Contribution of Digital Forensic Auditing on the Prevention of Cybercrime in the Business Sector in Latin America

Katherine Rubí Tumbalobos Gamboa[1]; Karina Alessandra Alarcón Gutierrez[1]; Wilfredo Galíndez Azorza[1]; Fernando Guido Aguirre León[1]
[1]Facultad de Ciencias Empresariales, Carrera de Contabilidad y Finanzas, Universidad de Lima, Perú
20222590@aloe.ulima.edu.pe, 20213207@aloe.ulima.edu.pe, wgalinde@ulima.edu.pe, faguirre@ulima.edu.pe

***Abstract*– The increasing incidence of cybercrime has become a major challenge for organizations, promoting the adoption of digital forensic auditing as a tool to strengthen information security. This study aimed to analyze the contribution of digital forensic auditing on the prevention of cybercrime in the business sector in Latin America during the 2020–2026 period. To achieve this, a systematic literature review of scientific articles indexed in Scopus was conducted. The results show that digital forensic auditing strengthens internal control, improves risk management, and facilitates detection and investigation of cyber incidents. It is concluded that its implementation is an effective strategy for preventing cybercrime and enhancing organizational information security.**

***Keywords*-- Digital forensic auditing, cybercrime, internal control, risk management, cybersecurity.**

Resumen- La creciente incidencia del cibercrimen representa un desafío para las organizaciones, lo que ha impulsado la adopción de la auditoría forense digital como herramienta para fortalecer la seguridad de la información. El objetivo de este estudio fue analizar la contribución de la auditoría forense digital en la prevención del cibercrimen en el sector empresarial de Latinoamérica durante el periodo 2020-2026. Para ello, se realizó una revisión sistemática de literatura de artículos científicos indexados en Scopus. Los resultados evidencian que la auditoría forense digital fortalece el control interno, mejora la gestión de riesgos y facilita la detección e investigación de incidentes informáticos. Se concluye que su implementación constituye una estrategia efectiva para prevenir el cibercrimen y reforzar la seguridad de las organizaciones.

Palabras clave-- Auditoría forense digital, cibercrimen, control interno, gestión de riesgos, ciberseguridad.

I. Introducción

La transformación digital ha favorecido la automatización y el manejo de grandes volúmenes de datos, pero también ha incrementado la exposición de las organizaciones latinoamericanas al cibercrimen [1]. Durante la aceleración digital posterior a la emergencia sanitaria se registraron más de 41 mil millones de intentos de ciberataques en la región [1]. Las amenazas más frecuentes son el ransomware, el phishing, la suplantación de identidad, el robo de información, el acceso no autorizado y la manipulación fraudulenta de estados financieros [1, 2, 10]. Cuando ocurre alguno de estos incidentes se afectan la continuidad operativa y los activos de información, y también se resiente la confianza de los grupos de interés [2, 3].

La región no es vulnerable solo porque falten herramientas tecnológicas. El problema se extiende a la poca cultura de ciberseguridad, baja percepción del riesgo, escasez de especialistas y la infraestructura obsoleta [1, 3, 20]. En las PYME el problema es mayor. No hay presupuesto ni personal capacitado [4]. Las entidades públicas locales ni siquiera cuentan con políticas de seguridad formales [20]. De ahí la importancia del control interno, de la auditoría interna y la capacitación [2].

En este contexto, la auditoría forense digital combina conocimientos de contabilidad, tecnología y jurídicos para localizar, conservar, estudiar y presentar pruebas digitales. Con ello se refuerza el control de la institución y sirve de respaldo en procesos administrativos o judiciales [5]. Pero no debería usarse solo después de que ocurre un incidente, conviene incorporarla de forma preventiva en la gestión de la organización [5].

Por otro lado, la literatura advierte también que el desarrollo tecnológico va más rápido que la actualización de las normas, y eso complica la cooperación judicial entre países y la regulación de la cadena de custodia en tecnologías emergentes como la inteligencia artificial [6, 12]. Para responder a esto, esta investigación propone el Modelo de Auditoría Forense Digital Preventiva (MAFD-P), un framework conceptual que reúne los principales hallazgos de la revisión y da una estructura para reforzar la prevención del cibercrimen en las organizaciones. Se desarrolla en la Sección VI.

II Marco teórico

A. Auditoría forense digital

Dentro de la auditoría, la forense digital es una especialidad que reúne conocimientos contables, tecnológicos y jurídicos para identificar, preservar y analizar evidencias digitales relacionadas con posibles actos de cibercrimen. Su finalidad no se queda en investigar lo que ya pasó: también busca reforzar los mecanismos de control interno y aportar evidencia válida para procesos administrativos o judiciales. Y esta herramienta ayuda a prevenir el fraude, porque permite detectar los riesgos a tiempo y hace que las organizaciones sean más transparentes [5].

También se sostiene que, como el cibercrimen crece, hacen falta procedimientos estandarizados que garanticen que

las evidencias digitales sean auténticas y que conserven su integridad [6]. Según los autores, aplicar bien las técnicas de informática forense hace más eficaces las investigaciones y facilita la cooperación entre las instituciones encargadas de combatir la ciberdelincuencia.

B. El cibercrimen en el sector empresarial

El incremento de la digitalización ha generado nuevas oportunidades para las organizaciones, pero también ha favorecido el aumento del cibercrimen como el ransomware, phishing, robo de información y ataques a los sistemas corporativos. Estas amenazas ocasionan pérdidas económicas, interrupción de operaciones y afectaciones a la reputación empresarial.

También se vio que muchas empresas, sobre todo las pequeñas y medianas, tienen deficiencias en la gestión de los riesgos tecnológicos, y eso hace que estén más expuestas a los ataques de ransomware [17]. Algo parecido se concluye para Latinoamérica: todavía persisten debilidades como la falta de cultura de ciberseguridad y la escasa actualización tecnológica, y siguen faltando políticas integrales para enfrentar las amenazas digitales [3].

C. Auditoría forense digital como estrategia de prevención

La literatura reciente señala que la auditoría forense digital no debe limitarse a la investigación de incidentes, sino que también debe incorporarse como una estrategia preventiva dentro de la gestión organizacional. La evaluación permanente de riesgos, el monitoreo de los controles y el análisis de vulnerabilidades permiten reducir la probabilidad de ocurrencia del cibercrimen.

Un estudio demostró que implementar modelos basados en el NIST Cybersecurity Framework 2.0 ayuda a identificar mejor las vulnerabilidades y mejora la capacidad de respuesta frente a incidentes de seguridad [17]. Otro estudio concluyó que la capacitación del personal, la cultura de la organización y el fortalecimiento del control interno son factores determinantes para prevenir ataques cibernéticos [20].

D. Importancia de la gestión de riesgos digitales

La gestión de riesgos digitales reúne el conjunto de políticas, procedimientos y controles con los que se protegen los activos de información frente a amenazas internas y externas. Esto bien implementado reduce la probabilidad de los incidentes y mejora la continuidad operativa.

