risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 14/11/2023
Aceitação/Acceptance: 17/02/2024

Auditoría de riesgos de ciberseguridad: Revisión de Literatura, propuesta y aplicación

I.D. Sanchez-Garcia[1], A.M. Rea-Guaman[2], T. San Feliu1 and J.A[1]. Calvo-Manzano[1].

isaacdaniel.sanchez@alumnos.upm.es; amrea1@espe.edu.ec; tomas.sanfeliu@upm.es; joseantonio.calvomanzano@upm.es.

[1] Universidad Politécnica de Madrid, ETS Ingenieros Informáticos Madrid, España.

[2] Universidad de las Fuerzas Armadas – ESPE, Departamento de Ciencias de la Computación Sangolquí, Ecuador.

DOI: 10.17013/risti.53.69–87

Resumen: Una de las etapas de la gestión de riesgos de ciberseguridad es el monitoreo y la revisión. Esta etapa forma parte del proceso de mejora continua de un sistema de gestión de riesgos de ciberseguridad. Este artículo tiene como objetivo llevar a cabo una exploración de una guía de auditoría de riesgos de ciberseguridad, tomando como referencia objetivos comunes y guías de la auditoría de riesgos de ciberseguridad. Para ello se tomó como partida una Revisión Sistemática de Literatura (SLR) considerando los estudios de los últimos diez años (2012-2022), a partir de los cuales se identificaron 23 estudios que mencionaban objetivos y guías de auditoría de riesgos de ciberseguridad. Además, se propusieron atributos que deben ser considerados para la creación de un guía de riesgos de ciberseguridad. Posteriormente, en el presente trabajo se define una guía de auditoría de riesgos de ciberseguridad (CRAG). Finalmente, se expone la aplicación de CRAG por medio de un caso de estudio, considerando los parámetros identificados en los estudios previamente mencionados.

Palabras-clave: Auditoría de ciberseguridad, Guía de auditoría, Aseguramiento, Cumplimiento, Mejora de la ciberseguridad, Monitoreo, Revisión sistemática de literatura, Aplicación.

Cybersecurity Risk Audit: Literature Review, Proposal, and Application

Abstract: One of the stages of cybersecurity risk management is monitoring and review. This stage is part of the continuous improvement process of a cybersecurity risk management system. This article aims to conduct an exploration of a cybersecurity risk audit guide by referencing common objectives and guidelines of cybersecurity risk auditing. To do so, a Systematic Literature Review (SLR) was conducted considering studies from the last ten years (2012-2022), from which 23 studies mentioning cybersecurity risk audit objectives and guidelines were identified. Additionally, attributes to be considered for the creation of a cybersecurity risk guide were proposed. Finally, an application and validation of the identified parameters in the previously mentioned studies are presented.

Keywords: Cybersecurity Audit, Audit Guide, Assurance, Compliance, Cybersecurity Enhancement, Monitoring, Systematic Literature Review, Implementation.

1. Introducción

La norma ISO 27005:2018 establece como marco de referencia para la gestión de riesgos de ciberseguridad cuatro etapas: 1) establecimiento del contexto, 2) evaluación de riesgos, 3) tratamiento de riesgos, 4) monitoreo y revisión. La nominación de estas etapas puede variar según el marco de referencia utilizado. Comúnmente, la etapa de monitoreo y revisión suele cerrar el ciclo de gestión de riesgos de ciberseguridad.

La etapa de monitoreo y revisión de riesgos de ciberseguridad incluye el monitoreo regular de los riesgos y contramedidas definidas en las etapas de evaluación y tratamiento de riesgos. Además, revisiones periódicas (auditorías) son necesarias para un monitoreo adecuado para validar la efectividad de las contramedidas en abordar los riesgos (Slapničar et al., 2022). Este estudio se centrará en los problemas relacionados con las auditorías de riesgos de ciberseguridad, que son parte de la etapa de monitoreo y revisión de riesgos de ciberseguridad.

La evaluación de riesgos de ciberseguridad implica examinar regularmente los mecanismos de seguridad para detectar deficiencias donde no hayan sido diseñados de manera efectiva o no estén operando como se esperaba. Estas evaluaciones pueden abarcar áreas como las aplicaciones de tecnologías de la información, las operaciones de TI, la gobernanza y el personal, todas las cuales son componentes específicos en la implementación de sistemas de información.

El estudio publicado por la Confederación Europea de Institutos de Auditores Internos (ECIIA) (European Confederation of Institutes of Internal Auditors, 2020) resalta la importancia de las auditorías de riesgos de ciberseguridad, colocándolas como la principal preocupación de los Chief Audit Executives (CAE, por sus siglas en inglés). Diversos autores como Slapničar et al., (2022) y Duncan & Whittington, (2014) coinciden en que la auditoría de riesgos de ciberseguridad es un campo relativamente nuevo.

A pesar de su importancia, la auditoría de riesgos de ciberseguridad aún no ha alcanzado un nivel de madurez que pueda ser comparable respecto a otras áreas de auditoría, como lo es la auditoría contable, que se ha venido desarrollando durante décadas. Esta falta de madurez es justificable, pues la ciberseguridad es un campo que está en constante evolución, con nuevos riesgos y amenazas surgiendo continuamente. Autores como Duncan y Whittington (2014) enfatizan en la necesidad de avanzar en este sentido.

Para que la auditoría de riesgos de ciberseguridad alcance un nivel de madurez considerado óptimo, se requiere de una mayor claridad en tres aspectos fundamentales, que son los conceptos, las pruebas y los procedimientos. Estos tres elementos son requeridos para que el correcto funcionamiento de las medidas de seguridad pueda ser validado.

