SEMINARIO DE INVESTIGACION – ESPECIALIZACIÓN

Facultad de Administración, Finanzas y Ciencias Económicas,
Especialización en Administración de Empresas virtual

INFORME TECNICO DE RESULTADOS DE INVESTIGACION

RIESGOS EN CIBERSEGURIDAD Y SUS EFECTOS SOBRE LA TRANFORMACIÓN DIGITAL EN LA NUEVA NORMALIDAD, SEGÚN LAS EMPRESAS OPERADORAS DE SEGURIDAD

AUTORES – GRUPO 3

Arelis Taimati Ramos Gallardo
Erika María Arango Hurtado
Antonio Amador Tinoco

TUTOR:

RICARDO PRADA OSPINA

UNIVERSIDAD EAN

NOVIEMBRE DE 2020, BOGOTA D.C.

TABLA DE CONTENIDO

1. LISTADO DE TABLAS Y FIGURAS.

2. RESUMEN

El Covid-19 se ha convertido en el acelerador de transformación digital en las organizaciones y la sociedad materializado en un creciente desarrollo y uso de la internet de las cosas – IoT, computación en la nube y trabajo remoto. Según Caballero (2020), la seguridad tradicional debe transformarse para afrontar los nuevos retos y los constantes ataques y amenazas. Debemos adaptarnos a la necesaria y rápida implantación de las nuevas tecnologías del futuro y del presente.

Esta investigación es de carácter descriptivo, no experimental y cuantitativa, mediante un análisis correlacional, describe los efectos que generan los riesgos por ciberseguridad en la transformación digital, a partir de la experiencia del analista que gestiona incidentes de seguridad en los centros de operaciones de seguridad - SOC.

Los resultados demuestran una significativa correlación entre el aumento de la frecuencia con la que se presentan ciberataques y la nueva normalidad, además, de la naturaleza de los riesgos tecnológicos y no tecnológicos relacionados.

En conclusión, la transformación digital es una fuente natural de ciberataques, ha incrementado la superficie tecnológica para su materialización, apalancado en nuevas técnicas ciber amenazas y explotación de vulnerabilidades conocidas y desconocidas, propiciado en algunos casos por la necesidad de responder rápidamente a los retos planteados por la nueva normalidad, dejando la ciberseguridad en segundo plano.

Se hace necesario fortalecer de forma inmediata los conocimientos del talento humano encargado de gestionar la ciberseguridad para minimizar los riesgos presentes y futuros, así como también abordar la ciberseguridad con un carácter preventivo para una pandemia tecnológica cuyos efectos van a permanecer en el tiempo, a través de una transformación digital que necesita ser confiable. Lo identificado desde los centros de operaciones de seguridad – SOC, es repetible en cualquier tipo de organización y a su talento humano encargados de gestionar la ciberseguridad en la nueva normalidad.

Palabras clave: Ciberseguridad, transformación digital, conocimiento, vulnerabilidades, nueva normalidad, ciberataques, ciber amenazas.

3. INTRODUCCION

La pandemia generada por la propagación del virus Covid-19 en 2020, ha impactado todos los estadios de la vida cotidiana y las organizaciones no han sido ajenas a esta situación. Las organizaciones se vieron en la necesidad de tomar medidas preventivas para proteger la salud de sus empleados, al mismo tiempo que tuvieron que tomar decisiones para poder adaptar sus procesos de negocio y operaciones a una nueva realidad, en la que predomina el trabajo remoto, colaboración en línea, la incursión o avance acelerado en nuevas tecnologías como lo son servicios en la nube, internet de las cosas, escritorios remotos y virtuales, movilidad, entre otras.

Este contexto ha propiciado un escenario ideal para la evolución de amenazas a la seguridad digital, con incremento en el ciber crimen y ciber delitos, los autores Santiago y Allende (2017) indican que esta nueva realidad digital exige la implantación de medidas de ciberseguridad y la gestión del riesgo tanto en la infraestructura tecnológica como en los procesos de negocio, resaltando que de no hacerlo las empresas estarán expuestas a una gran cantidad de amenazas que de exponer sus vulnerabilidades podrían comprometer seriamente sus activos de información.

Los centros de operaciones de seguridad – SOC, son actores claves en el escenario de la ciberseguridad, estos experimentan el impacto de la transformación digital y sus riesgos asociados. El SOC cuenta con analistas de ciberseguridad, encargados de la gestión incidentes de seguridad; su experiencia y conocimiento son insumo para la transformación digital, misma que enfrenta un panorama dinámico por la innovación tecnológica, nuevas amenazas y técnicas de ataque, que sin las adecuadas competencias y conocimientos enfocados en ciberseguridad, impactan la competitividad en un mundo globalizado, limitando a las economías, sociedad y gobiernos, para poder estar a tono con el avance tecnológico y la transformación digital propias de la nueva normalidad.

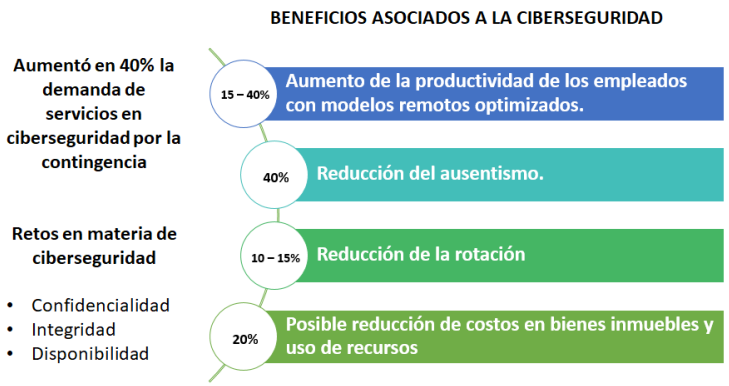
La presente investigación pretende describir el riesgo en ciberseguridad y sus efectos en la transformación digital, a partir de la experiencia en dos de las empresas prestadoras de servicios SOC, quienes a su vez gestionan la seguridad para empresas del sector industrial, público y privado en Colombia.

4. PLANTEAMIENTO DEL PROBLEMA

La pandemia mundial del Covid-19, está marcando un punto de inflexión fundamental que expone deficiencias estructurales en múltiples sistemas como salud, economía, empleo y educación; resaltando a la tecnología como instrumento para afrontar y gestionar los cambios impuestos por la pandemia y acentuando la dependencia de la infraestructura digital; el reporte del Banco Interamericano de Desarrollo - BID (2020) hace referencia que en un lapso de tres meses se ha experimentado una aceleración de la transformación digital que se había anticipado ocurriría en tres años.

Para la consultora Gartner (2020), el 74% de los líderes de áreas financieras consultados, consideran mantener de forma indefinida el trabajo remoto dentro de la nueva normalidad. El trabajo remoto, la internet de las cosas - IoT, infraestructura crítica OT, servicios en la nube, colaboración en línea y las nuevas formas de consumo, son referenciados por Deloitte (2020) como nuevos actores en la llamada nueva normalidad, influyendo directamente en el incremento a las amenazas a la ciberseguridad. La figura a continuación nos presenta un ejemplo de lo anterior con énfasis en el teletrabajo.

Figura - 1 - El aumento de la ciberseguridad y el teletrabajo.



Fuente: Elaboración propia tomando cifras y referencias de Vargas (2020).

4.1. Descripción del problema

Para Caballero (2020, p.34) “la Transformación Digital está empujando a las empresas y a los profesionales a cambiar radicalmente su manera de pensar y trabajar. En un mundo donde tanto el

Cloud como los procesos de desarrollo *Agile* están a la orden del día, la seguridad tradicional debe transformarse para afrontar los nuevos retos y los constantes ataques y amenazas.

El entorno de la transformación digital requerirá dotar a la gente, de la mezcla correcta de competencias y conocimientos para transitar con éxito los ambientes laborales cambiantes y ricos en tecnología, así como una fuerte capacidad para seguir aprendiendo (OCDE, 2019). Según el Centro de Estudios Estratégicos Internacionales – CSIS (2016), en su estudio sobre el estado de la oferta de recurso humano para la industria de la ciberseguridad indica:

> a) 76% de los encuestados manifestaron que los gobiernos no invierten suficiente en talento en ciberseguridad, b)7% de las universidades ofrecen programas específicos y c) 44% manifestó que los programas educativos no preparan profesionales con conocimientos y habilidades suficientes y concluye que para garantizar una seguridad eficaz es fundamental contar con una plantilla de personal sólida, ahora más que nunca.

En el informe de ISACA (2020), el 78% de los encuestados manifiesta, que la necesidad de perfiles técnicos va a seguir creciendo para 2020 y 2021, especificando que las mayores brechas están enfocadas en un 32% de habilidades blandas, 30% en conocimientos de tecnología, 23% en experiencia y práctica relacionada con la tecnología.

Dentro del contexto referenciado anteriormente, se enmarca la siguiente pregunta de investigación, proponiendo como población de estudio el área de gestión de incidentes, conformada por los analistas de ciberseguridad y sus respectivos supervisores, en las empresas Digiware y Etek; dos de las más reconocidas en Colombia por su trayectoria, alcance y oferta especializada en servicios de gestión para la ciberseguridad.

4.2. **Pregunta general de investigación**

¿Cuáles son los riesgos por ciberseguridad, y cuáles son sus efectos sobre la transformación digital acelerada por la nueva normalidad; según las empresas operadoras servicios de seguridad Digiware y Etek?

5. OBJETIVOS

5.1. Objetivo general

Determinar los efectos que producen los riesgos en ciberseguridad sobre la transformación digital en la nueva normalidad, según las empresas operadoras de servicios en seguridad Digiware y Etek.

