Polo del Conocimiento

Pol. Con. (Edición núm. 68) Vol. 7, No 3
Marzo 2022, pp. 706-723
ISSN: 2550 - 682X
DOI: 10.23857/pc.v7i3.3758

Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019

Cybersecurity Oriented IT Governance Framework for the Banking Sector under COBIT 2019

Estrutura de governança de TI orientada para a segurança cibernética para o setor bancário no COBIT 2019

Ximena Elizabeth Orellana-Cabrera [I]
xeorellanac55@est.ucacue.edu.ec
https://orcid.org/0000-0003-3699-3406

Maria Daniela Álvarez-Galarza [II]
maria.alvarez@ucacue.edu.ec
https://orcid.org/0000-0001-6702-7783

Correspondencia: xeorellanac55@est.ucacue.edu.ec

Ciencias Técnicas y Aplicadas
Artículo de Investigación

***Recibido:** 30 de enero de 2022 ***Aceptado:** 18 de febrero de 2022 * **Publicado:** 10 marzo de 2022

I. Ingeniera de Sistemas, Universidad Católica de Cuenca, Ecuador.
II. Magister en Seguridad Informática Aplicada , Master Universitario en Derecho de la Ciberseguridad y Entorno Digital , Ingeniero de Sistemas , Universidad Católica de Cuenca, Ecuador.

Resumen

En la actualidad, la seguridad de la información es un tema crucial para el sector bancario debido a que la gestión de la información es parte fundamente del Gobierno Corporativo y requiere un nivel adecuado de protección de sus activos de información. Razón por la que se hace necesario utilizar un modelo de seguridad apropiado el cual cumpla con las necesidades de las entidades financieras y que le permita conocer el nivel de madurez de ciberseguridad. Este estudio tiene como objetivo analizar los estándares como la NIST Cybersecurity Framework y COBIT 2019 Framework para determinar un marco de trabajo de gobierno de tecnología de información orientado a la ciberseguridad. Además, se describen los pasos para poder llevar a cabo la implementación de este y así permita preparar a las entidades financieras a la creación de valor. En conclusión, la implementación permitirá evaluar el nivel de madurez de ciberseguridad como parte de la mejora continua y ciclo de vida de gobierno de TI.

Palabras clave: Ciberseguridad; COBIT; Gobierno TI; NIST; Sector bancario.

Abstract

Currently, information security is a crucial issue in the banking sector due to the fact that information management is a fundamental part of corporate governance which requires an adequate level of protection of its information assets. For this reason, it's necessary to use an appropriate security model that meets the needs of financial institutions and allows them to know the level of cybersecurity maturity. This study aims to analyze standards such as the NIST Cybersecurity Framework and COBIT 2019 Framework to determine an information technology governance framework oriented to cybersecurity. In addition, the steps to be able to carry out the implementation of the same and thus prepare financial institutions to value creation are described. In conclusion, the implementation will allow evaluating the level of cybersecurity maturity as part of the continuous improvement and IT governance lifecycle.

Keywords: Cybersecurity; COBIT; IT Government; NIST; Banking Sector.

Resumo

Atualmente, a segurança da informação é uma questão crucial para o setor bancário, pois a gestão da informação é parte fundamental da Governança Corporativa e requer um nível adequado de proteção de seus ativos informacionais. Razão pela qual é necessário utilizar um modelo de

segurança adequado que vá ao encontro das necessidades das entidades financeiras e que lhes permita conhecer o nível de maturidade da cibersegurança. Este estudo tem como objetivo analisar padrões como o NIST Cybersecurity Framework e o COBIT 2019 Framework para determinar uma estrutura de governança de tecnologia da informação orientada para a segurança cibernética. Além disso, são descritos os passos para poder realizar a implementação desta e assim permitir preparar as entidades financeiras para a criação de valor. Em conclusão, a implementação permitirá avaliar o nível de maturidade da cibersegurança como parte do ciclo de vida de melhoria contínua e governança de TI.

Palavras-chave: Cibersegurança; COBIT; Governança de TI; NIST; Indústria bancária.

Introducción

Las empresas a nivel mundial y nacional determinan objetivos estratégicos según su modelo de negocio y proyectan la transformación estratégica en búsqueda de consolidar y fortalecer su posición competitiva. Sin embargo, no se consigue estrechar la relación entre las áreas directivas, funcionales, tecnología de la información y seguridad de la información. Por lo que, algunos reguladores claves de todo el mundo están comenzando a reconocer el gobierno de tecnología de la información como un elemento fundamental para responder a este requerimiento [1].