La evidencia es clara. Cuando la auditoría forense digital, la ciberseguridad y la gestión de riesgos trabajan juntas, las empresas quedan mejor preparadas para prevenir el cibercrimen. Conviene verlas como herramientas complementarias y necesarias para sostener la seguridad de la información en un entorno más digitalizado.

III. METODOLOGÍA

Este trabajo sigue un enfoque cualitativo, desarrollado como una revisión sistemática de literatura. Es un método que permite examinar la producción científica sobre un tema de forma rigurosa y verificable.

La selección de estudios siguió el método PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), que fija etapas y criterios de inclusión, exclusión y reporte. Este método solo se usó para seleccionar los estudios. El análisis, la interpretación y las conclusiones se construyeron a partir de los 27 artículos que resultaron del proceso.

TABLA I
ECUACIONES DE BÚSQUEDAS EN SCOPUS

Ecuaciones de la búsqueda para Scopus
("digital forensic" OR "forensic audit" OR "cyber forensic" OR "digital investigation") AND ("cybercrime" OR "cybersecurity" OR "cybersecurity threats" OR "online crime") AND ("prevention" OR "mitigation" OR "deterrence" OR "reduction") AND ("Latin America" OR "South America" OR "Central America" OR "Latin American countries")
("forensic" OR "digital" OR "computer" OR "cyber") AND ("auditing" OR "audit" OR "assessment" OR "evaluation") AND ("cybercrime" OR "cybersecurity" OR "information security" OR "online crime") AND ("prevention" OR "deterrence" OR "mitigation" OR "protection") AND ("corporate" OR "business" OR "enterprise" OR "organization") AND ("Latin America" OR "South America" OR "Central America" OR "Latin American")
("legal framework" OR "legislation" OR "regulations" OR "compliance") AND ("digital evidence" OR "computer forensics" OR "forensic computing") AND ("computer crimes" OR "cybercrime") AND ("Latin America")
("digital forensics" OR "digital forensic auditing") AND ("cybercrime" OR "computer crimes") AND ("Colombia" OR "Mexico" OR "Peru" OR "Chile" OR "Argentina" OR "Brazil" OR "Ecuador")

A. Planeamiento de la investigación y estrategia de búsqueda

En esta etapa se buscó saber qué evidencia existe sobre lo que aporta la auditoría forense digital a la prevención del cibercrimen en las empresas latinoamericanas.

La búsqueda se ejecutó en Scopus y se consideró el periodo 2020 a 2026 para capturar la producción posterior al punto de inflexión que significó la pandemia.

Las variables del estudio auditoría forense digital como variable independiente y prevención del cibercrimen como dependiente se tradujeron en cuatro ecuaciones de búsqueda que combinan términos relacionados al estudio con delimitadores geográficos, tal como se presenta en la Tabla I.

Por lo tanto, con el objetivo de identificar los artículos de mayor relevancia, se definieron los términos de búsqueda "auditoría forense", "informática forense", "cibercrimen", "ciberseguridad", "prevención", "evidencia digital", "marco legal" y "sector empresarial", junto con delimitadores geográficos referidos a América Latina y sus países, lo que condujo a las cuatro ecuaciones de búsqueda que se presentan en la Tabla I.

B. Criterios de selección de estudios

A partir de la aplicación de los términos de búsqueda en la base de datos Scopus, se identificaron un total de 235 artículos vinculados con el objetivo del estudio. Tras excluir los artículos duplicados, quedaron 197 registros únicos. Después se aplicó el filtro por título y resumen, que descartó 49 documentos ajenos a las variables del estudio.

Estos 148 registros se evaluaron con los criterios de inclusión y exclusión de la Tabla II, lo que permitió seleccionar artículos que cumplían con las condiciones iniciales. Los artículos finalmente incluidos se examinaron a fondo para el desarrollo de la investigación.

TABLA II
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

N°	Inclusión	Exclusión
1	Disponibilidad del documento completo	Documentos con solo el resumen (abstract)
2	Publicaciones de acceso abierto y/o disponibles para consulta	Acceso restringido al documento completo
3	Estudios publicados (2020 -2026)	Estudios publicados fuera del período establecido
4	Publicaciones disponibles en español o inglés	Publicaciones en idiomas diferentes al español y/o inglés
5	Estudios relacionados con auditoría forense digital y similares	Estudios no relacionados con la auditoría forense digital o aspectos sin vinculación
6	Estudios realizados en países de América Latina	Documentos duplicados
7	Publicaciones de artículos científicos, artículos de revisión, revisiones breves y trabajos de conferencia.	Publicaciones de tesis, libros y capítulos de libros

Según la Tabla II, la selección de los documentos se basó en criterios de inclusión como la disponibilidad del texto completo, un rango de publicación (2020-2026), idioma (español o inglés). Se priorizaron artículos científicos y trabajos de conferencia enfocados en Latinoamérica que abordaran la auditoría forense digital y su contribución legal o normativo sobre la evidencia digital en las organizaciones, descartando cualquier tema ajeno a esta materia. Este proceso de filtrado excluyó 108 estudios elegibles.

Posteriormente, para validar la información, se aplicaron los criterios de calidad de la Tabla III, concluyendo con 27 artículos finales para el desarrollo del análisis detallado.

TABLA III
CRITERIOS DE EVALUACIÓN DE CALIDAD

N°	Criterios de evaluación	Descripción del criterio	Valorización
1	Claridad y coherencia	Se revisó que las ideas fueran claras y estuvieran relacionadas entre sí	Si=1/ Parcial=0.5/ No=0
2	Claridad metodológica	Se verificó que el método utilizado estuviera explicado	Si=1/ Parcial=0.5/ No=0
3	Relación con el tema	Se consideró su relación con la auditoria forense digital y el cibercrimen	Si=1/ Parcial=0.5/ No=0
4	Relevancia de los resultados	Se evaluó el aporte de los resultados al tema investigado	Si=1/ Parcial=0.5/ No=0
5	Cumplimiento de objetivo	Se verificó que los resultados respondieron al objetivo del estudio	Si=1/ Parcial=0.5/ No=0

C. *Extracción de datos y síntesis*

Cada criterio se calificó con valores numéricos (Sí = 1, Parcial = 0.5, No = 0) para obtener un puntaje total sobre 5.0 puntos. Para asegurar la calidad, al final se incluyeron solo los artículos que tenían una nota igual o mayor a 4.0/5.0 y que no tuvieran ninguna calificación como "No". Aplicando este criterio a los 40 artículos evaluados, 27 estudios superaron el umbral y formaron la muestra final. El diagrama de flujo de la Figura 4 resume este proceso.

D. *Construcción de un framework conceptual*

Estas investigaciones analizadas dejan ver cuáles son los elementos esenciales de la auditoría forense digital preventiva en el entorno corporativo. Con ello se armó un esquema metodológico que junta la ruta operativa de cuatro fases con los pilares de la cultura humana y cumplimiento legal. El framework desarrollado tiene como propósito estructurar las conclusiones clave de la literatura y guiar las próximas líneas de acción para salvaguardar los activos tecnológicos de las compañías.

