Desarrollo de un Plan Director de Seguridad para infraestructuras tecnológicas virtuales en instituciones educativas públicas: aplicación de COBIT® 2019

Development of a Security Master Plan for Virtual Technological Infrastructures in Public Educational Institutions: Application of COBIT® 2019

Pablo Roberto Sandoval-Barrantes[1]

Fecha de recepción: 16 de noviembre, 2024
Fecha de aprobación: 29 de marzo, 2025

Sandoval-Barrantes, P.R. Desarrollo de un Plan Director de Seguridad para infraestructuras tecnológicas virtuales en instituciones educativas públicas: aplicación de COBIT® 2019. *Tecnología en Marcha*. Vol. 38, Nº 4. Octubre-Diciembre, 2025. Pág. 66-86.

https://doi.org/10.18845/tm.v38i4.7590

1 Ingeniero de Infraestructura Tecnológica de la Dirección de Tecnología de Información y Comunicaciones de la Universidad Estatal a Distancia. Costa Rica.
psandoval@uned.ac.cr
https://orcid.org/0000-0002-5969-9480

Palabras clave

Educación a distancia; universidad pública; plataforma digital; seguridad de los datos; centro de datos; normalización; gestión de riesgos; COBIT® 2019.

Resumen

Este artículo presenta el desarrollo de un Plan Director de Seguridad basado en COBIT® 2019, aplicado a la infraestructura tecnológica virtual de una institución educativa pública; la Universidad Estatal a Distancia (UNED) de Costa Rica. Se indaga el contexto de la plataforma tecnológica de la institución, además mediante el uso de normas acordes al campo de la seguridad informática, se identifican las principales falencias de la infraestructura virtual con el fin de establecer un caso de estudio. A partir del caso, se proponen soluciones basadas en las buenas prácticas de gobernanza y gestión de TI a través de las iniciativas incluidas en el Plan Director de Seguridad obtenido. El enfoque metodológico para lograr la meta de la investigación incluyó el análisis situacional de la UNED y la aplicación de la guía de diseño COBIT® 2019 para personalizar controles de gobernanza y gestión. Los resultados obtenidos permitieron seleccionar procesos críticos relacionados a la necesidad de trabajar en un Sistema de Gestión de Seguridad de la Información (SGSI) como prioridad organizacional a la luz de COBIT® 2019 y otros aspectos como cumplimiento, gestión de la continuidad del negocio y gestión de incidentes, entre otros. En consecuencia, este trabajo brinda una alternativa sólida para generar planes de seguridad en instituciones con infraestructuras virtuales, aun cuando el modelo de negocio de estas sea distinto al caso de estudio en la UNED.

Keywords

Distance education; public education; digital platforms; data protection; computer security; data centers; standardization; risk management; COBIT® 2019.

Abstract

This article presents the development of a Security Master Plan based on COBIT® 2019, applied to the virtual technological infrastructure of a public educational institution, the Universidad Estatal a Distancia (UNED) in Costa Rica. The study explores the context of the institution's technological platform and using standards in accordance with the field of computer security, identifying the main weaknesses of the virtual infrastructure to establish a case study. Based on this case study, solutions are proposed following best practices in IT governance and management through the initiatives included in the resulting Security Master Plan. The methodological approach to achieve the research goal included a situational analysis of UNED and the application of the COBIT® 2019 design guide to customize governance and management controls. The results obtained allowed us to select critical processes pointing to the need to implement an Information Security Management System (ISMS) as an organizational priority in light of COBIT® 2019, along with other aspects such as compliance, business continuity management, and incident management, among others. Consequently, this work provides a solid alternative to generate security plans in institutions with virtual infrastructures, even when their business model is different from the UNED case study.

Introducción

La rápida evolución tecnológica ha transformado los modelos educativos, especialmente a los que acuden al uso de plataformas virtuales para ofrecer educación universitaria a distancia, cuyas infraestructuras tecnológicas virtuales son fundamentales para garantizar la continuidad operativa de los servicios administrativos, académicos, extensión, investigación, innovación y desarrollo, donde se requiere un acceso digital o remoto a diferentes recursos de aprendizaje, incluso a diferentes husos horarios. Sin embargo, esa fuerte dependencia de la tecnología genera desafíos para la adecuada gestión de la disponibilidad, integridad y confidencialidad de la información, lo cual se traduce en potenciales amenazas cibernéticas para los activos de información. Como objeto de estudio, se aborda el caso de la Universidad Estatal a Distancia (UNED) [1], la cual enfrenta desafíos particulares debido a su modelo operativo a distancia dependiente de su infraestructura tecnológica virtual para proporcionar servicios educativos para todo Costa Rica a través de Internet.

En este contexto, el marco COBIT® 2019 se presenta como “un marco de gobierno y gestión de información y tecnología más amplio y completo y continúa estableciéndose como un marco de referencia generalmente aceptado para el gobierno de I&T.” [2, pp. 9], proporcionando un enfoque integral para alinear la tecnología con los objetivos estratégicos de las organizaciones según ISACA [2]. Este marco también permite gestionar los riesgos asociados a las infraestructuras tecnológicas, proporcionando pautas para establecer controles específicos que permitan asegurar la protección de los activos de información de valor para cualquier institución.

Ahora bien, el objetivo de esta investigación es desarrollar un Plan Director de Seguridad para la UNED, empleando COBIT® 2019 como marco de trabajo. Según [3] un Plan Director de Seguridad “consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial”, lo cual para el caso de estudio se traduce en entregar pautas para la gestión de la seguridad informática de los equipos físicos, virtuales y servicios ofrecidos a través de la infraestructura tecnológica institucional, enfocándose en los objetivos estratégicos de la organización y priorizando asegurar la continuidad de los servicios críticos.

Además, se propone un conjunto de indicadores de mejora esperada que permitirían evaluar el impacto de la implementación del Plan Director de Seguridad en la organización.

Marco teórico

Gobernanza de TI en instituciones educativas

La gobernanza de las tecnologías de información (TI) es un componente fundamental en las instituciones educativas, principalmente por los desafíos actuales como la transformación digital, la protección de los activos digitales y el cumplimiento de los marcos regulatorios entre otros. El marco de gobierno y gestión de la información y la tecnología; denominado COBIT® 2019, desarrollado por ISACA, constituye una referencia internacional para estructurar los procesos de gobernanza TI, permitiendo alinear las capacidades tecnológicas con los objetivos estratégicos institucionales y fortalecer la seguridad de la información [4].

En concordancia con lo anterior, diversos estudios han señalado la relevancia de adoptar marcos robustos y modernos de gobernanza TI en el ámbito educativo. Moran Arellano et al. [5] demuestran que la aplicación de COBIT® 2019 en instituciones educativas contribuye a mejorar la alineación estratégica de TI y la gestión de riesgos tecnológicos, evidenciando beneficios

en la madurez organizacional. Sacón-Klinger et al. [6] documentan cómo la planificación estratégica de TI basada en COBIT® 2019, en una universidad pública ecuatoriana, permite optimizar la gobernanza institucional, fortalecer la seguridad de la información y alinear los procesos tecnológicos con los objetivos académicos.