El Gobierno de TI tiene como objetivo garantizar que tecnología de la información contribuya con estrategias, enfoques y valores de la organización. Además, de la rendición de cuentas de la alta dirección y junta directiva, teniendo exactamente el mismo peso de compromiso como Gobierno Corporativo y Empresarial [2]. Por otro lado, la ciberseguridad en los últimos años ha tomado auge y los bancos comprenden su importancia, debido al aumento de la dependencia entorno a los medios cibernéticos.

Los bancos están constantemente obligados a actualizar y mejorar sus sistemas, y algunos de ellos no tienen los recursos para tal asignación presupuestaria. Además, al no mantenerse al día con las demandas tecnológicas de la industria y la implementación de la ciberseguridad se corre el riesgo de atentar contra la confidencialidad, disponibilidad e integridad de los datos generados y administrados. ESET Security Report 2021, detalla que el 60% de las organizaciones en América Latina tienen como su principal precaución el robo de información y el ransomware ataques dirigidos a grandes y pequeñas empresas [3].

Existen un sinnúmero de marcos de seguridad de la información en el mercado para ser implementados, pero no hay mucha claridad sobre qué marco aplicar en el sector bancario. Pese a que los bancos están fuertemente regulados por entes de cumplimiento, como la Superintendencia de Bancos, Ley de protección, de datos, etc., debido a la sensibilidad, criticidad y el impacto de su infraestructura.

Sintetizando los conceptos anteriormente descritos, se observa una problemática para todas las áreas productivas a nivel mundial, sin ser ajena al sector bancario. Por tanto, se tiene como objetivo realizar un marco de trabajo de tecnología de la información orientado a la ciberseguridad bajo la óptica de COBIT 2019. Para el desarrollo de esta investigación se utilizará un análisis analítico-descriptivo a través de técnicas de indagación y análisis.

En el presente artículo se tienen las siguientes secciones: en la sección 2 se presentan los conceptos relacionados son necesarios para la compresión al lector de los resultados, en la sección 3 se presentan trabajos relacionados con la ciberseguridad, el gobierno de TI y las normas aplicadas en el sector bancario, en la sección 4 se describe la metodología utilizada para la obtención de resultados, en la sección 5 se presentan los resultados de los pasos a seguir en el marco de gobierno TI; finalmente, en la sección 6 se presentan las conclusiones en base a los resultados que se han obtenido en este estudio.

Conceptos relacionados

COBIT 2019

Es un punto de referencia para la gobernanza y la gestión de la tecnología de la información, permite a las empresas diseñar, operar y mejorar un sistema de gobernanza adaptado a sus necesidades. Dentro del modelo básico de COBIT hay 40 objetivos de gobierno y gestión de los cuales 5 son para gobierno. Por lo cual ofrece opciones más flexibles para implementar medidas de madurez y capacidad para que los objetivos de TI puedan mantenerse al día con los objetivos comerciales basados en datos. El modelo del núcleo de COBIT cuenta con siete componentes detallados en la Figura 1 [4].

Figura 1 Componentes del Sistema de Gobierno - COBIT 2019
Fuente: ISACA (2018)

Para ayudar a las organizaciones a satisfacer las necesidades de las partes interesadas COBIT 2019 utiliza la cascada de objetivos. Dicha cascada fluye desde las necesidades de las partes interesadas y las metas corporativas; la priorización de dichas metas recae en las metas de alineación y estas a su vez en los objetivos de Gobierno y Gestión detallados en la Figura 2. La cascada de metas permite priorizar los objetivos con base a las metas institucionales [4].

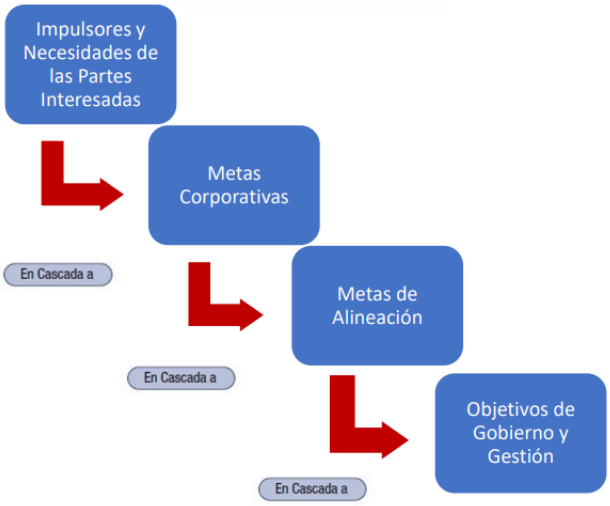

Figura 2 Cascada de Metas - COBIT 2019
Fuente: ISACA 2018.

