INNOVA Research Journal, ISSN 2477-9024
(Septiembre-Diciembre 2020). Vol. 5, No.3.2 pp. 196-213
DOI: https://doi.org/10.33890/innova.v5.n3.2.2020.1608
URL: http://revistas.uide.edu.ec/index.php/innova/index
Correo: innova@uide.edu.ec

Activos informáticos: un referente en la caracterización de procesos de la gestión riesgos de TI

IT assets: a benchmark in the characterization of IT risk management processes

Alejandra Mercedes Colina Vargas
https://orcid.org/0000-0003-1514-8852
Universidad ECOTEC, Ecuador

José J. Túa Ollarves
https://orcid.org/0000-0001-5054-5920
Universidad Nacional Experimental Francisco de Miranda (UNEFM), Venezuela

Autor para correspondencia: acolina@ecotec.edu.ec; jah120@gmail.com
Fecha de recepción: 09 de octubre de 2020 - Fecha de aceptación: 07 de diciembre de 2020

Resumen
Evaluar y administrar los riesgos asociados con los activos de TI es una de las tareas más desafiantes que enfrenta una organización en la actualidad. Existe un entorno marcado por presiones diarias sobre el tiempo y los recursos, las cuales a menudo no reciben toda su atención. Sin embargo, una actividad esencial debe comprender la presentación de informes frecuentes de nuevas vulnerabilidades, ataques de piratería y filtraciones de datos. Se requiere entonces, la gestión de activos como un proceso que permite alcanzar un manejo adecuado de los activos de TI con miras a mejorar la eficiencia y el rendimiento de la organización y con ello minimizar costos, entre otras cosas. Este trabajo presenta una revisión teórica que permita dar respuesta a ¿cómo la gestión de activo de TI es pertinente e indispensable en los procesos de gestión de riesgos de tecnologías? Para ello, se articularon las metodologías de investigación de tipo exploratoria y descriptiva. Se siguió la metodología de revisión de literatura propuesta en la Declaración de PRISMA, consultados en las bases de datos SCOPUS y IEEE Xplore Digital con descriptores en español e inglés, cuya fecha están entre el año 2018 a 2020. Se plantea finalmente, que a partir de la revisión a modo general el hecho de que existe pocas investigaciones en la cuales se relaciona los activos de TI y la gestión de riesgos. Al hacer referencia a activos TI eran vinculados a los riesgos financieros, lo cual no están vinculados a los fines de la investigación.
Palabras claves: activos TI; riesgos; procesos; gestión.

Abstract
Assessing and managing the risks associated with IT assets is one of the most challenging tasks facing an organization today. There is an environment marked by daily pressures on time and resources, which often do not receive your full attention. However, one essential activity should

include frequent reporting of new vulnerabilities, hacking attacks, and data breaches. Thus, asset management is required as a process that allows achieving adequate management of IT assets with a view to improving the efficiency and performance of the organization and thereby minimizing costs, among other things. This paper presents a theoretical review that allows us to answer how is IT asset management pertinent and indispensable in technology risk management processes? For this, exploratory and descriptive research methodologies were articulated. The literature review methodology proposed in the PRISMA Declaration was followed, consulted in the SCOPUS and IEEE Xplore Digital databases with descriptors in Spanish and English, whose date is between 2018 and 2020. It is finally proposed, that from the review in general, the fact that there is little research that relates to IT assets and risk management. When referring to IT assets, they were linked to financial risks, which are not linked for the purposes of the investigation.
Keywords: IT assets; risks; processes; management.

Introducción

Hoy por hoy, las organizaciones en general se encuentran ante un convulsionado y cambiante entorno, apoyándose en el uso de la tecnología de información (TI) para lograr la continuidad de sus operaciones (Vanegas D. y Pardo, 2014). Tratan de optimizar sus procesos empleando un conjunto estructurado de herramientas que permitan mejorarlos y en esa medida satisfacer los requerimientos de sus beneficiarios; de forma adecuada con productos y servicios de calidad. La aplicación de dichas herramientas requiere que existan en la organización un conocimiento de sus procesos y áreas, para ser capaz de ajustar su forma de trabajo de manera rápida y competitiva (Arcilla-Cobián, San Feliu Gilabert, Feliz, y Calvo-Manzano Villalón, 2017).

Tomando en cuenta el entorno dinámico actual, la dependencia en el uso de la tecnología, ya sea para la automatización de sus procesos y sus actividades ha provocado que las organizaciones se expongan a riesgos y a explotar las vulnerabilidades de una gran variedad los activos de TI (Saeidi, 2020) que pueden afectar de forma crítica a la empresa, requiriendo que tomen conciencia del valor que tiene la información y los procesos que apoyan los sistemas y las redes, considerados activos valiosos para la misma (Villafranca, Sánchez, Fernández-Medina, y Piattini, 2005). Siendo importante destacar que, no se tiene conocimiento de la existencia de capital y recursos para protegerlas de forma completa y suficiente, afectando el poder cumplir con su misión propuesta (Alvarado-Zabala, Pacheco-Guzmán, y Martillo-Alchundia, 2018).

Dentro de los retos que enfrenta la organización se encuentra garantizar que las tecnologías para los activos informáticos y de información sean seguras, rápidas y de fácil interacción, una de las dificultades que se le presenta a los gerentes de sistemas es la falta de guías de seguridad de la información, que permitan responder a las preguntas de ¿dónde tengo que buscar? y de ¿qué tengo que controlar y cómo? (Villafranca, Sánchez, Fernández-Medina, y Piattini, 2005).

