43estudiante

EL CONCEPTO DE CIBERSEGURIDAD EN EL ÁMBITO ORGANIZACIONAL

Maricela Ramírez
Estudiante de doctorado en Ciencias Económicas y Empresariales
Universidad de Granada
Área temática:
Responsabilidad Social Corporativa

El concepto de ciberseguridad en el ámbito organizacional

Resumen

El acelerado ritmo al que se desarrollan las tecnologías y las comunicaciones en la sociedad digitalizada y conectada de hoy incide en el quehacer de las organizaciones. Los retos en el ámbito corporativo consisten en afrontar desde la ciberseguridad los desafíos ante la violación de la privacidad, las amenazas a la seguridad de la información y la pérdida de la salvaguarda de algunos activos físicos. En este sentido, el objetivo de este escrito es presentar la evolución del concepto de ciberseguridad y su vínculo con los elementos que direccionan la operación de las organizaciones: la gobernanza, la estrategia, la gestión de riesgo cibernético y las implicaciones financieras.

1.1. La ciberseguridad

En la actualidad no existe un concepto único de aceptación mundial del término "ciberseguridad"; sin embargo, desde diferentes miradas se pretende observar la multidimensionalidad e interdisciplinariedad de su significado, el cual, en tan solo tres décadas, ha obtenido una cobertura global sin precedentes. Como muestra de ello, la iniciativa inglesa CYBOK (2021), a partir de una investigación mundial, vinculó veintiuna áreas del conocimiento al término "ciberseguridad". Hoy en día, y acorde con la literatura previa, la evolución del significado del término abarca la seguridad de la información, la protección de las personas y los activos físicos dentro del denominado "ciberespacio".

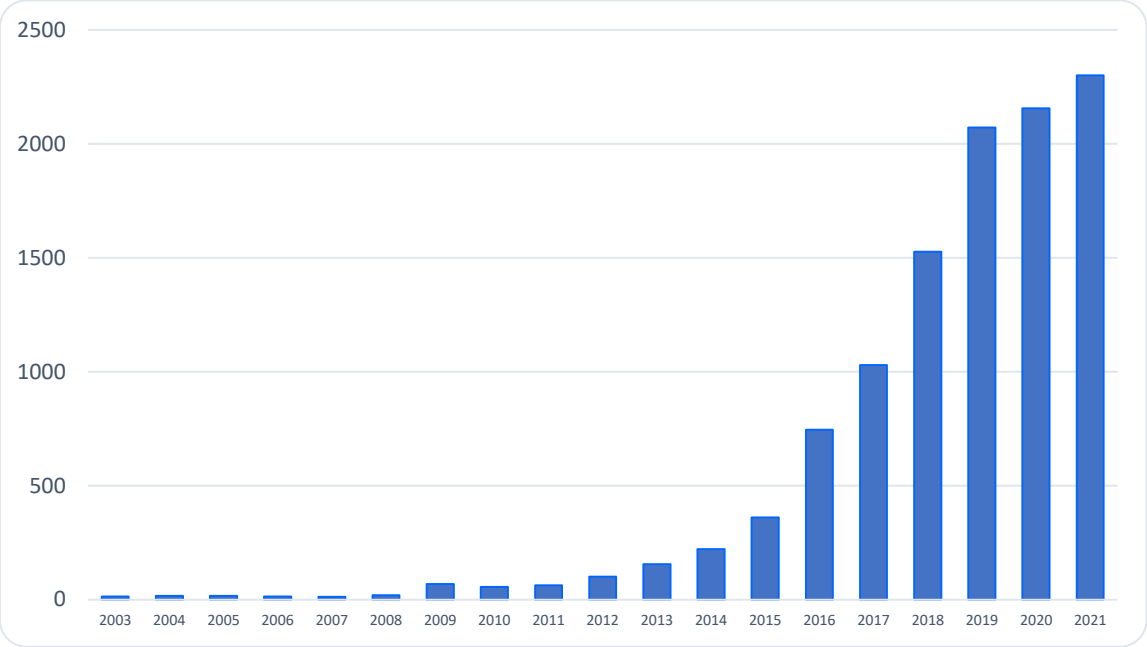
1.1.1. Concepto de ciberseguridad

Se puede afirmar que la ciberseguridad es una palabra relativamente nueva para un conjunto de prácticas antiguas en torno a la protección de las redes informáticas (Von Solms y Van Niekerk, 2013). El término "ciberseguridad" probablemente se utilizó por primera vez en 1989 (Williams, 2020). Esta es la fecha dada por el diccionario (Merriam -Webster, 2021). No obstante, este concepto surge a partir del término "cibernética", utilizado originalmente por el matemático Norbert Wiener en 1941, en el libro *Cybernetics.* Según el diccionario de la lengua española, la palabra cibernética viene del griego *κυβερνητική kybernētiké* "arte de gobernar una nave", y su definición hace referencia a una "ciencia que estudia las analogías entre los sistemas de control y comunicaciones de los seres vivos y los de las máquinas" (RAE; ASALE, 2020): Es a partir de estas bases que la actual definición de ciberseguridad obtiene algunos de sus principales matices.

La revisión de la literatura previa a través de la búsqueda de la palabra clave *"cybersecurity"* en la colección principal de la base de datos *Web of Science,* reporta 10.671 resultados en el período 2002 – 2021, y confirma cómo "su presente uso es relativamente reciente" (Stevens, 2018). En esta búsqueda se identifican 4.875 artículos, de los cuales el 37% tienen su origen en Estados Unidos, seguido de un 9% en la República Popular de China, 7% en Inglaterra, 6% España y 6% Australia. Como se observa en la Figura 1, los artículos de investigación en temas de ciberseguridad muestran un aumento exponencial en la última década. Es probable que el incremento de publicaciones entre 2018 y 2019 se relacione con "los ciberataques de *Wannacry* y *NotPetya* en junio de 2017, los cuales dominaron las noticias mundiales con un impacto colosal" (Eijkelenboom & Nieuwesteeg, 2021). El aumento de la producción en los años 2020 - 2021 seguramente esté conexo con "la aparición de COVID – 19 como agente catalizador de la transformación digital y el aumento de forma exponencial de los ataques cibernéticos" (Fidler, 2020).

Figura 1

Artículos de investigación período 2002-2021

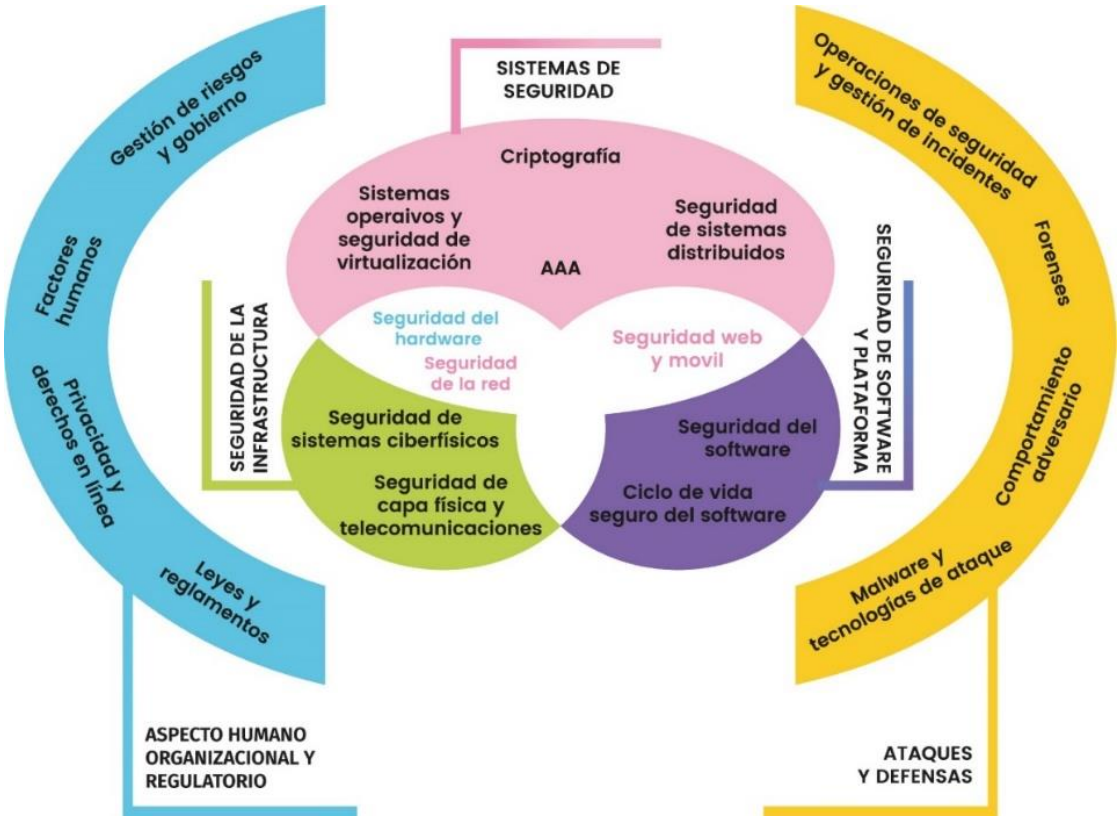


Nota. Elaborado con base en *Web of Science,* enero de 2022

Cabe señalar que en la actualidad existe una iniciativa conocida como CyBOK cuyo objetivo es codificar el conocimiento fundamental y generalmente reconocido sobre ciberseguridad (Martin et al., 2021). El equipo del proyecto CyBOK llevó a cabo un extenso ejercicio que involucró un mapeo y análisis de textos relevantes, así como una variedad de consultas comunitarias tanto en el Reino Unido como a nivel internacional a través de talleres, una encuesta en línea y entrevistas (Martin et al., 2021). Como resultado, los temas sobre ciberseguridad se agruparon en veintiuna áreas de conocimiento asociadas en cinco dimensiones: (1) aspectos humano, organizacional y regulatorio; (2) ataques y defensas; (3) sistemas de seguridad; (4) seguridad de la infraestructura, y (5) seguridad de software y plataforma. Así, la cobertura del concepto de ciberseguridad corrobora su naturaleza multidisciplinaria y la omnipresencia de las preocupaciones de seguridad cibernética en toda la sociedad (Cains et al., 2021).