Aportes de COBIT® 2019 a la seguridad de la información y la gestión de riesgos

Otro aspecto clave de COBIT® 2019 es su enfoque flexible para la gestión de riesgos y controles de seguridad de la información. Tiglla Tumbaico y Solís Acosta [7] evidencian que los procesos de gobierno basados en COBIT® 2019 contribuyen significativamente a la mitigación de ataques informáticos, reforzando la postura de ciberseguridad institucional. Asimismo, Orellana-Cabrera y Álvarez-Galarza [8] resaltan la aplicabilidad del marco en sectores críticos como el bancario, mostrando cómo su integración fortalece la resiliencia organizacional y el cumplimiento normativo.

De forma complementaria, Cuervo Forero [9] subraya la importancia de integrar el gobierno TI, la ciberseguridad y las comunidades digitales en la cultura organizacional como eje clave para la sostenibilidad institucional en entornos digitales, Además, remarca las diferencias y necesarias relaciones entre gobierno TI y ciberseguridad para garantizar la protección de la información.

Brecha en estudios empíricos en universidades públicas iberoamericanas

Por lo descrito, es claro que la literatura científica actual presenta una limitada cantidad de estudios empíricos que documenten la implementación de COBIT® 2019 en universidades públicas iberoamericanas, no así en otras latitudes, lo cual representa una oportunidad para ampliar el conocimiento académico y evolucionar más allá de enfoques puramente técnicos ante los desafíos de seguridad informática.

Aplicaciones internacionales de COBIT® 2019 en el sector educación

A nivel internacional, se han desarrollado estudios recientes mediante el marco COBIT® 2019, que han demostrado ser especialmente valiosos para universidades y entidades públicas con limitaciones presupuestarias o alta complejidad operativa. Por ejemplo, Fitriyani y Muhammad [10] aplicaron COBIT® 2019 para estandarizar procesos y mejorar la resiliencia de la gobernanza TI en PUSTIK STMIK Lombok, una universidad con recursos limitados de Indonesia. Wattimury y Faza [11] destacaron el uso del marco en la Fundación Educativa Bunda Hati Kudus de Indonesia para identificar el nivel de gobernanza institucional, mejorar la integración de sistemas descentralizados y alinear TI con objetivos académicos.

Mangoki et al. [12] desarrollaron un sistema de gobernanza para una universidad basado en COBIT® 2019, alineado con la planificación estratégica institucional, fundamentado en los 10 factores de diseño y 40 procesos de TI que propone el marco. Asimismo, Utomo et al. [13] resaltaron la importancia de adaptar COBIT® 2019 en instituciones de educación superior con características de PYME, evidenciando su aplicabilidad en contextos organizativos pequeños.

Aplicaciones internacionales de COBIT® 2019 en el sector público y seguridad

Por otra parte, en sectores relacionados, Hidayat et al. [14] demostraron que COBIT® 2019 contribuye a elevar la madurez de gobernanza en la industria de ciberseguridad, particularmente en dominios críticos de gestión de riesgos. Bagja et al. [15] presentaron un caso aplicado en el sector público (Unidad de Policía del Servicio Civil de Lombok Central), resaltando su efectividad en mejorar la continuidad operativa y la seguridad de los datos en organizaciones con recursos limitados.

De igual manera, Toaza et al. [16] aplicaron COBIT® 2019 en el contexto estratégico del sector público militar en un país en desarrollo (Ecuador), destacando la necesidad de personalización del marco en organizaciones grandes y centralizadas, con restricciones legales, operativas y presupuestarias, características típicas de los entornos públicos en América Latina.

Justificación metodológica del presente estudio

El presente estudio se apoya en estos aportes que consideraron variables clave como recursos, tamaño organizativo, sector y complejidad operativa. Además, consolida como un acierto el empleo del *COBIT® 2019 Design Toolkit* como herramienta metodológica base para el diseño del Plan Director de Seguridad, en línea con las recomendaciones presentadas en [17].

La integración de estas experiencias fortalece la base teórica del trabajo y refuerza la pertinencia de los resultados obtenidos para el contexto de la UNED, ofreciendo un enfoque integral que contribuya al fortalecimiento de la seguridad de la información y de la gobernanza TI en el ámbito educativo.

Materiales y métodos

El enfoque metodológico adoptado para desarrollar el Plan Director de Seguridad de la UNED, se sustentó en los lineamientos para elaborar informe modalidad proyecto y la estructura de la tesis de maestría elaborada por el autor de este artículo [1], como se detalla a continuación:

Tipo de Investigación

La investigación adopta un enfoque cuantitativo [18] debido a la necesidad de medir el impacto de las políticas y controles de seguridad con el marco de trabajo COBIT® 2019. La cuantificación se centra mayormente en el análisis de eficiencia operativa, cumplimiento, gestión de incidentes, reducción de riesgos y disponibilidad de sistemas. Además, tiene un alcance exploratorio [18], ya que busca examinar un campo relativamente novedoso: la aplicación de COBIT® 2019 para la gestión de la seguridad de infraestructuras virtuales.

Lugar y Contexto de la Investigación

La investigación se llevó a cabo como tesis de Magister en Seguridad Informática de la Universidad de Buenos Aires, Argentina, elaborada por el autor de este artículo [1] y fue aplicada en la Universidad Estatal a Distancia (UNED), una institución pública de educación superior que depende de plataformas tecnológicas virtuales para su funcionamiento. El contexto educativo y la infraestructura tecnológica de la UNED constituyen el entorno donde se realiza y evalúa el Plan Director de Seguridad resultante.

Métodos y Herramientas Utilizadas

Se aplicó la guía de diseño "*COBIT® 2019 Design Toolkit*" [19] como herramienta principal para personalizar los controles de seguridad, adaptando el marco COBIT® 2019 [2],[20] a las necesidades específicas de la institución. Se recurrió a las normas ISO/IEC27001, ISO/IEC27002 e ISO/IEC27014 [21],[22],[23], así como a la guía de Introducción y Metodología de COBIT® 2019 [4] para brindar sustento a los insumos que fueron ingresados en la herramienta de diseño.

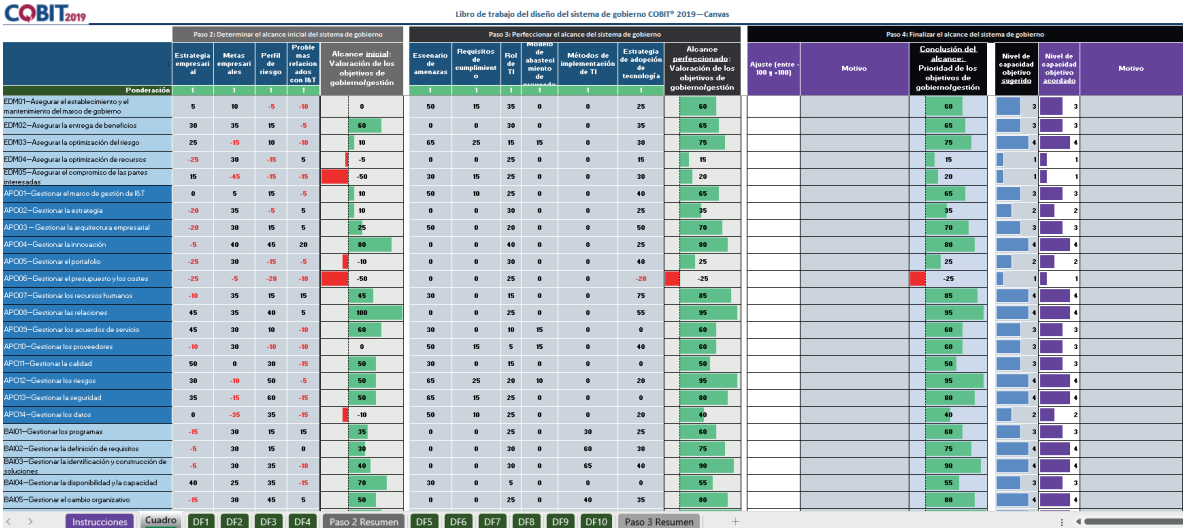

Figura 1. Vista general de la herramienta guía de diseño (COBIT® 2019 Design Toolkit) utilizada para cuantificar la situación de la seguridad de la información al caso de la UNED y posterior análisis de resultados. Fuente: [19].