En la guía de implementación de COBIT 2019 se reconoce que no es buena práctica separar la línea del negocio y actividades relacionadas con las tecnologías de la información. Es por ello, que la gobernanza empresarial, cubre todas las áreas de responsabilidad empresarial y funcional de TI de un extremo a otro. Para ello comprende las siguientes fases:

¿Cuáles son los motivos?

¿Dónde estamos ahora?

¿Dónde queremos estar?

¿Qué debemos hacer?

¿Cómo llegamos allí?

¿Llegamos allí?

¿Cómo mantenemos el impulso?

El enfoque de implementación de COBIT se resume en la Figura 3 [4].

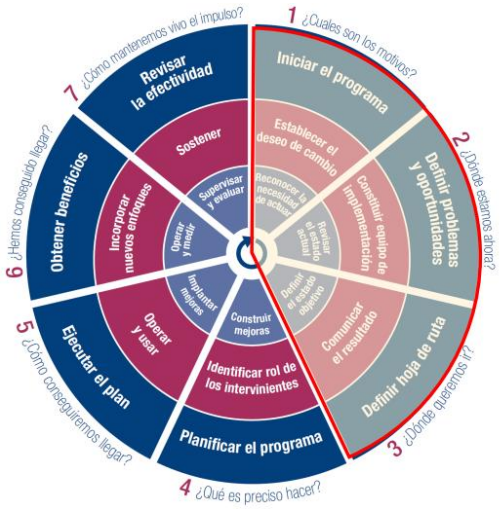

Figura 3 Ciclo de vida de la implementación COBIT 2019
Fuente: ISACA (2018)

NIST CSF

El marco se considera ampliamente como el estándar de oro para crear un programa de ciberseguridad. Ya sea que esté comenzando a establecer un programa de ciberseguridad o ya esté ejecutando un programa bastante maduro, el marco puede proporcionar valor, actuando como una herramienta de gestión de seguridad de alto nivel que ayuda a evaluar el riesgo de ciberseguridad

en toda la organización, debido a que proporciona un conjunto uniforme de reglas, pautas y estándares [5].

NIST CSF comprende tres aspectos importantes: componentes centrales del marco, niveles de implementación y perfiles, los cuales se detallan a continuación:

1. Niveles de implementación: se lo define como el grado en que su organización ha implementado los controles NIST:
    - Nivel 1: parcial
    - Nivel 2: riesgo informado
    - Nivel 3: repetible
    - Nivel 4: adaptable
2. Núcleo del marco: comprende los estándares, pautas y prácticas de la industria de una manera que permite la comunicación de las actividades y los resultados de ciberseguridad:
    - Funciones: identificar, proteger, detectar, responder, recuperar
    - Categorías
    - Subcategorías
    - Referencias informativas
3. Perfiles del marco: es la alineación única de su organización de sus requisitos y objetivos de seguridad, el apetito por el riesgo y los recursos, medidos contra los resultados deseados citados en el núcleo del marco.

Por otro lado, el núcleo del marco describe cinco funciones previas a la gestión de riesgos y la seguridad de la información, a saber, identificar, proteger, detectar, responder y recuperar las cuales se detallan en la Figura 4 [6].

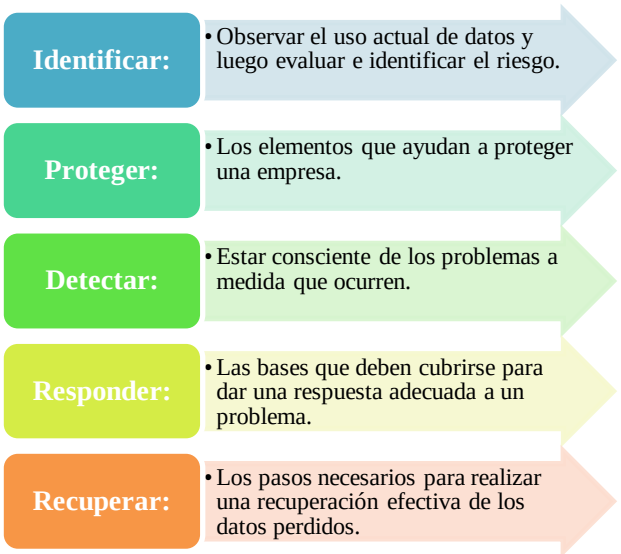

Figura 4 Funciones principales del marco de ciberseguridad del NIST
Fuente: Autoría Propia

Cada una de estas funciones incluye actividades de nivel inferior para mitigar el riesgo cibernético. Estos se dividen en 23 categorías, que a su vez incluyen 108 subcategorías que enumeran los requisitos y controles que se deben cumplir [6].

