Experior
Revista de investigación ADEN

Experior: Revista de Investigación de ADEN University
ISSN L 2953-3090
Vol. 5 (2) julio-/diciembre 2026

Enfoques híbridos de controles informáticos. Integración de ISO 27001, COBIT y NIST para la seguridad

Hybrid IT Control Approaches. Integrating ISO 27001, COBIT, and NIST for Enhanced Information Security

Ibrain Kadir Lin Ríos
Universidad de Panamá, Panamá
Ibrain.lin@up.ac.pa
https://orcid.org/0009-0009-0690-6261

Carlos V. Bruce
Universidad de Panamá, Panamá
carlos.bruce@up.ac.pa
https://orcid.org/0009-0004-4223-0821

Alonso Gonzalez Vega
Universidad de Panamá, Panamá
alonso.gonzalez-v@up.ac.pa
https://orcid.org/0000-0002-7173-4031

Recibido: 23/10/2025.
Aceptado: 14/04/2026.
Publicado: 15/07/2026.

Cómo citar: Lin Ríos, I., Bruce, C., Gonzalez Vega, A. (2026). Enfoques híbridos de controles informáticos. Integración de ISO 27001, COBIT y NIST para la seguridad. *Experior, 5*(2), 136-148. https://doi.org/10.56880/experior52.3

Resumen

El estudio diseña un enfoque híbrido de controles informáticos integrando las normas internacionales ISO/IEC 27001, COBIT 2019 y NIST CSF para fortalecer la seguridad de la información en las organizaciones. Se realizó una investigación de tipo proyectivo y descriptivo con metodología cualitativa, basada en el análisis documental y comparativo de los tres marcos normativos. El proceso se estructuró de acuerdo con un análisis individual y comparativo de sus estructuras y fortalezas, la identificación de puntos de convergencia y complementariedad, y la síntesis proyectiva para diseñar el modelo. El análisis mostró el valor único y complementario de cada marco: ISO/IEC 27001 (gestión sistémica), COBIT 2019 (gobernanza y alineación) y NIST CSF (operación táctica y resiliencia). La contribución del estudio es la propuesta del Modelo Híbrido de Controles Informáticos MHCI, una arquitectura tridimensional que conecta las tres capas en un ciclo que se retroalimenta constantemente, para que la cobertura de seguridad sea completa y esté alineada con las necesidades de cada organización. Se concluye que la integración híbrida de los tres marcos proporciona una mejor cobertura que su aplicación aislada mejorando la gestión de riesgos, el uso de recursos y fortaleciendo la capacidad de respuesta y recuperación. Se presenta como una

propuesta teórica proyectiva que necesita, como segundo paso, ser validada empíricamente, lo que se propone como línea de investigación.
Palabras clave: controles informáticos, seguridad de la información, ISO 27001, COBIT, enfoque híbrido.

Abstract

This study designs a hybrid approach to IT controls, integrating the international standards ISO/IEC 27001, COBIT 2019, and NIST CSF to strengthen information security in organizations. A projective and descriptive research approach was used, employing a qualitative methodology based on documentary and comparative analysis of the three regulatory frameworks. The process was structured according to an individual and comparative analysis of their structures and strengths, the identification of points of convergence and complementarity, and a projective synthesis to design the model. The analysis revealed the unique and complementary value of each framework: ISO/IEC 27001 (systemic management), COBIT 2019 (governance and alignment), and NIST CSF (tactical operation and resilience). The study's contribution is the proposal of the Hybrid Model of Computer Controls MHCI, a three-dimensional architecture that connects the three layers in a constantly self-reinforcing cycle, ensuring comprehensive security coverage aligned with the needs of each organization. It is concluded that the hybrid integration of the three frameworks provides better coverage than their isolated application, improving risk management, resource utilization, and strengthening response and recovery capabilities. This is presented as a projective theoretical proposal that, as a second step, requires empirical validation, which is proposed as a line of research.
Keywords: IT controls, Information security, ISO 27001, COBIT, hybrid approach.

Introducción

La seguridad de la información se ha convertido en una prioridad estratégica para las organizaciones del siglo XXI, por la digitalización masiva de los procesos y la sofisticación de las amenazas cibernéticas que aumentan cada día. Los controles informáticos han evolucionado de medidas técnicas sin conexión entre ellas a elementos necesarios de un sistema de gestión encargados de preservar la confidencialidad y disponibilidad de los activos más importantes. Como la efectividad se esos controles constantemente se ve desafiada por la aparición de las vulnerabilidades que surgen y los vectores de ataque, se ven expuestas las limitaciones de los enfoques de seguridad que no se encuentran cohesionados o están basados en un estándar único.