"En la imagen anterior se muestra una vista de la herramienta de diseño COBIT® 2019 con valores detallados. Además, se indican las 4 principales interfaces que permiten elaborar el flujo de trabajo para obtener un diseño de sistema de gobierno personalizado. La primera pestaña corresponde a instrucciones generales de llenado de información y uso de la herramienta, la segunda pestaña es el cuadro consolidado a interpretar. Las pestañas DF1-10 corresponden a los 10 factores de diseño específicos que se trabajan a partir del contexto previamente analizado, y las pestañas de resumen corresponden al Paso 2 de valores obtenidos y el Paso 3 para refinamiento de todos los valores."[1, pp. 56]

Actividades realizadas

Se realizó un diagnóstico del estado actual mediante recopilación de información de activos de información y entrevistas a personal clave con el fin de crear la documentación relacionada al modelo de plataforma tecnológica existente en la UNED y alineada a normas competentes en seguridad de la información como ISO/IEC27001, ISO/IEC27002 e ISO/IEC27014 [21],[22],[23].

Se continuó con un análisis de las necesidades relacionadas a los procesos y servicios críticos para la UNED que requieren controles adicionales. Además, se construyó el caso a partir de la guía de Introducción y Metodología de COBIT® 2019 [4, pp. 53] y se evaluaron las políticas de seguridad existentes y posibles brechas en la gestión de seguridad de la infraestructura virtual.

Finalmente se aplicó la guía de diseño "*COBIT® 2019 Design Toolkit*" [19, pp. 31-66] al caso de estudio y se obtuvo el diseño del Plan Director de Seguridad para los equipos físicos y virtuales, así como para los servicios ofrecidos a través de la infraestructura tecnológica de virtualización en la UNED, considerando incluso la definición de métricas específicas para cada control propuesto, alineando las acciones con los objetivos estratégicos de la organización. Las principales fases del plan director obtenido a saber:

- Análisis de la situación actual (a partir de los resultados al aplicar COBIT® 2019).
- Identificación de riesgos y vulnerabilidades.
- Propuesta de **iniciativas de seguridad** claves para el caso particular de la UNED.

Resultados y discusión

Para el diagnóstico de la situación de la UNED se recurrió al personal de la Dirección de Tecnología de Información y Comunicaciones (DTIC) de la institución para comprobar el modelo de Plataforma Tecnológica de la UNED, así como los equipos físicos y virtuales de la infraestructura tecnológica que soportan la operación de la Institución. Lo anterior evidenció que "la UNED tiene un modelo de plataforma tecnológica orientado a la virtualización de equipos y uso de redes de datos, brindando sus servicios a través de Internet"[1, pp. 45] y además "se comprobó que la UNED maneja un inventario de activos de información (reflejado en varios documentos) que contempla los equipos físicos y virtuales de la infraestructura." [1, pp. 46]

Con el apoyo de las normas ISO/IEC 27001/27002 [21],[22] se realizó un análisis de la situación descubierta en el diagnostico anterior, se logró hacer una valoración de la gestión de activos y responsabilidades de la infraestructura tecnológica virtual así como una clasificación de los mismos, encontrando una "necesidad de mejora en cuanto a buenas prácticas e incluso controles específicos en materia de seguridad de la información, principalmente en los procedimientos del manejo de equipos virtuales" [1, pp. 51]

Debido a la situación anteriormente expuesta para el caso de estudio en la UNED, es que se plantea la oportunidad de utilizar la "herramienta de diseño COBIT® 2019 que provee ISACA para comprender el alcance inicial a partir de la influencia de factores de diseño sobre los objetivos de gobierno o gestión de COBIT® 2019" [1, pp. 53] y así poder hacer " un mapeo inicial de los objetivos de gobierno y gestión a priorizar en relación con la seguridad de la información de la infraestructura tecnológica virtual y servicios ofrecidos" [1, pp. 53]. A partir de los datos del caso de estudio ingresados en la herramienta de diseño COBIT® 2019 se obtienen los siguientes resultados cuantificados:

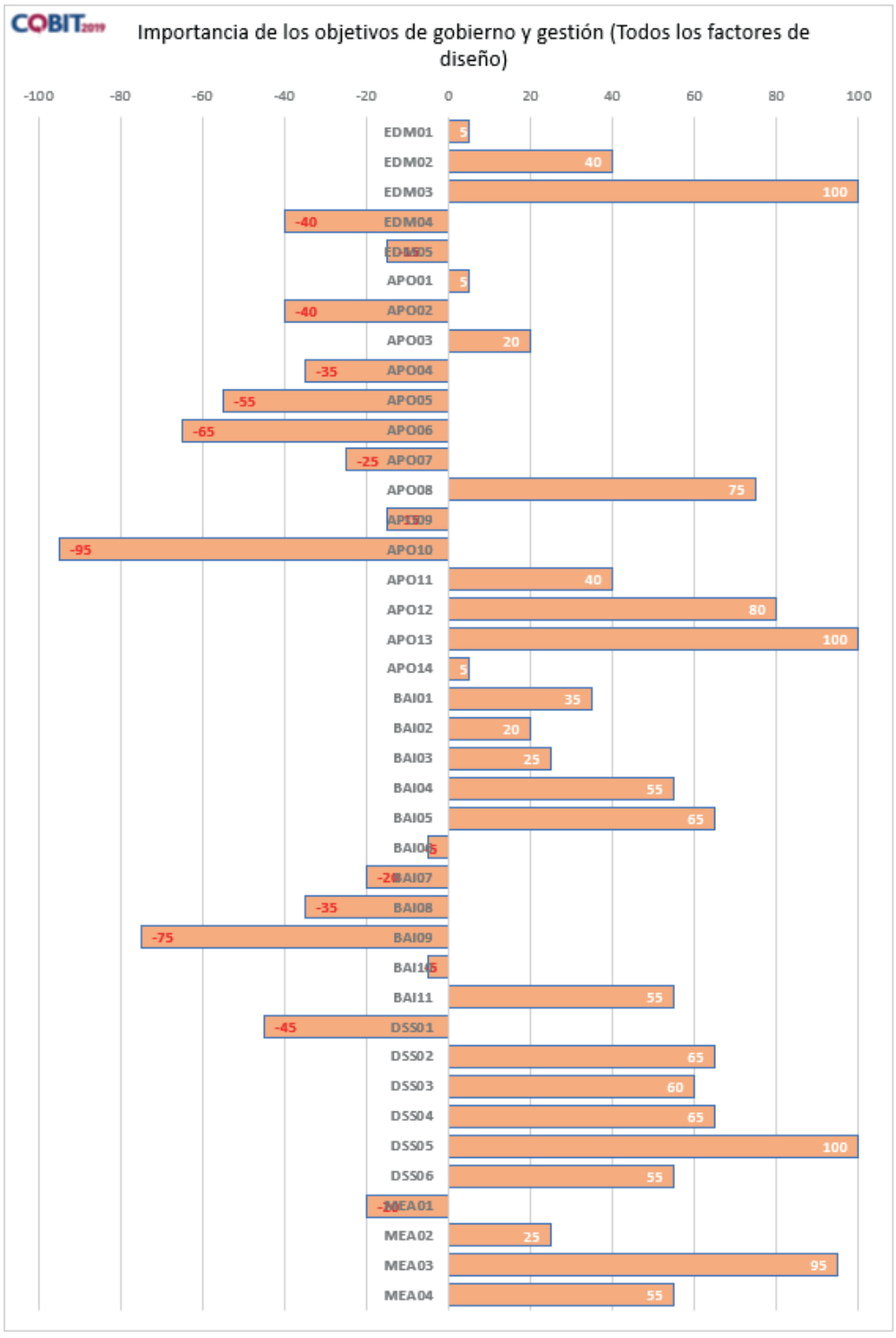

Figura 2. Resumen de objetivos de gobierno y gestión COBIT® 2019 obtenidos al aplicar la guía de diseño al caso de estudio de la UNED. Fuente: [1].

La Figura 2 anterior muestra los resultados que detallan los rasgos propios de la situación en seguridad de información para la UNED, destacando los valores del objetivo "de gobierno EDM03-Asegurar la optimización del riesgo, así como para los objetivos de gestión APO12-

Gestionar el riesgo, APO13-Gestionar la seguridad, DSS05-Gestionar los servicios de seguridad y MEA03-Gestionar el cumplimiento de los requisitos externos" [1, pp. 68], como los de mayor ajuste (+80 o +100) en importancia para realizar conclusiones sobre seguridad.

Consecuente con los resultados anteriores obtenidos de la herramienta de diseño COBIT® 2019, fue posible cuantificar la situación y establecer prioridades para las áreas claves relacionadas a la infraestructura tecnológica virtual de la institución y la seguridad de la información de estas, dando como resultado la propuesta del Plan Director de Seguridad.

Plan Director de Seguridad desarrollado

A continuación, se presentan las siguientes siete (7) iniciativas que conforman el "Plan director para la gestión de la seguridad informática de los equipos físicos, virtuales, y para los servicios ofrecidos a través de la infraestructura tecnológica de virtualización en la UNED [1, pp. 76]":

Cuadro 1. Extracto de las iniciativas incluidas en el Plan Director de Seguridad obtenido para el caso de la UNED Modificado de: [1, pp. 76-80].

INICIATIVA 1: Desarrollar políticas y/o normativa de seguridad para los diferentes componentes físicos y virtuales de la infraestructura tecnológica y servicios contenidos en esta.
DESCRIPCIÓN:
Generar normativa interna que responda a los requerimientos mínimos de seguridad de la información para proteger la infraestructura tecnológica actual, en concordancia con las políticas institucionales existentes, sustentada en la valoración existente de riesgos en I&T y en normas propias de la seguridad de la información, compatibles con la UNED.
-Obtener el compromiso de las unidades estratégicas de la DTIC.
-Elaborar controles mínimos de seguridad informática acorde a los riesgos identificados.
-Mejorar la gestión del inventario de activos de información, incluyendo su actualización periódica y gestión de responsables.
APOYO DOCUMENTAL:
- Sistema Específico de Valoración de Riesgo Institucional (SEVRI) de la UNED.
- Ley General de Control Interno N°8292.
- ISO/IEC 27005.
- CMMI Data Management Maturity Model.
- ISF, The Standard of Good Practice for Information Security.
- ISO/IEC 27001.
- CMMI Cybermaturity Platform.
- PMBOK Guide, 6.ª edición.

INICIATIVA 2: Diseño inicial de un SGSI. DESCRIPCIÓN: Diseñar un Sistema de Gestión de la Seguridad de la Información (SGSI), con alcance integral, a fin de proteger la infraestructura tecnológica virtual y los servicios. -Contemplar las actividades actuales de atención de eventos y amenazas de seguridad informática, continuidad y disponibilidad de los servicios. -Definir el alcance del SGSI, los activos de información que son abarcados y los procesos involucrados, incluyendo sus controles, responsabilidades. -Definir la ruta o pasos a seguir para la implementación y mantenimiento del SGSI. APOYO DOCUMENTAL: - ISO/IEC 20000-1 - ISO/IEC 27001, ISO/IEC 27002. - ITIL V3. - COBIT® 2019: APO13-Gestionar la seguridad - Estrategia Nacional de Ciberseguridad Costa Rica 2017. San José, CR, MICITT, 2017. - ISF, The Standard of Good Practice for Information Security. - CMMI Data Management Maturity Model. - The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1. -CMMI Cybermaturity Platform. - Skills Framework for the Information Age V6. - Institute of Standards and Technology Special Publication 800-53. - HITRUST CSF versión 9
INICIATIVA 3: Plan de continuidad del negocio DESCRIPCIÓN: Incluir los equipos y servicios de la infraestructura tecnológica virtual de la UNED, dentro del alcance del plan de continuidad del negocio. -Atender las interrupciones ocasionadas por eventos no planificados que puedan afectar la infraestructura tecnológica virtual. -Establecer para la UNED los valores aceptables de recuperación de las operaciones, y de disponibilidad de la infraestructura y sus servicios críticos. APOYO DOCUMENTAL: - Política de gestión del riesgo y continuidad de los servicios en la UNED.

INICIATIVA 4: Optimizar la atención de incidentes recurrentes relacionados a la operación de la infraestructura tecnológica virtual. DESCRIPCIÓN: Documentar los incidentes operativos recurrentes que afecten o puedan afectar la infraestructura tecnológica virtual y los servicios críticos, para realizar un análisis que permita optimizar su resolución y crear oportunidades de prevención y mejora. -Documentar incidentes de manera exhaustiva. -Identificar causas de incidentes relacionadas a la infraestructura tecnológica virtual, y establecer pasos a seguir para corregir o modificar los aspectos disfuncionales, a fin de corregir problemas de disponibilidad del servicio, adquirir equipos más adecuados o utilizar los recursos existentes de manera más efectiva. APOYO DOCUMENTAL: - ISO/IEC 20000-1 sección 8.2 Administración de problemas. - CMMI Cybermaturity Platform. - ITIL V3.
INICIATIVA 5: Gestionar la capacidad de la infraestructura tecnológica virtual DESCRIPCIÓN: Gestionar la capacidad de la infraestructura tecnológica virtual en función de los requisitos de los servicios soportados en la DTIC y para la UNED, considerando el rendimiento y los valores óptimos de disponibilidad esperada para estos servicios. -Documentar los requerimientos de recursos actuales y a futuro que resulten adecuados para la UNED. -Establecer valores óptimos de nivel de recursos para los requerimientos y brindar seguimiento continuo. -Propuesta de Marco de Gobierno y Gestión TI de la UNED (En desarrollo con CONARE). -Documentación interna de la UNED, plan de capacidad, suministro y nivel de servicio. -CMMI Cybermaturity Platform. APOYO DOCUMENTAL: - ISF, The Standard of Good Practice for Information Security. - ISO/IEC 20000-1. - ITIL V3.
INICIATIVA 6: Establecer y documentar controles de integridad de la información para la infraestructura tecnológica virtual. DESCRIPCIÓN: Proponer uso de normativas para la seguridad de la información, específicamente con el fin de atender la integridad de los activos de información de la infraestructura tecnológica virtual. -Extender el uso de estas normativas o buenas prácticas de seguridad a los proveedores que brinden servicios a la infraestructura tecnológica virtual. APOYO DOCUMENTAL: - ISO/IEC 27002 sección 7. - National Institute of Standards and Technology Special Publication 800-37. - The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1. - ISF, The Standard of Good Practice for Information Security 2016: BA1.4 Information Validation. - CMMI Cybermaturity Platform: gestion de acceso. - Skills Framework for the Information Age V6, 2015, seguridad y gestión secciones SCTY y SCAD.