Los desafíos principales, a los cuales se enfrentan las organizaciones al momento de realizar las auditorías de riesgo de ciberseguridad son las siguientes:

a. La constante aparición de nuevas amenazas y vulnerabilidades representan un obstáculo para llevar a cabo auditorías de ciberseguridad.
b. La escasez de profesionales que posean las habilidades y conocimientos para realizar auditorías de riesgo de ciberseguridad es otro problema común. Muchas organizaciones recurren a la ayuda de consultores externos cualificados para tomar decisiones estratégicas en este ámbito (Galligan & Rau, 2015).

Por otro lado, las organizaciones también enfrentan un reto al intentar cumplir con un estándar o guía de auditoría de riesgos de ciberseguridad. De acuerdo con Sabillón et al. (2018), es crucial contar con una orientación clara o un consenso sobre qué áreas, subáreas, dominios o subdominios deben ser considerados en una auditoría de riesgos de ciberseguridad. Un ejemplo que ilustra las dificultades asociadas con los estándares actuales de auditoría de riesgos de ciberseguridad es el estudio realizado por Gauthier & Brender, (2021).

Un estudio realizado por Megan et al. (2022) recopila datos de diversos estudios relacionados con las auditorías de riesgos de ciberseguridad. El estudio revela que las organizaciones, especialmente en países en vías de desarrollo, se encuentran realizando esfuerzos significativos para mejorar la ejecución de estas auditorías.

Aquellas organizaciones que han experimentado problemas de ciberseguridad por la falta de auditorías de riesgos de ciberseguridad han sido las promotoras impulsoras de este cambio, pues han reconocido la importancia de estas auditorias para de esta manera, ser capaces de proteger sus activos de información (Gale, Bongiovanni, & Slapnicar, 2022).

Para ser prácticos, los objetivos de la auditoría de riesgos de ciberseguridad deben estar alineados desde un punto de vista de control interno (Sabillon et al., 2018). Diversos estudios de investigación, como los realizados por Steinbart et al. (2016) y Stafford et al. (2018) han analizado el papel fundamental que juega la auditoría interna en la gestión y gobernanza de riesgos de ciberseguridad. Estos estudios resaltan la importancia de que la auditoría interna se enfoque en evaluar la eficacia del control interno en materia de ciberseguridad.

Gale et al., (2022) recopilan datos de estudios relacionados con auditorías de riesgos de ciberseguridad. Como resultado, Gale et al., (2022) mencionan que las organizaciones están realizando esfuerzos significativos, especialmente en países en desarrollo, para mejorar la ejecución de las auditorías de riesgos de ciberseguridad. Las organizaciones que ya han experimentado problemas de ciberseguridad debido a la falta de auditorías de riesgos de ciberseguridad han trabajado en mejorar la competencia de los comités de auditoría interna e implementar guías prácticas dentro de la organización, definiendo objetivos claros (Gale et al., 2022).

Para ser prácticos, los objetivos relacionados con la auditoría de riesgos de ciberseguridad deben ser vistos desde un punto de vista de control interno (Sabillon et al., 2018). Algunos estudios de investigación (por ejemplo, (Steinbart et al., 2016); (Stafford et al., 2018)) han analizado el papel de la auditoría interna en la gestión y gobernanza de riesgos de ciberseguridad.

Los esfuerzos actuales para abordar las auditorías de riesgos de ciberseguridad se basan en el uso de guías y marcos de referencias conocidos. Entre las guías más utilizadas se

encuentran la familia ISO 27000, específicamente la ISO/IEC 27005 (2018), el NIST Cybersecurity Framework (CSF) (National Institute of Standards and Technology, 2018) y Control Objectives for Information and Related Technologies (COBIT) (ISACA, 2018). Para implementar efectivamente estas guías, es necesario integrar estos conceptos al campo del control interno para abordar la ciberseguridad de manera integral, no solo considerando los aspectos técnicos, sino también los procesos y las personas involucradas (Islam, Farah, & Stafford, 2022).

Según Ezzamouri & Hulstijn (2018), una auditoría de riesgos de ciberseguridad realizada con la guía adecuada permite a los auditores ofrecer una garantía razonable sobre la criticidad e impacto potencial de un riesgo. Esta garantía se basa en la evaluación de la efectividad de las contramedidas implementadas para mitigar dicho riesgo. Los resultados obtenidos de esta auditoría de riesgos de ciberseguridad se plasman en un informe de auditoría. El monitoreo continuo suele ser responsabilidad de la dirección, ya que afecta a los controles internos integrados en los procesos tecnológicos de la empresa.

Derivado de esta problemática relacionada con la auditoría de riesgos de ciberseguridad se decidió realizar una Revisión Sistemática de la Literatura (SLR, por sus siglas en inglés) utilizando como guía a Kitchenham et al., (2009) presentada en la sección 2. En la sección 3 se presenta la Guía de Auditoría de Riesgos de Ciberseguridad (CRAG, por sus siglas en inglés)

Se seleccionó la Técnica Estructurada de Análisis y Diseño (SADT) de Congram & Epelman, (1995) para su desarrollo. En la sección 4 se presenta validación de la guía CRAG, esta validación se realizó por medio de un caso de estudio. Finalmente, en la sección 5 se presentan las conclusiones y líneas de investigación futuras.

Las contribuciones de este trabajo de investigación serán:

1. Establecer objetivos comunes aplicables a las auditorías de riesgos de ciberseguridad.
2. Discutir las contribuciones y beneficios de las guías de auditoría de riesgos de ciberseguridad.
3. Realizar una propuesta de guía de auditoría de riesgos de ciberseguridad.
4. Realizar la validación de la guía previamente propuesta por medio de la aplicación de un caso de estudio.

