INVESTIGACIÓN

Análisis de marcos de referencia sobre gestión de riesgos a la seguridad de la información

Analysis of reference frameworks on information security risk management

Clayret Echenique Quintana[1*]

Recibido: /06/2023 | Aceptado: /04/2023 | Publicado: 12/2023

Resumen

En un mundo cada vez más dependiente de la infraestructura tecnológica, las organizaciones enfrentan múltiples riesgos a la seguridad de la información, lo que puede afectar a su desempeño y sostenibilidad. Gestionarlos se ha convertido en una herramienta esencial para identificar, evaluar y mitigar las amenazas, es por ello que se han desarrollado varios marcos de gestión de riesgos destinados a ayudar a las organizaciones a tratar estos incidentes de forma eficaz. En la presente investigación se hizo un estudio sobre los marcos de referencia de gestión de riesgos de ciberseguridad, enfocándose precisamente en NIST, COBIT e ISO/IEC 27005, los cuales ofrecen diferentes puntos de vista acerca de la evaluación de los riesgos, pero con el mismo objetivo, contribuir a la seguridad de la información en las organizaciones. Se hizo una caracterización de forma general de estos marcos, se compararon en cuanto a diferentes criterios y además se exponen las principales limitaciones que tienen cada uno de estos. Los métodos teóricos que ayudaron a conformar el estudio exploratorio realizado fueron: histórico-lógico, analítico-sintético, inductivo-deductivo y sistémico-estructural-funcional. Este estudio ayuda a comprender las

1* Universidad de las Ciencias Informáticas. La Habana, Cuba. cechenique@ uci.cu

fortalezas y debilidades de estos modelos tan utilizados, para contribuir a una posterior evaluación de impacto de ciberseguridad en las organizaciones cubanas.

Palabras clave: COBIT; gestión de riesgos; ISO/IEC 27005; NIST; seguridad de la información

Abstract

In a world increasingly dependent on technological infrastructure, organizations face multiple risks to information security, which can affect their performance and sustainability. Managing them has become an essential tool to identify, assess and mitigate threats, which is why several risk management frameworks have been developed to help organizations deal with these incidents effectively. In the present investigation, a study was carried out on the cybersecurity risk management frameworks, focusing precisely on NIST, COBIT and ISO/IEC 27005, which offer different points of view about risk assessment, but with the aim of same objective, to contribute to information security in organizations. A general characterization of these frameworks was made, they were compared in terms of different criteria and the main limitations of each of these were also exposed. The theoretical methods that helped shape the exploratory study carried out were historical-logical, analytical-synthetic, inductive-deductive and systemic-structural-functional. This study helps to understand the strengths and weaknesses of these widely used models to contribute to a subsequent evaluation of the impact of cybersecurity in Cuban organizations.

Keywords: *COBIT; risk management; ISO/IEC 27005; NIST; information security*

Introducción

Desde hace unos años las organizaciones apuestan por la transformación digital pues son evidentes los beneficios que aportan al negocio. Es importante destacar que esta pretende obtener beneficios en cuanto al manejo de la información, procesos, recursos e incluso reduce errores humanos. Sin embargo, no se trata de implementar nuevas tecnologías, sino de lograr un cambio cultural y organizacional que garantice el

éxito en las organizaciones (Liendo Afonso, 2023). Es evidente que una vez realizadas las inversiones en infraestructura tecnológica se debe garantizar la seguridad de las mismas y es que hoy están muy presentes las amenazas cibernéticas, las cuales representan una vulnerabilidad para las organizaciones. Es por ello que se hace necesario centrar esfuerzos en implementar medidas de seguridad adecuadas para reducir los niveles de riesgos a los que se expone la información (Martínez Landrove, 2019).

El crecimiento de las infraestructuras de Tecnologías de la Información (TI), trae consigo además un auge de las investigaciones sobre el impacto que ellas representan para las organizaciones (Casanova & Calderón, 2020). Los resultados de varias investigaciones permitieron identificar que en la medida que sea mayor la alineación entre las TI y los objetivos del negocio, más amplio es el valor añadido que representan las infraestructuras TI para una organización (Pérez Lorences, 2014).