En respuesta a ello, la comunidad global ha desarrollado diferentes tipos de estándares, normativas y buenas prácticas, donde está la familia ISO/IEC 27000 (ISO, 2018), COBIT (León-Acurio *et al.*, 2018), y el NIST *Cybersecurity Framework*, cada uno ofreciendo visiones de valor nuevas pero parciales, para la gestión de la ciberseguridad. La aplicación aislada de cualquiera de ellos, va limitando la capacidad organizacional para lograr una postura de seguridad adaptativa. Esta situación es evidente en contextos donde la convergencia de los requisitos regulatorios, tecnológicos y operativos necesita de una visión holística y sinérgica.

Ante la problemática surgida, la pregunta de investigación es: ¿de qué manera la integración de los principios y controles de las normas internacionales como la ISO/IEC 27001, COBIT y el NIST *Cybersecurity Framework* (Pascoe,

2023) en un enfoque híbrido puede fortalecer la seguridad de la información en las organizaciones? Esta pregunta puede ser respondida en este artículo, desarrollando el objetivo de diseñar un enfoque híbrido de controles informáticos que combine normas internacionales de buenas prácticas para fortalecer la seguridad de la información en las organizaciones modernas.

Revisión de la literatura

La gestión de la seguridad de la información se sustenta en estándares de buenas prácticas reconocidos internacionalmente, entre los que se encuentran como más influyentes las normas ISO/IEC 27000, que proporciona los fundamentos para el Sistema de Gestión de Seguridad de la Información (SGSI) basado en riesgos y mejora continua (ISO, 2018); COBIT, un marco integral enfocado en la gobernanza y gestión de las tecnologías de la información, necesario para la alineación estratégica y el control (León-Acurio *et al.*, 2018); y el NIST *Cybersecurity Framework* (CSF), que ofrece un enfoque práctico para gestionar los riesgos cibernéticos, organizado en las funciones de identificar, proteger, detectar, responder y recuperar (NIST, 2018).

Se identificaron limitaciones en la adopción de una metodología única, y Alcaraz & Zeadally (2015) ya habían señalado que la estructura de un SGSI, que está basado solo en la ISO 27001, dificulta la respuesta rápida a las ciberamenazas dinámicas (entendiendo que son dinámicas porque evolucionan, se adaptan y cambian constantemente para evadir las defensas creadas). Esta observación se ha visto reforzada por análisis comparativos más recientes, como los de Salihu & Dervishi (2024), con la evaluación del impacto de varios marcos en las auditorías de TI, destacando que cada uno organiza el proceso y descubre brechas de control desde una perspectiva particular, lo que da a entender que la dependencia de uno solo deja atrás críticas sin cubrir.

Sulistyowati *et al.* (2020) encontraron en su estudio que, a pesar de implementar múltiples estándares de seguridad, una organización gubernamental no alcanzaba un nivel óptimo de preparación, señalando la necesidad de contar con un enfoque integrado para medir la madurez de la ciberseguridad de forma holística. la complejidad de la gobernanza con COBIT también puede representar una barrera importante para las organizaciones que tienen menos tiempo trabajando con la tecnología, como se observa en contextos de aplicación específica (Rochmadi *et al*., 2025).

Para tratar estas limitaciones, se encontraron diversos artículos que buscan la integración y los modelos híbridos. La noción de un enfoque híbrido ha demostrado su utilidad en la gestión de proyectos de TIC en la administración pública, para darle una alineación más segura a la estrategia institucional (Cristaldo *et al.*, 2019). Trasladando este tema al área de la ciberseguridad, este concepto adquiere mayor relevancia, demostrado por autores que sostienen de forma convergente que la combinación de los marcos es el camino más objetivo para construir la resiliencia.

Metin *et al*. (2025) proponen una guía para desarrollar una estrategia de ciberseguridad integrando la gobernanza de COBIT 2019 con los controles de la

serie de normas ISO/IEC 27000, siendo el único documento en la revisión que se realizó que llena ese vacío en la literatura estratégica. Batte (2025) concluye que los modelos de adopción híbrida que combinan ISO 27001 con otros marcos como COBIT, NIST CSF u OCTAVE, son superiores, porque no se centran en cumplir la lista sino que alinean los controles de seguridad con la gestión de los riesgos empresariales.

Esa tendencia se materializa en propuestas de modelos sintetizados, siendo Harizaj *et al*. (2025) los autores de un análisis de vulnerabilidad estratégica para proponer un modelo híbrido que fusiona la estructura de gobierno de ISO/IEC 27001 con la flexibilidad operativa del NIST CSF, buscando mejorar la capacidad de decisión organizacional. Los hallazgos que realizaron Boné-Andrade *et al*. (2023) sobre estrategias en entornos laborales modernos refuerzan esta idea, señalando cómo la eficacia depende de la integración de la tecnología con procesos organizacionales bien establecidos y marcos de gobernanza adaptativos.