Para implementar o mejorar el programa de ciberseguridad, NIST propone los pasos detallados en la Figura 5. El Marco puede adaptarse a un entorno cambiante a medida que el panorama de la ciberseguridad continúa evolucionando.

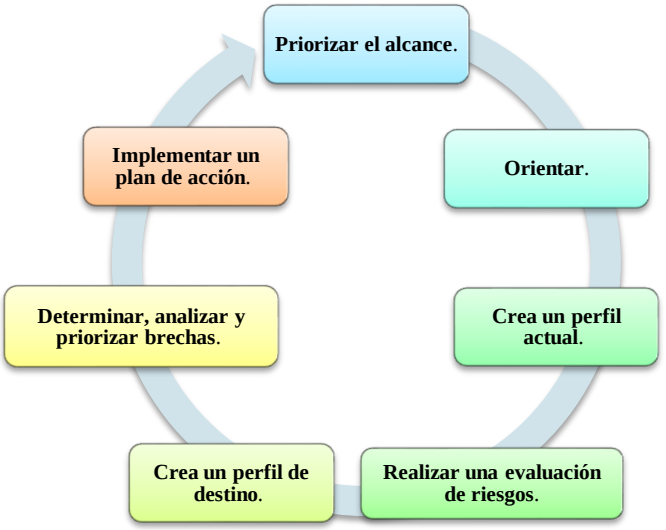

Figura 5 Fases para implementar las NIST.
Fuente: Autoría propia

Trabajos relacionados

A medida que avanzan los esfuerzos de transformación digital corporativa, activos como los datos de los clientes, los procesos comerciales y la propiedad intelectual se han convertido en activos cibernéticos que son vitales para el valor global de una empresa [7]. El departamento de TI o los CISO cumplen roles de misión crítica, la ciberseguridad ya no puede ser vista como el único dominio de estas funciones [8]. Esto se aplica a empresas de todos los sectores, permitiendo comprender la importancia de la ciberseguridad, a cómo gestionarla, así como también se convertirá en un tema de gobernanza definitorio para el futuro previsible [1].

Jerome Powell, presidente de EE. UU. La Reserva Federal (FedL), recientemente calificó al riesgo cibernético como un foco importante en términos de grandes riesgos. Dijo que la Reserva Federal no solo asigna una gran cantidad de tiempo a recursos para protegerla FedL, sino también para proteger las instituciones y los mercados financieros [9]. La ciberseguridad debe verse como un indicador de la competencia de gestión al igual que las prácticas de contabilidad y auditoría.

La ciberseguridad figura constantemente entre los directores y la alta gerencia como el riesgo de la empresa sobre el que menos saben [10]. Simplemente categorizar el ciberdelito como riesgo macroeconómico es insuficiente si las empresas aún lo gestionan como un micro riesgo económico que cae bajo alguna competencia combinada del departamento de TI, asesoría legal, auditores o consultores de estrategia. En otras áreas de negocio donde un problema se define como riesgo macro, las empresas dedicarán recursos permanentes a la mitigación del riesgo. De hecho, en algunos casos, habrá departamentos o sucursales, específicos dedicado a prevenir estos incidentes.

A pesar de la elevación de la ciberseguridad como un tema prioritario, las empresas, aún no se han equipado con este tipo de toma de decisiones o aplicación de políticas de reducción de riesgos en la infraestructura. La persona a cargo, a menudo, es un director de TI o, en una empresa más grande el CISO, pero estos puestos por sí solos están mal equipados para asumir un riesgo que podría dañar gravemente, o incluso arruinar, una marca sin el enfoque estratégico adecuado [11].

La ciberseguridad ha ganado visibilidad, con una serie de incidentes de seguridad ampliamente publicitados, ataques de piratería y violaciones de datos que llegan a las noticias en los últimos años. La escalada en el número de incidentes cibernéticos no muestra signos de disminuir, y parece apropiado analizar la manera en que se conceptualiza la ciberseguridad y considerar si existe la necesidad de un cambio de mentalidad. Para ello, aplicamos un enfoque de "problematización" con

el propósito de evaluar las concepciones actuales del problema de ciberseguridad por parte del gobierno, la industria y los piratas informáticos [12].

