Relación del ecosistema de ciberseguridad en la transformación digital de las organizaciones

Autores: Giraldo Ríos, Lucas Adolfo*; Duque Oliva, Jair; Sánchez Torres, Jenny Marcela
Contacto: *lucasgiraldor@gmail.com
País: Colombia

Resumen
La Revolución 4.0, el creciente impulso de la digitalización y el desarrollo de tecnologías emergentes cada vez más acelerado hacen que el ciberespacio sea un nuevo escenario de operación y encuentro de las organizaciones en todo el planeta. Lo anterior presenta nuevos retos para las empresas y así mismo para los países en términos de servicios, procesos, actividades y por supuesto ciberseguridad (Dadkhah y Lagzian, 2018).

Este documento presenta la teoría tripartita del ciberespacio, basada en el statu quo del ciberespacio. Se proponen las estrategias correspondientes y una arquitectura de investigación para las redes públicas comunes (RPC), las redes clasificadas seguras (CS) y las redes de infraestructuras clave (IC), basándose en sus características individuales. Luego de ellos se analizan las características y requisitos de seguridad de estas redes. Tomando como ejemplo el espacio RPC, presentamos el bucle de CSGD (conocimiento de la situación, supervisión y gestión, defensa cooperativa, respuesta y recuperación, y contramedidas y rastreo) para construir un ecosistema de seguridad del ciberespacio. La complejidad del Ecosistema se detalla desde la visión del Diagrama de Influencia de la Dinámica de Sistemas y el Diagrama de Dominio. El modelo resultante evidencia la ciberseguridad como un componente estratégico para el desarrollo empresarial.
Palabras claves: transformación digital; ciberseguridad; ecosistema ciberseguridad.

1. Introducción

En un mundo cada vez más acelerado y permeado por las tecnologías asociadas a la cuarta revolución industrial hacen que la Transformación Digital y el ciberespacio constituyen un nuevo espacio de encuentro de las organizaciones en todo el planeta. Por lo tanto nuevos retos para las empresas y así mismo para los países en términos de servicios, procesos, actividades y por supuesto ciberseguridad se presentan (Dadkhah y Lagzian, 2018).

Este artículo tiene por objetivo presentar la relación del ecosistema de ciberseguridad en la transformación digital de las organizaciones. A partir de una revisión sistemática de literatura (RSL) se encontró evidencia que muestra una posible relación entre la Transformación Digital y cómo esta está permeada por la ciberseguridad, adicionalmente se puedo presentar una primera aproximación del ecosistema de ciberseguridad en organizaciones. El articulo está constituido por siete sesiones incluyendo esta introducción; una segunda que describe el método de construcción del artículo, una tercera que presenta el ecosistema de ciberseguridad con sus elementos; una cuarta con la definición de transformación digital; la sexta presenta la relación entre ecosistema de ciberseguridad y transformación digital y finalmente la séptima presenta la propuesta de ecosistema de ciberseguridad y transformación digital para terminar con las conclusiones del artículo.

2. Método

Para abordar el presente artículo se utilizó el método de RSL propuesto por Kitchenham et al., (2009) y ampliado por Sánchez-Torres (2017) en el cual se definen dos fases de operación, la primera de ellas es la planificación donde se definieron las preguntas orientadoras y los criterios de inclusión. Las preguntas orientadoras fueron a). ¿Cuáles son los elementos de un ecosistema de ciberseguridad? b). ¿Qué es la transformación digital? c). ¿Cuál es la relación entre transformación digital y ciberseguridad? Para responder estas preguntas, en la segunda fase se realizaron las búsquedas de información. El flujo de operación de este método de RSL se presenta en la Figura 1.

FIGURA 1. Fases de búsqueda para RSL

Fuente: Elaboración propia a partir de Kitchenham et al. (2009) y (Sanchez-Torres (2017).

Para la RSL se construyeron las estrategias de búsqueda para las bases de datos de WoS, Scopus y Emerald presentadas en la Tabla 1 con sus respectivos resultados de aplicación.

