Revista de Climatología

Volumen 23 Edición Especial Ciencias Sociales

Vol. 23 (2023): 1510-1519 ISSN 1578-8768

Ciberseguridad y su relación con la empleabilidad para egresados de Ingeniería de Sistemas en una Universidad Pública

Frano Santiago Capeta Mondoñedo[1]*, Carlos Miguel Franco Del Carpio[1], Hernán Oswaldo Villafuerte Barreto[1]
Cristina Asunción Alzamora Rivero[1], Edgar Franklin Espinoza Silverio[1], Mayumi Rooshina Evaristo Cruz[1]

[1] Universidad Nacional Federico Villarreal. Perú.

*Autor para correspondencia: Frano Santiago Capeta Mondoñedo, fcapeta@unfv.edu.pe

(Recibido: 12-07-2023. Publicado: 12-08-2023.)

DOI: 10.59427/rcli/2023/v23cs.1510-1519

Resumen

La ciberseguridad es una materia que está en plena vigencia en los ámbitos empresarial, estatal, bancario, personal, que afecta directamente el resultado económico de las organizaciones, por lo tanto es muy importante que tanto las instituciones públicas y las empresas privadas tengan el recurso humano adecuado y capacitado para afrontar técnicamente los ataques cibernéticos de hackers y organizaciones internacionales dedicadas al robo, tráfico de datos y extorsión en la modalidad de secuestro de datos, es de sumo interés entonces que las universidades puedan proveer personal capacitado tanto en conceptos teóricos como en habilidades prácticas para afrontar con éxito los ciberataques, el presente proyecto ha identificado una relación directa entre la empleabilidad de un egresado de la carrera de ingeniería de sistemas y su conocimiento de ciberseguridad, siendo que las instituciones requieren profesionales capacitados desde la universidad para adoptarlos y que la curva de aprendizaje sea la menor posible, pero sin embargo en la realidad eso no está sucediendo. El estudio se llevó a cabo con egresados de la carrera de ingeniería de sistemas de la universidad y con gerentes y/o jefes de sistemas de empresas privadas y entidades del sector público, los resultados mostraron que existe una relación entre el nivel de conocimientos de ciberseguridad la empleabilidad de estos en áreas de ciberseguridad, a menor nivel de conocimientos menor nivel de empleabilidad, y en base a esos resultados se propone una línea de cursos de ciberseguridad que permita mejorar su nivel de empleabilidad y adaptarse a las necesidades de las organizaciones.

Palabras claves: *Ciberseguridad, ciberataque, protección de la información, empleabilidad.*

Abstract

Cybersecurity is a matter that is in full force in the business, state, banking, and personal spheres, which directly affects the economic results of organizations, therefore it is very important that both public institutions and private companies have the human resources suitable and trained to technically face cyber-attacks by hackers and international organizations dedicated to theft, data traffic and extortion in the form of data hijacking, it is therefore of great interest that universities can provide trained personnel in both theoretical concepts and skills practices to successfully deal with cyberattacks, this project has identified a direct relationship between the employability of a systems engineering graduate and their knowledge of cybersecurity, since institutions require professionals trained from the university to adopt them and that the learning curve be as little as possible, but nevertheless in reality that is not happening. The study was carried out with graduates of the systems engineering career of the university and with managers and/or heads of systems of private companies and public sector entities, the results showed that there is a relationship between the level of knowledge of cybersecurity the employability of these in cybersecurity areas, the lower the level of knowledge, the lower the level of employability, and based on these results, a line of cybersecurity courses is proposed to improve their level of employability and adapt to the needs of organizations.

Keywords: *Cybersecurity, cyberattack, information protection, employability.*

1. Introducción

La Ciberseguridad es una materia que está en plena vigencia en el mundo empresarial, estatal, bancario, personal, que afecta directamente el resultado económico de las organizaciones y también a nivel personal, es muy importante que tanto las instituciones públicas, empresas privadas y sobre todo la academia tengan los conocimientos adecuados y necesarios para entender la problemática y para poder tener las herramientas y conocimientos necesarios que permitan establecer medidas de protección sobre ataques de ciberseguridad. Las tecnologías de la información y las comunicaciones (TIC) han transformado las concepciones de la delincuencia organizada. En concreto, las TIC han influido en la naturaleza de las actividades de la delincuencia organizada y en los tipos de personas que pueden participar en ella. Esta transformación incluye no solo los cambios en los tipos de delitos cometidos y los modus operandi utilizados por los grupos delictivos organizados, sino también la variedad de personas que pueden participar en la delincuencia organizada.

