Universidad Autónoma de Querétaro
Facultad de Contaduría y Administración
Maestría en Gestión de la Tecnología

Análisis de Inclusión de la Ciberseguridad en la Educación y su Relevancia Empresarial

TESIS

Que como parte de los requisitos para obtener el Grado de

Maestro en Gestión de la Tecnología

Presenta:

Yesenia Matilde Espino

Dirigido por:

Dr. Luis Rodrigo Valencia Pérez

Dr. Luis Rodrigo Valencia Pérez
Presidente
Dr. Arturo Castañeda Olalde
Secretario
Dr. Héctor Fernando Valencia Pérez
Vocal
Dra. Carla Patricia Bermúdez Peña
Suplente
Dr. Francisco Flores Agüero
Suplente

Centro Universitario, Querétaro, Qro.

Mayo 2023

México

Análisis de Inclusión de la Ciberseguridad en la Educación y su Relevancia Empresarial

por

Yesenia Matilde Espino

I. RESUMEN

El presente trabajo muestra una investigación de enfoque mixto y de tipo exploratorio, descriptivo, no experimental, transversal; orientada a esclarecer si existe una diferencia considerable en el nivel de conocimientos en ciberseguridad, entre los requerimientos de las empresas y lo que saben los egresados de carreras afines a temas de ciberseguridad, así como a ilustrar la relevancia que este tipo de conocimientos tiene dentro de las empresas.

Entre los resultados más relevantes se tiene que existe una leve diferencia entre el nivel de conocimientos en ciberseguridad solicitados por las empresas y el que realmente tienen los egresados de carreras afines a la seguridad cibernética, ya que, conforme a los resultados de las pruebas t-student para muestras independientes realizadas, no puede rechazarse la hipótesis nula.

Aunado a esto, se encontró que las empresas aún no consideran el nivel de este tipo de conocimientos como una capacidad determinante para que sus colaboradores o aspirantes sean merecedores de un ascenso o un contrato de trabajo. Además, las organizaciones mencionan que el nivel de conocimientos en ciberseguridad que poseen sus colaboradores o aspirantes no suelen ser verificados antes de adquirir tecnología.

Por estos motivos se piensa que la ciberseguridad no es considerada de manera proactiva dentro de las organizaciones, y que es necesario seguir investigando por qué existe un déficit tan grande de profesionales especialistas en ciberseguridad.

Palabras clave: ciberseguridad, educación, empresas, métodos mixtos, pruebas t-student.

II. ABSTRACT

This document shows an investigation done from a mixed methods approach, with a type of investigation known as exploratory, descriptive, non-experimental, transversal; aimed to clarify whether there is a considerable difference between the level of knowledge about cybersecurity topics that companies require and those that graduates from courses related to cybersecurity have, as well as communicate the relevance companies set in this type of knowledge.

Among the most relevant results is found that there is a slight difference between the level of knowledge in cybersecurity that companies require and the level that graduates from courses related to cybersecurity actually have, since, according to the results of the student's t-test for independent samples performed, the null hypothesis cannot be rejected.

In addition to this, it was found that companies still do not consider the level of this type of knowledge as a key skill for their employees or applicants to be worthy of a promotion or a job offer. Moreover, organizations mention that the level of knowledge in cybersecurity that their collaborators or applicants have is not usually verified before acquiring technology.

For these reasons, it is thought that cybersecurity is not considered proactively within organizations, and that it is necessary to continue investigating the reason why there is such a large deficit of cybersecurity professionals.

Keywords: cybersecurity, education, companies, mixed methods, student's t-test.

III. AGRADECIMIENTOS

a) Por la beca otorgada a lo largo de este programa, hago extensivo mi agradecimiento tanto al Consejo Nacional de Ciencia y Tecnología como a la Universidad Autónoma de Querétaro.

b) Muchas gracias al Dr. Luis Rodrigo Valencia Pérez, por su apoyo como profesor, director de tesis y coordinador del programa.

c) Gracias a la plantilla docente de la Maestría en Gestión de la Tecnología, por compartir sus conocimientos y pasión por la gestión tecnológica en cada una de sus cátedras.

d) Mi más sincero agradecimiento a los profesores y personal administrativo de la Universidad de Santiago de Compostela, por brindarme su amable apoyo antes, durante y después de mi estancia en esta prestigiosa institución gallega.

e) Un agradecimiento especial por su ayuda desinteresada: a todas las organizaciones que difundieron las encuestas utilizadas para la recolección de datos y a las personas que voluntariamente las respondieron. Así como al M.C. Alberto Lamadrid y al Dr. Luis Cruz.

f) Al personal administrativo de la Facultad de Contaduría y Administración, así como al personal de la Dirección de Movilidad Académica; que apoyó la gestión de todos los trámites necesarios para el correcto cumplimiento de los requerimientos del programa, así como de la movilidad internacional realizada. Gracias.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

1.1. Planteamiento del Problema

En la actualidad se ha dado prioridad a la digitalización de las actividades, por lo que el acceso y divulgación de información [en algunos casos sensible] se vuelve cada vez más fácil de obtener y vulnerar, poniendo en riesgo la seguridad de empresas e individuos.

A pesar del riesgo latente de ataques, se estima que un 53% de las empresas no cuenta con personal cualificado para actuar frente a emergencias de seguridad (PwC, 2020).

Esto debido, entre otras cosas, a la falta de individuos profesionalmente formados para atender las problemáticas relacionadas a la ciberseguridad.

Una de las razones por las que este tipo de perfil profesional escasea, es que solo un 23% de los expertos en temas de ciberseguridad afirma que los programas educativos a nivel universitario realmente están preparando a los estudiantes para poder desempeñarse dentro este sector, cuyo perfil requiere no solo de habilidades técnicas; con base en datos a nivel mundial (Martínez, 2019).

Esto podría estar relacionado a que si bien México cuenta con una estrategia de ciberseguridad, presentada en 2017, que tiene el objetivo de identificar y establecer las acciones de seguridad cibernética en el ámbito social, político y económico.

En ella hace falta mencionar temas referentes a: la implementación de programas académicos que permitan formar a más profesionales especializados en ciberseguridad; la inclusión de temas relacionados al ciberespacio y la ciberseguridad en la retícula de los niveles educativos básica y media superior; así como la definición de estrategias de difusión

pública para inculcar y mejorar la cultura de ciberseguridad entre todos los niveles socioeconómicos y generacionales de la población, incluyendo la cultura de denuncia de los delitos cibernéticos (American Chamber México, 2020).

Por otra parte, en 2020 se detectó que dentro del territorio nacional existen solamente ocho universidades que ofrecen programas de formación académica tales como diplomados, licenciaturas y posgrados, puramente relacionados a la ciberseguridad (Gutiérrez, 2020).

Debido a estos motivos, es oportuno preguntarse: ¿están los egresados de carreras altamente relacionadas con la ciberseguridad lo suficientemente preparados para coadyuvar en la implementación de medidas de defensa cibernética en las implementaciones sistemáticas de las que sean partícipes?, ¿cómo estos conocimientos [o falta de ellos] en los profesionistas influyen en las decisiones de una empresa?, ¿qué tan relevantes son los temas relacionados a la ciberseguridad dentro de una empresa?, ¿por qué?.

Adicional a los cuestionamientos anteriores, surge también la necesidad de evaluar: ¿qué tanto invierten las empresas en temas o tecnologías referentes a la ciberseguridad?, ¿cuál es el nivel de participación que las empresas permiten a los empleados en temas de ciberseguridad?, ¿qué tanto se preparan en estos temas los egresados de carreras altamente afines a la ciberseguridad?. Esto con el propósito de identificar qué tipo de conocimiento puede estar faltando en los planes de estudio actuales, así como medir tendencias y proponer líneas de acción.

1.2. Justificación

Una vez conocido el problema, es importante destacar que de acuerdo a cifras de América Latina, provistas por Kaspersky, México es la segunda nación con mayor cantidad de intentos de ciberataques a comercios (El Universal, 2020b). Ya que según datos de esta misma firma, para México, la media de ataques de malware fue de 9.5 por segundo durante 2019, dando como resultado un promedio de 572 ataques por minuto (Hernández, 2019a).

Por otra parte, es necesario mencionar que durante 2018 para que una empresa restablezca en totalidad sus sistemas tras un hackeo, el costo promedio fue de 2.5 millones de pesos y en 2019 aumentó a 6.5 millones de pesos (Chávez, 2020).

Debido a estas alarmantes circunstancias, las compañías han decidido invertir cada vez más en ciberseguridad, por lo que en el caso de México esto se traduce a que las empresas destinan a la seguridad alrededor de un 5.1% del presupuesto total de TI (El Universal, 2019). Mientras que, de manera global y conforme a cifras de Forcepoint México, se han invertido cerca de 1 billón de dólares en temas de ciberseguridad en los últimos 7 años (Valle, 2019).

Si bien las organizaciones han incrementado los montos pecuniarios que se dedican a prevenir ataques cibernéticos, el enfoque que se le da a estas inversiones no siempre es el más conveniente (Chávez, 2019) ya que solo el 5% del total de la cifra invertida a nivel mundial ha resultado efectiva (Valle, 2019).

Uno de los motivos por los que la inversión de una empresa en tecnologías relacionadas a la ciberseguridad no son las más idóneas, se debe a que en la mayoría de las firmas la elección de tecnologías no la hacen ellos mismos si no que contratan externos;

incluso se estima que el 50% de la compra de tecnología dentro de las organizaciones se realiza con la ayuda de un tercero (Chávez, 2019). La contratación de terceros para la evaluación de las condiciones y la implementación de la ciberseguridad en las empresas, en lugar de utilizar a un empleado ya contratado, se debe a que no cuentan con personal calificado para abordar el desarrollo y solución de esta problemática.

Con respecto a no contar con personal calificado en ciberseguridad, este es un factor que puede deberse a que, a nivel mundial existe una gran brecha con respecto a la fuerza laboral especializada existente y la demanda que se tiene por estos perfiles, siendo tan grande que para poder cerrarla, la cantidad de profesionales dedicados a la ciberseguridad debe crecer en un 145% (PwC, 2020). En México existen aproximadamente 341 mil profesionales en ciberseguridad (PwC, 2020) y aunque esta cantidad pudiera parecer elevada, las instituciones de educación estiman que el país tendrá una demanda de 2 millones de este tipo de especialistas desde 2019 y al menos en los 3 años siguientes (Martínez, 2019).

Por otra parte, para mejorar la gestión de los riesgos cibernéticos a los que está expuesta una organización es necesario mejorar las capacidades en ciberseguridad en todos los niveles de ésta; además, si el personal no cuenta con los conocimientos y capacidades necesarias para gestionar las nuevas tecnologías empleadas en el desarrollo del negocio así como conocer y medir el impacto de los riesgo, estas inversiones no serán suficientes. Por lo que es importante mencionar que aquellas organizaciones que invierten en el desarrollo de este tipo de conocimientos se han visto beneficiadas en la actualidad (PwC, 2021).

De igual manera, algunas firmas tecnológicas como “Accenture” sugieren que no solo se debe invertir de forma más oportuna en tecnologías que permitan a la empresa volverse

más resiliente ante un ataque cibernético, si no que la seguridad debe ser considerada desde el diseño inicial de la organización, entendiendo dos puntos fundamentales: cuál es el riesgo de negocio que la empresa enfrentaría de ser vulnerada su ciberseguridad y si se está llevando a cabo la medición de la eficiencia de sus políticas en temas de ciberseguridad a largo plazo (Chávez, 2019).

Es sabido que la prevención y/o eliminación de riesgos potenciales optimiza las inversiones, ahorra costos y tiempos, por lo que para establecer indicadores actuales, encontrar tendencias y discrepancias entre lo que se tiene actualmente y el estado objetivo; es de vital importancia entender, estudiar y analizar el nivel de inclusión que tiene la ciberseguridad dentro de las empresas, así como el nivel de profundidad de los conocimientos y habilidades con los que cuentan los egresados de carreras directamente relacionadas con las Tecnologías de la Información y las Comunicaciones. Con estos indicadores y hallazgos que se generen, será posible crear y/o ajustar estrategias y planes de estudio, que ayuden a una mejor integración de la ciberseguridad en las entidades económicas y educativas, a manera de incrementar la seguridad y la confianza que ofrecen las compañías a sus clientes, así como coadyuvar al aumento en la oferta de personal capacitado para afrontar retos de ciberseguridad.

1.3. Pertinencia

De acuerdo a Brito et al. (1998, párr. 20 y 21):

“la gestión tecnológica surge y se desarrolla en el seno de las empresas y que su objetivo fundamental es el logro de una mejor vinculación investigación-industria-sociedad, la cual debe entenderse como una relación de mercado. Esto implica comprender que la mima se rige fundamentalmente por leyes de oferta y demanda.

La gestión tecnológica busca integrar el proceso de cambio tecnológico con los aspectos estratégicos y operativos del control y la toma de decisiones de la empresa. Así, se concibe la tecnología como un arma competitiva y como tal, debe constituir un punto esencial del planteamiento estratégico a largo plazo."

Mientras que, de manera similar, para Muñiz et al. (2001, p.188):

"la función principal de la gestión tecnológica es ser el instrumento de vinculación entre el sector productivo y el de la investigación-desarrollo en el proceso de innovación tecnológica. Se requiere una preparación conceptual y ejecutiva y se realiza para apoyar los procesos de innovación tecnológica que permitan identificar las necesidades y oportunidades tecnológicas, la capacidad de manejo del cambio técnico."

Además, el Consejo Nacional de Investigaciones (National Research Council, 1987) de Estados Unidos de América, define: la gestión tecnológica vincula la ingeniería, la ciencia y las disciplinas administrativas para planificar, desarrollar e implementar capacidades tecnológicas, para con ellas dar forma y lograr los objetivos estratégicos y operativos de una organización.

Con base en los argumentos previamente descritos, es posible establecer que tanto el tema principal de la presente investigación como los subtemas tratados dentro de ésta pertenecen a las líneas de investigación definidas por la gestión tecnológica. Esto debido a que todos ellos están relacionados con la ciberseguridad, que es un tema de ingeniería; la inclusión de ésta dentro de las organizaciones, que apunta en cierta medida a temas propios de las disciplinas administrativas; y las discrepancias encontradas en temas de ciberseguridad entre la industria y los programas educativos, que cumplen con la mejora de la relación industria-investigación planteada con anterioridad.

1.4. Relevancia

Hoy en día el acelerado avance de la tecnología, la conectividad y el uso de las TIC han traído consigo grandes y variadas fuentes de conocimiento, desarrollo e innovación a nivel global; sin embargo, esto también ha provocado un rápido acenso en los ataques cibernéticos, motivo por el cual los temas referentes a la ciberseguridad han ido adquiriendo relevancia en los últimos años.

Además, esta situación ha provocado que cada vez sean más las empresas que buscan invertir en tecnologías que provean o ayuden a incrementar la ciberseguridad de la organización, también, el requerimiento de personal calificado en este tipo de temas ha crecido con el pasar de los años y la sofisticación de los ataques cibernéticos.

Por otra parte, pese al incremento de las inversiones y la consideración de los temas referentes a la ciberseguridad en las empresas; estudios realizados por diferentes compañías del sector informático afirman, entre otras cosas que: durante el año 2020, a nivel global, el 81% de las organizaciones sufrieron afectaciones derivadas de un ciberataque y el costo de éstos fue de alrededor de 6 mil millones de dólares (Excelsior, 2021); lo que deja ver que entre las muchas dificultades que acechan a la empresas en temas relacionados a la ciberseguridad, se encuentran la falta de especialistas y de tecnologías para contrarrestar las brechas de seguridad (Reyes, 2020); puesto que de contar con las recursos tecnológicos y humanos para hacer frente a estos problemas, las cifras de ataques y costos irían a la baja.

Debido a todo lo mencionado en éste apartado, es importante incrementar y diversificar los estudios científicos referentes a la ciberseguridad en territorio nacional, como es el caso de la presente investigación; donde se busca analizar la situación actual del país

con respecto a la ciberseguridad, la relación de ésta con la industria y lo académico, así como resaltar los puntos de mejora.

1.5. Factibilidad

Este estudio pretende servir de apoyo para futuros investigadores que deseen indagar en los temas poco explorados y relacionados con la ciberseguridad en las empresas e instituciones educativas mexicanas, así también, será una referencia para aquellos interesados en conocer las tendencias encontradas a raíz de este análisis y con las cuales podrán proponer alternativas e ideas innovadoras que contrasten o mejoren las problemáticas y/o las soluciones planteadas en la presente investigación.

Si bien los resultados obtenidos en este trabajo podrán ser consultados por cualquier persona interesada en el tema, es importante recordar que el estudio fue desarrollado tomando como punto focal a dos planteles de una de las instituciones mexicanas más reconocidas en la formación de ingenieros (Soriano, 2019).

La elección de esta casa de estudios como objeto viable de análisis para esta investigación se debe, entre otros factores, a que: a) esta institución cuenta con casi el 13% de la matrícula en educación superior a nivel nacional (SEP, 2021), b) el 67.79% de su matrícula se encuentra en programas reconocidos por su buena calidad; contando también con 691 programas de buena calidad y 102 programas de posgrado PNPC (Soriano, 2019), y que pese a ser una institución tan inmensa y que atiende a una gran cantidad de la población que busca formarse como ingeniero, ésta aún tiene retos por enfrentar, varios de ellos relacionados al método de enseñanza, a la actualización de los planes educativos y el hecho

de que estos últimos tengan una relación más estrecha con las necesidades reales de la industria (Hernández, 2018).

2. ANTECEDENTES

A continuación se abordan algunos estudios de relevancia con respecto al panorama general de la ciberseguridad en México, que se han revisado previo al detalle de esta propuesta de investigación:

En términos económicos, a pesar de las altas cifras en gastos derivados de ataques cibernéticos, aún existen brechas importantes en las organizaciones mexicanas con respecto a la ciberseguridad, entre ellas destacan que sólo un 65.3% de las organizaciones se consideran medianamente preparadas para poder hacer frente a las amenazas de seguridad; mientras que, el 47.54% está tomando acción con respecto a la ciberseguridad ya que consideran que existe un aumento preocupante de nuevas y más complejas amenazas; y un 46.7% afirma que la probabilidad de que sus activos digitales sean robados o dañados es media (CANIETI. Como se citó en Gobierno de México, 2017).

Para combatir estos riesgos hace falta que existan más profesionales especializados en temas de ciberseguridad, así como instruir a los usuarios en buenas prácticas de seguridad, esto último debido a que las organizaciones expresan que uno de los puntos que más preocupación les genera son las amenazas internas, que surgen por la falta de comprensión que tienen los usuarios con respecto a las amenazas existentes; además de que es necesario crear una mejor sinergia entre los equipos de IT y los encargados de la seguridad para que mediante su colaboración se logren detectar las amenazas a la seguridad; todos estos motivos solamente dejan en claro que uno de los principales ejes que se deben atender para mejorar la ciberseguridad en cualquier organización es la inversión en capacitaciones para el personal (UNAM-CERT, 2017).

A manera de tener una guía que ayude a dirigir los esfuerzos de la nación para mitigar las ciberamenazas, el poder Ejecutivo del Gobierno de México, con participación del Instituto Federal de Telecomunicaciones, emitió en 2017 la Estrategia Nacional de Ciberseguridad; estableciendo en ésta, objetivos estratégicos enfocados en 5 rubros primordiales (IFT, 2018):

1) sociedad y derechos: crear condiciones dignas y respetuosas con los derechos humanos para que los connacionales puedan llevar a cabo sus actividades en el ciberespacio con garantías de confiabilidad y libertad (IFT, 2018);

2) economía e innovación: contribuir al desarrollo económico de la nación mediante el estímulo al desarrollo e innovación tecnológica, robusteciendo los mecanismos en temas de ciberseguridad (IFT, 2018);

3) instituciones públicas: proteger los sistemas informáticos de las instituciones públicas nacionales garantizando su confiabilidad y disponibilidad (IFT, 2018);

4) seguridad pública: mantener el orden público mediante el aumento de las capacidades en ciberseguridad que ayuden a prevenir e investigar conductas criminales dentro del espacio cibernético (IFT, 2018);

5) seguridad nacional: prevenir riesgos y mitigar amenazas que puedan llegar a afectar la soberanía nacional de alguna manera, mediante el desarrollo de las capacidades en ciberseguridad pertinentes (IFT, 2018).

Sin embargo, en el documento existen temas que no fueron acotados ni precisados de manera completa como lo son los temas específicos sobre ciberseguridad que deben reforzare en los planes académicos y las capacitaciones impartidas por las empresas a sus empleados.

Siendo los usuarios del ciberespacio y las TIC uno de los principales factores de riesgo para la ciberseguridad pero también la primera línea de defensa ante las ciberamenazas, las propuestas enfocadas en solucionar los problemas de ciberseguridad no solo deben contemplar temas puramente tecnológicos sino también aquellos relacionados con procesos y personas como son la educación, la capacitación y la concientización. Dada la importancia de la educación, lo mejor sería optar por construir un sistema educativo en el que los programas referentes a la ciberseguridad sean de calidad y diseñados en conjunto con las empresas y los gobiernos; requiriendo esta tarea que los gobiernos generen una prospectiva que les permita planificar a futuro con base en las necesidades del mañana (Arreola, 2018).

Por otra parte, con respecto a la ciberseguridad en la industria, se conoce que en 2018 alrededor de un 80% de las empresas en México aseguró haber sufrido un incidente de seguridad, lo que no es de extrañar ya que un 44% de las organizaciones no posee su propia estrategia general de seguridad de la información; además, el reporte resalta que los crímenes a los que se han enfrentado con mayor frecuencia son: los ataques al transporte de la cadena de suministro con un 42.1%, la extorsión virtual que llegó al 39.9% y el robo con el mismo porcentaje (El Universal, 2019).

Pese a esto, numerosas organizaciones se toman en serio o ignoran la verdadera función de los requisitos de cumplimiento en ciberseguridad y se preocupan solamente por evitar penalizaciones derivadas de la mala implementación de los estándares o regulaciones, pasando por alto el desarrollo e integrar estrategias de ciberseguridad sólidas (CIO México, 2020). Lo que trae como consecuencia que sigan enfocando sus esfuerzos en el cumplimiento de las normativas y no en analizar y controlar los riesgos reales. Por ejemplo y

específicamente en el caso de México, la pérdida de datos y la filtración de información son problemas que afectan a un 60% de las organizaciones, siendo los errores humanos una de las causas principales de estas brechas (Expansión, 2020); esto se debe, entre otras cosas, a la falta de conciencia, conocimiento y cultura de prevención que trae consigo que la ciberseguridad no sea una prioridad para las empresas.

En este mismo orden de idas, se conoce que "el denominador común para muchas empresas con problemas de ciberseguridad es la escasez de talento humano capacitado y preparado" (CIO México, 2020). Esto último es, en parte, consecuencia de que en territorio nacional se tienen escasos programas educativos a nivel licenciatura, posgrado y líneas de investigación relacionados con la ciberseguridad, por lo que se vuelve imprescindible promover la creación y mejora de este tipo de programas, contando con la ayuda del gobierno federal y de las empresas especialistas en ciberseguridad (Gutiérrez, 2020).

En consecuencia, se vuelve crucial crear políticas públicas que establezcan a la educación digital como eje transversal para tocar los temas relacionados a la ciberseguridad. Además, es preciso tomar en cuenta las peculiaridades y necesidades de los diversos contextos legales, políticos, sociales, culturales, económicos y éticos para integrar las tecnologías al proceso de enseñanza y aprendizaje; así se podrá concientizar de una mejor manera a las personas, las empresas y los gobiernos sobre cómo evitar ser víctimas de vulneraciones a la seguridad y cómo actuar ante los riesgos del uso masivo de las nuevas tecnologías y la conectividad (Moreno et al, 2019).

Así también, es importante que la ciberseguridad sea vista de manera holística. Y se vuelve necesario comprender y analizar las amenazas existentes, conocer los agentes que las

planifican y financian, así como entender los riesgos que éstas traen consigo para establecer una gestión adecuada de éstos (Becerril, 2019).