El impacto se mide de acuerdo a la misión de la entidad, por lo que es vital comprender todos los activos de TI. Cada activo tiene un valor, muchos son componentes clave para respaldar los servicios críticos que se brindan a los usuarios. Estos, además, influyen directamente en el capital y la valoración de la organización, y los riesgos de TI pueden tener un impacto directo en el presupuesto. Para cada organización, es vital y desafiante determinar las condiciones que realmente impactan a la misión; es muy importante analizar y comprender continuamente los recursos que permiten cumplir con los objetivos y que pueden verse comprometidos por los riesgos de ciberseguridad (Qui*nn, e*t al., 2022).

Un estudio exploratorio realizado por Casanova (2020) describe el estado de la gestión de las infraestructuras de TI en Cuba, este arrojó que en las organizaciones, las mayores medias de impacto “se corresponden con la lentitud en la respuesta a las necesidades de la organización, lo cual implica un serio problema de alineamiento” (p. 41). En segundo lugar, destaca “los problemas de implementar nuevos sistemas, debido a que implica un incremento de la complejidad de la gestión” (p. 41).

Las organizaciones cubanas dependen tecnológicamente de sus proveedores, lo que dificulta la renovación periódica y pertinente de las infraestructuras TI. De ahí que surge una conciencia sobre la importancia de la evaluación del impacto sobre la infraestructura. Cuba,

por su condición de país en desarrollo, no produce tecnología y por tanto debe importarla, lo que representa un mayor esfuerzo debido al Embargo Económico, de ahí que la evaluación del impacto reviste una importancia especial (Casanova & Calderón, 2020).

La presente investigación tiene como objetivo estudiar los diferentes marcos de referencia para la gestión de riesgos dentro de las organizaciones y poder determinar qué elementos son más adecuados para llevar a cabo la evaluación de impacto de la ciberseguridad en las organizaciones cubanas.

Materiales y métodos

Para el desarrollo de la investigación se realizó un estudio exploratorio sobre los marcos de referencia para la gestión de riesgos a la seguridad de la información, para lograr el alineamiento entre los objetivos y las tecnologías de la información de las organizaciones en cuanto disponibilidad, integridad y confidencialidad de los servicios prestados.

Los métodos teóricos utilizados son:

Histórico-lógico: se aplicó para determinar las tendencias actuales de los principales fundamentos teóricos y metodológicos, además de los antecedentes y el comportamiento de los marcos de referencia de gestión de riesgos.

Analítico-sintético: se utilizó este método para el procesamiento de la información referente a los marcos de referencia de gestión de riesgos y arribar a las conclusiones de la investigación, así como para precisar las características del trabajo a realizar.

Inductivo-deductivo: se empleó principalmente para la elaboración del marco teórico de la investigación.

Sistémico-estructural- funcional: posibilitó la integración de todos los elementos investigados de manera independiente para conformar toda la investigación realizada.

Resultados y discusión

En esta investigación se definen los principales fundamentos teóricos metodológicos vinculados a la evaluación de impacto de la ciberseguridad haciendo énfasis en los marcos de referencia de gestión de

riesgos. Se realiza una caracterización y comparación de dichos marcos, además de analizar las principales limitaciones de su adopción.

1. Marcos de ciberseguridad

Los marcos de ciberseguridad proporcionan una guía a las organizaciones para fortalecer sus sistemas de seguridad ante la ocurrencia de algún incidente. Un factor muy importante es ayudar a desplegar un sistema para la gestión de riesgos a la seguridad de la información (Ortega Candel, 2021). Algunos de estos se describen a continuación.

1.1 Marco de ciberseguridad del Instituto Nacional de Estándares y Tecnologías de Estados Unidos (NIST, por sus siglas en inglés)

El marco de ciberseguridad de NIST se diseñó con un conjunto de buenas prácticas para mitigar los riesgos asociados a la ciberseguridad en una organización. Promueve la protección y resiliencia de infraestructuras críticas y está diseñado para fomentar la gestión de riesgos y la ciberseguridad (Ortega Candel, 2021).