5.2. Objetivos específicos

1) Identificar a partir de la literatura, artículos y publicaciones científicas, informes de industria y de gobierno, sobre las diferentes definiciones de riesgos en ciberseguridad y su relación con la transformación digital.
2) Establecer la relación existente entre las variables del riesgo en ciberseguridad y los efectos asociados a la transformación digital en su dimensión tecnológica, utilizando como herramienta un cuestionario con pregunta cerrada en escala Likert, para consultar la perspectiva del analista de ciberseguridad que labora gestionando incidentes de seguridad en las empresas Digiware y Etek.
3) Establecer cuáles son los principales riesgos en ciberseguridad, la frecuencia y tipo de ataques en la nueva normalidad y sus efectos más comunes sobre la transformación digital a partir de las respuestas obtenidas sobre la población objetivo.
4) Establecer de dos a tres recomendaciones que ayuden a minimizar el efecto de los riesgos por ciberseguridad en la transformación digital en la nueva normalidad.

6. JUSTIFICACION

Desde el punto de vista social, el análisis de resultados debe permitir identificar aspectos relevantes de ciberseguridad en la nueva realidad para una transformación digital confiable, fácil de implementar y sostenible en la nueva normalidad de la actividad humana. Se pretende identificar elementos prácticos que contribuyan a la ciberseguridad de la transformación digital, conocimientos necesarios para el talento humano en ciberseguridad presente y futuro, en una industria caracterizada por un recurso humano con necesidades de mejora e insuficiente.

Desde el punto de vista económico, la incorporación de las tecnologías emergentes asociadas a la transformación digital genera y fortalece el consumo de servicios gestión tecnológica, lo que a su vez se convierte en fuente de nuevos empleos, en los que gobierno e instituciones educativas encuentran oportunidades. La transformación digital debe ser sostenible, los riesgos en ciberseguridad no deben comprometerla para favorecer el desarrollo del país.

Desde el punto de vista tecnológico, la ciberseguridad y la transformación digital hacen parte de las tecnologías de información y comunicaciones (TIC), son claves en la política de desarrollo de Colombia según el Nodo de Desarrollo e Innovación - NDI en Ciberseguridad, que a su vez se integra con la iniciativa de Investigación, Desarrollo, e Innovación – IDI, el Marco de Transformación Digital para mejorar la relación entre el Estado y los ciudadanos, los Centros de Transformación Digital empresarial, todas, estrategias lideradas por el Ministerio de las tecnologías de la información y las Comunicaciones – MinTic.

Desde el punto de vista académico, se espera identificar los conocimientos necesarios en ciberseguridad para la transformación digital, aportando a la academia y otras organizaciones públicas y privadas, interesadas en promover el talento humano; elementos para fortalecer sus metodologías organizacionales y programas de estudio.

Desde la óptica del gestor de emprendimientos, líder funcional y del administrador según su especialidad, la ciberseguridad debe ser entendida como un factor fundamental para proteger el desarrollo y sostenibilidad de las organizaciones, del estado y la sociedad, cuando se incorpora la transformación digital como un aliado, motor de generación nuevos puestos de trabajo, con empleos de calidad para un país que requiere más oportunidades para disminuir la brecha social.

7. MARCO TEORICO

El reporte anual sobre el panorama mundial de riesgos para la economía publicado por Foro Económico Mundial (WEF, 2020, p.62)., indica que el riesgo por ciberataques es el "séptimo más probable y octavo riesgo más impactante en corto plazo, y el segundo mayor riesgo para hacer negocios a nivel mundial durante los próximos 10 años".

Para Nayia Barmpaliou, jefe de políticas e iniciativas del Centro para la Ciberseguridad del Foro Económico Mundial, la pandemia mundial del COVID-19 ha marcado un punto de inflexión fundamental en nuestra senda mundial y ha acentuado como nunca nuestra dependencia de la infraestructura digital (BID, 2020).

7.1. **Riesgos en ciberseguridad.**

"La existencia de riesgos constituye una realidad a las que las personas y las organizaciones deben enfrentarse día a día" (Tamayo y González, 2020, p.59).

Tabla 1 - Definiciones de Riesgo

Año	Autor	Definición de Riesgo
2015	Diz	"Riesgo es todo aquello que puede generar un evento no deseado y traer como consecuencias pérdidas y/o dadaños".
2018	Organización Mundial para la Estandarización ISO 31000:2018	Riesgo se define como el efecto de la incertidumbre sobre los objetivos. La incertidumbre es el estado, incluso parcial, de la deficiencia de la información relacionada, la comprensión o el conocimiento de un evento, su consecuencia o probabilidad.
2017	Chávez	El concepto de riesgo más cercano a su significado se ha forjado en el pensamiento occidental del capitalismo y la teoría económica, para las que el riesgo es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre.
2016	Norma directiva de Unión Europea – UE	El riesgo en el espacio digital se define como "toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información".

Fuente: Autores.

"La evolución de las TIC's conlleva situaciones de riesgo que se van revelando día a día. Tecnologías emergentes habilitan el tratamiento de gran cantidad de datos, pero también habilitan su exposición" (Díaz, et al., 2018, p.1), lo que a su vez "conlleva serios riesgos y amenazas que pueden afectar a la seguridad" (Leiva, 2015, p. 161). "La ciberseguridad emerge ante el creciente uso del ciberespacio como nueva dimensión para la interacción social, resultado de la revolución

de la tecnología de la información y comunicación (TIC), que ha acelerado el proceso de globalización y periódicamente sorprende con su constante innovación" (Sancho, 2017, p.8).

Tabla 2 - Definiciones de ciberseguridad.

Año	Autor	Definición de Ciberseguridad
2015	ISACA	"Ciberseguridad se define como la protección de activos de información, mediante la gestión de amenazas sobre los datos procesados, almacenados y transportados por sistemas interconectados".
2015	Leiva	"Ciberseguridad se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio"
2011	CONPES 3701	"Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética"
2018	Urcuqui, Garcia M y Osorio.	"La ciberseguridad es el área de las ciencias de la computación encargada del desarrollo y la implementación de los mecanismos de protección de la información y de la infraestructura tecnológica".

Fuente: Autores.

Las organizaciones y gobiernos deben implementar medidas de ciberseguridad y gestión del riesgo tanto en la infraestructura tecnológica como en los procesos de negocio, para no exponerlas a una gran cantidad de amenazas que de aprovechar sus vulnerabilidades podrían comprometer seriamente sus activos de información (Santiago y Allende, 2017).

De acuerdo con las exigencias y complejidad de los negocios que demanda, la economía moderna, está expuesta cada vez más amenazas y a ser vulnerable frente a los ciberataques; si no cuenta con un robusto sistema de prevención y control de riesgos de ciberseguridad (Caamaño y Gil, 2017).

7.1.1. Vulnerabilidades en sistemas de información.

Vulnerabilidad se refiere a la cualidad de lo que puede ser dañado física o moralmente (RAE, 2020). Una "vulnerabilidad es, en primer lugar, un concepto con múltiples significados, aplicables a ámbitos muy diversos: desde la posibilidad de un humano de ser herido hasta la posible intromisión en un sistema informático" (Feito, 2007). "Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene" (Tarazona, 2017, p.137).

Tabla 3 - Tipos de vulnerabilidades informáticas.

Tipo de vulnerabilidad informática
Vulnerabilidades ya conocidas en recursos instalados (sistemas o aplicaciones).
Vulnerabilidades ya conocidas en recursos no instalados (el opuesto al caso anterior).
Vulnerabilidades no conocidas.

Fuente: Mateo y Cedillo (2017).

Las vulnerabilidades son defectos o debilidades en el diseño, implementación, funcionamiento o administración de los sistemas informáticos que pueden ser usados para comprometer los requisitos de seguridad (Viano, 2017). "Todo activo de información podría tener por lo menos una vulnerabilidad que podría ser aprovechada por una amenaza. La explotación de esta debilidad da como resultado la materialización del riesgo intrínseco o 'propio' del activo de información sin protección alguna" (Santiago y Allende, 2017, p.9).

7.1.2. Ciber amenazas o amenazas cibernéticas.

Según la definición del Instituto Español de Estudios Estratégicos – IEEE, una ciber amenaza se define como "aquellas actividades realizadas en el ciberespacio, que tienen por objeto la utilización de la información que circula por el mismo, para la comisión de distintos delitos mediante su utilización, manipulación, control o sustracción" (Ruiz, 2016, p.3).

Para Tarazona (2017), se puede agrupar las amenazas a la información en cuatro grandes categorías: Factores Humanos (accidentales, errores); fallas en los sistemas de procesamiento de información; desastres naturales o fuerza mayor y; actos maliciosos o malintencionados. Para Costas (2015), las amenazas a un sistema informático pueden ser provocadas por personas, lógica de los sistemas involucrados y aprovechamiento de las debilidades físicas, tal y como se presenta en la tabla a continuación:

Tabla 4 – Clasificación de amenazas.

Amenazas originadas en personas	Amenazas lógicas	Amenazas físicas
Personas de la organización, ex - empleados, curiosos, *hackers*, *crackers*, intrusos pagados.	Software desactualizado o mal configurado, herramientas de seguridad mal configuradas, puertas traseras, bombas lógicas, canales abiertos, virus, gusanos, troyanos, programas conejo.	Robo, sabotaje, destrucción, afectaciones suministro eléctrico, condiciones atmosféricas, catástrofes naturales o artificiales.

Fuente: Costas (2015).

7.1.3. Ciberataques o ataques cibernéticos.

"La sociedad a nivel global se ha visto impactada de manera notoria por el efecto generado por las TIC en todas sus dimensiones; las transformaciones sociales, económicas, educacionales y culturales han posibilitado nuevos escenarios" (Jin y Cho, 2015 p.235). Para Bakdash J., Hutchinson S., Zaroukian E., Marusich L., Thirumuruganathan S., Sample C., Hoffman B., y Das G (2018), la infraestructura de Internet juega un papel crucial en una serie de actividades diarias. La naturaleza omnipresente de los sistemas cibernéticos asegura consecuencias de gran alcance de los ciberataques.

