2023

Reporte sobre el desarrollo de la

FUERZA LABORAL DE CIBERSEGURIDAD

en una era de escasez de talento y habilidades

OEA | Más derechos para más gente

Cybersecurity Innovation Councils

CISCO

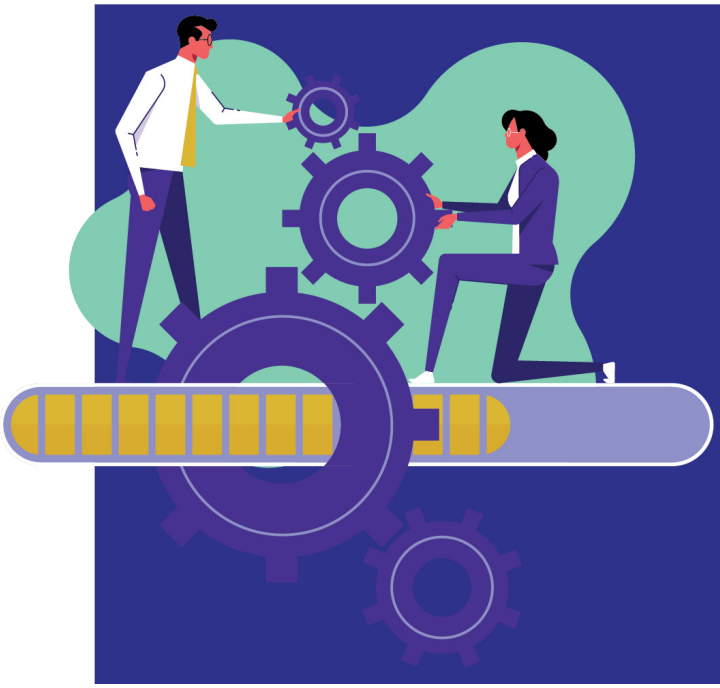
Preparado y publicado por el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (cybersecurity@oas.org)

RESUMEN

La pandemia COVID-19 y la postpandemia han generado un fuerte impacto en la economía global[1], una expansión del panorama de amenazas y riesgos[2] y un cambio importante en la forma de trabajar en las organizaciones[3]. Existe, además, un envejecimiento generalizado de la población[4], grandes problemas en las economías de la región debidos al alto desempleo[5] y una reversión generalizada en el progreso de paridad de género[6].

En el mercado laboral de ciberseguridad se ha creado una brecha (escasez) en su fuerza laboral en el corto plazo[7] generando riesgos debidos no solo a la escasez de talento en las organizaciones sino también a la escasez de habilidades en la fuerza laboral. Esta situación, si bien global, se presenta de manera exacerbada en América Latina y el Caribe, generando fuertes presiones en las organizaciones tanto públicas como privadas con el subsiguiente impacto en la ciberseguridad de los países de la región.

Actualmente, el desarrollo de la fuerza laboral de ciberseguridad se analiza bajo dos enfoques: cuantitativo y cualitativo, es decir en el contexto de la escasez de profesionales y en el de la brecha de habilidades tanto de los profesionales que desean entrar a formar parte de la fuerza laboral en ciberseguridad como de los profesionales que hacen parte de ella. El análisis de la situación tanto por el lado de la demanda como por el lado de la oferta en el mercado laboral de ciberseguridad es crucial para identificar los retos y desafíos que todas las múltiples partes interesadas deben abordar con el fin de cerrar las brechas en los países de la región.



Por ejemplo, desde la oferta, para aquellas personas que tienen interés en ingresar al mercado laboral de ciberseguridad, la información sobre lo que implica una carrera es abrumadora, confusa y contradictoria. El camino para seguir en la preparación para una carrera cibernética y la progresión, una vez en la fuerza laboral, pueden ser procesos complejos. Para las organizaciones, que están del lado de la demanda, existen dificultades para identificar los requisitos necesarios para cubrir los puestos vacantes, reclutar y retener talento, mientras intentan mantener una sólida postura de ciberseguridad. Los gobiernos vienen adoptando e implementando políticas y estrategias nacionales de ciberseguridad abordando problemas relacionados con falta de capacidades de ciberseguridad, no obstante, las iniciativas estratégicas propuestas en torno al desarrollo de fuerza laboral de ciberseguridad en la región tardarán años o incluso décadas en madurar.

1 Según (WORLD BANK, 2022), tras un fuerte repunte en 2021, la economía mundial está entrando en una desaceleración pronunciada en medio de nuevas amenazas de variantes de COVID-19 y un aumento de la inflación, la deuda y la desigualdad de ingresos que podrían poner en peligro la recuperación de las economías emergentes y en desarrollo. Se proyecta que el crecimiento de América Latina y el Caribe se desacelere a 2,6 % en 2022 antes de aumentar levemente a 2,7 % en 2023.
2 Según (FORTINET, 2022), la región de América Latina y el Caribe sufrió 137 mil millones de intentos de ciberataques de enero a junio de 2022, un aumento del 50% en comparación con el mismo período del año pasado (con 91 mil millones). México fue el país más atacado (con 85 mil millones), seguido por Brasil (con 31,5 mil millones) y Colombia (con 6,3 mil millones).
3 Según (FORBES, 2022), el futuro del trabajo será más híbrido, más colaborativo y más automatizado.
4 Según (Oxford Martin School, 2022), durante los próximos cincuenta años, se espera que los ancianos superen en número a los jóvenes en casi todos los países. Este cambio en la composición de la edad tiene enormes implicaciones para todos los aspectos de la sociedad y la economía.
5 Según (ILO, 2022), se estima que el número total mundial de jóvenes desempleados alcance los 73 millones en 2022, una ligera mejora con respecto a 2021 (75 millones), pero todavía seis millones por encima del nivel anterior a la pandemia de 2019.
6 Según (WEF, 2022) se necesitarán otros 132 años para cerrar la brecha global de género.
7 Según (ISC2, 2022a), hay una escasez mundial de 3,43 millones de trabajadores calificados en ciberseguridad.

El desarrollo de la fuerza laboral en ciberseguridad es fundamental para que los países estén preparados para enfrentar conflictos en el ciberespacio. También para que las organizaciones definan las habilidades y capacidades necesarias de su fuerza laboral para cumplir su estrategia y objetivos comerciales, identifiquen brechas clave en la fuerza laboral actual y creen estrategias y programas innovadores para atraer, reclutar, contratar y desarrollar al mejor talento.

La escasez de mano de obra y de habilidades en ciberseguridad seguirá creciendo en América Latina y el Caribe, por lo tanto, el ecosistema de ciberseguridad en la región debe trabajar integralmente y de manera coordinada en el desarrollo de la fuerza laboral con el fin de abordar una combinación única de desafíos y retos, pero siempre pasando de la formulación de soluciones a la acción.

CRÉDITOS

Luis Almagro
Secretario General
Organización de los Estados Americanos

Luis Oliveira
Secretaria de Seguridad Multidimensional
Organización de los Estados Americanos

Alison August Treppel
Secretaria Ejecutiva
Comité Interamericano contra el Terrorismo
Organización de los Estados Americanos

Equipo Técnico de la Organización de los Estados Americanos
Kerry-Ann Barrett
Orlando Garcés
David Moreno
Mariana Cardona

Equipo Técnico de CISCO
Rebeca De La Vega
Mario De La Cruz
Ned Cabot
Frederico Vasconcelos
Vinita Venugopal

TABLA DE CONTENIDO

LISTA DE GRÁFICAS

LISTA DE CUADROS

01

INTRODUCCIÓN

América Latina y el Caribe continúa apostando por maximizar los beneficios aportados por el uso de las Tecnologías de la Información y las Comunicaciones -TIC-, ya que son herramientas poderosas que ayudan a transformar la vida de todos y cada uno de sus ciudadanos. La creación de más y mejor infraestructura que permita el acceso a Internet repercute directamente en el desarrollo económico y social de la región. Es por ello que **los países de la región deben elevar los niveles de confianza digital.**

Debido al gran aumento de las amenazas cibernéticas, los esfuerzos por mejorar las capacidades de ciberseguridad han crecido sustancialmente en la región. No obstante, un área que sigue estando rezagada es el desarrollo de la fuerza laboral en ciberseguridad. Es decir, existe una escasez de personal capacitado y calificado en el mercado laboral para trabajar en roles de ciberseguridad que pueda abordar estas amenazas y sus riesgos relacionados.