Las organizaciones se encuentran en el dilema de contar con una gran cantidad y variedad de activos tecnológicos, y tener que establecer y clasificar estos activos puede ser una tarea de grandes proporciones, sobre todo en aquellas grandes organizaciones (Valencia Duque y Orozco

Alzate, 2017). Dentro de las acciones a considerar como medida está el hecho de que los activos de tecnológicos deben ser valorados el impacto dentro de la organización, valiéndose para ello de herramienta de análisis de riesgos que comprendan la identificación de las amenazas, vulnerabilidades y riesgos de la información.

En ese contexto, en el ámbito de la seguridad de la información se elabora el plan de tratamiento de riesgos de seguridad de la información. Este proceso comprende el identificar y clasificar los activos de acuerdo a los requerimientos de seguridad y el nivel de criticidad para el negocio, así como establecer quién es el propietario de ese activo y quien debería ser el responsable de su seguridad en una determinada organización (Pallas y Corti, 2009).

Ante lo cual, es fundamental para las organizaciones en el marco de la caracterización de los procesos y actividades de una gestión de riesgos la identificación de los activos de TI, por su valor o utilidad a nivel de la continuidad de sus operaciones comerciales; éstos necesitan control, clasificación, protección, para garantizar las operaciones comerciales y la continuidad del negocio (Vanegas D. y Pardo, 2014).

Siendo importante dilucidar que el término activo es acuñado con diferentes connotaciones, en el ámbito financiero o empresarial, a los fines del presente artículo se delinea como una actividad en el contexto empresarial que denota el "conjunto de todos los bienes y derechos con valor monetario que son propiedad de una empresa, institución o individuo" (Española, 2020).

La gestión de activos de TI (ITAM) de acuerdo a la Asociación Internacional de Administradores de Activos de TI (IAITAM) comprende aquellas prácticas administrativas relacionadas con los activos de toda una organización que se "suma a las responsabilidades financieras, de inventario, contractuales y de gestión de riesgos para gestionar el ciclo de vida general de estos activos, incluida la toma de decisiones tácticas y estratégicas" (Management, 2015).

Tomando como base las consideraciones anteriores, este articulo pretende a partir de una revisión bibliográfica sistemática dar respuesta a ¿cómo la gestión de activo de TI es pertinente e indispensable en los procesos de gestión de riesgos? Para ello, se tomaron como referentes teóricos que sustentaron la investigación información consultada en fuentes documentales, entre ellas las bases de datos científicas SCOPUS y IEEE Xplore Digital, con la finalidad explicitar las características del objeto de estudio desde diferentes posiciones teóricas, lo que permitió asumir una postura crítica resaltando la importancia de la gestión de activo de TI medida tomar decisiones efectivas en torno a la seguridad.

Finalmente, se destaca que la gestión de activos no solo implica la realización de un inventario y clasificación de activos físico y lógico dentro de la infraestructura tecnológica de una organización, debe concebirse desde visión holística, que contemple los elementos direccionadores de la mejora continua entre sus múltiples áreas de negocio, generando una alta competitividad e innovación (Gonzales E., 2018).

Marco teórico

Explorando la definición de gestión de activos de TI

La gestión de activos es conocido como el proceso de gestión global a través del cual se pueden tomar y ejecutar decisiones acerca del valor, el uso y cuidado de los bienes adquiridos el cual ha tomado cada vez más relevancia en las áreas de mantenimiento, revolucionando la dinámica en la industria, pues intenta optimizar los recursos, desde su adquisición hasta su disposición final (Cañaveral Vargas y Heredia, 2017).

La gestión de activos de TI (ITAM) comprende un conjunto de etapas o fases dentro de un ciclo de vida, que no se limita únicamente a supervisar activos, garantiza que no se pierden o que empiezan a deteriorarse. Se requiere descubrir, normalizar y recuperar los activos de TI para evitar el riesgo financiero de hardware y software que no sea gestionado (Management, 2015).

Se destaca dentro de una gestión correcta de los activos en general de la empresa, el poder evidenciar y contar los bienes que hacen parte del inventario, teniendo como mínimo información como el nombre o descripción, el estado físico en el que se encuentra, la ubicación física de los equipos, herramientas, muebles, entre otros, el valor, la vida útil, entre muchos otros datos a tener en cuenta (Medina Villarreal, Cantuca Blandón, y Bautista León, 2018).

Según la Asociación Internacional de Administradores de Activos de TI (IAITAM), la Gestión de Activos de TI (ITAM) es "conjunto de prácticas comerciales que incorpora activos de TI en todas las unidades de negocios dentro de la organización. Se suma a las responsabilidades financieras, de inventario, contractuales y de gestión de riesgos para gestionar el ciclo de vida general" (Management, 2015). Los activos incluyen todos los elementos de software y hardware que se encuentran en el entorno empresarial.

La gestión de activos de TI a veces se denomina gestión de inventario de TI porque normalmente implica recopilar información detallada del inventario de hardware y software que luego se utiliza para tomar decisiones sobre compras y cómo se utilizan los activos. Tener un inventario de activos de TI preciso ayuda a las empresas a utilizar sus activos de manera más eficaz y evitar compras innecesarias de activos al reutilizar los recursos existentes. La gestión de activos de TI también permite a las organizaciones reducir los costos de riesgo de construir, sin saberlo, nuevos proyectos de TI sobre bases de infraestructura obsoletas o desconocidas.

Existen un conjunto de herramientas que facilitan una gestión efectiva de activos de TI utilizando metadatos y registros electrónicos para rastrear y categorizar los activos de la organización. Estos metadatos consisten en la descripción del activo físico o digital y cualquier información de apoyo que se necesite para informar las decisiones de gestión de activos, variando la profundidad de los metadatos según las necesidades de la organización (Martins, 2014).

