Visión Antataura
Vol.6, No.2: 103-122
Diciembre 2022-Mayo 2023
Panamá
ISSN 2520-9892

Percepción de la ciberseguridad: ciberdelitos, normas legales y políticas de seguridad

Perception of cybersecurity: cybercrimes, legal regulations and security policies

Oscar E. Rodríguez C.[1], Raúl E. Dutari D.[2], David A. Rodríguez F.[3], Libertad Fernández G. [4], Kevin J. Díaz R.[5], Juan G. Quintero P.[6], Humberto J. Chang M.[7]

[1]Universidad de Panamá, Centro Regional Universitario de Veraguas, Facultad de Informática, Electrónica y Comunicación, Panamá; oseroca.rodriguez@up.ac.pa; https://orcid.org/0000-0001-5438-8037
[2]Universidad de Panamá, Centro Regional Universitario de Veraguas, Facultad de Informática, Electrónica y Comunicación, Panamá; raul.dutari@up.ac.pa; https://orcid.org/0000-0002-7954-5999
[3]Universidad Tecnológica de Panamá, Centro Regional de Veraguas, Facultad de Ingeniería en Sistemas Computacionales, Panamá; david.rodriguez12@utp.ac.pa; https://orcid.org/0000-0002-7167-944X
[4]Universidad de Panamá, Centro Regional Universitario de Veraguas, Facultad de Administración de Empresas y Contabilidad, Panamá; libertad.fernandez@up.ac.pa; https://orcid.org/0000-0002-3705-4761
[5]Universidad Tecnológica de Panamá, Centro Regional de Veraguas, Facultad de Ingeniería Mecánica, Panamá; kevin.diaz@utp.ac.pa; https://orcid.org/0000-0001-9878-4920
[6]Universidad de Panamá, Centro Regional Universitario de Veraguas, Facultad de Informática, Electrónica y Comunicación, Panamá; juan.quinteroo@up.ac.pa; https://orcid.org/0000-0002-7308-2102
[7]Universidad de Panamá, Centro Regional Universitario de Veraguas, Facultad de Derecho y Ciencias Políticas, Panamá; humberto.chang@up.ac.pa; ; https://orcid.org/0000-0003-1126-2826

Resumen: Con el objetivo de establecer una relación entre la ciberseguridad, los ciberdelitos, las normas legales vigentes y las políticas de ciberseguridad asociados a los medios electrónicos e informáticos en Panamá, se aplicó un formulario en línea de manera remota durante los meses de junio-julio del año 2022, a los coordinadores de facultad y profesores que pertenecen a la Escuela de Informática para la Gestión Educativa y Empresarial en ocho unidades académicas, que cuentan con estudios especializados en el área de Administración de Centros de Información, Auditoría y Seguridad de Sistemas de Información. El 92.59% respondieron dicho instrumento, el cual recopiló los resultados de los años de prestaciones y servicios académicos, categoría docente y la formación académico-profesional en el área de especialidad, así como información relacionada con políticas de ciberseguridad y respaldos de información importante. Como aspecto concluyente, se determinó que el 96.96% de los encuestados está totalmente de acuerdo que se requieren de acciones de docencia en materia de políticas de ciberseguridad aplicadas al uso y manejo de los equipos informáticos, recursos tecnológicos y medios de comunicación digital.

Palabras clave: ciberseguridad, ciberdelitos, normas legales, políticas de seguridad, recursos humanos.

Abstract: The objective of the study is to establish a relationship between cybersecurity, cybercrimes, current legal regulations and cybersecurity policies associated with electronic and computer media in Panama, an online form was applied remotely during the months of June-July year 2022, to the faculty coordinators and professors who belong to the School of Informatics for Educational and Business Management in eight academic units, and who have specialized studies in the area of Administration of Information Centers, Auditing and Security of Information Systems. A percentage 92.59% responded to this instrument, which compiled the results of the years of academic benefits and services, teaching category and academic-professional training in the specialty area, as well as information related to cybersecurity policies and backups of important information. As a conclusive aspect, it was determined that 96.96% of the respondents fully agree that teaching actions are required in terms of cybersecurity

Fecha de recepción: 06 de septiembre de 2022 *Fecha de aceptación: 09 de noviembre de 2022*

policies applied to the use and management of computer equipment, technological resources and digital media.

Keywords: cybersecurity, cybercrimes, legal regulations, security policies, human resources.

1. Introducción

Cada vez es más difícil ignorar la importancia, trascendencia y aplicación de la seguridad, en cada una de las actividades que realizamos en nuestro diario vivir; sin embargo, olvidamos que el concepto de seguridad se remonta hasta los primeros relatos de la existencia del hombre. Por lo que, la seguridad es una de esas palabras con la que se convive de manera transparente; y que, en segundo plano forma parte del desarrollo social y evolución de la humanidad.

Las primeras formas de registro de su presencia, se remontan a los tiempos de las cavernas, en las cuales se evidenció su significado a través de las diversas pinturas rupestres encontradas en distintos lugares del mundo; por lo cual, dicho concepto en primera instancia se vinculó de manera casi obligatoria a la preservación de la vida y la relación familiar, a la conservación de los alimentos y bienes materiales.

Hoy queda claro que la seguridad es dinámica y que evoluciona junto al desarrollo de la sociedad, y que, en su proceso de avance dejó atrás aquella primera idea expuesta y diversificó sus orientaciones a otros campos del quehacer humano; lo que ha permitido comprender el cambio sustancial desde sus inicios hasta la actualidad y de sus distintas aplicaciones (Instituto Nacional de Ciberseguridad de España, 2022).

En ese mismo orden de ideas, el concepto de seguridad involucra una serie de aspectos, elementos y circunstancias actualizadas al entorno ya que se considera como un estado o sensación que produce la percepción de ausencia de amenazas que coloque en riesgo la existencia, la propiedad, los intereses, los valores o el particular modo de ser de quien percibe (van Woudenberg y O'Flynn, 2022).

Un hito en el ámbito informático que se considera como punto de partida en este proceso, fue la aparición de la llamada red de redes, Internet; y que surgió a finales de los años sesenta, con una propuesta financiada por el Pentágono a través de su Advanced Research Projects Agency Network (más conocido por su acrónimo ARPANet), involucrando desde sus inicios el apoyo de varias universidades en los Estados Unidos (Universidad de California (UCLA), el Instituto de Investigación de Stanford, la

Universidad de California en Santa Bárbara (UCSB) y la Universidad de Utah (Tanenbaum et al., 2021).