Las habilidades en ciberseguridad pueden ser adquiridas, cambiadas y mejoradas **a través de la educación, la capacitación o la formación,** lo que convierte a la fuerza laboral de ciberseguridad en un grupo de talentos en evolución que las organizaciones públicas y privadas en la región deben desarrollar y mantener.

La escasez de profesionales y de habilidades en ciberseguridad es un asunto de política multidimensional en el que participan múltiples partes interesadas (sector público, sector privado, academia y sociedad civil) y se ve agravada por muchos factores. Evitar afrontar los retos relacionados con esta escasez representaría problemas tanto para el desarrollo económico como para la seguridad nacional de los países de la región América Latina y el Caribe.

En virtud de lo expuesto, el presente documento presenta un **análisis detallado del mercado laboral de ciberseguridad y de su fuerza laboral en la región** bajo el contexto actual de ciberseguridad, que permite identificar una problemática que puede ser explicada mediante desafíos que deben ser abordados de forma integral por las múltiples partes interesadas, en línea con las mejores prácticas internacionales. La investigación involucró una revisión de la literatura académica y gris, así como de otro material producido por gobiernos y otras organizaciones para comprender sobre la brecha de profesionales y habilidades de la fuerza laboral en ciberseguridad.

Este documento está dividido en cinco (5) capítulos, siendo este el primer capítulo. En el segundo capítulo se presenta el contexto actual de la ciberseguridad e identifica factores que impactan el mercado laboral de ciberseguridad y su fuerza laboral. En el tercer capítulo se describe de manera esquemática este mercado laboral y las condiciones que lo afectan tanto por el lado de la oferta laboral como por el lado de la demanda laboral, caracterizando la actual fuerza laboral. Adicionalmente, se describe el problema principal y se identifica una combinación única de desafíos que enfrenta dicho mercado bajo el contexto actual. En el cuarto capítulo se hace una propuesta de solución para que las múltiples partes interesadas pasen a la acción, con el fin de promover el desarrollo de la fuerza laboral y resolver la problemática identificada. Finalmente, el quinto capítulo presenta las referencias bibliográficas consultadas.

02

LA CIBERSEGURIDAD BAJO EL CONTEXTO ACTUAL

El desarrollo de una economía digital contribuye positivamente a la generación de prosperidad económica y social de los países de la región América Latina y el Caribe. Esto requiere la construcción de un entorno digital seguro y confiable, acorde con la multiplicación de las actividades digitales de los gobiernos, de las organizaciones y de los ciudadanos. Ahora, muchos de los retos que afronta la economía digital se deben en gran parte a la dependencia de Internet y de su rápido crecimiento tanto en usuarios como en aplicaciones.

Esta situación exige que en la región existan las suficientes capacidades para la gestión adecuada y oportuna de riesgos inherentes de ciberseguridad, de forma tal que aunque exista mayor nivel de exposición a los riesgos por el uso incremental del entorno digital, las acciones que se adelanten reduzcan los incidentes digitales para evitar consecuencias de tipo económico o social derivadas de amenazas, ataques e incidentes cibernéticos que deterioran la confianza digital y ralentizan la adaptación para el futuro digital. Al responder adecuadamente a los actuales desafíos de la ciberseguridad, se puede aprovechar al máximo la transformación digital y capitalizar nuevas oportunidades para individuos, organizaciones y en general, para toda la sociedad.

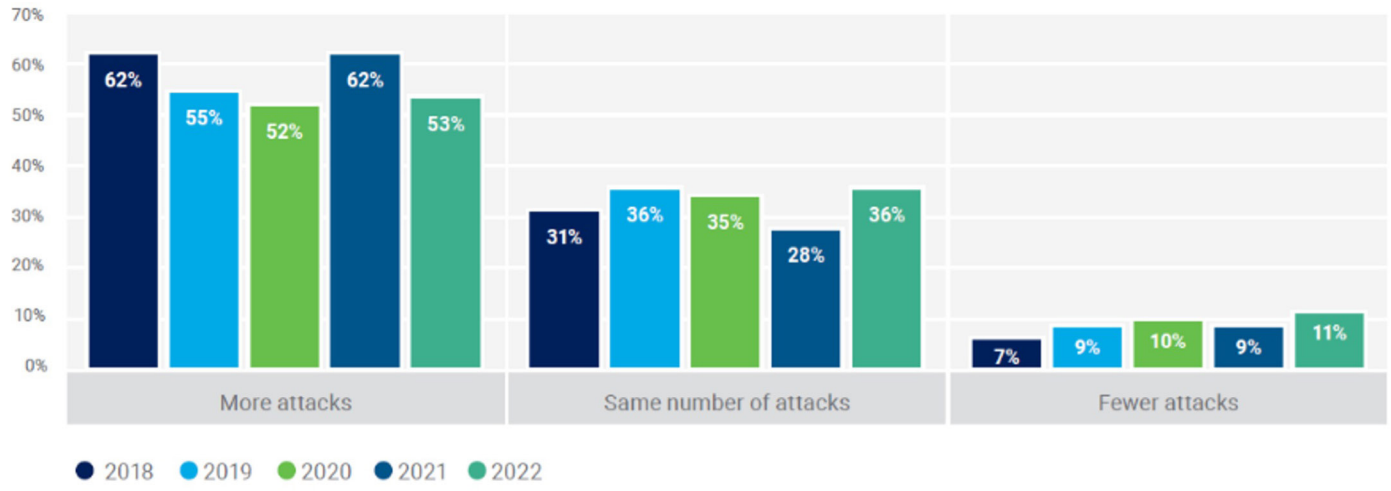
La situación económica en América Latina y el Caribe durante los últimos 3 años ha sido compleja debido a la pandemia de COVID-19. Las restricciones y otras intervenciones de salud pública implementadas para reducir el contagio han tenido un fuerte impacto en la economía de la región. Las organizaciones y los ciudadanos se desplazaron masivamente hacia los canales digitales y en línea para eludir las medidas de distanciamiento social, continuar con las operaciones comerciales, asegurar las fuentes de ingresos y mantenerse solventes durante la pandemia (BID, CEPAL & KAS, 2021). No obstante, algunos sectores económicos como el sector TIC experimentaron no solo incrementos en las horas trabajadas sino crecimiento en el empleo con respecto a años previos a la pandemia (OECD, 2021).

Las organizaciones, especialmente las PYMES[8] en la región, enfrentaron apresurados procesos de digitalización y transformación digital. No obstante, la falta de habilidades digitales se ha convertido en un desafío transversal para este segmento empresarial y se ha perfilado como un obstáculo clave para abordar estos procesos. Muchas de estas organizaciones carecen de una cultura digital tanto a nivel estratégico como operacional donde los beneficios potenciales de la digitalización a menudo se desconocen o no se comprenden completamente.

8 Las PYMES comprenden el 99,5% de las empresas de la región América Latina y el Caribe (con casi 9 de cada 10 clasificadas como microempresas) y generan el 60% del empleo productivo formal. Sin embargo, las PYMES latinoamericanas tienen una brecha de productividad particularmente significativa, siendo responsables de solo una cuarta parte del valor total de la producción de la región (OECD, 2022).

Hay una expansión creciente del panorama de amenazas y riesgos a nivel global y en la región América Latina y el Caribe. A medida que la dependencia de las tecnologías digitales continúa aumentando, también lo hace el delito cibernético. Los ciberdelincuentes están aprovechando cada oportunidad para explotar las vulnerabilidades contra las personas y las organizaciones a través de la tecnología, adaptando rápidamente nuevas tecnologías y sus ataques utilizando métodos novedosos y cooperando estrechamente entre sí (WEF, 2022). Según (ISACA, 2022), durante los años 2018 y 2022, entre el 52% y 62% de las organizaciones percibieron que recibían más ataques[9] que el año inmediatamente anterior.