Tipos de gestión de activos de TI

1. Gestión de activos digitales

Comprende esa parte de las funciones de gestión de propiedad intelectual de la empresa y es una forma de gestión de contenido de medios electrónicos que se ocupa de la gestión de activos digitales como fotos, videos y datos digitales que la empresa produce o licencia de terceros.

2. Gestión de activos de software y gestión de licencias

En este caso, se preocupan por la gestión, el control y la protección eficaces de los activos de software. Esto incluye los producidos por la empresa y aquellos con licencia de terceros para garantizar que todo el software en uso dentro de la organización se pague correctamente y cumpla con los acuerdos de licencia.

En relación a la importancia de la Gestión de activos para TI

Las organizaciones de TI gestionan una gran proporción de la huella total de activos de la empresa. Dentro de esos activos se encuentran los activos de TI costosos de adquirir y mantener, por lo cual desempeñan un papel fundamental para ayudar a los equipos de TI a garantizar el uso eficiente de los recursos de la organización para respaldar las necesidades de los usuarios y las funciones comerciales.

La gestión de activos de TI (ITAM) es conocida por "proporcionar una cuenta precisa de los costos y riesgos del ciclo de vida de los activos tecnológicos para maximizar el valor comercial de la estrategia tecnológica, la arquitectura, la financiación, las decisiones contractuales y de abastecimiento" (Management, 2015). Esta definición destaca que la gestión de activos de TI no se trata solo de inventariar activos, sino de utilizar la información que se captura para impulsar las decisiones. Cada vez más, las organizaciones de TI se centran en la usabilidad y el valor informativo de los datos de activos de TI para impulsar el valor comercial en lugar de centrarse únicamente en la cantidad y precisión de los datos.

Dentro de los principales objetivos clave de la gestión de activos en TI se encuentran el hacer cumplir las políticas de seguridad corporativas y los requisitos normativos, mejorar la productividad mediante la implementación de la tecnología para respaldar las necesidades comerciales y de los usuarios, reducir los costos de licencia y soporte al eliminar o reasignar recursos y licencias infrautilizados y limitar los costos generales de administración del entorno de TI, preferiblemente.

Dentro de los principales beneficios de la gestión de activos de TI, se tienen: Decisiones de compra e implementación informadas. Continuidad del negocio. Cumplimiento de licencias y suscripciones. Costo total de la propiedad. Estandarización.

¿Qué es un ejemplo de activo de TI?

Dado que se presentan hoy entornos de TI cada vez más complejos y diversos a partir de la evolución de la tecnología habiendo más ofertas disponibles de terceros, proporciona una clara definición de lo que es un activo de TI puede ser. Muchas empresas han comenzado a alejarse de

las definiciones estrictas y, en cambio, la definición de los activos de TI variará de una organización a otra según la naturaleza del negocio, el papel de tipos específicos de cosas dentro del ecosistema de TI general y las necesidades de información para respaldar la decisión (Martins, 2014). En la Tabla 1, se presentan algunos ejemplos de activos:

Tabla 1

Ejemplos de activos de TI

Tipo de activo	Descripción general
Hardware de infraestructura	Dispositivos de red, centros de datos, servidores físicos, etc., que su empresa haya comprado y operado.
Convenios de alquiler o rentas de instalaciones e infraestructura de TI	La infraestructura proporcionada por terceros no se considera un activo de su empresa. Los acuerdos para acceder y utilizar la infraestructura de terceros pueden considerarse activos.
Software desarrollado internamente	Cosas que su personal de TI ha escrito o construido internamente que su empresa posee.
Licencias de software	A veces denominado software Common Off the Shelf (COTS), son cosas que otra persona creó para las que usted compró una licencia para usar por un período de tiempo. Siendo el activo la licencia y, no el software en sí.
Equipos de usuario final propiedad de la empresa	Las computadoras de escritorio, monitores, impresoras, teléfonos y otros dispositivos del usuario final se han considerado tradicionalmente activos de TI. Tenga en cuenta que los dispositivos personales de los empleados no son activos de la empresa.
Datos digitales de operaciones	Cada vez más, los datos se tratan como un activo de TI que se valora, calcula, gestiona y mantiene a lo largo de su ciclo de vida.

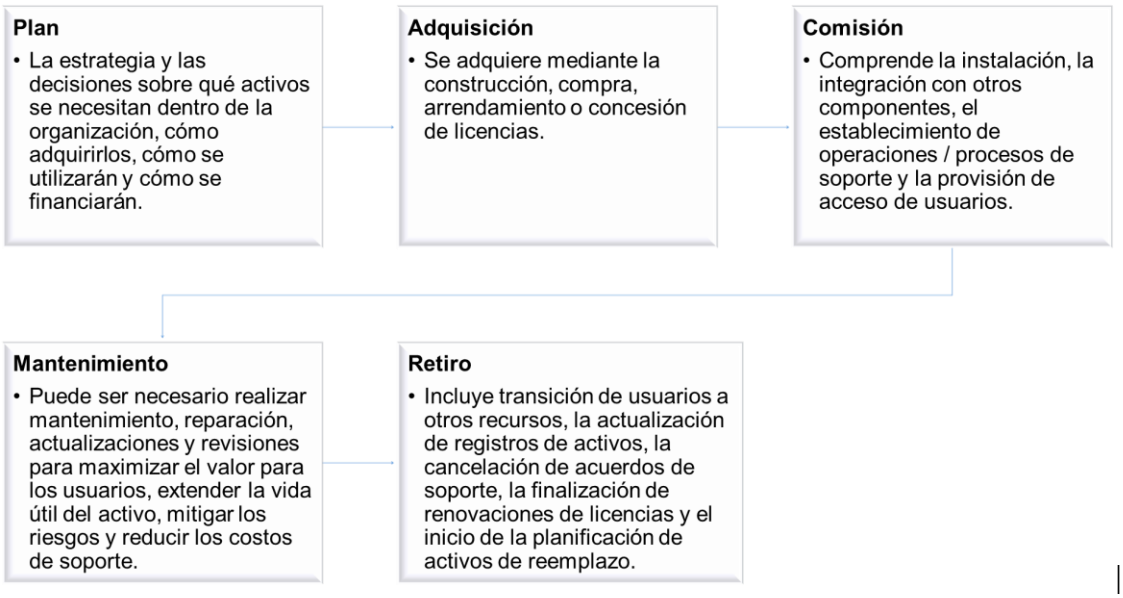
Fuente: Elaboración propia.