2. Revisión sistemática de literatura

La metodología propuesta por B. Kitchenham fue seleccionada para llevar a cabo esta Revisión Sistemática de la Literatura (SLR, por sus siglas en inglés) (Kitchenham et al., 2009). La SLR es un proceso formal y verificable que el investigador realiza para documentar el estado del conocimiento sobre un tema en particular. Según B. Kitchenham, una revisión sistemática evalúa e interpreta toda la investigación disponible relevante para una pregunta de investigación dada en el área temática o fenómeno de interés (Fernandez et al., 2015). Esta SLR incluye los siguientes pasos: (1) Proponer un protocolo de revisión y definir las preguntas de investigación, (2) Realizar la revisión (identificar estudios primarios y evaluar estos estudios), (3) Extraer y discutir los resultados de la revisión sistemática de la literatura.

2.1. Proponer un protocolo de revisión y definir las preguntas de investigación

Pregunta de Investigación 1 (RQ1): ¿Qué objetivos se utilizan en las auditorías de riesgos de ciberseguridad según la literatura?

Con el propósito de responder la pregunta de investigación RQ1, se identificarán los objetivos primordiales de las auditorías de riesgos de ciberseguridad que se encuentran plasmados en la literatura existente. Asimismo, estos objetivos serán clasificados según su enfoque específico (auditoría interna, seguridad de la información o ciberseguridad) con la finalidad de delimitar el conjunto de aquellos aplicables a la ciberseguridad. La formulación de la RQ1 se fundamenta en el objetivo a) identificar los principales objetivos de las auditorías de riesgos de ciberseguridad.

Pregunta de Investigación 2 (RQ2): ¿Cuáles son las pautas más utilizadas en la literatura sobre auditorías de riesgos de ciberseguridad y sus características?

El propósito fundamental de la RQ2 consiste en identificar las directrices, estándares, marcos o modelos que guarden relación con las auditorías de riesgos de ciberseguridad. Adicionalmente, persigue el objetivo de detectar tendencias o brechas en las mencionadas pautas y estándares. La formulación de la RQ2 se basa en el objetivo b) identificar y analizar las pautas de auditoría de riesgos de ciberseguridad.

2.1.1. Protocolo PICO

El protocolo PICO (población, intervención, comparación y resultado), establecido en el modelo de Kitchenham et al. (2009), el cual ha sido ampliamente utilizado y extensamente probado en la ejecución de revisiones sistemáticas de la literatura, fue seleccionado para su implementación en nuestro estudio.

- Población: Se consideran las publicaciones relacionadas con los objetivos de las auditorías de riesgos de ciberseguridad. Además, también se toman en cuenta las pautas vinculadas con las auditorías de riesgos de ciberseguridad.
- Intervención: Los estudios de investigación mencionan diferentes objetivos y pautas relacionados con las auditorías de riesgos de ciberseguridad.
- Comparación: Identificar y comparar objetivos y pautas relacionadas con las auditorías de riesgos de ciberseguridad mencionadas por las publicaciones.
- Resultado: Objetivos de las auditorías de riesgos de ciberseguridad, frecuencia y enfoque de las pautas de auditoría de riesgos de ciberseguridad.

2.1.2. Generación de cadena de búsqueda de investigación

Se ha llevado a cabo una cuidadosa selección de un conjunto de palabras clave con el objetivo de obtener los resultados más relevantes posibles. Con la finalidad de evitar la exclusión de estudios pertinentes y construir la cadena de búsqueda de manera eficiente, se han incluido sinónimos para las palabras clave. Dichos sinónimos, así como las palabras clave, se encuentran detallados en la Tabla 1.

Las cadenas de búsqueda han sido construidas utilizando las palabras clave y sus respectivos sinónimos presentes en la Tabla 1. Se han añadido los conectores lógicos

"AND" y "OR" para unir las palabras clave y sinónimos, dando lugar a la siguiente cadena de búsqueda genérica: ("Auditoría" OR "Aseguramiento" OR "Guía" OR "Ley" OR "Estándar") AND ("Ciberseguridad" OR "Seguridad Cibernética" OR "Seguridad de la Información").

Palabra Clave	Sinónimos
Cybersecurity	Cyber security, Information security
Audit	Assurance, Guide, Law, Standard

Tabla 1 – Palabras clave y sinónimos para construir las cadenas de investigación

2.2. Realizar la revisión

Los criterios establecidos para la selección de fuentes (bases de datos) se fundamentaron en: a) la experiencia reportada por Dyba et al. (2007), y Petersen et al. (2008); b) la disponibilidad de estudios de texto completo encontrados a través de las cadenas de búsqueda; c) estudios disponibles en la web de forma gratuita; y d) revistas especializadas en ciberseguridad accesibles en la biblioteca de la Universidad Politécnica de Madrid. Las fuentes seleccionadas para esta Revisión Sistemática de Literatura son 1) ACM Digital Library, 2) IEEE Digital Library, 3) ISI Web of Science, 4) ScienceDirect, 5) Scopus y 6) Springer Link. Google Scholar fue seleccionado únicamente para aplicar la técnica de bola de nieve.

La cadena de búsqueda definida en la sección anterior fue introducida en los motores de búsqueda de las fuentes mencionadas.

2.2.1. Criterios de inclusión y exclusión

Es necesario definir criterios de inclusión y exclusión (I&E) con el propósito de seleccionar los estudios relacionados con la Revisión Sistemática de Literatura. Los criterios de I&E fueron definidos en base a la experiencia de Kitchenham et al. (2009), y Petersen et al. (2008). La selección de estudios se ha llevado a cabo utilizando los siguientes criterios de I&E.

Criterios de inclusión:

- Bibliotecas digitales precisas: Se evaluó la calidad, cantidad y confiabilidad de los estudios publicados en siete bibliotecas digitales (seleccionadas según los criterios establecidos para la selección de fuentes).
- Contenido de los estudios: Se constató que el tema principal de los estudios identificados estaba relacionado con las preguntas de investigación PI1 y PI2. Para este análisis, se validaron el título, el resumen y las palabras clave de los estudios.
- Coherencia del estudio: Se confirmó que los estudios estuvieran relacionados con el campo de la ciberseguridad. Para ello, se identificaron el área y el título de los estudios, asegurando su coherencia con los objetivos de la Revisión Sistemática de Literatura.