Gráfica 1.
Comparación año tras año de informes de ataques de ciberseguridad

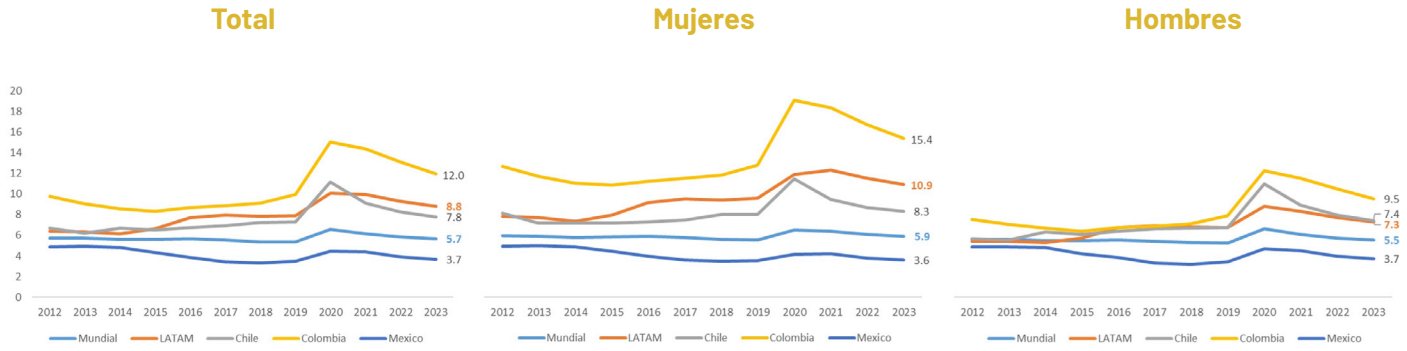


Fuente: (ISACA, 2022)

Los mercados laborales se encuentran en un período de profunda transformación. Los trabajos y las habilidades se han visto afectados por la automatización[10], la transformación de la industria y la transición ecológica, coincidiendo con cambios en las prácticas laborales impulsados por la pandemia que antes parecían imposibles[11]. En especial, el rol de la tecnología ha crecido exponencialmente en todos los sectores de la economía, generando nuevas ocupaciones y cambiando las tareas que realizan los seres humanos y las habilidades que necesitan para abrir camino en el mercado laboral (BID, 2021). No obstante, la tecnología puede generar desempleo tecnológico y aumentar tanto la desigualdad como la polarización en la región si los gobiernos, organizaciones e individuos no responden de manera adecuada (BID, 2020).

9 Según (WEF, 2022), el ransomware, la ingeniería social y la actividad interna maliciosa son los tres principales ataques cibernéticos que más preocupan a las organizaciones. Mientras que las fallas de infraestructura debido a un ciberataque, el robo de identidad y el ransomware son los tres principales ataques cibernéticos que más preocupan a los ciber líderes.
10 Casi la mitad (48%) de los encuestados de Cyber Outlook del Foro Económico Mundial dicen que la automatización y el aprendizaje automático introducirán la mayor transformación en ciberseguridad en el futuro a corto plazo (WEF, 2022).
11 https://www.weforum.org/events/world-economic-forum-annual-meeting-2022/sessions/a-new-vision-for-jobs

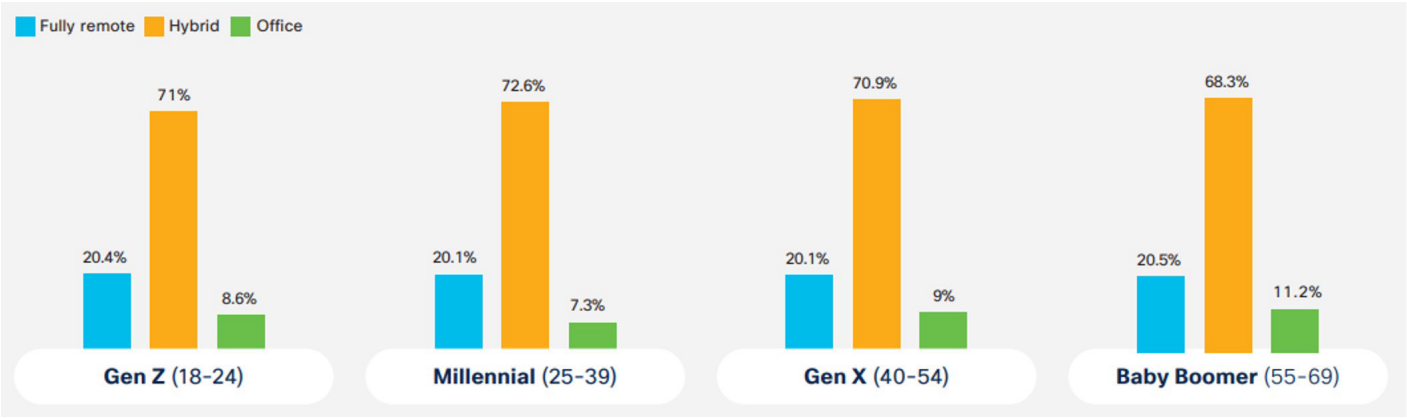
Gráfica 2.
Evolución y proyección de la tasa de desempleo en América Latina



Fuente: Elaboración propia a partir de (ILO, 2022)

Se han presentado cambios importantes en la forma de trabajar en las organizaciones de la región. Según (MichaelPage, 2022) se destaca que menos del 20% de las organizaciones en América Latina y el Caribe continúa actualmente trabajando exclusivamente desde casa, el 37,5% han retornado al modelo presencial y el 44,3% asegura que se encuentra trabajando bajo la modalidad híbrida o mixta. Según (WEF, 2022), un 28% de ejecutivos de organizaciones estima que el entorno de trabajo remoto/híbrido será una de las mayores influencias en la transformación de la ciberseguridad en los próximos dos años.

Gráfica 3.
Preferencias del lugar del trabajo por generación



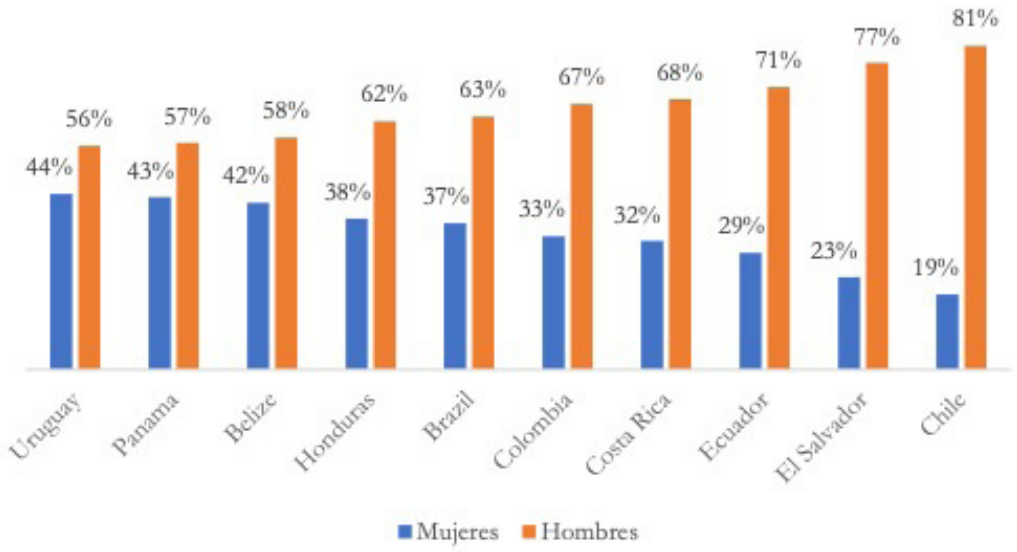
Fuente: (CISCO, 2022)

En algunas regiones del mundo se experimentan fenómenos como *la Gran Reorganización o la Gran Renuncia*[12] *o la Renuncia Silenciosa*[13]. Una gran cantidad de personas optaron por dejar sus trabajos en busca de roles más satisfactorios con mayor flexibilidad provocado un número récord de puestos vacantes y escasez de personal en algunas industrias[14]. A partir de este fenómeno, las organizaciones a nivel global están reexaminando las estrategias comerciales, los modelos de fuerza laboral, los valores y la cultura, a menudo guiados por las nuevas demandas de los propios empleados (LinkedIn, 2022).