El marco está organizado en cinco funciones clave los cuales proporcionan una visión integral del ciclo de vida para la gestión del riesgo de ciberseguridad en el tiempo. La figura 1 muestra las funciones y las actividades que brindan un punto de partida para la mejora de la organización (Ma*hn, e*t al., 2021):

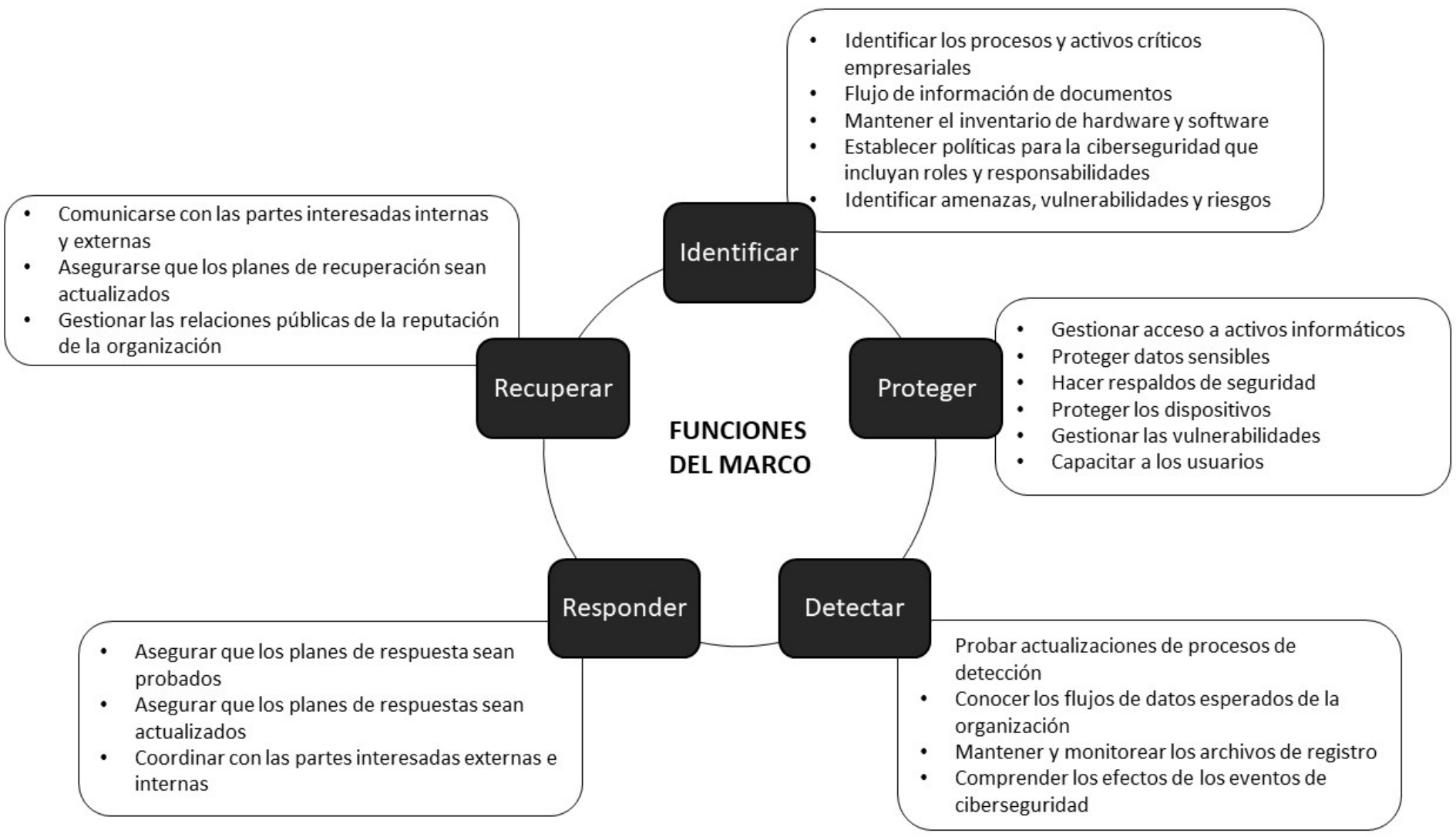

Figura 1. Funciones y actividades de NIST (Mahn, et al., 2021)

NIST provee un Marco de Gestión de Riesgos (RMF, por sus siglas en inglés) con siete pasos completos para que cualquier organización pueda administrar el riesgo de seguridad y privacidad de la información. Este se vincula con un conjunto de estándares y pautas para respaldar la implementación de programas de gestión de riesgos (Computer Security Division, 2016b).