Con lo descrito en los párrafos previos, es posible visualizar que las investigaciones realizadas al momento en México, sugieren deficiencias tanto en la inversión y manejo de la ciberseguridad dentro de las corporaciones como la escasez de instituciones y programas enfocados en formar personal calificado en temas de ciberseguridad. Sin embargo, estas investigaciones no especifican cuales son las discrepancias y las brechas que se deben cerrar, ni la importancia que actualmente se le está otorgando a estos conocimientos.

Mientras que, en el contexto internacional se pueden encontrar investigaciones con diferentes enfoques sobre la ciberseguridad, como: riegos, tendencias, estrategias, avances, futuro, guías de implementación, políticas efectivas, modelos de auditorías, comparación de herramientas, entre otros.

Esta diversidad de contenidos y bibliografía demuestra que la ciberseguridad es un tema de relevancia a nivel global y que la mayoría de los distintos países están realizando estudios sobre el tema.

Para ejemplificar lo mencionado anteriormente, en los párrafos siguientes se mencionan datos de relevancia encontrados en algunas investigaciones revisadas sobre la ciberseguridad a nivel internacional:

Con respecto a la inversión en ciberseguridad, se prevé que el mercado mundial de ciberseguridad crezca de 167.1 mil millones de dólares en 2019 a 248.26 mil millones de dólares para 2023, alcanzando una Tasa de Crecimiento Anual Compuesto (TCAC) de 10.4%,

según Statista (Columbus, 2020). Las organizaciones enfocan sus estrategias de gestión del riesgo cibernético principalmente en la prevención, por lo que destinan la mayoría de sus inversiones a la adquisición de tecnologías de ciberdefensa de primera línea; sin embargo, otro tipo de ítems como seguros cibernéticos o entrenamiento para la respuesta a eventos de ciberseguridad obtienen solo una fracción del presupuesto (Columbus, 2020).

El país que lidera las inversiones en ciberseguridad es Estados Unidos, en esta nación preponderan los inversores de capital de riesgo en materia de ciberseguridad. Aunque se debe considerar que los inversionistas están comenzando por apostar en otros países y sus empresas, tal es el caso de China, que se posiciona en el segundo lugar (Tilves, 2019).

En cuanto a los profesionales de la ciberseguridad, de acuerdo con datos del Consorcio Internacional de Certificación de Seguridad de Sistemas de Información, a nivel global existen aproximadamente 3.12 millones de vacantes relacionadas con la ciberseguridad; estos puestos de trabajo requieren habilidades que van desde el nivel básico de analista de seguridad, hasta niveles ejecutivos en los que se debe ser capaz de exponer a rangos elevados de la organización, los riesgos que los ciberataques representan para las diferentes áreas que la componen (Duffy, 2021).

Para tratar de enfrentar este déficit de profesionales especializados en ciberseguridad, se ha estado trabajando en una serie de programas educativos, de formación complementaria y de perfeccionamiento; sin embargo, pese a la existencia de este tipo de programas, se estima que la escasez de mano de obra especialista en ciberseguridad, a nivel mundial, se incremente entre un 20% y 30% anualmente en los años siguientes. Por lo que los expertos opinan que tanto el sector privado como el público precisa comprometerse a invertir más en el aumento

de los profesionales en ciberseguridad, mediante el replanteamiento de los sistemas educativos desde el nivel básico hasta el superior para incluir formación enfocada en la ciberseguridad (Duffy, 2021).

Por otra parte, en términos de investigación y divulgación de resultados referentes a la educación en ciberseguridad, los Estados Unidos cuenta con 170 publicaciones en tópicos relacionados, lo que lo convierte en la nación con mayor producción académica de una lista de países entre los que se encuentran la India, Italia, Alemania, Japón, Australia, Grecia, China, Finlandia y Reino Unido; ocupando este último la segunda posición con un total de 17 publicaciones referentes a estos temas. Con estos datos se puede observar que es urgente incrementar la cantidad de estudios que se realizan con respecto a temas relacionados con la ciberseguridad y el aprendizaje (Valencia et al., 2020).

Finalmente, en relación a la situación actual de la ciberseguridad en América Latina y el Caribe, el nivel de madurez promedio de la región se encuentra entre los niveles 1 o “Inicial” y 2 o “Formativa”, esto significa que la mayor parte de los países latinoamericanos y del caribe han empezado a crear iniciativas relativas a la ciberseguridad, con algunas incluso ya implementadas, aunque sin la coordinación requerida entre los actores clave. Para mejorar su clasificación, estas naciones deben promover la cooperación entre todos los actores importantes de cada una de ellas, además de implementar mecanismos para el monitoreo, el análisis y la evaluación de impactos referentes a la ciberseguridad (Banco Interamericano de Desarrollo, 2020).

3. ESTADO DEL ARTE

Con el creciente uso de la tecnología en diferentes rubros de la sociedad, han surgido diversos cuestionamientos y estudios relacionados a la ciberseguridad y su importancia para la tranquilidad de las empresas y la nación, sin embargo, con frecuencia, las investigaciones que hablan de la ciberseguridad en México tienden a abordar temas reactivos pero no de prevención.

Es decir, en ellos se pueden encontrar contraposiciones sobre las estrategias de defensa para ciberataques o recomendaciones sobre la importancia de invertir en sistemas de protección pero no detallan si las instituciones, a manera de prevención o como parte de su estrategia, por ejemplo, consideran el nivel de conocimiento o capacitación sobre seguridad informática de sus colaboradores antes de decidir invertir en nuevos sistemas o infraestructura informática o qué tipo de conocimientos buscan, en caso de que la formación en ciberseguridad si sea tomada en cuenta para la toma de decisiones.

En este apartado se describirán algunos de los estudios más recientes en materia del estado actual de la ciberseguridad, los riesgos potenciales que ésta representa para las organizaciones, la inversión en ciberseguridad y las carencias que se observan con respecto a este tema.

3.1. Investigaciones Locales

De manera local, en el estado de Querétaro, no se han encontrado resultados de investigaciones profundas y específicas con respecto a la ciberseguridad y sus cifras, sin embargo, existen artículos donde se menciona la necesidad de formar profesionales que ayuden a conducir de manera correcta y segura el avance hacía la industria 4.0, y algunos

otros donde se menciona la creación de organismo capaz de ayudar a la empresas a tener en cuenta la ciberseguridad en su transición digital.

A continuación se presentan los extractos más importantes de esos artículos:

3.1.1. Carencias con Respecto a la Ciberseguridad

En el artículo "*Industria 4.0, un reto para las universidades*", publicado por El Universal Querétaro, se muestra una entrevista realizada a Judith Aguilar Acosta, directora de la empresa de programación BUSEM y miembro de la comisión de innovación de Coparmex, Querétaro.

Aquí se menciona la carencia de personal calificado para cubrir la demanda de la industria 4.0 en el estado de Querétaro; así como la falta de alineamiento entre las empresas, el gobierno y las universidades para generarlo.

Con respecto a las casas de estudios superiores, encargadas de generar el capital humano especializado, se hace alusión a que en el estado solamente la Universidad Autónoma de Querétaro, la Universidad Politécnica de Santa Rosa Jáuregui y la Universidad Tecnológica de Corregidora tienen la carrera de ingeniería en software con una matrícula que, en conjunto en 2017, no superaba los 600 estudiantes, de acuerdo a la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES).

Otro problema detectado es la falta de comunicación y planificación entre las empresas dedicadas a las TIC, el gobierno del estado y las universidades queretanas, provocando que estas últimas no generen los perfiles técnicos e ingenieros que se necesitan para el desarrollo de software; y que las instituciones educativas generadoras de tecnología

no propongan desarrollos adecuados ni aprovechables para las verdaderas necesidades de la industria.

Finalmente, Acosta también declara que “se necesitan más universidades que desarrollen capacidades en software embebido, seguridad informática, ciberseguridad, Big Data, Cloud Computing, internet de las cosas, modelación 3D y programación Java” (Cano, 2018).

3.1.2. Inversión en Ciberseguridad en el Estado

De acuerdo con el comunicado de prensa publicado en 2019 por EY México, titulado “EY invierte 40 millones de pesos en centro de ciberseguridad para Querétaro”:

Querétaro es líder en innovación y desarrollo tecnológico, siendo también un gran nicho de talentos en estos sectores. Por ello, por el crecimiento de EY, y la creciente necesidad del mercado de implementar sistemas de ciberseguridad; EY ha decidido instalar en el estado un centro de ciberseguridad avanzada, invirtiendo 40 millones de pesos y estimando crear 109 nuevos empleos al inicio del proyecto.

Las funciones del centro serán: proveer servicios en detección de respuestas y amenazas cibernéticas, gestión de la exposición de amenazas, protección de información de datos e identidad digital. Y su misión es actuar como consultor y proveedor de servicios administrados de seguridad [Managed Security Service Provider o MSSP, por sus siglas en inglés], atendiendo principalmente a las organizaciones con las que ya colaboran.

Ya en 2020 a través del comunicado de prensa “EY México inaugura su Centro de Operaciones de Ciberseguridad en Querétaro”, emitido por EY México; se da a conocer que

la firma ha inaugurado este centro de ciberseguridad en el estado de Querétaro, así como los objetivos del mismo y algunos datos acerca de sobre la ciberseguridad en México.

Entre la información provista por la compañía se encuentra que: solo el 72% de las grandes empresas cuenta con un Centro de Operaciones de Seguridad [o SOC, por sus siglas en inglés], sin embargo, un 60% de las Pymes no lo tienen o incluso carecen de herramientas para el monitoreo; además, un 53% de las empresas manifiestan que no disponen de personal cualificado que pueda hacer frente a eventos de ciberseguridad. Atender esta creciente demanda es una de las razones de la creación del CyberSOC en Querétaro.

Además, el Presidente y Director General de EY México, Víctor Soulé, menciona que la firma ha elegido a Querétaro como sede del CyberSOC y la inversión de 40 millones de pesos que esto representa, debido a que la entidad Queretana es uno de los líderes en cuanto a conglomerados de alta tecnología.

3.2. Investigaciones Nacionales

A nivel nacional, en México, no se han detectado estudios especializados acentuados en proveer un panorama acerca de lo que las empresas están esperando de manera granular sobre los expertos en ciberseguridad, cuánto y cómo están integrando éstas la ciberseguridad dentro del negocio, así tampoco se tiene información que muestre de manera detallada los elementos que conforman la brecha entre lo que las empresas están esperando y lo que sus trabajadores pueden brindarles. Sin embargo, existen diversos artículos que exhiben la situación actual del país frente a la ciberseguridad; los jóvenes y su interacción con la ciberseguridad; así como las expectativas que diferentes empresas en al ámbito de la ciberseguridad, tienen con respecto a ésta.

En los siguientes párrafos se encuentra un breve análisis de los artículos más relevantes seleccionados para este apartado:

3.2.1. Situación de la Ciberseguridad en México

a) En el artículo “76% de los mexicanos encuestados manifiesta estar expuesto en internet de acuerdo con el Índice de civilidad digital de Microsoft” publicado por Microsoft Latinoamérica en Febrero de 2021, Se da a conocer que México se ubica en la posición 30 del ranking mundial sobre el Índice de civilidad digital. Este índice se basa en medir las percepciones que tienen adolescentes y adultos en diferentes países, sobre el nivel de civilidad digital.

El Comisario GN Mtro. Jacobo Bello Joya, Responsable de Ciberdelitos de la Dirección General Científica de la Guardia Nacional; ofreció algunos comentarios para este artículo. Los más importante de ellos es la insistencia en hacer un reforzamiento de la cultura de la ciberseguridad, la alusión al cibercivismo, así como la mención del apoyo de la SEP con la inclusión de nuevas materias que ayuden a fortalecer estos temas entre la población estudiantil. También, el Comisario destacó que actualmente en México, los aspectos cibernéticos más importantes a combatir son los fraudes, robo de datos y ataques cibernéticos en general, por lo que se está trabajando bajo la dirección de la Presidencia de México para la estrategia de seguridad, lo que ha logrado la implementación de acciones como el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, para entre otras cosas, promover las buenas prácticas y la prevención.

Por su parte, Microsoft ha creado una guía gratuita para educar a las personas respecto al riesgo cibernético y auxiliarlos en cómo prevenirlos, abordarlos y enfrentarlos. Esto para ayudar en la mejora de la experiencia en línea de personas, empresas y gobiernos.

b) Por otra parte, en el artículo "2020, en 12 hackeos o incidentes de seguridad en México" de Rodrigo Riquelme, publicado en Enero de 2021 por El Economista; se muestra una parte del escenario actual que enfrenta México con respecto a la ciberseguridad, ya que nos deja ver las instituciones públicas que han sido afectadas con ataques de esta índole.

Tres instituciones que se encuentran entre las principales encargadas de regular y supervisar el sistema financiero mexicano (Condusef, Banxico, SAT) sufrieron un "Defacement", que es una técnica de hacking con la cual los perpetradores modifican la apariencia de una página web administrada por las víctimas de su ciberataque; a lo largo de una semana en Julio de 2020.

La Secretaría de la Función Pública también vio su seguridad vulnerada entre mayo y junio de 2020, el incidente expuso las declaraciones patrimoniales del 58% de los empleados de la Administración Pública Federal. Entre la información confidencial que se vio vulnerada se encuentran el RFC, CURP y Sexo de los funcionarios.

Entre Abril y la segunda mitad del año 2020, datos sensibles como el nombre completo, sexo, edad, diagnóstico y procedimientos quirúrgicos de al menos 551 asegurados del ISSSTE, pudieron ser encontrados en los principales buscadores de internet en lo que fue un ataque cibernético a esta institución.

En Noviembre de 2020 la Comisión Nacional de Seguros y Fianzas, encargada de supervisar que las aseguradoras y afianzadoras operen bajo el marco normativo mexicano; sufrió un ataque de ransomware, con el que los atacantes secuestraron la información de los equipos de la institución y al no recibir rescate por ella decidieron poner a subasta el acceso a cuentas de administración de red y 10GB de datos confidenciales de la institución.

Existieron más ataques cibernéticos a los largo de 2020 para diferentes instituciones mexicanas tanto públicas como privadas, sin embargo, con estos ejemplos ya es posible distinguir que los ataques cibernéticos, que ponen en riesgo los datos confidenciales de cientos de miles de personas; han ido en aumento no solo para las empresas privadas sino también para instituciones pública de toda índole, incluyendo una tan delicada como la salud.

3.2.2. Ciberseguridad y Estudiantes Mexicanos

a) En el trabajo “La seguridad en las competencias digitales de los millennials”, se realiza un estudio mixto en donde se utilizan cuestionarios en línea y entrevistas semiestructuradas dirigidos a universitarios de Oaxaca, para evaluar sus competencias en seguridad de la red. Entre los resultados más importantes destaca que, los encuestados llevan a cabo prácticas básicas de seguridad en su día a día (Castillejos et al., 2016).

b) Dentro del estudio “Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios”, se llevaron a cabo pruebas no paramétricas de Wilcoxon para encontrar las diferencias en las respuestas de los encuestados, antes y después de una capacitación en ciberseguridad; encontrando que el evento trajo resultados positivos y que se debería considerar una implementación permanente (Roque et al., 2018).

c) La investigación de método descriptivo de Arellano Martínez (2017), muestra los resultados de aplicar cuestionarios de preguntas cerradas con respecto a la cultura en seguridad informática dentro de redes sociales, a los alumnos de la Preparatoria 193 de San Diego Cuentla. Las respuestas fueron analizadas de manera estadística para obtener sus frecuencias. Detectándose que a los estudiantes les hace falta una mejor cultura en seguridad.

d) En el trabajo de investigación de Martínez López et al., (2018) se aplica una encuesta con preguntas cerradas de respuesta dicotómica, a una muestra no probabilística por conveniencia, que miden variables sobre si existe o no conocimiento en temas de ciberseguridad por parte de los alumnos de una preparatoria del estado de Oaxaca. Resultando que es necesario establecer un plan de estudios que incluya asignaturas relacionadas a la seguridad informática.

3.2.3. Expectativas Futuras Sobre la Ciberseguridad en México

a) En la nota "¿Qué esperar del mundo de la ciberseguridad en 2021?" de CIO México publicado en Enero de 2021, se muestran los retos de ciberseguridad que se esperan enfrentar para 2021 de acuerdo a los análisis de Check Point Software Technologies, compañía de ciberseguridad.

Para el entorno corporativo se espera el incremento no solo de ciberataques tradicionales, sino también la aparición de algunos nuevos como el "Vishing", o delincuentes que usan la ingeniería social para engañar a las víctimas y lograr accesos a sus credenciales más importantes como las bancarias.

Otro tipo de ataque cibernético que se encuentra a la alza y evolucionando es el ransomware. La última variante detectada es la denominada "doble extorsión" donde los delincuentes no solo cifran los equipos vulnerados sino que también extraen grandes cantidades de datos sensibles para amenazar a la víctima con publicarlas a no ser que se pague el rescate.

Por último, la implantación de la 5G, traerá consigo no solo un entorno de alta velocidad sino que abre las posibilidades para que se lancen ataques con el objetivo de bloquear las conexiones entre dispositivos.

Por estos motivos es que Check Point Software Technologies incita a posicionar la ciberseguridad como una necesidad de primer orden.

b) En el artículo “Ciber-resiliencia: la evolución de la ciberseguridad en 2020” de Juan Francisco Aguilar, publicado por Forbes México en Enero de 2021; es posible observar que el autor incita a los líderes negocios a conocer a priori el impacto que una amenaza cibernética puede traer, para definir cuál será la postura que tomarán con respecto a la ciberseguridad.

El escritor recomienda que las empresas deben pronunciarse por una visión integral que se acompañe de un pensamiento de ciber-resilencia, es decir, pensar cómo pueden responder, recuperarse, y aprender de cualquier circunstancia cibernética negativa que hayan enfrentado.

Por otra parte, el autor llama a las compañías a realizar un balance de la tecnología con las metodologías correctas, talento y personal con el que cuentan. A manera de lograr construir la seguridad desde la base de la organización y su infraestructura de tecnología.

Además, el escritor incita a las empresas a involucrar a los profesionales en ciberseguridad en el desarrollo de futuros productos, es decir, incorporarlos en el diseño del producto desde el principio y no hasta el final como se ha estado haciendo.

c) También, en otro artículo de CIO México llamado “Cinco tendencias en ciberseguridad empresarial para 2021”, escrito por Mireya Cortés y publicado en Diciembre de 2020; se menciona que la compañía de ciberseguridad Fluid Attacks, después de analizar el panorama en ciberseguridad para 2021, sugirió a la organizaciones tener en cuenta ciertas tendencias preventivas en ciberseguridad, como: cubrir todo el ciclo de vida del desarrollo de software con pruebas de seguridad continuas, crear equipos multidisciplinarios que colaboren en la ciberseguridad de la empresa, reevaluar la ciberseguridad con la que cuentan y determinar si es necesario agregar algún otro tipo de procesos de autenticación, y finalmente, abordar la ciberseguridad desde un enfoque preventivo.

3.3. Investigaciones Internacionales

Internacionalmente se han realizado estudios, reportes y artículos acerca de la situación actual de la ciberseguridad en las diferentes regiones del mundo, las expectativas a futuro que diferentes profesionales en al ámbito de la ciberseguridad tienen con respecto a ésta, así como el contraste de los contenidos de ciertos programas académicos referentes a la ciberseguridad con la opinión de expertos en materia y la descripción de puestos de trabajo que publican diversas compañías.

A continuación, se describen las ideas principales de estos escritos:

3.3.1. Situación de la Ciberseguridad en el Mundo

En el contexto internacional se pueden observar diversos artículos sobre la calificación de la ciberseguridad de diferentes países, uno de ellos es “Which countries have the worst (and best) cybersecurity?” de Paul Bischoff publicado en Marzo de 2021 por Comparitech, empresa británica dedicada a proveer información comparativa de diversas tecnologías para ayudar a los consumidores a tomar mejores decisiones.

De acuerdo a los resultados del análisis realizado por Comparitech, mostrados en el artículo; los países con mejor calificación son: Dinamarca, Suecia e Irlanda; mientras que los países con peor calificación son: Tayikistán, Bangladesh y China. Bajo este análisis, México se sitúa en la posición 37 de 75 países examinados.

Los criterios que el estudio tomó en cuenta para determinar la calificación son: la cantidad de infecciones de malware en diferentes dispositivos y sectores, el porcentaje de ataques cibernéticos a diferentes dispositivos y sectores, la capacidad de reacción ante ataques cibernéticos, e información de El Sector de Desarrollo de las Telecomunicaciones (ITU-D, por sus siglas en Inglés), que es responsable de crear políticas, regulaciones y proporcionar programas de capacitación y estrategias a los países en vías de desarrollo; entre otros para un total de quince categorías.

El puntaje total se logró promediando el puntaje de cada país en las quince categorías. Comparitech declara que sólo se incluyeron los países donde la información disponible les permitiera cubrir todos los puntos a considerar.

3.3.2. Situación de la Ciberseguridad en Europa

En esta sección se toma como referencia el artículo “Latent groups of cybersecurity preparedness in Europe: Sociodemographic factors and country-level contexts” de Claire Seungeun Lee y Ji Hye Kim publicado en Octubre de 2020 por ScienceDirect.

La investigación menciona que el grupo de los países mejor preparados en cuanto a ciberseguridad incluye a: Dinamarca, Luxemburgo, Suecia y Holanda.

Mientras que, los países menos preparados en términos de ciberseguridad son: Bulgaria, Chipre, Grecia, Hungría, Italia, Lituania, Malta, Polonia, Portugal, Rumania, Eslovaquia,

Para este estudio, la muestra se compuso por 27,868 personas de 30 países Europeos, tales como: Austria, Bélgica, Bulgaria, Croacia, Chipre, República Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania (Este y Oeste), Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal , Rumania, Eslovaquia, Eslovenia, España, Suecia y el Reino Unido (Gran Bretaña e Irlanda del Norte).

La variable dependiente establecida para esta investigación fue: la preparación en ciberseguridad, que indica si el encuestado está preocupado por alguno de los once elementos en la cuesta realizada. Para describir las características de los grupos identificados, se crearon cuatro factores (comportamiento de compra en línea, configuración de seguridad del usuario, configuración del software y confianza en la Web) para medir la conciencia sobre la ciberseguridad, utilizando una escala de Likert de cinco puntos, luego se realizó un análisis factorial confirmatorio para probar la confiabilidad del agrupamiento.

Mientras que, las variables independientes establecidas para esta investigación fueron las variables sociodemográficas más importantes, como: género, edad, clase social, tamaño de la comunidad, Gross Domestic Product (GDP), y GCI obtenido de la Unión Internacional de Telecomunicaciones (ITU). A cada una de estas variables se les asignó un valor numérico.

3.3.3. Situación de la Ciberseguridad en América Latina y el Caribe

Para este apartado se ha utilizado el Reporte 2020 sobre "Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y El Caribe" elaborado por el Banco Interamericano de Desarrollo y publicado por la misma institución en 2020.

El estudio menciona que Uruguay fue el país calificado con la madurez más alta, de la región Cono Sur, en cuatro de las cinco dimensiones calificadas.

Colombia fue el país con mayor desarrollo en seguridad cibernética en el Grupo Andino, particularmente en las dimensiones "Política y estrategia" y "Cultura y sociedad".

México presenta la mejor posición de la región Centroamérica, con un nivel de madurez de entre 2 y 3 en casi todas las dimensiones.

En la región del Caribe, Trinidad y Tobago y Jamaica son los países con mayor desarrollo en seguridad cibernética ya que tienen una estrategia nacional de seguridad cibernética, a saber: Trinidad y Tobago y Jamaica.

El estudio se llevó a cabo evaluando treinta y dos países, tales como: Antigua y Barbuda, Argentina, Bahamas, Barbados, Belice, Bolivia, Brasil, Chile, Colombia, Costa Rica, Dominica, Ecuador, El Salvador, Granada, Guatemala, Guyana, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, San Cristóbal

y Nieves, San Vicente y las Granadinas, Santa Lucía, Surinam, Trinidad y Tobago, Uruguay, y Venezuela.