Figura 2

Áreas de conocimiento de ciberseguridad en el alcance CYBOK

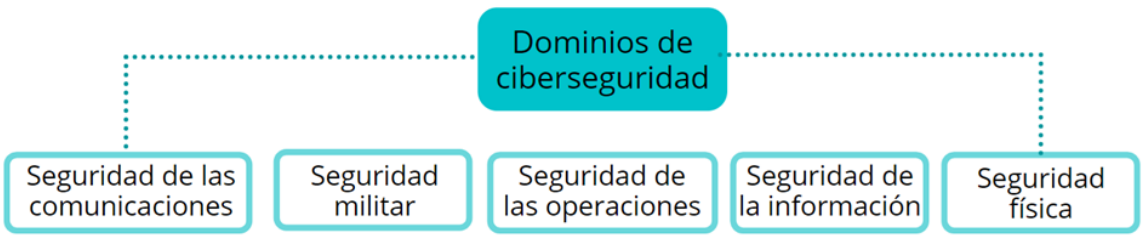


Nota. Elaborado con base en Martin et al. (2021)

En la misma línea, la Agencia Europea de Seguridad de las Redes y de la Información ENISA (2015), resume en cinco los aspectos que abarca la ciberseguridad en cuanto a la seguridad de las naciones se refiere: seguridad de las comunicaciones, seguridad de las operaciones, seguridad de la información, seguridad militar y seguridad física. Estos dominios igualmente representan la amplitud del alcance global del término (Figura 3). Desde estas dos iniciativas CYBOK, Martin et al. (2021) y ENISA (2015), podemos ratificar la importancia de la ciberseguridad en la esfera global como un renglón con repercusiones sociales, políticas y económicas, tanto en el ámbito nacional como internacional.

Figura 3

Dominios del término ciberseguridad



Nota. Elaborado con base en ENISA (2015)

Una vez visto el alcance del tema de la ciberseguridad, nos concentraremos en revisar su concepto desde el punto de vista de la literatura previa, resultado de

investigaciones. Respecto al avance conceptual de la ciberseguridad, según Rashid et al. (2019) no existe un consenso sobre lo que la diversa comunidad de investigadores, educadores y profesionales ve como conocimiento fundamental en ciberseguridad. De acuerdo con Stevens (2018), "hasta la fecha, la lucha por regular y gobernar este complejo paisaje se refleja en la falta de diversidad en la teoría y los métodos utilizados para comprender este entorno novedoso y para interpretar las respuestas políticas a sus problemas, esta temática espera una oferta de ideas para re vestir este desequilibrio".

La ciberseguridad en el ámbito mundial "ha evolucionado y atravesado varias fases a lo largo de los años, resultando en un legado teórico granular que actualmente necesita unificarse para fomentar más teorías beneficiosas y aplicabilidad" (Althonayan & Andronache, 2018). La ausencia de una definición concisa y universalmente aceptable que capture la multidimensionalidad de la ciberseguridad impide los avances tecnológicos y científicos al reforzar la visión predominantemente técnica de la misma, al tiempo que separa las disciplinas que deberían actuar en conjunto para resolver sus complejos desafíos (Craigen et al., 2014).

En esta línea, Dunn Cavelty & Wenger (2020) afirman que la ciberseguridad trasciende los niveles de análisis, requiere un conocimiento interdisciplinario considerable y será moldeada por la disponibilidad de nuevos datos y métodos (Henshel et al., 2015). La ciberseguridad ha construido progresivamente su posición actual sobre sus raíces tempranas en los principios de la informática, la seguridad de la información, la garantía de la información y la gestión de riesgos. Fruto de algunos estudios (Alshaikh et al., 2014; Althonayan & Andronache, 2018; Chang, 2016; Craigen et al., 2014; Kotulic & Clark, 2004; Ramirez & Choucri, 2016; Schatz et al., 2017; Von Solms & Van Niekerk, 2013; Von Solms & Von Solms, 2018; Da Veiga & Eloff, 2007) se ha enriquecido la semántica y la etimología entorno a la palabra ciberseguridad.

Según nuestra búsqueda, en los estudios relacionados con ciberseguridad es común encontrar que las investigaciones no plantean una definición del término; en la mayoría de los casos se omite y en otros se toman definiciones ya existentes emanadas desde diferentes organismos nacionales o internacionales. Tan solo un número reducido de autores se dan a la tarea de proponer una definición de ciberseguridad: Craigen et al. (2014); Gordon et al. (2006); Haapamäki & Sihvonen (2019); Le & Hoang, (2017); Reid & Van Niekerk, 2014; Schatz et al. (2017); Tissir et al. (2020); Von Solms & Von Solms (2018).

Tabla 1

Definiciones de ciberseguridad

Autor	Definición
Gordon et al. (2006)	Los objetivos de la ciberseguridad se pueden dividir en tres grandes categorías. Primero, la ciberseguridad protege la confidencialidad de la información privada; segundo, asegura que los usuarios autorizados puedan acceder a la información de manera oportuna y tercero, la ciberseguridad protege la precisión, confiabilidad y validez de la información.
Craigen et al. (2014)	La ciberseguridad es la organización y el conjunto de recursos, procesos y estructuras que se utilizan para proteger el ciberespacio y los sistemas habilitados para éste, de sucesos que desalinean de jure los derechos de propiedad de facto.
Reid & Van Niekerk, 2014	La seguridad cibernética es la protección de los intereses de una persona, sociedad o nación, incluidos sus activos de

	información y no información que necesitan protección contra los riesgos relativas a su interacción con el ciberespacio.
Schatz et al. (2017)	El enfoque y las acciones asociadas con procesos de gestión de seguridad seguido por organizaciones y estados para proteger la confidencialidad, integridad y disponibilidad de datos y activos utilizados en el espacio cibernético. El concepto incluye lineamientos, políticas y colecciones de salvaguardas, tecnologías, herramientas y capacitación para brindar la protección para el estado del entorno cibernético y sus usuarios.
Le & Hoang (2017)	La ciberseguridad puede considerarse sistemas, herramientas, procesos, prácticas, conceptos y estrategias para prevenir y proteger el espacio cibernético de la interacción no autorizada por parte de agentes con elementos del espacio para mantener y preservar la confidencialidad, integridad, disponibilidad y otras propiedades del espacio y sus recursos protegidos.
Von Solms & Von Solms (2018)	Define la ciberseguridad como esa parte de la seguridad de la información que se enfoca específicamente en proteger la confidencialidad, integridad y disponibilidad (CIA) de los activos de información digital contra cualquier amenaza que pueda surgir de dichos activos que se ven comprometidos. a través de (usando) Internet.
Haapamäki & Sihvonen, (2019)	La ciberseguridad comprende tecnologías, procesos y controles que están diseñados para proteger sistemas, redes y datos de ataques cibernéticos. La ciberseguridad eficaz reduce el riesgo de ciberataques y protege a las sociedades, organizaciones e individuos de la explotación no autorizada de sistemas, redes y tecnologías.
Tissir et al. (2020)	El término "ciberseguridad" puede describirse como un término que refleja las relaciones e interconexiones entre el ciberespacio y el mundo físico; y la información es el elemento clave en esta relación.

Los antecedentes relacionan términos como: seguridad informática (Madnick, 1978); seguridad de la información (Blakley et al., 2002; Von Solms & Von Solms, 2018); riesgo cibernético (Cebula & Young, 2010; McShane et al., 2021; Strupczewski, 2021) y ciberseguridad (Althonayan & Andronache, 2018; Chang, 2016; Von Solms & Van Niekerk, 2013). Estos términos están relacionados con la definición de ciberseguridad, más no son necesariamente sinónimos (Sattarova Feruza & Kim, 2007):

Respecto a la seguridad informática, ésta se define como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, y cuyos efectos puedan conllevar daños sobre la información, equipo o software (Gómez, 2006). Por su parte, autores como Rashid et al. (2019) refieren la seguridad de la información como una gran contribución a la noción de ciberseguridad, a partir de los tres elementos principales que la componen: preservación de la confidencialidad, integridad y disponibilidad de la información.