Según los autores Díaz, Venosa, Macia, Lanfranco, Sabolansky, Rubio (2016), un mundo con más dispositivos interconectados, con más funcionalidades que a su vez omiten, los problemas de seguridad que su uso trae asociado lo cual se debe a que se desarrollan dispositivos pensando en la funcionalidad y usabilidad de los productos y no en la seguridad de la información que los mismos manipulan.

El documento sobre la política nacional de seguridad digital Colombia, establece que un ataque cibernético es una "acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del ciberespacio" (CONPES - 3854, 2016, p.88). Los investigadores Sánchez, Rotondo, Escobet, Puig y Quevedo (2019), indican que los ataques cibernéticos pueden ser maliciosos (caballos troyanos, gusanos informáticos, ataques de sabotaje, programas maliciosos, amenazas persistentes) o no intencionales (actualizaciones de software incorrectas, protocolos erróneos o conexiones de red no deseadas), y pueden ocurrir en el espacio cibernético, el mundo físico o en ambos. La motivación de los ataques malintencionados puede surgir del terrorismo, la geopolítica, la criminalidad o las organizaciones impulsadas por problemas sociales. Ante tal panorama, "los cibercriminales aprovechan rápidamente los nuevos vectores de ataque y se benefician de los vacíos en la cooperación de las fuerzas del orden público en las diferentes jurisdicciones, dada la naturaleza inherentemente transnacional de sus actividades maliciosas" (BID, 2020, p.28).

Este entorno de avance tecnológico, riesgos por amenazas y ataques, implica una complejidad para los gobiernos y organizaciones que deben implementar estrategias para prevenir y proteger su entorno y, en consecuencia, como las configuraciones se vuelven más complejas, el esfuerzo

requerido para administrarlas se vuelve más pronunciado, sin embargo, gran parte de esto es necesario el esfuerzo permanece invisible y mal administrado en las organizaciones (Baptista, Stein, Klein, Watson, Lee, 2020).

7.1.4. Centros de operaciones de seguridad – SOC.

Organizaciones a nivel internacional tales como ISO (2019), promueven estándares en gestión de ciberseguridad definidos bajo la norma ISO 27001:2018, la cual establece un conjunto de procesos para el aseguramiento, confidencialidad e integridad de los datos y de la información, así como también de los sistemas que hacen parte del proceso del Sistema de Gestión de Seguridad de la Información o SGSI. Esta norma se complementa con el estándar ISO 27035:2018 que establece las mejores prácticas destinadas a la gestión de la información de incidentes de seguridad, así como también identificar, examinar y gestionar vulnerabilidades de seguridad de información y procesos de mejora continua.

Normativas, estándares, procesos que llevan a que "en la mayoría de los casos, la necesidad de ciberseguridad deba equilibrarse con la productividad, ya que varias opciones pueden resultar engorrosos e interferir con el funcionamiento de un sistema y una organización" (Pate, Kuypers, Smith, Kedler, 2018, p. 227). Para Ganshani (2017) un ejemplo de cómo responde la industria ante esta complejidad es la aparición y evolución de los Centros de Operaciones de Seguridad, también conocidos como SOC que, según el autor, bajo una estructura bien definida, ayudan a obtener una visibilidad inicial de las amenazas de la función empresarial, de gestión de riesgos e inteligencia.

"Los SOC se constituyen como un área de gestión capaz de articular procesos, personas y tecnologías con el fin de proteger los activos de la organización" (Biggeri, 2018, p.1). Desde la perspectiva de procesos se define al SOC como "una instalación dedicada a prevenir, detectar, evaluar y responder a amenazas e incidentes de ciberseguridad, así como a cumplir y evaluar el cumplimiento normativo" (Hámornik y Krasznay, 2018, p.107).

Según la metodología "una operación de SOC está conformada por analistas de tres diferentes niveles" (Muniz, McIntyre, AlFardan, 2016, p.11). Uno de esos niveles está conformado por el equipo de respuesta y gestión de incidentes de seguridad (CSIRT) quienes "permiten dinamizar bajo una línea base estándar de gestión, los diferentes aspectos de esas emergencias y buenas

prácticas para prevenir situaciones que afecten los tres pilares de la seguridad de la información asociado a un riesgo cibernético determinado" (Ortiz, 2020, p.4). Por la naturaleza del SOC, un analista tiene un rol muy específico y debe ser capaz de desempeñar ese rol de la manera más impecable y eficiente posible (Nathans, 2014).

7.2. **Transformación Digital.**

El mundo se encuentra en camino a la Cuarta Revolución Industrial (4RI), caracterizada por la aparición de nuevas tecnologías que están fusionando el mundo físico, digital y biológico (Schwab, 2016). "Las TIC ya están incorporadas en todos los aspectos de la vida cotidiana, los precios más accesibles de dispositivos de conexión a Internet han masificado su uso, convirtiéndose en un accesorio imprescindible para las personas y las organizaciones" (Díaz, Molnari, Venosa, Macia, Lanfranco, Sabolansky, 2018, p.1056).

Tabla 5 - Definiciones de transformación digital.

Año	Autor	Transformación Digital
2019	Kaplan y Haenlein	"Transformación digital es el cambio asociado con la aplicación de tecnologías digitales en todos los aspectos de la sociedad humana".
2019	Pirni, Giampellegrini, Raffini.	"La estrategia adoptada para orientar la digitalización en una dirección específica con objetivos igualmente específicos, que socialmente cambian el tipo de interacciones, estructuras de referencia, formas de trabajo e influyen en la toma de decisiones".
2018	Globe	Es la profunda transformación de las actividades, procesos, competencias y modelos empresariales y organizativos para aprovechar plenamente los cambios y oportunidades de una combinación de tecnologías digitales y su impacto acelerado.
2020	Brunetti, Matt, Bonfanti, De Longhi, Pedrini, Orzes.	"Es un desafío generalizado del sistema innovador que requiere un conjunto multifacético de acciones estratégicas que se dividen en tres pilares principales. El primer pilar, denominado "cultura y habilidades", incluye tres campos estratégicos de acción de la siguiente manera: la educación digital, los talentos y la cultura digital. El segundo pilar, denominado "infraestructuras y tecnologías", señala la necesidad de información, interacción e inteligencia artificial como campos estratégicos clave de acción. El tercer pilar, denominado "ecosistemas", destaca la importancia de invertir en visiones a medio y largo plazo, asociaciones y calidad de vida".

Fuente: Autores.

7.2.1. Infraestructuras y tecnologías emergentes.

Las infraestructuras apoyan y dan forma a nuestro mundo social, haciéndolo a menudo de formas a menudo invisibles (Frith, 2020). La infraestructura cibernética es aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión

o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública (CONPES, 2016). ¨Debemos adaptarnos a la necesaria y rápida implantación de las nuevas tecnologías del futuro (y del presente) como Blockchain, Cloud, Digital ID, Inteligencia Artificial y Machine Learning, Internet of Things e Industria 4.0¨ (Caballero, 2020).

Según Makhdoom, Abolhasan, Lipman, Ping Liu, Ni (2019), estas infraestructuras tecnológicas emergentes, crecientes, en adopción, como lo son la nube o la internet de las cosas, resultan en una cantidad significativa de datos que beneficia el desarrollo de tecnologías como el big data y otras.

7.2.2. Internet de las cosas – IoT.

Un ejemplo de la dimensión infraestructura y tecnología es la internet de las cosas o IoT, considerada como la cuarta revolución industrial (Schwab, 2016). Según Márquez (2019), se puede encontrar en electrodomésticos, teléfonos inteligentes, ropa inteligente, *wereables* (pulseras inteligentes, gafas de realidad aumentada, etc.), televisores inteligentes, videoconsolas, sistemas de transporte, edificios (cámaras de seguridad, climatización, controles de acceso, etc.), infraestructuras públicas (puentes, autopistas, parques, etc.), servicios públicos, componentes industriales, etc.

Se trata de tecnología que facilita el control y la supervisión de los dispositivos inteligentes. Su uso abarca sistemas de control industrial (ICS), salud, comercio electrónico, ciudades inteligentes, gestión de cadena de suministro, automóviles inteligentes, sistemas ciber físicos y más" (Makhdoom, et. al, Ni, 2019). El mismo autor también considera, que al mismo tiempo son propensas a numerosas amenazas a la disponibilidad y privacidad de los datos del usuario, a los mensajes y la integridad del dispositivo, la vulnerabilidad de los dispositivos de IoT, los ataques de *malware* y el riesgo de compromiso físico de los dispositivos representan un peligro significativo para el sustento de IoT.

7.2.3. Servicios en la nube.

La llamada computación en la nube consiste en "un modelo que permite acceso a la red bajo demanda a un conjunto de recursos informáticos (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un esfuerzo de gestión

mínimo" (Mell y Grance, 2011, p.3). La nube es entonces "un nuevo paradigma para representar las capacidades informáticas como un servicio para compartir recursos en internet" (Farrag, Mohamad, El-Horbaty, 2019, p.14).

El contexto actual, hace que empresas experimenten problemas de rendimiento, escalabilidad y disponibilidad con la infraestructura de TI. Acelerando la migración a la nube, con el personal de ciberseguridad detrás vigilando que tanto beneficios como riesgos de este fenómeno sean considerados (Deloitte, 2020).

7.2.4. Servicios escritorios remotos y virtuales.

La virtualización de escritorios es una tecnología que permite que los usuarios simulen una carga de estación de trabajo para acceder a un escritorio desde un dispositivo conectado de forma remota o local. Esto separa el entorno de escritorio y sus aplicaciones del dispositivo cliente físico utilizado para acceder a él. La virtualización de escritorios es un elemento clave de los espacios de trabajo digitales y depende de la virtualización de aplicaciones (Villegas, 2017).

Según Vmware (2019). Debido a que la virtualización solo comenzó en los servidores y, una vez comprobada, se trasladó al entorno de escritorio, la nube es el nuevo escenario para la infraestructura de escritorio como servicios (DaaS – *Desktop as a Service).* Los escritorios virtuales alojados en la nube erradican las barreras de adopción, entregan un escritorio completo desde la nube y proporcionan todos los beneficios de la infraestructura de escritorios virtuales - VDI.