Se ha revertido el progreso en la paridad de género en la participación laboral con consecuencias importantes para otras dimensiones del empleo y en la distribución del trabajo no remunerado, que afectan la forma en que las mujeres acceden a oportunidades en el ámbito económico, así como en otras esferas de la vida. La brecha global de género en 2022 está cerrada en un 68,1 %. Otro ejemplo es que las mujeres están subrepresentadas en los mercados laborales relacionados con campos STEM[15] y la brecha de género es más frecuente en el sector TIC[16]. América Latina y el Caribe cerrará su brecha de género en aproximadamente 67 años (WEF, 2022).

Gráfica 4.

Porcentaje de hombres/mujeres graduadas en educación terciaria de programas STEM en América Latina



Fuente: Elaboración propia a partir de información presentada en (WEF, 2022)

12 Según (MERCER, 2022), la Gran Renuncia ciertamente ha agudizado el enfoque en la retención dentro de las organizaciones, que es una de las principales peticiones de los directores ejecutivos a sus líderes de recursos humanos este año. Curiosamente, las razones de los empleados para quedarse en su empresa no difieren mucho según el país y la industria, pero sí difieren según la generación. Los empleados de la Generación Z les dan más valor a los líderes inspiradores, pero no a los salarios competitivos. Para los Baby Boomers, las políticas de vacaciones/tiempo libre son la razón número dos por la que se han quedado. La seguridad laboral es el número uno en todos los grupos generacionales en la fuerza laboral.

13 Durante 2022, ha surgido una nueva tendencia en el mercado laboral llamada Renuncia Silenciosa (en inglés, Quiet Quitting) que se trata de rechazar la noción de que el trabajo tiene que hacerse cargo de la vida y que los empleados deben ir más allá de lo que implican las descripciones de su trabajo.

14 https://www.weforum.org/agenda/2022/02/great-reshuffle-jobs-market-resignation/

15 El término STEM es el acrónimo de los términos en inglés Science, Technology, Engineering and Mathematics (Ciencia, Tecnología, Ingeniería y Matemáticas).

16 El porcentaje de mujeres tituladas en TIC a nivel global es del 1,7%, frente al 8,2% de los hombres titulados (WEF, 2022).

El ritmo acelerado de la digitalización y el cambio de los hábitos de trabajo está impulsando la resiliencia cibernética[17]. Los ejecutivos están planeando mejorar la resiliencia cibernética en sus organizaciones al fortalecer las políticas, procesos y estándares de resiliencia sobre cómo involucrar y administrar a terceros (WEF, 2022). Esto no solo ocurre en las organizaciones privadas sino también en el sector público.

Frente a este contexto, los países en América Latina y el Caribe vienen adoptando e implementando políticas y estrategias nacionales de ciberseguridad[18], en cuyo marco se desarrollan acciones tendientes a generar un entorno digital más confiable, que resulte adecuado para lograr sus objetivos de desarrollo económico y social, para lo cual, resulta particularmente importante la formulación e implementación de iniciativas para fomentar el desarrollo de capacidades para que las organizaciones y los ciudadanos gestionen los riesgos de ciberseguridad.

En línea con las mejores prácticas[19], las políticas y estrategias nacionales en la región abordan los problemas relacionados con la capacitación en materia de ciberseguridad y la sensibilización de las entidades gubernamentales, los ciudadanos, las empresas y otras organizaciones, que son fundamentales para hacer posible la economía digital en la región. Entre las buenas prácticas se encuentra el establecimiento de planes de estudio y programas de sensibilización sobre ciberseguridad, la ampliación de los planes de formación y de los programas de formación profesional, la adopción de planes de certificación internacionales y el fomento de agrupaciones de innovación e investigación y desarrollo -I+D-. Por ejemplo, se destacan algunas iniciativas:

A La *Política Nacional de Confianza y Seguridad Digital de Colombia* (2020-2022)[20] establece como uno de sus tres objetivos específicos fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país mediante la formulación de estrategias y acciones para la formación profesional y el desarrollo de competencias bajo enfoque diferencial e inclusivo.

B La *Política Nacional de Ciberseguridad de Chile* (2017-2022)[21] establece como uno de sus cinco objetivos desarrollar una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales mediante la implementación de iniciativas que fomenten y desarrollen una cultura digital consciente, competente, informada y responsable que incluya a todos los actores relevantes.

C La *Estrategia Nacional de Ciberseguridad de México* (2017-2021)[22] establece como uno de sus cinco ejes transversales el desarrollo de capacidades mediante el establecimiento de acciones encaminadas a la generación y fortalecimiento de las capacidades organizacionales, de capital humano y recursos tecnológicos en materia de ciberseguridad, que permitan a la sociedad, academia, sector privado e instituciones públicas contar con los recursos para la gestión de riesgos y amenazas en el ciberespacio, así como el incremento de la resiliencia nacional.

17 (WEF, 2022) define resiliencia cibernética como *"la capacidad de una organización para trascender (anticipar, resistir, recuperarse y adaptarse) a cualquier estrés, falla, peligro y amenaza a sus recursos cibernéticos dentro de la organización y su ecosistema, de modo que la organización pueda cumplir con su misión con confianza, permitir su cultura y mantener su forma deseada de operar".*

18 Actualmente, un total de diecisiete (17) Estados miembros de la Organización de Estados Americanos -OEA- han aprobado sus políticas / estrategias nacionales de ciberseguridad (OEA & GPD, 2022) y 14 de ellos pudieron hacerlo con el apoyo técnico de la OEA.

19 La *Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad* de la Unión Internacional de Telecomunicaciones -UIT- presenta buenas prácticas en la materia (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/NCS%20Guide_s.pdf)

20 La Política Nacional de Confianza y Seguridad Digital de Colombia se expidió mediante el Documento CONPES 3995 de 2020 (https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf)

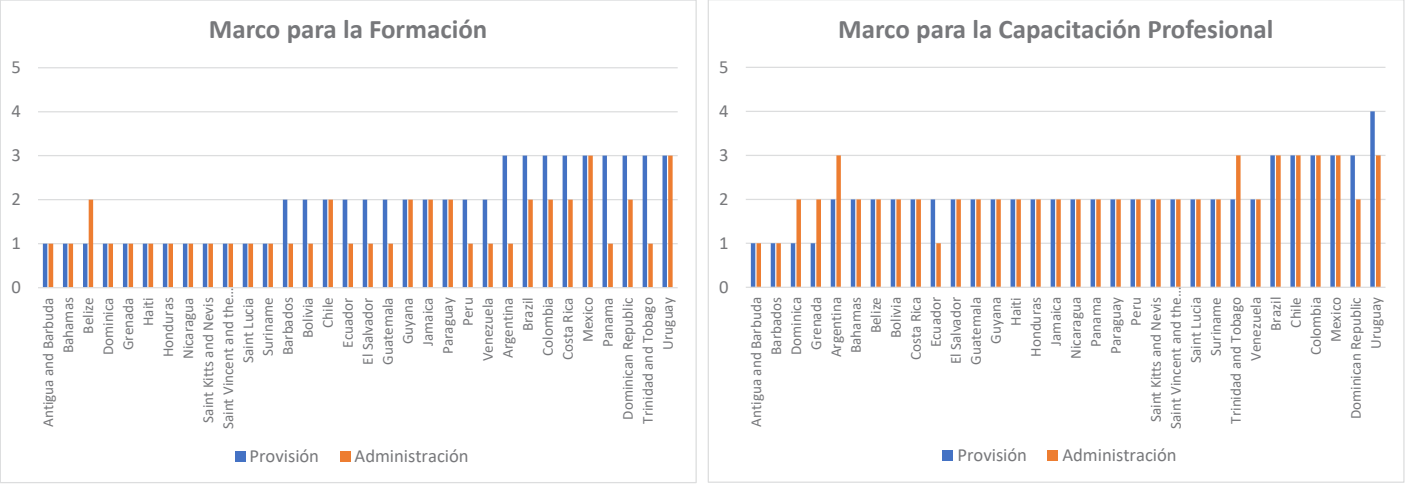
21 https://www.cnc.cl/wp-content/uploads/2020/02/Pol%C3%ADtica-Nacional-Ciberseguridad.pdf

22 https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad

No obstante, este tipo de iniciativas estratégicas que tienen relación con el mercado laboral de ciberseguridad tardarán años o incluso décadas en madurar. Según (OEA & GPD, 2022), se necesitan muchos años para desarrollar una fuerza laboral digitalmente inteligente con habilidades orientadas a una economía del conocimiento, debido a las altas tasas de deserción en el sector público para trabajos de ciberseguridad y bajas tasas de disponibilidad de oportunidades educativas específicas en el área. Por tal razón, los países de la región deben priorizar iniciativas de desarrollo de fuerza laboral para asignar el presupuesto con el fin de implementar los programas lo más pronto posible.