En los documentos revisados se presentan pruebas de que los marcos ISO 27001, COBIT y NIST CSF funcionan con solidez, pero se confirma que hay una limitación con su aplicación de forma aislada, especialmente con las ciberamenazas dinámicas. También se confirmó que los investigadores convergen a favor de los enfoques integrados (o híbridos), capaces de proporcionar una cobertura más completa y una gobernanza más alineada con el negocio. Aunque existen las propuestas para integrar los marcos por pares (como ISO y COBIT, o ISO y NIST) y un reconocimiento general de la ventaja que ofrece la combinación, se identificó la oportunidad de desarrollar y presentar un modelo híbrido tridimensional que represente la unión de la gestión con las normas ISO 27001, la gobernanza con el marco COBIT y la operación táctica con las NIST CSF, de manera unificada, y es por eso que este artículo pretende ser una contribución en esa área.

Metodología

Para alcanzar el objetivo del estudio, la investigación se desarrolló bajo un enfoque proyectivo y descriptivo, con una metodología cualitativa. El diseño fue no experimental y se basó en un análisis documental y comparativo de los marcos normativos internacionales, siguiendo tres etapas.

El estudio es de tipo proyectivo, porque su propósito fue proponer un modelo a partir del diagnóstico y análisis de la situación actual de los marcos de seguridad. Es descriptivo porque se buscó caracterizar y comparar los marcos ISO/IEC 27001, COBIT 2019 y NIST CSF en cuanto a su estructura, propósito y controles. Las unidades de análisis fueron los tres marcos internacionales de seguridad de la información y ciberseguridad ISO/IEC 27000:2018 con su Anexo A de controles; el marco COBIT 2019 y el NIST Cybersecurity Framework (CSF).

La población son todos los dominios, controles, objetivos y funciones que estructuran estos marcos, de donde se realizó un muestreo intencional seleccionando para el análisis los componentes considerados por los mismos marcos como ‘críticos’ para la gestión integral de seguridad: los procesos de

gestión de riesgos, gobierno y alineación estratégica, la respuesta a incidentes, y los controles operativos de protección y resiliencia.

Con la técnica de revisión de la literatura y documentos normativos se recolectaron en el mismo orden para comparar estos elementos: el propósito de cada marco, la estructura organizativa (los dominios, funciones y objetivos), los tipos de controles o prácticas, y el enfoque principal para conocer si eran de gestión, de gobierno o de operación. Los datos se agruparon en una tabla en Excel, donde posteriormente se agruparon las fuentes que abordaban cada uno de los tres marcos.

Se triangularon las fuentes para cumplir con la validez, donde las primarias se identificaron como los documentos oficiales y normativos publicados por la ISO, ISACA y NIST, y las secundarias los artículos científicos y estudios de casos que analizaron la aplicación o unión de estos marcos, centrándose en los más actuales, con excepción de la información que se considera clásica, según la explicación de Cruz García (2019).

Los datos se analizaron según la explicación de Bernete (2013): el análisis de contenido se aplicó a los documentos normativos para conocer su estructura y los componentes de cada marco; el análisis comparativo sirvió para contrastar los marcos e identificar en qué se especializaba cada uno, dónde y cómo se relacionaban entre sí. Luego se aplicó un análisis sintético y de diseño, ya que a partir de los hallazgos de la comparación se hizo la síntesis creativa para diseñar el modelo híbrido, tomando en cuenta que los tres marcos tuvieran coherencia entre sí en lo que se estaba proponiendo.

Operativamente se puede observar que el análisis condujo a un proceso de tres pasos, donde en el primero de ellos se procedió con el análisis individual y comparativo de los tres marcos; en el segundo se identificaron las dependencias, y los flujos potenciales de información con un análisis cruzado de los componentes de los marcos; y en el tercero se visualizó el diseño del modelo a partir de la integración de todos los hallazgos.