Los pasos para implementar RMF, (ver Figura 2) en las organizaciones propuestos por NIST son (Computer Security Division, 2016a):

- Preparación: define las actividades esenciales para preparar a la organización para gestionar los riesgos de seguridad y privacidad.
- Catalogación: categoriza el sistema y la información procesada, almacenada y transmitida en función de un análisis de impacto.
- Selección: selecciona el conjunto de controles de NIST SP 800-53 para proteger los sistemas en función de las evaluaciones de riesgos.
- Implementación: implementa y documenta cómo se implementan los controles.
- Evaluación: evalúa para determinar si los controles están en su lugar, funcionando según lo previsto y produciendo los resultados deseados.
- Autorización: el directivo toma una decisión basada en el riesgo para autorizar el sistema (para operar).
- Monitorización: monitorea continuamente la implementación del control y los riesgos para el sistema.

El RMF de NIST se enfatiza en la importancia de la gestión continua de riesgos y estimula a las organizaciones a integrar procesos de gestión durante todo el ciclo de vida del desarrollo del sistema. Al proporcionar un enfoque estructurado, repetible y mensurable para la gestión de riesgos, el RMF permite a las organizaciones salvaguardar eficazmente sus sistemas de información y mantener el cumplimiento de las regulaciones pertinentes (Ahmet, 2023).

Figura 2. Pasos propuestos por NIST para implementar RMF en las organizaciones (Computer Security Division, 2016a).

1.2 Serie ISO/IEC 27000

La serie ISO/IEC 27000 está compuesto por estándares internacionales que contiene directrices para la seguridad de la información. Presenta buenas prácticas y procedimientos tanto físicos como de seguridad. Incorpora reglas que permiten reducir el creciente número de amenazas, resolver problemas de seguridad existentes y mejorar los objetivos de seguridad en general (Meriah & Rabai, 2019).

La norma ISO/IEC 27001 que define un modelo para establecer, implementar, operar, monitorear, revisar y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI). Agrupa once categorías con requisitos de seguridad de la información, estas a su vez están comprendidas por subcategorías, cada una con los correspondientes requisitos de cumplimiento de alto nivel (Meriah & Rabai, 2019).

La norma ISO/IEC 27002 comprende un código de buenas prácticas para la gestión de la seguridad de la información. Describe cientos de controles que se pueden implementar introducidos por la norma ISO/IEC 27001 (Meriah & Rabai, 2019).

La norma ISO/IEC 27005 contiene las pautas para la Gestión de Riesgos de Seguridad de la Información (ISRM, por sus siglas en inglés) en una organización. Basa sus conceptos, modelos, procesos y terminologías de conocimiento definidos por la norma ISO/IEC 27001 y ofrece ayuda para su implementación adoptando un enfoque de la gestión de riesgos (Meriah & Rabai, 2019).

La norma ISO/IEC 27011 ofrece un manual de interpretación de la implementación y gestión de la seguridad de la información en organizaciones de telecomunicaciones basada en ISO/IEC 27002:2005 (Bernal Medina, 2022). Permite establecer políticas, procedimientos y controles para minimizar los riesgos de las organizaciones de telecomunicaciones. Se ha visto la necesidad de implementar esta norma para gestionar adecuadamente los activos de la empresa y continuar con el éxito de las actividades (Avilés Armijos & Uyaguari Guartatanga, 2012).

La norma ISO/IEC 27033 está dedicado a la seguridad de la red (Bernal Medina, 2022). Ofrece una guía completa para el desarrollo de la seguridad en las redes y los servicios de la red. Se ocupa de la

planificación e implementación de la seguridad mediante sus directrices y medidas (Ochoa Palomino, 2019).

La norma ISO/IEC 27034 se dedica a la seguridad de las aplicaciones informáticas (Bernal Medina, 2022). Proporciona consideraciones para el desarrollo seguro de software, así como factores que pueden afectar a la seguridad general de las aplicaciones (Karakaneva, 2014). Garantiza que los softwares aseguren sus niveles de seguridad para el apoyo a los SGSI.

1.3 COBIT

Los Objetivos de Control de la Información y Tecnologías Afines (COBIT, por sus siglas en inglés) es un marco integral diseñado para que las organizaciones puedan alcanzar sus objetivos estratégicos a través de una gobernanza y gestión efectivas de las TIC a nivel empresarial. COBIT 2019 en su última versión se enfatiza en la alineación de los objetivos comerciales de TI y ofrece un enfoque holístico para el gobierno de TI. Contiene diversos aspectos como la gestión de riesgos, el cumplimiento y la medición del desempeño (Ahmet, 2023).