Diversos países en el Mundo están constantemente bajo ataques de grupos organizados de ciberdelincuentes, teniendo especial incidencia las entidades públicas, las entidades del sector financiero y los sectores que manejan las infraestructuras criticas (centrales de energía, potabilizadoras de agua, control de tráfico aéreo, control de tráfico terrestre, represas, sistemas de transporte masivo, entre las principales) por lo tanto la implementación desde la academia de planes de estudio que contengan una línea de cursos sobre Ciberseguridad y que permitan brindar habilidades sobre este tema a los estudiantes se torna en muy significativo y una necesidad es así que en instituciones académicas de países más desarrollados, concretamente en los Estados Unidos tenemos una gran cantidad de universidades tanto públicas como privadas que ofrecen este grado académico (https://cybersecurityguide.org/programs/cybersecurity- bachelors-degree/#Schools), según el informe conjunto de la OEA (Organización de Estados Americanos) y el BID (Banco Interamericano de desarrollo) "Ciberseguridad, Riesgos, avances y el camino a seguir en América Latina y el Caribe" del año 2020 se ha identificado una brecha referida a la ausencia de talento humano calificado en ciberseguridad que se estima en 600,000 personas. En 2015, Frost & Sullivan (2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk) pronosticó una escasez de 1,5 millones de trabajadores a nivel mundial, para el 2020. A la luz de los acontecimientos recientes y el cambio dinámica de la industria, ese pronóstico se ha revisado a una escasez de 1,8 millones de trabajadores para 2022. Esto se refleja por el número extraordinariamente alto de empresa e instituciones que indican que no hay suficientes trabajadores en las áreas de ciberseguridad en las empresas, por otra parte Según el Dr. Edward Humphreys, especialista en ciberseguridad y coordinador del grupo de trabajo de información en gestión de sistemas de seguridad de ISO, se estima que para el año 2021 habrá hasta 3,5 millones de puestos de trabajo relacionados con la ciberseguridad que quedarán vacantes, ya que no existen suficientes profesionales preparados.

La pertinencia de este proyecto es dejar en claro que nuestra universidad debe ponerse a la vanguardia en la implementación de cursos sobre ciberseguridad, teniendo como base la amplia cantidad de conocimientos existente en esta materia y que debe ser aprovechada por los estudiantes y egresados, este liderazgo genera un ecosistema beneficioso para la facultad y por ende para la universidad pues esta será identificada como una casa de estudios que lidera este tipo de conocimientos y las entidades privadas que difunden están materias y que siempre buscan que auspiciar estas iniciativas podrán ven en nuestra universidad una institución a la que poder auspiciar entregando aportes como licencias para uso de tecnologías y visitas de docentes y especialistas. En ese sentido, el objetivo de la investigación fue, determinar la manera de como la ciberseguridad incidirá en la empleabilidad de los egresados de ingeniería de sistemas de una universidad pública.

2. Bases teóricas de la investigación

La ciberseguridad se define con la protección de los activos digitales en el ciberespacio, desde las redes hasta el hardware y la información que es procesada, almacenada o transportada por sistemas de información interconectados siendo el ciberespacio un entorno complejo resultante de la interacción entre las personas, el software y los servicios en Internet por medio de dispositivos tecnológicos conectados a redes, las cuales no existen en ningún tipo de forma física.

Según la página web de la SUNEDU, más concretamente el portal tuni.pe del sistema de información universitaria, existen solo en la ciudad de Lima veintitrés (23) universidades que ofrecen la carrera de ingeniería de sistemas, ingeniería informática, ingeniería de computación y sistemas, ingeniería de sistemas de información, ingeniería de sistemas y gestión de tecnologías de información, ingeniería de tecnología de información y sistemas, ingeniería empresarial y de sistemas, sistemas de información, tomamos una muestra representativa de 03 universidades públicas y 02 universidades privadas, al revisar y analizar sus planes de estudio se puede claramente observar la inexistencia de una línea de carrera de cursos específicos sobre ciberseguridad, existen en cada malla curricular por universidad un curso sobre materias genéricas de seguridad o seguridad y auditoria, no existiendo una línea concreta sobre cursos de ciberseguridad, siendo que dada la necesidad del mercado y de las instituciones públicas y privadas, es necesario tener una línea de cursos de por lo menos 3 cursos obligatorios y algunos

adicionales como electivos, es necesario también recalcar que en la Universidad Tecnológica del Peru, en el año 2007 se creó la carrera de ingeniería de seguridad informática y auditoria (a la fecha esta carrera ya está desactivada) existe pues por lo tanto un vacío de conocimientos, una falta de profesionales de las carreras de sistemas e informática sobre temas relacionados a ciberseguridad y son muy necesarios para el mercado laboral. Existe una iniciativa de La OEA, el Ministerio de Relaciones Exteriores, el Concytec y la Fundación Citi para capacitar a 60 estudiantes peruanos en ciberseguridad, desde el año 2017, alumnos de diferentes universidades del Peru, mediante El Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) y la Fundación Citi, junto al Ministerio de Relaciones Exteriores de Perú, y el Consejo Nacional de Ciencia, Tecnología e Innovación (CONCYTEC), iniciaron el capítulo peruano del programa internacional 'Creando una Trayectoria Profesional en Ciberseguridad, Pathways to Progress', pero esta cantidad es a todas luces insuficientes, pues como se ha demostrado los requerimientos tanto locales como internacionales son significativos.