Por otro lado, y muy de cerca a estos primeros acontecimientos, el advenimiento de las Tecnologías de Información y Comunicación en la década de los noventas, dio inicio a una serie de transformaciones sociales que trascendieron a muchas actividades empresariales, institucionales y personales, permitiendo nuevas oportunidades de acceso a innumerables sitios web, fuentes de información y recursos disponibles sobre la red internet; pero también, dando margen a la presencia de nuevas conductas no reguladas en este entorno digital (Ghonge et al., 2022).

Sin embargo, los ataques del 11 de septiembre de 2001 se presentaron como acontecimientos que elevaron el nivel de la seguridad y a su vez, marcaron la historia con hechos trágicos que desencadenaron muchas acciones en miras a la protección de la vida, de la información y de la seguridad nacional (Marín, 2017).

Queda claro y la historia lo demuestra que, estos hitos marcaron un antes y un después en la comprensión, interpretación, ejecución e importancia de la seguridad, como medio y escudo ante situaciones que surgen bajo el contexto de las redes informáticas, de las nuevas tecnologías, del ciberespacio y del entorno web; ya que su presencia incide en el DoS y DDoS, desarrollo y transformación social en un mundo digital.

Bajo la perspectiva anterior, se conjugan un sinnúmero de circunstancias que transgreden directamente sobre la seguridad en el ciberespacio y entorno web; dentro de los cuales prevalecen el acceso ilícito a los medios informáticos a través de la web, la interceptación, ataques a la integridad y conservación de los datos y de los sistemas, el acceso a los dispositivos tecnológicos vía web, acceso a las redes inalámbricas, falsificación, fraude informático sobre internet, pornografía infantil y las infracciones de la propiedad intelectual digital, entre otros eventos que se suscitaban a nivel mundial; por ello, se firma por los Estados miembros del Consejo de Europa y demás miembros signatarios, un Convenio sobre la Ciberdelincuencia el 23 de noviembre de 2001 en Budapest (Fratti, 2018).

Aunado a lo anterior, la disrupción producto de la pandemia COVID-19, aceleró en gran medida las acciones que se desarrollaban, ya que aumentaron los desafíos en materia de ciberseguridad, lo que provocó la revisión de las medidas de mitigación,

políticas de seguridad, estrategias y las normas legales asociadas a las actividades que día a día se realizan sobre la red internet; y como parte del diario vivir, el uso masivo de las redes sociales y el desarrollo y aplicación de un sinnúmero de apps para dispositivos móviles personales, lo que aumentó la incidencia de conductas delictivas, hechos ilícitos y de nuevas estructuras dogmáticas del delito a través de éstos entornos y medios digitales (Agustina, 2021).

Contextualizando esta definición, la cual trasciende más allá y se establece que los delitos a nivel informático que sean realizados propiamente dentro de la web, Alexandrou (2022), establece y aplica el concepto de ciberdelitos, los cuales describen de forma genérica los aspectos ilícitos cometidos en el ciberespacio; y que tienen cuatro características específicas: se cometen fácilmente, requieren escasos recursos en relación al perjuicio que causan, pueden cometerse en una jurisdicción sin estar físicamente y se benefician de lagunas de punibilidad y vulnerabilidades legales que pueden existir en determinados Estados (Pons, 2017).

En Panamá, el Código Penal actualizado al 2019, establece en su artículo 4 que, solo se puede castigar a la persona por la comisión del hecho ilícito, siempre que la conducta esté previamente descrita por la ley penal (Ministerio Público de Panamá, 2019). En consecuencia, la República de Panamá reporta un aumento en denuncias por el delito contra la seguridad informática y medios tecnológicos, donde el incremento del 2016 a la fecha, ha sido de 421%, siendo estos los años 2020 y 2021 los de mayor incidencia de casos (Ministerio Público de Panamá, 2021). Aunado a esto, según las estadísticas, se reportaron 715 casos de delitos contra la seguridad jurídica de los medios electrónicos (Ministerio de Seguridad Pública, 2021).

Extrapolando esta definición y acciones delictivas al contexto de Internet, de la web y de las tecnologías de la información y comunicación, el nuevo concepto que envuelve los procesos, actividades, acciones, aspectos técnicos de funcionamiento, transmisión de información, tecnologías emergentes, movilidad y acceso al ciberespacio; se denomina ciberseguridad, la cual en su primera aproximación conceptual señala que se necesita el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad, en el contexto de una realidad digital y de información instantánea (Santos, 2022).

También Kremling y Sharp (2018), señalan que la ciberseguridad abarca las medidas sobre las funciones vitales para la sociedad y la infraestructura crítica, que tienen como objetivo lograr la capacidad de gestión predictiva y, en su caso, tolerancia a las ciberamenazas y sus efectos que pueden causar un daño o peligro significativo para un país o su población.

De igual forma y asociado a lo anterior, se destaca que la ciberseguridad teórica (como rama propuesta de la ciberseguridad), utiliza abstracciones de tecnologías, sistemas y organizaciones reales para racionalizar, explicar e innovar en el cuerpo de trabajo y conocimiento en materia de ciberseguridad (Oakley et al., 2022).

Lo expuesto deja en evidencia que se requiere de profesionales idóneos (recursos humanos) en materia de ciberseguridad, por lo que la capacitación surge como la estrategia adecuada para el desarrollo del proceso de enseñar, adiestrar, instruir y preparar a los profesionales (nuevos o activos), en las competencias necesarias para analizar y comprender los riesgos, amenazas y vulnerabilidades, producto de la presencia y actividades desarrolladas en el entorno digital, de la web y del ciberespacio (Skulmoski, 2022).

Como objetivo y aspecto prioritario del estudio, se propone establecer una relación entre la ciberseguridad y los ciberdelitos, las normas legales panameñas vigentes que se vinculan a éstos; además de las políticas de seguridad que minimicen los eventos en esta materia y la importancia del respaldo de la información asociados a los medios electrónicos, dispositivos informáticos y recursos tecnológicos, dentro del contexto de internet y acceso a la web.

Esta es una valiosa oportunidad para enfatizar la gran importancia, utilidad e implementación de nuevos procedimientos en materia de ciberseguridad, como estrategia ante los diversos ciberdelitos que día a día se llevan a cabo sobre la red internet; y a su vez, hacer docencia en materia legal y sobre todo de la puesta en práctica de nuevas políticas de seguridad en la llamada nueva normalidad social, en un mundo cada vez más digital.