En cuanto a gestión y gobernanza de riesgos, este marco proporciona un enfoque estructurado que permite identificar, evaluar y mitigar sistemáticamente los riesgos de TI. Ofrece una serie de objetivos de control genéricos y una lista completa de procesos de TI, que pueden ser adaptadas a las necesidades específicas y al panorama de riesgos de una organización *(COBIT | Control Objectives for Information Technologies*, 2023).

El enfoque del marco para el gobierno de riesgos se centra en la importancia de incorporar la gestión de riesgos en la estructura general de gobierno de TI. Los directivos y los profesionales de TI participan en el proceso de gestión de riesgos para garantizar una toma de decisiones y una rendición de cuentas exitosa. El marco también alienta a las organizaciones a adoptar una estrategia de gestión de riesgos (Ahmet, 2023).

COBIT se divide en tres componentes: marco, principios y objetivos de gobernanza y gestión, dedicados a ofrecer un modelo integral que satisfaga a las partes interesadas y vinculado a los objetivos específicos de la organización. Por otra parte, en lo que a gestión

de riesgos se refiere COBIT (Risk IT) incluye tres grandes procesos: evaluar, dirigir y monitorear (EDM, por sus siglas en inglés); alinear, planificar y organizar (APO, por sus siglas en inglés) y monitorear, evaluar y valorar (MEA, por sus siglas en inglés) que ayudan a las organizaciones a gestionar los riesgos (Ahmet, 2023).

2. Comparación entre los marcos de referencia NIST RMF, COBIT (Risk IT) e ISO/IEC 27005

Cada uno de estos marcos ofrece una metodología única medir el impacto de los riesgos. NIST RMF se centra en los sistemas de TI y la gestión de riesgos de ciberseguridad (Force, 2018). COBIT en cuanto a este aspecto aborda específicamente la gestión de riesgos relacionados con TI dentro del contexto de la gobernanza y la gestión de TI (Ahmet, 2023) y dentro de la serie de ISO/IEC 27000, la ISO/IEC 27005 específicamente trata la conceptualización general de la gestión de riesgo de la seguridad de la información (Torres Hallo, 2020).

En cuanto al alcance y cobertura dentro del contexto de gestión de riesgos organizacionales NIST RMF gestiona los riesgos en los sistemas de información federales y aunque está diseñado específicamente para este sector ofrece la posibilidad de ser utilizados en otros sectores para la gestión de riesgos de seguridad de la información (Force, 2018). La extensión de COBIT (Risk IT) proporciona un enfoque estructurado para gestionar los riesgos de TI, teniendo en cuenta las perspectivas y aseguramiento del negocio con TI. Está diseñado solo para abordar los riesgos de las TI, lo que lo hace muy necesario para organizaciones que dependen de la tecnología de la información (Ahmet, 2023). La ISO/IEC 27005 se puede aplicar a todo tipo de organizaciones que pretenden gestionar los riesgos que puede sufrir la seguridad de la información (Norma técnica colombiana NTC-ISO 27005, 2009).

Estos marcos ofrecen pasos y etapas de procesos únicos, para tratar con la gestión de riesgos. NIST RMF está diseñado para gestionar los riesgos de seguridad de la información (Force, 2018). COBIT (Risk IT) se dirige específicamente a la gobernanza y gestión de los riesgos de TI (Ahmet, 2023). ISO/IEC 27005 establece un alineamiento entre los cuatro procesos de un SGSI y sus propios procesos de ISRM (Norma técnica colombiana NTC-ISO 27005, 2009).

En cuanto a terminología y conceptos NIST RMF se centra en los sistemas de información y la ciberseguridad (Force, 2018), COBIT (Risk IT) aborda específicamente los riesgos de TI (Ahmet, 2023). La norma ISO/IEC 27005 aplica los términos y definiciones de las normas ISO/IEC 27001 e ISO/IEC 27002 (Norma técnica colombiana NTC-ISO 27005, 2009).

