Revista Científica Mundo de la Investigación y el Conocimiento

DOI: 10.26820/recimundo/6.(4).octubre.2022.671-680
URL: https://recimundo.com/index.php/es/article/view/1898
EDITORIAL: Saberes del Conocimiento
REVISTA: RECIMUNDO
ISSN: 2588-073X
TIPO DE INVESTIGACIÓN: Artículo de investigación
CÓDIGO UNESCO: 1203.17 Informática
PAGINAS: 671-680

Procesos de gobierno basado en COBIT 2019 para mitigar ataques informáticos

Governance processes based on COBIT 2019 to mitigate computer attacks

Processos de governação baseados em COBIT 2019 para mitigar os ataques informáticos

Brayan Damián Tiglla Tumbaico[1]; Edgar Fernando Solís Acosta[2]

RECIBIDO: 02/11/2022 **ACEPTADO:** 26/11/2022 **PUBLICADO:** 30/11/2022

1. Ingeniero de Sistemas y Computación; Pontificia Universidad Católica del Ecuador; Ambato, Ecuador; bdtiglla@pucesa.edu.ec; bdtiglla@pucesa.edu.ec; https://orcid.org/0000-0002-0789-2297
2. Magíster en Evaluación y Auditoría de Sistemas Tecnológicos; Diploma Superior en Gestion para el Aprendizaje Universitario; Ingeniero de Sistemas y Computación; Universidad de las Fuerzas Armadas; Sangolquí, Ecuador; efsolis@espe.edu.ec; https://orcid.org/0000-0002-9009-4359

CORRESPONDENCIA

Brayan Damián Tiglla Tumbaico
bdtiglla@pucesa.edu.ec

Ambato, Ecuador

RESUMEN

La seguridad de la información es un tema fundamental para todas las áreas empresariales y de negocios, considerando que la gestión de la información es parte vital del Gobierno Corporativo, razón por la cual requiere un nivel adecuado de protección de la información como activo. COBIT 2019 plantea un modelo de seguridad apropiado que se adapta a las necesidades de las organizaciones y permita conocer el nivel de madurez de las mismas, con el fin de determinar un marco de trabajo de gobierno de tecnología de información orientado a la ciberseguridad. La presente revisión bibliográfica se ha desarrollado con el objetivo de analizar los procesos de gobierno que se desprenden de la normativa COBIT 2019 que evitan o minimizan los ataques informáticos dentro de la estructura de Gobierno de la Tecnología e Información (T&I) de las organizaciones.

Palabras clave: COBIT 2019; Ataques Informáticos; Procesos de Gobierno; Buenas Prácticas; Seguridad de la Información.

ABSTRACT

Information security is a fundamental issue for all business and business areas, considering that information management is a vital part of Corporate Governance, which is why it requires an adequate level of protection of information as an asset. COBIT 2019 proposes an appropriate security model that adapts to the needs of organizations and allows knowing their level of maturity, in order to determine an information technology governance framework oriented towards cybersecurity. This bibliographical review has been developed with the aim of analyzing the governance processes that emerge from the COBIT 2019 regulations that prevent or minimize computer attacks within the organizations' Technology and Information (T&I) Governance structure.

Keywords: COBIT 2019; Computer Attacks; Government Processes; Good Practices; Security of the Information.

RESUMO

A segurança da informação é uma questão fundamental para todas as áreas empresariais e de negócios, considerando que a gestão da informação é uma parte vital da Corporate Governance, razão pela qual requer um nível adequado de protecção da informação como um activo. COBIT 2019 propõe um modelo de segurança adequado que se adapta às necessidades das organizações e permite conhecer o seu nível de maturidade, a fim de determinar um quadro de governação das tecnologias de informação orientado para a ciber-segurança. Esta revisão bibliográfica foi desenvolvida com o objectivo de analisar os processos de governação que emergem dos regulamentos de COBIT 2019 que previnem ou minimizam os ataques informáticos dentro da estrutura de governação da Tecnologia e Informação (T&I) das organizações.

Palavras-chave: COBIT 2019; Ataques informáticos; Processos Governamentais; Boas Práticas; Segurança da Informação.