2. Materiales y métodos

Las instituciones de educación superior en Panamá, al igual que otras entidades dedicadas a la capacitación y adiestramiento profesional, adecuan sus esfuerzos en

miras a formar profesionales que, según las necesidades del contexto laboral, académico, tecnológico, científico y social, actualicen las competencias para enfrentar un mundo digital, que presenta un sinnúmero de aspectos y características cada vez más cambiantes.

En ese orden de ideas, la Facultad de Informática, Electrónica y Comunicación de la Universidad de Panamá, cuenta en el Departamento de Informática con profesionales especializados en el área de Administración de Centros de Información, Auditoría y Seguridad de Sistemas de Información (Universidad de Panamá, 2022), lo que permite contar con docentes que ejercen su praxis educativa en asignaturas de esta área.

Lo antes expuesto permite desarrollar una investigación de tipo exploratoria, descriptiva, no experimental, que se realizó en ocho unidades académicas a nivel nacional, por lo que, al aplicar el concepto de población al estudio, se define como la colección completa de todos los elementos a estudiar (Metcalfe et al., 2019); y que a su vez, presenta en su totalidad tanto de los sujetos seleccionados, como los aspectos u objetos de estudio dentro de la población. Sin embargo, Chaudhuri, (2019) define dicho concepto como la totalidad de los elementos o individuos que tienen ciertas características similares y sobre las cuales se desea hacer inferencia o bien, es la unidad de análisis del estudio.

Al conocer la población encuestada (27 docentes), se efectuaron los cálculos estadísticos para determinar la muestra por accesibilidad en atención a la cantidad de profesores previamente señalada. La muestra es en esencia, parte de un subgrupo o subconjunto de la población estudiada; a la que pertenecen ese conjunto definido como profesores al que llamamos población (Chaudhuri y Pal, 2022).

Existen diferentes procedimientos estadísticos para determinar y establecer el tamaño requerido de la muestra, que se debe extraer de la población de profesores encuestados; lo cual se fundamenta en las siguientes fórmulas (Hernández-Sampieri y Mendoza, 2018).

1. $n' = \frac{P(1-P)}{V^2} = \frac{P(1-P)}{(se)^2}$
2. $n = \frac{n'}{1 + \frac{n'}{N}}$
3. $S = se = V$

Donde se consideró:

$n =$ Tamaño de la muestra ajustada.

$se = 0.06 = 6\% =$ Error estándar establecido por los investigadores.

$P = 0.5 = 50\% =$ Probabilidad de ocurrencia de que el elemento seleccionado en la población, presente el atributo de interés en la encuesta (sin premuestreo) (Triola, 2018).

Sustituyendo los valores conocidos, se obtiene que el tamaño de la muestra ajustada es:

$$n = 19.4412 \approx 20$$

Es importante señalar que, respondieron 25 de ellos, lo que representó un 92.59% de la población total investigada; es decir, se deben muestrear al menos a 20 profesores de la población total de 27 miembros. En consecuencia, dado que el formulario fue respondido por 25 docentes, se puede establecer que el tamaño mínimo de la muestra es inferior a la cantidad de profesores que respondieron dicho instrumento; lo que significa, que se trabajará con un tamaño de muestra mayor que el mínimo requerido, lo que se expresa de la siguiente manera (Rodríguez et al., 2021).

$$\#(PT) = 27, \#(TMM) = 20, \#(PE) = 25$$

$$\therefore$$

$$\#(TMM) \leq \#(PE) \leq \#(PT) \quad \wedge \quad \forall p_{TMM} \in \{TMM\}, p_{TMM} \in \{PE\}$$

Por otro lado, el instrumento diseñado para la recolección de la información, se aplicó en línea de manera remota y fue estructurado a través de 11 ítems; para los cuales se utilizó la escala de Likert con la intencionalidad de recabar la mayor cantidad de opiniones sobre el tema de investigación.

Para el análisis estadístico de los datos, se utilizó la plataforma de software IBM SPSS Statistics, la cual ofrece un amplio análisis estadístico, facilidad de uso y gran flexibilidad para el manejo de los datos. También es importante señalar, que dicho instrumento fue validado por tres profesores especialistas en Metodología de la Investigación, y se realizó una prueba piloto con otros docentes del Centro Regional Universitario de Veraguas.

El instrumento aplicado, se estructuró para determinar en primera instancia aspectos académicos de los encuestados y luego, se organizó las preguntas en materia de ciberseguridad asociados a uso, manejo de los equipos informáticos, recursos

tecnológicos y a los medios de comunicación digital, adicional al proceso de seguridad y respaldo de información.

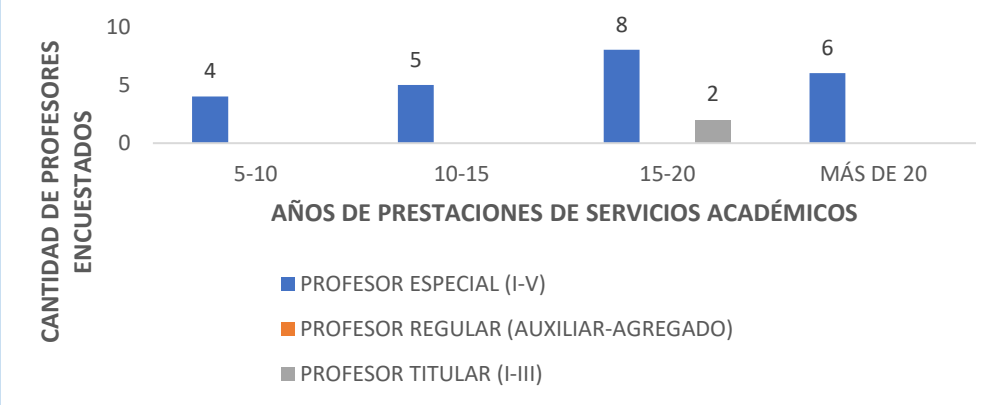
Se investigaron y analizaron cuatro (4) aspectos fundamentales y referentes principales en este estudio: (a) políticas de seguridad en el uso y manejo de equipos informáticos, recursos tecnológicos y medios de comunicación digital, (b) aspectos legales tipificados en la leyes, códigos y demás normas penales asociadas a los delitos contra la seguridad jurídica de los medios electrónicos en Panamá, (c) aspectos relacionados al incremento de los ciberdelitos y, (d) los métodos y procedimientos aplicados al respaldo de información y copias de seguridad.