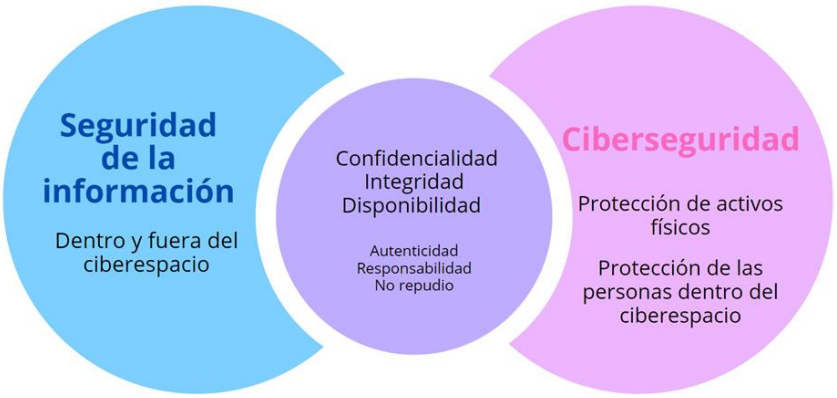
Frente al riesgo cibernético, según (Cebula & Young, 2010), este se define como el riesgo operativo a los activos de información y tecnología que tienen consecuencias que afectan los sistemas de información. Bajo este panorama sobre la complejidad del significado de ciberseguridad, es importante distinguir muy bien este concepto del de "seguridad de la información". Rowe et al.(2012), expresan: "La seguridad de la información ha sido diseñada para proteger la información y lo hace muy bien, pero sus limitaciones no le permiten hacer frente a la protección de los activos, recursos claves, entrelazados con la vida cotidiana, la infraestructura crítica y los sistemas globales; esta distinción es lo que separa la seguridad de la información de la ciberseguridad".

En este sentido, según Von & Van Niekerk (2013), “la ciberseguridad debe consistir en proteger algo más que la información o los recursos de los sistemas de información de una persona u organización; ésta también se refiere a la protección de la(s) persona(s) que utilizan los recursos en un ciberentorno y a la salvaguarda de cualquier otro activo, incluidos los pertenecientes a la sociedad en general, que hayan estado expuestos a riesgos como resultado de vulnerabilidades derivadas del uso de las TIC”. Según Le & Hoang (2017), actualmente una parte integral de la definición de ciberseguridad la constituye su función de prevención, no solo la protección. Tiene sentido mirar la seguridad en un contexto más amplio donde la prevención y la protección van de la mano. Prevenir que alguna vulnerabilidad sea explotada y dañe un ciberespacio puede considerarse proteger el espacio y, por otro lado, saber cómo proteger el ciberespacio implica en cierta medida el conocimiento de las brechas de seguridad que ocurren y cómo se pueden prevenir.

Como ilustra la Figura 4, la seguridad de la información (SI) aporta a la ciberseguridad los elementos que componen los activos conexos con la información: confidencialidad, integridad y disponibilidad. No obstante, la SI tiene un campo de aplicación que no se limita al ciberespacio. También se ocupa de la información, independientemente de su formato: abarca documentos en papel, propiedad digital e intelectual en la mente de las personas y comunicaciones verbales o visuales (Von Solms & Von Solms, 2018). La ciberseguridad protege “los activos digitales, desde las redes hasta el hardware y la información que se procesa, almacena o transporta mediante sistemas de información interconectados. Además, conceptos como los ataques patrocinados por el estado-nación y las amenazas persistentes avanzadas (APT) pertenecen casi exclusivamente a la ciberseguridad” (Von Solms & Von Solms, 2018). En general, todos los activos relacionados con la información, todos los que se encuentren en el ciberespacio, como son los activos físicos, infraestructuras y las personas que actúan en él.

Figura 4

Seguridad de la información y ciberseguridad



Nota. Elaboración propia

Como también ilustra la Figura 4, de la relación entre el concepto de seguridad de la información y ciberseguridad podemos colegir que se tratan de términos con significados diferentes cuyo tema común lo constituye la defensa y la protección de las cualidades de la información en el ámbito organizacional contempladas en ISO 27002 (2013): preservación de la confidencialidad, integridad y disponibilidad de la información. Pueden estar involucradas otras propiedades, como la autenticidad, la responsabilidad y el no repudio. Whitman & Mattord (2011) agregan: precisión, autenticidad, utilidad y posesión a la lista de características de la información que deben protegerse.

Respecto a la digitalización aplicada a la ciberseguridad, si bien se aplica en una organización, al final lo que hay son personas, el *core* son las personas. Así, el componente “factor humano” es un elemento decisivo de tal definición (Adams & Sasse, 1999; Cains et al., 2021; Henshel et al., 2015; Rashid et al., 2019; Von Solms & Van Niekerk, 2013 y Whitten & Tygar, 1999). Henshel et al. (2015) aseveran cómo el ser humano juega un papel en la creación, propagación y mitigación del riesgo de ciberseguridad como usuario, defensor y atacante. Esta dimensión adicional tiene implicaciones éticas para la sociedad en su conjunto, ya que significa la protección de ciertos grupos vulnerables; por ejemplo, los niños (Von Solms & Van Niekerk, 2013).

Otro componente conceptual importante lo constituye la diferenciación de los activos específicos del ciberespacio. Los activos que la ciberseguridad pretende proteger incluyen una dimensión adicional que se extiende más allá de los límites formales de la seguridad de la información (Von Solms & Van Niekerk, 2013). En este marco, Collier et al. (2013) argumentan que la ciberseguridad debe pasar de un enfoque en "problemas técnicos a nivel de componentes" hacia un análisis de sistemas que integre los dominios físicos, de información, cognitivo y social, a partir de estas visiones y de la definición de ciberespacio entendido como el “ambiente en donde interactúan los seres humanos, el software y los servicios que en Internet se ofrecen” (ISO 27032, 2012). El ciberespacio no es estático; es un ecosistema dinámico, en evolución y de múltiples niveles de infraestructura física, software, regulaciones, ideas e innovaciones (Craigen et al., 2014). Así recientemente, el ciberespacio ha crecido para incluir redes sociales, nubes, ciudades inteligentes de internet de las cosas (IOT), redes inteligentes y otros sistemas definidos por software (Le & Hoang, 2017).

La Figura 5 presenta los diversos componentes que pueden hacer parte de la definición de ciberseguridad, tomando como referencia a ENISA (2015). Esta asegura que para analizar las definiciones existentes sobre ciberseguridad es importante evaluar como primer componente el tipo de documento, considerando lo vinculante o no de su aplicación, por lo que puede ser voluntario u obligatorio, dependiendo del contexto y del ente emisor. Como segundo componente se estudia el tipo de organización emisora: puede ser de gobierno, emisora de estándares, una asociación o una corporación. El tercer componente hace referencia a la fuente de la amenaza cibernética; se analiza si el concepto contempla si la amenaza surge de forma intencional o no intencional; y, además, se tiene en cuenta si se expresa el origen de la fuente de amenaza, si ha sido la red, los sistemas de información o un activo físico. El cuarto componente, denominado activos invertidos, evalúa si el significado de ciberseguridad tiene su origen dentro del ciberespacio o se relaciona como objetivos con el ciberespacio; también en este componente se revisan los activos amenazados, a cuáles hace referencia el concepto, ya sea la información, los activos cibernéticos o los activos físicos. El quinto componente coincide con Rashid et al. (2019), al referirse a los tres elementos que componen la seguridad de la información: confidencialidad, integridad y disponibilidad (CID); en este aparte se evalúa si la definición analizada, los contempla o no.

Figura 5

Diferentes componentes en la definición de Ciberseguridad

Nota. Elaborado con base en (ENISA, 2015)

A continuación, se analizan algunas definiciones de ciberseguridad planteadas por organismos internacionales, tomando como referencia los componentes que pueden constituir la definición de Ciberseguridad con base en ENISA (2015):

Tabla 2

Definiciones de ciberseguridad planteadas por organismos internacionales

Definición del término ciberseguridad ITU, (2008)	Detalles
El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicación, las comunicaciones multimedia, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad. **ITU, (2008) Unión Internacional de Telecomunicaciones. Organización internacional. Documento UIT-T X.1205-(04/2008)**	**Tipo de documento:** de aplicación voluntaria. **Organización:** emisora de estándares internacionales de telecomunicaciones **Motivación fuente de amenaza**: no se menciona. **Origen de amenazas**: los sistemas de información, la red. **El significado de ciber:** contempla su origen en el ciberespacio **Tipo de activos amenazados:** información **CID:** si refiere. La definición describe la seguridad de la información como una gran contribución a la noción de ciberseguridad, a partir de los tres elementos principales que la componen: preservación de la confidencialidad, integridad y disponibilidad de la información. La Recomendación UIT-T X.1205 proporciona una taxonomía de las amenazas a la seguridad desde el punto de vista de la organización. Es un documento de cobertura internacional. Contempla la protección de las personas y la protección de los activos dentro del ciberespacio. Esta definición describe de forma amplia las actividades que involucra la ciberseguridad desde las organizaciones.

https://www.itu.int/rec/T-REC-X.1205-200804-I	

Definición del término ciberseguridad (ISO 27032, 2012)	**Detalles**
Condición de estar protegido contra las consecuencias físicas, sociales, espirituales, financieras, políticas, emocionales, ocupacionales, psicológicas, educativas o de otro tipo de fallas, daños, errores, accidentes, daños o cualquier otro evento en el Ciberespacio que pueda ser considerado no deseable. Nota 1: Esto puede tomar la forma de estar protegido del evento o de la exposición a algo que cause pérdidas económicas o de salud. Puede incluir la protección de las personas o de los bienes. Nota 2: La seguridad en general también se define como el estado de certeza de que algún agente no causará efectos adversos en condiciones definidas. La ciberseguridad seguridad del ciberespacio: preservación de la confidencialidad, integridad y disponibilidad de la información en el Ciberespacio. Nota 1: Además, también pueden estar involucradas otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la confiabilidad. Nota 2: Adaptado de la definición de seguridad de la información en ISO/IEC 27000:2009. **(ISO 27032, 2012) Organización internacional de Normalización. Documento ISO/IEC 27032:2012** https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27032:ed-1:v1:en	**Tipo de documento: d**e aplicación voluntaria. **Organización:** emisora de estándares internacionales de Seguridad de la Información **Motivación fuente de amenaza:** no se menciona. **Origen de amenazas:** los sistemas de información **El significado de ciber:** contempla su origen en el ciberespacio **Tipo de activos amenazados**: información **CID:** si refiere. La definición describe la seguridad de la información como una contribución a la noción de ciberseguridad, a partir de los tres elementos principales que la componen: preservación de la confidencialidad, integridad y disponibilidad de la información. Este estándar propone directrices para la ciberseguridad. En definición contempla la protección de las personas y la protección de los activos dentro del ciberespacio. Esta definición describe de forma amplia las actividades que involucra la ciberseguridad desde las organizaciones. Es un documento de cobertura internacional. Incluye la protección de las personas o de los bienes. Inicia expresando las consecuencias de los eventos no deseables en el ciberespacio.