INICIATIVA 7: Otras consideraciones en seguridad de la información.
DESCRIPCIÓN:
Complementar la seguridad de la información de la infraestructura tecnológica virtual mediante actividades de concientización, ampliando las existentes o generando nuevas y mejorar la comunicación entre las diferentes áreas involucradas, a fin de trabajar la seguridad de la información de la infraestructura tecnológica virtual de una manera integral y transversal a las áreas de la UNED.
APOYO DOCUMENTAL:
- ISO/IEC 27001
- Creating a Culture of Security, ISACA, 2011

Fuente: [1]

El Cuadro 1 anterior es el producto de la construcción del caso de estudio con el marco de trabajo COBIT® 2019, que permitió identificar los objetivos de gobierno y gestión que tienen mayor relevancia para la seguridad de la información de la UNED, permitiéndole enfocar sus esfuerzos en áreas de alto impacto, tales como la gestión de riesgos, servicios de seguridad, cumplimiento normativo, incluso preparar a la organización para enfrentar futuros desafíos tecnológicos, optimizando recursos y creando resiliencia para su infraestructura crítica.

Finalmente, a partir de los resultados, es necesario destacar las siguientes iniciativas que resultaron relevantes para la UNED:

- El Sistema de Gestión de Seguridad de la Información (SGSI) está en línea con los objetivos COBIT® 2019 de mayor ajuste positivo (+100), como la optimización del riesgo y gestión de servicios de seguridad (Figura 2). Esto indica que implementar el SGSI es una prioridad institucional según el marco de referencia COBIT® 2019.
- La importancia asignada al cumplimiento de requisitos externos (ajuste +95) justifica las iniciativas sobre políticas y normativas de seguridad, la UNED se debe mantener en conformidad con los estándares y regulaciones para brindar estabilidad de la infraestructura tecnológica y dar transparencia como universidad pública.
- No menos importante se tiene el objetivo DSS04-la gestión de la continuidad del negocio y objetivo DSS02- la gestión de peticiones e incidentes (ambos con ajustes de +65) alertan a la UNED sobre la importancia en la atención de incidentes y asegurar la continuidad operativa mediante respuestas eficaces a eventos inesperados, siendo un aspecto crítico para una institución de educación a distancia y en línea.

Indicadores de mejora esperada

El desarrollo del Plan Director de Seguridad basado en COBIT® 2019 es una propuesta metodológica, para la cual se identifican una serie de indicadores clave de desempeño (KPI) de referencia que permitirían evaluar el impacto esperado en su implementación dentro de la UNED, incluso se pueden utilizar como base para un sistema de monitoreo continuo de la seguridad de la información y medición de resultados a futuro en cualquier otra organización. A continuación, la lista de los indicadores:

Cuadro 2. Indicadores clave de desempeño KPI 01 como referencia para evaluar impacto del Plan Director de Seguridad.

KPI 01: Cumplimiento de controles de seguridad para la mitigación de ataques informáticos.		
Iniciativa del Plan Director referenciada o relacionada	Iniciativa 1 (políticas y controles).	
Marco de referencia sugerido o utilizado en métrica.	-Sistema Específico de Valoración de Riesgo Institucional (SEVRI) de la UNED [24].	
Fórmula	1: Valoración de riesgo (SEVRI) completada. Y: Años desde que se realizó la última valoración.	
Valor actual estimado	50% (1 valoración de riesgos (SEVRI) cada 2 años)	
Meta esperada después de aplicar iniciativa del Plan Director propuesto.	100% (1 valoración de riesgos (SEVRI) anual)	
Frecuencia/Tiempo ejecución sugerido	1 año.	
Nivel de tolerancia sugerido		
Óptimo	Bueno	Deficiente
X = 100% (1 valoración de riesgos (SEVRI) anual)	50% ≤ X ≤ 90% (1 valoración de riesgos (SEVRI) cada 1,5 años)	X < 50% (1 valoración de riesgos (SEVRI) cada 2 años o más)
Iniciativa del Plan Director referenciada o relacionada	Iniciativa 6 (integridad).	
Marco de referencia sugerido o utilizado en métrica.	-ISO/IEC 27002 [22].	
Fórmula	Y: Controles de seguridad identificados como críticos o aplicables a la institución. Seleccionados a partir de los 93 controles relacionados a seguridad establecidos en la norma ISO/IEC 27002. Z: Controles de seguridad efectivos o debidamente aplicados en la institución.	
Valor actual estimado	32.05% (Porcentaje (%) de controles de seguridad efectivos: 25 controles críticos actualmente aplicados en la UNED de un máximo de 78 aplicables a la misma institución)	
Meta esperada después de aplicar iniciativa del Plan Director propuesto.	70.51% (Porcentaje (%) de controles de seguridad efectivos: 55 controles críticos y de mejora en el caso de la UNED de un máximo de 78 aplicables a la misma institución)	
Frecuencia/Tiempo ejecución sugerido	18-36 meses	
Nivel de tolerancia sugerido		
Óptimo	Bueno	Deficiente
X > 90%	70% ≤ X ≤ 90%	X < 70%

Cuadro 3. Indicadores clave de desempeño KPI 02 como referencia para evaluar impacto del Plan Director de Seguridad.