TABLA 1. Estrategias de búsqueda y número de artículos obtenidos en la RSL

Base de datos	Ecuación utiliada	Resultado	Filtrados
Web of Science WoS	(("digital transformation" OR "digital innovation" OR "digital technologies" OR "digital technology" OR digitalization) AND (cybersecurity OR "CYBER SECURITY" OR "cyber security")) Período de tiempo: Todos los años. Índices: SCI-EXPANDED, SSCI, A&HCI, ESCI.	150	32
Scopus	TITLE-ABS-KEY (("digital transformation" OR "digital innovation" OR "digital technologies" OR "digital technology" OR digitalization) AND (cybersecurity OR "CYBER SECURITY" OR "cyber security")) AND (LIMIT-TO (DOCTYPE , "re"))	20	8
Base de datos	Ecuación utiliada	Resultado	Filtrados
Emerald	(("digital transformation" OR "digital innovation" OR "digital technologies" OR "digital technology" OR digitalization) AND (cybersecurity OR "CYBER SECURITY" OR "cyber security")	551	35

Fuente: Elaboración propia (2023).

A partir de los hallazgos en la RSL se realiza una propuesta de ecosistema y su relación con la transformación digital. A continuación, se presentan los resultados de la aplicación de este método dando respuesta a las preguntas orientadoras.

3. Ecosistema de ciberseguridad

A partir de la RSL se define el Ecosistema de Ciberseguridad en el cual se establecen sus componentes, la visión estratégica de la ciberseguridad en las instituciones y el análisis de la complejidad del ecosistema utilizando el Modelo de Influencias de la Dinámica de Sistemas y el Modelo de Dominio de la Ingeniería de Software. Como lo define Schaffernich (2009), ambos modelos fueron creados como una forma de representar aspectos relevantes del sistema, y ayudan a comprenderlo adecuadamente.

El concepto de ecosistema fue desarrollado inicialmente por los estudios de ecología partiendo de la relación entre los organismos vivos y su entorno. Sin embargo, desde entonces este concepto ha sido adoptado y utilizado por las ciencias sociales, económicas y tecnológicas. El enfoque basado en la tecnología ha provocado que los Estados y las empresas generen enormes cantidades de información, cuyo almacenamiento y difusión requieren una gran potencia tecnológica, perspectivas estratégicas y sistemas de gestión del conocimiento orientados a los procesos. Este enfoque necesita apoyarse en métodos que informen oportunamente la toma de decisiones como paso esencial de cualquier proceso (Oropeza, Urciaga y Ponece, 2015).

Según este enfoque, el ecosistema tecnológico consiste en un compuesto de componentes de tecnología interrelacionados mediante flujos de información a través de soportes físicos (Markoff, 2011). Estos medios funcionan como soporte principal del citado flujo de información.

Un ecosistema cibernético sano interoperaría ampliamente, colaboraría eficazmente en un entorno distribuido, respondería con agilidad y se recuperaría con rapidez (Hagiu, Wright, 2020). Con un rico entramado de asociaciones de seguridad, estrategias compartidas, políticas digitales preaprobadas y preposicionadas, intercambios de información interoperables y participantes "sanos" -personas, dispositivos y procesos-, un ecosistema cibernético sano podría defenderse contra todo el espectro de amenazas conocidas y emergentes, incluidos los ataques contra la cadena de suministro, los ataques remotos basados en la red, los ataques próximos o físicos y los ataques internos; mejorar la fiabilidad y resistencia de las infraestructuras críticas; y garantizar mejor la privacidad, los procesos empresariales y las misiones (ISO/IEC 27032).

3.1. Ciberespacio

En la Tabla 2 se realiza una recopilación de las diferentes definiciones del Ciberespacio, la cual es elaborada teniendo en cuenta el documento “Controles de Seguridad Propuesta inicial de un Framework en el contexto de la Ciberdefensa” (Sack y Ierache, 2015, pp. 3-4).