E. *Limitaciones metodológicas*

La presente revisión presenta algunas limitaciones que deben considerarse al interpretar sus resultados. En primer lugar, se utilizó únicamente la base de datos Scopus, por lo que algunos estudios relacionados con el tema que no se encuentren indexados en esta plataforma pudieron quedar fuera de la revisión, generando un posible sesgo de cobertura. En segundo lugar, la búsqueda se limitó a estudios realizados en países de Latinoamérica, lo que restringe la posibilidad de generalizar los resultados a otros contextos geográficos.

IV. RESULTADOS

A. *Revisión sistemática de la literatura*

Durante el desarrollo del trabajo se examinaron las investigaciones que fueron publicadas entre los años 2020 y 2026. En lo que respecta al comportamiento de dicha producción, los datos de la Figura 1 demuestran que los dos años iniciales representan la cifra menor de todo el intervalo. Tras superar ese periodo inicial, se ha venido registrando un aumento progresivo en la cantidad de estudios.

Según la distribución anual de las publicaciones (Figura 1) en 2020 y 2021, hubo dos estudios por año, desde 2022 y se pasó a cinco y el máximo fue de seis en 2025. Este ascenso posterior a 2021 coincide con las consecuencias medibles de la digitalización pandémica, lo que sugiere que la ciencia reaccionó al delito con uno o dos años de rezago. Asimismo, que la tercera parte de los artículos se haya publicado entre 2025 y 2026 indica que el campo está lejos de agotarse y que la conversación sobre prevención forense recién empieza.

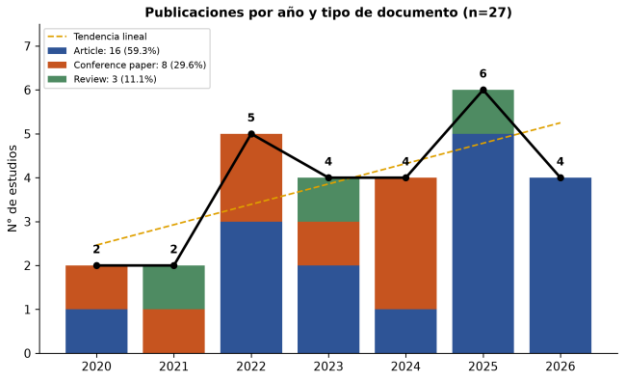


Figura 1: Publicaciones por año y tipo de documento (2020-2025)

Al analizar el corpus muestra que el 59.3% (16) de las publicaciones son artículos de revista (article), seguidos por un 29.6% (8) de artículos de conferencia (conference papers) y solo un 11.1% (3) de revisiones de literatura (reviews). Con esta distribución queda claro que el tema ya superó la fase exploratoria inicial y se convirtió en un campo de investigación maduro y validado formalmente.

En relación con el origen de las publicaciones científicas y sus contribuciones temáticas (Figura 2), se observa que la producción académica en Latinoamérica, con un total de 10 publicaciones. A nivel de países individuales, Ecuador lidera la producción con 5 artículos, seguido de cerca por Perú con 4 y Brasil con 3. Por su parte, Colombia registra 2 artículos, mientras que Argentina, Uruguay y Costa Rica una sola publicación cada uno. En cuanto a los temas, predominan la Ciberseguridad (11 estudios) y la Auditoría/forense (9), seguidas por el Cumplimiento normativo (5) y la Gestión de riesgos (2). Esto muestra una tendencia a priorizar la seguridad técnica y el control, y deja ver un espacio que aún no se ha explorado: la planeación y la mitigación anticipada de riesgos corporativos.

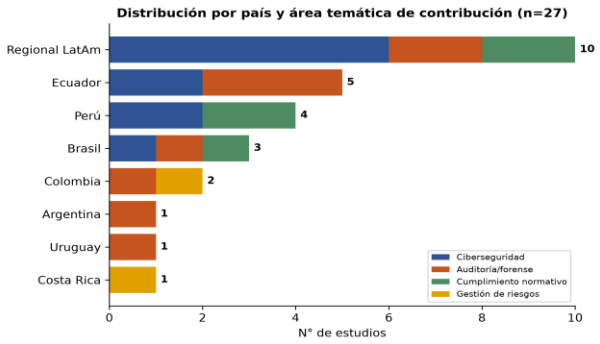


Figura 2: Distribución por país y área temática de contribución (n=27)

Metodológicamente (Figura 3), predomina la revisión sistemática con 8 estudios, seguida de protocolos (5) y análisis normativo (4), este último centrado en auditoría/forense. Asimismo, los enfoques cualitativos y de caso (2 cada uno) abordan la ciberseguridad, mientras que los cuantitativos (3) se dividen entre auditoría y cumplimiento. lo que dejaría claro que los temas de auditoría se estudian revisando normas y leyes, mientras que la ciberseguridad se analiza investigando casos reales dentro de las empresas.

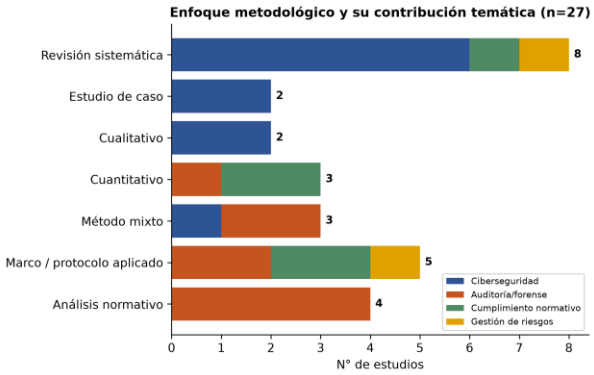


Figura 3: Enfoque metodológico y su contribución temática (n=27)

A partir de la tabla IV y los estudios seleccionados, prevenir el cibercrimen exige fortalecer controles, gestionar riesgos, proteger información y tratar la evidencia digital. Asimismo, destaca la necesidad de capacitar al personal y estructurar procedimientos para responder oportunamente a los incidentes.