La gobernanza de la ciberseguridad tiene como objetivo desarrollar, implementar y administrar un programa de seguridad en una organización para mantener mitigados los riesgos. Los bancos están regulados por la Superintendencia de Bancos y por el Banco Central del Ecuador, pese a ello en los últimos tiempos el sector bancario ha sufrido ataques como el suscitado al Banco del Pichincha, donde la entidad emitió un comunicado el 18 de febrero de 2021, donde especificó que "…fue un acceso no autorizado al sistemas sin pérdida de datos…"; por otro lado, en el 2013 también se evidenció un desvío de fondos desde el Banco Central del Ecuador y pese a que se llevó a cabo una auditora, no se determinó el o los autores de este incidente de seguridad de la información [13].

Como se mencionaba anteriormente los incidentes cibernéticos aumentan de manera exponencial en la medida en que las empresas no tomen la decisión o iniciativa de poder proteger sus sistemas e infraestructuras, estas estarán vulnerables ante un ciberdelito, lo que se traduce en pérdidas y retrasos para toda la organización, en estos tiempos es más costoso pagar por tratar de remediar un ataque cibernético que blindar a la empresa con la inversión en una infraestructura adecuada. Por lo que, el análisis de riesgos es una actividad importante que las organizaciones deben realizar, para evitar los ataques y / o consecuencias negativas que puedan surgir de ellos. De hecho, muchos investigadores ya han propuesto modelos de ciberseguridad destinados a ayudar a las organizaciones a contrarrestar los ataques cibernéticos [14].

Dado el entorno cambiante, tanto las empresas de servicios financieros como sus supervisores están haciendo de la ciberseguridad una alta prioridad. De hecho, el sector bancario es una de las industrias que más ha sumado sus esfuerzos por combatir las amenazas a la seguridad cibernética, es por ello por lo que han reforzado sus defensas y están detectando infracciones de manera más oportuna, debido a su implementación de buenas prácticas de seguridad. El informe de la Organización de los Estados Americanos (OEA) (2018) identifica las normas que las entidades bancarias han adoptado en temas de seguridad de la información. Tabla 1 [15].

Tabla 1 Porcentaje del total de entidades bancarias adoptado por norma

Normas	%
Security Management System (ISMS)	68%
ISO27001	68%
COBIT	50%
ITIL	43%
IT Service Management (ITSM)	43%
PCI-DSS	42%

Fuente: OEA (2018)

Metodología

La metodología de investigación llevada a cabo para este trabajo fue cualitativa, método basado en datos secundarios. Al recolectar la información, se adoptó una técnica de revisión del alcance basada en fuentes relevantes como ScienceDirect, Scopus, ACM y Saltador. Las palabras claves utilizadas para el proceso de búsqueda van desde gobernanza de TI, seguridad de TI, marcos, y ciberseguridad, seleccionando los artículos más relevantes y apropiados.

Una vez recopilada información relacionada al Gobierno de TI, así como los marcos de seguridad de TI disponibles, se cotejan COBIT 2019 y NIST. Así que, tras un previo análisis, se ha considerado sincronizar las prácticas de COBIT 2019 con las categorías de NIST, esto ha permitido que, los modelos puedan ser ajustados con el propósito de proponer, un marco de trabajo de gobierno de TI para el sector bancario orientado a la ciberseguridad. A continuación, se aprecia en la Figura 6 las fases de la implementación.

Figura 6 Alineación en la implementación del NIST CSF y COBIT 2019
Fuente: Autoría Propia

Resultados

La aplicación en el sector bancario de las NIST usando COBIT, es posible gracias al alineamiento entre las fases de la implementación de los dos marcos de referencia. La adopción de estos framework se puede realizar gradualmente, a través de la alineación de las NIST y COBIT 2019, como resultado de ello se obtiene un enfoque lógico, para la implementación de la ciberseguridad en el gobierno de TI, a continuación, se detallan cada una de las fases:

Fase 1: ¿Cuáles son los motivos? / Priorizar el alcance.

Para implantar la ciberseguridad el primer paso tiene como objetivo conocer a la entidad financiera, es decir comprender su misión, visión, las partes interesadas, detallar cuáles son sus objetivos, sus estrategias y sus procesos, para ello se necesita una serie de tareas clasificadas en tres grupos: actividades de mejora continua, actividades de habilitación del cambio, actividades de gestión del programa, como se puede visualizar en la siguiente Figura 7.