7.2.5. Conocimientos para la ciberseguridad.

El mundo se encuentra en camino a la Cuarta Revolución Industrial (4RI), caracterizada por la aparición de nuevas tecnologías que están fusionando el mundo físico, digital y biológico (Schwab, 2016). En informe publicado por la Organización para la Cooperación y el Desarrollo Económico – OCDE (2015), establece que la primera etapa del enfoque de gestión de riesgos de seguridad digital es la concientización, adquisición de habilidades y conocimientos para capacitar a las partes interesadas en la gestión de riesgos. "Se necesita más investigación sobre los tipos de actores organizacionales, las habilidades que necesitan y cómo involucrarse productivamente con los

efectos impredecibles de las nuevas tecnologías y las configuraciones digitales / humanas emergentes" (Baptista, et al., 2020, p.9).

"La mayor parte de la región latinoamericana carece de personal especializado y el equipo necesario para contrarrestar las amenazas cibernéticas" (Parragues y Caldera, 2016, p.3). El Centro de Estudios Estratégicos Internacionales – CSIS (2016) enfatiza en su investigación sobre la escasez mundial de profesionales de ciberseguridad, que se requiere la incorporación de individuos más cualificados, mejoras en la educación y conocimientos específicos, una mayor diversidad de empleados, la adopción de tecnologías de seguridad y la recopilación de datos.

La prevención de los riesgos en ciberseguridad requiere para su adecuado tratamiento, de un conocimiento profundo de la ciberdelincuencia y de las competencias necesarias para trabajar en pro de su prevención e investigación, ya sea en el ámbito policial o en el empresarial (Santos, Guisado y Morán, 2017). Por la naturaleza de su actividad, el SOC se convierte en una fuente que permite comprender el efecto de los riesgos por ciberseguridad en la transformación digital en la nueva normalidad, al mismo tiempo que puede ayudar a identificar necesidades de conocimientos específicos que favorezcan su implementación y permanencia en el tiempo, convirtiendo al talento humano en un aliado estratégico y no un riesgo en sí mismo.

7.1. Definición de Variables.

A continuación se listan las variables y sus respectivas dimensiones, las cuales serán consideradas para la formulación de las hipótesis de la presente investigación.

Tabla 6 – Variables y sus dimensiones.

Variable Independiente (VI): Riesgos en Ciberseguridad	**Variable Dependiente (VD): Transformación Digital**
VID1: Vulnerabilidades en sistemas de información.	VDD4: Internet de las cosas – IoT.
VID2: Ciber amenazas.	VDD5: Servicios de nube.
VID3: Ciberataques.	VDD6: Servicios de escritorios remotos y virtuales.
	VDD7: Conocimientos para la ciberseguridad.

Fuente: Elaboración propia.

8. HIPÓTESIS.

Tabla 7 – Hipótesis a ser comprobadas con el instrumento de medición.

H1 o principal: Los riesgos por ciberseguridad, inciden sobre la transformación digital. La confianza es clave en el proceso de adopción y mantenimiento en el tiempo de la transformación digital, a partir de la experiencia del analista de ciberseguridad, se pretende identificar el nivel de incidentes de ciberseguridad contrastado con la situación antes del impacto del Covid-19. Hipótesis H0 o contraria: Los riesgos por ciberseguridad, no inciden sobre la transformación digital.
H2: Las vulnerabilidades tecnológicas asociadas a configuraciones erradas, configuraciones por defecto, software desactualizado, y/o puertas traseras, son más frecuentes en incidentes de seguridad relacionados con tecnologías de la internet de las cosas – IoT, servicios en la nube y servicios de escritorios remotos y virtuales en la nueva normalidad. La tecnología es vulnerable, requiere la intervención humana para reducir los riesgos, se pretende identificar el comportamiento de incidentes asociados a la introducción acelerada de tecnologías emergentes durante la pandemia, sin que se cumplan algunos estándares de seguridad.
H3: Las ciber amenazas como programas maliciosos, redes de robots, *ramsonware*, son más frecuentes en incidentes de seguridad relacionados con tecnologías de la internet de las cosas – IoT, servicios en la nube y servicios de escritorios remotos y virtuales en la nueva normalidad. La transformación se apalanca en el uso de tecnologías emergentes, las que a su vez propician la aparición y/o complejidad de ciber amenazas, que combinan múltiples técnicas, se pretende establecer el nivel de presencia de estas nuevas ciber amenazas en el entorno llamado nueva normalidad.
H4: Los ciberataques tales como inundación, amenazas persistentes, *phishing*, acceso no autorizado y robo de información sensible o nuevas técnicas, son más frecuentes en incidentes de seguridad relacionados con tecnologías de la internet de las cosas – IoT, servicios en la nube y servicios de escritorios remotos y virtuales en la nueva normalidad. La presencia de las tecnologías emergentes como IoT, nube, virtualidad, genera un aumento de la superficie para los ataques cibernéticos, identificar el nivel de frecuencia y complejidad de estos es fundamental para establecer estrategias de gestión del riesgo por ciberseguridad oportunamente.
H5: El incremento en el uso de tecnologías tales como como internet de las cosas – IoT, servicios en la nube y servicios de escritorios remotos y virtuales, en la nueva normalidad, evidencia la falta de conocimientos por parte de los analistas de ciberseguridad responsables de gestionar incidentes en los SOC. El analista SOC es uno de los más activos actores en el ámbito de la ciberseguridad, conocer de primera mano su actual nivel y necesidades de conocimiento asociados a las vulnerabilidades, ciber amenazas, ciber ataques y tecnologías emergentes, puede ayudar a identificar oportunidades para una transformación digital más confiable.

Fuente: Elaboración propia.

9. METODOLOGÍA GENERAL O DE PRIMER NIVEL

9.1. Enfoque, diseño de la investigación y alcance o tipo de estudio.

Tabla 8 - Definición del enfoque, diseño y alcance de la investigación.

	Tipos y características de investigación definidos para el presente estudio
Alcance o tipo de estudio	**Descriptivo**: Reseña rasgos, características, cualidades o atributos de la población objeto de estudio; y **correlacional**: Mide el grado de relación entre las variables de una población estudiada, además no hay manipulación de datos, solo medición de las variables. (Hernández-Sampieri y Mendoza, 2008, p. 189).
Diseño	**No experimentales:** Se implementan sin manipular variables, los fenómenos o variables ya ocurrieron; y **transversales o transeccionales:** Medición en un tiempo único (Hernández-Sampieri y Mendoza, 2008).
Enfoque de la Investigación	**Cuantitativo:** Con base en la correlación de las variables. Implica definir la unidad de muestreo que es el caso a seleccionar de una población y cuyo conjunto integra la muestra; y la **unidad de análisis** que produce los datos e información para ser examinados (Hernández-Sampieri y Mendoza, 2008).

Fuente: Elaboración propia, definiciones tomadas de Hernández-Sampieri y Mendoza (2008).

9.2. Método de investigación (encuesta).

Para llevar a cabo el estudio y análisis propuesto en el presente proyecto, se utilizará como instrumento de investigación la encuesta, la cual, por medio de enunciados afirmativos, analizará el nivel de frecuencia y grado de percepción por parte de los analistas de ciberseguridad de las Empresas Digiware y Etek de las diferentes situaciones expuestas relacionadas con los riesgos en ciberseguridad dentro de la actual transformación digital.

Tabla 9 - Calculo del tamaño de la población en función del nivel de confianza.

Descripción	**Valores**
Tamaño de población (N) =	128
Variabilidad positiva (P) =	0,5
Variabilidad negativa (Q) =	0,5
Nivel de confianza (Z) =	95%
Grado de precisión o error (E) = +/-	5%
	Resultado
Muestra (n) =	90
Para contar con un nivel de confianza del 95%, se deben mínimo realizar 90 encuestas, dentro de una población total de 128 analistas en de las empresas Digiware y Etek.	

Fuente: Elaboración propia.

La encuesta está compuesta por los siguientes puntos:

Introducción general: Descripción de aspectos importantes para la ejecución.

Dimensiones de la variable independiente: Se solicita evaluar en escala de 1 a 7, lo enunciado para las dimensiones: Vulnerabilidades en sistemas de información, ciber amenazas y ciberataques.

Dimensiones de la variable dependiente: Se solicita evaluar en escala de 1 a 7, lo enunciado para las dimensiones: La internet de las cosas - IoT, servicios en la nube, servicios de escritorios remotos y virtuales y, conocimientos para la ciberseguridad.

En la tabla a continuación se presentan las variables, dimensiones y correlaciones a partir del análisis de los resultados obtenidos posteriormente a la aplicación del instrumento de medición.

Tabla 10 – Correlación de variables, dimensiones y resultados.

	VARIABLES		DIMENSIONES DE LAS VARIABLES							CORRELACIONES	
Hipótesis	**VI**	**VD**	**VID1**	**VID2**	**VID3**	**VDD4**	**VDD5**	**VDD6**	**VDD7**	**SI**	**NO**
H1	X	X								X	
H0	X	X									X
H2			X			X	X	X	X	X	
H02			X			X	X	X	X		X
H3				X		X	X	X	X	X	
H03				X		X	X	X	X		X
H4					X	X	X	X	X	X	
H04					X	X	X	X	X		X
H5			X	X	X				X		X
H05			X	X	X				X	X	

Fuente: Elaboración propia.

10. ANALISIS DE RESULTADOS

El instrumento de medición se aplica a 128 colaboradores que desempeñan el rol de analista de ciberseguridad en las empresas Digiware y ETEK. Como resultado final se obtuvieron 102 respuestas, logrando un nivel de confianza del 100%. Para el análisis de resultados se empleó el programa SPSS de IBM v.26 aplicando metodologías de correlación.