TABLA 2. Definiciones de Ciberespacio

Organismo o País	Definición
Real Academia Española.	Ámbito artificial creado por medios informáticos. Esto quiere decir que para implementar el ciberespacio se necesita de una infraestructura física de computadoras y líneas de comunicaciones que las mantengan interconectadas.
National Institute of Standards and Technology (NIST).	Dominio global dentro del entorno de la información que consta de redes interdependientes de infraestructuras de sistemas de información que incluyen: internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores.
Unión Europea.	Espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo.
Unión Internacional de Telecomunicación.	Lugar creado a través de la interconexión de sistemas de ordenador mediante Internet.
España.	Conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos.
Estados Unidos (DoD).	Dominio global dentro del entorno de la información, consistente en la red interdependiente de las infraestructuras de tecnología de la información incluida la Internet, redes de telecomunicaciones, sistemas informáticos, los procesadores y controladores.
Reino Unido.	Todas las formas de actividades en redes digitales; esto incluye el contenido y acciones realizadas a través de redes digitales.

Fuente: Adaptado del documento "Controles de Seguridad Propuesta inicial".

3.2. Ciberseguridad

De acuerdo con la definición entregada por el doctor Jeimy J. Cano, Ph.D., miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho y Profesor de la misma Facultad de la Universidad de los Andes, Colombia y miembro del Subcomité de Publicaciones de ISACA, la seguridad informática es:

La disciplina se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que—articulados con prácticas de gobierno de tecnología de información—establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo. (Cano, 2011)

Lo anterior, conlleva a la importancia de buscar diferentes medios como estrategia de protección ante las amenazas que se generan por la dependencia de la sociedad en el uso del ciberespacio.

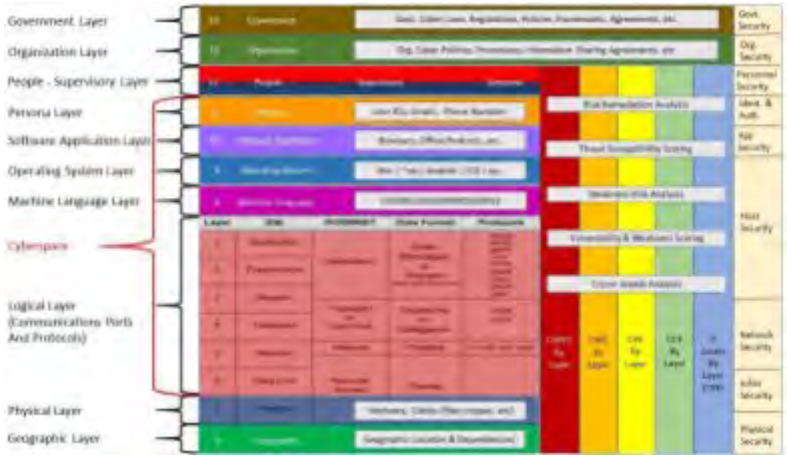
La ciberseguridad ya no es un problema de seguridad puramente informática, es un asunto de política nacional porque el uso ilícito del ciberespacio podría obstaculizar las actividades económicas, de salud pública, de seguridad ciudadana y de seguridad nacional y dado que los gobiernos existen principalmente para mantener el orden social, proteger las vidas y las propiedades de sus ciudadanos y permitir el comercio, por lo tanto, deben utilizar todos los instrumentos de poder nacional para reducir adecuadamente los riesgos cibernéticos. En particular, elaborando una estrategia de seguridad cibernética y fomentar la cooperación intersectorial local, nacional e internacional (Piccini, Andre, Gregory, Kolbe, 2015).

4. Transformación Digital

La Transformación Digital ha surgido como un fenómeno importante en la investigación estratégica y de negocios (Bharadwaj et al., 2012; Piccinini et al., 2015) así como para los profesionales (Fitzgerald et al., 2013; Westerman y Bonnet, 2014). El mundo digital es un espacio en crecimiento que ofrece importantes oportunidades para la transformación de las organizaciones debido al alto potencial cibernético y la interconectividad existentes. En este espacio la materia prima y por tanto la base de la transformación digital son los datos como quiera que tienen un crecimiento exponencial (Hagiu y Wright, 2020; Sammut y Webb, 2017; Schwartz y Ben-David, 2014). De las diferentes definiciones encontradas en la RSL, la utilizada para este artículo es la que presenta Vial (2019, p. 4), que la define como: "un proceso que tiene como objetivo mejorar una entidad mediante la activación de cambios significativos en sus propiedades a través de combinaciones de tecnologías de información, informática, comunicación y conectividad".