Recorriendo el ciclo de vida de los activos de TI

El ciclo de vida de los activos de TI comprende un conjunto de pasos o fase, entre las cuales destacan en la Figura 1:

Figura 1

Representación de las fases del ciclo de vida de los activos de TI



Fuente: elaboración propia.

Gestión de riesgos

El uso de las tecnologías de la información (TI) han evolucionado rápidamente en los últimos años, constituyéndose como un eje transversal en las organizaciones vinculadas a diversos sectores: económico, financiero, industrial, educación etc. Un gran porcentaje de los procesos que se ejecutan se encuentran vinculados con TI, para lo cual resulta inherente gestionar los riesgos con el fin de minimizar el impacto que pueda causar la violación de las dimensiones de la seguridad (Confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad) (Ramírez y Ortiz, 2011).

La gestión del riesgo se soporta principalmente en las normas ISO 31000 (Administración de riesgos) y la ISO 27005 (Administración de riesgos de seguridad de la información), donde se conciben dos etapas: el análisis y evaluación de riesgos, a través de la verificación de la existencia de controles de seguridad existentes, las pruebas con software y el monitoreo de los sistemas de información permiten establecer el estado actual de la organización, identificar las causas de vulnerabilidades y proponer soluciones de control que permitan su mitigación (Solarte, Enriquez, y Benavidez, 2015).

Proceso de Gestión de Riesgos

El proceso comprende una colección sistemática de actividades que están vinculados entre sí para apoyar tareas específicas relacionadas a la gestión de riesgos de TI, tomando en cuenta las pautas identificadas en las normas de gestión de riesgos existentes ISO 310000, NIST

SP800-30 marco y normas NERC CIP para definir el proceso. Siendo fundamental comprender el activo, vulnerabilidades y amenazas que pueden generar riesgos para la infraestructura tecnológica critica de la organización. Dentro de las actividades propuestas por (Halima y Shareeful, 2019) se tiene:

1. Identificación y categorización de activos:

Para una gestión de riesgos exitosa, la identificación de activos es crucial y debe iniciarse antes de que se identifique cualquier riesgo. Pretende identificar y priorizar los activos de acuerdo con sus niveles de criticidad en la organización. La lista de activos resultante y la categorización se utilizan luego como entrada a la evaluación de vulnerabilidad.

2. Identificación de vulnerabilidad y evaluación de amenazas:

Constituye una parte esencial de un proceso de gestión de riesgos permite determinar la vulnerabilidad de un sistema o activo y la consecuencia de posibles amenazas. Para ello, esta actividad identifica vulnerabilidades, causas y consecuencias de las amenazas, tipos de amenazas, efectos en cascada de las amenazas y cómo pueden afectar el sistema y sus activos. Comprende, además, evaluar el nivel de riesgo planteado por un sistema o un activo, requiriendo una comprensión de las amenazas, vulnerabilidades y las incertidumbres inherentes.

3. Riesgos y vulnerabilidades en cascada:

La identificación de riesgos es esencial para cualquier infraestructura tecnológica crítica de la organización. Se enfoca en identificar y evaluar los aspectos críticos de los activos, y las vulnerabilidades y amenazas relacionadas que podrían generar riesgos. La vulnerabilidad se define como la debilidad de un activo, explotada por un actor de amenazas que es un individuo, una organización o un grupo ejecutar un programa con la intención de comprometer el cumplimiento de los indicadores de rendimiento de un activo vulnerable. Esto conduce a una amenaza de la infraestructura tecnológica de la organización y causa riesgos para el negocio la continuidad en general.

Marcos de trabajo o Framework de gestión de riesgos

Existen diferentes enfoques dentro de los marcos de trabajo o framework de gestión de riesgos en la actualidad, éstos son conocidos como aquella capa abstracta de gestión enfocada en la evaluación de riesgos, según (Haji, Sami, y Tan, 2019). La Tabla 2 contiene la descripción de algunos marcos de gestión.

Tabla 2

Marcos de gestión de riesgos

Marco de gestión de riesgos	Características
ISO / IEC 27005	Proporciona un enfoque estandarizado. Constituye un requisito clave en la información sistema de gestión de la seguridad (Normalización, 2018). Aplicable a organizaciones de todo tipo.
NIST SP 800-37	Guía que pretende ayudar a las organizaciones y al sistema de información federal en seguir un enfoque sistemático de identificación y evaluación de riesgos para los sistemas de información (Normalización, 2018) Considera el proceso de evaluación de riesgos como parte de una jerarquía de gestión de riesgos más amplia dentro de la organización. Semejante a la ISO / IEC 27005 cumple todo el ciclo de riesgo de seguridad de la información (Normalización, 2018).
Método de análisis y gestión de riesgos (CRAMM)	Metodología para gestionar los riesgos de seguridad de la información a través de una revisión sistemática. Ha sufrido múltiples revisiones y fue adoptado por Insight Consulting
Método ISRAM	Utiliza métodos cuantitativos para arriesgar evaluación mediante cálculo matemático utilizando un enfoque típico basado en ecuaciones de probabilidad e impacto para deducir la gravedad del riesgo identificado (Karabacaka y Sogukpinar, 2005)

Fuente: elaboración propia.