Introducción

COBIT 2019 permite a las empresas diseñar, operar y mejorar un sistema de gobierno adaptado a sus necesidades, basándose este diseño de sistema de gobierno esbelto, efectivo y eficiente en una serie de factores de diseño, construido a partir de los contenidos centrales de COBIT 2019, es decir, 40 objetivos de gobierno y gestión, procesos subyacentes y otros componentes de gobierno, así como un número abierto de áreas de enfoque específicas[1].

Además, COBIT 2019 se ha simplificado enormemente a nivel de marco, eliminando los modelos habilitadores, los cuales eran bastante abstractos, así como el nombre "habilitador". Sin embargo, COBIT 2019 sigue fundamentado en el concepto de que un buen sistema de gobierno requiere un conjunto de diferentes componentes de gobierno, tales como procesos, estructuras, habilidades, comportamientos, entre otros, cooperando entre sí de manera holística[2].

Un último cambio significativo es el reemplazo del Modelo de Evaluación de Procesos (PAM) de COBIT 5 basado en ISO/IEC15504 por un modelo de capacidad de proceso inspirado en la Integración del Modelo de Madurez de la Capacidad (CMMI). La guía de objetivos de gobierno y gestión, en el nivel de actividad del proceso, asocia cada práctica con un nivel de capacidad del proceso. El nuevo sistema es más fácil de usar y requiere procesos menos complejos para los niveles de capacidad más bajos en comparación con el modelo anterior. Sin embargo, las empresas que usan COBIT 5 PAM pueden continuar usando ese modelo si así lo desean, porque la guía relacionada con el proceso contiene toda la información requerida para hacerlo[3].

En la actualidad, la seguridad de la información es un tema fundamental para todas las áreas empresariales y de negocios, debido que la gestión de la información es parte vital del Gobierno Corporativo y requiere un nivel adecuado de protección de sus activos de información. Por esta razón es necesario utilizar un modelo de seguridad apropiado el cual cumpla con las necesidades de las organizaciones y le permita conocer el nivel de madurez de las mismas, con el fin de determinar un marco de trabajo de gobierno de tecnología de información orientado a la ciberseguridad[4].

En base a lo anterior se plantea la siguiente revisión bibliográfica con el objetivo de analizar los procesos de gobiernos que se desprenden de la normativa COBIT 2019 que evitan o minimizan los ataques informáticos dentro de la estructura de T&I de las organizaciones.

Metodología

La presente investigación se desarrolló en base a la normativa de revisión sistemática de la literatura establecida por Kitchenham [5], con el fin de obtener información relacionada con las preguntas de investigación que se plantean para el desarrollo de la misma.

Esta metodología establece las siguientes etapas:

- Planificación de la revisión.
- Realización de la revisión.
- Análisis de resultados.

Planificación de la revisión

La finalidad del estudio es analizar los procesos de gobiernos que se desprenden de la normativa COBIT 2019 que evitan o minimizan los ataques informáticos dentro de la estructura de T&I de las organizaciones, siempre con la finalidad de proteger y mantener la seguridad de la información que manejan.

Para el desarrollo del tema se plantearon las siguientes preguntas de investigación:

P1: ¿Cuáles son los dominios y procesos de seguridad informática que propone COBIT versión 2019 para mitigar ataques informáticos?

P2: ¿Cuáles son los instrumentos orientados a la medición de madurez de la seguridad informática que propone COBIT versión 2019?

P3: ¿Cuáles son las buenas prácticas de implementación de procesos de gobierno basados en un marco de referencia COBIT 2019 para mitigar ataques informáticos?.

Se emplearon bases de datos digitales, tal como ACM Digital Library, IEEE eXplorer, Science Direct Elsevier, Scopus y Springer Link, que trataban sobre temas asociados a la aplicación de COBIT 2019, procesos de gobierno, buenas prácticas, ciberseguridad, ataques informáticos y tecnología, identificando entre las fuentes de información revistas académicas y publicaciones técnicas, comprendidas entre los años 2018 y 2022.