El valor generado por el ecosistema, los atributos deseados del ecosistema y de los participantes, y los elementos constitutivos del ecosistema funcionan conjuntamente. Por ejemplo, un ecosistema con la capacidad de realizar ajustes automáticos en la configuración en respuesta a las elecciones de confianza ofrecería una mayor fiabilidad y resistencia para los procesos empresariales, sociales y cívicos respaldados, al tiempo que mejoraría la privacidad y las libertades civiles de los usuarios. Un ecosistema con tales capacidades también se autodefendería. Un ecosistema autodefensivo con participación humana podría obligar a los atacantes a asumir más riesgos y a estar más expuestos. Estas actividades, combinadas con una mayor atribución, podrían permitir que la aplicación de la ley u otras medidas disuasorias fueran más eficaces. En otras palabras, un ecosistema sano refuerza mutuamente la seguridad, la facilidad de uso, la fiabilidad y la protección de la intimidad y las libertades civiles. Finalmente, todo el sistema inicial puede evidenciarse en la Figura 2 de manera resumida.

FIGURA 2. SEQ Figura * ARABIC 2. Ecosistema de ciberseguridad



Fuente: Modelo de capas de Shawn Riley.

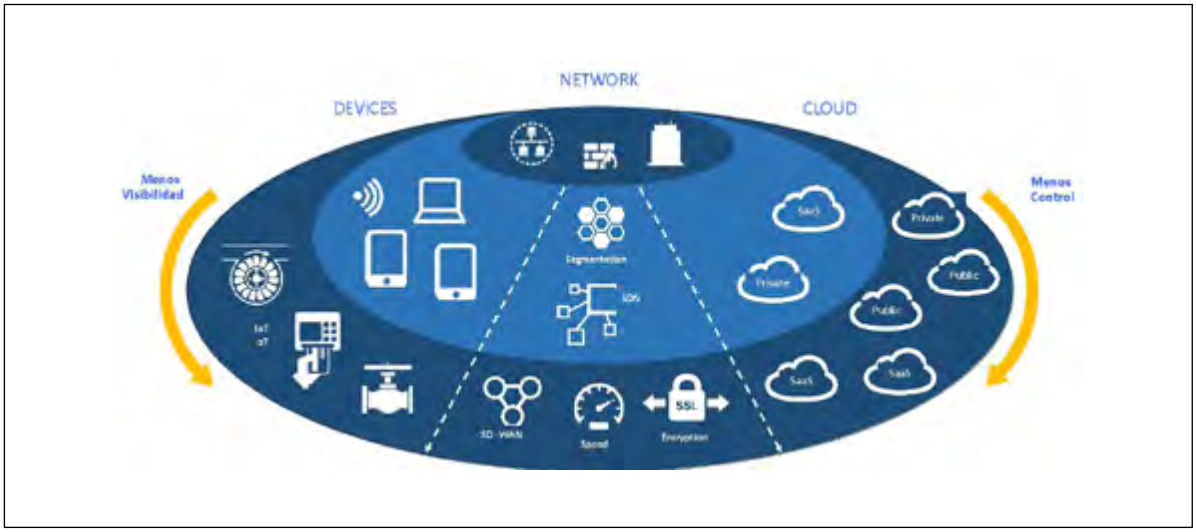
5. Relación entre Transformación Digital y la Ciberseguridad

El análisis del efecto en la transformación digital por las tecnologías digitales en las organizaciones requiere una visión general del complejo relacionamiento de sus sistemas, dispositivos y redes inteligentes e interconectadas utilizadas para cumplir con el respectivo trabajo. Por tanto, analizar el impacto de las tecnologías digitales avanzadas en las organizaciones requiere una amplia visión en cuanto a la interacción de las tecnologías digitales así como sus problemas de ciberseguridad, que se convertirán en un riesgo intrínseco a través de los ataques de ciberamenazas (Dadkhah, Lagzian y Borchardt, 2018; Habibzadeh et al., 2019; NIST - National Institute of Standards and Technology, 2013).