Resultados

El objetivo del estudio se alcanzó a través de tres pasos en específico: en primer lugar se procedió a realizar una comparación entre los marcos ISO/IEC 27001, COBIT 2019 y NIST CSF, posteriormente se realizó un análisis de los puntos en común y cuál es el valor añadido, para tener las bases con las cuales se pudo proponer el modelo. El desarrollo quedó conformado como se presenta a continuación:

Comparación de marcos ISO/IEC 27001, COBIT 2019 y NIST CSF

Se identificó que cada marco tiene una contribución muy particular a la seguridad de la información. Si se analizan sus fortalezas y los aportes únicos, la ISO/IEC 27001 es hasta el momento el estándar de referencia para la gestión sistemática y la certificación formal (Shojaie *et al*., 2014). El valor que tiene esta norma es la forma en que proporciona un modelo integral para establecer, implementar, mantener y mejorar un Sistema de Seguridad de la Información

(SGSI) basado en el ciclo de mejora continua PDCA (Planificar, Hacer, Verificar, Actuar). En el Anexo A, que organiza 114 controles en 14 dominios, se ofrece una estructura de gobernanza operativa que le da a las organizaciones la opción de mitigar los riesgos de manera documentada y justificada en una declaración de aplicabilidad (Fathurohman & Witjaksono, 2020). Su principal fortaleza es la capacidad de generar un sistema auditado y certificable que le imprime un sello de confianza reconocido internacionalmente (ISO, 2018).

El COBIT 2019 tiene su valor en la gobernanza estratégica y la alineación con el negocio, porque su propósito es gobernar y gestionar la Tecnología de la Información (TI) para crear valor y hacer que las inversiones de seguridad estén directamente vinculadas a los objetivos corporativos (ISACA, 2019). A través de sus 40 objetivos de gobierno (dominio EDM) y gestión (dominios APO, BAI, DSS y MEA), y mediante otros componentes como estructuras organizativas y flujos de información, COBIT convierte la estrategia empresarial en acciones de TI (Adams, 2024).

Estos cinco dominios son el núcleo estructural del marco COBIT 2019 para organizar los procesos de gobierno y gestión de TI; en sus categorías principales, EDM (Evaluar, Dirigir y Supervisar) es el dominio central del Gobierno, porque es donde la Junta Directiva y la Alta Dirección evalúan las opciones estratégicas, dirigen a la gerencia estableciendo las prioridades y marcos de trabajo, y supervisan el logro de los objetivos. Su foco está en asegurar que las inversiones en TI (incluyendo seguridad) generen valor y mitiguen riesgos, alineándose con la estrategia corporativa e incluye 5 objetivos de gobierno.

Los otros cuatro son dominios de gestión (APO, BAI, DSS, MEA) que ejecutan las decisiones estratégicas tomadas en EDM, se basan en el ciclo de vida clásico de Planificar, Construir, Mantener, Monitorear, adaptado a la gestión de TI. APO (Alinear, Planificar y Organizar) se centra en la planificación estratégica y táctica. Aquí se definen la estrategia de TI, la arquitectura, la innovación, el portafolio de proyectos, la gestión de riesgos y la alineación con el negocio (Anoruo *et al.*, 2019). Es donde se planifica cómo creará valor la TI.

BAI (Construir, Adquirir e Implementar) cubre todo el ciclo de desarrollo y adquisición de soluciones de TI. Incluye la gestión de proyectos, definición de requisitos, desarrollo, implementación y gestión de cambios, que es donde las ideas y los planes se llevan a cabo. DSS (Entregar, Servir y Soportar) se ocupa de la operación y el servicio diario. Aquí están los procesos de operaciones de TI, gestión de incidentes y problemas, seguridad operativa, soporte a usuarios y gestión de servicios; es donde se entrega el valor a los usuarios finales y se mantiene la continuidad. MEA (Monitorear, Evaluar, Verificar) es el dominio que se asegura del control y la mejora continua, evaluando el desempeño y el cumplimiento de los procesos de TI, supervisando los controles internos y revisando que el sistema de gobierno esté funcionando correctamente. Este es el dominio que proporciona la retroalimentación necesaria para todos los demás dominios (Anoruo *et al.*, 2019).

El NIST *Cybersecurity Framework* (CSF) se centra en la operación táctica y la ciberresiliencia, porque ha sido diseñado inicialmente para la infraestructura crítica, pero es aplicable a cualquier organización. Proporciona un lenguaje práctico y orientado a la acción a través de sus cinco funciones de Identificar, Proteger, Detectar, Responder y Recuperar, desglosadas en 23 categorías y 108 subcategorías (NIST, 2018). El valor que se puede considerar como único con respecto a los otros dos es que ofrece una guía para la implementación de los controles técnicos, la gestión continua de incidentes y la mejora adaptativa de la postura de seguridad. A diferencia de los marcos anteriores, el NIST CSF se centra en el 'cómo' operativo, facilitando la respuesta dinámica a las amenazas en evolución y fortaleciendo la capacidad de recuperación organizacional (Clomera, 2025).