Los principios y prácticas clave tratados por NIST RMF ofrecen un proceso estructurado para gestionar los riesgos de seguridad de la información y ciberseguridad (Force, 2018), mientras que COBIT (Risk IT) es particularmente adecuado para gestionar riesgos relacionados con TI en entornos complejos (Ahmet, 2023). La norma ISO/IEC 27005 fue concebida para la gestión del riesgo en la seguridad de la información estableciendo el contexto, evaluando y tratando los riesgos a través de un plan de tratamiento para implementar las recomendaciones y decisiones con el fin de reducir el riesgo hasta un nivel aceptable (Norma técnica colombiana NTC-ISO 27005, 2009).

En cuanto a la integración con otros marcos NIST RMF adecuado para la integración con otros marcos de ciberseguridad, como el NIST Cybersecurity Framework (CSF) y la serie ISO/IEC 27000, además promueve la interoperabilidad con diversos sistemas de gestión (Force, 2018). Mientras que el componente de riesgo de TI de COBIT se puede integrar con otros marcos de gestión, como ITIL, PMBOK e ISO/IEC 27001 (Ahmet, 2023). La norma ISO/IEC 27005 está se integra perfectamente con ISO/IEC 27001, 27002, 31000 y con la serie de NIST (Norma técnica colombiana NTC-ISO 27005, 2009).

3. Problemas y restricciones

3.1 NIST RMF

Una de las principales restricciones de NIST RMF es la falta de conocimiento y comprensión de los principios y componentes del marco. Este es un modelo complejo que requiere de mucha comprensión e implica recursos sustanciales lo que puede ser un conflicto para las organizaciones. La adopción de un marco requiere de educación y capacitación para una implementación exitosa, por lo que se debe invertir en la formación de los empleados para evitar

una aplicación inadecuada. Anteriormente se destacó la adaptabilidad de NIST RMF, sin embargo, la personalización se debe hacer con cuidado para evitar posibles impactos negativos en la eficacia del marco y debe estar alineada con sus principios y objetivos. Para garantizar el éxito de la aplicación de NIST RMF es fundamental monitorear los procesos de gestión de riesgos para identificar posibles brechas o debilidades en los procesos de gestión de riesgos (Ahmet, 2023), (Force, 2018).

3.2 COBIT

Las limitaciones de COBIT se centran en la falta de comprensión y conciencia sobre el gobierno de TI, varias organizaciones carecen de los conocimientos por lo que la adopción se puede convertir en un desafío. Es importante garantizar capacitación y educación sobre los componentes del marco y muchas organizaciones carecen de los recursos para formar adecuadamente a su personal. A la hora de adaptarlo y personalizarlo con otros marcos requiere de un amplio conocimiento y experiencia en gobierno de TI. Por último, COBIT requiere que las organizaciones monitoreen y revisen consistentemente sus procesos de gobierno de TI, sin embargo, carecen de los recursos y la experiencia necesarios para un sistema eficaz de seguimiento y evaluación (Ahmet, 2023).

3.3 ISO/IEC 27005

La norma tiene como limitantes que no proporciona específicamente una metodología concreta para analizar riesgos, sino que a través de sus procesos una recomendación para su análisis. Incluye en sus anexos carácter informativo, no normativo con orientaciones precisas para tratar con los riesgos distinguiéndose entre un análisis de alto nivel y análisis detallado. Según la propia norma no cuenta con una medición de riesgos, esta se trata indirectamente a través de la estimación de riesgo (Tipán Guayta, 2012).

Conclusiones

Los marcos de referencia para la gestión de riesgos juegan un papel fundamental en la identificación, evaluación y mitigación de los mismos para garantizar la gobernanza y correcto funcionamiento de la

organización. Los marcos NIST y COBIT manejan riesgos de sistemas de TI, pero con la diferencia de que NIST se enfoca hacia la gestión de ciberseguridad y COBIT hacia la gobernanza. Todos estos marcos, pese a la complejidad de su implementación, pueden ser adoptados por cualquier organización. Ofrecen procesos particulares sobre el manejo con los riesgos, pero en el caso de ISO/IEC 27005 no permite la medición, lo que supone una limitación a la hora de calcular el impacto de un incidente de seguridad. Adoptar cualquiera de estos marcos de referencia supone un compromiso entre los directivos y el personal, requiere de recursos y la capacitación adecuada para garantizar su comprensión y sus componentes. Las investigaciones posteriores podrían explorar los desafíos y limitaciones con más profundidad de estos y otros marcos, centrándose en contextos específicos, además, de la eficacia en la gestión de riesgos, el gobierno de TI y su impacto en el desempeño organizacional. Implementar uno de estos en las organizaciones cubanas constituye un reto debido a bajo uso de este tipo de modelos y sobre todo a la falta de alineamiento entre los objetivos y las TI, pero a partir de este estudio se tiene como referencia algunos marcos que sirven de guía para comenzar a construir un modelo de evaluación de impacto de ciberseguridad.