En la actualidad existen muchos centros de enseñanza formales e informales que pretenden cubrir el vacío sobre la enseñanza de cursos de ciberseguridad, también existen casas internacionales de certificación de diversa reputación y grados de dificultad sobre cursos y programas o pseudo programas de aprendizaje, es pues en la academia en donde se debe formar la base de estos profesionales, pues el conocimiento holístico que reciben dentro de un plan de estudios o malla curricular va a permitir un mejor aprovechamiento, también existe un desconocimiento de términos que es fundamental para el mejor entendimiento de la problemática, se confunden y/o mezclan los términos de seguridad informática, seguridad de sistemas, ciberseguridad, seguridad cibernética, seguridad del ciberespacio, seguridad de la información, sistema de gestión de seguridad de la información, como si todos estos conceptos significan lo mismo, siendo que existen diferencias muy marcadas y fundamentales. Con base en ese orden de ideas, el Problema principal, se basa en ¿Determinar la manera de como la ciberseguridad incidirá en la empleabilidad de los egresados de ingeniería de sistemas de una universidad pública?, esta investigación se justifica debido a que actualmente la Universidad Nacional Federico Villarreal dentro de su plan de estudios para la carrera de ingeniería de sistemas tiene programado el curso de "seguridad de los sistemas de información" que es el único curso que trata la compleja temática de la protección de la información y ciberseguridad en las organizaciones, este curso bajo su concepción ha sido pensado para brindar materias específicas sobre cómo proteger los sistemas de información, y permiten que el estudiante luego de llevar este curso tenga un conocimiento básico de la tecnología y maneras de proteger la información, pues un solo curso es insuficiente para ello, se necesita dotar de toda una línea de cursos en los que por lo menos se dicten tres (3) cursos de esta materia y estos sean complementados con cursos electivos. Los egresados generalmente tienen un choque frontal al salir al mercado y encontrarse con las exigencias de este, sobre materias de ciberseguridad, y están en una clara desventaja con frente a otros candidatos que pueden haber financiado cursos externos o certificaciones profesionales, se debe tener en cuenta que en nuestro país existen leyes, regulación y decretos que sobre desarrollan la temática de la ciberseguridad y sientan las bases de uso y gestión, siendo que tenemos los siguiente documentos normativos:

· Superintendencia de banca y seguros (SBS) ha publicado y hecho de uso obligatorio la resolución SBS N.º 504-2021 "reglamento Para la Gestión de la seguridad de la información Y la ciberseguridad"

· Superintendencia del mercado de valores (SMV) ha publicado y hecho obligatorio Resolución SMV N.º 014-2019-SMV/01 "Reglamento de Gestión del Riesgo Operacional" el cual en el "Título III Gestión de seguridad de la información Y Ciberseguridad" desarrolla ampliamente los requerimientos técnicos y funcionales que sobre ciberseguridad deben cumplir las empresas bajo su supervisión.

· El congreso de la república ha publicado la siguiente ley: LEY N.º 30999, Ley de Ciberdefensa

· La Presidencia del Consejo de ministros (PCM) ha publicado los siguientes dispositivos legales:

-Decreto Legislativo n° 1412, decreto legislativo Que aprueba la ley de gobierno digital, en el CAPÍTULO VI SEGURIDAD DIGITAL, se abarca todos los temas referidos a la protección de la información y ciberseguridad.

-RESOLUCIÓN MINISTERIAL N.º 004-2016-PCM: Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014

Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática. Por lo tanto se puede observar que a lo largo de los últimos años el sector público ha promulgado un conjunto de leyes y dispositivos legales que obligan el cumplimiento de aspectos relacionados con la ciberseguridad, tanto en entidades del sector público como en entidades del sector privado, en donde por obvias razones se incrementan las posibilidades de trabajo para egresados que dominen estos conceptos, es pues necesario dotar al estudiante y posterior egresado con las herramientas conceptuales y metodológicas necesarias que les permitan afrontar con éxitos una entrevista laboral y como por consiguiente la obtención de una plaza laboral, pues los requerimientos de los empleadores en

ambos sectores -públicos y privados-requieren de este tipo de conocimientos. con los cursos que actualmente se dictan dentro del plan de estudios de la carrera de ingeniería de sistemas, referidos a la temática de ciberseguridad, el egresado no tiene ninguna posibilidad de competir, frente a otros candidatos que si pueden tener mejor nivel de conocimiento sobre estos temas. La importancia de este proyecto radica en la necesidad de proponer una línea de cursos sobre ciberseguridad tanto teóricos como prácticos o mejor dicho cursos de aprendizaje sobre conceptos y cursos sobre el uso de plataformas automatizadas que permiten la protección e identificación de los riesgos y vulnerabilidades de la infraestructura de una empresa.

Estos cursos deben estar enmarcados dentro de una línea de conocimiento sobre ciberseguridad, en la cual se cuente con material bibliográfico. El desarrollo de esta línea de cursos se basará en la utilización de estándares internacionales y cuerpos de conocimientos usados de manera profusa tanto internacionalmente como de manera local y estarán adaptados a los requerimientos legales vigentes (Superintendencia de Banca y Seguros, Superintendencia del mercado de valores, Presidencia del consejo de ministros). Asimismo, se demostrará que la implementación de esta línea de cursos sobre ciberseguridad en la Universidad permitirá un gran beneficio a los egresados, así como también a los estudiantes de los últimos años, quienes tienen un desfase entre los conocimientos adquiridos durante su permanencia en la universidad y los requeridos por el mercado, generando a su vez, nuevos conocimientos durante su participación en los cursos y en el desarrollo de trabajos de campo y trabajos de investigación.

3. Metodología

La Investigación fue de tipo aplicada – tecnológica, ya que se utilizó una metodología ágil en la construcción del diseño instruccional y su implementación en el marco de especialización, cuyo propósito es construir desde el conocimiento científico. En el estudio se emplearon los métodos inductivos – descriptivo, analítico y causal, procedimiento que consiste fundamentalmente en establecer la relación causa efecto, de la variable independiente (ciberseguridad) con la variable dependiente (empleabilidad) con la implementación de un diseño instruccional de una línea de cursos relacionados a la ciberseguridad contenidos en la carrera profesional de ingeniería de sistemas de la Facultad de Ingeniería Industrial y de Sistemas y su relación significativa, que permita demostrar las hipótesis planteadas.