- Estudios de texto completo: Se revisaron todos los estudios identificados en las bibliotecas digitales, validando la integridad de la información. De esta manera, únicamente se incluyeron estudios completos.

Criterios de exclusión:

- Estudios duplicados: Se eliminaron los estudios duplicados presentes en las diferentes bibliotecas digitales. Este criterio de exclusión tiene como finalidad reducir el volumen de información innecesaria.
- Estudios basados únicamente en una opinión particular: Se excluyeron los estudios que solo mencionaban una opinión particular. Este criterio de exclusión busca contar con estudios basados en hipótesis científicas validadas.
- Estudios anteriores a 2012: Debido a la continua actualización del campo de la ciberseguridad, se excluyeron los estudios previos a 2012. Por lo tanto, la información de un estudio anterior a 2012 se consideraría irrelevante para esta Revisión Sistemática de Literatura.
- Estudios irrelevantes para las preguntas de investigación o no relacionados con el tema: También se excluyeron los estudios no relacionados con ninguna de las preguntas de investigación PI1 y PI2.
- Estudios poco claros o ambiguos: Se descartaron los estudios que no aclaraban sus contribuciones o no especificaban su relación con la ciberseguridad.
- Estudios que mencionan auditoría de riesgos, pero no en el campo de la ciberseguridad: Se descartaron los estudios que mencionaban pautas de auditoría relacionadas con áreas distintas de la ciberseguridad.
- Literatura gris, o literatura publicada por editores no tradicionales: Este tipo de literatura fue excluido.

2.3. Selección de estudios primarios

La selección de los estudios primarios se ha dividido en un procedimiento compuesto por tres actividades. Se creó un conjunto de datos para realizar estas actividades (ver https://short.upm.es/xljfp). Este conjunto de datos contiene los resultados de las tres actividades.

En la primera actividad, se insertó la cadena de búsqueda creada en el protocolo de revisión en los motores de búsqueda de la base de datos. Después de la primera actividad, se encontraron 2,032 estudios. Los resultados se presentan en la Tabla 2.

Fuente	Estudios iniciales (Primera actividad)	Estudios relevantes (Segunda actividad)	Estudios primarios Tarea 1 (Tercera actividad)	Estudios primarios-Tarea 2 (Tercera actividad)
ACM Digital Library (ACM)	464	12	4	4
IEEE Digital Library (IEEE)	107	24	7	7
ISI Web of Science (WOS)	61	9	2	2
Springer Link (SP)	1015	33	3	3

Fuente	Estudios iniciales (Primera actividad)	Estudios relevantes (Segunda actividad)	Estudios primarios Tarea 1 (Tercera actividad)	Estudios primarios-Tarea 2 (Tercera actividad)
Science Direct (SD)	53	1	0	0
Scopus (SC)	332	13	4	4
Google Scholar (GS)	0	0	0	3
Total	2032	92	20	23

Tabla 2 – Distribución de estudios por fuentes

Posteriormente, en la segunda actividad se aplicaron los criterios de exclusión (criterios de I&E), leyendo el título, el resumen y las palabras clave. Se encontraron y excluyeron 63 estudios duplicados. Después de aplicar los criterios de I&E, se excluyeron 1,877 estudios adicionales por no ser relevantes para responder las preguntas de investigación. Un total de 92 publicaciones se consideraron relevantes. Todos los resultados se muestran en el conjunto de datos del proceso de RSL (consultar https://short.upm.es/xljfp para obtener más información).

En la tercera actividad, se seleccionaron los estudios basándose en lo siguiente:

- Tarea 1, leyendo el texto completo. Si el estudio proporcionaba suficiente información, entonces se seleccionaba y se guardaba.
- Tarea 2, se aplicó una búsqueda adicional utilizando la técnica de bola de nieve descrita por C. Wohlin (2014). Como resultado, se agregaron dos estudios adicionales.

Después de aplicar la tercera actividad, se rechazaron 72 estudios y se aceptaron tres estudios de navegadores de Internet, obteniendo así 23 estudios aceptados después de la tercera actividad.

2.3. Extraer y discutir los resultados de la revisión sistemática de la literatura

Tras analizar los estudios primarios, se identificó que podrían clasificarse según los objetivos que debe cumplir la auditoría de riesgos de ciberseguridad. Para establecer la relación entre estos objetivos, resulta conveniente clasificar los conceptos y objetivos en cuatro objetivos principales, tomando como referencia el trabajo de Duncan et al. (2014).

Este trabajo encontró que los cuatro objetivos de la auditoría de riesgos de ciberseguridad se encuentran estrechamente relacionados, debido a que el proceso de auditoría de riesgos de ciberseguridad debe mejorarse además de realizar una evaluación, medir el cumplimiento y validar la garantía.

Figura 1 – Objetivos de auditoría de riesgos de ciberseguridad

Tras analizar los cuatro objetivos de la auditoría de riesgos de ciberseguridad, se determinó que se encuentran interrelacionados (ver Figura 1). Por ejemplo, uno de los objetivos de una auditoría es realizar una revisión para garantizar la efectividad de un sistema de gestión. Además, según el Diccionario Oxford de inglés, una auditoría es "un examen oficial de la calidad o estándar de algo", por lo que una auditoría puede estar relacionada tanto con la garantía como con el cumplimiento de un estándar o regulación. El objetivo final de una auditoría de un sistema de gestión de ciberseguridad es mejorar el estado actual de la ciberseguridad.

Resumiendo, los resultados de esta sección, dentro de los conceptos relacionados con la ciberseguridad centrados en la realización de auditorías de riesgos, se identificó que los autores mencionan los objetivos "Evaluación", "Garantía", "Cumplimiento" y "Mejorar la Ciberseguridad". Estos objetivos están interrelacionados, ya que constituyen los pilares fundamentales de las auditorías de riesgos de ciberseguridad.