Con base en los planteamientos de Torgerson y Iannone (2020), con respecto a "The success case method" se diseñó un sistema de evaluación para identificar el nivel de importancia y el índice de criterios (IC), como elementos básicos del estudio.

3. Resultados y discusión

Cada respuesta y resultado obtenido a través del instrumento aplicado en línea y de forma remota a los profesores especialistas en el área de Administración de Centros de Información, Auditoría y Seguridad de Sistemas de Información, permite hacer el análisis de los datos recopilados según sus prácticas profesionales y formación académica en materia de ciberseguridad; por lo que, en primera instancia se vincula su experiencia docente, años de servicios y prestaciones académicas, y su relación a su categoría docente actual, como se observa en la figura 1.

Figura 1. Años de prestaciones de servicios académicos, según categoría docente



Fuente: Los autores.

Los resultados obtenidos son muy claros y señalan que 21 (84.0%) de los encuestados, evidencian tener más de 10 años de servicios académicos y que

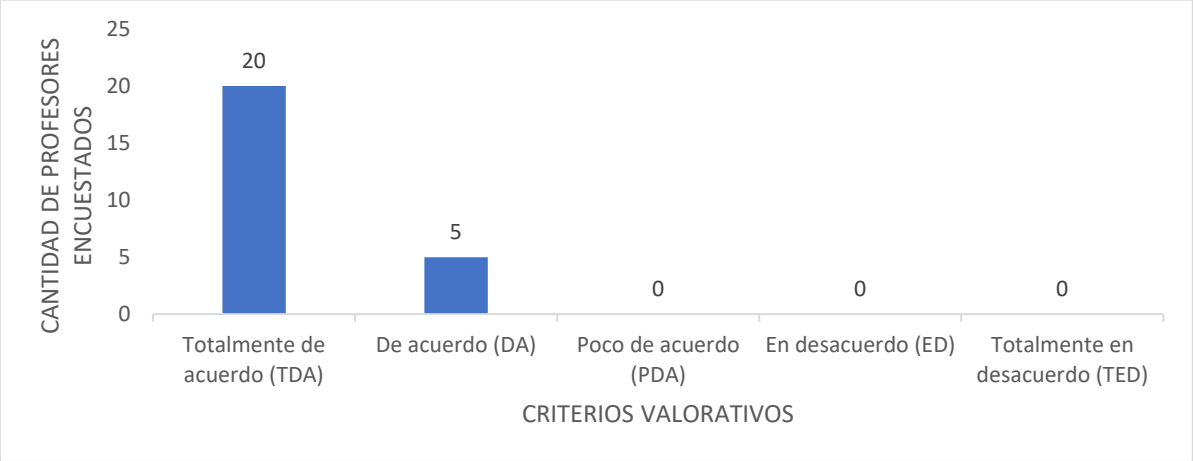
corresponden a la categoría de profesores especiales (nombrados por resolución y se incluyen dos profesores regulares); lo que asegura que son docentes que ya tienen ciertas experticias en la administración de las asignaturas y del contenido teórico-práctico que imparten en el área de investigación.

Aunado a lo anterior, un aspecto fundamental y que desde hace varias décadas se ha venido señalando, es la relación de la experiencia docente, perfeccionamiento, mejoramiento académico y capacitación profesional, de la persona que enseña a nivel superior, como lo destaca SUMMA (2021); ya que, tiene exigencias muy específicas y particulares, y más por el contexto tecnológico donde se desarrolla.

Es muy importante señalar, que el recurso humano profesional del sector tecnológico, debe considerar que la capacitación es un proceso educativo de corto plazo, continuo y dinámico, y que, aplicado de manera sistemática y organizada, desarrollan habilidades y competencias en función de objetivos bien definidos en el área de ciberseguridad (Chiavenato, 2019).

Por otro lado, entrando en los detalles vinculantes a los aspectos de la ciberseguridad, se investigaron los criterios valorativos y la importancia de realizar acciones de docencia en materia de políticas de ciberseguridad en el uso y manejo de equipos informáticos, recursos tecnológicos y medios de comunicación digital; como se muestra en la figura 2.

Figura 2. Criterios valorativos aplicados a las políticas de ciberseguridad



Fuente: Los autores.

Es significativo destacar que 20 (80.0%) de los profesores, están totalmente de acuerdo y si consideramos las respuestas del resto; o sea, 5 (20.0%) que están de

acuerdo, inferimos que en su totalidad dan mucha importancia al proceso de docencia de las políticas de ciberseguridad en el entorno digital.

Destaca Reznik (2022), que una política de seguridad define los objetivos y elementos de un sistema informático y del funcionamiento de las redes de computadoras en una organización, ya que dan seguimiento al flujo de datos a través de éstas; lo que resalta la gran importancia y trascendencia de las políticas de seguridad como primer anillo de protección contra los ciberdelitos que se desarrollan y llevan a cabo en el contexto de la web, de internet y de las redes informáticas.

Dado la importancia de las respuestas que se obtuvieron en cada pregunta del formulario aplicado, se establece el denominado índice de criterio (IC , por sus siglas en español), del cual Fernández et al. (2020), define como la operación matemática asociada al producto del valor de una métrica, por el total de respuestas obtenidas en ese criterio, y su posterior división entre el total de la población encuestada; dicho de otra forma:

$$\forall IC_j \in N, N, 1 \le j \le 5, \forall k \in N, 1 \le k \le CDE, IC_j = \frac{\sum_{k=1}^{CDE} C_{j,k}}{CDE}$$

Empleando la ecuación para calcular el índice de criterio (IC_1), a los resultados obtenidos en la figura 2, se puede representar de forma matemática de la siguiente manera:

$$IC_1 = \frac{\sum_{k=1}^{CDE} C_{1,k}}{CDE} \quad \therefore \quad IC_1 = 4.0$$