Los tres marcos, unidos, se complementan: LA ISO 27001 establece el sistema de gestión formal (el 'qué'), COBIT 2019 proporciona el gobierno estratégico (el por qué y para quién), y el NIST CSF es el cómo de la ejecución operativa. Si se aplican unidos, cubren toda el área de la seguridad de la información, es decir, van desde la definición estratégica, hasta la respuesta táctica ante los incidentes.

Análisis de puntos en común y valor añadido

En el análisis de los marcos se pudo determinar que están solapados, pero no es redundante, sino sinérgico y secuencial, porque cada marco organiza el proceso de seguridad desde una perspectiva distinta pero interconectada (Salihu & Dervishi, 2024), por lo tanto, la complementariedad se hace evidente en tres procesos de gran importancia para la seguridad de la información (Sulistyowati *et al.*, 2020) definidos a continuación.

En primer lugar está el ciclo de gestión de riesgos que se articula a través de los tres marcos. La norma ISO/IEC 27001 establece el proceso formal a través del dominio 'Evaluación de la seguridad de la información' (A.12.1), que exige identificar, analizar y evaluar los riesgos para los activos, que es una práctica necesaria para la implantación de un SGSI efectivo (ISO, 2018). Este proceso se opera a través de la función Identificar del NIST CSF, en la categoría Evaluación de Riesgos (ID.RA), que guía la realización de evaluaciones periódicas de vulnerabilidades y amenazas (NIST, 2018). A nivel estratégico, el COBIT 2019 ofrece el contexto de gobierno a través del objetivo para Evaluar, Dirigir y Supervisar el Riesgo (EDM03), para asegurarse de que los hallazgos de la evaluación sean priorizados según la estrategia del negocio y la disposición frente al riesgo organizacional, convirtiéndose en decisiones de inversión (Anoruo, 2019).

En segundo lugar, la respuesta y recuperación ante los incidentes es un ejemplo de cómo la resiliencia se construye en capas. ISO/IEC 27001 define el marco del sistema en el dominio Gestión de incidentes de seguridad de la información (A.16), necesitando procedimientos documentados para reportar y gestionar los eventos (ISO, 2018). El NIST CSF proporciona la guía operativa para actuar a través de sus funciones Responder (RS) y Recuperar (RC),

especificando las actividades de contención, comunicación y restauración (NIST, 2018). La efectividad de todo este ciclo es supervisada y evaluada por COBIT 2019 en su dominio Monitorear, Evaluar y Verificar (MEA), donde procesos como la evaluación del cumplimiento hacen que la respuesta cumpla con las obligaciones regulatorias y que se extraigan experiencias para asumir la mejora con la mejora continua (Adams, 2024).

En tercer lugar está la protección de activos y el control de acceso, que demuestran la integración entre política, tecnología y supervisión. La ISO/IEC 27001 establece los requisitos en los dominios Gestión de activos (A.8) y Control de acceso (A.9) (Fathurohman & Witjaksono, 2020). El NIST CSF especifica los controles técnicos y procesos para implementar esos requisitos bajo las categorías de la función Proteger (PR), como Seguridad de datos (PR.DS) e Identificación y control de acceso (PR.AC) (Pascoe, 2023). El COBIT 2019 hace que la alineación y el control estratégico mediante objetivos como el BAI09 Gestionar activos y el DSS05 Gestionar accesos de seguridad, garantice que esos controles estén diseñados para respaldar los procesos de negocio y se encuentren sujetos a auditorías y gobierno efectivo (León-Acurio *et al*., 2018).

ISO 27001 define el sistema, que es el *qué*, el COBIT dirige su alineación estratégica que es el *porqué* y el NIST CSF señala el camino operativo o el *cómo*, y así se constituye la base para los modelos integrados. Precisamente este tipo de enfoques híbridos son solicitados para que se resuelvan las limitaciones de los marcos aplicados de forma aislada y que se fortalezcan la gobernanza y la resiliencia organizacional, según lo señalan Metin *et al.* (2025) o Harizaj *et al*. (2025).

Arévalo Ascanio *et al.* (2015) demostraron el valor de la norma ISO/IEC 27001 para estructurar la gestión del riesgo de la información y concientizar sobre la protección de activos. Sin embargo, el estudio muestra también las limitaciones comunes que enfrentan los contextos reales, como la baja madurez tecnológica, la falta de una cultura de seguridad bien asentada y la percepción de la seguridad como un costo más que como un facilitador estratégico.