Se calificaron cinco dimensiones diferentes, consistentes en: Política y Estrategia de Ciberseguridad (Diseño de estrategia y resiliencia de ciberseguridad), Cultura Cibernética y Sociedad (Fomentar una cultura de ciberseguridad responsable en la sociedad), Educación, Capacitación y Habilidades en Ciberseguridad (Desarrollo del conocimiento de ciberseguridad); Marcos Legales y Regulatorios (Creación de marcos legales y regulatorios efectivos), Estándares, Organizaciones y Tecnologías (Control de riesgos a través de estándares, organizaciones y tecnologías).

Los datos de estas dimensiones se obtuvieron mediante el uso de un instrumento en línea que se hizo llegar a todos los Estados Miembros de la OEA.

Una vez recopilados los datos, se hizo una referencia cruzada con la investigación documental y la consulta con Estados Miembros para la validación de los resultados declarados.

Después de analizar los datos se realiza la asignación de alguna de las etapas establecidas. Estas etapas son: Inicial (falta evidencia observable de la capacidad de seguridad cibernética), Formativa (existe evidencia pero los aspectos están mal definidos), Consolidada (los indicadores están instalados y funcionando), Estratégica (se han tomado decisiones sobre qué indicadores de este aspecto son importantes y cuáles son menos para la organización o el Estado en particular), Dinámica (rápida toma de decisiones, reasignación de recursos, atención constante al entorno cambiante)

3.3.4. Expectativas Futuras sobre la Ciberseguridad en el Mundo

En el artículo “Diez años más tarde. Retos y amenazas a la seguridad y ciberseguridad en 2030.” de Gallardo, publicado por la revista Sistemas en 2020; entre otras cosas se presenta una entrevista realizada a diversos especialistas en ciberseguridad, entre ellos Juan Camilo Reyes Fierro, Líder Comercial de Servicios de Seguridad, Sudamérica Española, en IBM.

Juan Camilo Reyes Fierro menciona que desde su experiencia ha descubierto que dentro de las empresas, la definición de los conceptos básicos aún no se elabora de manera correcta, ya que no cuentan con una estrategia clara de ciberseguridad.

También, comenta que las compañías suelen adquirir tecnología sin saber exactamente la función que cumplirán dentro de la empresa, como lo muestran los datos relacionados con la inversión en seguridad.

De acuerdo con sus palabras, a cómo él observa la situación actual, piensa que la mayoría de las compañías siguen atacando los problemas de hace una década que aún no resuelven y pronostica que continuarán así al menos otros 10 años. Además, comenta que algunas organizaciones siguen considerando que la ciberseguridad es simplemente un costo por lo que su transformación digital estará muy propensa a los ciberataques; y se avanzará únicamente en temas que signifiquen un riesgo pecuniario tangible.

Por otra parte, en cuanto al factor humano, Reyes Fierro comenta que de acuerdo con su experiencia, pronostica que para 2030 la mayor relevancia a nivel directivo la tendrá el responsable de tecnología.

3.3.5. Oferta y Demanda de Habilidades en Ciberseguridad

a) En el trabajo de Kulal et al. (2022) se realiza un análisis comparativo de los planes de estudio en ciberseguridad a nivel maestría de 10 universidades de USA, y de las descripciones de puestos en ciberseguridad de 30 compañías estadounidenses. Encontrando que, se deben incluir asignaturas sobre servicios en la nube, Splunk, Linux, Python, Java y evaluaciones de seguridad; para que los egresados puedan ser considerados por las empresas.

b) En el trabajo de investigación cualitativa de Kreider et al. (2019) se llevan a cabo grupos de discusión con académicos y secretarios de educación para elaborar un marco que sirva de guía a las universidades, para realizar análisis donde detecten las brechas que necesitan cerrar con respecto a sus planes de ciberseguridad. Resultando en un marco que considera tres dimensiones principales: oferta de programas, capacidad del programa y flujo de estudiantes.

c) La investigación de Caelli et al. (2018), presenta un análisis comparativo de los programas de estudio, tanto a nivel licenciatura como maestría, enfocados en la ciberseguridad, de 40 universidades australianas. Como resultados se obtuvo que es necesario incluir asignaturas referentes a la seguridad de los servicios en la nube y la virtualización; así como clases que hablen de los acuerdos legales/regulatorios nacionales e internacionales.

Con lo descrito en los incisos previos es posible visualizar que la ciberseguridad es un tema de relevancia a nivel global y que la mayoría de los distintos países están realizando estudios sobre el tema. Aunque en México es necesario realizar más y mejores investigaciones.

4. MARCO TEÓRICO

4.1. Inclusión

La inclusión es comúnmente un concepto tratado en el ámbito social, pero sobre todo en el sector pedagógico, por lo que la mayoría de las descripciones referentes a esta noción se hacen con foco en la educación. Sin embargo, es posible adaptar estas ideas y crear descripciones que refieran a la ciberseguridad.

La ONG Plena inclusión España (2021) ofrece ejemplos para lograr diferenciar entre la inclusión y la integración (concepto que suele confundirse con la inclusión) social. Extrapolando estos ejemplos al tema de la ciberseguridad, se han elaborado las definiciones siguientes:

Integración: considerar el tópico de la ciberseguridad dentro de un programa académico pero con un solo foco específico (por ejemplo, la red), sin contemplar la interacción de esta con el contexto completo (por ejemplo, las bases de datos, las aplicaciones, etc…).

Inclusión: considerar el tópico de la ciberseguridad dentro un programa académico contemplando su interacción dentro del contexto general (en todas las asignaturas en las que intervenga la enseñanza de alguna tecnología o marco regulatorio).

De acuerdo a las definiciones anteriores, y con base en el crecimiento acelerado que tiene la tecnología, la masiva utilización de ésta en la mayoría de las actividades humanas y mercantiles, así como el aumento año con año de los ciberdelitos y los ciberataques; es

importante que la ciberseguridad pase del estatus “integrada” a “incluida” dentro de los programas académicos de las universidades y de los planes estratégicos de las organizaciones.

4.2. Ciberseguridad

Para el Banco de Pagos Internacionales [Bank for International Settlements] (2014):

La ciberseguridad se refiere a estrategias, políticas y estándares que abarcan la gama completa de reducción de amenazas, reducción de vulnerabilidades, disuasión, compromiso internacional, respuesta a incidentes, resiliencia, así como actividades y políticas de recuperación con respecto a la seguridad de una infraestructura.

En palabras de Urcuqui et al. (2018, p. 21), “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.”

De acuerdo con Arroyo et al. (2020, p.12):

> “podemos definir la ciberseguridad como el conjunto de técnicas, procedimientos y protocolos encaminados a la protección de la información vinculada a los usuarios de las cibertecnologías. Esta protección demanda la custodia no solo de la información en sí, sino también de todos los elementos precisos para su correcta gestión. Es decir, la ciberseguridad tiene como objetivo proteger todo tipo de activo o recurso de valor para una persona, empresa u organización.”

Con base en los argumentos previamente expuestos se entiende que la ciberseguridad es una rama compleja de las ciencias de la computación que no solo abarca el aspecto técnico para la implementación de medidas de protección a los activos tecnológicos de las organizaciones, sino que también incluye un acercamiento multidisciplinario para lograr el

objetivo de salvaguardar el patrimonio ciberfísico de las organizaciones, mediante el desarrollo e implementación de estrategias, estándares, y políticas que lo regulen.

4.2.1. Ciberseguridad en México

En México la ciberseguridad aún no cobra la relevancia que debería, por lo tanto no se toma con seriedad y muchas veces queda excluida o vagamente explicada dentro de diversos documentos oficiales, como de los planes de desarrollo del país.

Ejemplo de esto es que, de acuerdo con Arreola (2018), en el Plan Nacional de Desarrollo [PND] 2013-2018, donde se planteaba fortalecer las capacidades institucionales y de inteligencia del Estado Mexicano, referentes al ciberespacio, para prevenir y mitigar los riesgos y amenazas a la seguridad nacional; no quedó del todo precisado en el Programa de Seguridad Nacional. Además, en el PND 2013-2018 se utilizan los términos de ciberseguridad y seguridad de la información como sinónimos, algo que no es correcto, por lo que se crea confusión y vuelve poco clara o nula, la definición que en el PND se debe entender como ciberseguridad.

Otro ejemplo es el Plan Nacional de Desarrollo [PND] 2019-2024, donde no se hace referencia al ciberespacio, ni a la ciberseguridad o la seguridad informática. Por tanto, aunque se menciona la pretensión de mejorar las capacidades tecnológicas de investigación científica en los ámbitos de seguridad pública y seguridad interior, no se define si el ciberespacio está incluido en esto. Y se carece de una definición de estos términos.

Así mismo, otro documento del gobierno de México que carece tanto de una definición como de la inclusión de la ciberseguridad, es la recientemente publicada Estrategia

Digital Nacional 2021-2024. En este documento se menciona que la estrategia está enfocada tanto en potencializar el acceso a las TIC como promover su uso intensivo y responsable, orientándolas al bienestar social de los mexicanos; sin embargo, no habla sobre el ciberespacio o la ciberseguridad, aunque se mencionan algunos puntos con respecto a la seguridad de la información, como se había mencionado antes, no son sinónimos.

4.2.2. Componentes de la Ciberseguridad

Si bien no existe un consenso ampliamente aceptado sobre los temas específicos que la ciberseguridad debería abarcar, en diferentes estudios y en las ofertas educativas (de España, por ejemplo) es posible observar una mención reiterada de algunos tópicos. Como se muestra en la tabla 1.

En la tabla 1 se presenta de manera organizada aquellos temas encontrados de forma frecuente en 20 diferentes planes educativos de las instituciones que de acuerdo con el informe “Formación reglada en ciberseguridad en España, edición 2021” del Instituto Nacional de Ciberseguridad [INCIBE], ofrecen maestrías referentes a la ciberseguridad. Por otra parte, es importante mencionar que se ha tomado a España como país de referencia ya que éste es la cuarta potencia mundial en ciberseguridad (Departamento de Seguridad Nacional [DNS], 2021) y son hispanohablantes, lo que permite una comparativa más apropiada con respecto a México.

Tabla 1. *Temas de Ciberseguridad Más Frecuentes en Diferentes Planes Educativos.*

Tema	Frecuencia Absoluta	Tema	Frecuencia Absoluta
Desarrollo Seguro (software, web, aplicaciones)	12	Crimen digital	1
Seguridad en Redes	12	Defensa nacional y ciberterrorismo	1
Criptografía	9	Diseño, desarrollo e implantación de soluciones de ciberseguridad	1
Hacking Ético	9	El CISO y el RSI	1
Gobernanza/Legislación/Normativa/Estándares de la Ciberseguridad	8	Entornos ubicuos (SCADA, móviles) e Infraestructuras Críticas	1
Protección/Seguridad de la Información/Datos	8	Entornos Ubicuos: SCADA y Móviles	1
Amenazas, Malware, Código Malicioso	6	Formación CISA	1
Análisis Forense	5	Gestión de identidades y accesos	1
Auditoría	5	Gestión de las Cibercrisis	1
Análisis y/o Gestión de Riesgos	4	Gestión de servicios en el sistema informático	1
Arquitectura de Seguridad	4	Gestión y legislación en ciberseguridad	1
Ciberinteligencia	4	Hardening de sistemas	1
Gestión de Incidentes	4	Herramientas de ciberseguridad OSINT	1
Pentesting	4	Implantación de la ciberseguridad en sistemas de control industrial ICS/SCADA	1
Seguridad de las TIC	4	Inteligencia de Negocio / Business Intelligence	1
Ciencia de Datos/Data Mining	3	Mecanismos de protección y defensa	1
Respuesta a Incidentes	3	Modelos y Framework	1
Seguridad IoT e Industria	3	Monitorización de Acontecimientos de Seguridad	1
Vulnerabilidades	3	Organizaciones nacionales e internacionales	1
Ingeniería Inversa	2	Privacidad y anonimato	1
Peritaje Informático	2	Seguridad en aplicaciones y bases de datos	1
Sistemas de Gestión de la Seguridad	2	Seguridad en los sistemas operativos	1
Tendencias en Ciberseguridad	2	Seguridad perimetral	1
Administración electrónica	1	Seguridad web	1
Automatización y Orquestación de Seguridad (SOAR)	1	Tácticas de ataque del Equipo Rojo	1
Bases Tecnológicas	1	Técnicas de ciberseguridad	1
Blockchain y Autenticación	1	Tecnologías SIEM	1
Cloud Security y Edge Computing	1	Zero trust	1

Fuente. Elaboración propia con referencias obtenidas de INCIBE, 2021.

Todos estos temas podrían englobarse en cuatro diferentes categorías, como se propone a continuación:

Seguridad de Red.

"La seguridad de red es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos" (Cisco Systems, s.f, párr. 1). Para ello hace uso de diversas tecnologías tanto de software como de hardware, que permitan una mayor protección a las diferentes amenazas que pudieran propagarse por la red (Cisco Systems, s.f).

Seguridad de Software.

Son las actividades encaminadas a garantizar que el software desarrollado por parte de la compañía y/o aquel software adquirido a terceros por encargo, cumplan con las pautas de seguridad establecidas (ISC, s.f.)

Evaluación de la Seguridad.

Son todas aquellas pruebas internas, externas, y de terceros que permiten conocer el grado de seguridad que poseen los sistemas y las comunicaciones de la corporación; así como detectar posibles vulnerabilidades.

Cómputo Forense.

Es una rama de las ciencias forenses que se encarga de la búsqueda, preservación y presentación de evidencias digitales, logrando que éstas cobren valor probatorio en los procesos judiciales (López et al., 2002; Cano, 2008).

Estándares y Buenas Prácticas.

Los estándares de ciberseguridad cumplen un papel de guía para que las organizaciones puedan implementar procedimientos con base en modelos, normas y lineamientos que han sido creados a partir de la experiencia de los grupos que ayudaron a su definición. El seguimiento de estos estándares permite que las organizaciones que los adoptan establezcan políticas y procedimientos de seguridad de la información y de activos de TI, aumentando la seguridad de la organización en todos los niveles y ofreciendo con esto un mayor grado de confianza tanto interna como externa (Borbón, 2011).

5. HIPÓTESIS

5.1. Hipótesis de Investigación

Existe una gran diferencia entre los conocimientos sobre ciberseguridad requeridos por las empresas y los conocimientos que tienen los egresados de carreras altamente relacionadas con la ciberseguridad.

5.2. Hipótesis Nula

Existe una diferencia mínima entre los conocimientos sobre ciberseguridad requeridos por las empresas y los conocimientos que tienen los egresados de carreras altamente relacionadas con la ciberseguridad.

6. PREGUNTAS DE INVESTIGACIÓN

1.- ¿Qué tanta importancia se le da al tema de la ciberseguridad, con respecto a inversiones monetarias y nivel de conocimientos por parte de los empleados o aspirantes, dentro de las empresas?

2.- ¿Cuáles son las diferencias destacables, sobre el tema de ciberseguridad, entre los requerimientos de las empresas y los conocimientos que poseen los egresados de carreras altamente relacionadas con la ciberseguridad?

7. OBJETIVOS

7.1. Objetivo General

Informar cuáles son las áreas de oportunidad tanto de planes estratégicos como educativos con respecto a temas de ciberseguridad, mediante el análisis y evaluación de los conocimientos del grupo muestra y los requerimientos que la industria establece, para ayudar a crear planes adecuados que permitan y promuevan la inclusión de la ciberseguridad. Actuando a su vez como apoyo para futuras investigaciones relacionadas con la ciberseguridad, los negocios y la educación.

7.2. Objetivos Específicos

1.- Investigar y recopilar información de diferentes medios relevantes para el tema de ciberseguridad, por medio de una búsqueda sistemática, para verificar la existencia de apoyos literarios que puedan ser utilizados en la creación del instrumento de recolección de datos, así como para el análisis de los mismos.

2.- Elaborar y validar el instrumento de recolección de datos que se utilizará, mediante el análisis de la literatura proveniente de la búsqueda sistemática y la experiencia del investigador, para realizar las encuestas necesarias.

3.- Encuestar al grupo que conforma la muestra, utilizando como instrumento un cuestionario diseñado ad-hoc al presente estudio, para obtener la información a utilizar en el análisis.

4.- Analizar los datos recabados, comparando y contrastando la información obtenida por medio de la encuesta, para elaborar gráficas y tablas que permitan ilustrar el tema de manera simple y organizada.

5.- Informar a la comunidad los datos relevantes de la investigación, por medio de la publicación de un artículo, para contribuir en la generación de debates sobre el tema que aumenten su relevancia.

8. MÉTODO

8.1. Enfoque de Investigación

En esta investigación se hará uso del enfoque mixto de investigación debido a que se requiere entender el fenómeno de manera completa.

Es importante mencionar que la ciberseguridad es un área de estudio interdisciplinaria muy amplia, que abarca desde aspectos tecnológicos, como el desarrollo de nuevas tecnologías que puedan ser utilizadas para proteger los activos; legales, donde se define que puede hacerse y que no; psicológicos, como entender el comportamiento humano en el ciberespacio; y hasta sociológicos, que permiten entender como la sociedad influye en las acciones de las personas en el ciberespacio (Fujs et al, 2019).

Además, las ciencias de la computación [de las que forma parte la ciberseguridad] son ciencias relativamente nuevas, lo que ha llevado a los investigadores de la informática a adaptar los métodos y metodologías de investigación que han sido utilizadas por largo tiempo en ciencias consolidadas, siendo los métodos mixtos unos de los más comúnmente utilizados entre los investigadores. De hecho, los métodos de investigación mixtos son la mejor opción para investigaciones dirigidas a la informática, cuando en la investigación interfieren factores de alguna otra ciencia (Hassani, 2017), como ocurre con la ciberseguridad.

Igualmente, en otros trabajos se menciona que lo más recomendable es utilizar un enfoque mixto de investigación cuando es necesario indagar en factores y fases clave dentro de áreas como: economía, negocios, gestión estratégica y tecnología. Por ejemplo, para identificar, entender y analizar los factores y fases clave en un área de investigación relativamente nueva que combine elementos de otras áreas, se puede utilizar un enfoque

cualitativo. Luego, para expresar la importancia de cada factor y priorizar aquellos que sean clave, un enfoque cuantitativo de investigación sería útil (Basias y Pollais, 2018).

Por estos motivos y como se ha expresado con anterioridad, este estudio hace uso del enfoque mixto de investigación.

8.2. Tipo de Investigación

De acuerdo al nivel de profundización que se le dará a este estudio, se comenzará con un alcance de tipo exploratorio, terminando en uno descriptivo. Esto debido a que "los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes" (Hernández et al., 2014, p.91), como ocurre con el tema de la inclusión de la ciberseguridad en México. Además, el estudio exploratorio tiene como finalidad proporcionar un plano general de una realidad o alguno de sus aspectos (Niño, 2011), que es parte de lo que busca lograr el presente trabajo con respecto a la ciberseguridad en México, para establecer las bases iniciales que sustentan la importancia del desarrollo del tema y el análisis consecuente.

Por otra parte, el alcance descriptivo servirá para explicar los aspectos, las clases, las categorías y las relaciones que se establecen entre los objetos de estudio, con la intención de ilustrar con palabras la realidad, confirmar un postulado o comprobar una hipótesis (Niño, 2011), como las hipótesis y preguntas de investigación que se plantean en este estudio con respecto a la inclusión de la ciberseguridad en la actualidad, que al darles respuesta permitirán generar una descripción de la realidad de este tema que va ganando importancia con el progreso tecnológico acelerado de los últimos años.

Este estudio pretende obtener un panorama actual sobre la disparidad que podría existir entre el nivel de conocimientos y los tipos de temas referentes a la ciberseguridad que requieren las empresas y con los que cuentan los egresados de carreras afines. Para cumplir este propósito se ha seleccionado un diseño de investigación no experimental, transversal, inicialmente exploratorio y posteriormente descriptivo.

La propiedad "no experimental" fue elegida debido a que la variable independiente principal no se alterará de ninguna manera intencional para ver su impacto sobre ninguna otra, sino que se observará la situación tal cual se encuentra en las organizaciones sujetos que forman parte de las muestras a analizar (Hernández et al, 2014).

Es decir, se encuestará a las personas correspondientes de la muestra seleccionada para conocer el nivel de importancia que le ha otorgado la empresa a la ciberseguridad, adicionalmente, se cuestionará sobre el tipo y nivel de conocimientos que esperan que posean sus colaboradores o aspirantes. Como puede observarse en esta breve descripción, ambas situaciones, tanto el grado de importancia como los conocimientos que se tienen, se han establecido anteriormente e independientemente a la encuesta, sin intervención alguna por parte del investigador.

Ya que el estudio se realizará con datos recabados en una sola exhibición, que reflejen la realidad del año corriente en que se realice la recolección de datos con los instrumentos establecidos; se optó por el tipo transversal.

Esto significa que, el propósito del diseño transversal es detallar las variables para poder analizar su interrelación, esto mediante la recolección de datos en punto específico y

aislado en el tiempo; actuando como si fuera una pintura del suceso en cuestión (Hernández et al, 2014), que posibilite no solo la observación y el análisis en esa ocasión específica, sino que sirva como registro de lo acontecido para ser utilizado como referencia o base de análisis futuros exhaustivos o con enfoques diferentes pero relevantes para el tema principal de esta investigación.

8.3. Población

8.3.1. Egresados

Egresados de carreras altamente relacionadas con la ciberseguridad quienes hayan finalizado sus estudios entre 2015 y 2020, en cualquier institución educativa dentro de territorio nacional.

8.3.2. Empresas

Cualquier empresa dentro de territorio nacional que cuente con una unidad de negocio dedicada a administrar los sistemas y/o las tecnologías de la información y la comunicación.

8.4. Muestra

Las especificaciones de las características necesarias para que un sujeto sea parte del análisis, que se describen en las siguientes secciones, atienden a la decisión de establecer muestras no probabilísticas por conveniencia.

Siendo las muestras no probabilísticas por conveniencia aquellas que permiten seleccionar los casos o sujetos disponibles a los que el investigador tiene fácil acceso ya sea por proximidad o algún otro factor (Hernández et al., 2014; Otzen et al., 2017).

8.4.1. Egresados

Egresados de la carrera en Ingeniería en Sistemas Computacionales que hayan finalizado con el total de la carga académica entre 2015 y 2020 en el plantel “A” o “B”, que cuenten con un mínimo de 1 año de experiencia desempeñando actividades altamente relacionadas con las TIC y que hayan laborado en una misma empresa durante todo el año 2021.

En total, 32 egresados con estas características respondieron la encuesta.

8.4.2. Empresas

Empresas ubicadas en el norte y bajío del país que cuenten con una unidad de negocio dedicada a administrar los sistemas y/o las tecnologías de la información y la comunicación, en donde exista al menos una persona que haya laborado en ésta durante todo el año 2021 y con un cargo que le permita conocer los requerimientos de conocimientos con los que deben cumplir los empleados o postulantes así como las cantidades monetarias que se destinan a rubros como la ciberseguridad, la compra de software y hardware.

En total se obtuvo la respuesta de 15 personas que laboran para 15 compañías diferentes.

8.5. Variables, Dimensiones, e Indicadores del Estudio

Para dar respuesta a la hipótesis y preguntas de investigación del presente estudio, se ha delimitado una variable independiente principal y a la vez se han determinado una cantidad específica de dimensiones e indicadores a evaluar; descritos en la tabla 2.

Es necesario especificar que si bien la variable independiente principal fue definida de tal manera que pueda otorgar datos tanto de los egresados como de las empresas; en el

caso de los egresados se hace uso de cada uno de los indicadores, dado que se evalúa el nivel de conocimientos que poseen empleando los ítems que integran los indicadores, mientras que, para las empresas se hizo uso únicamente de las dimensiones ya que éstas abarcan de manera general los temas que cada uno de los indicadores sugieren.

Tabla 2.

Variables, Dimensiones e Indicadores.