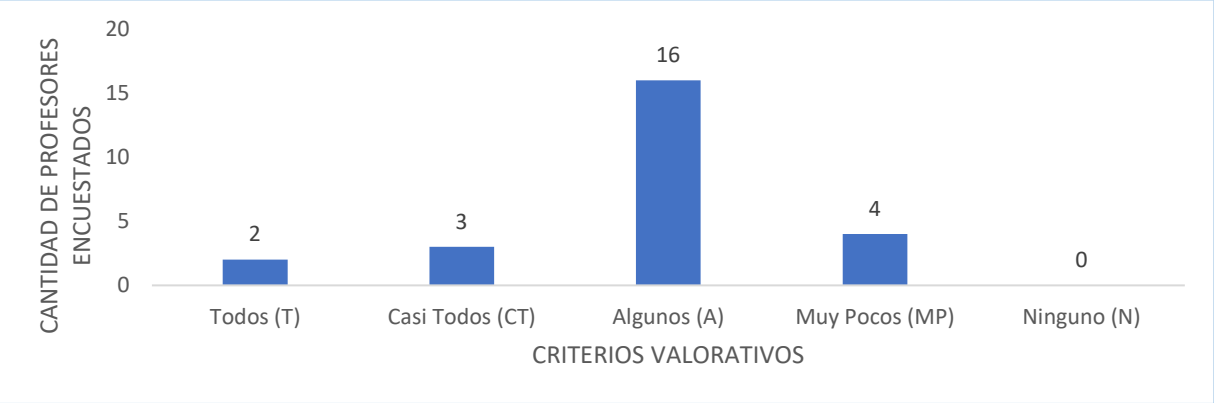
En la figura 3, se exponen los resultados obtenidos para los índices de criterios (IC_1) de cada respuesta obtenida, según los datos presentados en la figura 2.

Figura 3. Índice de criterios (IC_1)

Fuente: Los autores.

Profundizando en el análisis de las respuestas obtenidas, en el siguiente ítem del formulario aplicado, se investigó si conocían los aspectos legales tipificados en las leyes, códigos y demás normas penales asociadas a las actividades y delitos contra la seguridad jurídica de los medios electrónicos en Panamá, por lo que se obtuvieron las siguientes respuestas como se observa en la figura 4.

Figura 4. Aspectos legales de la seguridad jurídica de los medios electrónicos



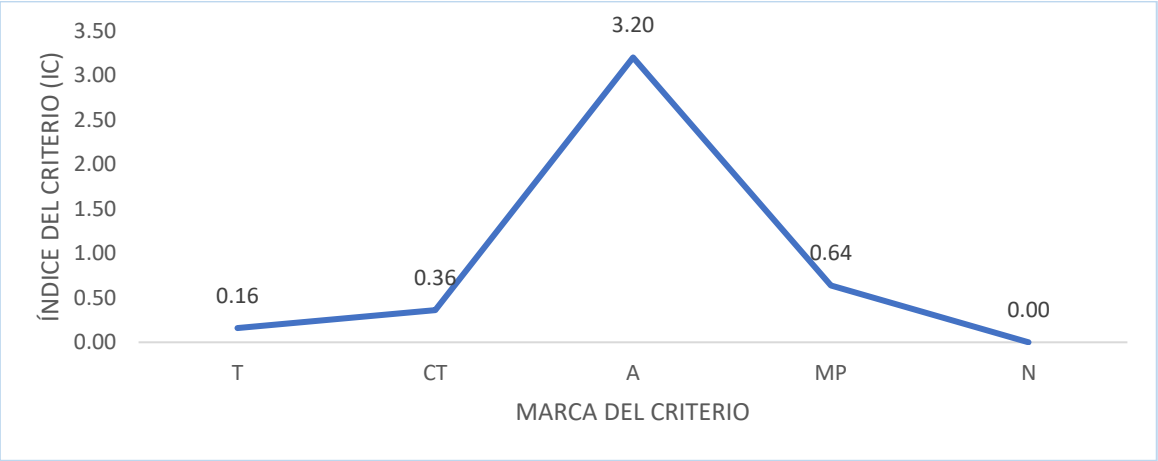
Fuente: Los autores.

Los resultados alcanzados sustentan que 20 (80.0%) de los encuestados, reconocen algunos y muy pocas de las normas legales asociadas a los medios electrónicos en Panamá; lo cual es muy preocupante, ya que pone en evidencia el gran desconocimiento de las normas legales en materia de los delitos contra la seguridad jurídica de éstos.

Aplicando la fórmula para determinar el IC_2, se obtienen los siguientes resultados como se muestran en la figura 5.

$$IC_2 = \frac{\sum_{k=1}^{CDE} C_{2,k}}{CDE} \qquad \therefore \qquad IC_2 = 3.20$$

Figura 5. Índice de criterios (IC_2)

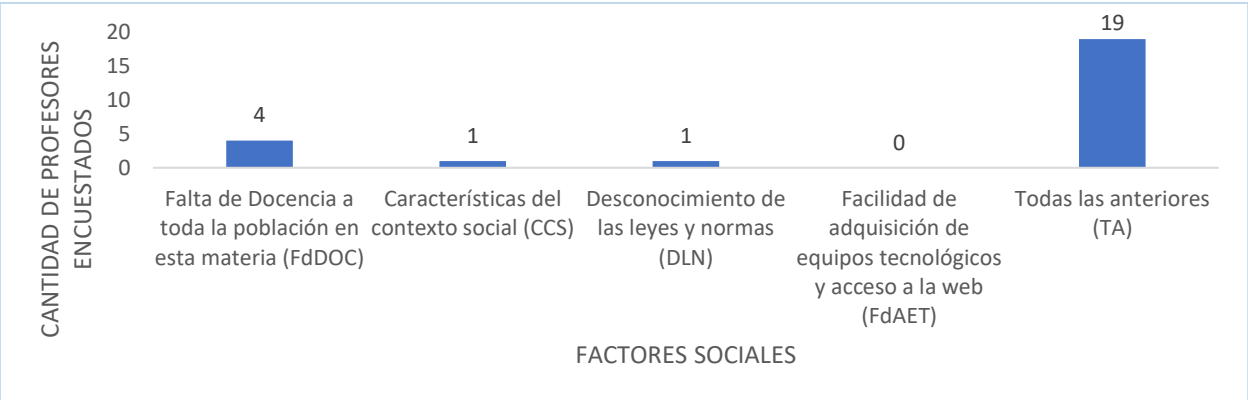


Fuente: Los autores.

Solo al conocer algunos de los aspectos legales en materia de la seguridad jurídica de los medios electrónicos, resulta muy interesante considerar como principio del derecho ignorantia legis non excusat y su asociación con la enseñanza de la seguridad de los medios electrónicos, redes de computadoras, las tecnologías informáticas actuales y los ciberdelitos, como elementos teóricos y prácticos fundamentales propios del concepto de ciberseguridad.