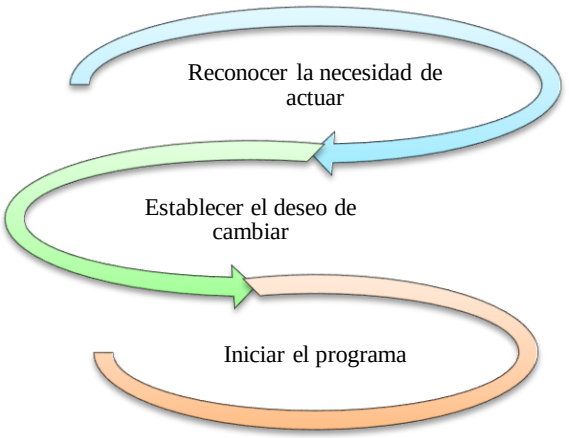

Figura 7 Tareas clave fase 1 determinar el alcance.
Fuente: Autoría Propia

La herramienta utilizada para cumplir con las tareas claves es la cascada de meta de COBIT ver Figura 2. La cual permite identificar las necesidades de las partes interesadas, las metas empresariales, las metas de alineamiento y a su vez determinar los objetivos del gobierno y gestión.

Fase 2: ¿Dónde estamos ahora? / Orientar y Crea un perfil actual.

Esta fase tiene como objetivo, identificar los procesos, procedimientos y activos relacionados, los requisitos reglamentarios y los riesgos a través de la identificación de las amenazas y vulnerabilidades. Es así como, para crear un perfil, el objetivo es identificar los requerimientos para definir el estado actual del programa de ciberseguridad de la entidad financiera, el cual se logra aplicando las siguientes tareas claves detalladas en la Figura 8.

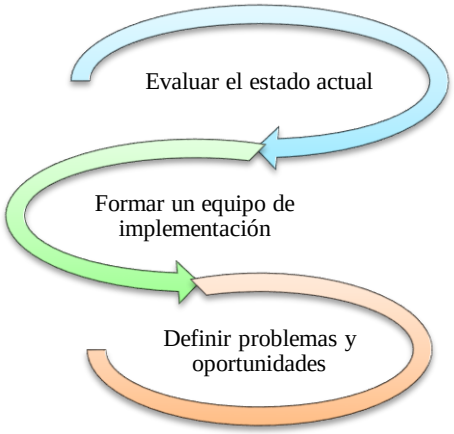

Figura 8 Tareas clave fase 2 evaluar el estado actual
Fuente: Autoría Propia

Se aplica la práctica de COBIT 2019 asociadas a las subcategorías del marco utilizando un esquema de calificación de gestión de desempeño de los componentes. Una vez seleccionadas las categorías y subcategorías, se debe relacionar las mismas a las prácticas de COBIT y evaluar el nivel de implementación. Cada una de ellas va, desde el Nivel 1 al Nivel 4. Ver detalle en la Figura 9.

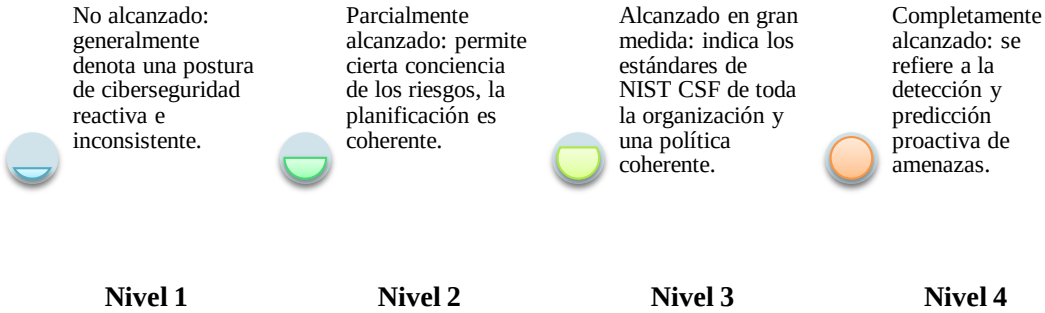

Figura 9 Escala de calificación de logros
Fuente: ISACA, 2018

Una vez que se hayan calificado todas las áreas, el resultado de esta etapa permitirá conocer el estado actual de los procesos en función de la selección de categorías y subcategorías relacionadas a las prácticas de COBIT 2019 identificando y evaluando el nivel de implementación las mismas. Y finalmente se realiza un análisis de riesgos utilizando metodologías como la ISO 27005 o Magerit. Las cuales permitirán mostrar los riesgos de seguridad, las vulnerabilidades y amenazas a la cual está expuesta la organización.