TABLA IV
RESUMEN DE LOS ESTUDIOS SELCCIONADOS

Autor	País	Metodología	Hallazgos principales	Aporte a la prevención
[1]	Latam	Revisión sistemática	Identifico el phising como una amenaza frecuente durante la pandemia	Permite reconocer amenazas y fortalecer medidas preventivas
[2]	Ecuador	Cuantitativo	Encontró relación entre control interno y prevención del fraude	Resalta la importancia de los controles internos
[3]	Latam	Revisión sistemática	Identifico falta de capacitación, estándares y actualización como vulnerabilidades	Orienta la identificación de riesgos
[4]	Latam	Cualitativo	Identifico desafíos de ciberseguridad en las PYMES	Ayuda a reconocer riesgos empresariales
[5]	Ecuador	Método mixto	Destacó la prevención y detección del fraude	Apoya la identificación de irregularidades
[6]	Latam	Método mixto	Evidenció dificultades para validar evidencia digital entre países	Resalta la necesidad de procedimientos comunes
[7]	Ecuador	Análisis normativo	Adaptó un protocolo de	Facilita el tratamiento de

			informática forense	evidencia digital
[8]	Argentina	Marco/protocolo aplicado	Propuso identificar indicadores de compromiso	Facilita la detección de incidentes
[9]	Latam	Revisión Sistemática	Identificó el malware como una modalidad frecuente	Ayudar a orientar medidas preventivas
10]	Ecuador	Revisión sistemática	Analizó cibercrímenes frecuentes y su prevención	Permite conocer riesgos recurrentes
11]	Latam	Revisión sistemática	Identificó el crecimiento del uso delictivo de la IA	Advierte sobre nuevos riesgos tecnológicos
12]	Brasil	Análisis normativo	Señaló dificultades sobre la evidencia digital generada con IA	Resalta la necesidad de regulación
13]	Latam	Marco/protocolo aplicado	Propuso una respuesta forense ante ciberincidentes	Orienta la atención de incidentes
14]	Perú	Marco/protocolo aplicado	El modelo aplicado mejoró aspectos de seguridad en PYMES	Apoya el fortalecimiento de controles
[15]	Perú	Marco/protocolo aplicado	Identificó brechas de seguridad en endpoints	Permite detectar puntos vulnerables
[16]	Latam	Revisión Sistemática	Analizó la aplicación de ISO27001	Apoya la gestión de seguridad
[17]	Perú	Modelo	Evaluó riesgos y mitigación del ransomware	Apoya la gestión de riesgos
[18]	Costa Rica	Marco/protocolo aplicado	Evidenció limitaciones en la madurez de ciberseguridad	Identifica áreas por fortalecer
[19]	Colombia	Revisión sistemática	Analizó la eficacia de controles de mitigación	Permite verificar la efectividad de controles
[20]	Ecuador	Cualitativo	Destacó el factor humano y la falta de capacitación	Refuerza la prevención mediante capacitación
[21]	Brasil	Método mixto	Identificó riesgos de ciberseguridad en DevSecOps	Ayuda a prevenir riesgos durante el desarrollo
[22]	Latam	Cuantitativo	Evaluó la información sobre ciberseguridad divulgada en empresas	Favorece la transparencia y gestión de riesgos
[23]	Brasil	Cuantitativo	Abordó la gestión de datos y cumplimiento de la LGPD	Apoya la protección de datos
[24]	Latam	Revisión Sistemática	Analizó técnicas de autenticación	Resalta la importancia de
			frente al fraude	reforzar la autenticación
[25]	Perú	Estudio de caso	Analizó un caso de sabotaje cibernético	Destaca la importancia de responder ante incidentes
[26]	Colombia	Análisis normativo	Identificó dificultades en el uso de evidencia digital	Resalta la necesidad de fortalecer su regulación
[27]	Uruguay	Análisis normativo	Señaló limitaciones de las reglas tradicionales para la evidencia digital	Apoya el desarrollo de normas especificas

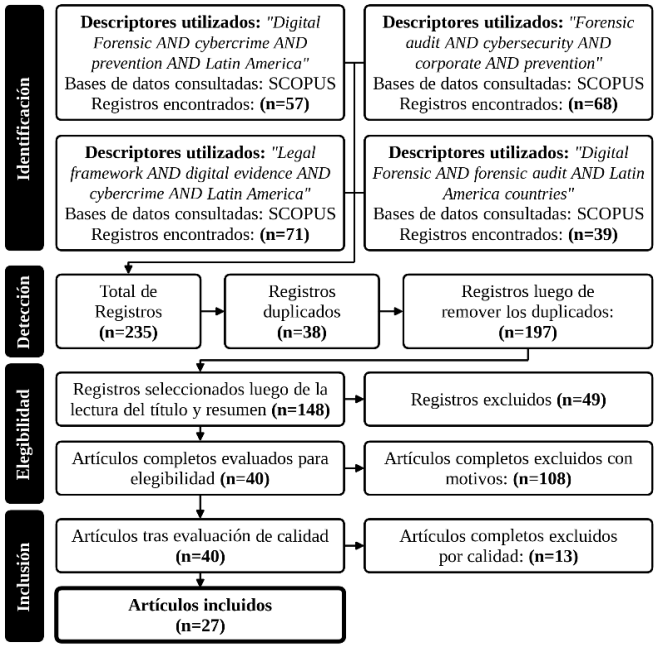


Figura 4: Diagrama de flujo PRISMA

B. Conformación del corpus

El corpus final de 27 documentos es muy variado, tanto en lo metodológico como en lo conceptual. Por un lado, hay revisiones sistemáticas y bibliométricas que delimitan el campo del cibercrimen y de las vulnerabilidades en la región [3, 9, 11]. Por otro, hay investigaciones empíricas cuantitativas que recurren a encuestas y a pruebas estadísticas de asociación para explicar el fraude y las prioridades de seguridad dentro de las organizaciones [2, 21].

Hay estudios de caso que aplican y validan marcos de gestión en pequeñas y medianas empresas [14, 15, 17]. Otros textos son protocolos forenses escritos para contextos concretos, sea el proceso penal, el análisis de malware o la telemedicina [7, 8, 13]. Aparecen análisis documentales y normas, sobre todo de cooperación transfronteriza y admisibilidad de la prueba, y algo de divulgación corporativa [5, 6, 12, 22]. Esa variedad de métodos puede contrastar los resultados, lo que da consistencia con lo hallado de la revisión.

La pandemia marcó un giro. Los trabajos de esos años registran el aumento de ataques y piden una cultura de ciberseguridad [1], es entonces cuando aparecen los primeros instrumentos periciales de la región dirigidos a esos mismos escenarios [7, 8, 13]. La evidencia posterior confirmó lo que se anticipaba. Con el trabajo remoto el fraude y la manipulación de datos financieros se multiplicaron, y el control interno quedó como la defensa más firme [2].

Pasada la emergencia, el delito siguió creciendo [10]. Los trabajos posteriores se ocupaban ya de cómo responder, desde tipificar el delito económico [9] hasta adoptar estándares de gestión [14, 16] y gobernanza de la ciberseguridad [22, 23]. Últimamente el interés se concentra en tres fuentes. Medir el riesgo [15], entender el factor humano [20, 21] y lidiar con lo que trae la inteligencia artificial para la prevención y la validez jurídica de la evidencia digital [11, 12].

C. La auditoría forense como línea de prevención

La auditoría forense se aplica de forma sistemática en instituciones públicas, ayuda a prevenir y detectar a tiempo el fraude y la corrupción, genera ahorros y mejora la transparencia. Esto demuestra que su efecto preventivo constituye un resultado observable y no solo una propuesta teórica [5].