KPI 02: Nivel de madurez en seguridad de la información (basado en COBIT® 2019).		
Iniciativa del Plan Director referenciada o relacionada	Iniciativa 2 (SGSI).	
Marco de referencia sugerido o utilizado en métrica.	-COBIT® 2019 [4]. -CMMI V3.0. CMMI Model Quick Reference Guide [25] apartado ESEC (Enabling Security)	
Fórmula	Asignar 1 de 3 niveles según guía CMMI V3.0: Nivel 1: Identificar, abordar y priorizar las necesidades y los problemas de seguridad. Nivel 2: Identificar, abordar y priorizar las necesidades y los problemas de seguridad para desarrollar un enfoque y objetivos de seguridad que aborden las necesidades físicas, de misión, de personal, de procesos y de ciberseguridad. Nivel 3: Requiere una capacidad de operaciones de seguridad organizacional para implementar una estrategia, un enfoque y una arquitectura de seguridad organizacional. Realizar revisiones y evaluaciones de seguridad y actúa en función de sus resultados. [25]	
Valor actual estimado	Nivel 2	
Meta esperada después de aplicar iniciativa del Plan Director propuesto.	Nivel 3	
Frecuencia/Tiempo ejecución sugerido	18-24 meses	
Nivel de tolerancia sugerido		
Óptimo	Bueno	Deficiente
Nivel 3	Nivel 2	Nivel 1
Iniciativa del Plan Director referenciada o relacionada	Iniciativa 2 (SGSI).	
Marco de referencia sugerido o utilizado en métrica.	-COBIT® 2019 [4]. -CMMI V3.0. CMMI Model Quick Reference Guide [25] apartado MST (Managing Security Threats & Vulnerabilities)	

KPI 02: Nivel de madurez en seguridad de la información (basado en COBIT® 2019).		
Iniciativa del Plan Director referenciada o relacionada	Iniciativa 2 (SGSI).	
Fórmula	Asignar 1 de 4 niveles según guía CMMI V3.0: Nivel 1: Identificar y registrar las amenazas y vulnerabilidades de seguridad, y tomar las medidas adecuadas para abordarlas. Nivel 2: Crear y mantener un método para gestionar las amenazas y vulnerabilidades de seguridad, incluyendo criterios de evaluación actualizados. Utilizar estos criterios para priorizar, supervisar y abordar las amenazas y vulnerabilidades críticas. Evaluar e informar sobre la eficacia del enfoque y las medidas adoptadas para gestionar estos problemas. Nivel 3: Crear, actualizar y aplicar una estrategia, un enfoque y una arquitectura de seguridad organizacional para evaluar, gestionar y verificar las amenazas y vulnerabilidades. Analizar los resultados de la verificación y validación de seguridad para garantizar la precisión y la coherencia en toda la organización. Evaluar la eficacia de la estrategia, el enfoque y la arquitectura de seguridad para abordar estas amenazas y vulnerabilidades. Nivel 4: Utilizar el análisis de inteligencia de amenazas, junto con técnicas estadísticas y cuantitativas, para mejorar el enfoque y la arquitectura de seguridad. Seleccionar soluciones de seguridad para abordar las amenazas y vulnerabilidades con base en este análisis. [25]	
Valor actual estimado	Nivel 2	
Meta esperada después de aplicar iniciativa del Plan Director propuesto.	Nivel 3	
Frecuencia/Tiempo ejecución sugerido	18-24 meses	
Nivel de tolerancia sugerido		
Óptimo	Bueno	Deficiente
Nivel 4	Nivel 2 - Nivel 3	Nivel 1

Cuadro 4. Indicadores clave de desempeño KPI 03 como referencia para evaluar impacto del Plan Director de Seguridad.

KPI 03: Disponibilidad de servicios críticos (plataforma virtual, sistemas de gestión académica, correo institucional, otros).		
Iniciativa del Plan Director referenciada o relacionada	Iniciativa 3 (continuidad del negocio).	
Marco de referencia sugerido o utilizado en métrica.	-Política de gestión del riesgo y continuidad de los servicios en la UNED [26]. -ISO/IEC 27001 [21]. (Anexo A.17). -ISO22301 [27].	
Fórmula	Y: Equipos y servicios de la infraestructura tecnológica virtual incluidos en el alcance del plan de continuidad del negocio. Z: Equipos y servicios de la infraestructura tecnológica virtual comprobados en el plan de continuidad del negocio.	
Valor actual estimado	Dato no confirmado.	
Meta esperada después de aplicar iniciativa del Plan Director propuesto.	50% o más. (Este valor lo debe definir cada organización según sus prioridades institucionales)	
Frecuencia/Tiempo ejecución sugerido	12-24 meses	
Nivel de tolerancia sugerido		
Óptimo	Bueno	Deficiente
X > 80%	50% ≤ X ≤ 80%	X < 50%

Cuadro 5. Indicadores clave de desempeño KPI 04 como referencia para evaluar impacto del Plan Director de Seguridad.

KPI 04: Número de incidentes/problemas operativos registrados por año.		
Iniciativa del Plan Director referenciada o relacionada	Iniciativa 4 (gestión de incidentes operativos que afectan la disponibilidad).	
Marco de referencia sugerido o utilizado en métrica.	-ISO/IEC 20000-1 [28]	
Fórmula	Y: Total de incidentes registrados en el periodo anterior. Z: Total de incidentes reportados en el periodo actual.	
Valor actual estimado	Línea base, se deben empezar a registrar los incidentes.	
Meta esperada después de aplicar iniciativa del Plan Director propuesto.	-Tomar datos primer periodo. -Reducir incidentes en 25% o más a partir del registro del segundo periodo, respecto al registro inicial del primer periodo. (Este valor lo debe definir cada organización según sus prioridades institucionales)	
Frecuencia/Tiempo ejecución sugerido	12-24 meses	
Nivel de tolerancia sugerido		
Óptimo	Bueno	Deficiente
X > 50%	0% ≤ X ≤ 50%	X < 0%

Cuadro 6. Indicadores clave de desempeño KPI 05 como referencia para evaluar impacto del Plan Director de Seguridad.

KPI 05: Capacidad de infraestructura tecnológica virtual.		
Iniciativa del Plan Director referenciada o relacionada	Iniciativa 5 (capacidad de infraestructura virtual).	
Marco de referencia sugerido o utilizado en métrica.	-COBIT® 2019 [4]. -DTIC UIT F01 Plan para la gestión de la capacidad de la Infraestructura TI [29].	
Fórmula	Y: Porcentaje (%) de consumo de equipos servidores. Z: Porcentaje (%) de consumo de equipos de red. W: Porcentaje (%) de consumo de equipos de respaldos.	
Valor actual estimado	Servidores: 80% Red: 20% Respaldos: 80%	
Meta esperada después de aplicar iniciativa del Plan Director propuesto.	Servidores: 80% Red: 50% Respaldos: 80%	
Frecuencia/Tiempo ejecución sugerido	12-24 meses	
Nivel de tolerancia sugerido		
Óptimo	Bueno	Deficiente
Servidores: 85% > X ≥ 70% Red: 85% > X ≥ 55% Respaldos: 90% > X ≥ 70%	Servidores: 70% > X > 50% Red: 55% > X > 20% Respaldos: 70% > X > 50%	Servidores: X ≥ 85% o X ≤ 50% Red: X ≥ 85% o X ≤ 20% Respaldos: X ≥ 90% o X ≤ 50%

Cuadro 7. Indicadores clave de desempeño KPI 06 como referencia para evaluar impacto del Plan Director de Seguridad.

KPI 06: Personal y contratistas capacitados en ciberseguridad.		
Iniciativa del Plan Director referenciada o relacionada	Iniciativa 7 (cultura y concientización).	
Marco de referencia sugerido o utilizado en métrica.	-ISO/IEC 27001 [21]. (Anexo A.7.2)	
Fórmula	Y: Total de personas funcionarias y contratistas activas en la organización. Z: Total de personas funcionarias y contratistas capacitados en ciberseguridad.	
Valor actual estimado	≤ 10%	
Meta esperada después de aplicar iniciativa del Plan Director propuesto.	Al menos 35% a partir del tercer año. (Este valor depende de la capacidad de cada institución para capacitar el volumen de empleados necesario en el año).	
Frecuencia/Tiempo ejecución sugerido	12-36 meses	
Nivel de tolerancia sugerido		
Óptimo	Bueno	Deficiente
X ≥ 95%	95% > X > 60%	X ≤ 60%

En los cuadros 2, 3, 4, 5, 6 y 7 anteriores se aprecian los indicadores recomendados para evaluar el impacto de llevar a cabo la implementación del Plan Director de Seguridad descrito en este artículo. Estos KPI representan importantes valores de referencia y metas esperadas orientativas que pueden requerir ajustes en función del contexto operativo y los recursos disponibles durante la fase de implementación efectiva del Plan Director de Seguridad en la organización, por lo que algunos valores se alinearon al caso de estudio en la UNED, pero las normas referenciadas permiten modificaciones si así lo requiere cualquier organización.