Gráfica 5.

Nivel de madurez de capacidades en América Latina y el Caribe en relación con la formación y la capacitación profesional



Fuente: Elaboración propia a partir de (OEA & BID, 2020)

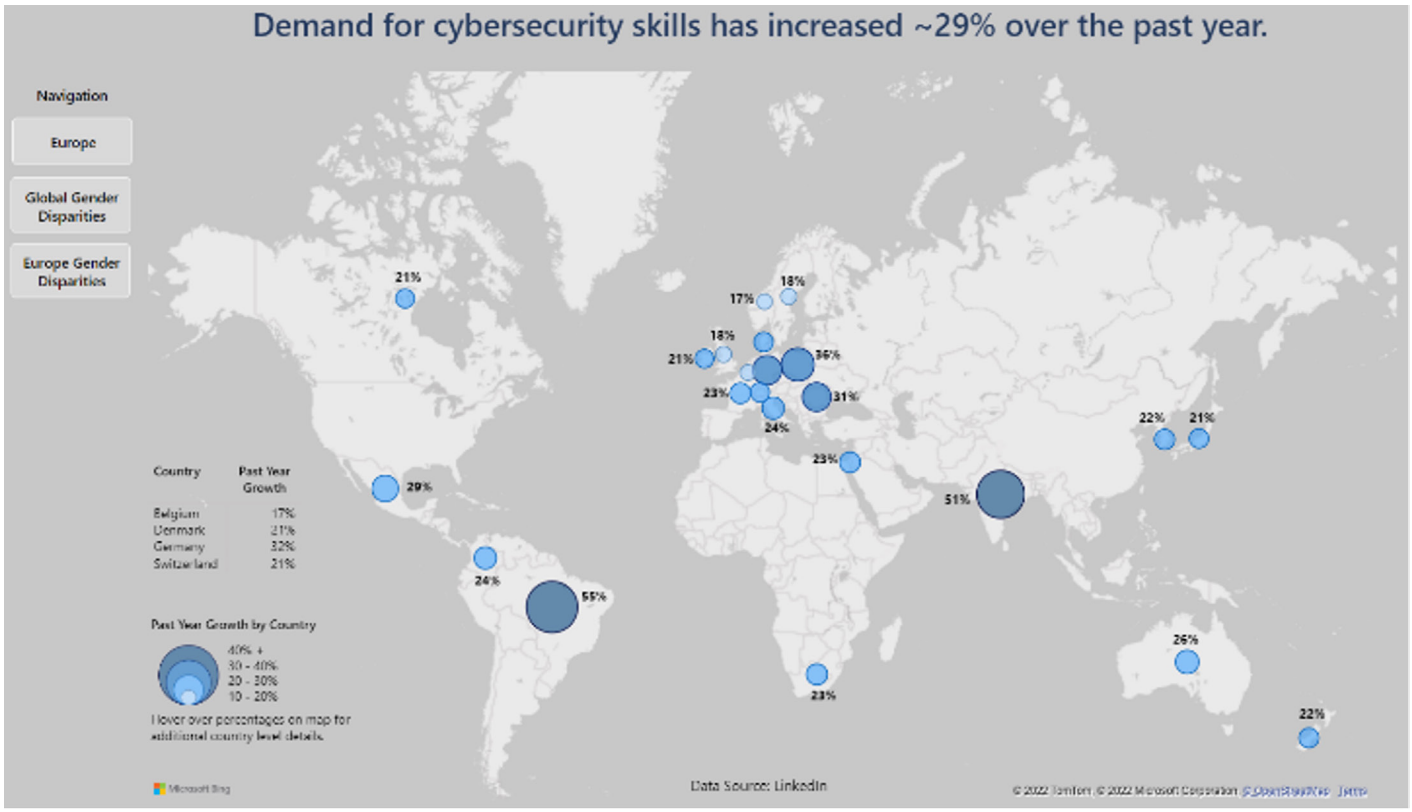
En el entretanto, el aumento en la demanda de profesionales de ciberseguridad[23] viene acompañado de un fuerte aumento en los salarios[24] y una gran competencia entre profesionales capacitados. En este tipo de mercado laboral, a corto plazo, la oferta de profesionales de ciberseguridad no responde a salarios más altos ya que se necesita tiempo para capacitar a trabajadores adicionales con las habilidades requeridas. Los esfuerzos de capacitación y educación pueden llevar años, incluso si los trabajadores individuales en otras ocupaciones, sectores o industrias tienen el conjunto adecuado de habilidades para convertirse en profesionales de ciberseguridad, es posible que no cambien de ocupación de inmediato.

23 Aumento debido a una mayor conectividad, una mayor vulnerabilidad y un crecimiento del cibercrímen, junto con shocks exógenos al mercado debidos de la pandemia del COVID-19.
24 Según (DCMS & IPSOS, 2022), en el Reino Unido los empleadores y los equipos cibernéticos continúan sintiendo el impacto de la pandemia. En particular, puede haber llevado a salarios de mercado más altos fuera de Londres y el sureste, presentando desafíos para los empleadores regionales más pequeños.

Esta situación en el mercado laboral de ciberseguridad de la región crea una brecha (escasez) en la fuerza laboral en el corto plazo. Según (ISC, 2021) y (ISC, 2022a), hay una escasez entre 515.000 y 701.000 trabajadores calificados en ciberseguridad en la región América Latina y el Caribe. Según este estudio, la brecha de la fuerza laboral sigue siendo la principal barrera para satisfacer las necesidades de seguridad de las organizaciones, encontrando que el 60% de los encuestados informa que la escasez de personal de ciberseguridad está poniendo en riesgo a sus organizaciones[25].

Pero no solo la escasez de talento genera riesgos en las organizaciones sino también la escasez de habilidades[26] en la fuerza laboral. Por ejemplo, al 59% de todos los encuestados en el estudio *Global Cybersecurity Outlook* 2022 respondieron que les resultaría difícil responder a un incidente de ciberseguridad en sus organizaciones debido a la escasez de habilidades dentro de su equipo (WEF, 2022).

Gráfica 6.
Incremento en la demanda de habilidades de ciberseguridad



Fuente: (MICROSOFT, 2022)

25 (ISC2, 2021) confirma, desde la perspectiva de la fuerza laboral global de ciberseguridad, que cuando el personal de ciberseguridad es reducido, las consecuencias negativas son reales: sistemas mal configurados, ciclos de parches lentos, implementaciones apresuradas, tiempo insuficiente para una evaluación de riesgos adecuada, supervisión insuficiente de procesos y procedimientos, y más.

26 En línea con lo dispuesto en el *Marco del Personal para la Ciberseguridad de la Iniciativa Nacional para la Educación en Ciberseguridad* (en inglés, National Initiative for Cybersecurity Education -NICE-) del Instituto Nacional de Normas y Tecnología de los Estados Unidos (en inglés, National Institute of Standards and Technology -NIST-), se entiende que las habilidades representan una combinación de destrezas, conocimientos y experiencia que permiten a un individuo completar bien una tarea bajo un rol de ciberseguridad en una organización.

Esta situación ha generado fuertes presiones en las organizaciones tanto públicas como privadas[27], ya que estas deben, por un lado, identificar, atraer y reclutar al mejor talento disponible y, por otro, deben retenerlo implementando, entre otras, estrategias innovadoras de capacitación y entrenamiento, tales como: i) *Upskilling* (procesos de aprendizaje de nuevas habilidades o de enseñar nuevas habilidades a los empleados), ii) *Reskilling* (procesos de capacitación a empleados en un conjunto completamente nuevo de habilidades para prepararlos para asumir un rol diferente dentro de la empresa), y iii) *New Skilling* (procesos de aprendizaje continuo para ayudar a desarrollar habilidades de alta demanda, ya sea que una persona esté tratando de mejorar las capacidades actuales o que necesite una actualización completa para desarrollar capacidades completamente nuevas). De igual forma, fomentando programas de aprendizaje basados en el trabajo, incluidos las pasantías (en inglés, apprenticeships) y las prácticas laborales (en inglés, traineeships).