Definición del término ciberseguridad (NIST, 2015)	**Detalles**
Prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio. https://csrc.nist.gov/glossary/term/cybersecurity	**Tipo de documento:** de aplicación voluntaria. **Organización:** de gobierno. **Motivación fuente de amenaza**: no se menciona. **Origen de amenazas**: los sistemas de información y la red. **El significado de ciber:** contempla su origen en el ciberespacio **Tipo de activos amenazados:** información **CID:** Si refiere. Este documento hace referencia al glosario del Instituto Nacional de Estándares y Tecnología de Estados Unidos NIST es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos

Definición del término ciberseguridad (NICCS, 2017)	Detalles
La actividad o proceso, habilidad o capacidad, o estado mediante el cual los sistemas de información y comunicaciones y la información contenida en ellos están protegidos y/o defendidos contra daños, uso o modificación o explotación, no autorizados. Definición ampliada: estrategia, política y estándares relacionados con la seguridad y las operaciones en el ciberespacio, y que abarcan toda la gama de políticas y actividades de reducción de amenazas, reducción de vulnerabilidades, disuasión, compromiso internacional, respuesta a incidentes, resiliencia y recuperación, incluidas operaciones de redes informáticas, seguridad de la información, aplicación de la ley, diplomacia, misiones militares y de inteligencia en lo que respecta a la seguridad y estabilidad de la infraestructura mundial de información y comunicaciones. **Adaptado de: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, Meta Nacional de Preparación del DHS; Revisión de la política del ciberespacio de la Casa Blanca, mayo de 2009. (NICCS, 2017) Iniciativa nacional de carreras y estudios en ciberseguridad.** **https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#C**	**Tipo de documento:** de aplicación voluntaria. **Organización:** de gobierno. **Motivación fuente de amenaza**: no se menciona. **Origen de amenazas**: los sistemas de información y la red. **El significado de ciber:** contempla su origen en el ciberespacio **Tipo de activos amenazados:** información **CID:** no refiere. NICCS como Iniciativa Nacional de Carreras y Estudios de Ciberseguridad, propone una definición. Este es un documento de cobertura nacional, de aplicación voluntaria. La definición incluye la protección de la información y las comunicaciones en el ámbito nacional. Abarca la protección de los activos dentro del ciberespacio. No precisa los términos 'Confidencialidad', 'Integridad' y 'Disponibilidad. Describe el origen de algunas amenazas. Es una definición planteada desde el contexto país.

Definición del término ciberseguridad EU, (2019).	Detalles
Todas las actividades necesarias para la protección de las redes y sistemas de información de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas. **EU, (2019). Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación.** **https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=EN**	. **Tipo de documento**: de aplicación obligatoria **Organización:** de gobierno **Motivación fuente de amenaza:** no se menciona. **Origen de amenazas:** no menciona. **El significado de ciber:** contempla su origen en el ciberespacio **Tipo de activos amenazados**: información, redes. **CID**: no refiere. El documento constituye el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2009. La definición de ciberseguridad incluye la protección de las redes, sistemas de información y usuarios. No precisa los términos 'Confidencialidad', 'Integridad' y 'Disponibilidad. No señala la protección a determinados activos, ni contempla la frontera del ciberespacio. Describe el origen de algunas amenazas.
Definición del término ciberseguridad (IOSCO, 2016)	**Detalles**

La seguridad cibernética se refiere en términos generales a la capacidad de protegerse contra los ataques cibernéticos y recuperarse de ellos. A los efectos de este informe, la seguridad cibernética se entiende como un concepto muy amplio, que abarca todas las actividades importantes asociadas con la mitigación del riesgo cibernético, es decir, identificar, proteger, detectar, responder y recuperarse de los ataques cibernéticos. **(IOSCO, 2016) Organización Internacional de Comisiones de Valores.** **https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf**	**Tipo de documento:** de aplicación voluntaria para sector financiero. **Organización:** organización internacional **Motivación fuente de amenaza:** no se menciona. **Origen de amenazas:** no refiere. **El significado de ciber:** no menciona el ciberespacio **Tipo de activos amenazados:** información **CID**: no refiere. Este marco denominado "Seguridad cibernética en los mercados de valores: una perspectiva internacional" es un informe sobre los esfuerzos de coordinación de riesgos cibernéticos de IOSCO. La definición relaciona la ciberseguridad con el riesgo cibernético. No precisa los términos 'Confidencialidad', 'Integridad' y 'Disponibilidad. No especifica la protección de las personas, ni activos dentro del ciberespacio. No describe los activos, no especifica el origen de las amenazas.
Definición del término ciberseguridad (IDB;OAS,2020)	**Detalles**
Más allá de la protección operativa de los sistemas y redes, la ciberseguridad es, y seguirá siendo, fundamental para garantizar la integridad y la capacidad de recuperación de los procesos socioeconómicos interconectados, de gobierno y de negocios que operan en el marco del siempre complejo ecosistema tecnológico, por lo que aborda el riesgo cibernético en todos los ámbitos requiere continuos esfuerzos y adaptación. **(IDB; OAS,2020)** **https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf**	**Tipo de documento:** de aplicación voluntaria **Organización:** organización internacional **Motivación fuente de amenaza:** no se menciona. **Origen de amenazas:** no refiere. **El significado de ciber:** no menciona el ciberespacio **Tipo de activos amenazados:** información **CID**: no refiere. Este informe "Riesgos, avances y el camino a seguir en América Latina y el Caribe 2020" expone la situación actual de la ciberseguridad en América Latina. La definición que presentan es de aplicación voluntaria y hace referencia al papel en aspectos sociales, económicos y de gobierno. No precisa los términos 'Confidencialidad', 'Integridad' y 'Disponibilidad. No especifica la protección de las personas, ni la protección de los activos dentro del ciberespacio. No describe los activos, no especifica el origen de las amenazas.

A partir de las definiciones analizadas en la Tabla 2, se puede observar la falta de uniformidad en torno al concepto de ciberseguridad, y como dos de éstas, ITU (2008) e ISO (2012), relacionan el mayor número de componentes. Las demás presentan un alcance reducido, al no abordarlos en su mayoría y no incluir los elementos de la seguridad de la información, la protección de las personas y omitir la salvaguarda de los activos físicos.

En general, el número de opciones por cada componente y las diferencias marcadas en el concepto desde la mirada transnacional, dificultan su estudio y por ende su aplicación. De acuerdo con Martin et al. (2021), gran parte de estas definiciones depositan una confianza excesiva en los controles técnicos y se centran, casi exclusivamente, en la información; extenderlos para relacionarlos con los sistemas físicos cibernéticos conectados a la red es un desafío apremiante para evitar que los dispositivos físicos presenten comportamientos no deseados. Bajo este panorama, coincidimos con ENISA, (2015): “Se debe considerar una definición contextual de ciberseguridad, basada en una que sea relevante, se ajuste y se use por parte de una organización emisora de estándares internacionales o en una organización en particular. No es necesario que exista una definición de ciberseguridad, en el sentido convencional que tendemos a aplicar definiciones a las cosas simples. El problema es que ciberseguridad es un término envolvente, y no es posible hacer una definición para cubrir el alcance de las cosas que abarca”.

En esta misma línea, según Cavelty (2010), el discurso y la investigación en ciberseguridad “necesariamente cambia a contextos y condiciones que determinan el proceso por el cual los actores clave llegan subjetivamente a una comprensión compartida de cómo conceptualizar y, en última instancia, responder a una amenaza a la seguridad”. Respecto a la afirmación de ENISA (2015), probablemente resume la incertidumbre entre los muchos actores en este campo sobre lo que implica exactamente la ciberseguridad. Esta interpretación de la ciberseguridad como un "término envolvente", junto con las muchas definiciones e interpretaciones diversas, hacen que no sea fácil explicar ya en el terreno de las organizaciones exactamente cuál es su responsabilidad y el alcance de la rendición de cuentas hacia la ciberseguridad (Von Solms & Von Solms, 2018). En general, podemos concluir que una definición de ciberseguridad requiere contemplar aspectos mínimos como la protección de las cualidades de la seguridad de la información, la protección de las personas y los activos físicos e infraestructuras que se encuentran en el ciberespacio.