Otro tópico de suma importancia y que forma parte esencial en el proceso de investigación, fue lo referente a los aspectos y factores sociales que tienen mayor incidencia en el incremento de los ciberdelitos en nuestra provincia/región/país; por lo que, se identificaron cuatro áreas temáticas que son muy importantes y que se pueden asociar a tales actividades, como se presenta en la figura 6.

Figura 6. Factores sociales de mayor incidencia



Fuente: Los autores.

Es evidente señalar que el 76.0% de los profesores, (19 de ellos), respondieron fuerte y claro que en conjunto estas cuatro áreas temáticas, tienen un alto porcentaje de vinculación con la práctica de conductas no legales asociadas en una primera aproximación a los ciberdelitos. De igual forma, el 16% de los encuestados (4 participantes), reiteran la falta de docencia en materia de seguridad de los medios informáticos y electrónicos; lo que conlleva con urgencia notoria el desarrollo de una cultura de ciberseguridad.

Cabe reiterar que es aquí donde las políticas de seguridad juegan un papel muy importante vinculado a estas áreas temáticas, ya que toda política requiere de un propósito, un ámbito de acción y un responsable para su desarrollo y ejecución (Santos, 2019).

Consecuentemente, empleando la ecuación para calcular el IC_3, se alcanzan los siguientes resultados como se exponen en la figura 7.

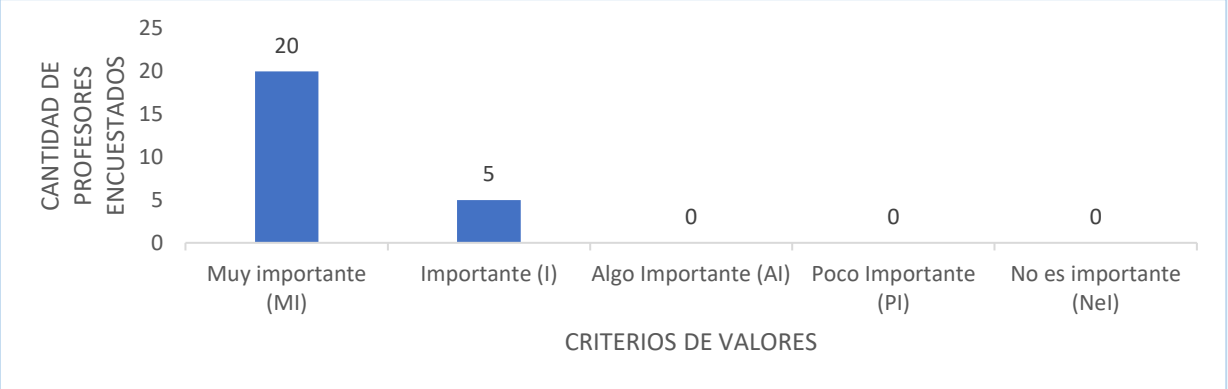
$$IC_3 = \frac{\sum_{k=1}^{CDE} C_{3,k}}{CDE} \quad \therefore \quad IC_3 = 4.75$$

Figura 7. Índice de criterios (IC_3)

Fuente: Los autores.

Otro aspecto investigado y que cada vez más cobra realce a nivel del uso y manejo de los equipos informáticos y dispositivos electrónicos, se vincula a la aplicación de las políticas y procedimiento para el respaldo de la información digital y copias de seguridad; por lo que, 80.0% de los encuestados (20), señalan que es muy importante y 20.0% (5) que es importante, realizar con cierta periodicidad dicho proceso, como se observa en la figura 8.

Figura 8. Respaldo de la información y copias de seguridad

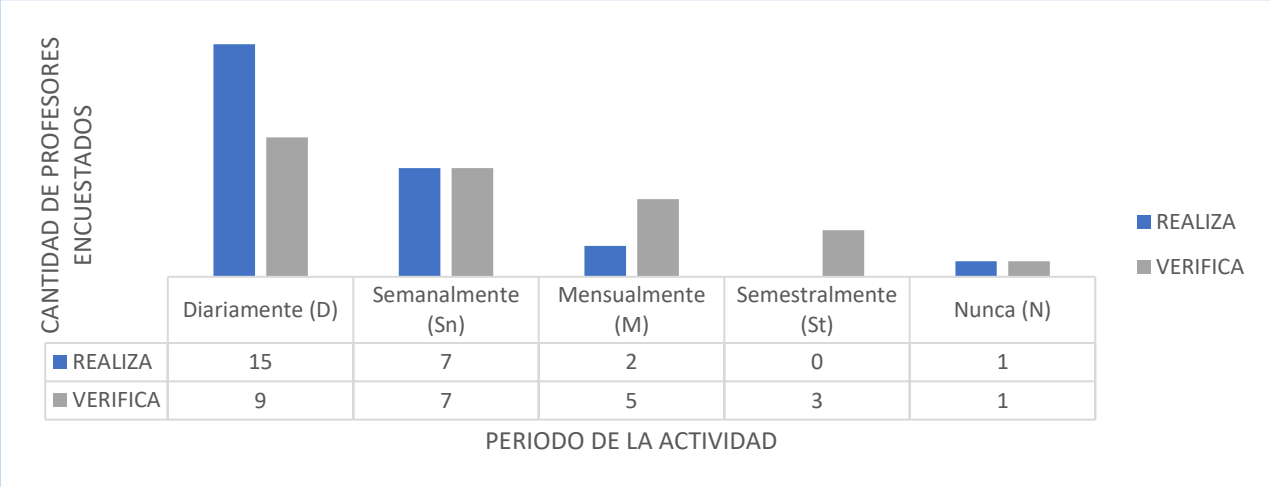


Fuente: Los autores.

Destaca Melone (2021), que el respaldo y la seguridad de la información se vincula a la preservación de la confidencialidad, integridad y disponibilidad de la información; además de otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad, que también pueden estar involucradas.

Derivado de la pregunta antes realizada y de las respuestas obtenidas, se indagó sobre la periodicidad con la cual Realizan y Verifican el respaldo de información y copias de seguridad; por lo que se obtuvieron las siguientes respuestas como se evidencian en la figura 9.