10.1. Análisis descriptivo.

Para el análisis se ingresan a SPSS los promedios de cada conjunto de afirmaciones por cada dimensión de las variables así: Vulnerabilidades (vulnerabilidades en sistemas de información), amenazas (ciber amenazas), ataques (ciberataques), IoT - (internet de las cosas), nube - servicios en la nube, escritorios (servicios de escritorios remotos y virtuales), conocimientos (conocimientos para la ciberseguridad).

Tabla 11. Medidas de tendencia central.

Estadísticos

		PROM (Vulnerabilidades)	PROM (C. Amenazas)	PROM (C. Ataques)	PROM (IoT)	PROM (Nube)	PROM (Escritorios)	PROM (Conocimiento)
N	Válido	102	102	102	102	102	102	102
	Perdidos	100	100	100	100	100	100	100
Media		4,600	4,606	4,678	4,325	4,594	4,559	3,467
Mediana		4,600	4,600	4,600	4,400	4,600	4,600	3,400
Moda		4,6	4,4	4,6	4,6	4,4	4,4[a]	3,0
Desv. Desviación		,5930	,6059	,6755	,6540	,6988	,7303	,8105
Asimetría		,260	-,116	-1,508	,275	-,286	-1,119	,353
Error estándar de asimetría		,239	,239	,239	,239	,239	,239	,239
Curtosis		,569	,672	7,779	1,757	1,763	4,144	-,158
Error estándar de curtosis		,474	,474	,474	,474	,474	,474	,474
Rango		3,6	3,4	5,2	4,2	4,6	4,8	3,6

a. Existen múltiples modos. Se muestra el valor más pequeño.

Fuente: Elaboración propia.

Los resultados obtenidos en la tabla anterior indican una media aritmética de 4,6 para las variables vulnerabilidad, amenazas, ataques, nube y escritorios, donde la moda es igual 4,6 siendo esta la respuesta que más se repite en esta serie de variables. Para la variable IoT la media es de 4,3 con una moda de 4 y para la variable de conocimiento la media es de 3,4, con moda de 3 como la respuesta que más se repite.

La desviación estándar en el análisis de la variable de vulnerabilidad es de 0,5930 lo que quiere decir que si se suman a la media 4,6 + 0,5930 el resultado obtenido es de 5.1. Para las demás variables los resultados obtenidos corresponden a continuación: Ciber amenazas 5.2, ciberataques 5.3, IoT 4.9, nube 5.2, escritorios 5.2, conocimiento 4.2. La desviación estándar de la dimensión

de conocimientos para la ciberseguridad es de 0,8105 siendo la variable más alejada de la serie de dimensiones, lo que indica que se tiene en esta una mayor dispersión de los datos.

10.1.1. Gráficos de frecuencia.

Los histogramas de las dimensiones confirman que el comportamiento de los datos es normal con respecto a su ubicación bajo la campana de Gauss, lo cual se corrobora simultáneamente con el grafico de comprobación de la normalidad de los datos promedio, verificando la cercanía en su mayoría, a excepción de contados puntos, con la línea de progresión aritmética.

Figura - 2 - Histograma y comprobación de la normalidad de los datos para la dimensión: Vulnerabilidad (vulnerabilidades en sistemas de información).

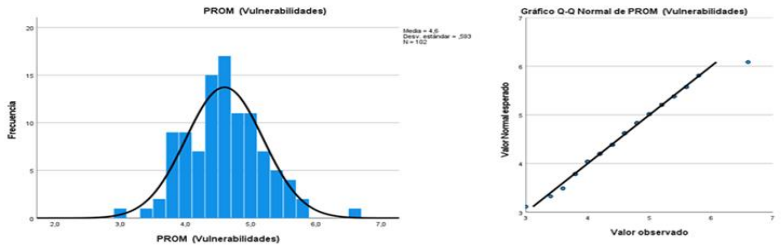


Figura - 3 Histograma y comprobación de la normalidad de los datos para la dimensión: Amenazas (ciber amenazas).

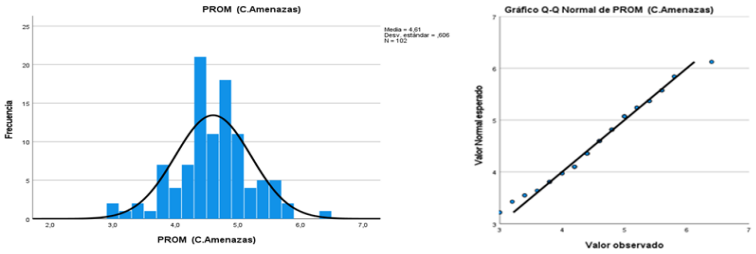


Figura - 4 Histograma y comprobación de la normalidad de los datos para la dimensión: Ciberataques (ciberataques).

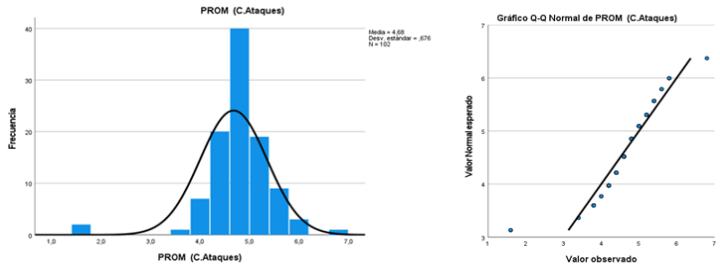


Figura - 5 Histograma y comprobación de la normalidad de los datos para la dimensión: IoT - (internet de las cosas).

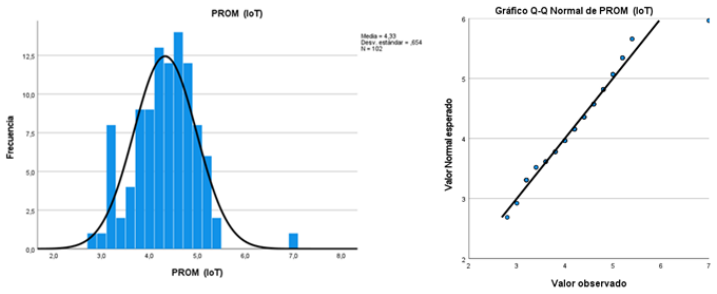


Figura - 6 - Histograma y comprobación de la normalidad de los datos para la dimensión: Nube - servicios en la nube.

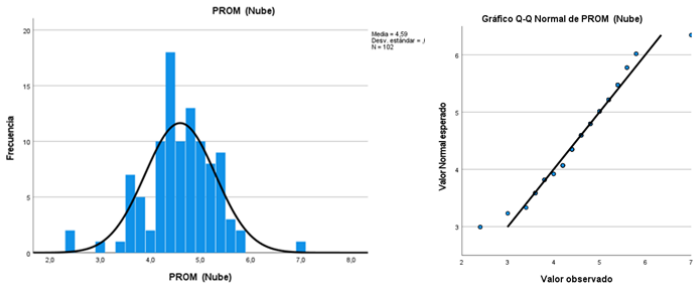


Figura - 7 - Histograma y comprobación de la normalidad de los datos para la dimensión: Escritorios (servicios de escritorios remotos y virtuales).

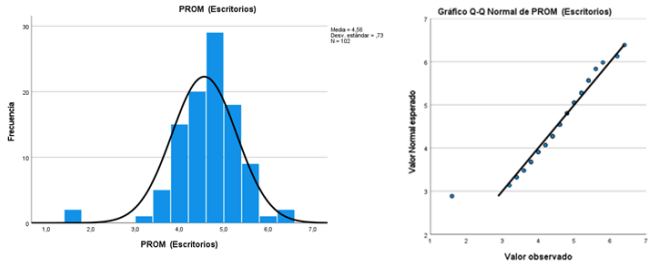
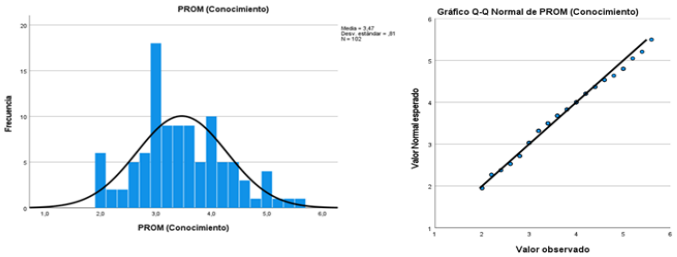


Figura - 8 Histograma y comprobación de la normalidad de los datos para la dimensión: Conocimientos (conocimientos para la ciberseguridad).



Fuente: Elaboración propia.

En síntesis, los datos procesados se reflejan en la siguiente tabla.

Tabla 12 - Resumen del procesamiento de casos.

		PROM (Vulnerabilidades)	PROM (C. Amenazas)	PROM (C. Ataques)	PROM (IoT)	PROM (Nube)	PROM (Escritorios)	PROM (Conocimiento)
Longitud de serie o secuencia		202	202	202	202	202	202	202
Número de valores perdidos en el gráfico	Perdido por el usuario	0	0	0	0	0	0	0
	Perdido por el sistema	100	100	100	100	100	100	100

Los casos no están ponderados.

Fuente: Elaboración propia.

10.2. **Análisis correlacional o comprobación de hipótesis de la investigación.**

El análisis para comprobar las hipótesis planteadas se realiza mediante la correlación de Pearson buscando medir el grado de relación de dos variables cuantitativas.

Tabla 13 - Relación entre riesgos en ciberseguridad y transformación digital, según Pearson.

		VI	VD
VI	Correlación de Pearson	1	,659**
	Sig. (bilateral)		,000
	N	102	102
VD	Correlación de Pearson	,659**	1
	Sig. (bilateral)	,000	
	N	102	102

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia.

Con un índice de Pearson de 0,659 se identifica una correlación fuerte entre las variables riesgos en ciberseguridad y transformación digital, el nivel de significancia 0,000 indica que los datos son confiables y existe una relación significativa positiva entre las variables de la hipótesis principal H1. Lo anterior permite inferir que los riesgos por ciberseguridad tienen efectos sobre la transformación digital en la nueva normalidad, y a la vez se rechaza la hipótesis nula o contraría H0.