En las organizaciones públicas y privadas, la manipulación de datos económicos y el fraude en estados financieros están entre las principales amenazas. Frente a ellas, el control interno y la auditoría interna actúan como mecanismos centrales de prevención, y por eso es más eficiente fortalecer con capacidades forenses que crear estructuras independientes [2].

La efectividad de esta prevención también depende de procedimientos claros para recolectar, adquirir y preservar evidencias digitales con validez legal [7]. Cuando las pruebas puedan estar contaminadas con malware, el análisis de archivos, conexiones y otras huellas permite identificar patrones de ataque, alertar a otros sistemas y convertir cada investigación en conocimiento preventivo [8].

En sectores sensibles como la telemedicina, la respuesta forense debe organizarse según la urgencia y volatilidad de la información, dando prioridad a proteger los datos críticos, controlar los accesos y preservar las evidencias completas [13]. Lo que muestran estos estudios es que la prevención forense debe integrarse en la gestión cotidiana de las organizaciones y no limitarse a una respuesta posterior al incidente. El siguiente desafío consiste en asegurar la validez legal de las pruebas durante el proceso judicial.

D. Evidencia digital y articulación jurídica

En Latinoamérica todavía es difícil que se acepte evidencia digital en juicios transfronterizos. El análisis de México, Colombia, Argentina y Chile identificó siete problemas, entre ellos la falta de uniformidad procesal y la limitada aceptación de peritos extranjeros. Esto complica la valoración de correos electrónicos, chats, archivos multimedia, registros de geolocalización, información en la nube y operaciones con criptomonedas, y muestra que hay que reforzar la cooperación internacional [6].

La normativa de Ecuador sanciona delitos como la suplantación de identidad, la falsificación documental y la apropiación fraudulenta por medios electrónicos., pero prevenirlos exige que el Estado, las empresas y la ciudadanía, así como procedimientos adecuados para preservar la evidencia digital según lo que piden las leyes [10].

La inteligencia artificial añade desafíos relacionados con la cadena de custodia, la explicabilidad de los hallazgos y con los posibles sesgos algorítmicos. La cadena de custodia sigue siendo fundamental para garantizar la integridad de la prueba, pero todavía faltan reglas específicas para la evidencia obtenida mediante estos sistemas, por lo que la transparencia y la supervisión humana resultan indispensables [12].

Dos análisis legales recientes completan este panorama. El primero compara Colombia, Estados Unidos, Argentina y España confirma que ninguno define jurídicamente la evidencia digital, limitándose al concepto general de "mensaje de datos" (información electrónica básica), el cual ignora los detalles técnicos de un cibercrimen [26]. El segundo, sobre Uruguay concluye que aplicar las reglas de la "prueba documental" tradicional (firma, testigos, papel) no funciona y que hace falta una regulación desde cero [27]. Ambos casos muestran un vacío legal que le quita valor a las pruebas informáticas ante los jueces y hace más difícil perseguir el cibercrimen.

La cooperación internacional, la legislación interna y el desarrollo tecnológico dejan ver la misma brecha: la tecnología avanza con mayor rapidez que la regulación. Mientras esta diferencia siga existiendo, la evidencia digital puede perder validez judicial, lo que refuerza la necesidad de estándares técnicos claros.

E. Estándares, madurez y resultados medibles

Una PYME peruana con recursos limitados puede alcanzar un nivel adecuado de ciberseguridad mediante la integración de ISO/IEC 27001 y el marco NIST. La propuesta, estructurada en siete pasos del ciclo PDCA, fue aplicada en una PYME tecnológica mediante doce dominios y cuarenta controles, logrando una mejora del 40 % en ciberseguridad y un salto de madurez, de un nivel insuficiente a uno maduro.

Quispe-Kobashikawa et al. [15] sumaron a este enfoque un modelo que integra ISO/IEC 27001, NIST e indicadores financieros para medir el riesgo cibernético. Tras seis meses de seguimiento, el sistema incrementó en nueve puntos el cumplimiento normativo y redujo en veintidós puntos el riesgo residual. El estudio se hizo en una sola empresa, pero demostró que la efectividad de los controles puede evaluarse mediante indicadores objetivos.

La revisión de Hinostroza et al. [16], revisaron veintitrés estudios latinoamericanos y confirmaron que implementar ISO

27001 reduce los incidentes de seguridad y mejora el cumplimiento normativo. Asimismo, Biggi et al. [17] diseñaron un modelo contra el ransomware para una microempresa peruana de transporte. Tiene cinco etapas: definir el perfil, identificar los activos, analizar los riesgos, seleccionar los controles y elaborar el plan de acción. La propuesta obtuvo una valoración de 3,74 sobre 5, destacando en evaluación de riesgos y sostenibilidad.

Lo que muestran los estudios es organizaciones de cualquier tamaño pueden mejorar y medir su nivel de protección digital, pero la efectividad de los estándares depende de que el personal los aplique todos los días, sobre todo cuando hay restricciones presupuestarias, prácticas deficientes y errores humanos.

F. El factor humano y organizacional

En entrevistas a responsables tecnológicos de municipios ecuatorianos se vio que la vulnerabilidad frente al ransomware se debe sobre todo a problemas de organización: se percibe poco el riego, la capacitación es insuficiente, no hay políticas formales y el personal está expuesto a técnicas de ingeniería social. Como alternativas de bajo costo, se identificaron comités internos de seguridad, capacitaciones breves y redes de colaboración entre empleados [20].

Las PYMES latinoamericanas tienen como principales limitaciones son la falta de recursos económicos y de personal especializado, y los cibercrímenes son especialmente frecuentes en Brasil, México y Chile [4]. Ante estas restricciones, desde el ámbito universitario una herramienta gratuita para evaluar riesgos digitales en empresas costarricenses, que demostró que una buena postura de ciberseguridad protege la información y puede generar ventajas competitivas [18].

En Brasil, el cumplimiento de la Ley General de Protección de Datos de Brasil impulsó a que las empresas de servicios, comercio e industria incorporan delegados de protección de datos. Se ve así que la regulación impone obligaciones y, la vez, promueve la formación de capacidades especializadas para gestionar la privacidad y seguridad de la información [23]. En conjunto, los estudios muestran que las fallas humanas, la limitada capacitación y la debilidad de la gestión interna.

G. Panorama regional del cibercrimen y gobernanza

La pandemia hizo más graves los riesgos de ciberseguridad en Latinoamérica, una región que registró más de 41 mil millones de intentos de ciberataques. Además del *phishing* y el *malware*, se identificaron vulnerabilidades estructurales como la baja conciencia de seguridad, la escasez de especialistas y el uso de software obsoleto [1]. Estas debilidades están relacionadas también con la limitada educación digital, la insuficiencia normativa y la falta de profesionales especializados [3].

Según la literatura, el 43 % de las investigaciones trata el cibercrimen con fines económicos, el 41 % en problemas sociales y el 16 % en asuntos políticos y los virus, el robo de información y el fraude financiero aparecen entre las principales amenazas [9]. Al mismo tiempo, la inteligencia artificial se utiliza cada vez más para detectar fraudes y analizar evidencias digitales, aunque los criterios de evaluación siguen siendo distintos y se presta poca atención a la transparencia y la equidad de estos sistemas [11].