Además de alinearse con el marco COBIT® 2019 y diversas normas ISO/IEC [21][22][27][28], los KPI propuestos enfatizan las prácticas recomendadas en las áreas de Enabling Security (ESEC) y Managing Security Threats & Vulnerabilities (MST) del modelo CMMI® v3.0 [25] con el fin de avanzar hacia la madurez en seguridad operativa y gestión de amenazas en cualquier organización.

Limitaciones y consideraciones de la implementación

Si bien el Plan Director de Seguridad propuesto proporciona un marco estructurado y alineado con las mejores prácticas internacionales para fortalecer la seguridad de la información en la Universidad Estatal a Distancia (UNED), su implementación efectiva podría enfrentar diversos desafíos y limitaciones que es importante considerar:

- En primer lugar, la resistencia al cambio organizacional puede ser un obstáculo importante, especialmente en entornos académicos donde la autonomía de las diferentes unidades y departamentos podría dificultar la adopción uniforme de los controles y políticas de seguridad propuestos, incluso con limitaciones relacionadas con conflictos de espacios de poder entre las áreas de la institución [6].
- Por otra parte, la asignación de recursos humanos y financieros son un desafío para el despliegue de nuevas medidas de seguridad de la información, lo cual depende en gran medida del compromiso institucional de ir más allá de la implementación de controles a establecer medidas integrales que evolucionen con las amenazas y los requisitos normativos.
- Asimismo, la existencia de infraestructuras tecnológicas heterogéneas y sistemas heredados puede representar una lucha técnica abrumadora, ya que es posible que algunos sistemas no soporten fácilmente los niveles de control y monitoreo que el plan sugiere o no se cuente con el conocimiento por parte del personal a cargo. Esto requerirá esfuerzos adicionales de integración, capacitación y modernización.
- Adicionalmente, se identificaron algunas limitaciones durante el uso de la herramienta COBIT® 2019 Design Toolkit. Tal como advierte [17], la herramienta presenta un nivel limitado con vocabulario y lenguaje técnico que pueden dificultar la comprensión a usuarios con menos experiencia, incluso a aquellos del área de TI [17]. Estos aspectos se subsanaron durante el estudio mediante esfuerzos adicionales de interpretación y validación de resultados, lo cual constituye un factor a considerar en futuras aplicaciones.
- Finalmente, el éxito del Plan Director de Seguridad dependerá en gran medida del desarrollo de una cultura institucional de seguridad de la información que empieza por las autoridades. Sin un compromiso activo por parte de la alta dirección y una adecuada capacitación y concientización de todas las personas funcionarias, incluso el mejor diseño de controles podría resultar insuficiente para mitigar los riesgos en seguridad de manera efectiva.

Estas consideraciones resaltan la necesidad de abordar la implementación del plan como un proceso progresivo y adaptable mediante estrategias específicas para superar las limitaciones mencionadas y maximizar su efectividad en el tiempo.

Conclusiones

- El diseño del Plan Director de Seguridad es eficaz y personalizado debido a que se obtiene a partir del enfoque integral para abordar las debilidades en seguridad de la información de la infraestructura tecnológica de UNED. Los controles y políticas propuestos se alinean con las mejores prácticas internacionales respaldadas por un marco de trabajo reconocido y probado como lo es COBIT® 2019.
- La herramienta de diseño COBIT® 2019 permitió obtener un Plan Director de Seguridad que alinea las políticas de seguridad con los objetivos institucionales.
- El Plan Director de Seguridad se debe actualizar y ajustar a medida que evoluciona la tecnología y las amenazas cibernéticas, con el fin de mejorar la gestión de seguridad en la UNED u otras entidades que repliquen el caso.
- La aplicación de COBIT® 2019 a la seguridad de la información de la UNED es una valiosa referencia para otras universidades y organismos académicos análogos, facilitando replicar la metodología utilizada para crear y ajustar un Plan Director de Seguridad a sus necesidades específicas, contribuyendo a la protección de la infraestructura tecnológica virtual y mitigar posibles riesgos en entornos académicos inclusive más complejos.

Recomendaciones

- Se pueden realizar estudios adicionales en un entorno operativo o técnico con los controles propuestos y evaluar la posibilidad de extender el Plan Director de Seguridad a otras áreas de la institución con el fin de adaptarlo a nuevos desarrollos tecnológicos y brindar una mejor protección.
- Es recomendable la adopción de marcos de gobernanza como COBIT® 2019 en otras instituciones públicas o privadas que dependan de infraestructuras virtuales para asegurar una gestión de riesgos eficiente.
- Los indicadores clave de desempeño (KPI) propuestos son una valiosa guía para facilitar la visión de los resultados esperados en un Plan Director de Seguridad en cualquier organización.

Agradecimientos

A la Universidad Estatal a Distancia en Costa Rica y su Consejo de Becas Institucional, por su colaboración y patrocinio de la tesis de maestría que brindó los insumos para este artículo científico, así como a la Mag. Patricia Prandini por su orientación en la dirección de tesis.

Referencias

[1] P. R. Sandoval Barrantes, “Desarrollo de un plan para la gestión de la seguridad de la información de la infraestructura tecnológica virtual y sistemas convergentes en la universidad estatal a distancia de la República de Costa Rica”, Trabajo Final de Posgrado, Univ. de Buenos Aires, CABA, Argentina, 2021. [En línea]. Disponible en: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-2127_SandovalBarrantesPR.pdf

[2] ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, Illinois, EE.UU.: ISACA, 2019.

[3] Incibe. “Plan director de seguridad”. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf. Accedido el 4 de octubre de 2024. [En línea]. Disponible: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf.

[4] ISACA, *COBIT® 2019 Marco de Referencia: Introducción y metodología*, Illinois, EE.UU.: ISACA, 2019.