Fase 3: ¿Dónde queremos estar? / Ejecutar una evaluación de riesgos y Crea un perfil de destino.

El paso: "Realizar una evaluación de riesgos", tiene como objetivo identificar los riegos a los que está expuesta la entidad financiera, determinando la probabilidad de ocurrencia de un evento de ciberseguridad. Para "Crear un perfil destino" ser requiere explicar con detalle las categorías y subcategorías y así obtener el riesgo organizacional. En esta fase las tareas claves son las detalladas en la Figura 10.

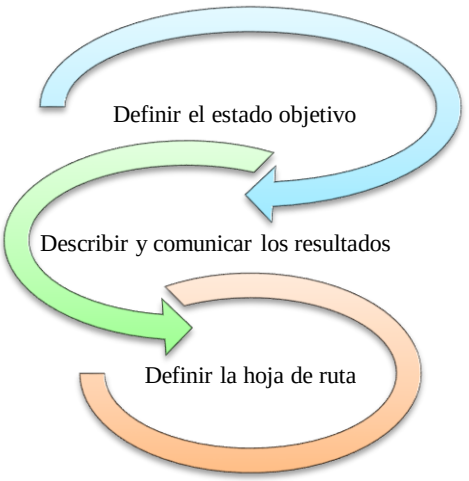

Figura 10 Tareas clave fase 3 creación del perfil deseado
Fuente: Autoría Propia

Una vez seleccionadas las categorías y subcategorías acorde a la entidad financiera, se evalúa el nivel de implementación de esas prácticas bajo la escala de COBIT antes mencionada, ver Figura 9. El perfil objetivo debe contar con los siguientes apartados: la función, la categoría, la subcategoría, los procesos relevantes de COBIT, el estado de la implementación, las prácticas,

políticas o procedimientos organizacionales, cometarios, acciones recomendadas y los recursos necesarios.

Fase 4: ¿Qué debemos hacer? / Determinar, analizar y priorizar brechas.

Esta fase tiene como objetivo, realizar un análisis de brechas entre el perfil actual y el perfil objetivo. Las tareas claves que se deben cumplir son las detalladas en la Figura 11.

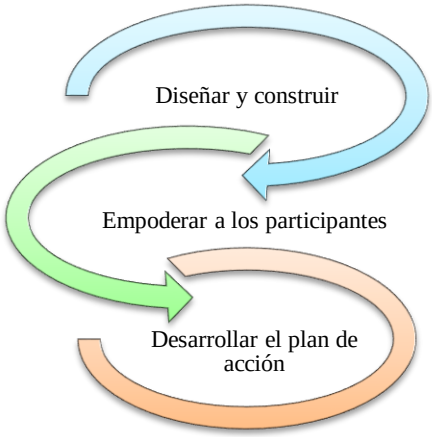

Figura 11 Tareas clave fase 4 análisis de brechas
Fuente: Autoría Propia

Como resultado de esta fase los planes de acción nacen del análisis de las brechas encontradas en el perfil actual con el perfil objetivo. Dichos planes deben tener como mínimo un identificador, la prioridad, limitaciones, acciones específicas, recursos necesarios, hitos, requisitos previos, asignación de acciones y los roles.

Fase 5: ¿Cómo llegamos allí? / Implementar un plan de acción.

Con una imagen clara del estado actual de sus defensas, un conjunto de objetivos, un análisis integral de brechas y un conjunto de acciones de remediación. En esta fase las tareas claves son las detalladas en la Figura 12.

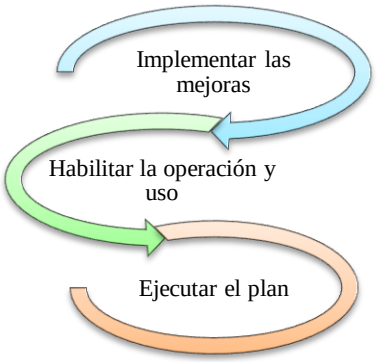

Figura 12 Tareas clave fase 5 implementar planes de acción
Fuente: Autoría Propia

El marco debe ser revisado continuamente para monitorear su desempeño y sus objetivos para asegurarse de que cumplen con el panorama cambiante del sector de la ciberseguridad.