Desde la perspectiva organizacional, los riesgos principales son la inseguridad de los proveedores, los sistemas obsoletos, la ausencia de políticas internas y los errores humanos. Entre las prioridades a futuro se señalan proteger los sistemas de inteligencia artificial, la resiliencia frente a los ataques y la aplicación del modelo de confianza cero [21].

La gobernanza corporativa ha llevado a que se divulguen más las estrategias de ciberseguridad, especialmente en el sector financiero [22]. En este ámbito, la autenticación multifactor alcanza una efectividad del 97.9 %, frente al 58 % de las contraseñas tradicionales y eso refleja el avance de los mecanismos biométricos y los controles reforzados [24].

Finalmente, las políticas que han adoptado los Estados frente a los ataques dirigidos contra servicios públicos esenciales demuestran una progresiva institucionalización de la ciberseguridad [25]. En conjunto, la región y cuenta con diagnósticos, tecnologías y marcos normativos relevantes, lo que falta es integrar todo eso en una estrategia coordinada.

V. DISCUSIÓN DE RESULTADOS

Los 27 estudios analizados se pueden responder, de una forma más realista, la pregunta con la que empezó este trabajo: qué contribución tiene la auditoría forense digital en la prevención del cibercrimen en las empresas. Esa contribución no se da de manera directa ni automática. Ninguna de las investigaciones logra demostrar que exista una relación directa de causa y efecto entre la auditoría forense y la reducción de los delitos. Lo que ocurre es más bien una cadena: la auditoría aporta herramientas para detectar amenazas a tiempo y asegurar pruebas con validez legal [5], eso a su vez ayuda a mejorar los controles internos que frenan los fraudes [2], y todo el sistema da resultados reales cuando se alinea con una gestión de seguridad basada en estándares, cuyos efectos sí se han podido medir [14, 15, 16]. La prevención en este ámbito, entonces, no se logra con una herramienta aislada, sino con un sistema de seguridad bien integrado.

Vistas de manera transversal, las subsecciones dejan ver además un patrón de composición. El corpus se reparte en tres bloques que se necesitan mutuamente, los cuales son la práctica forense y de control descrita en las subsecciones B y C, la gestión organizacional del riesgo detallada en las D y E, y los panoramas regionales que les dan contexto en la F. El conjunto de métodos empleados acompaña esa división, donde predominan las revisiones sistemáticas y bibliométricas, seguidas del análisis documental, los estudios de caso con

implementación y las propuestas de marco o protocolo, mientras que los diseños empíricos con sujetos, como encuestas y entrevistas, son minoría. Abunda la síntesis y la propuesta, escasea la comprobación prolongada en el tiempo, y esa carencia explica varios de los vacíos que se señalan más abajo.

Los consensos en los estudios analizados son sólidos. La vulnerabilidad estructural de las PYME aparece en todas las investigaciones organizacionales, sin importar el país de origen [4, 14, 17, 18]. Asimismo, la eficacia medible de los estándares se repite en diferentes contextos y escalas [14, 15, 16]. Por otro lado, el peso del factor humano por encima del técnico se confirma mediante la combinación de distintos métodos, ya que las entrevistas en Ecuador [20], las encuestas en Brasil [21] y el predominio de la ingeniería social como principal vía de ataque en la región [1] apuntan a la misma conclusión desde tres caminos independientes. Finalmente, el papel preventivo del control interno y de la auditoría, ya sea interna o forense, sirve como punto de encuentro entre las investigaciones de ambos sectores [2, 5].

Las tensiones detectadas resultan igual de instructivas. La más evidente divide a los estudios técnicos de los jurídicos, ya que mientras los protocolos operativos maduran y se validan [8, 13], el derecho probatorio acumula retos pendientes [6, 12], lo que genera una disciplina que avanza de manera desequilibrada. Hay una segunda tensión entre el optimismo por los buenos resultados de estas soluciones [14, 15] y la desconfianza que generan los diagnósticos estructurales, que muestran los mismos repitiéndose año tras año [3, 21]. Ambas lecturas pueden ser ciertas si se piensa que los casos de éxito son todavía la excepción dentro de un panorama de rezago general. La tercera discrepancia aparece con la inteligencia artificial. La literatura la trata como una herramienta clave de prevención [11], pero la mirada jurídica no piensa igual, advierte que su falta de transparencia pone en riesgo la confiabilidad de las pruebas en un juicio [12].

VI. PROPUESTA DE VALOR

De la literatura revisada surgió el Modelo de Auditoría Forense Digital Preventiva (MAFD-P), organizado como un ciclo continuo de prevención, detección, investigación y aprendizaje frente a posibles incidentes de ciberseguridad. La idea central es que la auditoría forense digital entre en acción antes del incidente, no después. Refuerza las medidas preventivas y la capacidad de respuesta de las organizaciones.

El MAFDF-P tiene cuatro fases: Prepararse, Vigilar y detectar, Responder e investigar, y Asegurar y aprender. Se cruzan dos ejes transversales, el factor humano junto con la cultura organizacional, y el marco normativo junto con la protección de datos. El modelo mira tanto la parte tecnológica como lo que hacen las personas y el cumplimiento de las normas de seguridad y el tratamiento de la información.

La Fase 1 arma la infraestructura operativa y estratégica. Aquí se adoptan controles de ISO/IEC 27001 y NIST CSF ajustados al tamaño de cada organización [14, 15, 17], también se identifican los activos críticos y qué datos se guardarán automáticamente como posible evidencia. Esos registros necesitan protección contra alteraciones o eliminaciones. Así, el sistema de seguridad se convierte en una plataforma de preparación forense.

La Fase 2 suma indicadores de fraude y revisiones continuas en la auditoría interna [2, 5], junto con evaluaciones periódicas de riesgos con herramientas accesibles [18]. La capacitación práctica y constante contra la ingeniería social también es clave porque el factor humano es todavía una de las principales puertas de acceso de los ataques [20, 21]. Detectar a tiempo depende tanto de la tecnología como de que la gente dentro de la organización actúe con cuidado.

La Fase 3 activa una respuesta inmediata ante incidentes o sospechas de fraude. Esa respuesta se organiza según la urgencia y volatilidad de los datos [13], y la evidencia se preserva con una cadena de custodia alineada con ISO/IEC 27037 [12]. En el análisis se busca identificar indicadores de compromiso útiles para prevenir nuevos ataques [8], cuidando que todo el proceso se ajuste a las normas procesales aplicables [7].

La Fase 4 cierra el ciclo. Se elabora el informe pericial, cuidando la validez jurídica de la evidencia y su dimensión transfronteriza [6]. Aquí también se mide el desempeño con indicadores como incidentes detectados, riesgo residual y pérdidas evitadas. La organización comunica su postura de seguridad a sus grupos de interés [22] y usa lo aprendido para reforzar de nuevo la fase de preparación.