[5] A. S. M. Arellano, P. R. J. Santana, M. de J. J. Santana, y J. C. F. Valverde, «Aplicación de COBIT® 2019 al gobierno y gestión de las tecnologías de información en instituciones educativas sin fines de lucro», South Florida Journal of Development, vol. 4, n.º 3, pp. 1388–1410, jun. 2023. [En línea]. DOI: https://doi.org/10.46932/sfjdv4n3-027

[6] H. A. Sacón-Klinger, S. Patiño, J. D. Rodríguez Vizuete, A. P. Mora-Olivero, N. Quiñonez Godoy, y R. A. Macías-Lara, “Planificación estratégica de tecnología de la información para la Universidad Técnica Luis Vargas Torres de Esmeraldas, basado en COBIT® 2019,” Sapienza International Journal of Interdisciplinary Studies, vol. 3, no. 1, pp. 1168–1186, 2022. [En línea]. DOI: https://doi.org/10.51798/sijis.v3i1.297

[7] B. D. Tiglla Tumbaico y E. F. Solís Acosta, «Procesos de gobierno basado en COBIT® 2019 para mitigar ataques informáticos», RECIMUNDO, vol. 6, n.º 4, pp. 671–680, nov. 2022. [En línea]. DOI: https://doi.org/10.26820/recimundo/6.(4).octubre.2022.671-680

[8] X. E. Orellana-Cabrera y M. D. Álvarez-Galarza, “Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT® 2019,” Polo del Conocimiento, vol. 7, no. 3, pp. 706–723, marzo 2022. [En línea]. DOI: https://doi.org/10.23857/pc.v7i3.3758

[9] A. R. Cuervo Forero, Importancia del Gobierno TI, Ciberseguridad y Comunidades Digitales, Universidad Piloto de Colombia, ensayo, jul. 24, 2023. [En línea]. Disponible en: https://repository.unipiloto.edu.co/handle/20.500.12277/13076

[10] B. Y. Fitriyani and A. H. Muhammad, “ COBIT® 2019 for Enhanced ICT Governance: A Case Study at a Higher Education Institution,” *Journal of Information Systems and Informatics*, vol. 7, no. 1, pp. 45–48, Mar. 2025. [En línea]. DOI: 10.51519/journalisi.v7i1.972

[11] G. Wattimury and A. Faza, “ COBIT® 2019 Implementation for Enhancing IT Governance in Educational Institutions,” *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 8, no. 3, pp. 210–221, Sep. 2023. [En línea]. DOI: 10.14421/jiska.2023.8.3.210-221

[12] W. Mangoki, D. Manongga, and A. Iriani, “IT Governance Design in XY University using COBIT® 2019 Framework,” *Jurnal Sistem Informasi Bisnis*, vol. 2, pp. 111–122, 2024. [En línea]. DOI: 10.21456/vol14iss2pp111-122

[13] D. Utomo, M. Wijaya, Suzanna, Efendi, and N. T. M. Sagala, “Leveraging COBIT® 2019 to Implement IT Governance in SME Context: A Case Study of Higher Education in Campus A,” *CommIT Journal*, vol. 16, no. 2, pp. 129–141, 2022. [En línea]. DOI: 10.21512/commit.v16i2.8172

[14] R. S. Hidayat, R. E. Indrajit, and E. Dazki, “Evaluation of Information Technology Governance Maturity Using COBIT® 2019: A Case Study on the IT Security Industry,” *Journal La Multiapp*, vol. 5, issue 4, pp. 478–487, 2024. [En línea]. DOI: 10.37899/journallamultiapp.v5i4.1514

[15] A. Bagja, Z. Amri, K. Imtihan, M. Rodi, and S. Y. Rusniatun, “Enhancing Public Sector IT Governance through COBIT® 2019: A Case Study on Service Continuity and Data Management in the Central Lombok,” *Journal of Information Systems and Informatics*, vol. 6, no. 4, pp. 2761–2764, Dec. 2024. [En línea]. DOI: 10.51519/journalisi.v6i4.924

[16] G. Toaza, C. Montenegro, and C. Salazar, “Designing an I&T Governance System in the Context of Strategic Public Sector Based on COBIT 2019 Framework. Case Study in a Developing Country,” *Proc. 5th Int. Conf. on Information Management and Management Science (IMMS 2022)*, Chengdu, China, pp. 401-406, Ago. 2022. [En línea]. DOI: 10.1145/3564858.3564920

[17] E. Amore, T. Dilger, M. Mezzenzana, C. Ploder, and R. Bernsteiner, “Leverage the COBIT® 2019 Design Toolkit in an SME Context: A Multiple Case Study,” *Economies of the Balkan and Eastern European Countries (EBEEC)*, vol. 2023, pp. 73–101, Feb. 2023. [En línea]. DOI: 10.18502/kss.v8i1.12636.

[18] R. Hernández Sampieri, C. Fernández y Pilar Baptista, *Metodología de la Investigación*, Mexico DF: McGraw-Hill, 2006.

[19] ISACA, *COBIT® 2019 Guía de diseño: Diseño de una solución de Gobierno de Información y Tecnología*, Illinois, EE.UU.: ISACA, 2019.

[20] ISACA, *COBIT® 2019 Guía de Implementación: Implementación y optimización de una solución de Gobierno de Información y Tecnología*, Illinois, EE.UU.: ISACA, 2019.

[21] *Sistemas de gestión de la seguridad de la información - Requisitos*, INTE/ISO/IEC 27001:2014, Instituto de Normas Técnicas de Costa Rica, San José, Costa Rica, 2014.

[22] *Código de buenas prácticas para controles de seguridad de la información, INTE/ISO/IEC 27002:2016, Instituto de Normas Técnicas de Costa Rica, San José, Costa Rica, 2016*.

[23] *Técnicas de seguridad – Gobernanza de seguridad de la información*, INTE/ISO/IEC 27014:2016, Instituto de Normas Técnicas de Costa Rica, San José, Costa Rica, 2016.

[24] C. d. R. CONRE-UNED. "ORIENTACIONES GENERALES PARA LA IMPLEMENTACION DEL SISTEMA ESPECIFICO DE VALORACIÓN DE RIESGO INSTITUCIONAL (SEVRI) EN LA UNED". https://www.uned.ac.cr/planificacion/proci/documentos-institucionales. Accedido el 20 de junio de 2025. [En línea]. Disponible: https://www.uned.ac.cr/planificacion/proci/images/VR/Orientaciones_SEVRI_UNED_2023.pdf

[25] ISACA, "CMMI Model Quick Reference Guide CMMI V3.0", 24 de octubre de 2024, CMMI-Model-Quick-Reference-Guide_Digital-1024, Illinois, United States of America, An overview of the Capability Maturity Model Integration (CMMI)® Model. Accedido el 20 de junio de 2025. [En línea]. Disponible en: https://www.isaca.org/resources/reference-guide/cmmi-model-quick-reference-guide

[26] C. U. UNED. "Política de gestión del riesgo y continuidad de los servicios en la UNED". https://www.uned.ac.cr/docencia/cidreb/cidi/normativa-universitaria/politicas-institucionales. Accedido el 20 de junio de 2025. [En línea]. Disponible: https://www.uned.ac.cr/docencia/images/Normativa/Política_gestión_riesgo_continuidad_servicios_UNED_200624.pdf

[27] *Security and resilience – Business continuity management systems – Requirements*, ISO 22301:2019, International Organization for Standardization, 2019.

[28] *Information technology – Service management system requirements (Part 1) – especificación de requisitos para SMS*, ISO/IEC 200001:2018, International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), 2018.

[29] Dirección de Tecnología de Información y Comunicaciones (DTIC), *DTIC UIT F01 Plan para la gestión de la capacidad de la Infraestructura TI*, Unidad de Infraestructura Tecnológica (UIT), Universidad Estatal a Distancia de Costa Rica (UNED), San José, Costa Rica, 13 de febrero de 2025. [Documento interno, no publicado].

Declaración sobre uso de Inteligencia Artificial (IA)

Los autores aquí firmantes declaramos que no se utilizó ninguna herramienta de IA para la conceptualización, traducción o redacción de este artículo.