La ciberseguridad como disciplina basada en la informática se ocupa de la presencia de adversarios y de los ataques de amenazas cibernéticas. Dentro de las ciencias de la computación, el área de ciberseguridad abarca muchas áreas, que incluyen (pero no se limitan a) seguridad de datos, criptografía, seguridad de software y hardware, seguridad de redes y sistemas, privacidad y muchas otras. (Möller, 2016).

Como consecuencia de lo presentado, entre más apropiación digital tiene una organización, más conexiones y puntos de acceso desarrolla lo que conlleva a una ampliación de su superficie de ataque digital, tal como se presenta en la Figura 3, lo que expone con mayor fuerza sus servicios, infraestructura tecnológica y la información, que desde los datos, se generan, procesan, almacenan y transmiten. Con lo anterior, se incrementa la probabilidad de que un ciber-riesgo se materialice y con ello la posibilidad de sufrir un incidente de ciberseguridad, con lo que la organización requiere una estrategia de ciberseguridad integral que, además de cubrir la operación diaria, participe de toda iniciativa de transformación digital.

FIGURA 3. Superficie de ataque digital



Fuente: INCIBE-CERT (2020).

6. Propuesta de Ecosistema de ciberseguridad y relación con la Transformación Digital

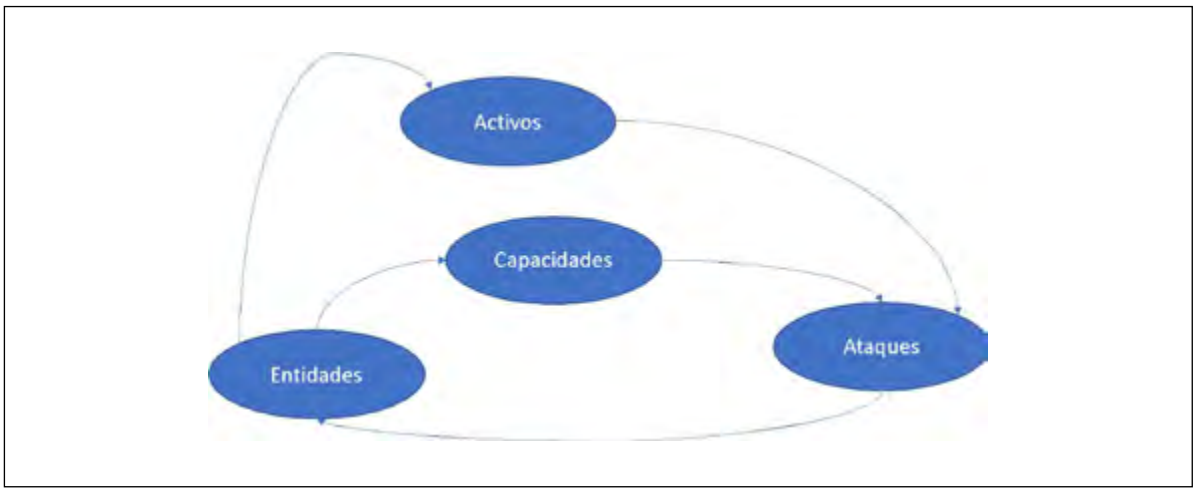
Considerando lo anteriormente presentado el ecosistema de ciberseguridad comprende unos actores, unas capacidades, las relaciones, sus activos y las amenazas conforme se presenta en la Figura 4.

FIGURA 4. Ecosistema de Ciberseguridad del país para desarrollo de operaciones

Fuente: Elaboración propia (2022).

La Figura 5 presenta el diagrama de influencias generales del Ecosistema de Ciberseguridad el cual ilustra cómo las Entidades cuentan con Activos que son susceptibles a Amenazas que luego pueden ser aprovechados para afectarlas, a su vez, las Entidades cuentan con Capacidades que les permiten estar protegidas de Amenazas. Las flechas en el diagrama representan las interacciones que se dan entre los diferentes componentes del ecosistema.