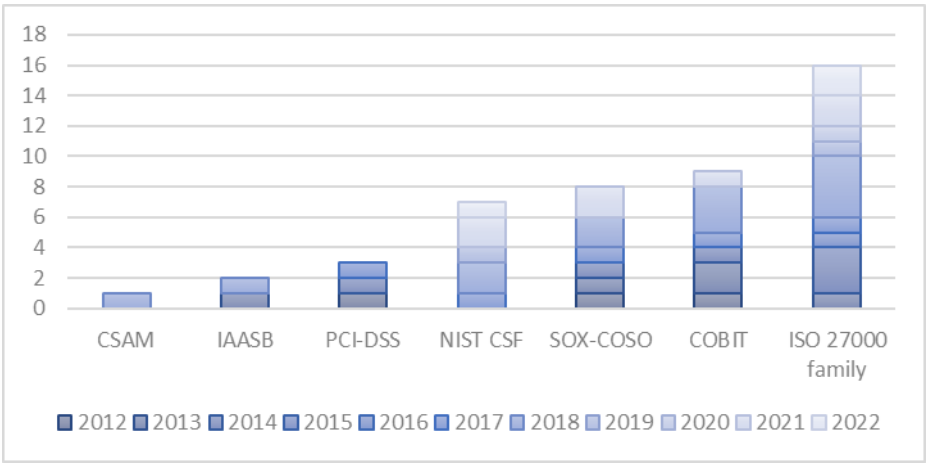

Figura 2 – Frecuencia de las guías de Auditoría de Ciberseguridad identificadas por año

Adicionalmente, se identificaron las siete guías utilizadas con mayor amplitud para las auditorías de riesgos de ciberseguridad: 1) la familia ISO 27000, 2) COBIT, 3) SOX-COSO, 4) NIST CSF, 5) PCI-DSS, 6) IAASB y 7) CSAM. De las guías previamente identificadas, solo el NIST CSF y el CSAM fueron creadas explícitamente para el ámbito de la ciberseguridad. Además, según los autores, el enfoque de las guías de auditoría de riesgos de ciberseguridad puede clasificarse en aquellas que se centran en procesos, tecnología o a nivel estratégico. (Véase Figura 2).

Una observación interesante es que se han identificado dos tendencias distintas en la investigación primaria. En primer lugar, algunos autores utilizan guías de auditoría centradas en el nivel estratégico sin considerar el componente técnico, y por otro lado, otros autores emplean guías de auditoría con un enfoque técnico sin considerar el enfoque estratégico. Estas dos tendencias demuestran la necesidad de complementarse mutuamente de manera equitativa para evaluar el sistema de gestión de ciberseguridad de manera objetiva y práctica.

3. Guía de riesgos de ciberseguridad propuesta

La guía Cybersecurity Risk Audit Guideline (CRAG) fue desarrollada considerando estándares internacionales tanto para ciberseguridad como para control interno. El propósito de la guía CRAG es abordar las auditorías de riesgos de ciberseguridad, teniendo en cuenta aspectos más allá de los técnicos y tradicionales.

La creación de la guía CRAG utilizó SADT como punto de partida, incorporando las fases de auditoría de control interno definidas en COSO ERM y complementándolas con las etapas de gestión de riesgos de seguridad propuestas por ISO 27001, adicionalmente se utilizó de referencia los modelos CSAM y NIST que son los que fueron identificados en la SLR (sección 2) como los utilizados para auditorías de riesgos de ciberseguridad.

3.1. SADT aplicado para crear la guía CRAG

Para la creación de la guía CRAG, se consideraron las siguientes fases (figura3), teniendo en cuenta y utilizando SADT:

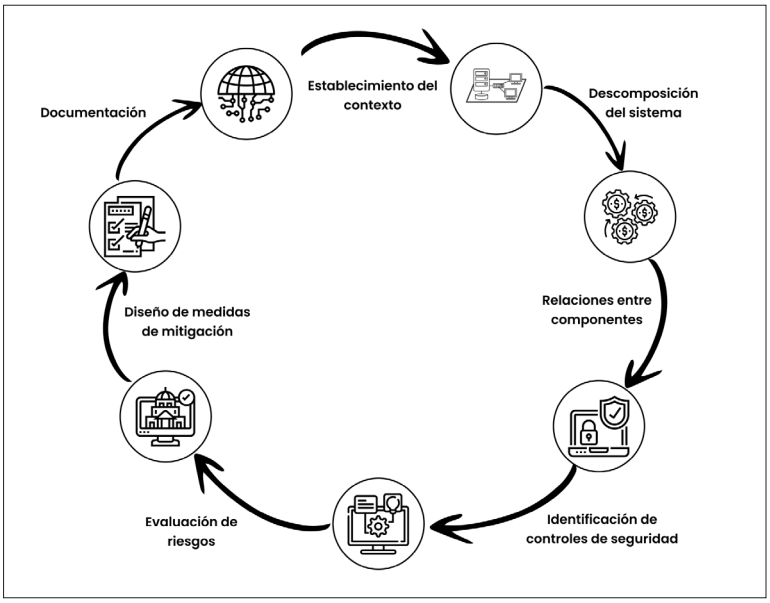

Figura 3 – Fases de la guía de auditoría CRAG

3.2. SADT Model Applied to Create CRAG Guideline

Para la creación de la guía CRAG, se consideraron las siguientes fases, teniendo en cuenta y utilizando SADT:

3.2.1. Establecimiento del contexto: Identificar el contexto de la auditoría de riesgos de ciberseguridad, considerando estándares y regulaciones aplicables. Dentro de esta fase de consideran las siguientes actividades:

- Establecer el alcance de la auditoría: Se definen los límites y la extensión de la auditoría.
- Identificar los objetivos de la auditoría: Se establecen los propósitos y objetivos de la auditoría.
- Identificar estándares y marcos de referencia: Se identifican los estándares y marcos que se utilizarán como base para evaluar los controles de ciberseguridad.
- Seleccionar una metodología de auditoría: Se define el enfoque y los métodos que se utilizarán durante la auditoría.
- Definir un equipo de auditoría: Se establece quiénes serían los miembros del equipo de auditoría.