Bajo este panorama, coincidimos con ENISA, (2015): “Se debe considerar una definición contextual de ciberseguridad, basada en una que sea relevante, se ajuste y se use por parte de una organización emisora de estándares internacionales o en una organización en particular. No es necesario que exista una definición de ciberseguridad, en el sentido convencional que tendemos a aplicar definiciones a las cosas simples. El problema es que ciberseguridad es un término envolvente, y no es posible hacer una definición para cubrir el alcance de las cosas que abarca”.

En esta misma línea, según Cavelty (2010), el discurso y la investigación en ciberseguridad “necesariamente cambia a contextos y condiciones que determinan el proceso por el cual los actores clave llegan subjetivamente a una comprensión compartida de cómo conceptualizar y, en última instancia, responder a una amenaza a la seguridad”. Respecto a la afirmación de ENISA (2015), probablemente resume la incertidumbre entre los muchos actores en este campo sobre lo que implica exactamente la ciberseguridad. Esta interpretación de la ciberseguridad como un "término envolvente", junto con las muchas definiciones e interpretaciones diversas, hacen que no sea fácil explicar ya en el terreno de las organizaciones exactamente cuál es su responsabilidad y el alcance de la rendición de cuentas hacia la ciberseguridad (Von Solms & Von Solms, 2018). En general, podemos concluir que una definición de ciberseguridad requiere contemplar aspectos mínimos como la protección de las cualidades de la seguridad de la información, la protección de las personas y los activos físicos e infraestructuras que se encuentran en el ciberespacio.

1.2. La ciberseguridad en las organizaciones

Las fallas de ciberseguridad en las organizaciones se han convertido en uno de los riesgos de mayor probabilidad e impacto. Bajo este panorama, la ciberseguridad desde las organizaciones es una práctica que sensibiliza y prepara a sus partes para enfrentar el riesgo cibernético propio de este ecosistema digital en donde se desarrolla, y establece un conjunto de estrategias y políticas para la protección, defensa, control y resiliencia. En este apartado se busca advertir del desenvolvimiento del riesgo cibernético en el mundo corporativo y los aspectos que las organizaciones requieren para mitigar y hacer frente a este tipo de amenazas.

La Confederación Europea de Asociaciones de Directores (ecoDa) ha descrito la ciberseguridad como la "amenaza de más rápido crecimiento y quizás la más peligrosa" a la que se enfrentan las organizaciones en la actualidad (Clinton & Higgins, 2020). Según EY (2020), seis de cada diez organizaciones han sufrido un incidente cibernético material o significativo en los últimos doce meses. Los riesgos no podrían ser mayores. Los atacantes cada vez más sofisticados están sondeando los rincones oscuros de los sistemas y redes, buscando y encontrando vulnerabilidades (PwC, 2022), apuntando a un área de superficie cada vez mayor y utilizando tácticas más impredecibles. Cano (2021) plantea que los ciber-riesgos son riesgos líquidos porque adquieren la característica de líquidos, pues se configuran y mutan de acuerdo con el nivel acoplamiento e interacción que tienen los objetos físicos digitalmente modificados, creando zonas ciegas de control que terminan motivando escenarios inciertos, con objetos no conocidos y consecuencias inesperadas.

De acuerdo con Ernst & Young (2021), la disrupción económica y operativa desatada por COVID-19 ha aumentado notablemente tanto la motivación como la oportunidad para atacantes cibernéticos: un grupo grande y diverso que va desde actores patrocinados por el estado y grupos del crimen organizado hasta individuos motivados financieramente y activistas políticos y sociales tecnológicamente habilitados. Teniendo en cuenta que la organización para su funcionamiento se estructura en dimensiones temáticas que representan los elementos de cómo operan, se describe a continuación cómo la ciberseguridad se involucra en la gobernanza, gestión de riesgos, estrategia corporativa y evaluación de las implicaciones financieras.

1.2.1. Gobernanza del riesgo de ciberseguridad

La gobernanza se presenta en este estudio como uno de los elementos que direccionan la operación de las organizaciones. Desde la óptica del riesgo de ciberseguridad se busca definir el papel de la junta directiva o la alta dirección en el manejo de este riesgo emergente. De acuerdo con Burnap (2021), la gobernanza de riesgos se define como un conjunto general de procesos y principios en curso que tiene como objetivo garantizar la conciencia y la educación de los riesgos que se enfrentan cuando ocurren ciertas acciones, y para inculcar un sentido de responsabilidad y rendición de cuentas a todos los involucrados en su gestión. Según Renn (2008), es la base de la toma de decisiones colectivas y abarca tanto la evaluación como la gestión de riesgos, incluida la consideración de los contextos legal, social, organizativo y económico en los que se evalúa el riesgo.

La Blue Ribbon Commission de la NACD sobre Gobernanza del Riesgo recomendó que la supervisión del riesgo debería ser una función de toda la junta (NACD, 2009). En relación con el riesgo de ciberseguridad, OEA Internet Security Allience (2020) señala que las juntas directivas deben asumir un papel de liderazgo en la supervisión de la seguridad de los sistemas cibernéticos de su empresa. Antes de considerar cómo la junta debe supervisar las actividades de la organización para administrar el riesgo, es útil considerar las metas y objetivos de este esfuerzo de supervisión. ¿Qué debe tratar de lograr la junta en su función de supervisión? Es importante señalar que "supervisión"

incorpora tanto la función de vigilancia de los directores como la toma de decisiones que involucra el juicio desde el negocio. Si bien los objetivos de supervisión de riesgos pueden variar de una compañía a otra, cada directorio debe estar seguro que (NACD, 2009):

- El apetito de riesgo implícito en el modelo de negocio, estrategia y ejecución de la compañía es adecuado.
- Los riesgos esperados son proporcionales a los beneficios esperados.
- La dirección ha implantado un sistema de gestión, seguimiento y mitigación de riesgos adecuado al modelo de negocio y estrategia de la empresa.
- El sistema de gestión de riesgos informa al directorio de los principales riesgos que enfrenta la compañía.
- Existe una adecuada cultura de concienciación del riesgo en toda la organización.
- Se reconoce que la gestión del riesgo es fundamental para la ejecución exitosa de la estrategia de la empresa.

Por su parte, el estándar COSO (2017) contempla cinco componentes para el manejo del riesgo; el primero de ellos, la gobernanza. Desde este marco, la gobernanza: (1) ejerce la supervisión de riesgos del directorio, (2) establece la estructura de las operaciones, (3) define la cultura deseada, y (4) demuestra compromiso con los valores fundamentales. ISO IEC 27014:2020 establece que la gobernanza de ciberseguridad es un sistema mediante el cual se dirigen y controlan las actividades de seguridad de la información de una organización (ISO, 2020) para la protección de los activos de información digital frente a los riesgos relacionados con el uso de Internet (Von Solms & Von Solms, 2018).

Las pautas de la Asociación Nacional de Directores Corporativos (NACD) aconsejan que las juntas evalúen los riesgos cibernéticos considerando toda la empresa y comprendan los posibles impactos legales: “Deben analizar, conjuntamente con la gerencia, los riesgos de ciberseguridad y la preparación y tener en cuenta las amenazas cibernéticas en el contexto de la tolerancia general al riesgo de la organización”(NACD, 2009). El papel principal de la junta en la organización puede ser la supervisión, pero los miembros de la junta están siendo cada vez más atraídos hacia el meollo de los problemas de seguridad cibernética (Deloitte, 2019). Los líderes organizacionales reconocen ahora la importancia de verificar y salvaguardar la información de su negocio; el hecho de que en muchas ocasiones este tipo de eventos sean el primer eslabón de una serie de acciones consecutivas que, mal gestionadas, pueden tener un gran impacto en la reputación de la compañía, han convertido a los ciberataques en una de las principales preocupaciones de los directivos (PwC, 2022). Es probable que la evaluación de riesgos y el desarrollo de principios de mitigación para gestionarlos sean efectivos siempre que exista una política de gobernanza coordinada y bien comunicada dentro el sistema que se gestiona (Rashid et al., 2019).

OEA; ISA (2020) propone cinco principios para la supervisión efectiva del riesgo cibernético, advierte que los directores adaptarán estas recomendaciones en función de las características únicas de su organización, incluyendo el tamaño, la etapa del ciclo de vida, la estrategia, los planes de negocios, el sector industrial, la huella geográfica, la cultura, los vínculos con las empresas familiares y las inquietudes de las partes interesadas mayoritarias. De acuerdo con Rashid et al. (2019), la seguridad cibernética debe pensarse como un conjunto claro de procesos que reducen el riesgo de daños a las personas y la empresa. Todos los involucrados en el diario funcionamiento del sistema en cuestión deben comprender que la seguridad es eficaz y hace parte de la cultura operativa diaria (PwC, 2022; Rashid et al., 2019). Vale la pena señalar que,

según EY (2021), los propios miembros de la junta pueden ser objetivos de interés para los piratas informáticos. Esto se debe a:

- Tienen acceso a datos comerciales confidenciales.
- Es posible que hayan recibido una capacitación limitada en seguridad cibernética y no necesariamente estarán en el radar del equipo de TI de la organización debido a su antigüedad.
- Pueden estar intercambiando información confidencial por correo electrónico, exponiendo inadvertidamente a la organización al riesgo de ataques cibernéticos y filtraciones de datos.