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES
INDEPENDIENTE Nivel de Conocimiento en Ciberseguridad	Profundidad del conocimiento con respecto a los aspectos que comprenden la ciberseguridad con el que cuenta el egresado, o que la empresa espera que tengan sus empleados y/o aspirantes.	Seguridad de Red	Principales Ataques y Cómo Funcionan
			Protocolos Seguros de Comunicación
			Red Privada Virtual
			Control de Acceso a la Red
		Seguridad de Software	Validación de Entrada
			Control de Roles y Privilegios
			Análisis de Vulnerabilidades
			Implementación de Parches
		Evaluación de la Seguridad	Análisis de Riesgos
			Pentesting
			Hacking Ético
			Gestión de Incidentes
		Cómputo forense	Cómo Ejecutar un Análisis Forense
			Software para Cómputo Forense
		Estándares, Buenas Prácticas	Estándares Relacionados a la Seguridad de la Información

Fuente. Elaboración propia.

8.6. Operacionalización de Variables, Dimensiones, e Indicadores del Estudio

8.6.1. Variables

La tabla 3 contiene la variable independiente del experimento, donde se detalla su ecuación, implicaciones, objetivo, y las dimensiones que intervienen en ella.

Tabla 3.

Variable Independiente

Variable	Nivel de Conocimiento en Ciberseguridad (NCC)
Ecuación	NCC = (SR*0.30) + (SS*0.10) + (ES*0.30) + (CF*0.20) + (EBP*0.10)
Implicaciones	Es la sumatoria de los resultados obtenidos en cada una de las dimensiones de la variable. Sus umbrales son de: 0<NCC ≤100
Meta	Obtener el nivel de conocimiento en ciberseguridad que posee el egresado. Para lograrlo se han establecido diferentes "pesos" a las distintas dimensiones, de acuerdo a su relevancia.
Dimensiones que intervienen	Seguridad de Red (SR) Seguridad de Software (SS) Evaluación de la Seguridad (ES) Cómputo Forense (CF) Estándares y Buenas Prácticas (EBP)

Fuente. Elaboración propia.

8.6.2. Dimensiones

Las tablas de la 4 al 8 contienen las dimensiones utilizadas dentro de la variable independiente principal, donde se detalla su ecuación, implicaciones, objetivo, y los indicadores que intervienen en cada una de ellas.

Tabla 4.

Dimensión Seguridad de Red

Dimensión	Seguridad de Red (SR)
Ecuación	SR = (PACF*0.25) + (PSC*0.25) + (RPV*0.25) + (CAR*0.25)
Implicaciones	Es la sumatoria de los resultados obtenidos en cada una de los indicadores de la dimensión. Sus umbrales son de: 0<SR ≤100
Meta	Obtener el nivel de conocimiento para la dimensión de seguridad de red.
Indicadores que intervienen	Principales Ataques y Cómo Funcionan (PACF) Protocolos Seguros de Comunicación (PSC) Red Privada Virtual (RPV) Control de Acceso a la Red (CAR)

Fuente. Elaboración propia.

Tabla 5.

Dimensión Seguridad de Software

Dimensión	Seguridad de Software (SS)
Ecuación	SS = (VE*0.25) + (CRP*0.25) + (AV*0.25) + (IP*0.25)
Implicaciones	Es la sumatoria de los resultados obtenidos en cada una de los indicadores de la dimensión. Sus umbrales son de: 0<SS ≤100
Meta	Obtener el nivel de conocimiento para la dimensión de seguridad de software.
Indicadores que intervienen	Validación de Entrada (VE) Control de Roles y Privilegios (CRP) Análisis de Vulnerabilidades (AV) Implementación de Parches (IP)

Fuente. Elaboración propia.

Tabla 6.

Dimensión Evaluación de la Seguridad

Dimensión	Evaluación de la Seguridad (ES)
Ecuación	ES = (AR*0.25) + (Pe*0.25) + (HE*0.25) + (GI*0.25)
Implicaciones	Es la sumatoria de los resultados obtenidos en cada una de los indicadores de la dimensión. Sus umbrales son de: 0<ES ≤100
Meta	Obtener el nivel de conocimiento para la dimensión de evaluación de la seguridad.
Indicadores que intervienen	Análisis de Riesgos (AR) Pentesting (Pe) Hacking Ético (HE) Gestión de Incidentes (GI)

Fuente. Elaboración propia.

Tabla 7.

Dimensión Cómputo Forense

Dimensión	Cómputo Forense (CF)
Ecuación	CF = (EAF*0.50) + (SCF*0.50)
Implicaciones	Es la sumatoria de los resultados obtenidos en cada una de los indicadores de la dimensión. Sus umbrales son de: 0<CF ≤100
Meta	Obtener el nivel de conocimiento para la dimensión de cómputo forense.
Indicadores que intervienen	Cómo Ejecutar un Análisis Forense (EAF) Software para Cómputo Forense (SCF)

Fuente. Elaboración propia.

Tabla 8.

Dimensión Estándares y Buenas Prácticas

Dimensión	Estándares y Buenas Prácticas (EBP)
Ecuación	EBP = ESI
Implicaciones	Es la sumatoria de los resultados obtenidos en cada una de los indicadores de la dimensión. Sus umbrales son de: 0<EBP ≤100
Meta	Obtener el nivel de conocimiento para la dimensión de estándares y buenas prácticas.
Indicadores que intervienen	Estándares Relacionados a la Seguridad de la Información (ESI)

Fuente. Elaboración propia.

8.6.3. Indicadores

Los indicadores definidos están constituidos por diferentes ítems que ayudan a obtener una calificación cuantitativa de los indicadores, que a su vez ayudan a calificar las dimensiones descritas en las secciones anteriores.

Cada uno de los indicadores tiene un ítem establecido con el cual es calificado, la tabla 9 muestra los ítems que cada uno de los indicadores contiene y a qué dimensión pertenece cada uno.

Tabla 9.

Indicadores e Ítems

Dimensión	Indicador	Ítem
Seguridad de Red	Principales Ataques y Cómo Funcionan	Ítem #1
	Protocolos Seguros de Comunicación	Ítem #2
	Red Privada Virtual	Ítem #3
	Control de Acceso a la Red	Ítem #4
Seguridad de Software	Validación de Entrada	Ítem #5
	Control de Roles y Privilegios	Ítem #6
	Análisis de Vulnerabilidades	Ítem #7
	Implementación de Parches	Ítem #8
Evaluación de la Seguridad	Análisis de Riesgos	Ítem #9
	Pentesting	Ítem #10
	Hacking Ético	Ítem #11
	Gestión de Incidentes	Ítem #12
Cómputo Forense	Cómo Ejecutar un Análisis Forense	Ítem #13
	Software para Cómputo Forense	Ítem #14
Estándares y Buenas Prácticas	Estándares Relacionados a la Seguridad de la Información	Ítem #15

Fuente. Elaboración propia.

8.7. Técnicas e Instrumentos

Como instrumento para la recolección de datos se utilizará la encuesta ya que permite obtener información de un grupo socialmente significativo de personas relacionadas con el problema de estudio; posteriormente mediante un análisis cuantitativo o cualitativo, generar las conclusiones que correspondan a los datos recogidos. También puede ser utilizada para entregar descripciones de los objetos de estudio, detectar patrones y relaciones entre las características descritas y establecer relaciones entre eventos específicos.

Al usarse como instrumento dentro de una investigación, las encuestas: 1) permiten identificar variables y relaciones, que surgen de la visión exploratoria que aporta este instrumento, así como sugerir hipótesis y actuar como guía de otras fases de la investigación; 2) posibilitan obtener información valiosa para la comprobación de hipótesis y la respuesta

a preguntas de investigación, esto dado que los cuestionamientos diseñados específicamente para poder medir las variables de investigación se incluyen en este instrumento principal; y 3) complementan otro tipo de instrumentos y métodos ya que facilitan el seguimiento a resultados no esperados, y es posible ahondar en los motivos detrás de las respuestas de los encuestados (Kerlinger, 1983, como se citó en La Red, 2017).

Cabe mencionar que las encuestas fueron realizadas bajo la modalidad “en línea”, por lo que los encuestados tuvieron la oportunidad de elegir el mejor momento y las mejores condiciones para responder el cuestionario que se les hizo llegar mediante un enlace enviado por correo electrónico.

Por otra parte, las encuestas fueron diseñadas de tal manera que las respuestas, en mayoría, obedezcan a la escala de Likert y algunas otras de forma dicotómica.

La escala de Likert se ha seleccionado ya que este tipo de escalas permite convertir hechos cualitativos, como las cualidades internas de un individuo como sus conocimientos y habilidades, en cuantitativos, para llevar a cabo su medición (Hechavarría, 2015). Los tipos de escalas Likert que se han empleado dentro del cuestionario son primordialmente aquellas denominadas como ordinales, ya que estas permiten a los individuos ser clasificados de acuerdo al grado en que disponen de un atributo determinado (Ospina et al., 2005). Mientras que, aquellas en forma dicotómica fueran configuradas de esta manera debido a que es necesario conocer si la respuesta dada es correcta e incorrecta para poder evaluar el nivel de conocimientos.

8.7.1. Encuesta Egresados

La encuesta aplicada a los egresados que formaron parte de la muestra, está conformada por 6 diferentes secciones, con un propósito diferente cada una e integradas de una cantidad diferente de ítems. La tabla 10 muestra la información referente al propósito de cada una de las secciones, la cantidad de ítems que las componen y el tipo de escala utilizada.

Tabla 10.

Secciones de la Encuesta para Egresados

Nombre de Sección	Propósito de la Sección	Cantidad de Ítems	Tipo de Escala
Información Básica	Conocer datos generales del egresado que permitan establecer el tipo de industria al que pertenece la empresa donde labora, así como sus años de experiencia dentro del ámbito informático, su nivel de preparación académica y su generación.	9 ítems	
Estudios	Conocer si los egresados consideran que la ciberseguridad formó parte de sus estudios durante la licenciatura y si piensan que sus profesores estaban lo suficientemente capacitados para impartir esa materia.	4 ítems	Likert de 5 puntos, Ordinal, Actitud cognitiva
Capacitaciones	Saber si los egresados han asistido a capacitaciones sobre seguridad durante su desarrollo académico o durante su vida laboral.	4 ítems	Likert de 5 puntos, Razón
Conocimientos A (Percepción)	Medir la percepción que tienen los egresados sobre el nivel de conocimientos que tienen en cada una de las dimensiones estipuladas para el estudio.	14 ítems	Likert de 5 puntos, Ordinal, Conocimiento
Conocimientos B (Examen)	Medir de manera cualitativa, mediante un examen, el nivel de conocimientos que tienen los egresados sobre las dimensiones estipuladas para el estudio.	15 ítems	Categórica dicotómica
Participación	Saber en qué medida los egresados participan de manera activa en las decisiones referentes a la ciberseguridad dentro de las empresas en las que laboran.	6 ítems	Likert de 5 puntos, Ordinal, Frecuencia de realización

Fuente. Elaboración Propia.

8.7.2. Encuesta Empresas

En la encuesta aplicada a las empresas que formaron parte de la muestra, se establecieron 5 diferentes secciones, con un propósito diferente cada una y conformadas por una cantidad

diferente de ítems. La tabla 11 muestra la información referente al propósito de cada una de estas secciones, la cantidad de ítems que las componen y el tipo de escala utilizada.

Tabla 11.

Secciones de la Encuesta para Empresas

Nombre de Sección	Propósito de la Sección	Cantidad de Ítems	Tipo de Escala
Información Básica	Conocer datos generales de la empresa que permitan establecer el tipo de industria al que pertenece, el cargo que tiene la persona que respondió la encuesta dentro de ésta, así como los años que lleva laborando en ella.	3 ítems	
Conocimientos	Medir de manera cuantitativa el nivel de conocimientos que las empresas esperan que tengan sus trabajadores o aspirantes sobre cada una de las dimensiones estipuladas para el estudio.	7 ítems	Likert de 5 puntos, Ordinal, Conocimiento
Inversión	Conocer la cantidad monetaria que las empresas destinaron a temas relacionados con la ciberseguridad durante todo el año en el que el estudio se basa.	8 ítems	Likert de 5 puntos, Intervalo
Participación	Saber en qué medida las empresas permiten que sus empleados participen de manera activa en las decisiones referentes a la ciberseguridad.	5 ítems	Likert de 5 puntos, Ordinal, Frecuencia de realización
Relevancia	Saber en qué medida las empresas consideran relevantes los temas relacionados a la ciberseguridad con respecto a los conocimientos de sus empleados, contratación de personal y adquisición de tecnologías.	13 ítems	Likert de 5 puntos, Ordinal, Intensidad, y entradas libres

Fuente. Elaboración Propia.

8.8. Fiabilidad de los Instrumentos

Para que un instrumento pueda ser considerado confiable o reproducible, las mediciones que se realizan con éste deben generar los mismos resultados aun cuando se utilice en épocas, situaciones y poblaciones diferentes, si se aplican en las mismas condiciones (Manterola et al., 2018).

Por tanto, una vez que se han definido todos los ítems que debe contener el instrumento de medición, es necesario obtener el valor global de consistencia interna de éste; siendo la opción seleccionada para este estudio el cálculo del Alfa de Cronbach, ya que éste es un índice para instrumentos en donde el valor final es una variable de tipo ordinal (Supo, 2013).

El cálculo del coeficiente de Alfa de Cronbach genera resultados que varían entre 0 y 1, siendo los valores más cercanos a 1 aquellos que indican una mejor consistencia interna, ya que denota que existe correspondencia entre el resultado de cada uno de los ítems y el resultado final (Supo, 2013).

La tabla 12 muestra las interpretaciones que se deben dar al resultado del cálculo del coeficiente alfa de Cronbach dependiendo del valor obtenido.

Tabla 12.

Interpretación del Coeficiente Alfa de Cronbach

Valor del Coeficiente	**Consistencia Interna**
De 0.90 a 0.95	Excelente
Mayor a 0.80	Buena
Mayor a 0.70	Aceptable
Mayor a 0.60	Cuestionable
Mayor a 0.50	Pobre
Menor de 0.50	Inaceptable

Fuente. Elaboración propia con base en Frías-Navarro (2022).

Si bien en este estudio se ha empleado el cálculo del coeficiente alfa de Cronbach para determinar la fiabilidad de los instrumentos ya que la mayoría de las secciones establecidas dentro de cada uno de los cuestionarios tienen como valor final una variable de tipo ordinal, es necesario mencionar que la sección “Conocimientos B (Examen)” dentro del

cuestionario dirigido a los egresados tiene como valor final una variable categórica dicotómica, por lo que también es posible obtener su valor de consistencia interna mediante el cálculo del índice de consistencia interna Kuder–Richardson o KR-20 (Supo, 2013).

8.8.1. Encuesta Egresados

Aun cuando el cuestionario que se hizo llegar a los egresados está conformado por un total de 52 ítems, son solo 43 los considerados dentro del cálculo del coeficiente de Cronbach, ya que los otros 9 ítems que han sido omitidos recaban únicamente información básica para perfilar a los sujetos de estudio.

El resultado del cálculo del coeficiente Alfa de Cronbach se muestra en la figura 1.

Figura 1. Alfa de Cronbach de Encuesta Egresados.

Resumen del proceso de casos

Casos	N	Porcentaje
Válido	32	100.0%
Excluido	0	.0%
Total	32	100.0%

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
.84	43

Fuente. Elaboración propia de acuerdo a la “salida” del programa PSPP.

Una vez calculado el alfa de Cronbach, utilizando el programa GNU-PSPP, se obtiene un valor de 0.84 lo que indica que el instrumento presenta una buena consistencia interna.

8.8.2. Encuesta Empresas

También haciendo uso del programa GNU-PSPP, se calcula el alfa de Cronbach para 26 ítems de un total de 36 ítems definidos dentro del cuestionario dirigido a las empresas; la omisión de 10 elementos se debe a que, 3 solo brindan información básica para perfilar a los

sujetos de estudio y los otros 7 ítems tienen el propósito de brindar información cualitativa que recibe un tratamiento diferente a la demás.

El resultado del cálculo del coeficiente Alfa de Cronbach se muestra en la figura 2.

Figura 2. Alfa de Cronbach de Encuesta Empresas.

Resumen del proceso de casos

Casos	N	Porcentaje
Válido	15	100.0%
Excluido	0	.0%
Total	15	100.0%

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
.93	26

Fuente. Elaboración propia de acuerdo a la “salida” del programa PSPP.

De calcular el alfa de Cronbach se obtiene un valor de 0.93, lo que indica que el instrumento presenta una excelente consistencia interna.

9. ANÁLISIS DE RESULTADOS

Para realizar los análisis presentes a lo largo de todo este apartado se ha utilizado el software libre para análisis estadísticos de datos, GNU-PSPP en su versión 1.4.1-g79ad47. En algunos casos también se ha empleado el programa Excel para mostrar los datos de manera gráfica.

9.1. Estadística Descriptiva

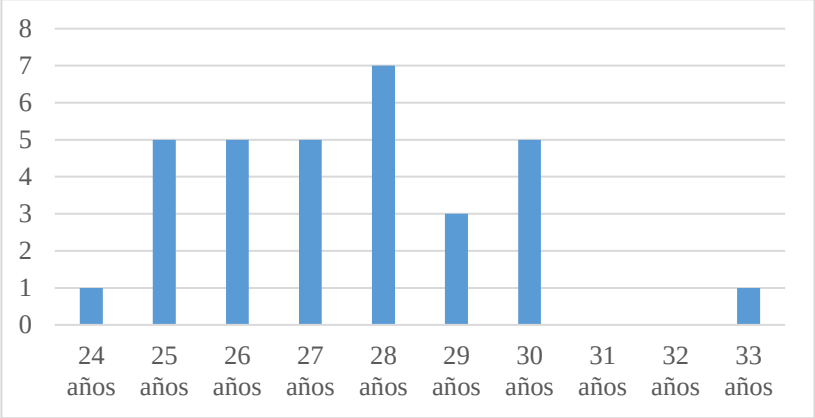
En esta sección se presentan gráficas que pretenden dar una visión general del perfil de los sujetos encuestados, con el propósito de explorar la situación y entender el contexto.

9.1.1. Egresados

En esta sección aparecen diversas figuras en las que se muestra información relevante al perfil de los egresados que han sido encuestados como parte de este estudio. Entre la información presentada de manera gráfica se encuentra: la generación poblacional a la que pertenecen, el plantel donde estudiaron, los años en los que estudiaron la carrera de ingeniería en sistemas computacionales, si cuentan o no con estudios de posgrado, cuantos años han laborado en actividades relacionadas con las TIC, el tipo de industria a la que pertenece el lugar donde laboran, cómo consideran que fueron sus estudios con relación a la ciberseguridad, las capacitaciones en temas de ciberseguridad a las que han asistido, su percepción con respecto al nivel de conocimientos en ciberseguridad que creen poseer y el nivel de participación que tienen dentro de su centro de trabajo con respecto a decisiones de la empresa enfocadas en la ciberseguridad.

Comenzando con la figura 3 que muestra la edad de los egresados que respondieron el cuestionario, permitiendo establecer la generación demográfica a la que pertenecen.

Figura 3. Edad de los Egresados Encuestados.

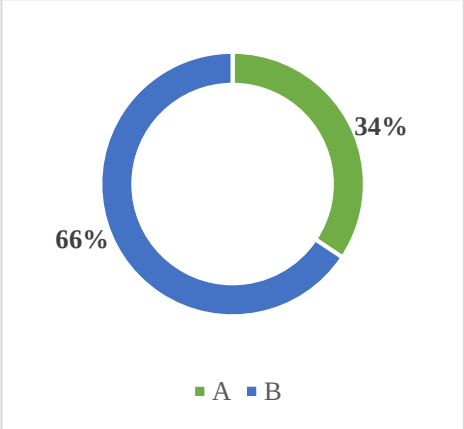


Fuente. Elaboración propia.

En la figura 3 se puede observar que el 84% o 27 de las personas que respondieron el cuestionario se encuentran en el rango de edad de 25 a 30 años, significando que pertenecen a dos generaciones demográficas diferentes, a la generación Y o 'MILLENNIAL' y a la generación Z o 'CENTENIAL'; lo que no es de extrañar ya que actualmente los millenials representan el 27% de la población mundial, mientras que los centenials conforma el 32% de la población global (Iberdrola, s.f.).

Con respecto a la cantidad de personas que egresaron de cada una de los planteles en los que se concentra el estudio, la información se encuentra representada de manera gráfica en la figura 4.

Figura 4. Porcentaje de Personas de Acuerdo a su Plantel de Egreso

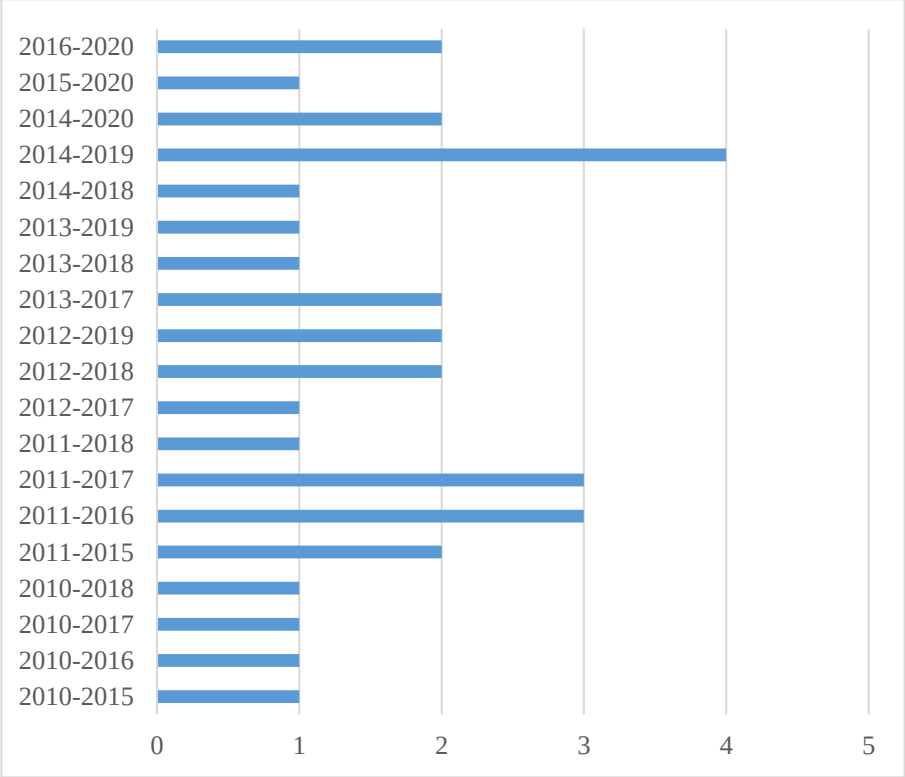


Fuente. Elaboración propia.

Por tanto, de la figura 4 se obtiene que de un total de 32 personas encuestadas, 11 o el 34% egresaron del plantel A; mientras que, 21 de ellas o el 66% egresaron del plantel B. Esto demuestra que las personas egresadas del plantel B tienen una mejor disposición para participar en estudios de este tipo; también, esto podría significar que el plantel B tiene mayor facilidad de contactar a sus egresados para difundir encuestas de este tipo.

En relación a la información sobre las generaciones académicas a las que pertenecen los encuestados, ésta se ve reflejada en la figura 5.

Figura 5. Generaciones Académicas a las que Pertenecen los Encuestados

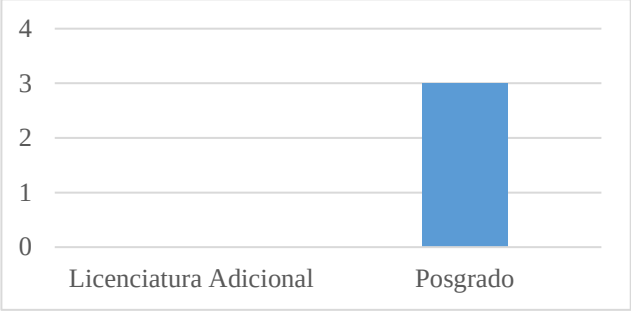


Fuente. Elaboración propia.

La figura 5 muestra que la generación académica 2014-2019 tuvo más participantes dentro de la encuesta, con 4 en total; además, la figura 5 deja ver que a la mayoría de los encuestados [34% u 11 de ellos] les tomó entre 5 y 6 años finalizar sus estudios de licenciatura.