3.2.2. Descomposición del sistema: Desglosar el sistema de ciberseguridad en sus principales componentes, como infraestructura tecnológica, activos de información, procesos comerciales y políticas de seguridad. Identificar áreas clave que deben evaluarse durante la auditoría. Estas áreas se definirán en función de clasificaciones generales de estándares como ISO 27001, NIST CSF (Ver Figura 3).

- Identificar la infraestructura tecnológica: Este componente se refiere al hardware, software e infraestructura de red que respalda los sistemas de información de una organización.
- Identificar los activos de información: Los activos de información abarcan los datos e información que una organización recopila, procesa, almacena y transmite.
- Identificar los procesos comerciales: Los procesos comerciales representan los flujos de trabajo, procedimientos y actividades que una organización lleva a cabo para alcanzar sus objetivos.
- Identificar las políticas de seguridad: Las políticas de seguridad establecen las reglas, pautas y mejores prácticas que rigen el enfoque de una organización hacia la ciberseguridad.
- Identificar las contramedidas de seguridad: Los controles de seguridad son las medidas técnicas y procedimentales implementadas para proteger los sistemas y datos de la organización.
- Identificar el plan de respuesta ante incidentes: Un plan de respuesta ante incidentes describe los pasos a seguir en caso de un incidente de ciberseguridad.
- Identificar los programas de concientización y entrenamiento en seguridad: El elemento humano es un componente crítico de un sistema de ciberseguridad.

***3.2.3. Relaciones entre componentes*:** Determinar las interacciones y relaciones entre los componentes del sistema de ciberseguridad. Por ejemplo, cómo los activos de información están protegidos por controles de seguridad física definidos en políticas y procedimientos (Dyba et al., 2007) (Ver Figura 3).

- Identificar las relaciones entre los componentes previamente identificados: Las relaciones se establecen cuando existen dependencias entre más de un componente que necesita ser asegurado.
- Clasificar las relaciones según su criticidad: Establecer una calificación de criticidad considerando los posibles impactos si el proceso crítico respaldado por los componentes evaluados deja de funcionar o experimenta una falla de seguridad.

3.2.4. Identificación de Controles de Seguridad: Establecer cómo diferentes controles se relacionan con los componentes del sistema y contribuyen a mitigar los riesgos de ciberseguridad.

- Identificar al responsable de la contramedida: Definir a la persona responsable de la gestión y ejecución del control.
- Definir la Frecuencia de la Contramedida: Establecer cuántas veces se ejecuta el control dentro de un período de tiempo determinado.
- Identificar Dependencias con la Contramedida: Identificar si el control tiene

alguna dependencia con la ejecución de un proceso o control.
- Definir la Granularidad: Aclarar si el control opera de manera uniforme en toda la organización o si existen variaciones en su ejecución.
- Mantener la Integridad y Precisión: En el caso de la información utilizada para la ejecución del control (informes y registros), se debe considerar la integridad y precisión de los informes.

3.2.5. Evaluación de Riesgos: Evaluar los riesgos de ciberseguridad asociados con cada componente del sistema, considerando los controles de seguridad identificados y los requisitos de los estándares aplicables. Determinar el impacto y la probabilidad de ocurrencia de los riesgos identificados (Ver Figura 3).

- Recopilar muestras: Las muestras se utilizan para evaluar y obtener evidencia sobre una población o conjunto de datos más grande.
- Evaluar la efectividad operativa: La efectividad operativa de una contramedida se refiere a su capacidad para cumplir su propósito y lograr resultados deseados en el ámbito de la seguridad.
- Identificar desviaciones: El proceso de detectar discrepancias o irregularidades entre la información examinada y los estándares, políticas, leyes o regulaciones aplicables.
- Identificar observaciones: Las observaciones de control son hallazgos o resultados identificados durante una auditoría que indican deficiencias en los controles internos de una organización.
- Evaluar la probabilidad de fallo de la contramedida: La probabilidad de fallo de una contramedida se refiere a la posibilidad de que una contramedida no funcione como se espera o no sea efectiva para mitigar o contrarrestar una amenaza o riesgo específico.
- Evaluar el impacto de la materialización del riesgo: La evaluación del impacto del riesgo tiene como objetivo evaluar las posibles consecuencias o efectos negativos que podrían ocurrir si un riesgo se materializa.

3.2.6. Diseño de Medidas de Mitigación: Establecer acciones correctivas y preventivas para reducir los riesgos a un nivel aceptable (Ver Figura 3).

- Establecer planes de acción: El objetivo principal del plan de acción es abordar las deficiencias identificadas, implementar medidas correctivas y mejorar los procesos y controles internos de la organización.
- Monitorear planes de acción: El monitoreo de los planes de acción de la auditoría es crucial para garantizar que las acciones correctivas se implementen de manera efectiva y que las deficiencias identificadas se resuelvan.
- Finalizar planes de acción: El cierre del plan de acción de la auditoría se realiza una vez que todas las acciones correctivas han sido implementadas y las deficiencias identificadas en la auditoría han sido abordadas.

3.2.7. Documentación: Documentar los resultados de la auditoría de riesgos de ciberseguridad. Esto puede incluir la creación de diagramas que muestren la estructura del sistema de ciberseguridad, los riesgos identificados, los controles de seguridad recomendados y las medidas de mitigación propuestas (Ver Figura 3).