En la tabla a continuación se observa una moderada correlación positiva entre las vulnerabilidades de los sistemas de información y las tecnologías como la internet de las cosas - IoT y los servicios en la nube, con coeficientes de Pearson de 0,371 y 0,378 respectivamente, con débil correlación para la dimensión de escritorios remotos (0,182); esta última con un nivel de significancia de 0,067 en escala de 0,01.

Tabla 14 – Relación entre vulnerabilidades de sistemas de información y tecnologías de IoT y servicios de nube.

		PROM (Vulnerabilidades)	PROM (IoT)	PROM (Nube)	PROM (Escritorios)
PROM (Vulnerabilidades)	Correlación de Pearson	1	,371**	,378**	,182
	Sig. (bilateral)		,000	,000	,067
	N	102	102	102	102

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia.

Lo anterior permite comprobar la hipótesis H2, el nivel de significancia de 0,000 confirma que los datos son confiables para establecer una correlación positiva entre las vulnerabilidades relacionadas a las tecnologías de IoT y servicios en la nube y el incremento en la frecuencia con la que se asocian a incidentes de seguridad, especialmente producto de sus debilidades intrínsecas a la tecnología y/o su implantación sin cumplir con los estándares mínimos en seguridad. Al mismo tiempo se comprueba la hipótesis nula para el caso específico de la correlación entre vulnerabilidades y escritorios remotos.

En la tabla a continuación, los coeficientes de Pearson establecen la existencia de correlación moderada entre las dimensiones de ciber amenazas en la nueva normalidad y la internet de las cosas – IoT, servicios en la nube y servicios de escritorios remotos y virtuales, con una relación confiable de 0,000 en escala de 0,01 para todos los casos, rechazando así la hipótesis contraria H03. Lo anterior, comprueba la hipótesis H3. Más del 85% de los encuestados confirman que la nueva normalidad ha generado un incremento en el uso de las tecnologías de IoT, servicios de nube y escritorios remotos, con incremento en la frecuencia de los incidentes que implican técnicas como el *malware*, pero también nuevas formas de amenazas desconocidas.

Tabla 15 - Relación entre ciber amenazas y tecnologías de IoT y servicios de nube.

		PROM (C.Amenazas)	PROM (IoT)	PROM (Nube)	PROM (Escritorios)
PROM (C.Amenazas)	Correlación de Pearson	1	,461**	,544**	,478**
	Sig. (bilateral)		,000	,000	,000
	N	102	102	102	102

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia.

En la tabla a continuación se observan los coeficientes de Pearson de la correlación entre ciberataques en la nueva normalidad y las dimensiones internet de las cosas – IoT, servicios en la

nube y servicios de escritorios remotos y virtuales, la relación es moderada y significativa en escala de 0.01 para todos los casos, rechazando la hipótesis contraria H04.

Tabla 16 - Relación entre ciberataques y tecnologías de IoT, servicios de nube y servicios de escritorios.

		PROM (C.Ataques)	PROM (IoT)	PROM (Nube)	PROM (Escritorios)
PROM (C.Ataques)	Correlación de Pearson	1	,500**	,612**	,624**
	Sig. (bilateral)		,000	,000	,000
	N	102	102	102	102

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia.

Lo anterior permite inferir que la nueva normalidad ha significado un incremento en los ciberataques, comprobando la hipótesis H4. Los coeficientes de Pearson son inclusive mayores que las correlaciones observadas para H2 y H3, tal y como lo confirman el 98% de los encuestados. La significancia de las relaciones confirma que el aumento en la activación de IoT, servicios de nube y servicios de escritorios en la nueva normalidad según el 85% de los encuestados, trae consigo el incremento en los niveles de riesgos por ciberataques.

La tabla a continuación presenta la no correlación entre los promedios de los datos de las dimensiones conocimiento y vulnerabilidades, ciber amenazas y ciberataques, la significancia es superior al 0,01 en todos los casos, confirmando la hipótesis nula H05. Por lo tanto se acepta la hipótesis contraria en esta primera aproximación. Los coeficientes de Pearson indican una débil correlación, negativa para el caso de vulnerabilidades, cercana al cero para las demás dimensiones.

Tabla 17 - Relación entre dimensiones de conocimiento, vulnerabilidades, ciber amenazas y ciberataques.

		PROM (Conocimiento)	PROM (Vulnerabilidades)	PROM (C.Amenazas)	PROM (C.Ataques)
PROM (Conocimiento)	Correlación de Pearson	1	-,039	,125	,163
	Sig. (bilateral)		,699	,211	,103
	N	102	102	102	102

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia.

Es decir, no se puede inferir que los niveles de la dimensión conocimientos actuales sobre las dimensiones de las dos variables correlacionadas, tengan relación directa con la hipótesis principal

de la investigación. Sin embargo, se debe observar nuevamente la estadística descriptiva y relacionar específicamente las afirmaciones sobre el conocimiento en las dimensiones de la variable transformación digital y con los conocimientos en las dimensiones de la variable riesgos en ciberseguridad como se presenta en la tabla a continuación.

Tabla 18 – Correlaciones en cuanto a conocimiento entre las dimensiones de las variables transformación digital y la variable independiente riesgos en ciberseguridad.

		Iot5	N5	E5	V4	CA4	CAT4
Iot5	Correlación de Pearson	1	,582**	,285**	,256**	,453**	,585**
	Sig. (bilateral)		,000	,004	,009	,000	,000
	N	102	102	102	102	102	102
N5	Correlación de Pearson	,582**	1	,229*	,119	,315**	,449**
	Sig. (bilateral)	,000		,021	,232	,001	,000
	N	102	102	102	102	102	102
E5	Correlación de Pearson	,285**	,229*	1	,113	,304**	,293**
	Sig. (bilateral)	,004	,021		,258	,002	,003
	N	102	102	102	102	102	102

**. La correlación es significativa en el nivel 0,01 (bilateral).

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia.

En la tabla anterior los coeficientes de Pearson indican una moderada correlación entre el estado del nivel conocimientos sobre IoT y las ciber amenazas (0,453) y ciberataques (0.585), con un nivel de significancia 0,000 en escala de 0,05 según SPSS. Similar situación se observa entre la correlación conocimientos en nube y ciber ataques (0,449), siendo la correlación más débil en escala de significancia de 0,05 para las correlaciones de conocimiento entre las dimensiones de nube y escritorios, frente a vulnerabilidades y ciber amenazas, lo cual permite rechazar la hipótesis contraria H05 para estos casos específicos.

Desde esta perspectiva, se puede inferir la hipótesis H5 puede ser comprobada si se acota el análisis de los resultados específicamente a la correlación positiva y moderada existente entre el conocimiento sobre la internet de las cosas – IoT y servicios en la nube y, su relación con las ciber amenazas y ciberataques en la nueva normalidad.

11. CONCLUSIONES

Los resultados confirman que existe una relación entre los riesgos en ciberseguridad y la transformación digital, dando cumplimiento al objetivo general de la investigación.

El 97% de los analistas encuestados, manifiestan un aumento en la frecuencia con la que se presentan incidentes de seguridad relacionados, en esta etapa llamada nueva normalidad; situación claramente asociada al incremento en la activación de dispositivos tipo internet de las cosas – IoT (87%), servicios de nube (98%) y servicios de escritorios remotos y virtuales (99%). La observación desde la experiencia del SOC permite confirmar lo estipulado por Leiva (2015), sobre la evolución de las TIC y su afirmación acerca de que esto "conlleva serios riesgos y amenazas que pueden afectar a la seguridad". Con base en lo anterior se da cumplimiento al objetivo específico No. 2. En promedio el 98% de los encuestados manifiesta estar de acuerdo con el incremento en incidentes en servicios de nube y de escritorios remotos, en los que el 88% de las respuestas se ubicaron en el rango de 5 a 7 en la escala de 1 a 7.

Los encuestados están de acuerdo con que los clientes del SOC activaron servicios en la nube y servicios de escritorios remotos y virtuales en esta llamada nueva normalidad, sin que estos cumplieran con los estándares mínimos de seguridad, el 92% de sus respuestas en esta particularidad se ubicaron en el rango de 5 a 7 en la escala de 1 a 7. Decisiones probablemente aceleradas por presiones de continuidad de negocio y trabajo remoto producidas por la pandemia del Covid-19, que lleva a las empresas y personas a un cambio radical en la forma de trabajar (Caballero, 2020), favoreciendo la materialización de los riesgos, en un escenario en el que hoy son frecuentes las amenazas mayormente relacionadas con programas maliciosos, redes de robots, *ramsonware*, tal y como lo confirma el 84% de los encuestados y, por ataques que combinan nuevas técnicas además de las amenazas persistentes – APTs, *phishing*, inundación, entre otras, según lo confirman las respuestas de los analistas del SOC. Lo anterior se alinea con los objetivos específicos No. 2 y No. 3 de la presente investigación.

Un capítulo aparte merece la situación relacionada con el creciente uso de las tecnologías de la internet de las cosas – IoT, tal y como lo confirma el 87% de los analistas de los SOC encuestados. Si bien a partir de los resultados se identifica que los ciberataques asociados a éstas no son tan frecuentes en la nueva normalidad tal y como sucede con los servicios en la nube y escritorios

remotos y virtuales, es cierto que se han venido incrementando, y que la mayor parte de los incidentes frecuentemente están asociados a la explotación de vulnerabilidades por configuraciones erradas, configuraciones por defecto, software desactualizado y/o puertas traseras, y también amenazas, tal y como se confirma en las correlaciones entre estas dimensiones, reforzando lo estipulado por Makhdoom, et. al (2019) para quien la vulnerabilidad de los dispositivos de IoT, los ataques de programas maliciosos y el riesgo de compromiso físico de los dispositivos representan un peligro significativo para su sustento. Lo anterior se relaciona con el objetivo específico No. 3 de la investigación. El 75% de los encuestados respondieron en el rango de 3 a 7 en la escala de 1 a 7, en que hay clientes que han decidido apagar, suspender, eliminar, restringir el uso de tecnologías como IoT, 71% en la misma escala para el caso de servicios de nube, entre los meses de Julio a Septiembre de 2020.