A los encuestados también se les cuestionó sobre si contaban con una licenciatura adicional o con un posgrado, esto con el propósito de conocer si alguno de ellos había decidido ampliar sus conocimientos con respecto a la ciberseguridad. Los resultados de este cuestionamiento se presentan de manera gráfica dentro de la figura 6.

Figura 6. Egresados con Estudios Adicionales

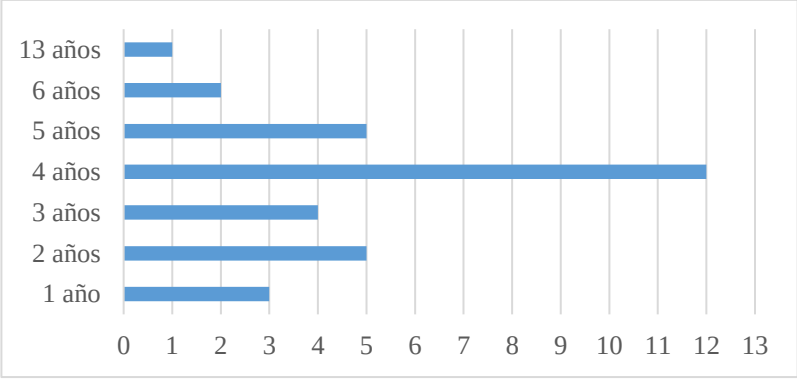


Fuente. Elaboración propia.

De la figura 6 se obtiene que ninguno de los egresados tiene alguna licenciatura adicional y solo 3 cuentan con un posgrado, sin embargo, uno de ellos no mencionó de qué trata su posgrado, otro mencionó que su posgrado fue en administración tecnológico y uno más respondió que su posgrado es en ciencias de la computación.

En cuanto a la cantidad de tiempo que los encuestados han estado laborando en actividades altamente relacionas con las TIC, la figura 7 muestra esta información.

Figura 7. Años Laborando en Actividades Relacionadas a las TIC.

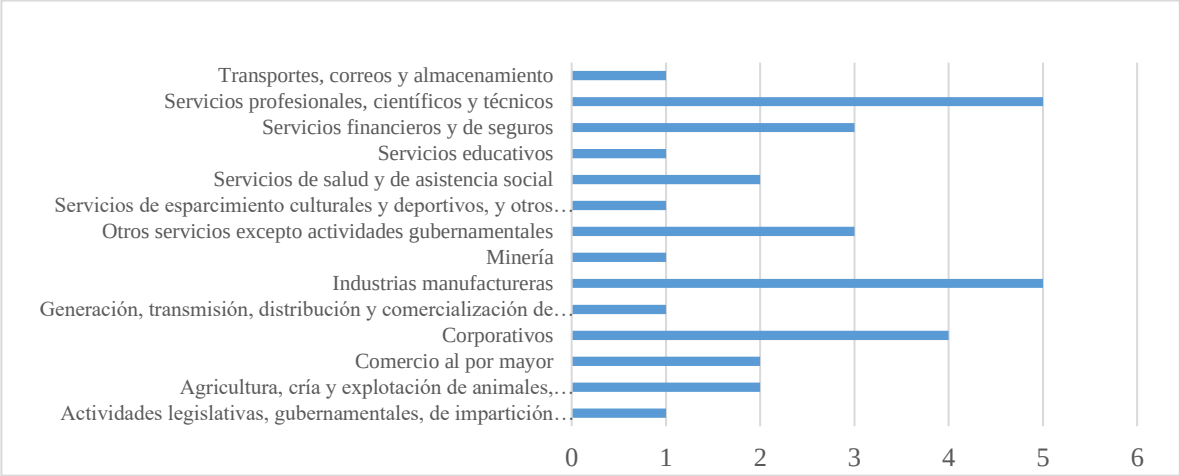


Fuente. Elaboración propia.

En la figura 7 se puede observar que la mayoría de los encuestados, 12 o el 37.5% de ellos, han laborado por 4 años en actividades relacionadas con las TIC; siendo la media de años laborados en este tipo de actividades de 4.8 años.

Otra de las preguntas que se hizo a los egresados es con respecto al tipo de industria a la que pertenece la empresa donde laboraron durante todo el año 2021, los datos referentes a este cuestionamiento se encuentran representados de manera visual en la figura 8.

Figura 8. Tipo de Industria a la que Pertenece la Empresa Donde Labora

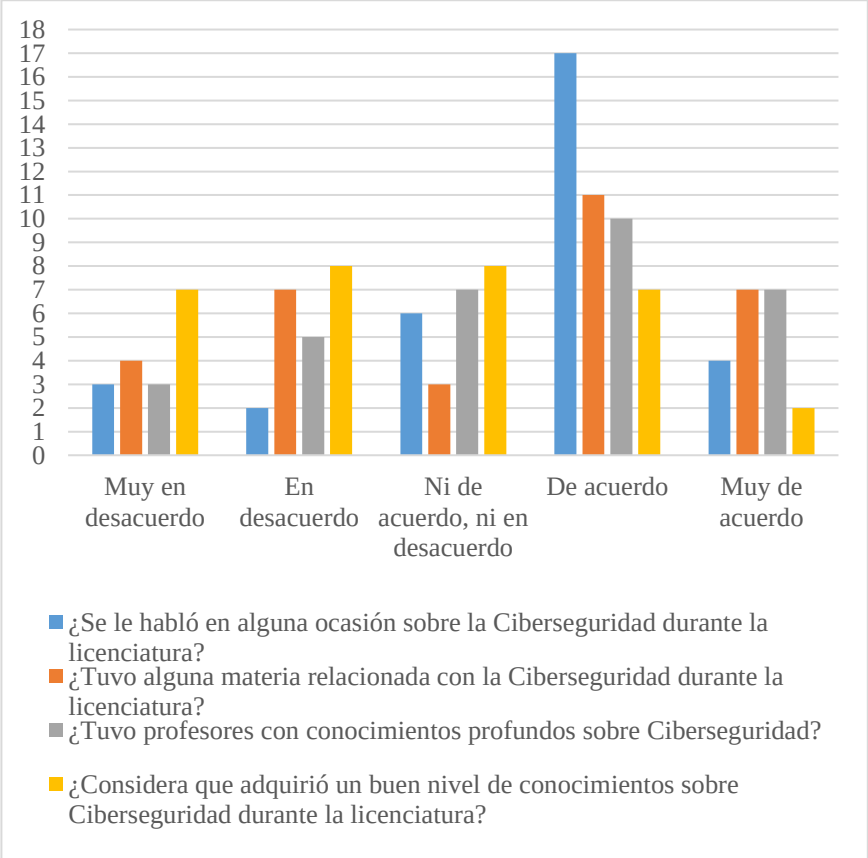


Fuente. Elaboración propia.

Como resultado, en la figura 8 se observa que una misma cantidad de encuestados, 5 o el 15.62% de ellos trabaja para empresas manufactureras o en aquellas denominadas como de servicios profesionales, científicos y técnicos; seguidas de los corporativos con un 12.5% o 4 personas que laboran en empresas de este tipo; por último aparecen las empresas categorizadas como otros servicios excepto actividades gubernamentales y aquellas dentro del rubro de servicios financieros y de seguros, con un 9.37% o 3 personas cada una.

Los egresados también respondieron cuestionamientos relacionados con su actitud ante ciertas afirmaciones relacionadas con sus estudios, la primera de estas aseveraciones busca conocer si los egresados recibieron educación relacionada con la ciberseguridad y su consideran que tuvieron catedráticos lo suficientemente preparados para impartir estos temas, así como si piensan que adquirieron un buen nivel de conocimientos en ciberseguridad a partir de estas asignaturas.

Figura 9. Actitud de los Egresados Ante Afirmaciones Relacionadas con su Educación



Fuente. Elaboración propia.

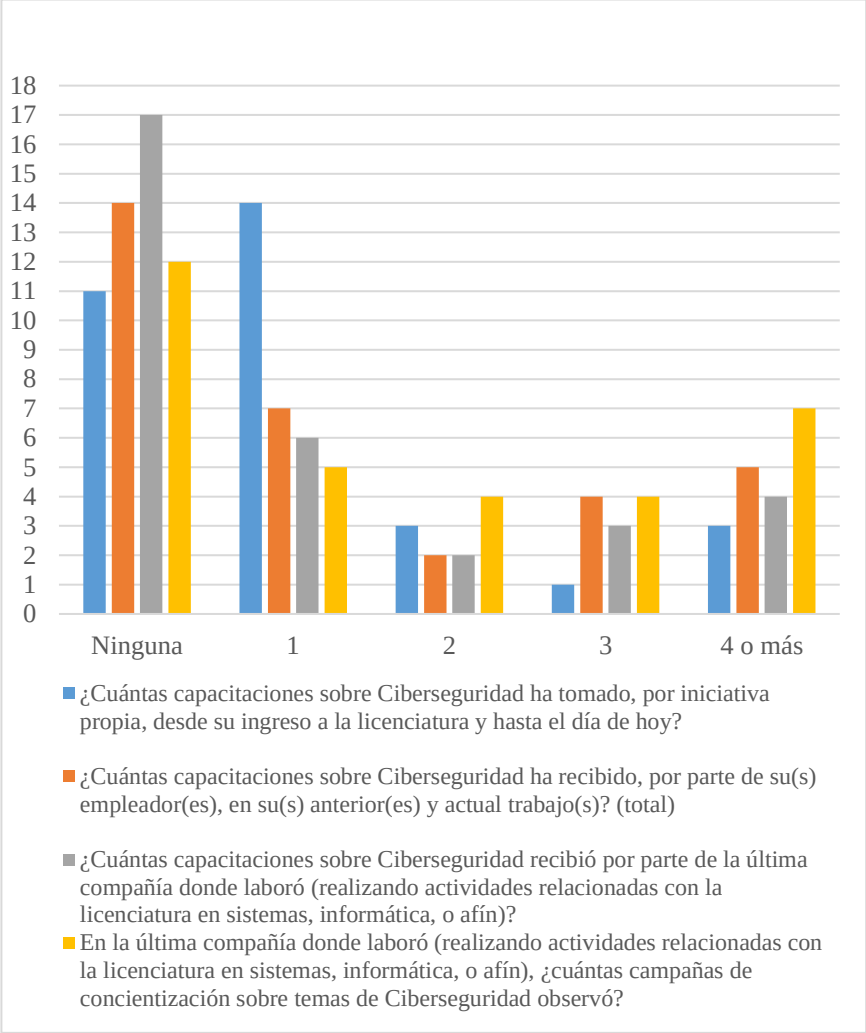
En la figura 9 se puede observar que: a) el 53.12% o 17 de los encuestados están de acuerdo con que durante la licenciatura se les habló sobre ciberseguridad, b) 34.37% u 11 de

las personas que respondieron el cuestionario están de acuerdo con que durante la carrera tuvieron alguna materia relacionada con la ciberseguridad y c) el 31.25% o 10 de los egresados encuestados está de acuerdo con que tuvo profesores con conocimientos profundos en ciberseguridad.

Pese a que estos resultados indicarían que los egresados se sienten confiados sobre sus conocimientos en ciberseguridad, es importante mencionar que ante la afirmación que hace alusión a si consideran que han adquirido un buen nivel de conocimientos en ciberseguridad durante la licenciatura, un 25% de ellos no está de acuerdo ni en desacuerdo, mientras que otro 25% está en desacuerdo; esto podría significar que si bien los egresados han tenido la oportunidad de adquirir estos conocimientos durante el curso de la licenciatura, algún factor provoca que estos conocimientos no se transfieran de la manera correcta o no permanezcan en el imaginario de los egresados por mucho tiempo.

Para solventar esta percepción de no estar lo suficientemente preparados en temas de ciberseguridad, los egresados podrían haber recurrido a tomar capacitaciones en estos temas, o bien, las empresas donde laboran podrían haber facilitado que los egresados asistieran a algún entrenamiento sobre temas de ciberseguridad; por esta razón se incluyó dentro del cuestionario una pregunta sobre la cantidad de capacitaciones que han cursado los sujetos de estudio, la información referente a este tópico se muestra en la figura 10.

Figura 10. Cantidad de Capacitaciones en Ciberseguridad a las que han Asistido los Encuestados



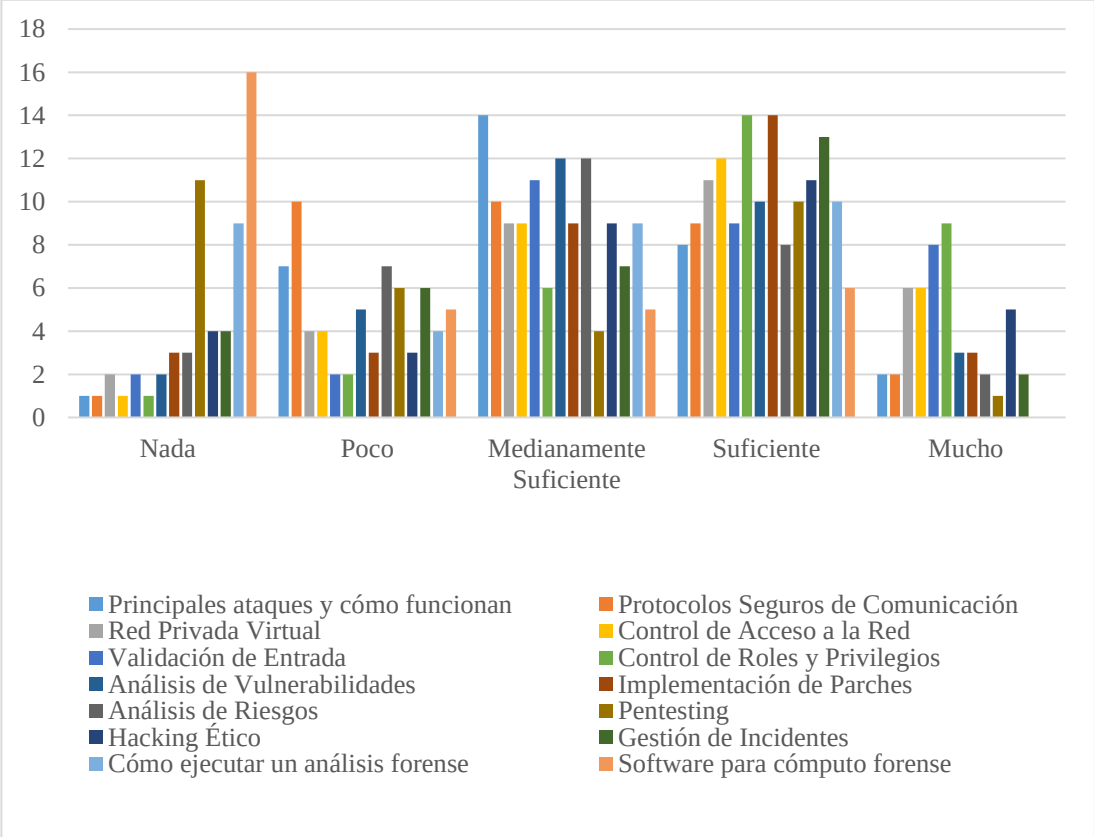
Fuente. Elaboración propia.

De la figura 10 se obtiene que: a) 14 o 43.75% de los encuestados han asistido, por iniciática propia, a 1 capacitación en temas de ciberseguridad, mientras que el 34.37% u 11 de ellos no han tomado ninguna capacitación en estos temas; b) 14 o 43.75% de los encuestados no han recibido ninguna capacitación por parte de ninguno de sus empleadores anteriores; c) el 53.12% o 17 de los encuestados manifiesta que en su empleo actual no ha

recibido ninguna capacitación en ciberseguridad y d) el 37.5% o 12 de los encuestados menciona que no han presenciado ninguna campaña de concientización sobre temas de ciberseguridad en su centro de trabajo actual.

Así como es importante saber si los encuestados han recibido algún tipo de orientación con respecto a temas de ciberseguridad, también es necesario conocer cuál es su percepción con respecto a su nivel de conocimientos en ciberseguridad, ya que ésta podría diferir de sus conocimientos reales y causar una brecha que no se busca cerrar por desconocimiento. Los resultados de esta cuestión se presentan dentro de la figura 11.

Figura 11. Percepción del Nivel de Conocimientos en Ciberseguridad



Fuente. Elaboración propia.

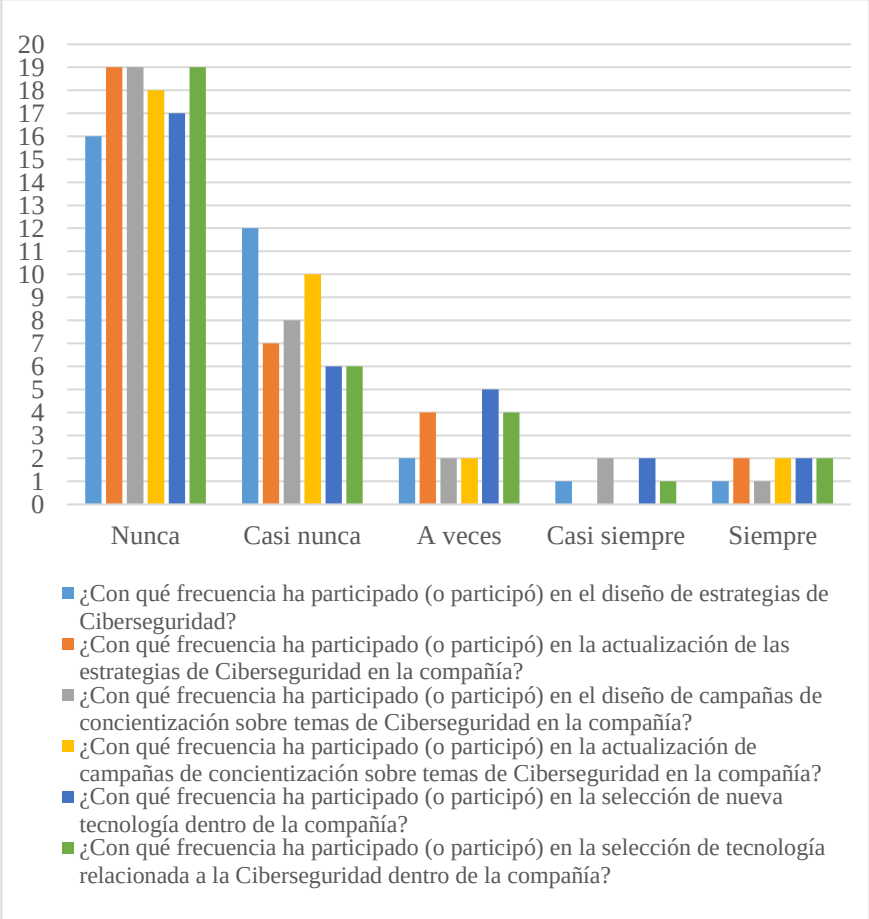
Para interpretar la figura 11 de tal manera que se hable en términos de las dimensiones estipuladas en la variable de estudio, es necesario establecer qué ítem pertenece a cada dimensión; por tanto, la categorización de los ítems es sigue el orden descrito a continuación:

a) Seguridad de Red: principales ataques y cómo funcionan, protocolos seguros de comunicación, red privada virtual, control de acceso a la red.
b) Seguridad de Software: validación de entrada, control de roles y privilegios, análisis de vulnerabilidades, implementación de parches.
c) Evaluación de la Seguridad: análisis de riesgos, pentesting, hacking ético, gestión de incidentes.
d) Cómputo Forense: cómo ejecutar un análisis forense, software para cómputo forense.

Una vez establecida esta categorización y generando las medias del total de los ítems por categoría, es posible mencionar que: a) la media de la categoría Seguridad de Red es "Medianamente Suficiente"; b) la media de la categoría Seguridad de Software es "Suficiente"; c) la media de la categoría Evaluación de la Seguridad es "Medianamente Suficiente"; y d) la media de la categoría Cómputo Forense es "Poco". Estos resultados son comparables con los obtenidos por cada ítem en particular, dado que la mayoría de las respuestas se concentran en los parámetros "Suficiente" y "Medianamente Suficiente" en todos los ítems.

Otro factor de interés es el nivel de participación que tienen los egresados dentro del lugar donde laboran, es decir, qué tanto se les permite participar en las decisiones y actividades de la empresa estrechamente ligadas con la ciberseguridad. Esta información está contenida de manera gráfica en la figura 12.

Figura 12. Nivel de Participación de los Egresados en las Empresas Donde Laboran.



Fuente. Elaboración propia.

En la figura 12 se puede observar que: a) el 50% o 16 de los encuestados afirma que nunca ha participado en el diseño de estrategias de ciberseguridad; b) 19 o el 59.37% de ellos nunca ha participado en la actualización de las estrategias de ciberseguridad, este mismo porcentaje menciona que nunca ha participado en el diseño de campañas de concientización sobre temas de ciberseguridad; c) el 56.25% o 18 de los encuestados nunca han participado en la actualización de campañas de concientización sobre temas de ciberseguridad; d) 17 o el 53.12% de ellos nunca ha participado en la selección de nueva tecnología; e) y el 59.37%

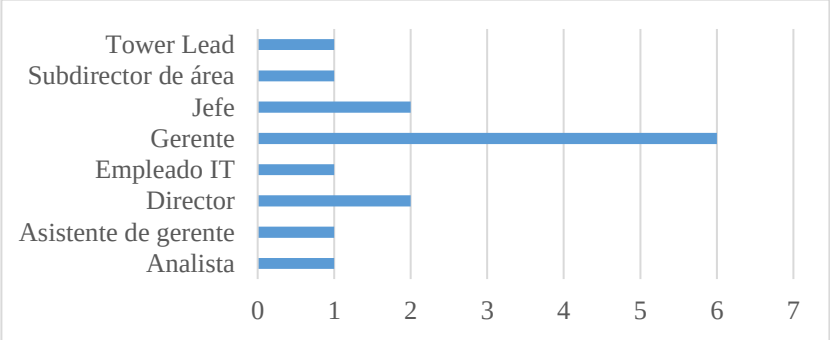
o 19 de los encuestados nunca ha participado en la selección de tecnología relacionada con la ciberseguridad. Estos resultados dejan ver que a los egresados se les permite muy poca participación en las decisiones que la empresa toma con respecto a la ciberseguridad.

9.1.2. Empresas

En este apartado se presentan diversas figuras que contienen información relevante al perfil de las empresas que han sido encuestadas como parte de este estudio. Entre la información mostrada en forma de gráficas se encuentra: la posición del empleado que respondió la encuesta a nombre de la empresa para la que labora, año en el que esta persona ingresó a laborar a la empresa que representa, el tipo de industria a la que pertenece la empresa y el nivel de participación la empresa permite a sus colaboradores con relación a la decisiones que se toman en temas de ciberseguridad.

Iniciando con la figura 13 que muestra la posición de los empleados que respondieron el cuestionario a nombre de la empresa que representan, permitiendo conocer el nivel jerárquico que ostenta el informante.

Figura 13. Puesto del Encuestado Dentro de la Empresa

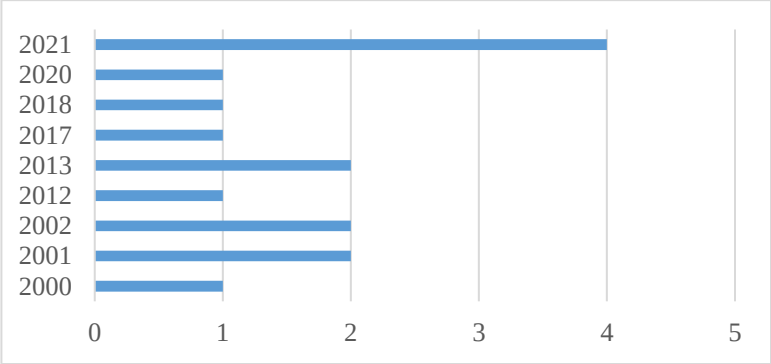


Fuente. Elaboración propia.

En la figura 13 se puede observar que el 40% o 6 de los encuestados ostentan la posición de gerente dentro de la empresa que representan, esto otorga mayor fiabilidad a los datos proporcionados.