La estrategia de búsqueda se basó en aspectos relacionados con las preguntas de investigación, empleando como parámetro las siguientes palabras claves: "ataques informáticos", "COBIT 2019", "procesos de gobierno" y "seguridad de la información", incluyendo las traducciones en inglés. Además, con el fin de refinar la selección se aplicaron los siguientes criterios (ver Tabla 1).

Realización de la revisión

Tabla 1. Criterios de selección

Criterios de inclusión	Criterios de exclusión
Artículos que abordan la definición de COBIT 2019, buenas prácticas, procesos de gobierno y ataques informáticos.	Información publicada en sitios web generales.
Documentos que señalan los procesos de gobierno basados en COBIT 2019.	Documentos con aportes irrelevantes.
Artículos con información acerca de métodos de defensa desarrollados para evitar los ataques informáticos basados en COBIT 2019.	Información de blogs.

En esta fase se seleccionaron los artículos en base a las cadenas de búsqueda y criterios de selección. En cada uno, se revisaron los títulos, contenido y conclusiones, lo que permitió determinar el aporte a las preguntas planteadas.

Como resultado de la búsqueda se identificaron 37 documentos, de los cuales se seleccionaron 15 que cumplieron con los criterios establecidos (ver Figura 1).

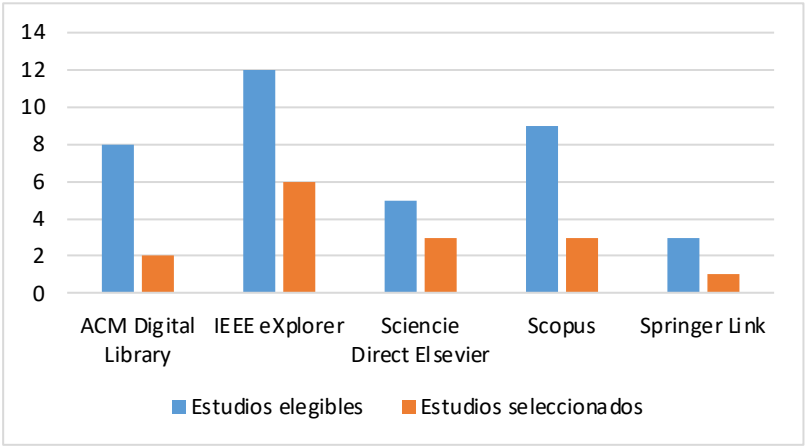

Figura 1. Documentos analizados para la revisión sistemática

Los dominios y procesos de seguridad informática basados en COBIT 2019 se identificaron al responder la P1: ¿Cuáles son los dominios y procesos de seguridad informática que propone COBIT versión 2019 para mitigar ataques informáticos?

Las nuevas tecnologías y la informática están creciendo a pasos agigantados, circunstancia que origina la aparición de sistemas y tipos de prestación de servicios novedosos que no se encontraban planteados en COBIT 5. En la actualidad, la información es la base principal de todo proceso de digitalización por lo que la gestión de la misma debe estar al más alto nivel dentro de la organización, razón por la cual este marco novedoso es llamado "Gobierno de la Tecnología e Información (T&I) de las empresas", considerando que no es lo mismo TI que T&I, debido que comúnmente se denomina TI al departamento que se dedica a la tecnología dentro de la empresa, mientas que T&I es toda la información recogida, tratada y usada por la empresa para conseguir los objetivos, así como la tecnología con la que cuenta para ello[6].

Por tanto, COBIT 2019 destaca la trascendencia de las tecnologías necesarias y de la información para las empresas, estableciendo seis principios que todo sistema de gobierno debe tener en cuenta a la hora de gestionar la tecnología y la información y, además, también establece tres principios para un marco de gobierno que puede usarse para crear un sistema de gobierno[7].