Metodología

Esta investigación se caracterizó por ser una revisión sistemática de literatura guiados por los referentes significativos de la Declaración de Preferred Reporting Items for Systematic Reviewsand Meta-Analyses (PRISMA) (Liberati, y otros, 2009). Como metodología de revisiones sistemáticas, propone a partir de veintisiete (27) ítems de verificación agrupados en siete (07) secciones los tópicos a nivel conceptuales y metodológicos que deben presentar las revisiones de literatura, entre ellos están: título, resumen, introducción, método, resultados, discusión y financiación.

La revisión sistemática constituye un medio que permite la evaluación e interpretación de toda investigación disponible y relevante para una pregunta de investigación, área temática o fenómeno de interés en particular, mediante el uso de una metodología confiable, rigurosa y auditable (Kitchenham y Charters, 2007). Comunica de manera completa y transparente a los lectores para que se evalúen las fortalezas y debilidades de investigación realizadas llegando a comprender o dar respuesta a las preguntas de investigación (Urrutia y Bonfill, 2010).

Siendo el caso que ocupa en este artículo, para el proceso de revisión se tomó en consideración algunos de los ítems declarados en PRISMA en el método utilizado, como son: definición de los criterios de elegibilidad, fuentes de información, búsqueda, selección de estudios, resultados y la clasificación de los artículos según distintas categorías. La revisión tomo como orientador una pregunta de investigación: ¿cómo la gestión de activos de TI es pertinente e indispensable en los procesos de gestión de riesgos?

Resultados

El proceso de la revisión sistemática propuesto en PRISMA comprende un conjunto de ítems utilizados en esta investigación que den respuesta a la pregunta de investigación objeto de estudio.

1. Criterios de elegibilidad

Se realizó la revisión de las variables "Activos de TI" y "Gestión de riesgos" para conocer el estado actual. Seleccionando artículos de revistas científicas con sistemas de arbitrajes por pares, que contengan documento en extenso, cuyas publicaciones estén entre enero 2018 al mes de agosto de 2020 y escritas en español e inglés. Se fijaron como criterios de elegibilidad el cumplimiento de lo siguiente:

- Trabajos que destacan la relación entre los activos de TI y los riesgos de tecnologías.
- Trabajos que expresan claramente dentro de la gestión de riesgos de TI se consideran los activos tangibles e intangibles.
- Trabajos que vinculen la seguridad informática con la gestión de riesgos, y los activos de TI.

2. Fuentes de información

Los artículos científicos fueron ubicados mediante búsquedas en bases de datos electrónicas publicados en inglés y español. Seleccionados de una base de datos generalista SCOPUS (2018-2020) y una base de datos especifica IEEE Explore Digital Library (2018-2020). Siendo el último día de búsqueda el 30 de agosto de 2020.

3. La búsqueda

Los descriptores utilizados en la búsqueda se definieron a partir de la pregunta de investigación establecida en español y en inglés:

- Los términos seleccionados fueron: "Activo de TI y gestión de riesgo", "IT assets and risk management".
- Criterios de búsqueda a partir de la combinación de los mismos con el uso de operadores booleanos.
- Se limita la búsqueda de los artículos cuyo tipo de acceso es "open access" para la base de datos IEEE Xplore y SCOPUS.

- Se limita la búsqueda de los artículos cuyo año de publicación sean del 2018 al 2020, tipo de documento artículos, idioma de publicación en español e inglés.

4. Selección de estudios

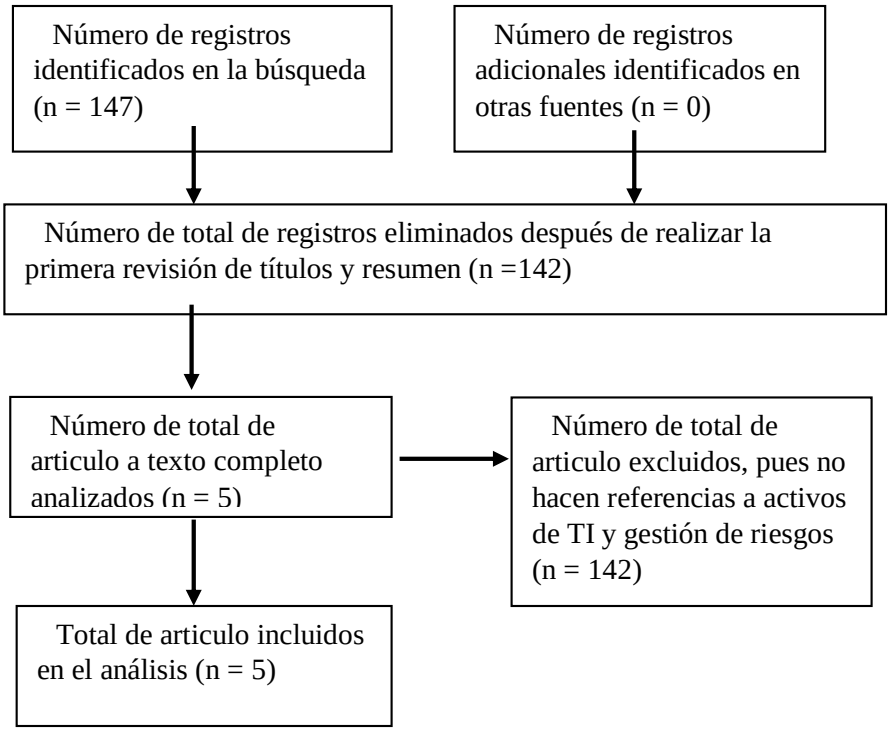
- Una vez seleccionados los artículos según los criterios fijados se exporta a un archivo de Ms Excel desde cada una de las bases de datos SCOPUS y la IEEE Xplore,
- Se procede a la evaluación de los artículos que cumplieran con los criterios de elegibilidad señalados en la sección anterior.
- Con cada artículo se hizo una revisión manual de las secciones de resumen, introducción y conclusión para seleccionar los artículos más relevantes para el estudio.
- Se procedió a confirmar la existencia de duplicidades analizando los artículos de forma más concreta.
- Se rechazaron un número considerable de artículos referentes a "activos de TI" y "gestión de riesgos", por no tributar al objetivo principal de esta revisión.