Se utilizó como técnica la encuesta, que se aplicó a egresados de la Universidad Nacional Federico Villarreal con el objetivo de conocer su percepción sobre su conocimientos y habilidades en aspectos de ciberseguridad y protección de la información y se usó la técnica de la encuesta para los gerentes de sistemas de entidades públicas y privadas para conocer sus requerimientos de habilidades y conocimientos sobre ciberseguridad que son requeridos en sus instituciones. Frente a la problemática planteada y siguiendo las orientaciones metodológicas precisamos lo siguiente:

El Universo de la presente investigación está conformada por las empresas e instituciones públicas y privadas de la ciudad de lima que requiere contratar profesionales de ciberseguridad.

La muestra seleccionada para la presente investigación será extraída del universo y conformado por los egresados de la carrera de ingeniería de sistemas que laboran en instituciones públicas y privadas, dicha muestra será aleatoria.

Se considera a los egresados de la carrera de ingeniería de sistemas y gerentes de sistemas de entidades públicas y privadas.

El tipo de muestro que se utilizará es el Muestreo Discrecional que permitirá obtener información sobre las actividades relevantes que generan mayor valor a éstos son: las entrevistas online, cuestionarios online, revisión y evaluación de información, clasificación de documentos y creación del diseño instruccional de la línea de cursos y presentado en web.

Se utilizó como técnica la encuesta, que se aplicó a egresados de la carrera de ingeniería de sistemas de la Universidad Nacional Federico Villarreal, así como también se aplicó la encuesta a gerentes y/o jefes de sistemas de entidades del sector público y privado.

4. Resultados

Debido a una serie de importantes violaciones en la ciberseguridad que se ha registrado durante la pandemia 2020-2021, se están generando oportunidades de trabajo, debido a que estas brechas están haciendo que las empresas en nuestro país y mundialmente inviertan más en ciberseguridad, entonces pues es una ventaja el tener conocimiento y habilidades sobre ciberseguridad, ya que la escasez de mano de obra en este sector, actualmente según un informe de la consultora de recursos humanos Michael Page sobre el mercado peruano y referenciado por la revista caretas el 16 de junio del 2022 los "Países de la Comunidad Andina requerirán más de 400 mil profesionales en tecnología al 2024" (https://caretas.pe/nacional/paises-de-la-comunidad-andina- requeriran-mas-de-400-mil-profesionales-en-tecnologia-al-2024/), así como también la empresa de análisis de mercado Analytics Insight, pronostica que para el 2023, serán necesarios cubrir 10 millones de vacantes en empleos de ciberseguridad a nivel mundial, (https://www.analyticsinsight.net/analytics-insight-estimates-10-million- new-jobs-in-cybersecurity-by-2023/) , es así que empresas de magnitud global, como Microsoft anuncia campaña a nivel mundial para dotar de capacidades y habilidades en ciberseguridad a los profesionales de las ramas de ingeniería de sistemas y tecnologías en general,(https://news.microsoft.com/es-xl/cerramos-la-brecha-de- habilidades-en-ciberseguridad-microsoft-expande-sus-esfuerzos-a-23-paises/)sabedores de el déficit de estos profesionales y es necesario también mencionar que las pymes, están enfrentando una cada vez mayor frecuencia y número de ataques de ciberdelincuentes, tal como se señala en el siguiente artículo, (https://latam.kaspersky.com/blog/pymes-latam-enfrentan-creciente-numero-ciberataques/24950/?reseller=mx_jul22 pymes_awarn_ona_smm b2c_kdaily_post &utm_source=linkedin&utm_ medium=social&utm_campaign=br_jul22-pymes_ns0208&utm_content=sm-post&utm_term=br_linkedin_organic_fye208u3cec8hjn), toda esta conjunción de situaciones hace pues más que necesaria la estructuración en las carreras de ingeniería de sistemas y/o Ingeniería informática y/o Ingeniería de computación y sistemas y/o ingeniería informática y/o ingeniería de gestión de tecnologías de información de una línea de cursos sobre ciberseguridad, la cual se describe a continuación.

La enseñanza de ciberseguridad a nivel universitario debe ser vista como un conjunto de habilidades que se fundamenten en cursos funcionales (teóricos) y cursos técnicos (prácticos), pues la ciberseguridad no es algo de "escritorio" es sobre todo poseer habilidades prácticas que permitan resolver los complejos problemas referidos a la protección de los activos de organización, pero sin descuidar los marcos de trabajo(normas técnicas de uso internacional y las buenas prácticas adoptadas por las empresas a nivel global) así como tener claramente identificado que es lo que se exige en la regulación propia de cada sector y del país en general.

Los resultados permiten concluir definitivamente que los egresados no se encuentran preparados en el área de ciberseguridad y por ende su nivel de empleabilidad para ocupar cargos en instituciones que estén directamente relacionadas con la protección de la información y la ciberseguridad es muy baja, según la figura 1, de solo el 5 %.