Respecto al sistema de gobierno, los principios son los siguientes:

- Es necesario un sistema de gobierno en la empresa que permita añadir más valor usando las tecnologías de la información, cumpliendo con las necesidades de los interesados.
- El sistema de gobierno está compuesto por diferentes elementos que trabajen unidos de forma completa.
- Es necesario un sistema de gobierno dinámico, es decir, que si se modifica alguno de los factores de diseño debe considerarse el efecto de esa modificación en todo el sistema.
- El sistema de gobierno tiene que diferenciar de forma clara las actuaciones y estructuras de gestión y el gobierno.
- Es necesario que el sistema de gobierno se adecue a las necesidades de la empresa, priorice y adapte los elemento tomando como medida determinados factores de diseño.
- Un sistema de gobierno no debe centrarse exclusivamente en el ámbito de TI sino que debe abarcar a toda la empresa, cubriendo todo el tratamiento de información y la tecnología utilizada[8].

Los principios referidos al marco de gobierno son:

- Automatización y coherencia: el marco de gobierno debe fundamentarse en un modelo conceptual que reconozca los elementos clave y las relaciones entre ellos.
- Flexibilidad y carácter abierto: con el marco de gobierno debe poder añadirse nuevo contenido y afrontar nuevos problemas de la forma más flexible posible.
- Adaptación a las regulaciones y estándares más destacados[9].

Por otra parte, para que la información y la tecnología contribuyan a los objetivos de la empresa, su gobierno y gestión deben alcanzar objetivos propios, encontrando conceptos básicos relacionados con los objetivos de gobierno y gestión, tales como:

- Un objetivo de gobierno o gestión siempre se relaciona con un proceso y una serie de componentes relacionados de otros tipos para ayudar a lograr el objetivo.
- Un objetivo de gobierno se relaciona

con un proceso de gobierno, mientras que un objetivo de gestión se relaciona con un proceso de gestión[10].

En consecuencia, los objetivos de gobierno y gestión en COBIT se agrupan en cinco dominios expresados con verbos que indican el propósito clave y las áreas de actividad del objetivo contenido en ellos. En el caso de los objetivos de gobierno se agrupan en el dominio Evaluar, dirigir y supervisar (EDM), es decir, en este dominio la dirección evalúa las opciones estratégicas, comunica a la alta gerencia las opciones estratégicas elegidas y supervisa el logro de la estrategia.

Con respecto a los objetivos de gestión, estos se agrupan en cuatro dominios:

- Alinear, Planificar y Organizar (APO): Aborda la organización general, la estrategia y las actividades de apoyo para T&I.
- Construir, Adquirir e Implementar (BAI): Se refiere a la definición, adquisición e implementación de soluciones T&I y la integración en procesos de negocio.
- Entrega, Servicio y Soporte (DSS): Aborda la entrega operativa y el soporte de los servicios de I&T, incluyendo la seguridad.
- Monitorear y Evaluar: Referido al monitoreo del desempeño y la conformidad de T&I con los objetivos de rendimiento, de control interno y requisitos externos[9].

P2: ¿Cuáles son los instrumentos orientados a la medición de madurez de la seguridad informática que propone COBIT versión 2019?

Determinar el nivel de madurez implica utilizar el nivel de capacidad combinado con otros factores para llegar a un puntaje que refleja no solo la existencia de las actividades, sino también una visión holística e integral de los procesos de la organización que, combinado con otras métricas, se puede presentar a la gerencia. Para lograrlo, es necesario correlacionar el nivel de capacidad con otros indicadores para obtener una mejor puntuación descriptiva de los procesos que pueda dar un enfoque conciso del estado organizacional. También es necesario crear hitos más allá de la descripción genérica del modelo de madurez de capacidad (CMMI) para cada práctica con el objetivo de identificar la evidencia esperada para el nivel de capacidad en cada actividad, lo cual es especialmente importante para crear hojas de ruta para la remediación y medir los resultados a lo largo del camino[11].

Según el nivel de capacidad de la actividad, el siguiente paso es determinar cómo reflejar ese nivel en su correspondiente práctica. Para las organizaciones en etapas tempranas de madurez, se puede utilizar un cálculo de promedio simple para los valores de las actividades con el fin de obtener el puntaje o nivel de práctica. Si una organización tiene una mayor capacidad para describir los niveles de madurez de sus actividades, entonces se recomienda un promedio ponderado, de acuerdo con la capacidad de la organización, para describir esas actividades[12].