Estas limitaciones coinciden con las brechas que los marcos de gobierno (COBIT) y la operación táctica (NIST CSF) están diseñados para cerrar. La implementación aislada de un SGSI puede encontrar estos obstáculos, mientras que un enfoque híbrido que desde el inicio integre la gobernanza estratégica de COBIT 2019 (con sus 40 objetivos claramente definidos para alinear, dirigir y supervisar, según lo señalan Lainhart *et al*., 2018) y las guías de acción continua del NIST CSF, podría proporcionar un camino más sólido y adaptado. El refuerzo mutuo mejoraría la implementación del sistema de gestión y transformaría la seguridad de la información en un componente integral de la creación de valor y la resiliencia organizacional.

Propuesta del Modelo Híbrido Tridimensional

Basándose en el análisis comparativo y en la identificación de sinergias, este estudio propone el Modelo Híbrido de Controles Informáticos (MHCI), diseñado para integrar de manera coherente y práctica los tres marcos

normativos. El principio rector del modelo es que una postura de seguridad fuerte necesita de la convergencia de tres dimensiones interdependientes entre sí: un sistema de gestión formal, una gobernanza estratégica alineada al negocio y una operación táctica resiliente.

Se fundamenta en el principio de que la seguridad es el resultado de un ciclo entre la definición (gestión), la dirección (gobierno) y la acción (operación). Este principio responde a la necesidad de unificar criterios a través de la integración de los estándares y protocolos (Cristaldo *et al*., 2019), buscando el cumplimiento, la creación de valor y la capacidad adaptativa ante las amenazas (Boné-Andrade *et al*., 2023). Se estructura en tres capas principales y cada una está sustentada por los estándares que más aporten a su función.

En la capa 1 de Gestión sistémica (sustentada por la ISO/IEC 27001), se establece el sistema de gestión, y su objetivo es institucionalizar la seguridad a través de un Sistema de Gestión de Seguridad de la Información (SGSI) certificable. En este nivel se ejecuta el ciclo PDCA, planificando las políticas (A.5) y la evaluación de riesgos (A.12); se implementan los 114 controles del Anexo A, justificados en la declaración de aplicabilidad; se verifican mediante auditorías internas y revisiones de la dirección; y se actúa para mejorar continuamente. Proporciona la base documentada, repetible y auditada que requiere el cumplimiento normativo (ISO, 2018; Everett, 2011).

En la capa 2 de Gobernanza y alineación (sustentada por COBIT 2019) se direcciona el proceso para que el SGSI genere valor para el negocio. Utiliza la cascada de objetivos de COBIT para convertir las metas corporativas en requerimientos de seguridad. Los procesos de los dominios Evaluar, Dirigir y Supervisar (EDM) establecen la tolerancia al riesgo y evalúan el desempeño estratégico. Los dominios de gestión como Alinear, Planificar y Organizar (APO), asignan recursos, definen indicadores de desempeño (KGI/KPI) y hacen que los controles de la capa 1 estén en concordancia con los procesos críticos del negocio. Esta capa responde a la pregunta si ¿estamos protegiendo lo correcto, de la manera correcta, para alcanzar los objetivos? (Anoruo, 2019).

En la capa 3, donde se encuentra la Operación táctica y resiliencia (sustentada por NIST CSF), para la ejecución y adaptación continua, que interactúa con el contexto de amenazas. Organiza todas las actividades de seguridad técnica y operativa en torno a las cinco funciones del NIST CSF para identificar, proteger, detectar, responder y recuperar. Aquí se implementan los *firewalls*, los sistemas de detección de intrusos, los programas de concientización, los planes de respuesta a incidentes y los procedimientos de recuperación ante desastres. Proporciona un lenguaje común y un camino para ejecutar las acciones de forma inmediata y la mejora adaptativa, fortaleciendo la resiliencia organizacional (NIST, 2018).

La integración del modelo es por ciclos y no secuencial, porque se retroalimenta constantemente, y el mecanismo de integración funciona mediante dos tipos de flujo:

Flujo ascendente (se comprende desde la operación a la gobernanza y la gestión). Los resultados operativos de la capa 3 (NIST CSF) se comunican a

la capa 2 (COBIT). Aquí son evaluados en el contexto del negocio (EDM03) para determinar su impacto estratégico y darle un orden a las acciones que se van a atender. A su vez, estos hallazgos alimentan la capa 1 (ISO 27001), actuando como desencadenante de la revisión de la evaluación de riesgos (A.12.1) y la actualización de la Declaración de Aplicabilidad, cerrando el ciclo de mejora del SGSI.

Flujo descendente (de la gobernanza y la gestión a la operación). Las estrategias y políticas definidas en la capa 2 (COBIT) y formalizadas en el sistema de la capa 1 (ISO 27001) se convierten en requisitos e indicadores de desempeño. Los requisitos son implementados como planes de acción, controles técnicos y procedimientos operativos en la capa 3 (NIST CSF), guiando el trabajo diario de los equipos de seguridad.