Los resultados también han develado uno de los aspectos tratados en el planteamiento del problema; lo relacionado al talento humano en ciberseguridad. El 70% de los encuestados manifiesta estar de acuerdo con la falta de conocimientos en conceptos asociados a las tecnologías que apalancan la transformación digital. Estos conocimientos específicos son un elemento más necesario en la gestión de incidentes de seguridad, de ahí la importancia de lo manifestado por los encuestados, en los que un 80% confirma no tener los conocimientos adecuados en las vulnerabilidades, ciber amenazas y ciberataques propios de la nueva normalidad, convirtiendo al analista de ciberseguridad en un factor de riesgo de carácter no tecnológico para la transformación digital. Es otro de los efectos que se pueden evidenciar. Esto reafirma lo expuesto por Parragues y Caldera (2016), sobre la carencia en América Latina del personal idóneo para contrarrestar las amenazas cibernéticas, misma situación recientemente corroborada por ISACA (2020) sobre la insatisfacción con la calidad del recurso humano parte de los líderes de equipos de ciberseguridad en las organizaciones.

“Los incidentes de seguridad digital también ejercen efectos negativos sutiles, pero de largo plazo, al debilitar la confianza en el entorno digital, limitar la innovación, desacelerar la adopción de las nuevas tecnologías, así como obstaculizar la transformación digital y sus beneficios relacionados” (OCDE, 2019, P.78). A continuación, algunas recomendaciones para el lector, cumpliendo así con lo establecido en el objetivo específico No.4:

- Es necesario fomentar la cultura de la prevención en seguridad. La adopción de metodologías como confianza cero, es una buena práctica para contrarrestar los efectos que producen comportamientos como la activación y uso de tecnologías sin el cumplimiento de los estándares de seguridad evidenciados en los resultados de esta investigación.
- La pandemia biológica desaparecerá cuando la vacuna alcance su mayor cobertura global, sin embargo, los efectos sobre la sociedad permanecerán en el tiempo, predominando el trabajo remoto, la consolidación de la nube como nuevo escenario de procesos de negocios y el uso creciente de dispositivos del internet de las cosas, aplicado a múltiples escenarios de la vida cotidiana, es decir; crecerán las amenazas, los ataques, aparecerán nuevas tecnologías vulnerables como lo indican nos resultados del presente informe corroborando a (Díaz, et at, 2018). Por tanto gobiernos, e instituciones educativas deberán fomentar y desarrollar el conocimiento en ciberseguridad, aspecto identificado como necesidad, más concretamente sobre arquitecturas tecnológicas (IoT, nube, SASE), arquitecturas de seguridad (*Zero Trust*), modelos de gestión de riesgo de forma ágil y simple; para enfrentar así los retos impuestos por la nueva normalidad, tal y como lo indican los encuestados y el análisis de los resultados. Futuras investigaciones podrían encontrar una oportunidad en identificar elementos para desarrollar metodologías, perfiles, habilidades y competencias en torno a la ciberseguridad para una transformación digital más confiable.
- El rol del SOC y su permanencia en la nueva normalidad debe ser investigado. La dinámica evidenciada a partir de los resultados de esta investigación sobre ciber amenazas y ciberataques, la evolución y adopción tecnológica acelerada, requerirán talento humano cada vez más especializado en ciberseguridad. En congruencia con lo manifestado por OCDE (2015), la nueva normalidad implica una nueva forma de gestionar los riesgos, generando impacto a sus procesos mediante inteligencia artificial, automatización, interoperabilidad, colaboración en línea, trabajo remoto, entre otros aspectos que redefinen su organización (Baptista, et al., 2020). Entender las implicaciones que esto conlleva es fundamental para la toma de decisiones de gobiernos y organizaciones en cuanto a la estrategia para responder a los retos que plantea la ciberseguridad.

12. LISTADO DE REFERENCIAS

Baller, S., Dutta S., y Lanvin, B. (2016) Global information technology report 2016, Geneva, Ouranos. Recuperado de: https://www.weforum.org/reports/the-global-information-technology-report-2016.

Baptista, J., Stein, M., Klein, S., Watson, M., Lee, J. (2020). Digital Work and organisational transformation: Emergent digital / Human Work configurations in modern organizations. The journal of Strategic information systems, vol. 29. Recuperado el 10 de septiembre de 2020, Elsevier host: https://www-sciencedirect-com.bdbiblioteca.universidadean.edu.co/science/article/pii/S0963868720300263.

Bakdash J., Hutchinson S., Zaroukian E., Marusich L., Thirumuruganathan S., Sample C., Hoffman B., Das G. Malware in the future? Forecasting of analyst detection of cyber events, *Journal of Cybersecurity*, Volume 4, Issue 1, 2018, tyy007, https://doi-org.bdbiblioteca.universidadean.edu.co/10.1093/cybsec/tyy007

BID (2020), Ciberseguridad riesgos, avances y el camino a seguir en América Latina y el Caribe Reporte 2020. Recuperado de: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

Biggeri, Patricio. (2018). Título de la tesis (Centro de operaciones de seguridad. Estrategia, diseño y gestión). Universidad de Buenos Aires, Argentina. Recuperado de: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1202_BiggeriPH.pdf

Brunetti, F., Matt, D.T., Bonfanti, A., De Longhi, A., Pedrini, G. and Orzes, G. (2020), "Digital transformation challenges: strategies emerging from a multi-stakeholder approach", The TQM Journal, Vol. 32 No. 4, pp. 697-724. Recuperado de: https://doi-org.bdbiblioteca.universidadean.edu.co/10.1108/TQM-12-2019-0309.

CCB – Cámara de Comercio de Bogotá, 2020. Descripción de actividades económicas (Código CIIU). Recuperado de: https://linea.ccb.org.co/descripcionciiu/

Caballero, M., Cilleros, D. (2020). Ciberseguridad y transformación digital: cloud, identidad digital, blockchain, agile, inteligencia artificial. Madrid, España. Editorial Ediciones Anaya Multimedia.

Caamaño Fernández, E.E., y Gil Herrera, R.J. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: Conjugando el talento humano organizacional, NOVUM, 1(10), 61 - 80. Recuperado el 27 de abril de 2020 de Academic Search Premier, EBSCOhost Academic Search Premier, EBSCOhost: https://revistas.unal.edu.co/index.php/novum/article/view/84210/73653

Chávez, S. (2018). El Concepto de Riesgo. Recursos Naturales y Sociedad, 2018. Vol. 4 (1): 32-52. https://doi. org/10.18846/renaysoc.2018.04.04.01.0003

Check Point Software Research. (2020). Cyber Attack Trends: 2020 Mid Year Report, Check Point Software Inc. Tel Aviv, Israel. Recuperado de: https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.

Clark, A., Slayton R. (2019). Regulation risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standads. Recuperado el 9 de septiembre de 2020, Stanford university science and public policy Vol. 46, (3), pp. (339 – 344). EBSCO host: https://eds-b-ebscohost-com.bdbiblioteca.universidadean.edu.co/eds/pdfviewer/pdfviewer?vid=7&sid=0674e7ab-0673-43af-ba79-2d4276b92695%40sdc-v-sessmgr03.

Cifuentes, V. (2018). De los bancos locales, 81% asigna presupuesto para ciberseguridad y seguridad informática. La República. Recuperado de: https://www.larepublica.co/finanzas-personales/de-los-bancos-locales-81-asigna-presupuesto-para-ciberseguridad-y-seguridad-informatica-2795612.

Costas Santos, J. (2015). Seguridad informática. RA-MA Editorial. https://elibro-net.bdbiblioteca.universidadean.edu.co/es/lc/bibliotecaean/titulos/62452.

Deloitte. (2020). COVID-19: Ciberseguridad y la fuerza de trabajo remoto cómo las vulnerabilidades cibernéticas y las eficiencias operativas están cambiando la próxima normalidad. Santiago de Chile, Chile. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/cl/Documents/povs-covid19/POV-covid-ciberseguridad-20-05.pdf

Departamento Nacional de Planeación. (2011, 14 de julio). Lineamientos De Política Para Ciberseguridad y Ciberdefensa (Documento CNPES 3701). Bogotá D.C., Colombia: DNP. Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeación. (2016, 11 de abril). Política Nacional de Seguridad Digital (Documento CONPES 3854). Bogotá D.C., Colombia: DNP. Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Díaz, F., Venosa, P., Macia, N., Lanfranco, E., Sabolansky, A., Rubio D. (2016). Análisis digital forense utilizando herramientas de software libre. Laboratorio de Investigación de Nuevas Tecnologías (LINTI) Universidad Nacional de la Plata. Recuperado de: http://sedici.unlp.edu.ar/handle/10915/52766

Díaz, F., Molnari, L., Venosa, P., Macia, N., Lanfranco, E., Sabolansky, A., (2018). Investigación en ciberseguridad: Un enfoque integrado para la formación de recursos de alto grado de especialización. Laboratorio de Investigación de Nuevas Tecnologías (LINTI) Universidad Nacional de la Plata. Recuperado de: http://sedici.unlp.edu.ar/bitstream/handle/10915/68355/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Diz Cruz, E. (2015). Teoría de riesgo (4a. ed.). Ecoe Ediciones. https://elibro-net.bdbiblioteca.universidadean.edu.co/es/lc/bibliotecaean/titulos/126443.

Farrag, A., Mohamad, S. y El-Horbaty E., (2019). Swarm Optimization for Solving Load Balancing in Cloud Computing, Springer Verlag, 921,102-113, DOI: 10.1007/978-3-030-14118-9_11.

Feito, L. (2007). Vulnerabilidad. Anales del Sistema Sanitario de Navarra, 30 (Supl. 3), 07-22. Recuperado en 12 de octubre de 2020, de http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1137-66272007000600002&lng=es&tlng=es.