Cada objetivo de gobierno y gestión incluye un componente de proceso, que abarca varias prácticas y cada una de estas prácticas tiene actividades que ayudan a asegurar el logro de los procesos asociados. Para ayudar a medir el logro del programa de una empresa, entre ellos la seguridad informática, así como la contribución al objetivo general de la empresa, se emplea un esquema de capacidad de proceso basado en la integración del modelo de madurez de la capacidad (CMMI), el cual va de 0 a 5[13].

Sin embargo, El uso de COBIT, que puede medir igualmente los mismos logros del programa empresarial, se realiza mediante un concepto llamado "gestión del rendimiento de COBIT" (CPM), gestión que puede representar qué tan bien funcionan el sistema de gobierno y gestión y todos los componentes de una empresa y cómo pueden mejorarse

para lograr los niveles de capacidad y madurez requeridos. Los niveles de capacidad y madurez se asignan a todas las actividades del proceso, lo que permite una definición clara de los procesos en diferentes niveles, circunstancia que puede ser efectiva a través de una evaluación exhaustiva del programa y las capacidades de la empresa utilizando la gestión del desempeño[14].

Existen algunas técnicas que pueden ayudar en la evaluación completa de un programa empresarial, entre ellas una técnica notable, que es eficaz y ha resistido la prueba del tiempo en el campo de la gestión de riesgos es la evaluación de riesgos tecnológicos (TRA) y, a pesar que su definición varía de una organización a otra, mantiene la misma funcionalidad. Esta evaluación examina las áreas clave de personas, procesos y tecnología en relación con un programa empresarial y mide su eficacia. Por lo tanto, el TRA puede proporcionar una calificación de puntaje de riesgo basada en la identificación de brechas en la evaluación, considerando que aunque la aplicación del método de la ruta crítica (CPM) puede parecer una tarea desalentadora para aplicar a las evaluaciones o técnicas realizadas por los profesionales de riesgo para su empresa, el hecho de dividirlo en varios pasos procesables hace que este esfuerzo sea más alcanzable y manejable[13].

P3: ¿Cuáles son las buenas prácticas de implementación de procesos de gobierno basados en un marco de referencia COBIT 2019 para mitigar ataques informáticos?

Para el logro de los objetivos de gobierno y gestión, cada uno de los componentes deben ser utilizados de tal manera que el objetivo general de creación de valor del gobierno se logre con éxito. Por tanto, entre las buenas prácticas de implementación de procesos, incluyendo minimizar los ataques informáticos, se puede mencionar:

- Los procesos describen un conjunto organizado de prácticas y actividades para lograr objetivos y deben producir un conjunto de resultados para respaldar el logro de los objetivos generales relacionados con T&I.
- Las estructuras organizacionales aseguran que existan entidades clave de toma de decisiones en la empresa y que sean conscientes de sus roles, responsabilidades y su participación esperada.
- Los principios, las políticas y los marcos traducen el comportamiento deseado en una guía práctica para la gestión diaria.
- La información requerida para el funcionamiento efectivo del sistema de gobierno de la empresa debe producirse, protegerse y estar disponible cuando sea necesario.
- La cultura, la ética y el comportamiento de las personas y de la empresa deben mantenerse continuamente, ya que ninguna política, proceso o tecnología se puede implementar de manera efectiva sin superar las limitaciones culturales.
- Las personas, las habilidades y las competencias son esenciales para las decisiones correctas, la ejecución de acciones correctivas y la finalización exitosa de las actividades planificadas.
- Los servicios, la infraestructura y las aplicaciones respaldan la gobernanza empresarial eficaz de T&I[15].