Estos problemas en las organizaciones pueden potencialmente socavar la ciberseguridad de las naciones y de la región. Por lo tanto, esta situación hace que las múltiples partes interesadas en el ecosistema de ciberseguridad que tienen relación con el desarrollo de estos mercados laborales enfrenten una combinación única de desafíos que los países de América Latina y el Caribe deben afrontar.

27 Según (DCMS & IPSOS, 2022), específicamente en el sector cibernético del Reino Unido, hay evidencia de un mercado laboral más desafiante desde la perspectiva de los empleadores. Más de la mitad de las empresas del sector cibernético (53%) han intentado contratar a alguien en los 18 meses anteriores. De todas las vacantes durante este período, se informó que en el 44% de empresas fue difícil de cubrir (frente al 37% en 2021 y el 35% en 2020). La razón más común que se da para que las vacantes sean difíciles de cubrir sigue siendo que los candidatos carecen de habilidades y conocimientos técnicos (43% de los empleadores con vacantes difíciles de cubrir). Este año, las menciones de la competencia de otros empleadores han aumentado (del 9% en 2021 al 25 % en 2022), y ahora más personas también mencionan una falta general de candidatos (del 13% al 25%).

03

EL MERCADO LABORAL DE CIBERSEGURIDAD ENFRENTA UNA COMBINACIÓN ÚNICA DE DESAFÍOS

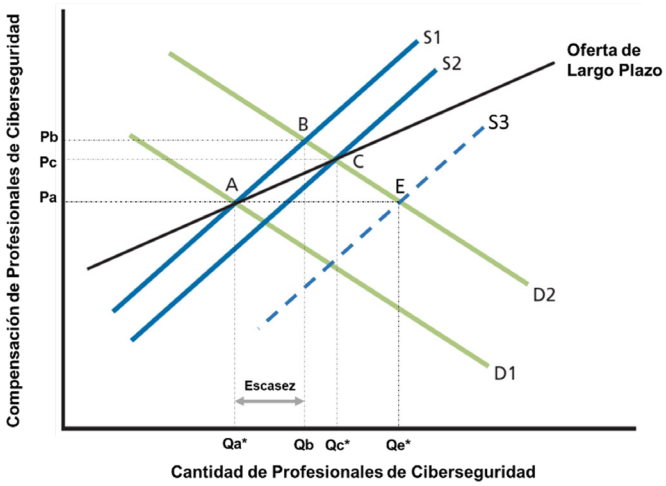
El análisis de los desafíos que enfrenta el mercado laboral de ciberseguridad ayuda a los países a estar preparados para enfrentar conflictos en el ciberespacio y a las organizaciones a identificar brechas clave en la fuerza laboral actual que pueden impactar el cumplimiento de objetivos empresariales y sectoriales. A continuación, se analiza dicho mercado laboral, se caracteriza de manera general y esquemática la oferta y la demanda laborales en ciberseguridad, se describe la fuerza laboral de ciberseguridad y se identifica una problemática y un conjunto de desafíos que se deben abordar de manera integral por las múltiples partes interesadas, especialmente en la región América Latina y el Caribe.

3.1. EL MERCADO LABORAL

Desde la perspectiva económica, el mercado laboral de ciberseguridad sigue los mismos principios del libre mercado, donde rige la regla de la oferta y la demanda. El mercado de trabajo es el lugar donde se encuentran la oferta y la demanda de puestos de trabajo, donde los trabajadores o la mano de obra prestan los servicios que demandan los empleadores.

La siguiente figura presenta una visión simplificada del mercado laboral de ciberseguridad. En el pasado reciente, la oferta y la demanda se encontraron en el punto A (una cantidad de profesionales Qa* con una compensación Pa). Como se ha evidenciado, la demanda de profesionales de ciberseguridad ha aumentado considerablemente. Este aumento puede deberse a múltiples factores, incluyendo mayor conectividad, mayor digitalización, mayor transformación digital, más actividades económicas en el entorno digital, mayores vulnerabilidades, entre otros. Estos eventos empujaron la curva de demanda hacia la derecha, de D1 a D2. El movimiento de la curva de demanda implica que, como se observa en el mercado actual, muchos empleadores están dispuestos a pagar más (Pb) para contratar la misma calidad y tipo de profesional que contrataban antes. El aumento de la demanda, en los últimos años, ha sido más exacerbado debido a la pandemia de COVID-19, y se necesita tiempo para desarrollar más profesionales de ciberseguridad en respuesta a la mayor demanda.

Gráfica 7.
Fuerzas del mercado laboral de ciberseguridad



Fuente: Adaptado de (RAND, 2014)

La capacitación y la educación pueden llevar años en generar otra situación de equilibrio en el mercado laboral de ciberseguridad. Incluso si los trabajadores individuales en otras ocupaciones y en otros sectores tienen el conjunto adecuado de habilidades para convertirse en profesionales de ciberseguridad, es posible que no cambien de ocupación o de sector de inmediato. Por lo tanto, a corto plazo, la curva de oferta es bastante inelástica o, en otras palabras, no responde mucho al precio. Esta situación también provoca escasez de profesionales, por ejemplo (ISC, 2021) y (ISC, 2022a) estiman una escasez entre 515.000 y 701.000 profesionales para la región América Latina y el Caribe. El punto B puede verse como un equilibrio a corto plazo y, a largo plazo, el mercado debería alcanzar un nuevo equilibrio en el punto C (una cantidad de profesionales Qc* con una compensación Pc).

Como se muestra en la anterior figura, es probable que la curva de oferta a largo plazo sea más elástica (más sensible al precio) que las curvas de oferta a corto plazo, porque es más fácil para las personas entrar y salir de una profesión a largo plazo. Por ejemplo, se podría encontrar un nuevo equilibrio en el punto E (una cantidad Qe* con una compensación Pa) cuando la curva de oferta se mueve hacia la derecha de S2 a S3, habiendo más profesionales de ciberseguridad en el mercado con compensaciones más bajas. No obstante, movimientos de las curvas de oferta y de demanda laboral junto con los efectos en las brechas y en los precios dependen de las acciones que adelanten todas las múltiples partes interesadas que intervienen en el mercado laboral de ciberseguridad.