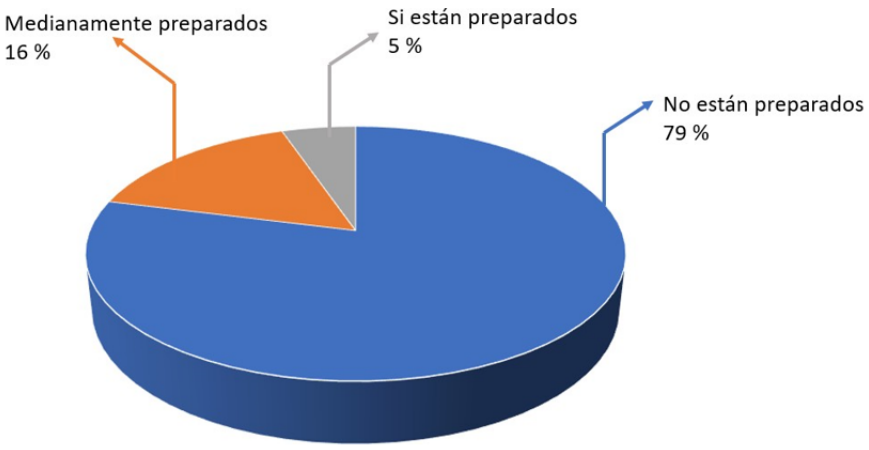

Figura 1: Nivel de preparación del egresado en el área de ciberseguridad.

De manera complementaria ante la pregunta sobre su nivel de conocimiento teórico de ciberseguridad el cual está relacionado a las metodologías, conceptos, indicadores, legislación, marcos de trabajo, se puede apreciar que el conocimiento teórico básico es bajo, en relaciona a su no conocimiento estas respuestas claramente nos permiten inferir que existe una deficiencia teórica en materia de conceptos referidos a la ciberseguridad. Como se puede observar en la figura 2.

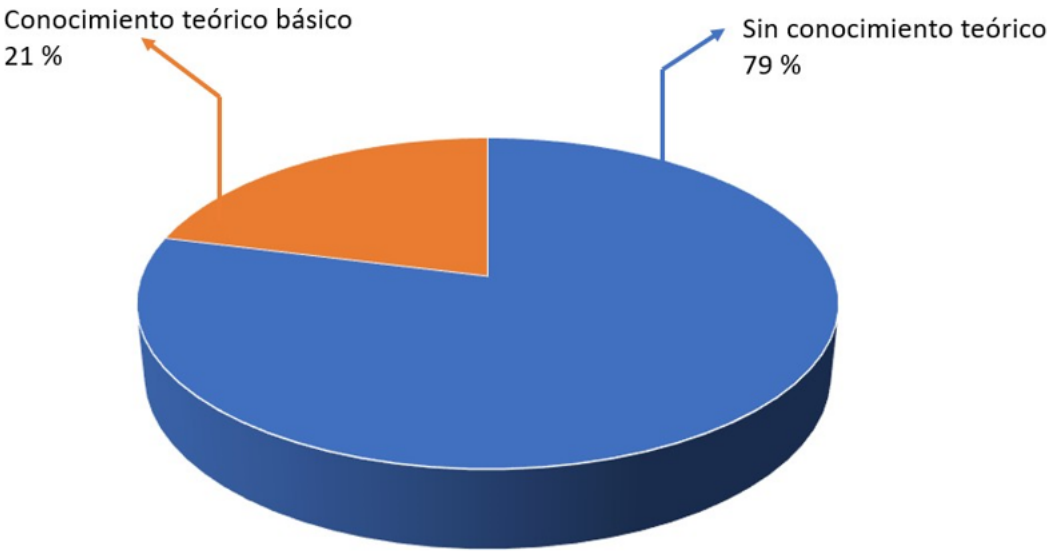

Figura 2: Nivel de conocimiento teórico.

El nivel de conocimiento practico sobre ciberseguridad, el que justamente es el más importante pues permite efectuar configuraciones en diversos equipos de protección, así como ejecutar pruebas con herramientas para identificar el nivel de protección de la infraestructura de la empresa, es ciertamente bajo el no tener habilidades prácticas en ciberseguridad, se aprecia pues la existencia de una deficiencia en habilidades prácticas. Como se puede observar en la figura 3.

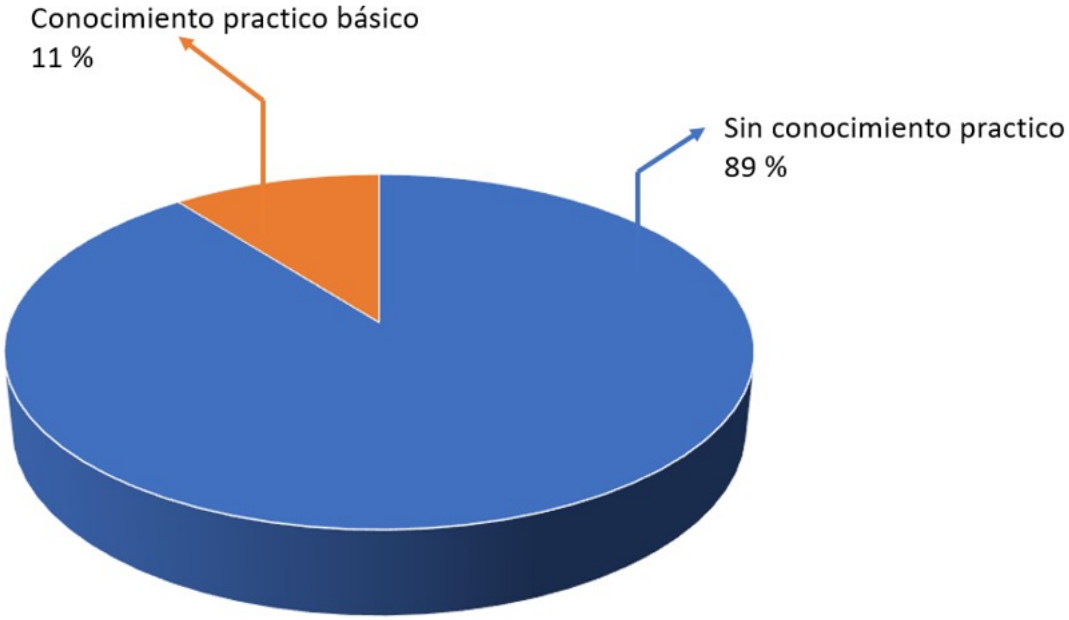

Figura 3: Nivel de conocimiento practico.