Por otra parte, las buenas prácticas en seguridad informática que son útiles para todas las organizaciones se fundamentan en la falta de conciencia en temas de seguridad de la información, incluyendo la ciberseguridad y la privacidad, lo que, sumado a la carencia de políticas en estos aspectos y la ausencia de planes de recuperación del negocio, ponen a las empresas en una situación de extrema vulnerabilidad y un alto riesgo que dificulta la supervivencia. De lo anterior se desprenden las siguientes recomendaciones, orientadas a temas de seguridad, privacidad y continuidad, a través de COBIT 2019:

- Entender el entorno con el fin de identificar vulnerabilidades en seguridad de información.
- Establecer principios y políticas para la seguridad y privacidad de la información.
- Establecer monitoreo sobre la infraestructura para identificar eventos de seguridad de la información.
- Definir acciones y comunicaciones de respuesta a incidentes que se deban tomar en caso de interrupción.

En la siguiente tabla se establece de forma más específica a que referencia COBIT 2019 corresponde:

Tabla 2. COBIT 2019

Buena práctica de gestión	Referencia COBIT 2019
Definición de políticas de seguridad de la información que sean aprobadas por la alta gerencia, igualmente la definición de roles y responsabilidades respecto al cumplimiento.	APO13.01
Instalación, activación, actualización y mantenimiento de herramientas de protección contra software malicioso.	DSS05.01
Realizar pruebas básicas de seguridad para las soluciones de T&I nuevas o para las actualizaciones.	BAI07.05
Configurar equipos de red seguros e implementar mecanismos de filtro de red, tal como Firewalls.	DSS05.02
Mejora de la seguridad de dispositivos de usuarios finales, tal como PC, portátiles o equipos móviles.	DSS05.03
Gestión de los accesos e identidades de los componentes claves de la infraestructura tecnológica.	DSS05.04
Gestión de los accesos físicos a los activos más importantes de T&I.	DSS05.05
Empleo de las herramientas tecnológicas de la que se dispongan con el fin de identificar de forma periódica vulnerabilidades y riesgos en la seguridad.	DSS05.07

En referencia al tema de la privacidad de la información es fundamental identificar datos sensibles y sus responsables, así como también especificar los roles y responsabilidades para soportar la gestión de información que se establezca como sensible. En el caso de las pequeñas empresas es importante la búsqueda de asesorías en agrupaciones empresariales y/o comunidades profesionales con el fin de lograr mayor eficacia en los esfuerzos de mejora continua, esto las ayudaría las empresas pequeñas definir la estrategia de negocios más adecuada antes de invertir y analizar el negocio y el proceso antes de tener soluciones en mente[16].

Lo anterior sin dejar de lado la importancia de aprovechar los recursos internos y promover una cultura cercana a empresas "startup", por lo que se debe siempre considerar establecer en los colaboradores, propietarios e interesados alrededor de la empresa, una genuina necesidad de cambiar, lo cual dentro de la actual cultura organizacional es más relevante que nunca[17].

Conclusiones

El COBIT 2019 es revolucionario, especialmente para aquellas organizaciones que desean tener un enfoque único para el T&I en lo que respecta a la gestión de riesgos y que también necesitan seguir normas y reglamentos muy específicos, debido que puede simplificar y reunir todos los procesos separados dentro de la empresa como un todo, un vínculo que usualmente falta, considerando que los departamentos de TI a menudo se tratan por separado del resto del negocio.

Este marco puede mejorar la gestión de riesgos de TI al recomendar las mejores prácticas tanto para los procesos de control de los sistemas técnicos como para las prácticas de gobierno ideales y, de esta manera, los sistemas de TI pueden alinearse mejor con los objetivos organizacionales del negocio.

Por otra parte, es complicado calcular el retorno de la inversión de los proyectos de TI en general, sin embargo, uno de los principales beneficios de COBIT 2019 es que incluye una forma de mostrar cómo TI puede marcar la diferencia en los objetivos comerciales y ayudar a la organización a alcanzar las metas planteadas y, especialmente, ayudar a monitorear la seguridad de la información mediante la aplicación de buenas prácticas que eviten o minimicen los efectos de los ataques informáticos.

Bibliografía

K. Harisaiprasad, «COBIT 2019 and COBIT 5 Comparison», ISACA, 2020. https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison (accedido 29 de diciembre de 2022).