Ese flujo bidireccional hace que la operación esté informada por la estrategia y que la estrategia -a su vez- se actualice de la realidad operativa, creando un sistema de seguridad vivo, adaptativo y que responda a los intereses del negocio.

Conclusiones

Con la propuesta de diseñar un enfoque híbrido de controles informáticos que combinara normas internacionales de buenas prácticas para fortalecer la seguridad de la información, se realizó un análisis proyectivo y descriptivo donde se lograron los siguientes resultados que permiten darle respuesta a la pregunta de investigación y cumplir con el objetivo presentado.

En primer lugar, el análisis comparativo de los marcos ISO/IEC 27001, COBIT 2019 y NIST CSF confirmó que cada uno tiene un valor central y complementario, ya que se identificó que la ISO 27001 aporta una estructura de gestión sistémica y certificable, el marco COBIT 2019 se enfoca en la gobernanza estratégica y la alineación con el negocio, mientras que el NIST CSF ofrece una guía para la operación táctica y la ciberresiliencia. El estudio agrupó estas normativas para cubrir el proceso completo desde la definición de las políticas hasta la respuesta a los posibles incidentes.

Los puntos de convergencia y complementariedad sinérgica entre estos marcos se pudieron identificar, al demostrar que los procesos críticos como la gestión de riesgos, la respuesta a incidentes y el control de acceso no se solapan de manera redundante, sino que se articulan en una secuencia lógica donde un marco establece el requisito, el otro dirige su alineación estratégica y el último describe la implementación operativa. Se realizó una interrelación que conforma una base lo suficientemente sólida para que la integración sea efectiva.

Se confirma que la principal contribución del artículo es proponer el modelo, donde los autores integraron la Capa de gestión y sistema (ISO 27001), la Capa de gobernanza y alineación (COBIT 2019) y la Capa operativa táctica de resiliencia (NIST CSF) en un ciclo que permite retroalimentarse constantemente. Con este diseño las organizaciones pueden trabajar con los estándares en conjunto, promoviendo en su lugar un sistema de seguridad adaptable que esté alineado con los objetivos de negocio y centrado en la resiliencia.

Por lo tanto, en respuesta a la pregunta de investigación, se concluye que la integración de los principios y controles de ISO/IEC 27001, COBIT y NIST CSF en un enfoque híbrido estructurado, como el MHCI, fortalece la seguridad de la información al proporcionar una cobertura completa. Este enfoque mejora la gestión de riesgos, facilita la asignación de recursos porque evita las redundancias, fortalece la gobernanza de TI y, lo más importante, incrementa la capacidad de respuesta y recuperación ante cualquier tipo de incidentes de seguridad.

Sin embargo, es importante señalar que el modelo apenas es una propuesta teórica y proyectiva, que tiene un diseño que se fundamenta en el análisis documental y comparativo. La principal limitación del estudio está en la necesidad de validarlo en la práctica para comprobar si es eficaz, viable y si puede adaptarse al contexto organizacional.

Como líneas de investigación se recomienda: 1) implementación y evaluación del modelo mediante estudios de caso en áreas específicas para comprobar su funcionamiento; 2) desarrollo de una guía de implementación con fases, roles y KPI; 3) exploración de la integración de herramientas tecnológicas para automatizar el flujo de información entre las capas del modelo.

Referencias

Adams, N-R. (2024). *COBIT 2019: IT governance framework*. https://itlawco.com/cobit-2019-it-governance-framework/#:~:text=de%20la%20organizaci%C3%B3n.-,Creaci%C3%B3n%20de%20valor,como%20personas%2C%20procesos%20y%20tecnolog%C3%ADa.

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, *8*, 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002

Anoruo, C., CISM, CGEIT & CRISC. (2019). *Employing COBIT 2019 for Enterprise Governance Strategy*. ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-for-enterprise-governance-strategy#:~:text=Objetivos%20de%20gobernanza%20y%20gesti%C3%B3n,de%20los%20objetivos%20que%20contienen:&text=Evaluar%2C%20dirigir%20y%20supervisar%20(EDM,%2C%20evaluar%20y%20valorar%20(MEA)

Arévalo Ascanio, J. G., Bayona Trillos, R. A., & Rico Bautista, D. W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Tecnura*, *19*(46), 123-134. http://dx.doi.org/10.14483/udistrital.jour.tecnura.2015.4.a10

Batte, B. (2025). ISO 27001 and Alternative Frameworks for Managing Information Security Risks. *Available at SSRN 5546398*. https://dx.doi.org/10.2139/ssrn.5546398