Herramientas y conocimientos requeridos

Las tecnologías de ciberseguridad son muy variadas y están enfocadas a diversos tipos de protección de la infraestructura de una institución, debido a que los ciberataques no son todos de la misma forma, se requiere por lo tanto diversas tecnologías, en la figura 4 se aprecia el orden de importancia otorgado por los gerentes de sistemas sobre 4 habilidades puntuales de carácter práctico que son requeridas en las instituciones, siendo la habilidad de análisis de vulnerabilidad la más importante.

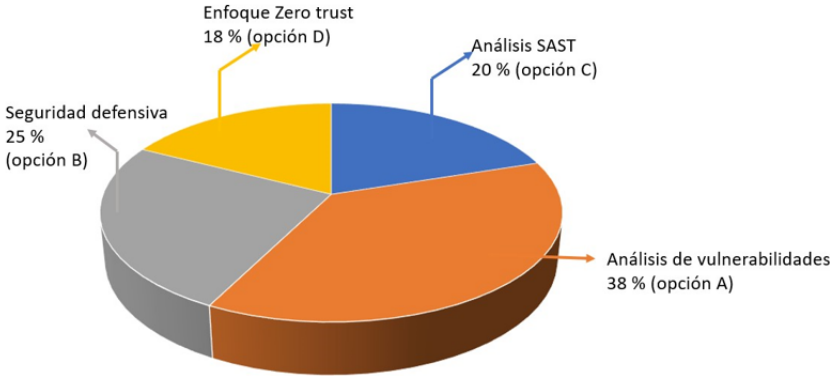

Figura 4: Orden de importancia sobre tecnologías de ciberseguridad.

En cuanto al conocimiento teórico requerido por los gerentes de sistemas al momento de contratar se observa que la arquitectura de ciberseguridad es la más importante, ello se justifica plenamente con la realidad de las organizaciones, pues el principal conocimiento teórico que requiere un egresado que va a laborar en ciberseguridad es saber cómo integrar todas las tecnologías dentro de una infraestructura y alinearla de acuerdo a lo especificado en los marcos de trabajo y estándares de ciberseguridad existentes. Como se puede observar en la figura 5.

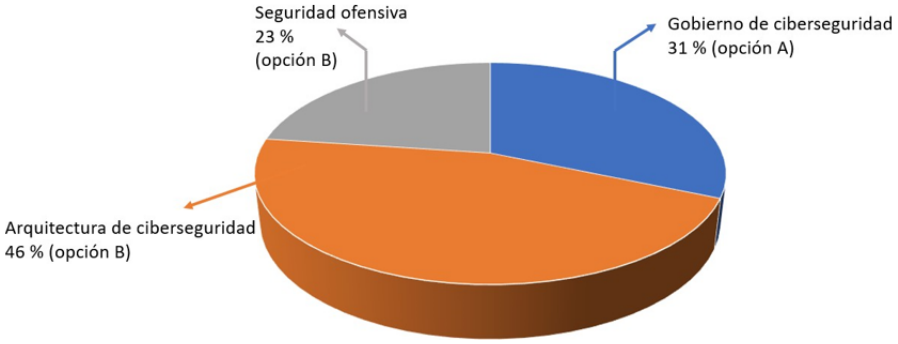

Figura 5: Orden de importancia sobre conocimientos teóricos de ciberseguridad.

Se demuestra con los resultados de la figura 6 que las empresas requieren profesionales con una combinación de conocimiento y habilidades teóricos – prácticas en ciberseguridad.

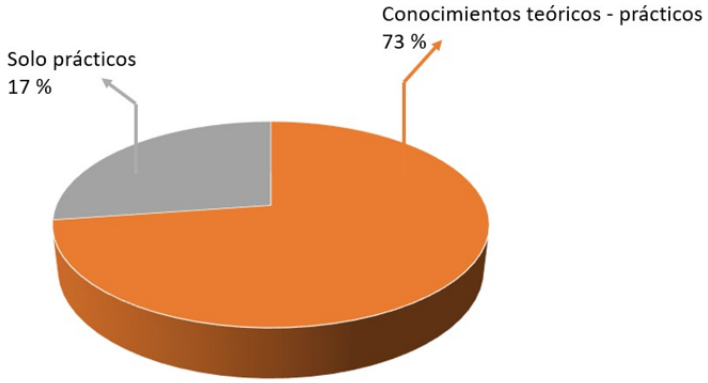

Figura 6: Tipo de conocimiento sobre ciberseguridad requerido por las empresas.