Las cuatro fases se sostienen dos ejes transversales. Uno es el factor humano y la cultura organizacional, indispensable para que las políticas de seguridad conviertan en prácticas cotidianas. El otro es el marco normativo y la protección de datos, que exige cumplir las leyes sobre información personal [23] y las reglas de cooperación regional [6] para que la evidencia sea admisible.

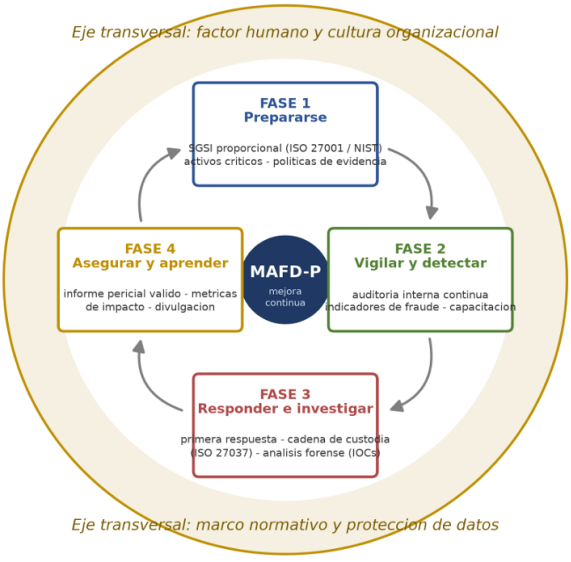


Figura 5: Modelo de Auditoría Forense Digital Preventiva (MAFD-P)

Nota: El modelo tiene cuatro fases de actuación y dos ejes transversales, y busca que la capacidad forense digital forme parte permanente de la prevención y de la gestión de incidentes de ciberseguridad.

La contribución del MAFD-P consiste en integrar dos enfoques tradicionalmente separados. Mientras ISO/IEC 27001 y NIST CSF se concentran en la prevención, mientras que los protocolos forenses suelen actuar después del incidente. El modelo incorpora la capacidad forense como componente preventivo y permanente, y agrega indicadores para evaluar si la inversión en seguridad realmente reduce los riesgos y el cibercrimen.

Cada componente responde a los vacíos detectados. Las Fases 1, 2 y 3 unifican la prevención de ISO/IEC 27001 y NIST CSF con la respuesta forense de ISO/IEC 27037, eliminando la división tradicional entre blindar los sistemas e investigar los incidentes. La Fase 4 agrega los indicadores de medición ausentes en esos marcos, y el eje transversal del factor humano, por su parte, pone la capacitación del personal al mismo nivel que las políticas tecnológicas, cuando en las guías técnicas suelen tener un papel secundario.

VII. Conclusiones

Después de analizar las 27 investigaciones seleccionadas, la respuesta al objetivo de este trabajo queda clara: la auditoría forense digital influye en la prevención del cibercrimen corporativo de forma indirecta pero verificable, y justamente esa naturaleza indirecta es el factor determinante para que se implemente de la manera correcta.

El primer hallazgo tiene que ver con la arquitectura del sistema. La capacidad forense tiene un efecto preventivo real únicamente cuando se integra de forma sistémica, porque así se detectan anomalías a tiempo y se documentan evidencias con plena validez probatoria [5]. También frena las malas, Asimismo, frena las malas prácticas al hacer transparente la trazabilidad de los procesos [2] y su impacto se multiplica si apoya en una gestión de seguridad estandarizada. Aplicada de forma aislada, en cambia, es una pericia costosa que llega recién cuando el daño ya está hecho.

El segundo hallazgo es la eficacia demostrada, cuando los estándares internacionales se adaptan a la escala de la empresa latinoamericana, las mejores se pueden cuantificar: un incremento del 40% en la madurez operativa [14], una reducción de 22 puntos en el riesgo residual [15] y una disminución de incidentes de datos en las implementaciones integradas [16]. Por eso ya no se sostiene la idea de que la prevención robusta sea un privilegio exclusivo de las grandes corporaciones.

El tercero corrige una creencia muy común: la vulnerabilidad de las organizaciones en la región es sobre todo humana y organizacional, y mucho menos tecnológica principalmente tecnológica. Así lo demuestran el predominio de la Ingeniería social [1], las entrevistas en Ecuador [20] y los sondeos en Brasil [21]. Por eso invertir en cultura y capacitación no se puede ver como un simple añadido a la prevención: es su verdadero núcleo.

El cuarto aspecto muestra la brecha que sigue abierta en el proceso. Todo el ciclo preventivo termino en el ámbito judicial, y ahí es donde la región tiene sus debilidades: una cadena de custodia sin regulación específica, una cooperación internacional pendiente y el uso de inteligencia artificial para analizar la prueba digital sin un marco normativo que la regule [6, 12]. Si esto no se resuelve, buena parte del esfuerzo preventivo se perderá en los tribunales y en los aspectos jurídicos.

El quinto aspecto apunta a una ruta de investigación futura. Hasta el momento, no se ha medido el efecto causal directo de la auditoría forense en la reducción de delitos dentro de la empresa privada, porque la evidencia disponible viene sobre toda del sector público y se limita a diseños de caso único. El MAFD-P que se propone incorpora esta medición como una fase explicita dentro de su ciclo. Así, las organizaciones que lo adopten generarán, con su uso, justamente los datos empíricos que la investigación académica todavía necesita.

VIII. Recomendaciones

En primer lugar, a las empresas se les recomienda adoptar la auditoría forense digital y los controles de ciberseguridad bajo un enfoque de proporcionalidad: implementar los controles de seguridad de manera progresiva y de acuerdo con la escala de organización [14, 17]. También conviene definir, antes de que ocurra cualquier incidente, qué registros se mantendrán como evidencia y cuáles serán los lineamientos de respuesta inicial que permitan protegerlos como corresponde [13]. Y la capacitación del personal frente a la ingeniería social tiene que recibir la misma relevancia que se le da a la adquisición de herramientas tecnológicas [20].

En segundo lugar, a los auditores se les recomienda ampliar su perfil profesional e incorporar habilidades forenses dentro de los procesos de auditoría interna. Esto incluye asegurar la cadena de custodia, preservar las evidencias e interpretar los indicadores de compromiso, apoyándose en los protocolos que ya han sido validados en la región [7, 8]. Asimismo, se les pide que adopten métricas de riego residual y de eventos detectados, e modo que puedan demostrar con números el verdadero valor preventivo que tiene su trabajo [15].

En tercer lugar, para los investigadores la brecha de conocimiento ya está claramente identificada: hace falta desarrollar estudios a largo plazo y multiorganizacionales que evalúen cuál es la contribución real de la capacidad forense sobre la mitigación de delitos dentro del sector privado. Esta necesidad existe porque la literatura científica disponible actualmente se limita a presentar análisis de casos únicos [15,

17] y a evidencias que son sobre todo de carácter público [5, 25].