Referencias

Ahmet, E. F. E. (2023). A comparison of key risk management frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT. Denetim ve Güvence Hizmetleri Dergisi, 3(2), 185-205.

Avilés Armijos, J. M., & Uyaguari Guartatanga, M. E. (2012). Diseño de una política de seguridad para la empresa de Telecomunicaciones PUNTONET en la ciudad de Cuenca, en base a las normas de seguridad ISO 27001 y 27011 como líneas base para las buenas prácticas de tratamiento y seguridad de la información.

Bernal Medina, H. C. (2022). Análisis de vulnerabilidad en dispositivos móviles con sistema operativo Android.

Casanova, M. P., & Calderón, C. A. (2020). Modelo para la gestión de infraestructuras de tecnologías de la información. Tecno-Lógicas, 23(48), 32-54. http://www.scielo.org.co/scielo.php?pid=S0123-77992020000200032&script=sci_arttext

COBIT | Control Objectives for Information Technologies. (2023). ISACA. https://www.isaca.org/resources/cobit

Computer Security Division, I. T. L. (2016a, noviembre 30). About the RMF - NIST Risk Management Framework | CSRC | CSRC. CSRC | NIST. https://csrc.nist.gov/Projects/risk-management/about-rmf

Computer Security Division, I. T. L. (2016b, noviembre 30). NIST Risk Management Framework | CSRC | CSRC. CSRC | NIST. https://csrc.nist.gov/Projects/risk-management

Force, J. T. (2018). Risk management framework for information systems and organizations. NIST Special Publication, 800, 37.

Karakaneva, J. (2014). Software applications security. Trakia Journal of Sciences, 12(4), 419.

Liendo Afonso, L. C. (2023). Optimización del proceso de reporting del análisis de impacto en el negocio en una consultora de ciberseguridad. http://titula.universidadeuropea.com/handle/20.500.12880/5414

Mahn, A., Topper, D., Quinn, S., & Marron, J. (2021). Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide (NIST Special Publication (SP) 1271). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1271

Martínez Landrove, N. (2019). Ciberseguridad y riesgo operacional en las organizaciones. https://repositorio.comillas.edu/xmlui/handle/11531/42317

Meriah, I., & Rabai, L. B. A. (2019). Comparative Study of Ontologies Based ISO 27000 Series Security Standards. Procedia Computer Science, 160, 85-92. https://doi.org/10.1016/j.procs.2019.09.447

NORMA TÉCNICA COLOMBIANA NTC-ISO 27005. (2009). dokumen.tips. https://dokumen.tips/documents/iso-27005-espanol.html

Ochoa Palomino, A. (2019). Diseño de una Red de Seguridad Informática para la Protección del Sistema Web de un Call Center ante Ataques Informáticos Aplicando la Norma ISO 27033. Universidad Peruana de Ciencias Aplicadas (UPC). https://doi.org/10.19083/tesis/625726

Ortega Candel, J. M. (2021). Ciberseguridad. Manual práctico. Ediciones Paraninfo, S.A.

Pérez Lorences, P. (2014). Procedimiento para mejorar la gestión de tecnologías de la información en el sector empresarial cubano. [Doctordo]. Universidad Central “Marta Abreu” de Las Villas.

Quinn, S., Ivy, N., Chua, J., Barrett, M., Feldman, L., Topper, D., Witte, G., & Gardner, R. K. (2022). Using business impact analysis to inform risk prioritization and response (NIST IR 8286D; p. NIST IR 8286D). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8286D

Tipán Guayta, K. I. (2012). Propuesta de políticas de seguridad de la información para la CORPAIRE. Quito, 2012.

Torres Hallo, M. (2020). MODELO DE GESTIÓN DE RIESGOS DE PROCESOS DE TECNOLOGÍA DE INFORMACIÓN BAJO LA NORMA ISO/IEC 27000 EN EMPRESAS AÉREAS DEL ECUADOR.