A partir de estos imaginarios, se puede decir que es desde la gobernanza donde se lidera y supervisa el proceso contra el riesgo de ciberseguridad y la actitud del gobierno corporativo es decisiva en este proceso porque de su conocimiento, compromiso y sus actuaciones puede depender el futuro de la organización. Los comités con responsabilidad destinada a la supervisión del riesgo (y para la supervisión de los riesgos relacionados con la cibernética en particular) deben recibir información general sobre ciberseguridad por lo menos trimestralmente y cuando surjan incidentes o situaciones específicas (OEA; ISA, 2020). El riesgo de ciberseguridad en las organizaciones puede ser designado bien sea al comité de auditoría o al comité de riesgos de ciberseguridad (Deloitte, 2016).

1.2.2. Estrategia de ciberseguridad

La estrategia de ciberseguridad se presenta en este estudio como el segundo elemento que direcciona la operación de las organizaciones. Acorde con el marco internacional COSO (2017), la estrategia se considera el segundo componente en el marco de la gestión de riesgos y le corresponde: (1) Analizar el contexto de los negocios (2) Definir el apetito del riesgo corporativo, (3) Evaluar la estrategia alternativa y (4) Formular los objetivos de los negocios. Las empresas entienden que las prácticas básicas de seguridad de la información, sustentadas en los estándares ISO 27002, NIST SP800-53, determinan los elementos que articulan las estrategias que se desarrollen para asegurar la nueva función de ciberseguridad de la organización (Cano, 2021).

Una estrategia de ciberseguridad se compone de planes de alto nivel sobre cómo una organización va a asegurar sus activos y minimizar el riesgo cibernético. Por lo general, se desarrollan con una visión de tres a cinco años y son objeto de actualización y revisión con la mayor frecuencia posible (AT&T Cybersecurity, 2021). Hoy en día, es crucial tener una estrategia bien articulada de cumplimiento y control legal y una gobernanza sólida para reducir los errores técnicos (Calderón et al., 2018). Uno de los objetivos más críticos para cualquier estrategia de ciberseguridad es lograr la ciber-resiliencia; para ello, los líderes empresariales deben tener en cuenta que cada organización es única y requiere un enfoque de estrategia personalizado (AT&T Cybersecurity, 2021). Si bien es responsabilidad de todos cooperar para garantizar una mayor resiliencia cibernética, los líderes que establecen la estrategia para una organización son los responsables en última instancia y se les ha hecho cada vez más responsables de incluir la resiliencia cibernética en la estrategia organizacional (WEF, 2017).

Desde esta perspectiva, podemos observar que la estrategia es el eje articulador de la gestión de riesgos corporativos. En el ámbito de la ciberseguridad, de acuerdo con Kent Baker et al. (2020), la junta directiva es de vital importancia para la empresa porque proporciona el enfoque estratégico y protege los intereses de los accionistas. Dentro del gobierno corporativo, el comité de auditoría es generalmente el responsable de la estrategia de ciberseguridad (Héroux & Fortin, 2020). En la elaboración de esta

estrategia las organizaciones enfrentan una batalla cuesta arriba al intentar definir procedimientos administrativos para cada posible situación de riesgo de seguridad. Por lo tanto, es necesario considerar la mentalidad de los empleados con respecto a la seguridad de la información (Karlsson et al., 2015). Las empresas deben considerar todo el ecosistema de ciberseguridad que consiste en el riesgo cibernético, los impactos en la sociedad, la capacitación y educación, la ética, las técnicas, etc. (Radu & Smaili, 2021). Cuando se trata de gestionar el riesgo, un enfoque proactivo siempre es superior a uno reactivo. Pero para ser proactivo, especialmente cuando se descubren y detectan nuevas amenazas a un ritmo tan alarmante (AT&T Cybersecurity, 2021), se requiere de una estrategia organizacional dinámica y pensada al largo plazo.

1.2.3. Gestión de riesgos de ciberseguridad

El riesgo está en el corazón de la vida cotidiana (Martin et al., 2021). Respecto a los indicios del riesgo, Slovic (1987) comenta: “Ha surgido como uno de los principales temas políticos de los años ochenta. El descubrimiento frecuente de nuevos peligros y la amplia publicidad que recibe está causando que más y más individuos se vean a sí mismos como las víctimas, más que beneficiarios, de la tecnología. Estos miedos y la oposición a la tecnología que producen han desconcertado a industriales y reguladores frustrados y han llevado a numerosos observadores para argumentar que la aparente búsqueda de un ‘riesgo cero’ amenaza la estabilidad política y económica de la nación”. Esta reseña, consignada en 1987, coincide con la definición de riesgos de Renn (1998): “los riesgos son siempre representaciones mentales de amenazas que son capaces de reclamar pérdidas reales”. El autor precisa que el riesgo es una construcción social y a la vez el resultado de una estimación técnica. Las personas han tenido que lidiar con peligros a lo largo de la historia, pero es solo recientemente que han podido hacerlo de una manera anticipada y sistemática para controlar el riesgo (NCSC, 2022).

Una de las definiciones más recientes es la de Strupczewski (2021): “El riesgo cibernético es un riesgo operativo asociado con la realización de actividades en el ciberespacio, amenazando los activos de información, los recursos TIC y los activos tecnológicos, que pueden causar daños materiales a los activos tangibles e intangibles de una organización, interrupción del negocio o daño a la reputación”.

Considerando el riesgo operativo como “la posibilidad de ocurrencia de pérdidas derivadas de la materialización de una amplia variedad de eventos que incluyen fraude, robo, piratería informática, pérdida de personal clave, juicios, pérdida de información, terrorismo, vandalismo y desastres naturales” (Moosa, 2007), vemos cómo el riesgo cibernético corresponde con esta definición; se espera que este tipo de riesgo opere a partir de un sistema de gestión de riesgo empresarial (ERM, por sus siglas en inglés) relevante, debidamente desarrollado y en operación, en el que se recopilan, evalúan, priorizan, mitigan e informan adecuadamente los principales riesgos estratégicos de la empresa y otros riesgos (OEA; ISA, 2020).

Un proceso de gestión de riesgos cibernéticos aplica técnicas de mitigación y transferencia de riesgos para reducir el riesgo residual a niveles aceptables (Gordon, Loeb, & Sohail, 2003; Marotta & McShane, 2018; Siegel et al., 2002). Algunos autores proponen la compra de seguros como una estrategia para mitigar y transferir el riesgo (Bolot & Lelarge, 2008; Gordon, Loeb, & Lucyshyn, 2003; Siegel et al., 2002; Zeller & Scherer, 2020). Durante el proceso de gestión de riesgos, existe una interacción entre la mitigación de riesgos y la compra de seguros, es decir, los compradores de seguros suelen pagar primas más bajas al invertir más en la mitigación de riesgos (McShane et al., 2021).

La evaluación holística de los riesgos de ciberseguridad es un problema complejo de múltiples componentes y niveles que involucra hardware, software, factores ambientales y humanos (Henshel et al., 2015). De acuerdo con McShane & Nguyen (2020), este riesgo es difícil de incluir en el proceso general de gestión de riesgos empresariales; es necesario avanzar hacia la resiliencia cibernética para hacer frente a un riesgo tan complejo. El ciberriesgo, como una propiedad emergente de las relaciones digitalmente modificadas de la realidad, establece un reto cognitivo y social que demanda romper con los paradigmas disciplinares para encontrar respuestas o mejores preguntas en escenarios cada vez más inestables e inciertos, fruto de una mayor densidad digital en la dinámica de los elementos sociales (Cano, 2021). De acuerdo con Eling & Schnell (2016a) los riesgos cibernéticos se pueden clasificar según la actividad (p. ej., delictiva y no delictiva), el tipo de ataque (p. ej., malware, ataque interno, spam, denegación de servicio distribuida) y la fuente (p. ej., terroristas, delincuentes y gobierno). Los ataques dependen principalmente de la actividad delictiva y se ven reforzados por efectos de red (por ejemplo, gusanos).

Von Solms & Van Niekerk (2013) definen como gestión del riesgo cibernético la protección de los activos de información y no información que se encuentran dentro del ciberespacio o que pueden verse afectados a través del ciberespacio. Para implementar un marco de ciberseguridad efectivo, el proceso de gestión de riesgos de una organización comienza con una comprensión clara del entorno de amenazas y vulnerabilidades, su particular apetito de riesgo y la disponibilidad de recursos necesarios para mitigar los riesgos cibernéticos potenciales, los cuales deben abordarse desde una perspectiva estratégica, económica, interdepartamental e inter divisional (Internet Security Alliance and American National Standards, 2010).

En tal sentido, el ciberriesgo se configura como una apuesta relacional entretejida en la conectividad de los objetos físicos y las realidades sociales, que cambia la manera como se percibe el mundo y crea escenarios inéditos que retan las prácticas de gestión de riesgos actuales (Cano, 2021). La evaluación del riesgo, tanto cuantitativa como cualitativa, son procesos imprescindibles para lograr modelos de gestión de riesgos maduros y confiables (Escuela Europea, 2022). Sin embargo, según PwC (2022), solo el 26% cuantifica los riesgos cibernéticos hoy. Para COSO ERM (2017) la evaluación de riesgos involucra un proceso dinámico e interactivo para identificar y analizar riesgos que afectan el logro de objetivos de la entidad, dando las bases para determinar cómo los riesgos deben ser administrados (COSO, 2017). La evaluación de riesgos es, por lo tanto, un proceso de recopilación de observaciones y percepciones del mundo que pueden justificarse mediante razonamiento lógico o comparaciones con resultados reales (Renn, 2008).