5. Resultados

Una vez realizada la búsqueda en las bases de datos SCOPUS y la IEEE Xplore se obtuvieron un total de 147 artículos. El bosquejo del flujo de trabajo se refleja en la Figura 2.

Figura 2

Bosquejo del flujo del proceso de la revisión sistemática realizada



Fuente: elaboración propia.

Se utilizaron las preguntas de investigación y una estrategia paso a paso para obtener la cadena de búsqueda final de los artículos de investigación, eliminando los artículos repetidos (Tabla 3).

Tabla 3

Resultados encontrados

Base de datos	Resultados encontrados	Primera selección	Selección final
SCOPUS	136	5	4
IEEE Xplore Digital Library	11	1	1

Fuente: elaboración propia.

5.1 Clasificación de los artículos según distintas categorías

Una vez que se obtuvo la muestra final de siete artículos (n=5), se procedió a clasificarlos en función de su contenido. Estableciéndose una serie de categorías, en donde se han catalogado en función de su contenido (Tabla 4):

Tabla 4

Clasificación de los artículos según categorías

Categoría	Subcategoría	Número de artículos encontrados
Año	2019	4
	2018	1
Tipo de artículo	Investigación	4
	Revisión de literatura	1
Contenido	Gestión de riesgos y activos	3
	Ciberseguridad y activos de TI	2

Fuente: elaboración propia.

5.1.1 En función del año de publicación

En los últimos años la publicación de trabajos sobre gestión de riesgos ha crecido considerablemente, observándose que entre los años 2018 y el 2020 se han publicado el 60% de la revisión realizada.

5.1.2 En función del tipo de trabajo presentado

Una vez analizados los artículos en su globalidad se procedió a categorizarlos en función del tipo de contenido, se tienen artículos de: revisión teórica y de investigación. Se define esta

clasificación en los términos de que algunas investigaciones incorporan elementos de un marco teórico sobre la temática, quedando ubicado en función del sentido principal y el tópico del artículo.

Los artículos de investigación encontrados en la revisión (Tabla 5) destacan en primer lugar la aplicación de metodologías sistemáticas para identificar y analizar activos críticos, sus posibles vulnerabilidades, amenazas y riesgos dado el auge de implementación en las empresas de diversas tecnologías que van desde computación en la nube, hasta IoT trayendo consigo cambios y énfasis la importancia de la gestión de riesgo ((Kure y Islam, 2019); (Haji, Sami, y Tan, 2019)) Se hace referencia la evaluación y gestión de riesgos de seguridad de la información y por qué es necesaria. Se identifica algunos marcos generales para llevar a cabo una evaluación y analiza sus características comunes, incluida la identificación de activos, amenazas y vulnerabilidades, impacto y probabilidad (Mackita, Shin,, y Choe, 2019).

Se resalta de igual manera, el papel que juegan las TI cada vez más significativas para las pequeñas y medianas empresas, las cuales deben proteger los activos de información y de tecnologías a raíz de la continua y constante exposición a riesgos y amenazas que han crecido en los últimos años estableciendo dentro de las acciones tres elementos que conforman la estructura de una política de seguridad son gestión de activos, gestión de riesgo y seguridad (Almeida, Carvalho, y Cruz, 2019).

Tabla 5

Listado de artículos de investigación

Autores	Año	Título
Halima Ibrahim Kure ; Shareeful Islam	2019	Assets focus risk management framework for critical infrastructure cybersecurity risk management
Mackita, M., Shin, S.-Y & Choe, T.-Y.	2019	ERMOCTAVE: A risk management framework for IT systems which adopt cloud computing
Haji, S. , Tan, Q. , Costa, RS	2019	A hybrid model for information security risk assessment
Almeida, F. , Carvalho, I. , Cruz, F.	2018	Structure and challenges of a security policy on small and medium enterprises

Fuente: elaboración propia.

Por su parte, en cuanto al artículo de revisión de literatura (Tabla 6), tratan de analizar el papel de la información como un activo en la organización puesto que ayuda a las organizaciones a cumplir sus objetivos organizacionales; así como los problemas y dificultades que llevan en la actualidad el incremento en los activos de información volviendo difícil para la organización hacer un uso efectivo de los mismos. Siendo la auditoría de información la herramienta eficaz que podría utilizarse para gestionar los activos de información y gestión de riesgo, como parte de una política de información (Lateef y Omotayo, 2019).

Tabla 6

Listado de artículos de revisión de literatura

Autores	Año	Título
Lateef, A., Omotayo, F.O.	2019	Information audit as an important tool in organizational management: A review of literature

Fuente: elaboración propia.