Empleabilidad y contratación de profesionales

La empleabilidad del egresado depende entre otros aspectos de sus conocimientos adquiridos tanto teóricos como prácticos, lo cual sale a relucir en una entrevista o en un examen para acceder a una posición, en ese sentido, en la encuesta dirigida a los gerentes de sistemas se incluyó una pregunta referida a si contratarían a un profesional egresado que no tenga conocimientos de ciberseguridad, una mayoría consistente indica que, si los profesionales no tienen estudios de ciberseguridad, no serían contratados, esto por la tanto hace menos empleables a los profesionales y egresados.

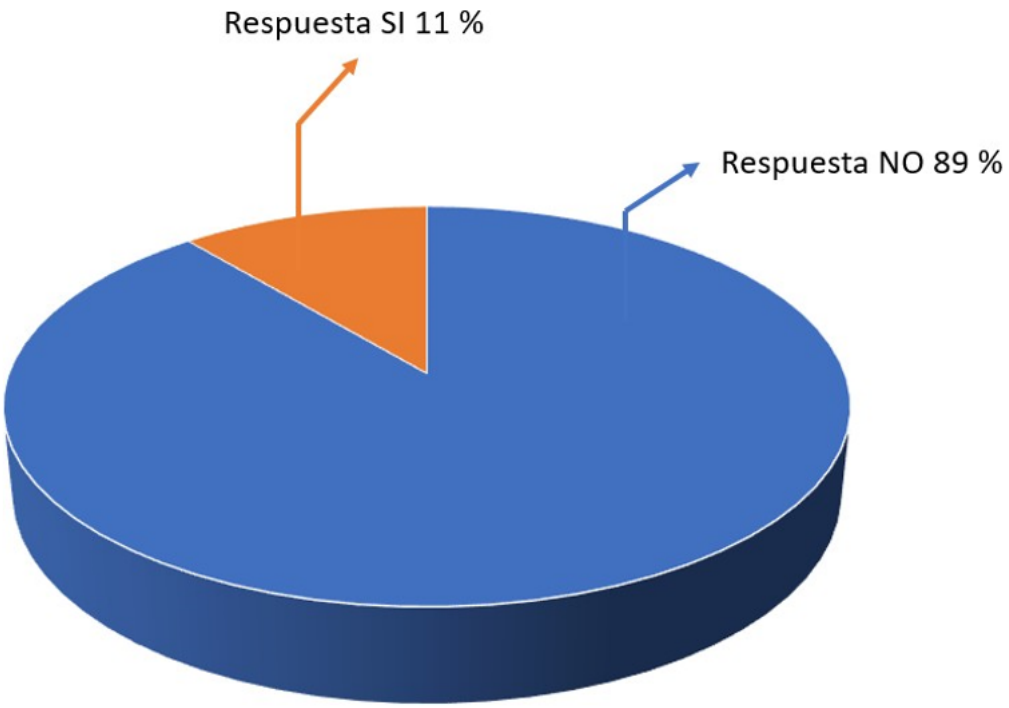

Figura 7: Nivel de aceptación y de contratación de un egresado que no tenga conocimientos de ciberseguridad.

5. Discusión

Es un hecho que durante el periodo más complejo de la pandemia en el año 2020,se origina una consolidación de una tendencia que tenía varios años gestándose, nos referimos concretamente a la transformación digital (DX), la cual estaba en muchas instituciones públicas y privadas en estado incipiente pero con la llegada de las restricciones de todo tipo durante ese periodo se tuvieron que dar grandes pasos para que dicha transformación digital se materialice, surge entonces el trabajo remoto, las video conferencias, las VPN, se consolidan los entornos de cómputo en la nube, el escritorio remoto, las aplicaciones web, las aplicaciones móviles, las conexiones API (Interfaz de programa de aplicación) que permitieron a las entidades llevar a delante su transformación, sin embargo y como pilar de esta transformación digital tenemos a la ciberseguridad, pues sin la protección de la confidencialidad, integridad y disponibilidad, no se puede pues habilitar un trabajo remoto seguro, no se puede habilitar un servicio de escritorio remoto seguro, no se pueden efectuar teleconferencias, clases virtuales seguras, no se pueden establecer conexiones seguras para los entornos en la nube, siendo pues la ciberseguridad un requerimiento indispensable para llevar adelante esas iniciativas en las instituciones, y es en ese orden de cosas en el cual se requieren cada vez más profesionales entrenados y con conocimientos de temas de ciberseguridad, no solo desde el conocimiento teórico si no también habilidades prácticas, pero sin embargo la academia no podía proporcionar estos profesionales, pues en sus planes de estudio no existen materias apropiadas a los requerimientos del mercado laboral, siendo pues que en este punto especifico en el que centro la presente investigación, estudiando la relación existente entre la ciberseguridad y empleabilidad para egresados de la carrera de ingeniería de sistemas, en el cual se demuestra al alta demanda requerida, pero esta demanda tiene que ser calificada, pues lo que las empresas necesitan es que la curva de aprendizaje sea lo más reducida posible, es entonces que la propuesta de una línea de cursos sobre ciberseguridad hace sentido tanto a los estudiantes y posteriormente egresados y a las empresas que los van a contratar.