4. Validación de la guía CRAG

Para llevar a cabo esta sección, decidimos aplicar un caso de estudio, tomando como referencia el trabajo de Yin (2018), que proporciona pautas para la realización de casos de estudio. Utilizamos como objeto de estudio un proceso de ciberseguridad en un banco internacional. La estructura del banco objeto de estudio está compuesta por 115.000 empleados y más de 89 millones de clientes a nivel mundial. Por lo tanto, el caso de estudio se limitará a la sede corporativa de México, que cuenta con 10.001 empleados con sede en la Ciudad de México.

El estudio de caso se llevó a cabo desde el noviembre de 2023, hasta el 30 de marzo de 2024. Comenzó con la presentación y mención de que la aplicación de este caso de estudio tenía propósitos puramente académicos y se centró en uno de los procesos de un departamento en el campo de la ciberseguridad.

Debido a su importancia en las revisiones de estados financieros por auditores externos, auditores internos y reguladores, el proceso seleccionado estaba relacionado con el ciclo de vida del usuario y era gestionado por el departamento de Gestión de Identidad y Acceso (IAM, por sus siglas en inglés).

El self risk assessment consiste en una evaluación independiente del control interno que no es formalmente una auditoría con el fin de identificar la madurez de los controles. Para la aplicación del caso de uso se propuso realizar por el área de control interno un "self risk assessment" (International Organization for Standardization, 2018).

Para esta autoevaluación se consideró la metodología de evaluación de la primera y segunda línea de defensa de la organización incorporando las fases y actividades de CRAG. Es relevante aclarar que CRAG no tiene por intención sustituir ninguna metodología de auditorías o evaluaciones internas de los controles de riesgos de ciberseguridad, el objetivo de CRAG es servir de guía para robustecer y facilitar la ejecución de auditorías de riesgos de ciberseguridad.

		Formulario CRAG
Establecimiento del contexto	Establecer el alcance de la auditoría:	
	Identificar los objetivos de la auditoría:	
	Identificar estándares y marcos de referencia:	
	Seleccionar una metodología de auditoría:	
	Definir un equipo de auditoría:	
Descomposición del sistema	Identificar la infraestructura tecnológica:	
	Identificar los activos de información:	
	Identificar los procesos comerciales:	
	Identificar las políticas de seguridad	
	Identificar las contramedidas de seguridad	
	Identificar el plan de respuesta ante incidentes	
	Identificar los programas de concientización y entrenamiento en seguridad:	
Relaciones entre componentes:	Identificar las relaciones entre los componentes previamente identificados	
	Clasificar las relaciones según su criticidad:	
Identificación de Controles de Seguridad:	Identificar al responsable de la contramedida	
	Definir la Frecuencia de la Contramedida	
	Identificar Dependencias con la Contramedida	
	Definir la Granularidad:	
	Mantener la Integridad y Precisión:	

Figura 4 – Formulario fases y actividades CRAG

Para ello, la oficina del chief information security officer (CISO) llenó un formulario (disponible en el siguiente enlace: https://short.upm.es/xb9e4) relacionado cada fase y

sus actividades ver figura 4. Este formato sirve como evidencia del informe de auditoría y resumen ejecutivo de la auditoría. El objetivo del formato es validar la correcta diferenciación de cada una de las fases y la aplicación de cada una de las actividades.

Una vez llenado el formulario (formulario completado disponible en el siguiente enlace: https://short.upm.es/r7gk0) se identificaron de un total de 20 aplicaciones en el alcance un total de 30 controles con un total de 3 fallos o desviaciones en el diseño del control (monitorización y gestión de cuentas privilegiadas de plataformas) y un total de 17 fallas en la eficacia operativa del control (bajas, bloqueos certificación y segregación de funciones de usuarios/perfiles).

Posteriormente de la implementación de la guía de auditoría CRAG el CISO identificó dentro de los tiempos invertidos para el self assessment un incremento de 1 semana a 2 semanas en la planeación del risk assessment por la utilización de la guía CRAG. A pesar del incremento en el tiempo de planeación el CISO validó que la ejecución del self assessment fue más practica por la incorporación de actividades definidas y que este se alineaba con los pasos utilizados en la metodología tradicional utilizada por la institución en las revisiones de control interno.

5. Conclusiones

En este se estudio ha demostrado que los autores de los estudios referenciados mencionan a la auditoría de ciberseguridad sin tomar en consideración los conceptos asociados ni los objetivos mínimos. Además, la auditoría de ciberseguridad está aún en sus inicios y le queda camino por recorrer antes de alcanzar la madurez necesaria. Otro punto mencionado en los estudios referidos indica que, dado las auditorías de TI, y especialmente las de ciberseguridad, no están tan estrictamente supervisadas como las auditorías contables, se cuestiona su efectividad.

Este estudio ha encontrado que en general, el cumplimiento, el aseguramiento y la auditoría son conceptos diferentes dentro de la ciberseguridad. Debido al costo que implica contratar especialistas en estos temas, los responsables de la aplicación de las directrices de auditoría intentan controlar el problema, limitándose a un ejercicio de marcar casillas. Siendo una actividad que no engloba el escenario real de una auditoría.

En 17 de los 23 estudios de auditoría analizados, los objetivos definidos que conforman la auditoría de riesgos de ciberseguridad: “Evaluar”, “Aseguramiento”, “Cumplimiento” y “Mejora de la ciberseguridad”. Como resultado de la relación identificada entre los objetivos, se considera que podría desarrollarse una nueva línea de investigación para establecer la viabilidad de desarrollar una guía de auditoría que cubra estos temas.

Actualmente, hay pocas directrices de auditoría enfocadas específicamente en los requisitos de ciberseguridad. Los modelos CSF (Cybersecurity Framework) y CSAM (Cybersecurity Assessment and Management) del NIST han sido los únicos identificados en esta investigación como directrices para auditar la madurez y eficacia de los mecanismos de mitigación de riesgos de ciberseguridad.