3.1.3 En función del contenido

De la revisión realizada se destaca una mayor preferencia a la existencia de artículos relacionados con el funcionamiento adecuado de los activos de TI y cualquier amenaza que pueda afectar negativamente al activo podría tener una interrupción grave. En cuanto a la gestión de riesgos se considera un aspecto importante para ello existen varios marcos y metodologías para identificar activos, cuantificar y analizar vulnerabilidades. Sin embargo, existe poca investigación en relación al enfoque en las interdependencias entre los activos y el efecto en cascada de las vulnerabilidades inherentes al activo que generan amenazas y generan riesgos.

Conclusiones

Las revisiones bibliográficas permiten localizar, procesar y reconstruir información relevante para un tema en tres sentidos: de acuerdo a su fuente, al proceso de análisis implicado y al resultado esperado (Calvo, 2002) Esta investigación comprendió una revisión sistemática de la literatura siguiendo como referencia la Declaración PRISMA (Liberati, y otros, 2009) descrita en la sección anterior. Se analizó publicaciones obtenidas de las bases de datos SCOPUS y la IEEE Xplore Digital de los años 2018 a 2020 donde se consideraron 147 artículos de los cuales 5 cumplieron los requisitos para responder a las preguntas de investigación en relación la relación entre los activos de TI y los riesgos de tecnologías.

De igual manera, se conoce que las revisiones sistemáticas permiten sintetizar la información existente sobre un fenómeno de forma minuciosa y empírica. Esta investigación permitió determinar lo poco que se ha desarrollado en un artículo científico relacionado a los activos de TI y los riesgos de tecnologías. Se plantea a modo general como resultado el hecho de que existe pocas investigaciones en la cuales se relaciona dichas variables. Se deduce principalmente que las investigaciones se han planteado para dar respuesta a las necesidades del continuo cambio en el entorno con la incorporación de tecnología, lo cual ha minimizado el interés en actividades que permiten mapear la gestión de riesgos de tecnologías orientados a políticas de seguridad.

Se plantea a partir de la revisión a modo general el hecho de que existe pocas investigaciones en la cuales se relaciona los activos de TI y la gestión de riesgos. Al hacer referencia a activos TI eran vinculado a los riesgos económicos - financieros, riesgos medio

ambientales, riesgos agrícolas y biológicos, riesgos de negocios, entre otros lo cual no están vinculados a los fines de la investigación.

En atención a la interrogante formulada, la mitigación de riesgos es conveniente de acuerdo a (Stoll, Felderer, y Breu, 2010) para la seguridad de los activos de información y el cumplimiento de los requisitos legales, reglamentarios, políticas y directrices de requisitos de seguridad.

Existe la necesidad de implementar prácticas tradicionales de gestión de riesgos aplicables al contexto empresarial de seguridad asociaciones con terceros y describir los requisitos aplicables a esta relación en el contexto empresarial.

De manera particular, a partir de esta la revisión sistemática el análisis gira entorno comprender a la ciberseguridad como la protección de activos de información a través del tratamiento de amenazas que ponen en riesgo la información. La gestión de los riesgos es una necesidad para las organizaciones, independientemente de su tamaño, deben gestionar los riesgos de para mejorar la seguridad y la capacidad de recuperación de sus activos.

La tendencia de los trabajos encontrados se enfocó hacia la conceptualización y definición de herramientas y buenas prácticas orientadas hacia la gestión de riesgos sin considerar la falta de enfoque en las interdependencias entre los activos y el efecto en cascada de las vulnerabilidades inherentes al activo.

Finalmente, queda para estudios posteriores analizar todos los referentes a los marcos y metodologías para la identificación de activos, cuantificar y analizar vulnerabilidades como mecanismo en la gestión de riesgos es un aspecto importante de la protección de la infraestructura de tecnologías de información de la organización.

Referencias Bibliográficas

Almeida, F., Carvalho, I., & Cruz, F. (2019). Structure and Challenges of a Security Policy on Small and Medium Enterprises. *KSII Transactions on Internet and Information Systems*(747-763). doi:DOI: 10.3837/tiis.2018.02.012

Alvarado-Zabala, J., Pacheco-Guzmán, J., & Martillo-Alchundia, I. (2018). El análisis y gestión de riesgos en gobiernos de ti desde el enfoque de la metodología MAGERIT. *Revista Contribuciones a las Ciencias Sociales*. Obtenido de https://www.eumed.net/rev/cccss/2018/11/gestion-riesgos-magerit.html

Arcilla-Cobián, M., San Feliu Gilabert, T., Feliz, A., & Calvo-Manzano Villalón, J. A. (2017). Implementación de una biblioteca de activos de proceso orientada a la gestión de la capacidad de servicios de TI. *International Journal of Information Systems and Software Engineering for Big Companies, (IJISEBC), 4*(2), 43-51.

Calvo, M. A. (2002). Metodología de investigación: la formulación del problema y la búsqueda bibliográfica. *Salud y Cuidados*.