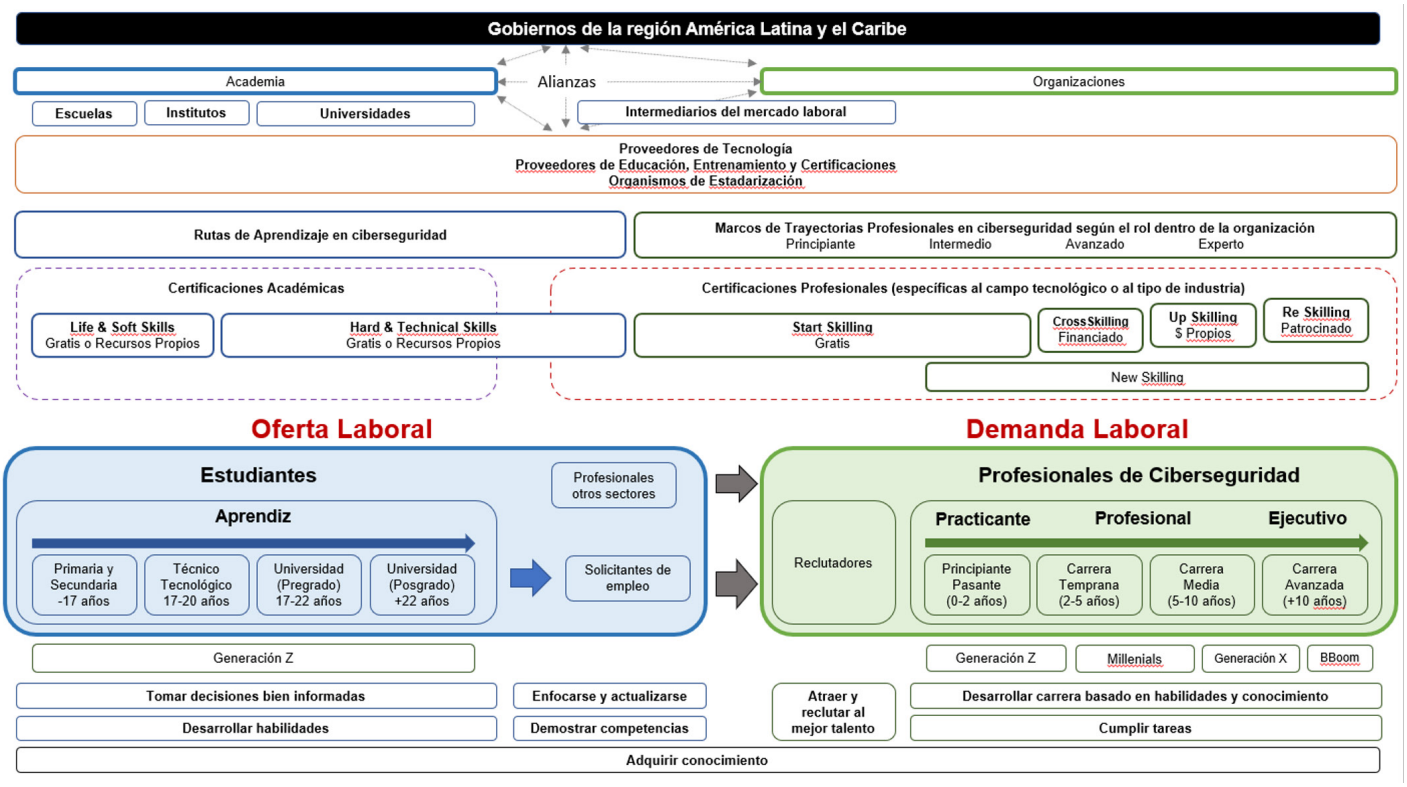
Ahora, en la siguiente figura se caracteriza de manera general y esquemática la oferta y la demanda laboral en ciberseguridad en la región. Por una parte, la oferta laboral la componen: i) aquellos recién graduados, ii) aquellos profesionales de otros sectores o industrias que pueden tener experiencia en tecnología y iii) aquellos quienes no tienen antecedentes técnicos, pero sí otros conocimientos que se pueden aplicar en un puesto de trabajo relacionado con la ciberseguridad[28].

También es importante tener en cuenta a los actuales estudiantes, los cuales se encuentran en los niveles primario, secundario y terciario de los sistemas educativos de la región. Algunos incluso en niveles de posgrado. En términos generales, estos estudiantes pertenecen a la Generación Z o *"Centenialls"*[29], personas que tienen características diferentes a las anteriores generaciones porque han nacido bajo normas, pautas y conceptos nuevos que corresponden al mundo digital.

Estos estudiantes deben desarrollar habilidades y tomar decisiones bien informadas mientras que los solicitantes de empleo deben demostrar competencias, enfocarse y actualizarse.

28 Según (CSES, 2018), desde la oferta laboral existen al menos seis caminos hacia trabajos de ciberseguridad de nivel de entrada: i) ruta de aprendizaje (secundaria con know-how), ii) ruta de educación continua (secundaria con certificaciones), iii) ruta del primer grado STEM (pregrado), iv) ruta del primer grado no STEM (pregrado), v) ruta de grado superior (posgrado), y vi) ruta de cambio de carrera.
29 Personas nacidas entre los años 1997 y 2010.

Gráfica 8.
Caracterización esquemática de la oferta laboral y de la demanda laboral de ciberseguridad en la región



Fuente: Elaboración propia

El actor más representativo y que genera impactos en la oferta laboral es la Academia, en particular las escuelas, institutos y universidades. Dado que el estudiante (futuro solicitante de empleo) es el *vendedor* en el mercado laboral de ciberseguridad, cuyo valor está determinado por las habilidades que posea, es muy importante que las instituciones que representan a la Academia le brinden la oportunidad de desarrollar una amplia gama de habilidades (habilidades de vida, habilidades blandas, habilidades técnicas y habilidades duras) para incursionar en el campo cibernético.

Por otra parte, la demanda laboral está representada por Organizaciones que demandan profesionales de ciberseguridad, los cuales puede clasificarse como aprendices o practicantes[30], profesionales y ejecutivos, dependiendo del tiempo que lleven siendo parte de la fuerza laboral. En esta fuerza laboral intervienen personas de varias generaciones, por ejemplo, los practicantes generalmente pertenecen a la Generación Z, los profesionales pueden estar conformados por personas que pertenecen a la Generación Z, Generación Y o *Millenials*[31] o Generación X[32], y finalmente los ejecutivos pueden personas que pertenecen a la Generación X o *Baby Boomers*[33].

Los profesionales de ciberseguridad de la fuerza laboral deben cumplir tareas y desarrollar una carrera basada en habilidades y conocimiento.

30 Según (DCMS & IPSOS, 2022), alrededor de 1 de cada 3 empresas cibernéticas (27%) en Reino Unido informó haber ofrecido pasantías o prácticas laborales desde principios de 2020 (aproximadamente durante un período de 18 meses).
31 Personas nacidas entre los años 1981 y 1996, llamados nativos digitales y la primera generación que es realmente global por compartir los mismos valores en todos los países gracias a la globalización y a la conexión a través de Internet.
32 Personas nacidas entre los años 1965 y 1980, que se han adaptado con gran facilidad a la llegada de Internet a sus vidas y al desarrollo tecnológico posterior.
33 Personas nacidas entre los años 1946 y 1964, que han tenido que adaptarse a las nuevas tecnologías y por esa razón son considerados como inmigrantes digitales.

Los actores más representativos y que generan impactos en la demanda laboral son las organizaciones tanto públicas como privadas en todos los sectores económicos, las cuales tienen áreas de recursos humanos encargados de identificar, atraer y reclutar el talento. El *comprador* del mercado laboral representa al sector empleador, ya sea privado o público, e ingresa al mercado laboral con la intención de comprar el servicio de una persona que pueda realizar las tareas demandadas.

Finalmente, se presentan los intermediarios del mercado laboral como las agencias reclutadoras e incluso plataformas integradoras de redes profesionales. Adicionalmente, se tiene a los Proveedores de Educación, Entrenamiento y Certificaciones y a los Proveedores de Tecnología que ofrecen herramientas, recursos y contenidos para desarrollar capacidades tanto a estudiantes como a profesionales, ya sea por medio de rutas de aprendizaje o por medio de marcos de trayectoria profesional mediante el otorgamiento de certificaciones que pueden ser académicas[34] o profesionales[35], éstas últimas específicas al campo tecnológico o al tipo de industria[36]. Con apoyo de estos proveedores, las organizaciones pueden implementar planes de *crosskilling, upskilling, reskilling* y *new skilling*, entre otros, con el fin de retener y mantener a su fuerza laboral de ciberseguridad.