D. Steuperaert, «Cobit 2019: A Significant Update», EDPACS, vol. 59, n.o 1, pp. 14-18, ene. 2019, doi: 10.1080/07366981.2019.1578474.

A. M. Syuhada, «Kajian Perbandingan Cobit 5 dengan Cobit 2019 sebagai Framework Audit Tata Kelola Teknologi Informasi», SLJIL, vol. 6, n.o 1, p. 30, ene. 2021, doi: 10.36418/syntax-literate.v6i1.2082.

X. E. O. Cabrera y M. D. Á. Galarza, «Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019», Polo del Conocimiento: Revista científico - profesional, vol. 7, n.o 3, p. 16, 2022.

B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, y S. Linkman, «Systematic literature reviews in software engineering – A systematic literature review», Information and Software Technology, vol. 51, n.o 1, pp. 7-15, ene. 2009, doi: 10.1016/j.infsof.2008.09.009.

«Introduction to the Minitrack on IT Governance and its Mechanisms», presentado en Hawaii International Conference on System Sciences, 2018, p. 3. [En línea]. Disponible en: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1578&context=hicss-51

P. Mulgund, P. Pahwa, y G. Chaudhari, «Strengthening IT Governance and Controls Using COBIT: A Systematic Literature Review», IJRCM, vol. 8, n.o 4, pp. 66-90, oct. 2019, doi: 10.4018/IJRCM.2019100104.

G. Braga, «COBIT 2019 and the IIA 2019 Guiding Principles of Corporate Governance: Two Frameworks, Many Similarities», ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-the-iia-2019-guiding-principles-of-corporate-governance (accedido 30 de diciembre de 2022).

Ciberseguridad, «COBIT», Ciberseguridad, 2022. https://ciberseguridad.com/normativa/espana/sgsi/cobit/ (accedido 19 de diciembre de 2022).

C. Anoruo, «Employing COBIT 2019 for Enterprise Governance Strategy», ISACA, 2019. https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-for-enterprise-governance-strategy (accedido 30 de diciembre de 2022).

L. Gorgona, «Construyendo un modelo de madurez para COBIT 2019 basado en CMMI», ISACA, 2021. Accedido: 19 de diciembre de 2022. [En línea]. Disponible en: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/building-a-maturity-model-for-cobit-2019-based-on-cmmi

A. A. Wagire, R. Joshi, A. P. S. Rathore, y R. Jain, «Development of maturity model for assessing the implementation of Industry 4.0: learning from theory and practice», Production Planning & Control, vol. 32, n.o 8, pp. 603-622, jun. 2021, doi: 10.1080/09537287.2020.1744763.

E. Elue, «Effective Capability and Maturity Assessment Using COBIT 2019», ISACA, 2020. https://www.isaca.org/resources/news-and-trends/industry-news/2020/effective-capability-and-maturity-assessment-using-cobit-2019 (accedido 19 de diciembre de 2022).

S. De Haes, W. Van Grembergen, A. Joshi, y T. Huygh, «COBIT as a Framework for Enterprise Governance of IT», en Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations, S. De Haes, W. Van Grembergen, A. Joshi, y T. Huygh, Eds. Cham: Springer International Publishing, 2020, pp. 125-162. doi: 10.1007/978-3-030-25918-1_5.

A. Sohail, «How COBIT 2019 Framework can be used to improve IT Governance», Business Beam, 7 de noviembre de 2019. https://www.businessbeam.com/blog/cobit-2019/ (accedido 19 de diciembre de 2022).

F. L. D. Pozos y M. P. A. Márquez, «Importancia y análisis del desarrollo empresarial», Pensamiento & Gestión, n.o 40, pp. 184-202, 2016.

D. M. Banegas y A. Z. Lenis, «Como aprovechar COBIT 2019 para afrontar el reto de transformación digital en las Pymes».

CITAR ESTE ARTICULO:

Tiglla Tumbaico, B. D., & Solís Acosta, E. F. (2023). Procesos de gobierno basado en COBIT 2019 para mitigar ataques informáticos. RECIMUNDO, 6(4), 671-680. https://doi.org/10.26820/recimundo/6.(4).octubre.2022.671-680