Cañaveral Vargas, C., & Heredia, D. (2017). Desarrollo de una metodología para correlacionar técnicas de análisis en confiabilidad con los ciclos de vida y la gestión de activos. (U. T. Pereira, Ed.) Pereira. Obtenido de https://core.ac.uk/download/pdf/92123454.pdf

Española, R. A. (2020). *Real Academia Española*. Obtenido de https://www.rae.es/

Gonzales E., J. (2018). Sistema automatizado de gestión de activos de TI basado en la norma ISO/IEC 19770-3:2017. *Tesis*. Obtenido de http://repositorio.uwiener.edu.pe/handle/123456789/2499

Haji, Sami, & Tan, Q. S. (2019). A Hybrid Model for Information Security Risk Assessment. *International Journal of Advanced Trends in Computer Science and Engineering, 8*(1.1), 100 - 1. doi:https://doi.org/10.30534/ijatcse/2019/1981.12019

Halima, I. K., & Shareeful, I. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems: Theory & Applications, 4*(1), 332-340. doi:10.1049/iet-cps.2018.5079

Izuakor, C., & White, R. (2016). CRITICAL INFRASTRUCTURE ASSET IDENTIFICATION: POLICY, METHODOLOGY AND GAP ANALYSIS. En M. Rice, & S. Shenoi, *CRITICAL INFRASTRUCTURE PROTECTION X* (págs. 27–41). doi:DOI: 10.1007/978-3-319-48737-3 2

Karabacaka, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers & Security, 24*, 147-159. Obtenido de https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.476.9691&rep=rep1&type=pdf

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering.* Obtenido de https://userpages.uni-koblenz.de/~laemmel/esecourse/slides/slr.pdf

Kure, H. I., & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems: Theory & Applications, 4*(4), 332-340. doi:doi: 10.1049/iet-cps.2018.5079

Lateef, A., & Omotayo, F. (2019). Information audit as an important tool in organizational management: A review of literature. *Business Information Review, 36*(1), 15-22. doi:https://doi.org/10.1177/0266382119831458

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P., . . . Moher, D. (2009). The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration. *PLOS MEDICINE, 6*(7), 1-28. doi:https://doi.org/10.1371/journal.pmed.1000100

Mackita, M., S. S.-Y., & Choe, T.-Y. (2019). ERMOCTAVE: A risk management framework for IT systems which adopt cloud computing. *Future Internet, 11*(9). doi:10.3390/fi11090195

Management, T. I. (2015). *Asset Management An Anatomy. Version 3. United.* Obtenido de https://theiam.org/media/1781/iam_anatomy_ver3_web.pdf

Martins, L. (2014). *Software asset management in an organization.* Instituto Universitario de Lisboa (ISCTE-IUL. Obtenido de http://hdl.handle.net/10071/11184

Medina Villarreal, M. I., Cantuca Blandón, W. A., & Bautista León, F. L. (2018). IMPLEMENTACION DE METODOLOGIA PARA LA GESTION DE ACTIVOS APLICADA A LA EMPRESA IMCO SOLUCIONES SAS. Colombia. Obtenido de http://35.227.45.16/bitstream/handle/20.500.12277/4130/00004398.pdf?sequence=1&isAllowed=y

Normalización, O. I. (2018). Information security risk. Obtenido de https://www.iso.org/standard/75281.html?browse=tc

Pallas, G., & Corti, M. E. (2009). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Montevideo. Obtenido de http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion3(4).pdf

Pathirana, A., Radhakrishnan, M., Bevaart, M., Voost, E., Mahasneh, S., & Rob, H. A. (2018). Fit-for-Purpose Infrastructure Asset Management Framework for Water Utilities Facing High Uncertainties. Infrastructures,. *MDPI AG*. Obtenido de http://dx.doi.org/10.3390/infrastructures3040055

Posner, E. (1972). *Archives in the Ancient World. Cambridge/ Massachusetts.* Obtenido de http://files.archivists.org/pubs/free/ArchivesInTheAncientWorld-2003.pdf

Ramírez, A., & Ortiz, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Revista en ingeniería*, *16*(2), 56-66. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=4797252

Rodríguez S., O., & Colina V., A. (2018). Propuesta tecnológica para la gestión eficiente del servicio médico de una universidad ecuatoriana. . *Revista Espacios, 50*. Obtenido de https://www.revistaespacios.com/a18v39n50/18395009.html

Saeidi, P. S. (2020). The influence of enterprise risk management on firm performance with the moderating effect of intellectual capital dimensions. *Economic Research-Ekonomska Istrazivanja*. doi:doi:10.1080/1331677X.2020.1776140

Salcedo-Muñoz, V., Quezada Abad, C., Núñez, L., Varela-Veliz, G., Novillo, E., & Viteri, C. (2017). Bienestar estudiantil universitario en Ecuador: Caso unidades de bienestar estudiantil en las universidades de la provincia de El Oro. *Revista Espacios*. Obtenido de https://www.revistaespacios.com/a17v38n30/a17v38n30p17.pdf

Solarte, F., Enriquez, E., & Benavidez, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL*, 492-507. Obtenido de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Stoll, M., Felderer, M., & Breu, R. (2010). Information management for holistic, collaborative information security manageme. *6th International Joint Conference on Computer, Information, and Systems Sciences, and Engineering, CISSE 2010*, (págs. 211-224).

Urrutia, G., & Bonfill, X. (2010). Declaración PRISMA: una propuesta para mejorar la publicación de revisiones. *Medicina Clínica*, *135*(11), 505-511. Obtenido de http://www.laalamedilla.org/Investigacion/Recursos/PRISMA%20Spanish%20Sept%202010.pdf

Valencia Duque, F. J., & Orozco Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 22*, 73-88. doi: https://dx.doi.org/10.17013/risti.22.73-88

Vanegas D., G. A., & Pardo, C. J. (2014). Hacia un modelo para la gestión de riesgos de TI en. *Revista S&T, 12*(30), 35-48. doi:10.18046/syt.v12i30.1860

Villafranca, D., Sánchez, L. E., Fernández-Medina, E., & Piattini, M. (2005). La norma ISO/IEC 17799 como base para Gestionar la Seguridad de la Información. *Tercer Taller de Seguridad en Ingeniería del Software y Bases de Datos (JISBD05)*, (págs. Pp. 13-21). Granada.

Yazar, Z. (2011). A Qualitative Risk Analysis and Management Tool – CRAMM. *SANS Institute InfoSec*.