FIGURA 5. Diagrama de influencia general de la estructura básica del Ecosistema de Ciberseguridad

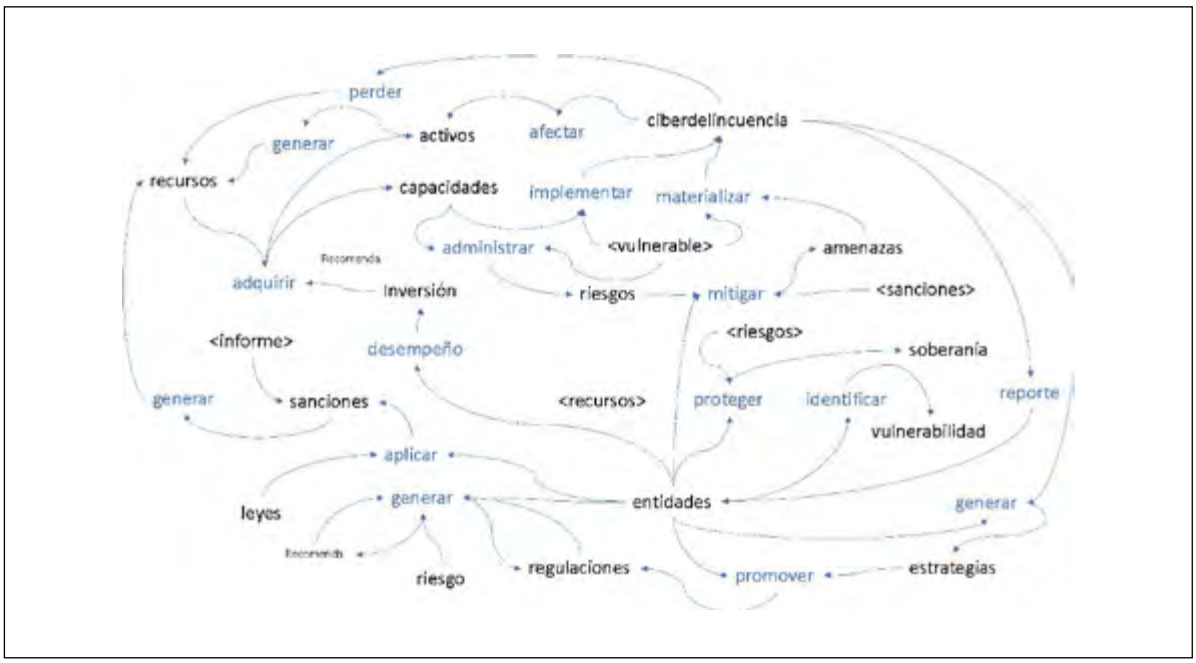


Fuente: Elaboración propia (2023).

Derivado de lo anterior, en la Figura 6, se plantean algunas relaciones no mencionadas anteriormente: Las Entidades son las encargadas de generar la dinámica de relación y los detonantes de acciones en su manejo de transformación digital que permitirán la gestión de riesgos para que se reduzcan las Amenazas en caso de que estas se lleven a cabo y den lugar a delitos de Ciberdelincuencia que sean en perjuicio de

otras Entidades. Además, se presenta que las Capacidades que se desarrollan pueden ser utilizadas tanto para cometer como prevenir Delitos Cibernéticos.

FIGURA 6. Relaciones ampliadas del ecosistema de ciberseguridad



Fuente: Elaboración propia (2023).