Figura 9. Respaldo de la información y copias de seguridad



	Diariamente (D)	Semanalmente (Sn)	Mensualmente (M)	Semestralmente (St)	Nunca (N)
REALIZA	15	7	2	0	1
VERIFICA	9	7	5	3	1

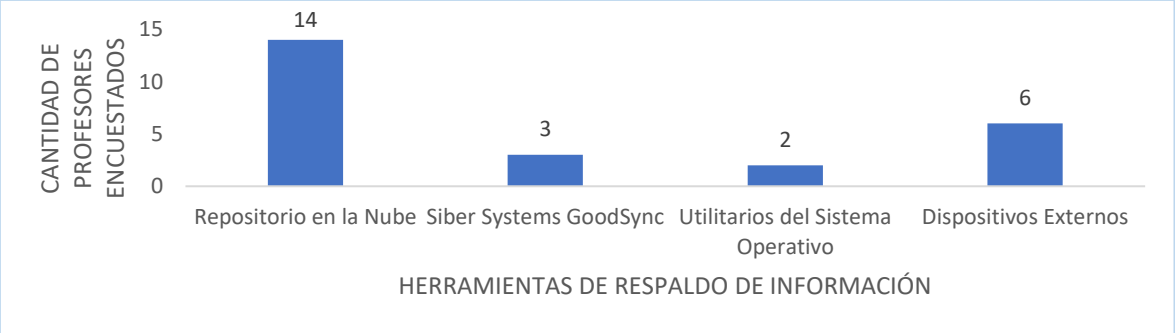
Fuente: Los autores.

Claramente existe una buena práctica para realizar y aplicar procedimientos para el respaldo de la información y sus respectivas copias de seguridad de forma diaria 60% (15 de ellos); sin embargo, el proceso de verificación de respaldo de dicha información, en promedio 20%, (5) lo realiza mensualmente.

Un aspecto muy importante y vinculado a lo antes expuesto, lo destaca National Institute of Standards and Tecchnology (2018), en donde señala la función de protección y salvaguarda de la información y admite que es una capacidad para limitar o contener el impacto ante un posible evento de pérdida de la misma.

Otro tópico fundamental que presenta los resultados que se asocian a la utilización de herramientas informáticas y tecnológicas para ejecutar el proceso de respaldo de la información y la preparación de copias de seguridad, se muestra en la figura 10.

Figura 10. Respaldo de la información y copias de seguridad



Fuente: Los autores.

Está claro que 16 (64%) de los docentes encuestados utilizan alguna aplicación informática y aplican procedimientos de respaldo de la información y copias de seguridad en la nube; lo que significa que, al depositar su información en la web, están sujetos a sufrir acciones malintencionadas producto de las nuevas actividades delictivas denominadas ciberdelitos.

Reconociendo lo expresado por Intelligent Networks for Critical Business (2022), establece que, en el momento en que se arriesga la información que se dispone, se coloca en una posición vulnerable no sólo a los sistemas; sino a las mismas personas que día a día utilizan las redes de computadoras, las tecnologías y el acceso a la web, como medios y elementos de trabajo, negocio, estudio y entretenimiento.

Para culminar, se han presentado los argumentos, explicaciones y los resultados obtenidos a través del formulario en línea de forma remota aplicado a los profesores de las ocho unidades académicas que participaron de la investigación.

4. Conclusiones

- La sociedad actual es altamente tecnológica y dependiente de procesos y actividades que requieren del uso constante de internet y del acceso a la web como medio de comunicación e intercambio de información; lo que conlleva la puesta en práctica de nuevas y mejores estrategias de defensa y salvaguarda de todos los bienes y recursos que, los usuarios día a día disponen, comparten, colaboran, intercambian o se depositan en la web.
- La omnipresencia de las tecnologías de la información y comunicación, el uso de las redes de computadoras, el acceso a la red internet y, por ende, a la web, son elementos fundamentales para modificar todos los hábitos y la manera de conectarnos, actuar, compartir, construir y colaborar; por lo que, se hace justo y necesario adoptar una cultura tecnológica y de ciberseguridad como un nuevo estilo de vida en un mundo digital.
- Un aspecto muy preocupante y que obedece al marco legal establecido en el Código Penal Panameño, se vincula a la ausencia directa en la presentación de las nuevas conductas criminales y prácticas delictivas que se presentan y desarrollan sobre el ciberespacio; lo que pone de manifiesto la falta de leyes que reglamenten dichas acciones en materia de ciberdelitos y ciberseguridad.
- A pesar de los múltiples esfuerzos realizados por parte del Ministerio Público, Policía Nacional, Ministerio de Seguridad Pública y de otras entidades del Estado, en materia de capacitación del recurso humano y docencia sobre ciberdelitos, es muy importante señalar que sólo se abordan temas sobre delitos como estafa, delitos contra la seguridad informática, la extorsión, criptomonedas, estructura de internet, análisis forense, entre otros; lo cual no es suficiente, ya que se requiere de un enfoque más técnico y práctico en esta materia.
- La evolución legal debe ir en concordancia con los avances tecnológicos, de manera que se minimicen los vacíos legales que permitan la impunidad en este tipo de acciones delictivas; por lo que, el estudio y análisis de la relación de la trilogía: ciberdelitos, normas legales y políticas de seguridad, cobran mayor importancia cada día.
- Se requiere de la experticia técnica para contrarrestar las nuevas acciones delictivas que aparecen día a día sobre el ciberespacio y la web, como, por ejemplo:

ransomware, rootkits, adware, zero day, ataques a redes wi-fi, suplantación de identidad digital, ataques de tipo man in the middle, DoS, DDoS, ingeniería social, sharenting, sexting, grooming, doxxing, entre otros más; y que existan las normales legales especializadas y reglamentadas que atiendan estas acciones criminales.

- Se debe desarrollar programas de capacitación del recurso humano y concienciación en todos los niveles académicos y profesionales en materia de ciberseguridad, en cada institución del Estado; ya que resulta una de las mejores y más económicas estrategias de prevención de riesgos contra los ciberdelitos.
- Desde el punto de vista de la investigación, se requiere del diseño, desarrollo y ejecución de nuevas políticas de ciberseguridad; las cuales deben estar encaminadas a las cuatro áreas temáticas propuestas, ya que recogen el sentir de los especialistas de seguridad.