6. Conclusiones

No existen planes de estudio adaptados a temas específicos de ciberseguridad y/o seguridad de la información, lo que existe son cursos dispersos que no permiten entregar al alumnado el conocimiento requerido que están necesitando las instituciones. Existe mucha confusión en cuanto a los temas y materias dictadas, se mezcla auditoria y seguridad, siendo cosas diferentes, se menciona seguridad informática, siendo que esta es una pequeña parte de todo el universo de la protección de la información, existen carreras de ingeniería de sistemas que directamente no dictan cursos referidos al tema de la seguridad y/o ciberseguridad. No existe pues desde la academia la oferta de profesionales que puedan directamente cubrir plazas vacantes existentes, puesto que no tienen conocimiento de la temática. También es evidente que no existen habilidades prácticas que los egresados desarrollen durante su paso por las aulas universitarias, puesto que en campo de la ciberseguridad es requerido de manera imperiosa el conocimiento de los equipos, las tecnologías y los diferentes métodos de configuración. Se pudo evidenciar mediante la encuesta dirigida a ejecutivos que tienen puestos de responsabilidad en el área de sistemas/tecnología de información, que las empresas requieren personal que tenga habilidades prácticas y el no tenerlas es una limitante para su contratación, del mismo modo se pudo conocer que las organizaciones no tienen presupuestos asignados a la capacitación de estos profesionales, por lo tanto lo que esta buscando el mercado es adoptar profesionales egresados con conocimientos y habilidades y reducir la curva de aprendizaje que siempre existente. En la encuesta dirigida a los egresados de la carrera de ingeniería de sistemas se pudo apreciar que estos consideran de valor y que el hecho de recibir formación específica teórica-practica en ciberseguridad les daría una ventaja y por ende tendrían mejores oportunidades laborales. Como resultado de la encuesta se observa que es el propio egresado que se siente y autocalifica como que no tiene un conocimiento practico ni teórico al respecto. Esta situación antes descrita origina la existencia de un mercado paralelo de dudosa reputación en la que abundan cursos de todo tipo sobre ciberseguridad los cuales son cursos independientes, orientados a ciertos conocimientos, pero no dentro de una formación integral, dando origen adicionalmente a un mercado de "certificaciones internacionales" o "pseudo certificaciones" que solamente están orientadas a obtener un beneficio económico para los patrocinadores, pero que no le garantiza al alumno ni mucho menos a las entidades contratantes que el candidato a puesto laboral tenga una preparación integral en ciberseguridad. Como producto de esta investigación se han identificado un conjunto de cursos y temas específicos de estos cursos que no están siendo desarrollados y que son claves para el adecuado aprendizaje del alumno sobre aspectos de ciberseguridad. Se han identificado un conjunto de cursos de laboratorio o cursos técnicos que no se están desarrollando y que justamente son los que el mercado requiere de profesionales egresados de la carrera de ingeniería de sistemas. Como conclusión final queda pues evidenciado que existe una relación directa entre la empleabilidad de los egresados y su conocimiento de ciberseguridad, que a mayor y mejor conocimiento se hacen más competitivos y mejora ostensiblemente su empleabilidad.

7. Referencias bibliográficas

Aguilar, E. (2016). Seguridad Informática para no informáticos. Editorial Palibrio. México.

Castro, S. (2013). Arquitectura de Seguridad Informática: Un manual para gerentes, directores y consultores. 1era edición. CreateSpace Independent Publishing Platform. USA.

Cisneros, J. (2019). Ciberseguridad para directores generales, empresarios y altos ejecutivos: Cómo minimizar los riesgos cibernéticos en su organización. Independently published. USA.

Fleitas, F. (2018). Guía fundamental en ciberseguridad: Políticas, normas, estándares y buenas prácticas en la seguridad de la información y ciberseguridad. Editorial Académica Española. España.

Jara, H – Pacheco, F (2012). Ethical Hacking 2.0. Editorial Fox Andina. Buenos Aires.

Estándar internacional Norma ISO/IEC 27032. Tecnología de la información. Técnicas de seguridad, Pautas para la ciberseguridad. Primera edición. USA.

Estándar internacional Norma ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de seguridad de información. Requisitos. Segunda edición. USA.

Estándar Internacional Norma ISO/IEC 27000. Tecnología de la información. Técnicas de Seguridad, Sistemas de gestión de Seguridad de la Información. Información general y Vocabulario. Tercera edición. USA.

Superintendencia de Educación Universitaria. Relación de carreras profesionales de las universidades del Perú.

Cybersecurity Guide, Guía online de carreras de pregrado de ciberseguridad. https://cybersecurityguide.org/programs/cybersecurity-bachelors-degree/#Schools

Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica. La OEA, el Ministerio de Relaciones Exteriores, el Concytec y la Fundación Citi capacitan a 60 estudiantes peruanos en ciberseguridad.

Reporte de Ciberseguridad 2020. Ciberseguridad, Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe. Banco Interamericano de Desarrollo.

Instituto Nacional de Normas y Tecnologías – NIST. Sitio web oficial del CSF. Disponible en: https://www.nist.gov/cyberframework/

Instituto Nacional de Normas y Tecnologías – NIST. Historia y creación del CSF.https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework

Instituto Nacional de Normas y Tecnologías – NIST. Estructura del CSF. https://www.nist.gov/cyberframework/online-learning/components-framework

Instituto Nacional de Normas y Tecnologías – NIST. Funciones del CSF.https://www.nist.gov/cyberframework/online-learning/five-functions

Instituto Nacional de Normas y Tecnologías – NIST. Evolución del CSF. https://www.nist.gov/cyberframework/evolution

Instituto Nacional de Normas y Tecnologías - NIST AWS. Cybersecurity Framework – Aligning to the NIST CSF in the AWS Cloud. https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_ CSF.246c0a886c7d16d2b370c20a04f99511d212613a.pdf