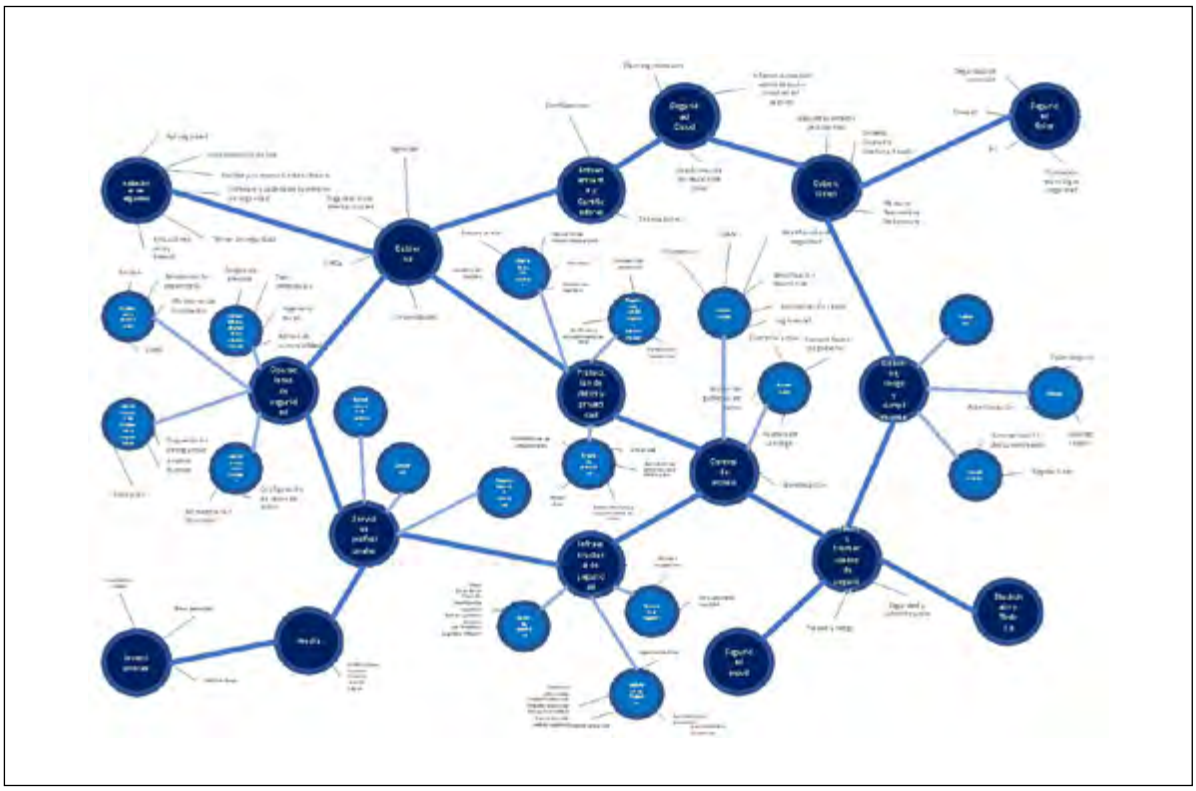
Una vez analizada la complejidad del sistema, se puede modelar el Ecosistema de Ciberseguridad a través de la Ingeniería de Software en un Modelo de Dominio, el cual se desarrolla a partir de un diagrama de clases para presentar las relaciones y acciones que realizan las entidades.

El Modelo de Dominio requiere una especificación detallada de las entidades, las cuales se muestran en el Diagrama de Influencias como una única variable general. Por eso, es necesario crear un modelo que enumere los estereotipos y facilite la creación del modelo el cual se puede observar en la Figura 7. Tener la información y las herramientas para navegar por el ecosistema de ciberseguridad es el camino hacia la claridad. Así es como podemos realmente marcar la diferencia y alcanzar nuestras propias versiones de éxito profesional. Al leer este artículo, espero que hayas encontrado el camino hacia una nueva herramienta y un conjunto de información que pueda beneficiarte durante años.

Mapear el ecosistema de ciberseguridad depende en gran medida del trabajo de los demás. Este trabajo es casi puramente derivado, un metaanálisis de varias referencias.

La racionalización de diferentes pensamientos y enfoques para definir la ciberseguridad tiene mucho valor en sí misma. Cuando existían discrepancias o matices sutiles, tenemos que detenernos y pensar cuidadosamente en cómo resolverlos. No todos usan los mismos términos, y la percepción se guía por las propias experiencias en ciberseguridad.

FIGURA 7. Mapa de ecosistema de ciberseguridad y transformación digital desde la integración de nodos detallada con actores de transformación



Fuente: Elaboración propia (2023).