Las características distinguen fundamentalmente al riesgo cibernético de otro tipo de riesgos. En primer lugar, la realidad virtual enfatiza el carácter intangible y, por tanto, las dificultades para evaluar las pérdidas. En segundo lugar, las redes están estrechamente relacionadas con el término ciberespacio, que con frecuencia se utiliza como sinónimo de Internet (Biener & Eling, 2012). Un aspecto importante para una buena gestión del riesgo cibernético es que el riesgo cibernético no es responsabilidad del departamento de TI; requiere un diálogo global entre los diferentes departamentos (p. ej., sensibilización, formación) (Eling & Schnell, 2016b). Además, el compromiso institucional, demostrado al tener un responsable de seguridad de la información, es muy importante. Las empresas deben contar con un director de seguridad de la información o un puesto similar (Eling & Schnell, 2016b)

El ciber-riesgo, como una propiedad emergente de las relaciones digitalmente modificadas de la realidad, establece un reto cognitivo y social que demanda romper con los paradigmas disciplinares, para encontrar respuestas o mejores preguntas en

escenarios cada vez más inestables e inciertos, fruto de una mayor densidad digital en la dinámica de los elementos sociales.(Cano, 2021). El riesgo cibernético puede mitigarse y minimizarse significativamente si se aborda como un problema de gestión de riesgos en toda la empresa. Sin embargo, al igual que con los riesgos tradicionales, los cibernéticos nunca podrán eliminarse por completo.

1.2.4. Implicaciones financieras

Según WEF (2021), en menos de una década la ciberseguridad se ha convertido en uno de los problemas sistémicos más importantes para la economía mundial; el gasto global colectivo ha alcanzado los 145.000 millones de dólares al año y los incidentes y ataques siguen aumentando. Las empresas afectadas por ciberataques tienden a sufrir pérdidas económicas y de reputación duraderas (Agrafiotis et al., 2018; Kamiya et al., 2020). Los riesgos e incidentes de ciberseguridad pueden afectar el desempeño financiero o la posición de una empresa (SEC, 2022). Estas consecuencias financieras negativas, se materializan en costos de investigación forense, honorarios de abogados, gastos de litigio, costos de mejora de la seguridad cibernética y aumentos de las primas del seguro de riesgo cibernético (Deloitte, 2019; Meisner, 2018).

Bajo este panorama, la inversión en seguridad debe analizarse utilizando un enfoque holístico que combine diferentes factores (Bose & Luo, 2014) que permitan, entre otros, proteger a las empresas contra eventos negativos (Gordon & Loeb, 2002). Sin embargo, las consecuencias de los diferentes incidentes cibernéticos y las violaciones de seguridad no solo repercuten al interior de las organizaciones sino que generan impactos globales asociados con una reacción negativa en los mercados (Berkman et al., 2018; Gordon et al., 2010).

Conclusiones

La ciberseguridad en los últimos treinta años ha obtenido un posicionamiento mundial sin precedentes. La multidimensionalidad e interdisciplinariedad de su significado nos permite afirmar hoy que no existe un único concepto de aceptación mundial de este término. Para ratificar la amplia cobertura de su significado podemos citar la iniciativa inglesa CYBOK (2021) y los dominios planteados por ENISA (2015).

Los antecedentes de la evolución del concepto de ciberseguridad presentan términos relacionados que aportan en la construcción de su definición. Se trata de expresiones que cuentan con significados diferentes: seguridad informática, seguridad de la información y riesgo cibernético. Al respecto, es de resaltar que la definición de la seguridad de la información aporta las cualidades de la información en el ámbito organizacional: preservación de la confidencialidad, integridad y disponibilidad. En general, el concepto de ciberseguridad requiere contemplar la protección de tres aspectos que necesariamente se adhieren a su definición: la protección de las personas, la protección de las cualidades de la seguridad de la información, y la protección de los activos físicos e infraestructuras que se encuentran en el ciberespacio.

Según nuestra búsqueda, un número reducido de autores se dan a la tarea de proponer una definición de ciberseguridad: Craigen et al. (2014); Gordon et al. (2006); Haapamäki & Sihvonen (2019); Le & Hoang, (2017); Reid & Van Niekerk, 2014; Schatz et al. (2017); Tissir et al. (2020); Von Solms & Von Solms (2018). De igual manera, y respecto a las definiciones de ciberseguridad planteadas por organismos internacionales, se puede observar la falta de uniformidad en torno al concepto, y el reducido alcance que presentan frente a los elementos que deben constituir hoy su definición: la seguridad de la información, la protección de las personas y la salvaguarda de los activos físicos.

Desde el ámbito corporativo, las fallas de ciberseguridad son uno de los riesgos de mayor probabilidad e impacto. Bajo este panorama, la ciberseguridad desde las organizaciones es una práctica que sensibiliza y prepara a sus partes para enfrentar el riesgo cibernético propio de este ecosistema digital en donde se desarrolla, y establece un conjunto de estrategias y políticas para la protección, defensa, control y resiliencia.

Es importante señalar que el proceso de seguridad cibernética se lleva a cabo por parte de toda la organización y para su funcionamiento se estructura en dimensiones temáticas que representan los elementos de cómo operan las organizaciones: (i) gobernanza (base para la toma de decisiones por parte de la junta directiva o la alta gerencia sobre las estrategias de las organizaciones con el objetivo de lograr la supervisión y liderazgo para el manejo del riesgo cibernético), (ii) estrategia corporativa (una estrategia de ciberseguridad se compone de planes de alto nivel sobre cómo una organización va a asegurar sus activos y minimizar el riesgo cibernético), (iii) gestión de riesgos (sistema de gestión de riesgo empresarial en el que se priorizan, mitigan e informan los principales riesgos de la organización), y (iv) evaluación de las implicaciones financieras (la afectación económica que traen consigo las pérdidas económicas y de reputación por posibles ciberataques o incidentes cibernéticos requieren ser evaluadas y valoradas dentro de la información financiera y no financiera de la organización).

Referencias

Adams, A., & Sasse, M. A. (1999). Users Are Not The Enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/CYBSEC/TYY006

Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). *Towards a Taxonomy of Information Security Management Practices in Organisations*. https://openrepository.aut.ac.nz/handle/10292/8174

Althonayan, A., & Andronache, A. (2018). Shifting from information security towards a cybersecurity paradigm. *ACM International Conference Proceeding Series*, *September 2018*, 68–79. https://doi.org/10.1145/3285957.3285971

AT&T Cybersecurity. (2021). *What is a Cybersecurity Strategy and How to Develop One*. https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Biener, C., & Eling, M. (2012). *Insurability in Microinsurance Markets: An Analysis of Problems and Potential Solutions*. *37*, 77–107. https://doi.org/10.1057/gpp.2011.29

Blakley, B., Mcdermott, E., Morganchase, J. P., & Geer, D. (2002). Information Security is Information Risk Management. *Proceedings of the 2001 Workshop on New Security Paradigms - NSPW '01*. https://doi.org/10.1145/508171

Bose, R., & Luo, X. (2014). Investigating security investment impact on firm performance. *International Journal of Accounting & Information Management*, *22*(3), 194–208. https://doi.org/10.1108/IJAIM-04-2014-0026

Burnap, P. (2021). Risk Management & Governance Knowledge Area. *The Cyber Security Body Of Knowledge*, 19–48.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert

Elicitation. *Risk Analysis*. https://doi.org/10.1111/RISA.13687
Calderón, R., Piñero, R., & Redín, D. M. (2018). Can compliance restart integrity? Toward a harmonized approach. The example of the audit committee. *Business Ethics: A European Review*, *27*(2), 195–206. https://doi.org/10.1111/BEER.12182
Cano, J. (2021). *Ciberseguridad empresarial Reflexiones y retos para los ejecutivos del siglo XXI*.
Cavelty, M. D. (2010). *Cyber-Security* (Routledge (ed.)). The Routledge Handbook of New Security Studies: 154-162.
Cebula, J. J., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks CERT ® Program A Taxonomy of Operational Cyber Security Risks The original document contains color images*. *December*. http://www.sei.cmu.edu
Chang, H. C. (2016). The Synergy of Scientometric Analysis and Knowledge Mapping with Topic Models: Modelling the Development Trajectories of Information Security and Cyber-Security Research. *Http://Dx.Doi.Org/10.1142/S0219649216500441*, *15*(4). https://doi.org/10.1142/S0219649216500441
Clinton, L., & Higgins, J. (2020). *Cyber-Risk Oversight Cyber-Risk Oversight*.
Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions. *Environment Systems and Decisions 2013 33:4*, *33*(4), 469–470. https://doi.org/10.1007/S10669-013-9484-Z
COSO. (2017). *COSO II ERM*.
Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/TIMREVIEW/835
Da Veiga, A., & Eloff, J. H. P. (2007). An Information Security Governance Framework. *Https://Doi.Org/10.1080/10580530701586136*, *24*(4), 361–372. https://doi.org/10.1080/10580530701586136
Deloitte. (2016). *Cyber security: The changing role of the Board and the Audit Committee*. *June*, 5. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-cyber-security-noexp.pdf
Deloitte. (2019). Managing Cyber Risk in a Digital Age. *Coso*, 28. https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf
Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855
Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law and Security Review*, *40*, 105513. https://doi.org/10.1016/j.clsr.2020.105513
Eling, M., & Schnell, W. (2016a). What do we know about cyber risk and cyber risk insurance? In *Journal of Risk Finance* (Vol. 17, Issue 5, pp. 474–491). Emerald Group Publishing Ltd. https://doi.org/10.1108/JRF-09-2016-0122
Eling, M., & Schnell, W. (2016b). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122/FULL/PDF
ENISA. (2015). Definition of Cybersecurity | Gaps and overlaps in standardisation. In *European Union Agency For Network And Information Security: Vol. v1.0* (Issue December).
Ernst & Young. (2021). *EY Global Information Security Survey 2021: Cybersecurity: how do you rise above the waves of a perfect storm?*
EU. (2019). *Regulation (EU) 2019/881*. Regulation (EU) 2019/881 of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN
Excelencia, E. E. de. (2022). *Evaluación del riesgo cuantitativa vs cualitativa: ¿cuál escoger?* https://www.escuelaeuropeaexcelencia.com/2020/11/evaluacion-del-