Dado que la muestra en este estudio es una muestra del tipo por conveniencia, es necesario asegurarse que los empleados tuvieran al menos 1 año de antigüedad dentro de la empresa que representan, es por ello que se les cuestionó acerca del año en el que ingresaron a laborar en dicha entidad. Los resultados de esta pregunta se encuentran en la figura 14.

Figura 14. Año en el que el Encuestado Ingresó a Laboral a la Empresa que Representa.

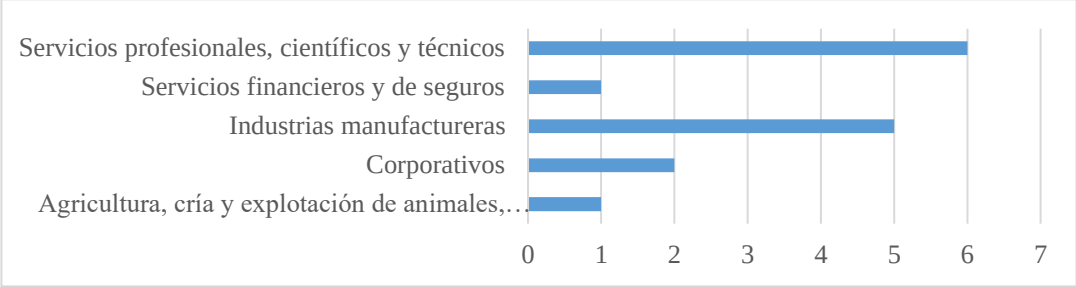


Fuente. Elaboración propia.

La figura 14 muestra que el 26.66% o 4 de los encuestados ingresaron a laborar a la empresa que representan en el año 2021, lo que indica que cumplen con el mínimo requisito de haber laborado al menos durante todo el año 2021 dentro de la compañía; mientras que el resto cuenta con aún más años de antigüedad.

Un dato importante a tener en cuenta con respecto a las empresas encuestadas es el tipo de industria a la que estas pertenecen, por lo que la figura 15 recoge los resultados de este cuestionamiento.

Figura 15. Tipo de Industria a la que Pertenece la Empresa que el Encuestado Representa

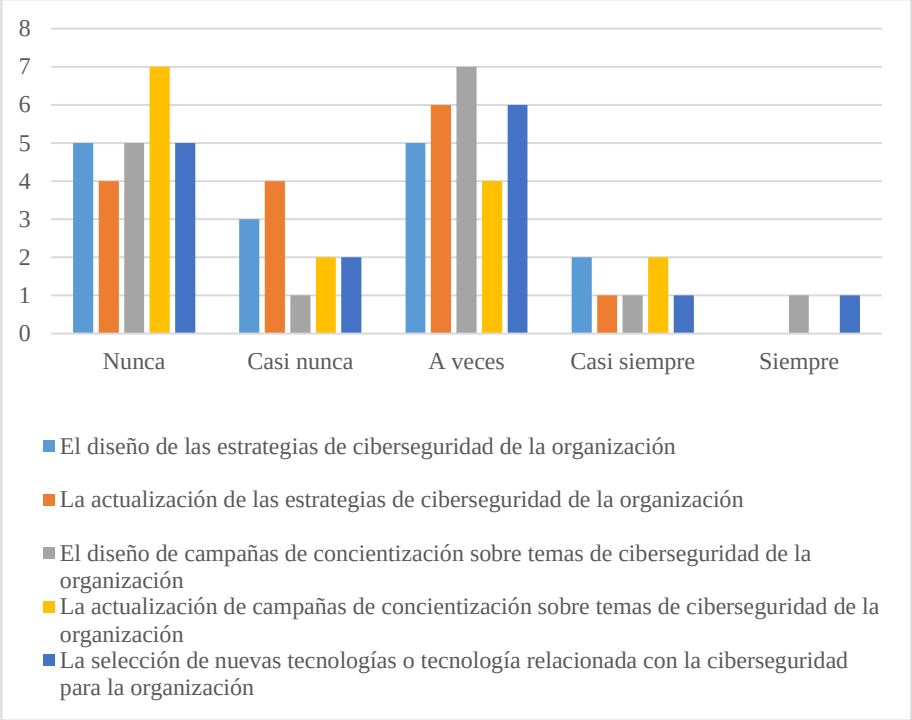


Fuente. Elaboración propia.

De la figura 15 se obtiene que el 40% o 6 de los encuestados provienen de la industria catalogada como servicios profesionales, científicos y técnicos; mientras que, 5 o el 33.33% de los encuestados pertenece a las industrias manufactureras. Estos resultados son similares a los mostrados en la figura 8 con respecto a la industria donde laboran los egresados, dado que el 15.62% pertenecía a cada uno de este tipo de industria; lo que indica que estos dos tipos de industria son mayoría dentro del estudio.

Con respecto a la participación que la empresa permite a sus empleados en las decisiones que se toman en relación a temas de ciberseguridad, la figura 16 concentra de forma gráfica las respuestas que dieron los representantes de cada una de las empresas que han participado en este estudio.

Figura 16. Participación Permitida a los Colaboradores de la Empresa



Fuente. Elaboración propia.

La figura 16 muestra que: a) un 33.33% o 5 de las empresas afirma que “A veces” permite que sus empleados participen en el diseño de las estrategias de ciberseguridad, mientras que este mismo porcentaje de participantes menciona que “Nunca” permite que sus empleados formen parte de este proceso; b) un 40% o 6 de las empresas afirma “A veces” invita a sus empleado a participar en la actualización de las estrategias de ciberseguridad de la organización; c) 7 o el 46.66% de los encuestados menciona que “A veces” autoriza que sus empleado participen en el diseño de campañas de concientización sobre temas de ciberseguridad, mientras que este mismo porcentaje asegura que “Nunca” permite que sus empleados colaboren en la actualización de estas campañas; d) un 40% o 6 de las empresas

afirma que “A veces” autoriza que sus empleados formen parte de la selección de nuevas tecnologías o tecnología relacionada con la ciberseguridad.

9.2. Comprobación de Hipótesis y Respuesta a Preguntas de Investigación

Para la comprobación de hipótesis se ha optado por utilizar la prueba t-Student para muestras independientes, debido a que este tipo de pruebas sirven para comparar dos muestras independientes de un tamaño igual o menor a 30 y examinar las diferencias entre ellas (Sánchez, 2015).

Con la utilización de este tipo de prueba es necesario conocer el valor crítico de t-student así como obtener su valor calculado, ya que la comparación entre estos dos valores determina qué hipótesis se rechaza. Es decir, si el valor absoluto de t –student calculada o estadístico t es mayor que el valor crítico o t de tablas, se rechaza la hipótesis nula o H0; aceptándose Hi. Si el valor absoluto de t –student calculada o estadístico t es menor que el valor crítico o t de tablas, no se puede rechazar la hipótesis nula o H0; rechazándose Hi (Minitab, s.f.).

Por otra parte, como se mencionó en los apartados anteriores, se han utilizado indicadores de tipo Likert y otros de tipo dicotómico; por lo que para poder homogeneizar los datos y utilizarlos en la comprobación de hipótesis, se han transformado los valores dicotómicos en Likert. Esto se llevó a cabo realizando intervalos de cambio de valor, es decir, el puntaje obtenido en cada una de las dimensiones se convirtió a un parámetro comprendido entre "Nada", "Poco", "Medianamente suficiente", "Suficiente", "Mucho" y en escala de Likert a "1", "2", "3", "4" y "5" respectivamente; en lugar de solo representarse con una calificación.

El cambio de valores se lleva a cabo únicamente para el examen de conocimientos y ha quedado establecido de la siguiente manera para cada una de las dimensiones:

- Seguridad de Red: una calificación entre 0 y 6 equivale a "Nada", que corresponde a "1" en escala de Likert; 7-12 = "Poco" = "2" en Likert; 13-18 = "Medianamente Suficiente" = "3" en Likert; 19-24 = "Suficiente" = "4" en Likert; 25-30 = "Mucho" = "5" en Likert.
- Seguridad de Software: una calificación entre 0 y 2 equivale a "Nada", que corresponde a "1" en escala de Likert; 3-4 = "Poco" = "2" en Likert; 5-6 = "Medianamente Suficiente" = "3" en Likert; 7-8 = "Suficiente" = "4" en Likert; 9-10 = "Mucho" = "5" en Likert.
- Evaluación de la Seguridad: una calificación entre 0 y 6 equivale a "Nada", que corresponde a "1" en escala de Likert; 7-12 = "Poco" = "2" en Likert; 13-18 = "Medianamente Suficiente" = "3" en Likert; 19-24 = "Suficiente" = "4" en Likert; 25-30 = "Mucho" = "5" en Likert.
- Cómputo Forense: una calificación entre 0 y 4 equivale a "Nada", que corresponde a "1" en escala de Likert; 5-8 = "Poco" = "2" en Likert; 9-12 = "Medianamente Suficiente" = "3" en Likert; 13-16 = "Suficiente" = "4" en Likert; 17-20 = "Mucho" = "5" en Likert.

9.2.1. Comprobación de Hipótesis

En esta sección vale la pena recapitular y mencionar nuevamente cuales son la hipótesis de investigación y nula de este estudio, formuladas de la siguiente manera:

Hipótesis de Investigación (Hi): existe una gran diferencia entre los conocimientos sobre ciberseguridad requeridos por las empresas y los conocimientos que tienen los egresados de carreras altamente relacionadas con la ciberseguridad.

Hipótesis Nula (Ho): Existe una diferencia mínima entre los conocimientos sobre ciberseguridad requeridos por las empresas y los conocimientos que tienen los egresados de carreras altamente relacionadas con la ciberseguridad.

Para comprobar la hipótesis se realizaron pruebas t-student para muestras independientes, dado que se tiene la muestra con respecto a los conocimientos que poseen los egresados y la muestra con respecto a los conocimientos que esperan las empresas, en la figura 17 se muestra el resultado de llevar a cabo estas pruebas utilizando el software estadístico mencionado con antelación.

Por otra parte, es indispensable establecer que el valor crítico de t para este estudio es de 2.014, obtenido de la tabla t, tomando en cuenta los grados de libertad que son 45 y un nivel de confianza del 95%.

Figura 17. Prueba t-student Para Comprobación de Hipótesis

Estadísticas de grupo

	Group	N	Media	Desviación Estándar	Err.Est.Media
Nivel de Conocimientos en Ciberseguridad	NCCEGR	32	3.03	.86	.15
	NCCEMP	15	3.47	.92	.24

Prueba para muestras independientes

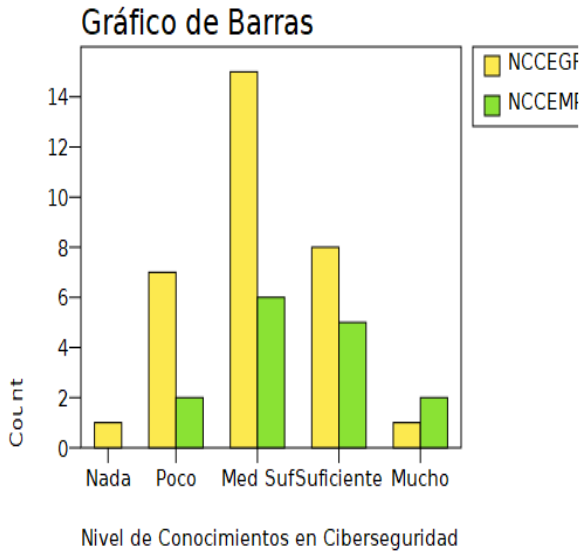
		Prueba de Levene para la igualdad de varianzas		T-Test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sign.	t	df	Sign. (2-colas)	Diferencia Media	Err.Est. de la Diferencia	Inferior	Superior
Nivel de Conocimientos en Ciberseguridad	Se asume igualdad de varianzas	.80	.375	-1.58	45.00	.120	-.44	.27	-.99	.12
	Igualdad de varianzas no asumida			-1.55	25.99	.134	-.44	.28	-1.01	.14

Fuente. Elaboración propia de acuerdo a la “salida” del programa PSPP.

De acuerdo con los resultados de la figura 17 y con la premisa que dicta que si el valor absoluto del valor t es menor que el valor crítico no se puede rechazar la hipótesis nula; se establece que en este estudio debe aceptarse la hipótesis nula la cual establece que existe una diferencia mínima entre los conocimientos sobre ciberseguridad requeridos por las empresas y los conocimientos que tienen los egresados de carreras altamente relacionadas con la ciberseguridad.

Además, en la figura 18 se muestra de manera gráfica la comparativa de los resultados con respecto al nivel de conocimientos que tienen los egresados y los que esperan las empresas, esto con el fin de tener una representación visual que permita comprender de mejor manera el resultado establecido en la figura 17.

Figura 18. Gráfico Comparativo del Nivel de Conocimientos en Ciberseguridad que Tienen los Egresados y el que Esperan las Empresas.



Fuente. Elaboración propia de acuerdo a la “salida” del programa PSPP.

Nota. El color amarillo representa los resultados con respecto al nivel de conocimientos que tienen los egresados y el color verde representa los resultados con respecto al nivel de conocimientos que esperan las empresas.

En la figura 18 se muestra una similitud entre los niveles de conocimiento que tienen los egresados y los que esperan las empresas, por ende se observa de manera más clara por qué no puede rechazarse la hipótesis nula.

Sin embargo, y ya que la variable principal del estudio se compone de 4 diferentes dimensiones, resulta interesante realizar la comprobación de hipótesis para cada una de ellas, ya que así se puede establecer cuál o cuáles de las dimensiones la cumplen o no y así conocer en qué dimensión o dimensiones es necesario que los egresados refuercen sus conocimientos.

De la figura 19 a la figura 22 se muestran los resultados de las pruebas t-studen para muestras independientes llevadas a cabo para contrastar los resultados de cada una de las dimensiones analizadas.

Iniciando con la figura 19 que contiene el resultado de analizar la dimensión Seguridad de Red.

Figura 19. Prueba t-student Para Comprobación de Hipótesis en Dimensión Seguridad de Red

Estadísticas de grupo

	Group	N	Media	Desviación Estándar	Err.Est.Media
Escala	EGSR	32	3.03	1.12	.20
	EMSR	15	3.73	.96	.25

Prueba para muestras independientes

		Prueba de Levene para la igualdad de varianzas		T-Test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sign.	t	df	Sign. (2-colas)	Diferencia Media	Err.Est. de la Diferencia	Inferior	Superior
Escala	Se asume igualdad de varianzas	.27	.607	-2.09	45.00	.042	-.70	.34	-1.38	-.03
	Igualdad de varianzas no asumida			-2.21	31.73	.034	-.70	.32	-1.35	-.05

Fuente. Elaboración propia de acuerdo a la “salida” del programa PSPP.

De la figura 19 y con la premisa que dicta que si el valor absoluto del valor t es mayor que el valor crítico se rechaza la hipótesis nula; se obtiene que para la dimensión Seguridad de Red debe aceptarse la hipótesis de investigación, la cual menciona que existe una gran diferencia entre los conocimientos sobre ciberseguridad requeridos por las empresas y los conocimientos que tienen los egresados de carreras altamente relacionadas con la ciberseguridad, acotando los conocimientos únicamente a la Seguridad de Red en este caso particular.

Para el caso de la dimensión de seguridad de software, los resultados de la comprobación de hipótesis se encuentran en la figura 20.

Figura 20. Prueba t-student Para Comprobación de Hipótesis en Dimensión Seguridad de Software

Estadísticas de grupo

	Group	N	Media	Desviación Estándar	Err.Est.Media
Escala	EGSS	32	3.19	1.18	.21
	EMSS	15	3.80	.94	.24

Prueba para muestras independientes

		Prueba de Levene para la igualdad de varianzas		T-Test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sign.	t	df	Sign. (2-colas)	Diferencia Media	Err.Est. de la Diferencia	Inferior	Superior
Escala	Se asume igualdad de varianzas	.15	.700	-1.77	45.00	.084	-.61	.35	-1.31	.09
	Igualdad de varianzas no asumida			-1.92	33.81	.064	-.61	.32	-1.26	.04

Fuente. Elaboración propia de acuerdo a la “salida” del programa PSPP.

De acuerdo con los resultados de la figura 20 y con la premisa que dicta que si el valor absoluto del valor t es menor que el valor crítico no se puede rechazar la hipótesis nula; se establece que para la dimensión seguridad de software debe aceptarse la hipótesis nula, la cual establece que existe una diferencia mínima entre los conocimientos sobre ciberseguridad requeridos por las empresas y los conocimientos que tienen los egresados de carreras altamente relacionadas con la ciberseguridad, acotando los conocimientos únicamente a la Seguridad de Software en este caso particular.

Con respecto a la dimensión de evaluación de la seguridad, los resultados de efectuar la comprobación de hipótesis para esta dimensión se muestran dentro de la figura 21.

Figura 21. Prueba t-student Para Comprobación de Hipótesis en Dimensión Evaluación de la Seguridad

Estadísticas de grupo

	Group	N	Media	Desviación Estándar	Err.Est.Media
Escala	EGES	32	3.34	.97	.17
	EMES	15	3.47	1.19	.31

Prueba para muestras independientes

		Prueba de Levene para la igualdad de varianzas		T-Test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sign.	t	df	Sign. (2-colas)	Diferencia Media	Err.Est. de la Diferencia	Inferior	Superior
Escala	Se asume igualdad de varianzas	1.94	.171	-.38	45.00	.708	-.12	.33	-.78	.53
	Igualdad de varianzas no asumida			-.35	23.13	.730	-.12	.35	-.85	.60

Fuente. Elaboración propia de acuerdo a la “salida” del programa PSPP.

De acuerdo con los resultados de la figura 21 y con la premisa que dicta que si el valor absoluto del valor t es menor que el valor crítico no se puede rechazar la hipótesis nula; se establece que para la dimensión evaluación de seguridad debe aceptarse la hipótesis nula, la cual establece que existe una diferencia mínima entre los conocimientos sobre ciberseguridad requeridos por las empresas y los conocimientos que tienen los egresados de carreras altamente relacionadas con la ciberseguridad, acotando los conocimientos únicamente a la Evaluación de Seguridad en este caso particular.

En relación a la dimensión de Cómputo Forense, los resultados de llevar a cabo la comprobación de hipótesis se observan en la figura 22.

Figura 22. Prueba t-student Para Comprobación de Hipótesis en Dimensión Cómputo Forense

Estadísticas de grupo

	Group	N	Media	Desviación Estándar	Err.Est.Media
Escala	EGCF	32	2.56	1.58	.28
	EMCF	15	2.60	.99	.25

Prueba para muestras independientes

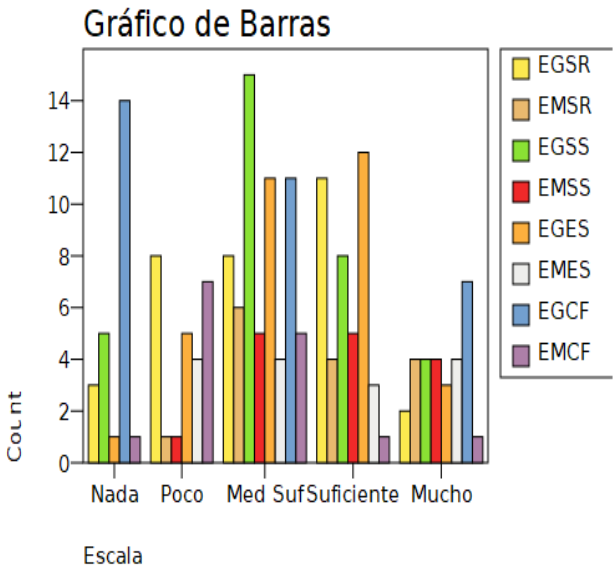
		Prueba de Levene para la igualdad de varianzas		T-Test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sign.	t	df	Sign. (2-colas)	Diferencia Media	Err.Est. de la Diferencia	Inferior	Superior
Escala	Se asume igualdad de varianzas	7.14	.010	-.08	45.00	.933	-.04	.45	-.94	.86
	Igualdad de varianzas no asumida			-.10	41.18	.922	-.04	.38	-.80	.73

Fuente. Elaboración propia de acuerdo a la “salida” del programa PSPP.

De acuerdo con los resultados de la figura 22 y con la premisa que dicta que si el valor absoluto del valor t es menor que el valor crítico no se puede rechazar la hipótesis nula; se establece que para la dimensión cómputo forense debe aceptarse la hipótesis nula, la cual establece que existe una diferencia mínima entre los conocimientos sobre ciberseguridad requeridos por las empresas y los conocimientos que tienen los egresados de carreras altamente relacionadas con la ciberseguridad, acotando los conocimientos únicamente al Cómputo Forense en este caso particular.

Para tener una representación visual de lo observado en la comprobación de hipótesis de cada una de las dimensiones, en la figura 23 se muestra de manera gráfica la comparativa de los resultados con respecto al nivel de conocimientos que tienen los egresados y los que esperan las empresas.

Figura 23. Gráfico Comparativo del Nivel de Conocimientos por Cada Dimensión de Ciberseguridad que Tienen los Egresados y el que Esperan las Empresas.



Fuente. Elaboración propia de acuerdo a la "salida" del programa PSPP.

Nota. Las siglas mostradas dentro de la figura tienen los siguientes significados: EGSR = Egresados Seguridad de Red, EMSR = Empresas Seguridad de Res, EGSS= Egresados Seguridad de Software, EMSS = Empresas Seguridad de Red, EGES = Egresados Evaluación de Seguridad, EMES = Empresas Evaluación de Seguridad, EGCF = Egresados Cómputo Forense, EMCF = Empresas Cómputo Forense.

En la figura 23 se muestra una similitud entre los niveles de conocimiento que tienen los egresados y los que esperan las empresas, por ende se observa de manera más clara por qué no puede rechazarse la hipótesis nula en la mayoría de los casos.

9.2.2. Respuesta a Preguntas de Investigación

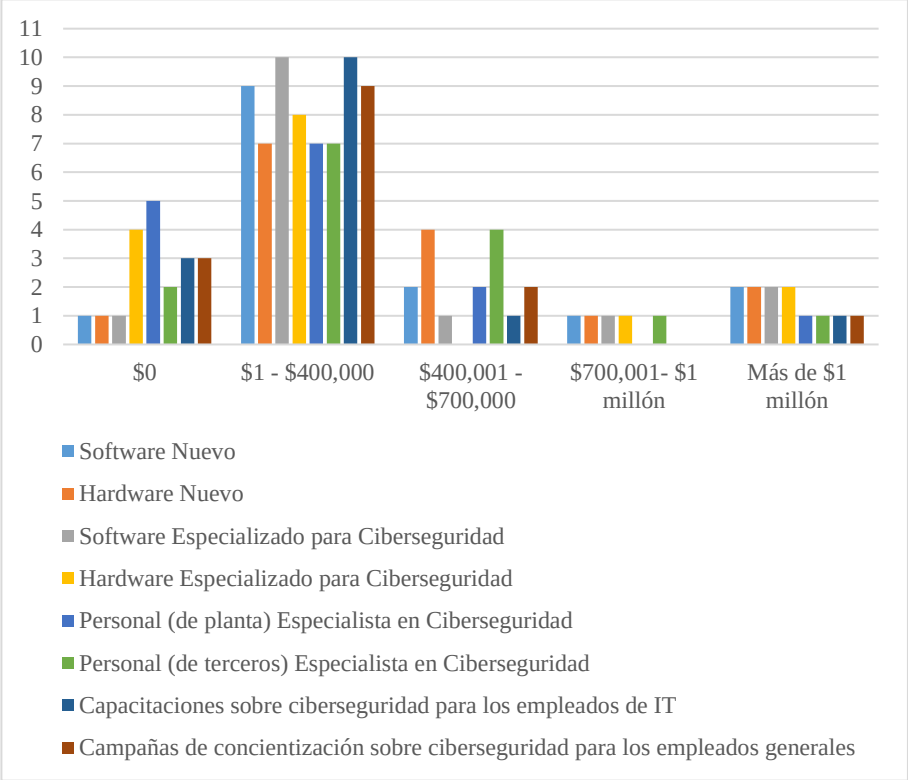
Para esta sección es importante tener presentes las preguntas de investigación que se formularon para este estudio, por ende se hace alusión a ellas una vez más:

a) ¿Qué tanta importancia se le da al tema de la ciberseguridad, con respecto a inversiones monetarias y nivel de conocimientos por parte de los empleados o aspirantes, dentro de las empresas?

b) ¿Cuáles son las diferencias destacables, sobre el tema de ciberseguridad, entre los requerimientos de las empresas y los conocimientos que poseen los egresados de carreras altamente relacionadas con la ciberseguridad?