7. Conclusiones

Parece claro que todo proceso de Transformación Digital se sustenta en los datos, en su análisis y procedimientos de obtención, optimización, aplicación. Actualmente casi la totalidad del tejido producto y de las AAPP se encuentran en algún punto de un proceso de Transformación Digital; en ocasiones sin ser realmente conscientes de ello ni haber realizado una planificación adecuada. La falta de planificación es uno de los errores más habituales a la hora de llevar a cabo un proceso de Transformación Digital. Sin planificación se producirán errores, ineficiencias, problemas de gestión, que conllevarán, entre otros efectos indeseables, problemas de seguridad de los datos.

La ciberseguridad está impulsando la transformación digital a nivel mundial, con la extracción, almacenamiento y protección de datos como prioridades para las empresas de todo el mundo, al mismo tiempo, los beneficios de invertir en transformación digital, en particular en la nube, son cada vez más claros, con ahorros de costos y mayores eficiencias.

Referencias bibliográficas

Bharadwaj, A., El Sawy, O., Pavlou, P. y Venkatraman, N. (2012). *Digital Business Strategy: Toward a next Generation of Insights*. 37(November), 471–82.

Cano, J. J. (6 de octubre de 2011). *Seguridad para todos*. http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

Dadkhah, M., Lagzian, M. y Borchardt, G. (2018). Academic Information Security Researchers: Hackers or Specialists? *Science and Engineering Ethics*, *24*(2), 785–90.

Fitzgerald, M., Kruschwitz, N., Bonnet, D. y Welch, M. (2013). Embracing Digital Technology: A New Strategic Imperative | Capgemini Consulting Worldwide. *MIT Sloan Management Review*, *55*(1), 1–13.

Gastón Sack, P. y Ierache, J. S. (2015). *Controles de Seguridad Propuesta inicial de un Framework en el contexto de la ciberdefensa*. http://sedici.unlp.edu.ar/bitstream/handle/10915/50588/Documento_completo.pdf-PDFA.pdf?sequence=1

Hagiu, A. y Wright, J. (2020). When Data Creates Competitive Advantege… and When It Doesn´t. *Harvard Business Review*, 94–102.

ISO/IEC (2012). *International Standard ISO/IEC 27032: Information Technology—Security techniques—Guidelines for Cybersecurity*. ISO/IEC.

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J. y Linkman, S. (2009). Systematic Literature Reviews in Software Engineering - A Systematic Literature Review. *Information and Software Technology*, *51*(1), 7–15.

Markoff, J. (2011). Researchers Show How a Car's Electronics Can Be Taken Over Remotely. *The New York Times*, March 9, Section B, Page 3.

Möller, D. P. F. (2016). *Guide to Computing Fundamentals in Cyber-Physical Systems* (1a ed.) Springer International Publishing.

Oropeza Cortés, M.G., Urciaga García, J.I. y Ponce Díaz, G. (2015). Importancia Económica y Social de los Servicios de los Ecosistemas: Una revisión de la Agenda de Investigación. *Rev. Glob. Negoc.*, *3*, 103–113.

Piccinini, E., Hanelt, A., Gregory, R. W. y Kolbe, L. M. (2015). Transforming Industrial Business: The Impact of Digital Transformation on Automotive Organizations. En *2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015* (pp. 1–20).

Sammut, C. y Webb, G. J. (2017). Encyclopedia of Machine Learning and Data Mining. Springer Nature.

Sánchez-Torres, J. M. (2017). *Guía de Aplicación Vigilancia Tecnológica, Inteligencia Competitiva y Prospectiva*. Bogotá DC.

Schaffernicht, M. (2009). *Indagación de Situaciones Complejas Mediante la Dinámica de Sistemas*. Editorial Universidad de Talca.

Schwartz, S. S. y Ben-David, S. (2014). *Understanding Machine Learning*. Cambridge University Press.

Vial, G. (2019). Understanding Digital Transformation: A Review and a Research Agenda. *Journal of Strategic Information Systems*, *28*(2), 118–44.