Frith, J. (2020). Technical Standards and a Theory of Writing as Infrastructure. Written Communication, 37(3), 401–427. https://doi.org/10.1177/0741088320916553.

Forbes. (2020). The Future Of Post-Covid-19 Digital Transformation: A Critical RELOADED Webinar Dialogue By The Digital Pioneers Network. Recuperado de: https://www.forbes.com/sites/markminevich/2020/07/22/the-future-of-post-covid19-digital-transformation-a-critical-reloaded-webinar-dialogue-by-the-digital-pioneers-network/#71e7f6711045

Ganshani, M. (2017). How SOC Brings Value to the Business. Recurperado de: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/how-soc-brings-value-to-the-business.

Gartner Group. (2020). CFO Actions in Response to COVID-19. Gartner, Arlington, VA, US. Recuperado de: https://www.gartner.com/en/finance/trends/cfo-responses-to-coronavirus

Gobble, M (2018). Digital Strategy and Digital Transformation, Research-Technology Management, 61:5, 66-71, DOI: 10.1080/08956308.2018.1495969.

Hámornik B.P., Krasznay C. (2018) A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers. In: Nicholson D. (eds) Advances in Human Factors in Cybersecurity. AHFE 2017. Advances in Intelligent Systems and Computing, vol. 593. Springer, Cham. https://doi-org.bdbiblioteca.universidadean.edu.co/10.1007/978-3-319-60585-2_21.

Hernández-Sampieri y Mendoza. (2008). Metodologías de la investigación: Rutas Cualitativa, cuantitativa y mixta. (p.p. 77-144). Recuperado de: https://www-ebooks7-24-com.bdbiblioteca.universidadean.edu.co/stage.aspx?il=&pg=&ed=

IBM. (2020). X-Force Threat intelligence Index 2020. Recuperado de: https://www.ibm.com/security/data-breach/threat-intelligence

ISACA. (2015). Cybersecurity Fundamentals. Recuperado de: https://www.isaca.org/bookstore/csx-certificate-exam-resources/csxg2

ISACA. (2020). (s.f.). Cybersecurity. En ISACA® Glossary of Terms. Recuperado el 27 de agosto de 2020, de https://www.isaca.org/resources/glossary.

ISACA. (2020). State of Cybersecurity 2019, Part 1: Current Trends in Workforce Development. Recuperado de: https://www.isaca.org/bookstore/state-of-cybersecurity-2019/whpsc191.

ISO. (2018). Gestión del riesgo. Técnicas de evaluación de riesgos (Norma ISO/IEC 31000:2018). Recuperado de: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es.

Jin, S., Cho, C. (2015). Is ICT a new essential for national economic growth in an information society?, Government Information Quarterly, 32:3, 253-260, DOI: doi.org/10.1016/j.giq.2015.04.007.

Kaplan, A., Haenlein, M. (2019). Digital transformation and disruption: On big data, blockchain, artificial intelligence, and other things. Business Horizons 62 (6), 679-681. https://doi.org/10.1016/j.bushor.2019.07.001

Kemp, S. (2020). Digital in 2020. Recuperado de: https://wearesocial.com/digital-2020.

Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en enfoque Top-Down desde una visión global a una visión local. Revista Latinoamericana de Ingeniería de Software, 3(4), 161-176, DOI: 10.18294/relais.2015.161-176.

Makhdoom, I., Abolhasan, M., Lipman, J., Ping Liu, R., Ni, W., (2019). Anatomy of threats to the internet of things. Journal IEEE Xplore Comunicatios Surveys & Tutorials Vol. 21, pp. (1636 – 1675). Recuperado el 9 de septiembre 2020 de: https://ieeexplore.ieee.org/document/8489954.

Márquez, J. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en Internet de las cosas. Revista de Bioética y Derecho, 46, 85–100. https://doi.org/10.1344/rbd2019.0.27068.

Mateo I., y Cedillo N. (2017). Tendencias De Seguridad Y Vulnerabilidades en Sistemas Basados en La Nube. Espirales: Revista Multidisciplinaria de Investigación, 1(6). https://doi.org/10.31876/re.v1i6.28

Mell, P. Grance T. (2011), The NIST Definition of Cloud C omputing Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, 800-145.

Muniz, J., McIntyre, G., AlFardan, N. (2016). *Security Operations Center*: *Building, Operating, and Maintaining Your SOC*. Indianapolis, United Stated: Pearson.

Normas APA sexta edición (2017). Licencia Creative Commons Atribution-Comercial- Compartir Igual 4.0 Internacional.

Nathans, D. (2014). Designing and Building Security Operations Center, Elsevier Science & Technology Books, 2014. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliotecaean-ebooks/detail.action?docID=1834659.

OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, https://doi.org/10.1787/9789264245471-en

OCDE (2019), Perfilando la transformación digital en América Latina: Mayor productividad para una vida mejor, OECD Publishing, Paris/ACUI, Barranquilla, https://doi.org/10.1787/4817d61b-es.

Ortiz, E. (2020). Ciberseguridad: metodología para la creación de equipos de investigación en seguridad cibernética. 10.13140/RG.2.2.29810.73925. Recuperado de: https://www.researchgate.net/publication/342644439_CIBERSEGURIDAD_METODOLOGIA_PARA_LA_CREACION_DE_EQUIPOS_DE_INVESTIGACION_EN_SEGURIDAD_CIBERNETICA

Pate, M., Kuypers, M., Smith, M., Kedler, P. (2018). Cyber risk management for critical infrastructure: A risk analysis model and three case studies. Risk Analysis Journal. Vol. 38, (2). Recuperado el 9 de septiembre de 2020, EBSCO host de: https://eds-b-ebscohost-com.bdbiblioteca.universidadean.edu.co/eds/pdfviewer/pdfviewer?vid=9&sid=0674e7ab-0673-43af-ba79-2d4276b92695%40sdc-v-sessmgr03.

Parragues, K., Caldera, E. (2016). Cyber security and habeas data: The latin american response to information securyty data protection. OASIS – Observatorio de análisis de los Sistemas Internacionales. Recuperado el 9 de septiembre de 2020, EBSCO host: https://eds-a-ebscohost-com.bdbiblioteca.universidadean.edu.co/eds/pdfviewer/pdfviewer?vid=11&sid=552e6293-71cb-4fa9-8cc4-c93c6037c347%40sdc-v-sessmgr03.

Pirni, A., Giampellegrini, P. and Raffini, L. (2019) Digital transformation and egovernment. For a research agenda on the Liguria Region. OBETS: Revista de Ciencias Sociales, 14(2): 471-490. doi: 10.14198/OBETS2019.14.2.07

REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., [versión 23.3 en línea]. <https://dle.rae.es> [Octubre 12, 2020].

Ruiz, J., (2016). Ciberamenazas: El terrorismo del futuro? Revista Documento Opinión. Vol. 86. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf.

Sánchez, H.S.; Rotondo, D.; Escobet, T.; Puig, V.; Quevedo, J. Bibliographical review on cyber attacks from a control oriented perspective. Annu. Rev. Control 2019, 48, 103–128. https://doi.org/10.1016/j.arcontrol.2019.08.002.

Sancho, C., (2017). Ciberseguridad. URVIO - Revista Latinoamericana de Estudios de Seguridad. Volumen No. 20, pp. 8-15. http://dx.doi.org/10.17141/urvio.20.2017.2859.

Santiago, E. J., y Allende, J. S. (2017). Riesgos de ciberseguridad en las empresas. Tecnología y desarrollo, (15), 10. Recuperado de: https://revistas.uax.es/index.php/tec_des/article/view/1174

Santos, T., Telha, A., Páscoa, C. (2017). The online organization. Volume 121, pp. (370-375). Recuperado el 10 de septiembre de 2020, Elsevier host: https://www-sciencedirect-com.bdbiblioteca.universidadean.edu.co/science/article/pii/S187705091732241X.

Santos, C. P., Guisado, Á. C., y Morán, J. J. D. (2017). El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito. Revista Policía y Seguridad Pública, 7(1), 237-270.

Schwab, K. (2016). The Fourth Industrial Revolution. Ginebra: World Economic Forum. SNCI. Recuperado de http://www.colombiacompetitiva.gov.co/sncei/Paginas/quienes-somos.aspx.

Tamayo, S. y Gonzalez, D. (2020). La gestión de riesgos: herramienta estratégica de gestión empresarial. Editorial Universo Sur. Recuperado de: https://elibro-net.bdbiblioteca.universidadean.edu.co/es/lc/bibliotecaean/titulos/131885.

Tarazona, C. (2017). Revistas Universidad Externado de Colombia No. 1640. Amenazas informáticas y seguridad de la información, pp. 137-146. Recuperado de: https://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915/

UE (2016). Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Recuperado de https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

Universidad EAN (2020). Grupos de investigación. Recuperado de: https://universidadean.edu.co/investigacion/grupos-de-investigacion.

Urcuqui L. C. C. García P. M. y Osorio Q. J. L. (2018). Ciberseguridad: un enfoque desde la ciencia de datos. Editorial Universidad Icesi. https://elibro-net.bdbiblioteca.universidadean.edu.co/es/lc/bibliotecaean/titulos/120435 p.21.

Vargas, P. (2020). El teletrabajo que han tenido que implementar las empresas ha traído consigo retos en materia de seguridad informática. *La República.* Recuperado de: https://www.larepublica.co/globoeconomia/ciberseguridad-otro-reto-que-deben-enfrentar-las-empresas-en-el-mundo-por-covid-3013083.

VIANO, E. C. *Cybercrime, Organized Crime, and Societal Responses.* Springer International Publishing, 2017.

Villegas, J. P. (2017). Teletrabajo: menos escritorios más movilidad y mejores experiencias. [artículo de revista]. Econtent.

Vmware. (2019). Migrando escritorios a la nube. Recuperado de: https://www.vmware.com/files/latam/pdf/products/daas/VMware-Moving-Desktops-to-the-Cloud-Whitepaper.pdf.