Adicionalmente se realizó una propuesta tomando como referencia las guías identificadas en la SLR, la cual se denominó Cibersecurity Risk Audit Guideline (CRAG). Esta guía

para realización de auditorías de riesgos de ciberseguridad se desarrolló considerando las 3 fases de la auditoría definidas por lo estudios primarios de la SLR 1) Establecimiento del contexto, 2) Realización de la auditoría y 3) preparación del informe de auditoría.

Para esto SDTA fue utilizado para obtener un total de 7 fases que deben ser consideradas en la auditoría de riesgos de ciberseguridad. De las cuales se desprenden un total de 28 actividades.

Igualmente, al desarrollar un caso de estudio se diseñó un formulario que sirva de punto inicial como una guía donde se documente la auditoría de riesgos de ciberseguridad. El objetivo del formulario es obtener un punto de partida para recoger opiniones y comentarios de diferentes organizaciones para poder consolidar una guía eficiente para la realización de riesgos de ciberseguridad.

5.1. Limitaciones del presente trabajo de investigación

Una limitación o sesgo potencial es la dificultad para comparar y obtener puntos de referencia comunes para las directrices que tienen enfoques tan diferentes, como las directrices de control interno, las directrices de seguridad de la información y las directrices de ciberseguridad.

Se recomienda la guía CRAG para evaluar contramedidas específicas de ciberseguridad, ya que al aplicarla a contramedidas creadas para otra área posible, podría no tener en cuenta las necesidades específicas de esta área (por ejemplo, riesgos de calidad, etc.).

Una de las limitaciones del presente trabajo es realizar a una mayor escala la validación del caso de estudio de CRAG para la identificación de mejoras y validación correcta de la eficiencia de esta guía.

Otra limitación puede ser la omisión de algún parámetro o características relevantes consideradas en las guías tomadas como referencia, para la creación de CRAG. Para ello se propone realizar un modelo de comparación y análisis extendido de todas las características recogidas en las guías para auditorías de riesgos de ciberseguridad.

Se propone como trabajo futuro realizar una comparativa y extracción de parámetros, conceptos y características de las guías para auditorías de riesgos de ciberseguridad. Adicionalmente relacionar los comentarios e información en formatos llenados por los CISO´s de diferentes organizaciones y utilizar esta información para identificar patrones o relaciones entre actividades, conceptos y características para poder establecer algún parámetro cuantitativo que ayude en la ejecución de las auditorías de riesgos de ciberseguridad.

Referencias

Congram, C., & Epelman, M. (1995). How to describe your service. International Journal of Service Industry Management, 6(2), 6–23. https://doi.org/10.1108/09564239510084914

Duncan, B., & Whittington, M. (2014). Compliance with standards, assurance and audit: Does this equal security? ACM International Conference Proceeding Series, 2014-September, 77–84. https://doi.org/10.1145/2659651.2659711

Dyba, T., Dingsoyr, T., & Hanssen, G. K. (2007). Applying Systematic Reviews to Diverse Study Types: An Experience Report. First International Symposium on Empirical Software Engineering and Measurement (ESEM 2007), 225–234. https://doi.org/10.1109/ESEM.2007.59

European Confederation of Institutes of Internal Auditors. (2020). "Risk in focus 2021. Hot topics for internal auditors." Available at: Https://Www.Eciia.Eu/Wp-Content/Uploads/2020/09/100242-RISK-IN-FOCUS-2021-52PP-ECIIA-Online-V2.Pdf.

Ezzamouri, N., & Hulstijn, J. (2018). Continuous monitoring and auditing in municipalities. Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, 1–10. https://doi.org/10.1145/3209281.3209301

Fernandez, A., Black, J., Jones, M., Wilson, L., Salvador-Carulla, L., Astell-Burt, T., & Black, D. (2015). Flooding and mental health: A systematic mapping review. In PLoS ONE (Vol. 10, Issue 4). Public Library of Science. https://doi.org/10.1371/journal.pone.0119929

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. Computers & Security, 121, 102840. https://doi.org/10.1016/j.cose.2022.102840

Galligan, M. E., & Rau, K. (2015). COSO in the cyber age.

Gauthier, M. P., & Brender, N. (2021). How do the current auditing standards fit the emergent use of blockchain? Managerial Auditing Journal, 36(3), 365–385. https://doi.org/10.1108/MAJ-12-2019-2513

Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: a case study. Journal of Supercomputing, 74(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2

Islam, Md. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function. Managerial Auditing Journal, 33(4), 377–409. https://doi.org/10.1108/MAJ-07-2017-1595

Information Systems Audit and Control Association. (2018). COBIT 2019. www.isaca.org/COBIT

International Organization for Standardization. (2018). ISO IEC 27000 2018 Information technology - Information security Management systems - Overview and vocabulary (pp. 1–26).

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering - A systematic literature review. In Information and Software Technology (Vol. 51, Issue 1, pp. 7–15). Elsevier B.V. https://doi.org/10.1016/j.infsof.2008.09.009

National Institute of Standards and Technology. (2018). NIST cybersecurity framework. Proceedings of the Annual ISA Analysis Division Symposium, 535, 9-25.

Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. Information and Software Technology, 64, 1–18. https://doi.org/10.1016/j.infsof.2015.03.007

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2018). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In Proceedings - 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017 (pp. 253–259). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/INCISCOS.2017.20

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548. https://doi.org/10.1016/j.accinf.2021.100548

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. Managerial Auditing Journal, 33(4), 410–424. https://doi.org/10.1108/MAJ-07-2017-1596

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. International Journal of Accounting Information Systems, 13(3), 228-243. https://doi.org/10.1016/j.accinf.2012.06.007

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An Instrument for Evaluating the Effectiveness of Enterprise Information Security Programs. Journal of Information Systems, 30(1), 71–92. https://doi.org/10.2308/isys-51257

Yin, R. K. (2018). Case Study Research and Applications (Sixth Edition). SAGE Publications India Pvt. Ltd. https://lccn.loc.gov/2017040835