Agradecimientos

A los coordinadores y profesores de la Facultad de Informática, Electrónica y Comunicación de las ocho Unidades Académicas que participaron en el estudio: Luis Carlos Poveda, Daniel Serrano, Ronald Mitre, Germán Alonso, César Delgado, Rafael Díaz, Obeth Ponte y Belén González, que brindaron su tiempo en la consecución de la información solicitada.

Referencias bibliográficas

Agustina, J. (2021). Nuevos retos dogmáticos ante la cibercriminalidad: ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma? *Estudios Penales Y Criminológicos, 41*(21), 705-777. https://doi.org/10.15304/epc.41.7433

Alexandrou, A. (2022). *Cybercrime and Internet technology theory and practice: the computer network infostructure and computer security, cybersecurity laws, internet of things (IoT), and mobile devices*. CRC Press.

Chaudhuri, A. (2019). *Survey Sampling*. CRC Press.

Chaudhuri, A., y Pal, S. (2022). *A Comprehensive Textbook on Sample Surveys*. Springer.

Chiavenato, I. (2019). *Administración de recursos humanos: El capital humano de las organizaciones*. (10º. ed.). McGraw-Hill.

Fernández, L., Rodríguez, D., Monge, R., Rodríguez, Ó., y Dutari, R. (2020). Nivel de formación y necesidad de capacitación en entornos virtuales como factores claves para el desarrollo académico-profesional del recurso humano en cuatro unidades académicas de la Universidad de Panamá. *Visión Antataura, 4*(2), 79-101. https://doi.org/10.48204/j.vian.v4n2a6

Fratti, S. (junio de 2018). *Panamá: Un país con la necesidad de una legislación sobre cibercrimen*. Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC), Derechos Digitales y Tecnología en América Latina. https://www.derechosdigitales.org/wp-content/uploads/minuta_ipandetec.pdf

Ghonge, M., Pramanik, S., Mangrulkar, R., y Le, D.-N. (2022). *Cyber Security and Digital Forensics* [*Ciberseguridad y análisis forense digital*]. John Wiley & Sons.

Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la Investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill.

Instituto Nacional de Ciberseguridad de España. (2022). *Conoce INCIBE*. https://www.incibe.es/que-es-incibe

Intelligent Networks for Critical Business. (2022). *Guía de Ciberseguridad*. Intelligent Networks for Critical Business.

Kremling, J., y Sharp, A. M. (2018). *Cyberspace, cybersecurity, and cybercrime*. SAGE Publications.

Marín, A. F. (2017). 11 de septiembre de 2001: seguridad global entre ayer y hoy. *Perspectivas en Inteligencia, 9*(18), 23-34. https://doi.org/10.47961/issn.2145-194X

Melone, M. (2021). *Designing Secure Systems*. CRC Press.

Metcalfe, A., Green, D., Greenfield, T., Mansor, M., Smith, A., y Tuke, J. (2019). *Statistics in Engineering with Examples in MATLAB and R (Second ed.).* CRC Press.

Ministerio de Seguridad Pública. (2021). *Consolidado de los 15 Títulos del Código Penal por mes y por provincias: Enero–Diciembre del 2021*. Ministerio de Seguridad Pública, Sistema Nacional Integrado de Estadísticas Criminales, Panamá.

Ministerio Público de Panamá. (2019). *Texto Único del Código Penal Actualizado*. Procuraduría General de la Nación, Oficina de Implementación del Sistema Penal Acusatorio, Panamá.

Ministerio Público de Panamá. (18 de mayo de 2021). *El Ciberdelito es Real*. *Ministerio Público y Policía Nacional lanzan campaña de prevención del delito.* https://ministeriopublico.gob.pa/el-ciberdelito-es-real-ministerio-publico-y-policia-nacional-lanzan-campana-de-prevencion-del-delito/

Muñoz Machado, S. (2022). *Ignorantia legis non excusat*. https://dpej.rae.es/lema/ignorantia-legis-non-excusat

National Institute of Standards and Tecchnology. (2018). *Framework for Improving Critical Infraestructure Cybersecurity*. United States Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

Oakley, J. G., Butler, M., York, W., Puckett, M., & Sewell, J. (2022). *Theoretical Cybersecurity: Principles and Advanced Concepts*. Apress. https://doi.org/10.1007/978-1-4842-8300-4

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Revista Latinoamericana de Estudios de Seguridad* (20), 80-93. https://doi.org/10.17141/urvio.20.2017.2563

Reznik, L. (2022). *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work for and Against Computer Security*. John Wiley & Sons.

Rodríguez C., O., Dutari D., R., Fernández G., L., Rodríguez F., D., y Díaz R., K. (2021). Identificación de criterios académicos y técnicos para la selección de simuladores como recursos didácticos aplicados a la enseñanza de asignaturas prácticas en la licenciatura en informática para la gestión educativa y empresarial. *Visión Antataura,* *5*(2), 50-66. https://revistas.up.ac.pa/index.php/antataura/article/view/2522

Santos, H. (2022). *Cybersecurity: a practical engineering approach*. CRC Press.

Santos, O. (2019). *Developing Cybersecurity Programs and Policies*. Pearson Education.

Skulmoski, G. (2022). Shields Up: Cybersecurity Project Management. Business Expert Press.

SUMMA. (2021). *Experiencias de desarrollo profesional docente en América Latina en contextos COVID-19 y su vinculación con tecnologías digitales*. Universidad Católica Silva Henríquez, Laboratorio de Investigación e Innovación en Educación para América Latina y el Caribe, SUMMA, y el Centro de Investigación para la

Transformación Socio-Educativa (CITSE). https://www.summaedu.org/wp-content/uploads/2021/10/Informe-EXPERIENCIAS-DE-DESARROLLO-2.pdf

Tanenbaum, A., Feamster, N., y Wetherall, D. (2021). *Computer Networks (Sixth ed.).* Pearson Education.

Torgerson, C., y Iannone, S. (2020). *What works in talent development: Designing Microlearning*. ATD Press.

Triola, M. (2018). *Estadística.* (12.ª ed.). Pearson Educación.

Universidad de Panamá. (15 de julio de 2022). *Estructuras Académicas Actualizadas hasta el 12 de abril de 2022*. Universidad de Panamá, Vicerrectoría Académica. Dirección Curricular y Evaluación de Documentación Académica. https://siged.up.ac.pa/eacademicas/?paso=2&cod_facultad=24

van Woudenberg, J., y O'Flynn, C. (2022). *The Hardware Hacking: Breaking Embedded Security with Hardware Attacks*. No Starch Press.