En cuarto lugar, los legisladores tienen como prioridad crear un marco legal sólido que regule la cadena de custodia de la evidencia digital y armonice su tratamiento procesal con el de los países vecinos [6]. También tendrían que definir reglas claras para el uso de inteligencia artificial en la obtención de pruebas [12] y reforzar las exigencias de divulgación sobre ciberseguridad en el mercado de valores [22].

En quinto lugar, las universidades deberán impulsar dos tareas que se complementan: una es formar profesionales que reúnan en un mismo perfil disciplinas que la literatura todavía aborda por separado, como la auditoría, la informática forense y el derecho probatorio en un mismo perfil, y la otra es consolidar los mecanismos de transferencia de conocimiento hacia las PYMES que la propia academia ya empezó a implementar [18].

Por último, las organizaciones públicas deberían aprovechar su ventaja competitiva, ya que el sector público concentra la experiencia forense de la región [5, 25]. Se propone que compartan ese conocimiento con las empresas mediante guías prácticas, convenios y programas colaborativos, y que así su experiencia acumulada se vuelva un recurso público impulsor de la economía digital latinoamericana.

REFERENCIAS

[1] J. Buzzio-Garcia et al., "Review of Cybersecurity in Latin America during the Covid-19 Pandemic. A brief Overview," ETCM 2021 — 5th Ecuador Technical Chapters Meeting, 2021. https://doi.org/10.1109/ETCM53643.2021.9590693.

[2] C. M. De La Torre Lascano y J. I. Quiroz Peña, "Ciberdelito y su asociación en el cometimiento de fraudes financieros en la pandemia de la COVID-19," Revista Venezolana de Gerencia, 2023. https://doi.org/10.52080/rvgluz.28.102.11.

[3] O. Flor-Unda et al., "A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America," Informatics, 2023. https://doi.org/10.3390/informatics10030071.

[4] D. P. C. Galvez y S. Y. Revinova, "Cybersecurity challenges for small and medium enterprises," Iberoamerica, 2025. https://doi.org/10.37656/s20768400-2025-02-03.

[5] C. M. Erazo Portilla et al., "Auditoría forense y su impacto en las organizaciones públicas del Ecuador," Revista de Ciencias Sociales, 2024. https://doi.org/10.31876/rcs.v30i.42279.

[6] L. C. Díaz-Pérez et al., "A review of cross-border cooperation regulation for digital forensics in LATAM from the soft systems methodology," Applied Computing and Informatics, 2026. https://doi.org/10.1108/ACI-01-2022-0010.

[7] F. A. Carrera Calderón y M. R. Aguilar Martínez, "Guía integral de empleo de la informática forense en el proceso penal de Ecuador," Universidad y Sociedad, 2020. https://rus.ucf.edu.cu/index.php/rus/article/view/1773/1771

[8] S. Trigo et al., "Searching for IOCs in forensic evidence," Proc. LACCEI, 2020. http://dx.doi.org/10.18687/LACCEI2020.1.1.647.

[9] Y. Riega-Viru et al., "Cybercrime: A systematic review of the literature," Proc. LACCEI, 2022. http://dx.doi.org/10.18687/LACCEI2022.1.1.576.

[10] R. A. Macías-Lara et al., "Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática," Sapienza, 2022. https://doi.org/10.51798/sijis.v3i2.324.

[11] F. Díaz, N. Cerna y R. Liza, "Artificial Intelligence and Crime in Latin America: A Multilingual Bibliometric Review (2010–2025)," Information, 2025. https://doi.org/10.3390/info16111001.

[12] R. X. M. Sampaio, "Inteligência artificial e (in)admissibilidade das provas digitais asseguradas pela cadeia de custódia," Revista do CAAP, 2025. https://doi.org/10.69881/8bmk6478.

[13] N. T. MacHado et al., "Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta," Rev. Científica General José María Córdova, 2021. https://doi.org/10.21830/19006586.726.

[14] M. L. Angelo Edu, G. P. Alexis y W. P. Lenis, "Marco de trabajo de ciberseguridad para PYMES en el Perú compuesto por controles ISO/IEC 27001 y CSF NIST," CISTI, 2023. https://doi.org/10.23919/CISTI58278.2023.10211874.

[15] G. Quispe-Kobashikawa et al., "Enhancing Information Security in Technology SMEs: A Metrics-Driven Model Based on ISO/IEC 27001:2022," ETASR, 2026. https://doi.org/10.48084/etasr.17248.

[16] L. A. S. Hinostroza et al., "ISO 27001 para la gestión de la seguridad de la información: una revisión sistemática en Latinoamérica," Proc. LACCEI, 2024. https://doi.org/10.18687/LEIRD2024.1.1.584.

[17] L. Biggi et al., "Development and Validation of a Cybersecurity Model for Ransomware Mitigation Based on NIST CSF 2.0," ETASR, 2025. https://doi.org/10.48084/etasr.12948.

[18] J. Rojas-Segura et al., "¿Cómo evaluar el riesgo cibernético de las PYMEs? Una estrategia de la Academia para crear ventajas competitivas," Proc. LACCEI, 2024. https://doi.org/10.18687/LACCEI2024.1.1.639.

[19] D. A. Gil Arenas et al., "Gestión del riesgo y evaluación de la eficacia de los controles de mitigación en las empresas de servicios públicos de Antioquia, Colombia," REDER, 2025. https://doi.org/10.55467/reder.v9i1.178.

[20] P. B. Vásquez-Méndez et al., "The Human Factor: Assessing Ransomware Vulnerability in Developing Nations' Governments," Information, 2026. https://doi.org/10.3390/info17020211.

[21] E. D. Canedo et al., "Cybersecurity risks, DevSecOps challenges, and emerging security priorities: An empirical study across Brazilian organizations," Computers & Security, 2026. https://doi.org/10.1016/j.cose.2026.105026..

[22] M. Ramírez et al., "The Disclosures of Information on Cybersecurity in Listed Companies in Latin America," Sustainability, 2022. https://doi.org/10.3390/su14031390.

[23] L. S. Sakamoto et al., "Professional Guidance of the DPOs-BR in Corporate Governance in Logistics Chains," IFIP AICT, 2022. https://doi.org/10.1007/978-3-031-16411-8_8.

[24] L. R. Puma Herencia et al., "Systematic Review of Authentication Techniques in Banking Applications in Latin America," Proc. LACCEI, 2024. https://doi.org/10.18687/LACCEI2024.1.1.201.

[25] F. Hilario et al., "Evaluation of Cyber Sabotage in Public Entities," J. System and Management Sciences, 2023. https://doi.org/10.33168/JSMS.2023.0434.

[26] M. M. Y. Gómez et al., "Application of Electronic Evidence in the Colombian Regulatory System," NovumJus, 2022. https://doi.org/10.14718/NovumJus.2022.16.1.11.

[27] A. S. Curbelo, "Towards an Autonomous Regulation of Digital Evidence," Derum, 2025. https://doi.org/10.47274/DERUM/48.6.