no. 2, Apr. 2024, doi: 10.56712/latam.v5i2.1910.

[11] F. Arellano, Í. Donoso Barraza, A. Flores Bustos, C. P. Soto, V. Flores Fon-seca, and R. Martínez-Peláez, "Examining cybersecurity culture in Leon city organizations: Insights from 2022 Examinando la cultura de ciberse-guridad en las organizaciones de la ciudad de León: percepción de 2022," 2024. [Online]. Available: https://orcid.org/0009-0003-5061-7746.

[12] R. Benaichouba, M. Brahmi, and L. Adala, "ECONOMIC OF CYBER-SECURITY AND SOCIETY DATABASES: PROTECTING THE DIGITAL ECOSYSTEM FROM CYBER-ATTACKS," International Journal of Pro-fessional Business Review, vol. 9, no. 7, p. e04803, Jul. 2024, doi: 10.26668/businessreview/2024.v9i7.4803.

[13] V. I. Capa Sanmartín, A. J. Romero Fernández, F. P. Cañizares Galarza, and S. A. Machuca Vivar, "La gestión de seguridad de la información para una empresa," CIENCIAMATRIA, vol. 8, no. 4, pp. 651–666, Aug. 2022, doi: 10.35381/cm.v8i4.877.

[14] A. P. da Silva Sotero and L. R. dos Santos, "O estelionato virtual e a in-eficácia da legislação brasileira para coibir o crime cibernético," Cuader-nos de Educación y Desarrollo, vol. 16, no. 8, p. e5183, Aug. 2024, doi: 10.55905/cuadv16n8-081.

[15] J. Guaña Moya, "La importancia de la seguridad informática en la educa-ción digital: retos y soluciones," RECIMUNDO, vol. 7, no. 1, pp. 609–616, Feb. 2023, doi: 10.26820/recimundo/7.(1).enero.2023.609-616.

[16] J. M. Trujillo Torres, C. Rodríguez Jiménez, S. A. García, and B. Berral Ortiz, "Revisión sistemática de la literatura sobre la seguridad digital en estudiantes de educación superior," Información tecnológica, vol. 35, no. 4, pp. 1–12, Aug. 2024, doi: 10.4067/s0718-07642024000400001.

[17] D. L. Carvajal Portilla, A. Cardona Londoño, and F. J. Valencia Duque, "Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana," Entre ciencia e ingeniería, vol. 13, no. 25, pp. 68–76, Jun. 2019, doi: 10.31908/19098367.4016.

[18] M. Ron, G. Ninahualpa, D. Molina, and J. Diaz, Estrategia Nacional de Ciberseguridad para Paises en Desarrollo. IEEE, 2020.

[19] F. Juca Maldonado and R. Medina Peña, "Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas.," Portal de la Ciencia, vol. 4, no. 3, pp. 325–337, Sep. 2023, doi: 10.51247/pdlc.v4i3.394.

[20] C. Su, "Big data security and privacy protection," in Proceedings - 2019 International Conference on Virtual Reality and Intelligent Systems, ICVRIS 2019, Institute of Electrical and Electronics Engineers Inc., Sep. 2019, pp. 87–89. doi: 10.1109/ICVRIS.2019.00030.

[21] R. D. Estrada Esponda, J. L. Unás Gómez, and O. E. Flórez Rincón, "Prác-ticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá," Revista Logos, Ciencia & Tecnología, vol. 13, no. 3, Oct. 2021, doi: 10.22335/rlct.v13i3.1446.

[22] A. K. Zharova and V. M. Elin, "Technical and Legal Principles of Infor-mation Security on the Example of Russia," in Proceedings of the 2021 IEEE International Conference "Quality Management, Transport and In-formation Security, Information Technologies", T and QM and IS 2021, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 131–135. doi: 10.1109/ITQMIS53292.2021.9642899.

[23] D. P. A. Peña Martha, "Amenazas emergentes en la computacion en la nube," 2024.

[24] O. Ñañez, "Modelo de gestión de riesgos de ti para mejorar la gestión de seguridad de la información en la," 2020.

[25] R. Sabillón and J. J. Cano M., "Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones," RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, vol. 2019, no. 32, pp. 33–48, Jun. 2019, doi: 10.17013/risti.32.33-48.

[26] H. Gao, "Design of Network Data Information Security Monitoring Sys-tem Based on Big Data Technology," in Procedia Computer Science, Elsevier B.V., 2023, pp. 348–355. doi: 10.1016/j.procs.2023.11.040.

[27] R. Madrigal, "IMPACTO DE LOS CIBERATAQUE EN LA SEGURIDAD INTERNACIONAL IMPACT OF THE CIBERATAQUE ON INTERNATIONAL SECURITY," 2020, [Online]. Available: https://www.eumed.net/rev/caribe/2020/01/ciberataque-seguridad-internacional.html.

[28] P. A. Villa Sánchez, J. Gutiérrez Obando, and A. M. López Echeverry, "Elementos de Seguridad para Gestión Documental con Blockchain," En-tre ciencia e ingeniería, vol. 17, no. 34, pp. 36–42, 2023, doi: 10.31908/19098367.2667.

[29] J. V. Cordero, "Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos*," 2021. [Online]. Available: https://idp.uoc.edu.

[30] A. Irsheid, A. Murad, M. Alnajdawi, and A. Qusef, "Information security risk management models for cloud hosted systems: A comparative study," in Procedia Computer Science, Elsevier B.V., 2022, pp. 205–217. doi: 10.1016/j.procs.2022.08.025.

[31] L. Isabel, O. Pedro, and G. Teresa, How ISO 27001 can help achieve GDPR compliance. IEEE, 2019.

[32] R. Romansky and I. Noninska, Cyber Space Features – Security and Data Protection Requirements. IEEE, 2019.

[33] P. Genchev, "An approach to support information security risk assess-ment," in Proceedings of the International Conference on Biomedical In-novations and Applications, BIA 2020, Institute of Electrical and Elec-tronics Engineers Inc., Sep. 2020, pp. 125–128. doi: 10.1109/BIA50171.2020.9244516.

[34] Y. Rojas, P. Tamayo, and M. Moreno, "METODOLOGÍA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LOS ASPECTOS MÁS RELEVANTES DE LA NORMA CUBANA NC ISO IEC 27001:2016," 2020, [Online]. Available: https://www.eumed.net/rev/rilcoDS/12/gestion-seguridad-informacion.html.

[35] J. M. Salazar, C. Cruz, A. Balderas, and H. Diaz, "LA SEGURIDAD INFORMÁTICA EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR," 2021.

[36] F. Javier et al., "Examining cybersecurity culture in Leon city organizati-ons: Insights from 2022 Examinando la cultura de ciberseguridad en las organizaciones de la ciudad de León: percepción de 2022," 2024. [Onli-ne]. Available: https://orcid.org/0009-0003-5061-7746.

[37] Juan Manuel Aguilar Antonio, "Retos y oportunidades en materia de ci-berseguridad de América Latina frente al contexto global de ciberamena-zas a la seguridad nacional y política exterior," 2021.

[38] F. Wulf, S. Strahringer, and M. Westner, "Information security risks, bene-fits, and mitigation measures in cloud sourcing," in Proceedings - 21st IEEE Conference on Business Informatics, CBI 2019, Institute of Electri-cal and Electronics Engineers Inc., Jul. 2019, pp. 258–267. doi: 10.1109/CBI.2019.00036.