Las respuestas a estas preguntas se obtienen mediante el análisis de resultados del cuestionario dirigido a las empresas. Los datos encontrados se presentan de manera gráfica de la figura 24 a la 26 y también de forma esquematizada en las tablas 13 y 14.

Figura 24. Inversión Monetaria en Temas de Ciberseguridad.



Fuente. Elaboración propia.

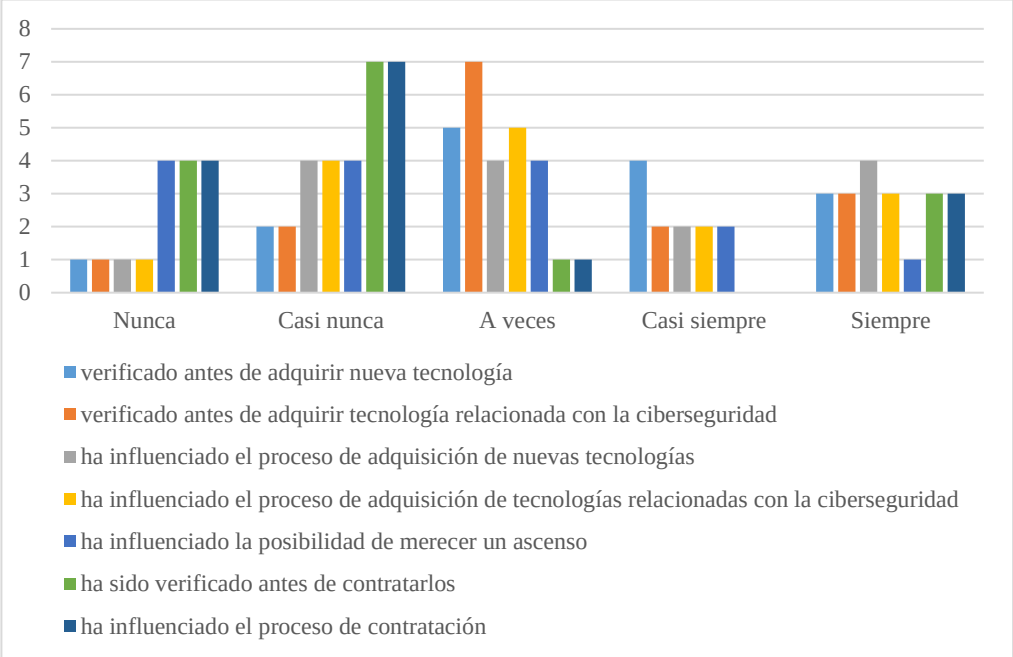
Nota. Las cantidades están presentadas en pesos mexicanos y representan solo al año 2021.

En la figura 24 puede observarse que las empresas encuestadas destinan cantidades entre $1 y $$400,000 pesos mexicanos de la siguiente manera: a) 9 o 60% de estas lo utilizan para la compra de Software Nuevo; b) el 46.64% o 7 de ellas lo usan para la compra de Hardware nuevo; c) 10 o el 66.67% de éstas utilizan esta cantidad de dinero para la compra de Software Especializado para Ciberseguridad; d) el 53.33% u 8 de las empresas encuestadas destina esta cantidad a la compra de Hardware Especializado para Ciberseguridad; e) 7 o el 46.67% de ellas invierte esta cantidad en el pago de Personal (de planta) Especialista en Ciberseguridad, mientras que este mismo porcentaje lo destina en Personal (de terceros) Especialista en Ciberseguridad; f) el 66.67% o 10 de las empresas encuestadas invierten esta cantidad en Capacitaciones sobre ciberseguridad para los empleados de IT; g) 9 o el 60% de ellas invierte esta cantidad en Campañas de concientización sobre ciberseguridad para los empleados generales.

Esto implica que las empresas si tienen contemplado el tema de la ciberseguridad dentro de sus presupuestos y destinan recursos monetarios a fortalecer sus estrategias.

Con respecto a la relevancia que tiene el nivel de conocimientos de los empleados o aspirantes, la figura 25 contiene la información relevante a este tema.

Figura 25. Relevancia del Nivel de Conocimientos de los Empleados o Aspirantes en la Toma de Decisiones Dentro de la Empresa.



Fuente. Elaboración propia.

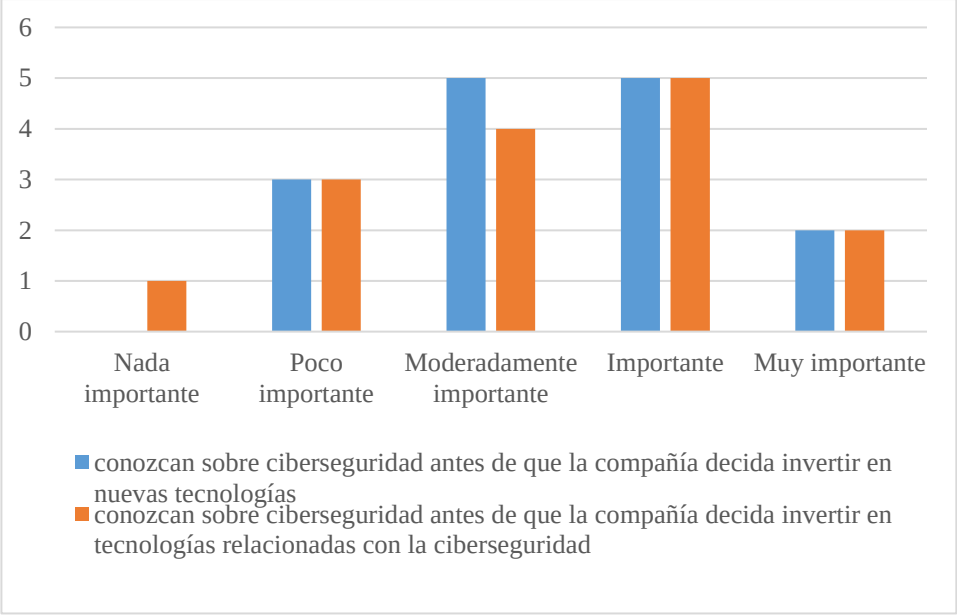
La figura 25 muestra que: a) el 33.33% o 5 de las empresas encuestadas han verificado el nivel de conocimientos de sus colaboradores antes de adquirir tecnología relacionada con la ciberseguridad; b) 7 o el 46.67% de ellas han verificado el nivel de conocimientos de sus empleados antes de adquirir tecnología relacionada con la ciberseguridad; c) la misma cantidad de empresas, 4 o el 26.67%, afirma 3 supuestos diferentes, que el nivel de conocimientos de sus empleados "Nunca", "Casi nunca" y "Siempre" ha influenciado el proceso de adquisición de nuevas tecnologías; d) el 33.33% o 5 de las empresas encuestadas menciona que el nivel de conocimientos en ciberseguridad ha influenciado el proceso de adquisición de tecnologías relacionadas con la ciberseguridad; e) la misma cantidad de empresas, 4 o el 26.67%, afirma 3 supuestos diferentes, que el nivel de conocimientos en

ciberseguridad de sus colaboradores "Nunca", "Casi nunca" y "a veces" ha influenciado la posibilidad de merecer un ascenso; f) el 46.67% o 7 de las empresas encuestadas ha verificado el nivel de conocimientos en ciberseguridad que poseen los postulantes antes de contratarlos; g) 7 o el 46.67% de ellas comenta que el nivel de conocimientos en ciberseguridad que poseen los postulantes ha influenciado el proceso de contratación.

Estos resultados demuestran que si bien las empresas invierten recursos monetarios en temas relacionados a la ciberseguridad, el nivel de conocimientos que tengan sus empleados o postulantes no es relevante a la hora de tomar decisiones.

Para contribuir al rubro tratado en la figura 25, la figura 26 muestra la importancia que se le da al nivel de conocimientos en ciberseguridad que poseen los empleados o aspirantes de una compañía cuando esta decide invertir en la adquisición de tecnología.

Figura 26. Importancia del Nivel de Conocimientos de los Empleados o Aspirantes en la Toma de Decisiones Dentro de la Empresa.



Fuente. Elaboración propia.

De la figura 26 se obtiene que a) la misma cantidad de empresas encuestadas, 5 o el 33.33%, considera "Moderadamente Importante" e "Importante" que sus empleados conozcan sobre ciberseguridad antes de que la compañía decida invertir en nuevas tecnología; b) también el 33.33% o de 5 de ellas considera "Importante" que sus colaboradores conozcan sobre ciberseguridad antes de que la compañía decida invertir en tecnologías relacionadas con la ciberseguridad.

Estos resultados no concuerdan mucho con los obtenidos en la figura 25 con respecto a qué tanta relevancia tenía el nivel de conocimientos en ciberseguridad para la toma de decisiones; dado que en ese apartado la frecuencia con la que las empresas verifican el nivel de conocimientos es mucho menor a la importancia que dicen darle a que los tengan; por ello se les cuestionó sobre el motivo de su respuesta y los resultados se presentan en la tablas 13 y 14.

Tabla 13.

Motivo de la Respuesta en Relación con la Importancia de los Conocimientos en las Inversiones en Nuevas Tecnologías.

¿Qué tan importante considera que sus empleados conozcan sobre ciberseguridad antes de que la compañía decida invertir en nuevas tecnologías?		
Empresa	**Nivel**	**Motivo**
A	Muy importante	Porque la inversión es alta
B	Moderadamente importante	Somos empresa de TI
C	Moderadamente importante	Actualmente el sector está sufriendo muchos ataques
D	Importante	Las amenzas y las vulnerabilidades son materia prima de la sociedad ventajosa de intereses ajenos, ninguna organización está exenta de riesgos. Los empleados deben saber en donde es necesario invertir y modernizarse, puesto que hay puntos críticos de acceso y control a la información. [*sic*]
E	Poco importante	La adquisiscion de nuevas tecnologias depende de las necesidades de los empleados, no es lo mismo personal que va usar herramientas para uso administrativo, a personal que va a descargar un entorno de desarrollo completo con bases de datos de clientes en produccion, en esta comparacion la seguridad es la misma (alta) pero equipos y caracteristicas totalmente diferentes. [*sic*]
F	Moderadamente importante	Debe existir responsabilidad del uso de las TIC´s y para tener mayores, libertades se requiere un mayor compromiso en temas de seguridad. [*sic*]
G	Poco importante	No es decisión de ellos
H	Poco importante	Para que se les de el entrenamiento debido [*sic*]
I	Importante	Por qué es importante que los empleados sepan de estos temas para que puedan seleccionar la mejor tecnología para la organización
J	Muy importante	Para prevenir fraudes
K	Importante	Siempre es importante que los empleados conozcan sobre ciberseguridad independientemente de si se va a invertir en nuevas tecnologías
L	Importante	Por ser usuarios responsables
M	Importante	Para poder proteger la información
N	Moderadamente importante	Hoy día debe ser prioridad
Ñ	Moderadamente importante	es mas importante que a la direccion tenga claro el alcance dada la sencibilidad de las operaciones de la empresa y los empleados operarla [*sic*]

Fuente. Elaboración propia.

Tabla 14.

Motivo de la Respuesta en Relación con la Importancia de los Conocimientos en las Inversiones en Tecnologías Relacionadas con la Ciberseguridad.

¿Qué tan importante considera que sus empleados conozcan sobre ciberseguridad antes de que la compañía decida invertir en tecnologías relacionadas con la ciberseguridad?		
A	Muy importante	Por el valor de la información
B	Moderadamente importante	Conciencia en el uso correcto de la tecnologia [*sic*]
C	Moderadamente importante	Actualmente el sector está sufriendo muchos ataques
D	Importante	Los empleados deben tener las nociones generales y elementales de ciberseguridad para poder ejercer un juicio permanente identificando posibles riesgos potenciales así como propuestas para la mitigación de los mismos.
E	Importante	Para el personal de TI es importante que conozca y este actualizado de las nuevas herramientas que puedan prevenir el robo de informacion o suplantacion de información [*sic*]
F	Moderadamente importante	Dado que labora en un lugar de desarrollos científicos, muchas ocasiones se requiere de nuevas plataformas o trabajo colaborativo, por lo que considero que no deben ser expertos en Ciberseguridad, pero si conocer los elementos mínimos que estarán supervisando con alguna tecnología para este tema.
G	Nada importante	Ni depende de ellos
H	Poco importante	Para que se les de el entrenamiento debido [*sic*]
I	Importante	Es importante para la organización
J	Muy importante	Para prevenir fraudes
K	Importante	Siempre es importante que los empleados conozcan sobre ciberseguridad independientemente de si se va a invertir en nuevas tecnologías
L	Moderadamente importante	Porque hay departamenos especialistas [*sic*]
M	Importante	Para estar protegidos
N	Poco importante	Se capacitan si es necesario
Ñ	Poco importante	Es mas importante que a la direccion tenga claro el alcance dada la sencibilidad de las operaciones de la empresa y los empleados operarla [*sic*]

Fuente. Elaboración propia.

Por otra parte, también se cuestionó a las empresas con respecto a los temas relacionados con los conocimientos en ciberseguridad que consideran deben poseer sus empleados o postulantes, incluyendo el nivel deseado de conocimiento que deben tener, así como el motivo por el cuál creen que deben tenerlo. Los resultados de estos cuestionamientos se encuentran en la tabla 15.

Tabla 15.

Temas de Ciberseguridad Adicionales que las Empresas Consideran Deben Tener sus Empleados o Postulantes.

Con respecto a la Ciberseguridad, ¿Qué otro tema de conocimiento considera que deben poseer sus empleados o postulantes?		
Empresa	**Nivel**	**Tema**
A	Suficiente	Pishing, seguridad en dispositivos moviles, seguridad en la nube [*sic*]
B	Suficiente	Antivirus y amenazas
C	Suficiente	"Tecnologías actuales para ciberseguridad"
D	Suficiente	Manejo ético de la información confidencial y altamente confidencial
E	Suficiente	Proteccion de Datos, internet de las cosas, Suplantación de identidad general, Phishing selectivo, Phishing selectivo avanzado, Estafas de compromiso de correo electrónico comercial, Computación en la nube [*sic*]
F	Suficiente	Control de puertos, nivelación de perfiles de usuarios y horarios de acceso
G	Mucho	Los riesgos
H	Medianamente suficiente	Phishing
I	Suficiente	Los diferentes tipos de ataques informáticos
J	Mucho	Ingeniería Social, Suplantación de Identidad, Phishing, etc
K	Suficiente	Deben saber como protegerse y como evitar caer en ataques de ciberseguridad [*sic*]
L	Medianamente suficiente	Trafico de red
M	Medianamente suficiente	Los diferentes tipos de ataques que puede tener una empresa y sus empleados
N	Medianamente suficiente	Sistemas de gestión de riesgos, cómo crear un sistema de gestión de la seguridad, amenazas, riesgos, tecnologías relacionadas.
Ñ	Mucho	mas que conocimiento tecnico, creo que EL IMPACTO que tiene en la organizacion el hacer o no hacer algo. CONOCER cual es el objetivo final de los conceptos tecnicos es lo que ayudará verdaderamente a valorar la ciberseguridad desde las necesidades que el negocio busca cubrir [*sic*]

Fuente. Elaboración propia.

Adicionalmente se les preguntó si tenían personal especializado en ciberseguridad a disposición de la empresa, el tipo de contrato y los motivos; los resultados de este cuestionamiento se concentran en la tabla 16.

Tabla 16.

Personal Especializado en Ciberseguridad

¿Cuenta con especialistas en ciberseguridad a disposición de la compañía?		
Empresa	**Respuesta**	**Motivo**
A	Si, son empleados de base (contratados directamente por la compañía)	
B	No	Contratar a un especialista en ciberseguridad o a una empresa especializada se considera un gasto que no trae los suficientes beneficios
C	Si, son empleados de base (por outsourcing)	
D	Si, son empleados de base (contratados directamente por la compañía)	
E	Si, son empleados de base (contratados directamente por la compañía)	
F	Si, otra empresa brinda sus servicios especializados mediante un contrato de soporte	
G	No	No se destinan los suficientes recursos monetarios para este rubro
H	Si, son empleados de base (contratados directamente por la compañía)	
I	Si, otra empresa brinda sus servicios especializados mediante un contrato de soporte	
J	Si, son empleados de base (contratados directamente por la compañía)	
K	Si, otra empresa brinda sus servicios especializados mediante un contrato de soporte	
L	Si, son empleados de base (contratados directamente por la compañía)	
M	Si, otra empresa brinda sus servicios especializados mediante un contrato de soporte	
N	Si, se les contacta en caso de eventualidad (por honorarios)	
Ñ	Si, son empleados de base (contratados directamente por la compañía)	

Fuente. Elaboración propia.

Nota. Solo se preguntó el motivo a aquellos que respondieron que no tenían personal especializado en ciberseguridad a disposición de la empresa.

CONCLUSIONES

- Aunque las carreras de ingeniería en México, en su mayoría están configuradas para que se concluyan en un plazo de 4.5 años, los resultados de la encuesta demuestran que las personas están finalizando sus estudios en un plazo de entre 5 y 6 años, algo que podría afectar sus conocimiento en ciberseguridad; es decir, demorar más de medio año en finalizar los estudios e integrarse al campo laboral después, podría suponer un desfase de los conocimientos que se poseen y los que son requeridos ya que la tecnología y los ataques cibernéticos evolucionan rápidamente.
- Que el 50% de los encuestados no considere o no esté seguro de que ha adquirido un buen nivel de conocimientos en ciberseguridad durante la licenciatura, puede deberse, entre otros factores a que: a) se esté utilizando un método de enseñanza poco efectivo, b) el temario de las asignaturas relacionadas con la ciberseguridad esté desactualizado, c) no se le da a la ciberseguridad la importancia que debería tener dentro de los temarios de las asignaturas relacionadas a ella, d) los recursos para que las escuelas impartan este tipo de temas es limitado, e) los alumnos no le dan a la ciberseguridad la importancia que merece dentro de su ciclo de formación y a lo largo de toda su carrera profesional, f) el tema de la ciberseguridad es tan extenso y complejo que una sola asignatura no puede brindar los conocimientos necesarios para que los alumnos puedan enfrentarse a las nuevas tendencias en ciberseguridad.
- Que los egresados consideren que durante la licenciatura no han adquirido un buen nivel de conocimientos en ciberseguridad y aun así no hayan asistido a muchas capacitaciones relacionada con el tema podrían significar, entre otras cosas, que: a) los egresados, al sentir que su nivel en conocimientos sobre ciberseguridad no es muy

elevado, se han dispuesto a solventar sus carencias con entrenamiento adicional que les permita ser más competitivos en el mercado laboral; b) otra gran mayoría considera que no contar con un buen nivel en este tipo de conocimientos no afecta su posicionamiento en el mercado laboral; c) los egresados consideran que su nivel de conocimientos en ciberseguridad no difiere mucho de los conocimientos que deben de tener para ser relevantes en el mercado laboral y por ello no creen que sea necesario asistir a muchas capacitaciones; d) las empresas no exigen que sus empleados o postulantes cuenten con este tipo de conocimientos en un nivel y por ello no dedican recursos a las capacitaciones o campañas de ciberseguridad.

- Resulta interesante observar que la percepción de los egresados con respecto a su nivel de conocimientos en cada una de las dimensiones evaluadas no difiere mucho del nivel real obtenido después del cuestionario de conocimientos.

  Siendo que la percepción sobre sus conocimientos en la categoría Seguridad de Red tiene una media de "Medianamente Suficiente" y la media después de realizar el examen resultó en que su nivel de conocimientos en este aspecto equivale a un "Medianamente Suficiente"; con respecto a la dimensión de Seguridad de Software, la percepción de los egresados es de tener un nivel "Suficiente", mientras que la prueba arrojó que su nivel es "Medianamente Suficiente"; en cuanto a la categoría de Evaluación de la Seguridad, tanto la percepción de los egresados como los resultados del examen muestran que su nivel de conocimientos en esta dimensión es de "Medianamente Suficiente"; finalmente, en relación con la dimensión de Cómputo Forense, la percepción de los egresados con respecto a su nivel de conocimientos es

de “Poco”, mientras que en los resultados del examen se puede observar un nivel “Medianamente Suficiente”.

- Dado que la cantidad de egresados a los que se les permite participar activamente en las decisiones de la empresa con respecto a temas de ciberseguridad es muy baja, esto puede influir en la decisión de los egresados en capacitarse en temas de ciberseguridad, dado que no hay participación, no hay aumento de los conocimientos por decisión propia. Esta baja participación puede deberse, entre otras cosas, a que las posiciones que tienen los encuestados dentro de la compañía donde laboran no están estrechamente relacionadas con el apoyo a la toma de decisiones, algo que no debería importar mucho cuando se busca llegar a un consenso con respecto a la ciberseguridad, ya que es necesario conocer el nivel de conocimientos con el que cuenta la organización para tomar decisiones apropiadas.
- El hecho de que la mayoría de las personas encuestadas, tanto egresados como empleados de diferentes empresas, pertenezcan al mismo tipo de industrias podría indicar que tanto las industrias manufactureras como las denominadas de servicios profesionales, científicos y técnicos son las que más egresados en sistemas computacionales contratan; también podría significar que este tipo de industria es el que está más presente dentro de territorio nacional.
- La diferencia entre el nivel de participación que dicen tener los egresados en la toma de dediciones referentes a la ciberseguridad dentro de su centro de trabajo y el nivel de participación que las empresas reportan que permiten, puede deberse única y sencillamente a que no se están comparando las mismas empresas; es decir, las empresas en las que laboran los egresados no necesariamente son las empresas a las

que se ha encuestado, esto porque, como medida de protección de identidad, no se tomó en cuenta la relación egresado-empresa dentro del análisis.

Por otra parte, en dado caso que la empresa coincidiera, la diferencia puede deberse a que el egresado no ostenta un cargo al que se le permita participar en el proceso de toma de decisiones, mientras que la empresa reporta que si se permite participar dado que no están considerando el rango de la persona en cuestión.

- Con la comprobación de hipótesis para cada caso, se tiene que la hipótesis de investigación se acepta para la dimensión de Seguridad de Red y se rechaza para las dimensiones de Seguridad de Software, Evaluación de la Seguridad y Cómputo Forense.

  Esto significa que la Seguridad de Red es un tema en el que las empresas requieren un conocimiento "Suficiente", mientras que los egresados tienen un conocimiento "Medianamente Suficiente"; para el tema de la Seguridad de Software las empresas requieren un conocimiento "Suficiente" y los egresados poseen un conocimiento "Medianamente Suficiente"; la Evaluación de Seguridad es un tema en el que las empresas requieren un conocimiento "Medianamente Suficiente" y los egresados tienen exactamente este nivel de conocimientos; para el tema del Cómputo Forense las empresas requieren un conocimiento "Medianamente Suficiente", siendo que los egresados poseen el nivel de conocimientos esperado.
- La mayoría de las empresas invierten cantidades entre $1 y $$400,000 en temas relacionados a la ciberseguridad como son la compra de software y hardware especializado; la contratación de personal, ya sea de planta o de terceros,

especializado en ciberseguridad; así como en capacitaciones y campañas de concientización para su personal.

Esto demuestra que todas las empresas encuestadas tienen en mente a la ciberseguridad dentro de sus presupuestos y que invierten recursos monetarios en estar preparados en este tema.