Bernete, F. (2013). Análisis de contenido. *Conocer lo social: estrategias y técnicas de construcción y análisis de datos*, 193-203. https://docta.ucm.es/rest/api/core/bitstreams/d7587d54-592d-416c-81b0-15685c3f3204/content

Boné-Andrade, M. F., Pinargote-Bravo, V. J., & Bonilla-Fierro, L. F. (2023). Estrategias de ciberseguridad en entornos de trabajo híbridos y remoto. *Revista Científica Ciencia y Método*, *1*(4), 31-43. https://doi.org/10.55813/gaea/rcym/v1/n4/21

Clomera, A. (2025). *Exploring the NIST CSF Categories and Subcategories: A Comprehensive Overview*. https://ipkeys.com/blog/nist-csf-categories/

Cristaldo, P. R., Ballejos, L. C., & Ale, M. A. (2019). Propuesta metodológica de enfoque "híbrido" para la gestión de proyectos de tics en la administración pública: Implementación y verificación. *Revista Tecnología y Ciencia*, (34), 16-36. https://doi.org/10.33414/rtyc.34.16-36.2019

Cruz García, M. A. (2019). Fuentes de información. *Boletín científico de las ciencias económico administrativas del ICEA*, *8*(15), 57-58. https://doi.org/10.29057/icea.v8i15.4864

Everett, C. (2011). Is ISO 27001 worth it? *Computer Fraud & Security*, *2011*(1), 5-7. https://doi.org/10.1016/S1361-3723(11)70005-7

Fathurohman, A., & Witjaksono, R. W. (2020). Analysis and design of information security management system based on ISO 27001: 2013 using Annex Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering*, *1*(1), 1-11. https://doi.org/10.25008/bcsee.v1i1.2

Harizaj, M., Qafa, R., & Idrizi, O. (2025). Strategic Vulnerability Analysis of Cybersecurity Frameworks: Toward a Hybrid Model for Governance and Resilience. In *International Conference on Intelligence-Based Transformations of Technology and Business Trends* (pp. 84-96). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-07370-9_8

ISO. (2018). *ISO/IEC 27000:2018. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Descripción general y vocabulario*. ISO/IEC. https://www.iso.org/standard/73906.html

Lainhart, J., Conboy, M., & Saull, R. (2018). COBIT 2019 Governance and Management Objectives. *Schaumburg: ISACA*. https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf

León-Acurio, J. V., Mora-Aristega, J. E., Huilcapi-Masacon, M. R., Tamayo-Herrera, A. del P. & Armijos-Maya, C. A. (2018). COBIT como modelo para auditorías y control de los sistemas de información. *Polo del Conocimiento: Revista científico-profesional*, *3*(4), 17-36. https://dialnet.unirioja.es/servlet/articulo?codigo=9573039

Metin, B., Sevim, S. B., & Wynn, M. (2025). Cybersecurity Strategy Development: Towards an Integrated Approach Based on COBIT and ISO 27000 Series Standards. *Standards*, *5*(4), 33. https://doi.org/10.3390/standards5040033

NIST. (2018). *Marco para la mejora de la seguridad cibernética eninfraestructuras críticas*. Instituto Nacional de Estándares y Tecnología. https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

Pascoe, C. E. (2023). *Public draft: The NIST cybersecurity framework 2.0.* National Institute of Standards and Technology. https://www.authonet.com/assets/National-Institute-of-Standards-and-Technology.(NIST).Cybersecurity-Framework.CSWP.29.ipd.pdf

Rochmadi, T., Fadlil, A., & Riadi, I. (2025). Developing a Delphi Validated Instrument for Assessing Digital Forensics Readiness Based on COBIT 2019. *International Journal of Advances in Data and Information Systems*, *6*(3), 749-762. https://doi.org/10.59395/ijadis.v6i3.1453

Salihu, A., & Dervishi, R. (2024). Evaluating the Impact of Risk Management Frameworks on IT Audits: A Comparative Analysis of COSO, COBIT, ISO/IEC 27001, and NIST CSF. In *2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE)* (pp. 1-8). IEEE. https://doi.org/10.1109/ICECCE63537.2024.10823548

Shojaie, B., Federrath, H., & Saberi, I. (2014). Evaluating the effectiveness of ISO 27001: 2013 based on Annex A. In *2014 Ninth International Conference on Availability, Reliability and Security* (259-264). IEEE. https://doi.org/10.1109/ARES.2014.41

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. *JOIV: International Journal on Informatics Visualization*, *4*(4), 225-230. https://dx.doi.org/10.30630/joiv.4.4.482