Conclusiones

Se concluye que, la implementación de las NIST CSF utilizando los principios y procesos de COBIT 2019 proporciona una armonización de procesos y comunicaciones tanto internas como externas con las partes interesadas (Tecnologías de la Información, Seguridad de la Información, directivos) logrando un enfoque holístico para que el gobierno de TI implemente buenas prácticas de seguridad para aquellos procesos que administran dentro de una organización o empresa.

La ciberseguridad es de gran importancia en el sector bancario y se vuelve más necesaria su adecuada gestión e implementación, dado que, el punto clave del negocio de este de sector radica en fomentar la confianza y la credibilidad en sus clientes. Por tanto, a medida que aumentan los ciberataques, los reguladores, se encuentran desarrollando soluciones enfocadas a normativas y leyes que regulen y dispongan la aplicación de las buenas prácticas de seguridad de la información.

Para la adquisición, implementación y operación de una adecuada Arquitectura de Ciberseguridad, es necesario ejecutar periódicamente evaluaciones de riesgos de seguridad, con el propósito de adquirir tecnología adecuada que permita proteger los activos de información del negocio dentro de una empresa, así como también optimizar recursos tanto humanos como económicos y operar la tecnología relacionada a ciberseguridad de manera eficiente y eficaz.

Finalmente, el marco propuesto ayuda a determinar planes de acción que permitan determinar e implementar soluciones de ciberseguridad como: DLP, FIREWALL, WAF, correlacionadores de

eventos, Anti-Spam, Sandbox, etc. Que forman parte de la arquitectura de ciberseguridad dentro de una organización y la cual deben ser administradas por los Departamentos de Ciberseguridad dentro de una organización.

Referencias

[1] A. C. Calzada, «Albert Coronado Calzada,» 2020. [En línea]. Available: https://n9.cl/gljtp. [Último acceso: 2021].

[2] F. J. García Peñalvo, «Gobierno de Tecnologías de la Información," en Proyecto Docente e Investigador.,» Departamento de Informática y Automática, pp. 389-449, 2018.

[3] ESET, «Malware: la principal preocupación de las empresas de América Latina,» ESET Security Report 2021, 2021. [En línea]. Available: https://n9.cl/4ms5p. [Último acceso: 2021].

[4] ISACA, «COBIT 2019 Introduction and Methodology,» Illiniois, 2018. [En línea]. Available: https://n9.cl/mgf6t. [Último acceso: 2021].

[5] J. Hall, «A guide to the NIST Cyber Security Framework,» Textual Healing, 2020. [En línea]. Available: https://n9.cl/oci1n. [Último acceso: 2021].

[6] Reciprocity, «Complete Guide to NIST: Cybersecurity Framework, 800-53, 800-171,» RECIPROCITY, 2020. [En línea]. Available: https://n9.cl/3rhck. [Último acceso: 2021].

[7] O. Tomo, «El estudio anual de 2015 sobre el valor de mercado de los activos intangibles,» Intangible Asset Market, 2017.

[8] D. Camacho, «Contribuciones en Ciberseguridad y Cibercrimen,» AIDACyber, 2020.

[9] J. Powell, «The Cyber Risk to Our Financial Infrastructure: Reflections on 60 Minutes and Jerome Powell,» unboundsecurity, 2019. [En línea]. Available: https://n9.cl/1ypbg. [Último acceso: 2021].

[10] H. Sarrazin y P. Willmott, «Adapting your board to the digital age,» mckinsey, 2016. [En línea]. Available: https://n9.cl/h9yt4. [Último acceso: 2021].

[11] I. L. Muñoz Periñán y G. Ulloa Villegas, «Gobierno de TI – Estado del arte,» Sistemas & Telemática, vol. 9, pp. 23-53, 2017.

[12] R. Kalyanam y B. Yang, «Try-CybSI: una plataforma extensible de aprendizaje y demostración de ciberseguridad,» SIGITE '17: Actas de la 18a Conferencia Anual sobre Educación en Tecnología de la Información, pp. 41-46, 2017.

[13] M. Álvarez A. y D. Ladino H., «Análisis preliminar de la ciberseguridad asociada al sistema financiero en algunos países de Latinoamérica y la contribución de la informática forense,» Cuaderno de investigaciones: semilleros andina, vol. 1, nº 14, 2021.

[14] A. P. Henriques, M. Mendonça , T. Poleto, L. Camara y A. P. Cabral Seixas Costa, «Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory,» International Journal of Information Management, Agosto 2018.

[15] Organizacion de los Estados Americanos, «Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe,» Canada, 2018.