- El hecho de que las empresas aún no consideren el nivel de conocimientos en ciberseguridad de sus colaboradores o postulantes como una habilidad distintiva para merecer un ascenso o ser contratados podría explicar el por qué el nivel de conocimientos que tienen los egresados y el que piden las empresas va tan a la par; es decir, si las empresas no consideran estos conocimientos como un valor agregado, los egresados no sienten la motivación suficiente para profundizar sus conocimientos y por ello la falta de profesionales en el área no ha podido ser disminuida. Sin embargo, es importante aclarar que dentro de sus respuestas no hacen referencia al tipo de empleado del que hablan, es decir, si es del departamento de TI o general.
- Las empresas mencionan que no es frecuente que verifiquen el nivel de conocimientos sobre ciberseguridad que tienen sus colaboradores o aspirantes antes de adquirir nueva tecnología, o que estos les traigan alguna ventaja laboral, sin embargo, si mencionan que es de “Moderadamente Importante” a “Importante” que los tengan antes de que la empresa decida invertir en nueva tecnología o tecnología relacionada a la ciberseguridad. Esto demuestra que no existe congruencia entre lo que la empresa hace y lo que espera, lo que podría dar una impresión diferente hacia los colaboradores y los aspirantes sobre lo que realmente necesita la empresa. Aunque,

es importante aclarar que dentro de sus respuestas no hacen referencia al tipo de empleado del que hablan, es decir, si es del departamento de TI o general.

- Entre los temas que las empresas encuestadas consideran que los empleados o postulantes deben saber "Mucho", están: a) los riesgos; b) la ingeniería social, la suplantación de identidad y otros temas relacionados con el manejo de información sensible; así como c) entender el impacto que trae consigo atender o desatender las tareas relacionadas con la ciberseguridad; d) y tener en claro las verdaderas necesidades de la empresa para así aprovechar al máximo el conocimiento que se tenga en este rubro.

  Estos datos permiten observar que la ciberseguridad es un tema que debe tratarse con proactividad, desde todos los niveles jerárquicos de la organización y colaborando de manera interdepartamental.

- Llama la atención que el 86.66% de las organizaciones que respondieron la encuesta mencionen que si cuentan con personal especializado en ciberseguridad a disposición de la empresa y que de éstas, el 53.33% manifieste que el personal ha sido contratado directamente por la empresa; ya que, como se mencionó antes, la mayoría de las organizaciones destina entre $1 y $400,000 pesos para el rubro de contratación de personal especializado. Esto podría indicar que, pese a que la ciberseguridad es un tema complejo que requiere de habilidades y competencias que van más allá de lo técnico, los salarios que perciben estos profesionistas aún distan de ser competitivos o lo suficientemente atrayentes para que más personas decidan enfocar sus estudios superiores en esta área.

- Si bien este estudio ha demostrado que no existe una gran diferencia entre el nivel de conocimientos que tienen los egresados de carreras altamente relacionadas con la ciberseguridad con el nivel de conocimientos que requieren los diferentes tipo de industria, es cierto que sigue existiendo un gran déficit de personas capacitadas en este tema, por tanto se vuelve necesario reflexionar sobre qué es lo que realmente hace que este problema exista y persista.
- Se recomienda realizar el cálculo del índice de consistencia KR-20 para la sección del cuestionario diseñada para medir el nivel de conocimientos sobre ciberseguridad con el que cuentan los egresados, esto con el propósito de detectar si un nivel de consistencia bajo pudiera estar generando estos resultados.
- Otra recomendación es repetir el estudio con una cantidad mayor de personas como parte de la muestra tanto con respecto a los egresados como a las empresas, ya que una muestra mayor puede dar una mejor referencia con respecto a esta situación; además, se recomienda ampliar la cantidad de dimensiones que intervienen en el estudio dado que la ciberseguridad es un tema mucho más amplio e integral.

POSIBLES APLICACIONES

1.- Artículo científico dónde se comuniquen los temas más importantes con respecto a la ciberseguridad que hace falta profundizar en futuros estudios, obtenidos del análisis bibliométrico de producción científica en México.

2.- Artículo científico o ponencia dónde se dé a conocer los resultados del análisis sobre la importancia que asigna la industria actual a los conocimientos sobre ciberseguridad con la que cuentan sus empleados del área de informática.

3.- Artículo y/o ponencia dónde se presenten los resultados obtenidos de contrastar los conocimientos sobre temas de ciberseguridad con el que cuentan los egresados que ya se encuentran laborando, de carreras afines a las tecnologías de información que estudian en las universidades seleccionadas; con las necesidades actuales de la industria.

4.- Exposición de los resultados del análisis sobre la inclusión de la ciberseguridad en la educación y la relevancia que ésta tiene en la industria.

5.- Tesis de Maestría donde se expliquen en profundidad tanto los resultados obtenidos de los análisis realizados durante la investigación como el proceso que se siguió para llegar a ellos.

REFERENCIAS

ACUERDO por el que se expide la Estrategia Digital Nacional 2021-2024. 6 de junio de 2021. DOF 06-09-2021.

Aguilar, J. F. (2021). *Ciber-resiliencia: la evolución de la ciberseguridad en 2020*. Forbes México. https://www.forbes.com.mx/red-forbes-ciber-resiliencia-la-evolucion-de-la-ciberseguridad-en-2020/

Aguilar, J. M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *Urvio. Revista Latinoamericana de Estudios de Seguridad, 25.* https://revistas.flacsoandes.edu.ec/urvio/article/view/4007

American Chamber Mexico. (2020). *Estrategia de Ciberseguridad en México Por un futuro ciberseguro*. https://www.amcham.org.mx/sites/default/files/publications/VF_Estrategia%20de%20Ciberseguridad%20en%20Me%cc%81xico%20(1).pdf

Arellano, I. (2017). La cultura sobre seguridad informática en las redes sociales: el caso de los estudiantes de la Preparatoria de San Diego Cuentla, México. *Revista Iberoamericana de las Ciencias Sociales y Humanísticas*, *6*(11). http://dx.doi.org/10.23913/ricsh.v6i11.106

Arreola, A. (2018). *Ciberseguridad Nacional en México y sus desafíos.* Academia. https://www.academia.edu/37870601/ciberseguridad_nacional_en_mexico_y_sus_desaf%C3%ADos_pdf

Arroyo, D., Gayoso, V., & Hernández, L. (2020). *Ciberseguridad.* Editorial CSIC Consejo Superior de Investigaciones Científicas.

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

Basias, N., & Pollalis, Y. (2018). Quantitative and Qualitative Research in Business & Technology: Justifying a Suitable Research Methodology. *Review of Integrative Business and Economics Research, 7*(1). http://buscompress.com/uploads/3/4/9/8/34980536/riber_7-s1_sp_h17-083_91-105.pdf

Becerril, A. (2019). La ciberseguridad en la Seguridad Nacional: amenazas y retos en el ciberespacio. *Revista de Administración Pública, 148.* https://revistas-colaboracion.juridicas.unam.mx/index.php/rev-administracion-publica/article/view/38399/35297

Bischoff, P. (2021). *Which countries have the worst (and best) cybersecurity?* Comparitech. https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

Borbón, J. (2011). Buenas prácticas, estándares y normas. *Revista Seguridad UNAM*. https://revista.seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas-est%C3%A1ndares-y-normas

Brito, B., Hernández, G., & ÁLvarez, A. (1998). Gestión tecnológica y desarrollo sostenible y solidario en los países latinoamericanos: experiencia cubana. *Revista ESPACIOS, Vol. 19(2).* http://www.revistaespacios.com/a98v19n02/40981902.html#gestion

Cano, J. (2008). Informática Forense en teléfonos celulares GSM. *Ciencia UNEMI, 1*(1). https://dialnet.unirioja.es/servlet/articulo?codigo=5210309

Cano, J. (2018). *Industria 4.0, un reto para las universidades.* El Universal Querétaro. http://www.eluniversalqueretaro.mx/metropoli/15-07-2018/industria-40-reto-de-universidadess

Castillejos, B., Torres, C., & Lagunes, A. (2016). La seguridad en las competencias digitales de los millennials. *Apertura, 8*(2). http://dx.doi.org/10.18381/Ap.v8n2.914

Chávez, G. (2019). *Invertir en estas tecnologías evitará que pagues 13 mdd por un hackeo.* Expansión. https://expansion.mx/tecnologia/2019/09/25/estas-tecnologias-evitaran-que-pagues-13-mdd-por-un-hackeo

Chávez, G. (2020). *El costo por ciberataques en México creció 38.4% en 2019.* Expansión. https://expansion.mx/tecnologia/2020/03/11/el-costo-por-ciberataques-en-mexico-crecio-38-4-en-2019

CIO México. (2020). *Ocho lecciones en ciberseguridad que nos deja el 2020.* https://cio.com.mx/ocho-lecciones-en-ciberseguridad-que-nos-deja-el-2020/

CIO México. (2021). *¿Qué esperar del mundo de la ciberseguridad en 2021?* https://cio.com.mx/que-esperar-del-mundo-de-la-ciberseguridad-en-2021/

Cisco Systems. (s. f.). ¿Qué es la seguridad de red? Cisco. https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

Columbus, L. (2020). *2020 Roundup of Cybersecurity Forecasts and Market Estimates.* Forbes. https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/?sh=58d30412381d

Committee on Payments and Market Infrastructures. (2014). *Cyber resilience in financial market infrastructures.* Bank for International Settlements. https://www.bis.org/cpmi/publ/d122.pdf

Cortés, M. (2020). *Cinco tendencias en ciberseguridad empresarial para 2021.* CIO México. https://cio.com.mx/cinco-tendencias-en-ciberseguridad-empresarial-para-2021/

Departamento de Seguridad Nacional. (2021). *España, a la cabeza mundial en Ciberseguridad*. https://www.dsn.gob.es/es/actualidad/sala-prensa/espa%C3%B1a-cabeza-mundial-ciberseguridad

Duffy, C. (2021). *Se busca: millones de expertos en ciberseguridad. Salario: lo que pidas.* CNN. https://cnnespanol.cnn.com/2021/05/30/se-busca-millones-expertos-ciberseguridad-salario-trax/

El Universal. (2019). *México invierte cada vez más en ciberseguridad empresarial.* https://www.eluniversal.com.mx/techbit/mexico-invierte-cada-vez-mas-en-ciberseguridad-empresarial

El Universal. (2020a). *La ciberseguridad no es prioridad en México.* https://www.eluniversal.com.mx/techbit/la-ciberseguridad-no-es-prioridad-en-mexico

El Universal. (2020b). *México es el segundo país con más ciberataques a negocios.* https://www.eluniversal.com.mx/techbit/mexico-es-el-segundo-pais-con-mas-ciberataques-negocios-kaspersky

Ernst & Young México. (2019). *EY invierte 40 millones de pesos en centro de ciberseguridad para Querétaro* [Comunicado de prensa]. https://www.ey.com/es_mx/news/2019/12/ey-invierte-40-millones-de-pesos-en-centro-de-ciberseguridad-par

Ernst & Young México. (2020). *EY México inaugura su Centro de Operaciones de Ciberseguridad en Querétaro* [Comunicado de prensa]. https://www.ey.com/es_mx/news/2020/01/ey-mexico-inaugura-su-centro-de-operaciones-de-ciberseguridad-en

Espinosa, E. (2015). Hacia una estrategia nacional de ciberseguridad en México. *Revista de Administración Pública, UNAM, L*(1). https://revistas-colaboracion.juridicas.unam.mx/index.php/rev-administracion-publica/article/view/19862/17821

Excelsior. (2021). *La ciberseguridad, cada vez más necesaria para organizaciones y gobiernos.* Excelsior México. https://www.excelsior.com.mx/nacional/la-ciberseguridad-cada-vez-mas-necesaria-para-organizaciones-y-gobiernos/1426942

Expansión. (2020). *Los aspectos prioritarios en ciberseguridad para 2021.* Expansión México. https://expansion.mx/bespoke-ad/2020/10/27/los-aspectos-prioritarios-en-ciberseguridad-para-2021

Expansión. (s. f.). *¿Qué es la inversión y de qué depende?* https://www.expansion.com/economia-para-todos/economia/que-es-la-inversion-y-de-que-depende.html

Frías-Navarro, D. (2022). *Apuntes de estimación de la fiabilidad de consistencia interna de los ítems de un instrumento de medida.* Universidad de Valencia. España. https://www.uv.es/friasnav/AlfaCronbach.pdf

Fujs, D., Mihelič, A., & Vrhovec, S. (2019). The power of interpretation: Qualitative methods in cybersecurity research. *Proceedings of the 14th International Conference on Availability, Reliability and Security.* https://doi.org/10.1145/3339252.3341479

Gallardo, S. (2020). Diez años más tarde. Retos y amenazas a la seguridad y ciberseguridad en 2030. *Sistemas, 155*. https://doi.org/10.29236/sistemas.n155a5

Gobierno de México. (2017). *Estrategia Nacional de Ciberseguridad.* Portal único del gobierno de México. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Grant, R. (2016). Contemporary Strategy Analysis (9.a ed.). Wiley.

Gutiérrez, E. (2020). *Plan estratégico para la creación de la unidad inteligente de ciberseguridad para la administración pública federal mexicana* [Tesis de Maestría, INFOTEC: Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación]. https://infotec.repositorioinstitucional.mx/jspui/handle/1027/424

Hassani, H. (2017). *Research Methods in Computer Science: The Challenges and Issues.* Academia. https://www.academia.edu/29605798/Research_Methods_in_Computer_Science_The_Challenges_and_Issues

Hechavarría, S. (2015). *Los tipos de escalas y ejemplos para su diseño*. Universidad Virtual de Salud. http://uvsfajardo.sld.cu/sites/uvsfajardo.sld.cu/files/tipos_de_escala_y_ejemplos_de_diseno.pdf

Hernández, M. (2018). La educación superior subalterna en México, caso del Tecnológico Nacional de México (TecNM). *Revista Conjeturas Sociológicas, 16*(6). https://revistas.ues.edu.sv/index.php/conjsociologicas/article/view/1425

Hernández, M. (2019a). *México registró 9.5 ataques de malware por segundo en 2019.* Forbes México. https://www.forbes.com.mx/mexico-registro-9-5-ataques-de-malware-por-segundo-en-2019/

Hernández, M. (2019b). *Para la ciberseguridad, no bastan inversiones millonarias para cuidar a tu empresa.* Forbes México. https://www.forbes.com.mx/para-la-ciberseguridad-no-bastan-inversiones-millonarias-para-cuidar-a-tu-empresa/

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6ta edición). McGraw Hill.

Iberdrola. (s. f.). *Características de la generación X, Y y Z.* https://www.iberdrola.com/talento/generacion-x-y-z

Instituto Federal de Telecomunicaciones. (2018). *Plan de Acciones en Materia de Ciberseguridad.* IFT. http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/upr-planaccionesciberseguridad.pdf

Instituto Nacional de Ciberseguridad. (2021). *Formación reglada en ciberseguridad en España* (Edición Noviembre de 2021). https://www.incibe.es/sites/default/files/paginas/talento/catalogos-formacion/catalogo-formacion-reglada.pdf

Kahneman, D., Lovallo, D., & Sibony, O. (2019). Un enfoque estructurado para las decisiones estratégicas. *Business Review, 293*. https://www.harvard-deusto.com/un-enfoque-estructurado-para-las-decisiones-estrategicas

La Red, D. (2017). ¿Cuáles son los métodos preferidos para el modelado de preferencias? – Estudio de la comparación entre pares frente a la valoración directa. *International Journal of Information Systems and Software Engineering for Big Companies: IJISEBC, 4*(1). https://dialnet.unirioja.es/servlet/articulo?codigo=6040459

Lee, C., & Kim, J. (2020). *Latent groups of cybersecurity preparedness in Europe: Sociodemographic factors and country-level contexts.* ScienceDirect. https://www.sciencedirect.com/science/article/pii/S0167404820302686

Lopátegui, M. (2019). *Evaluación de la estrategia nacional de ciberseguridad en México desde el enfoque CTS* [Tesis de Maestría, Universidad Nacional Autónoma de México]. http://132.248.9.195/ptd2019/mayo/0788717/0788717.pdf

López, B. (s.f.) *Las Inversiones y los inversionistas* [Archivo PDF]. http://www.economia.unam.mx/profesores/blopez/Riesgo-Pres3.pdf

López, J. (2018). Inversión. Economipedia. https://economipedia.com/definiciones/inversion.html

López, O., Amaya, H., León, R., & Acosta, B. (2002). *Informática Forense: generalidades, aspectos técnicos y herramientas.* Primer Congreso Iberoamericano de Seguridad Informática CIBSI ’02, Morelia, México. http://www.criptored.upm.es/guiateoria/gt_m180b.htm

Manterola, C., Grande, L., Otzen, T., García, N., Salazar, P., & Quiroz, G. (2018). Confiabilidad, precisión o reproducibilidad de las mediciones. Métodos de valoración, utilidad y aplicaciones en la práctica clínica. *Revista chilena de infectología*, *35*(6). http://dx.doi.org/10.4067/S0716-10182018000600680

Martínez, M. (2019). *México tendrá la demanda de 2 millones de especialistas en Ciberseguridad.* El Economista. https://www.eleconomista.com.mx/empresas/Mexico-tendra-la-demanda-de-2-millones-de-especialistas-en-Ciberseguridad-20190607-0054.html

Martínez, N., & Martínez, R. (2018). Los jóvenes y la ciberseguridad en zonas rurales del Estado de Oaxaca. Caso: Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO), plantel 165. *RECAI: Revista de Estudios en Contaduría, Administración e Informática*, *7*(20). https://dialnet.unirioja.es/servlet/articulo?codigo=6881871

Microsoft Latinoamérica. (2021). *76% de los mexicanos encuestados manifiesta estar expuesto en internet de acuerdo con el Índice de civilidad digital de Microsoft.* Microsoft News Center Latinoamérica. https://news.microsoft.com/es-xl/76-de-los-mexicanos-encuestados-manifiesta-estar-expuesto-en-internet-de-acuerdo-con-el-indice-de-civilidad-digital-de-microsoft/

Minitab. (s. f.). *Uso del valor t para determinar si se puede rechazar la hipótesis nula.* Soporte de Minitab® 20. https://support.minitab.com/es-mx/minitab/20/help-and-how-to/statistical-modeling/regression/supporting-topics/regression-models/using-the-t-value-to-determine-whether-to-reject-the-null-hypothesis/

Moreno, J., Albornoz, M., & Maqueo, M. (2019). Ciberseguridad: estado de la cuestión en América Latina. *Revista de Administración Pública, 148*. https://revistas-colaboracion.juridicas.unam.mx/index.php/rev-administracion-publica/article/view/38396/35294

Muñiz, M., Heredia, J., Valdivia, M., López, O., Arias, T., Mederos, C., & Domínguez, P. (2001). Gestión tecnológica en la producción porcina cubana. *Revista Computadorizada de Producción Porcina, 8*(3). http://www.iip.co.cu/rcpp/83/Art%C3%ADculo%206.pdf

National Research Council. 1987. Management of Technology: The Hidden Competitive Advantage. Washington, DC: The National Academies Press. https://doi.org/10.17226/18890.

Niño, V. (2011). *Metodología de la investigación. Diseño y ejecución* (1ra edición). Ediciones de la U.

Ospina, B., Sandoval, J., Aristizábal, C., & Ramírez, M. (2005). La escala de Likert en la valoración de los conocimientos y las actitudes de los profesionales de enfermería en el cuidado de la salud. Antioquia, 2003. *Investigación y Educación en Enfermería*, *23*(1). http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-53072005000100002

Otzen, T., & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *International Journal of Morphology, 35*(1). http://dx.doi.org/10.4067/S0717-95022017000100037

Papadakis V., & Barwise P. (1997) *Strategic Decisions.* Springer. https://doi.org/10.1007/978-1-4615-6195-8_1

Parraguez, L. (2017). *The state of cybersecurity in Mexico: An overview*. https://www.wilsoncenter.org/sites/default/files/media/documents/publication/cybersecurity_in_mexico_an_overview.pdf

Pérez, I. (2017). *Celebra 10 años clúster de TI en Querétaro.* CienciaMX. http://www.cienciamx.com/index.php/sociedad/politica-cientifica/13085-celebra-10-anos-cluster-de-ti-en-queretaro

Plan Nacional de Desarrollo 2019-2024. Documento rector del desarrollo nacional. 12 de julio de 2019. DOF 12-07-2019.

Plena inclusión España. (2021). *¿Qué diferencia hay entre inclusión e integración?* Plena inclusión. https://www.plenainclusion.org/discapacidad-intelectual/que-diferencia-hay-entre-inclusion-e-integracion/

PricewaterhouseCoopers. (2020). *Más del 50% de las empresas mexicanas asegura que su industria podría sufrir incidentes de ciberseguridad.* PWC. https://www.pwc.com/mx/es/prensa/2020/digital-trust.html

PricewaterhouseCoopers. (2021). *Digital Trust Insights 2021 Edición México.* PWC. https://explore.pwc.com/dti2021_mexico/ceo_ciso_ciberseguridad_mx_dti21?xs=219696

Reyes, E. (2020). *La firma EY invierte 40 mdp para dar ciberseguridad desde México.* Expansión. https://expansion.mx/tecnologia/2020/01/29/la-firma-ey-invierte-40-mdp-para-dar-ciberseguridad-desde-mexico

Rodríguez, E. & Pedraja, L. (2009). Análisis del impacto del proceso de toma de decisiones estratégicas sobre la eficacia de las organizaciones públicas. *INNOVAR. Revista de Ciencias Administrativas y Sociales, 19*(35). 33-46. https://www.redalyc.org/articulo.oa?id=81819026004

Roque, R., & Juárez, C. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. *Paakat: Revista de Tecnología y Sociedad, 8*(14). http://dx.doi.org/10.32870/Pk.a8n14.318

Rosenzweig, P. (2013). What Makes Strategic Decisions Different. *Harvard Business Review, November 2013.* https://hbr.org/2013/11/what-makes-strategic-decisions-different

Sánchez, R. (2015). t-Student. Usos y abusos. *Revista Mexicana de Cardiología*, *26*(1). https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-21982015000100009

Secretaría de Educación Pública. (2021). *TECNOLÓGICO NACIONAL DE MÉXICO (TecNM) - Ciclo escolar 2020-2021.* TecNM. https://www.tecnm.mx/menu/estadistica/basica/TecNM_2021.pdf?a=1

Soriano, R. (2019). El Tecnológico Nacional de México. Emergencia y procedencia. *Revista de la Educación Superior, 48*(192). http://www.scielo.org.mx/pdf/resu/v48n192/0185-2760-resu-48-192-119.pdf

Supo, J. (2013). *Cómo Validar un Instrumento*. https://www.cua.uam.mx/pdfs/coplavi/s_p/doc_ng/validacion-de-instrumentos-de-medicion.pdf

Tilves, M. (2019). *¿Cuál es el país que más invierte en ciberseguridad?* Silicon. https://www.silicon.es/cual-es-el-pais-que-mas-invierte-en-ciberseguridad-2403845

UNAM-CERT. (2017). La seguridad es responsabilidad de todos: Buenas prácticas para prevenir incidentes. *Seguridad. Cultura de prevención para TI, 30.* https://revista.seguridad.unam.mx/sites/default/files/revista30_0.pdf

Urcuqui L. C. C. García P. M. & Osorio Q. J. L. (2018). *Ciberseguridad: un enfoque desde la ciencia de datos.* Editorial Universidad Icesi. https://doi.org/10.18046/EUI/ee.4.2018

Valencia, A., Bermeo, M., Acevedo, Y., Garcés, L., Quiroz, J., Benjumea, M., & Patiño, J. (2020). Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico. *Revista Ibérica de Sistemas e Tecnologías de Informação, E29.* https://search.proquest.com/docview/2394537804/fulltextPDF/C7F9F769F5D84E0DPQ/1

Valle, M. (2019). *La inversión en ciberseguridad, ¿realmente está siendo efectiva?* Expansión. https://expansion.mx/tecnologia/2019/10/08/la-inversion-en-ciberseguridad-realmente-esta-siendo-efectiva

Vélez, I. (2010). *Decisiones de inversión: para la valoración financiera de proyectos y empresas.* (5a. ed.). Pontificia Universidad Javeriana.

Zurita, A. (2018). *La ciberseguridad en México ante desafíos y amenazas del siglo XXI* [Tesis de Licenciatura, Universidad Nacional Autónoma de México]. http://132.248.9.195/ptd2018/febrero/0770859/0770859.pdf