riesgo-cuantitativa-vs-cualitativa-cual-escoger/
EY. (2020). *EY Global Information Security Survey 2020. How does security evolve from bolted on to built-in?* https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-single-pages.pdf
EY. (2021). *Board Agenda 2021*. *1*(1), 21.
Fidler, D. P. (2020). Cybersecurity in the Time of COVID-19. *Council on Foreign Relations*, *2020*, 7–9. https://www.cfr.org/blog/cybersecurity-time-covid-19
Gómez Vieites, A. (2006). *Enciclopedia de la seguridad informática*.
Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274
Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach. In *Computer Security Journal* (Vol. 19, Issue 2, pp. 1–7). Computer Security Institute.
Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, *25*(5), 503–530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005
Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81–85. https://doi.org/10.1145/636772.636774
Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly: Management Information Systems*, *34*(SPEC. ISSUE 3), 567–594. https://doi.org/10.2307/25750692
Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. In *Managerial Auditing Journal* (Vol. 34, Issue 7, pp. 808–834). Emerald Group Publishing Ltd. https://doi.org/10.1108/MAJ-09-2018-2004
Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a Human Factor in Holistic Cyber Security Risk Assessment. *Procedia Manufacturing*, *3*, 1117–1124. https://doi.org/10.1016/J.PROMFG.2015.07.186
Héroux, S., & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220
International Telecommunication Union. (2008). Overview Cybersecurity. *ITU-T X.1205 Recommendation*, *1205*(Rec. ITU-T X.1205 (04/2008)), 2–3. https://www.itu.int/rec/T-REC-X.1205-200804-I
Internet Security Alliance and American National Standards. (2010). The Financial Management of Cyber Risk: An Implementation Framework for CFOs. *Order A Journal On The Theory Of Ordered Sets And Its Applications*.
IOSCO. (2016). *Cyber Security in Securities Markets – An International Perspective Report on IOSCO ' s cyber risk coordination efforts*.
ISO. (2012). *ISO/IEC 27032: Information technology — Security techniques — Guidelines for cybersecurity*. ISO 27032. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en
ISO. (2013). *ISO 27002*.
ISO. (2020). *ISO/IEC 27014:2020 - Information security, cybersecurity and privacy protection — Governance of information security*. https://www.iso.org/standard/74046.html
Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*. https://doi.org/10.1016/j.jfineco.2019.05.019
Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013. *Information & Computer Security*, *23*(3), 246–285. https://doi.org/10.1108/ICS-05-2014-0033

Kent Baker, H., Pandey, N., Kumar, S., & Haldar, A. (2020). A bibliometric analysis of board diversity: Current status, development, and future research directions. *Journal of Business Research*, *108*, 232–246. https://doi.org/10.1016/j.jbusres.2019.11.025

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, *41*(5), 597–607. https://doi.org/10.1016/J.IM.2003.08.001

Le, N. T., & Hoang, D. B. (2017). Can maturity models support cyber security? *2016 IEEE 35th International Performance Computing and Communications Conference, IPCCC 2016*. https://doi.org/10.1109/PCCC.2016.7820663

Madnick, S. E. (1978). Management policies and procedures needed for effective computer security. *Sloan Management Review*, *20*(1), 61–74.

Marotta, A., & McShane, M. (2018). Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach. *Risk Management and Insurance Review*, *21*(3), 435–452. https://doi.org/10.1111/RMIR.12109

Martin, A., Rashid, A., Chivers, H., Schneider, S., Lupu, E., & Danezis, G. (2021). Introduction to CyBOK Knowledge Areas. *The Cyber Security Body of Knowledge*, 22. www.cybok.org

McShane, M., Eling, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93–125. https://doi.org/10.1111/RMIR.12169

McShane, M., & Nguyen, T. (2020). Time-varying effects of cyberattacks on firm value. *Geneva Papers on Risk and Insurance: Issues and Practice*, *45*(4), 580–615. https://doi.org/10.1057/s41288-020-00170-x

Meisner, M. (2018). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting*, *6*(3), 63. https://doi.org/10.12775/cjfa.2017.017

Merriam -Webster. (2021). *Cybersecurity | Definition of Cybersecurity*. Merriam-Webster.Com Dictionary, Merriam-Webster. https://www.merriam-webster.com/dictionary/cybersecurity

Moosa, I. A. (2007). Operational Risk: A Survey. *Financial Markets, Institutions & Instruments*, *16*(4), 167–200. https://doi.org/10.1111/J.1468-0416.2007.00123.X

NACD. (2009). *Report of the NACD blue ribbon commission. Risk governance: balancing risk and reward*. https://www.wlrk.com/docs/1605831_1.pdf

NCSC. (2022). *Essential Topics - NCSC.GOV.UK*. https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics

NICCS. (2017). *Cybersecurity Glossary | National Initiative for Cybersecurity Careers and Studies*. Explore Terms: A Glossary of Common Cybersecurity Terminology. https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary#C (2017)

OEA; ISA. (2020). *Manual de supervisión de riesgos cibernéticos para juntas corporativas*. https://www.oas.org/es/sms/cicte/docs/ESP-Manual-de-Supervision-de-riesgos-ciberneticos-para-juntas-coporativas.pdf

PwC. (2022). *2022 Global Digital Trust Insights*.

Radu, C., & Smaili, N. (2021). Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure. *Journal of Business Ethics*, *1*, 3. https://doi.org/10.1007/s10551-020-04717-9

RAE ASALE. (2020). *Diccionario de la lengua española*. Edición 2020. https://dle.rae.es/cibernético?m=form

Ramirez, R., & Choucri, N. (2016). Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review. *IEEE Access*, *4*, 2216–2243. https://doi.org/10.1109/ACCESS.2016.2544381

Rashid, A., Chivers, H., Danezis, G., Lupu, E., & Martin, A. (2019). The Cyber Security Body of Knowledge (CyBoK) 1.0. *CyBoK*, 299. https://www.cybok.org/

Reid, R., & Van Niekerk, J. (2014). From Information Security to Cyber Security Cultures Organizations to Societies. *Information Security South Africa (ISSA)*, 1–

7. https://doi.org/978-1-4799-3383-9
Renn, B. O. (2008). Risk Governance new & Forthcoming Titles. In *Sustainable Development*. https://www.routledge.com/Risk-Governance-Coping-with-Uncertainty-in-a-Complex-World/Renn/p/book/9781844072927
Renn, O. (1998). The role of risk perception for risk management. *Reliability Engineering and System Safety*, *59*(1), 49–62. https://doi.org/10.1016/S0951-8320(97)00119-1
Rowe, D. C., Ekstrom, J. J., & Lunt, B. M. (2012). Cyber-Security, IAS and the Cyber Warrior. *The Colloquium for Information Systems Security Education*.
Sattarova Feruza, Y., & Kim, T. H. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering*, *2*(2), 17–32.
Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8. https://doi.org/https://doi.org/10.15394/jdfsl.2017.1476
SEC. (2022). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. *13*(34), 1–204.
Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. *Information Security Management Handbook, Sixth Edition*, 357–380. https://doi.org/10.1201/9781420072419-28
Slovic, P. (1987). Perception of Risk. *Science*, *236*(4799), 280–285. https://doi.org/10.1126/SCIENCE.3563507
Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. In *Politics and Governance* (Vol. 6, Issue 2, pp. 1–4). Cogitatio Press. https://doi.org/10.17645/pag.v6i2.1569
Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*, 105143. https://doi.org/10.1016/J.SSCI.2020.105143
Tissir, N., El Kafhali, S., & Aboutabit, N. (2020). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments 2020 7:2*, *7*(2), 69–84. https://doi.org/10.1007/S40860-020-00115-0
Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
WEF. (2017). Advancing Cyber Resilience - Principles and Tools for Boards. *World Economic Forum*, *January*, 40.
WEF. (2021). *Future Series: Ciberseguridad, tecnología emergente y riesgo sistémico | foro Economico Mundial*. https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk
Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. In *Cengage Learning*.
Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt. *USENIX Security Symposium*, 679–702. http://www.doug-tygar.com/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf
Williams, T. D. (2020). Epistemological Questions for Cybersecurity. *International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2020*, 1–4. https://doi.org/10.1109/CyberSecurity49315.2020.9138884
Zeller, G., & Scherer, M. (2020). A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal*. https://doi.org/10.1007/s13385-021-00290-1