3.2. LA FUERZA LABORAL

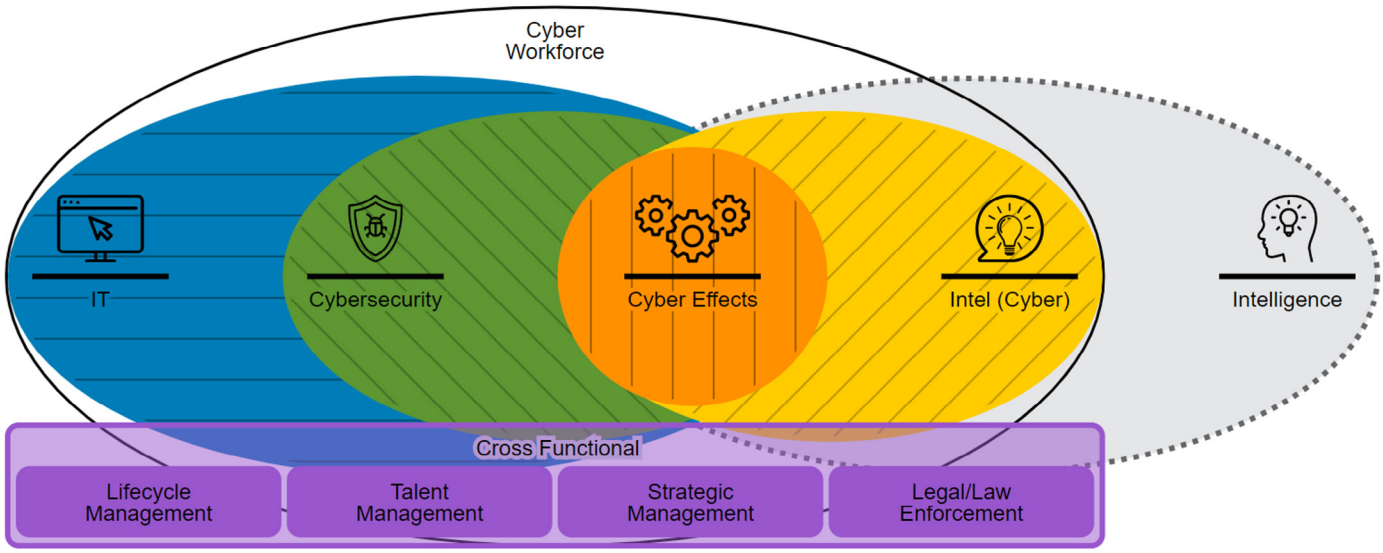
En línea con lo dispuesto en el *Marco del Personal para la Ciberseguridad*[37] de la *Iniciativa Nacional para la Educación en Ciberseguridad* (en inglés, National Initiative for Cybersecurity Education -NICE-) del *Instituto Nacional de Normas y Tecnología* de los Estados Unidos (en inglés, National Institute of Standards and Technology -NIST-), la fuerza laboral en ciberseguridad puede ser considerada como el conjunto de personas (que poseen conocimientos y habilidades) para ejecutar tareas con el fin de lograr los objetivos de gestión de riesgos de ciberseguridad de una organización. Estas personas pueden ser internas o externas a la organización[38].

Un ejemplo de definición de fuerza laboral se aprecia en la herramienta *"Cyber Career Pathways Tool"*[39] basada en el *Marco del Personal para la Ciberseguridad* del NICE y elaborada por la *Iniciativa Nacional de Carreras y Estudios en Ciberseguridad* (en inglés, National Initiative for Cybersecurity Careers and Studies -NICCS-). La fuerza de trabajo en ciberseguridad es el conjunto de profesionales dentro de una organización con habilidades necesarias para: i) construir, asegurar, operar, defender y proteger la tecnología, los datos y los recursos, ii) realizar actividades de inteligencia relacionadas, iii) permitir futuras operaciones, y iv) proyectar poder en o a través del ciberespacio.

34 Las certificaciones académicas de ciberseguridad están diseñadas para proporcionar a los estudiantes una formación profunda sobre algunos de los problemas actuales en el campo de la ciberseguridad. Estos cursos generalmente se combinan con otros cursos y programas de certificación para brindar a los estudiantes las habilidades y la experiencia necesarias para comenzar en la creciente industria de la ciberseguridad.
35 Las certificaciones profesionales de ciberseguridad están diseñadas para personas que ya trabajan en el campo de la ciberseguridad (o campos de TI y redes estrechamente relacionados) para capacitarse en algunas de las últimas herramientas y software para detectar, prevenir y combatir los problemas de ciberseguridad. Estas certificaciones se utilizan para demostrar competencia con tecnologías específicas.
36 Una hoja de ruta de certificaciones de ciberseguridad puede ser consultado en: https://pauljerimy.com/security-certification-roadmap/
37 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1es.pdf
38 Según (DCMS & IPSOS, 2022), alrededor de un tercio de las empresas en el Reino Unido subcontratan cualquier aspecto de la ciberseguridad.
39 https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool

Gráfica 9.

Representación esquemática de la fuerza laboral de una organización y las comunidades de profesionales que la componen



Fuente: (NICCS, 2022)

Según (NICCS, 2022), la fuerza laboral de una organización puede estar compuesta por las siguientes comunidades de profesionales, con habilidades distintas pero complementarias:

A *Tecnologías de la Información -TI-:* profesionales con habilidades necesarias para diseñar, construir, configurar, operar y mantener TI, redes y capacidades. Esto incluye acciones para priorizar inversiones de cartera; diseñar, adquirir, implementar, evaluar y disponer de TI, así como la gestión de recursos de información; y la gestión, almacenamiento, transmisión y visualización de datos e información.

B *Ciberseguridad:* profesionales con habilidades necesarias para asegurar, defender y preservar datos, redes, capacidades centradas en la red y otros sistemas designados al garantizar que se implementen los controles y medidas de seguridad adecuados y tomar medidas de defensa interna. Esto incluye el acceso a los controles del sistema, el monitoreo, la administración y la integración de la ciberseguridad en todos los aspectos de la ingeniería y la adquisición de capacidades cibernéticas.

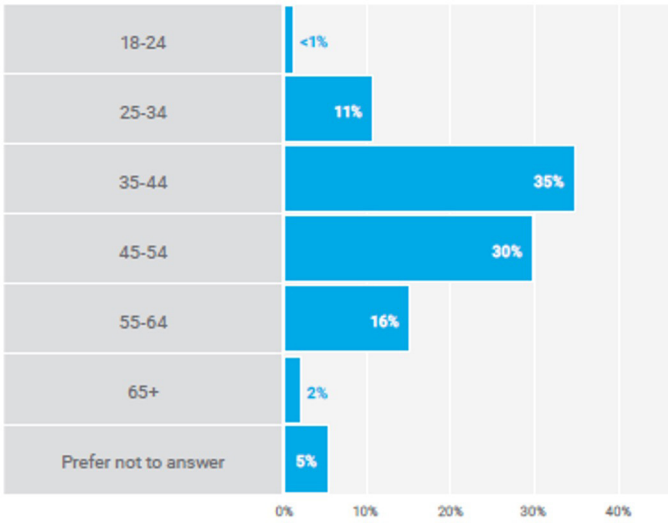
C *Efectos cibernéticos:* profesionales con habilidades requeridas para planificar, apoyar y ejecutar capacidades cibernéticas donde el propósito principal es defender externamente o realizar proyección de fuerza en o a través del ciberespacio.

D *Inteligencia cibernética:* profesionales con habilidades necesarias para recopilar, procesar, analizar y difundir información de todas las fuentes de inteligencia sobre programas cibernéticos, intenciones, capacidades, investigación y desarrollo y actividades operativas de actores extranjeros.

E *Funcional cruzado:* profesionales con habilidades necesarias para liderar, adquirir y gestionar iniciativas cibernéticas; desarrollar el talento de la fuerza laboral cibernética; y llevar a cabo actividades legales y de aplicación de la ley relacionadas con la cibernética.

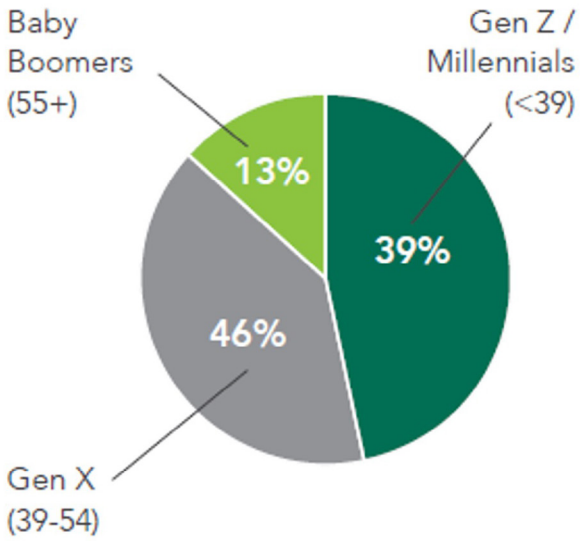
Actualmente, la fuerza laboral la componen profesionales entre los 25 y los 65 años[40] aproximadamente. Es decir, existe una diversidad generacional, ya que las personas pertenecen a las cuatro cohortes demográficas (Generaciones Z, Y, X y Baby Boomers). El conjunto de estas cuatro generaciones de talento no solo debe convivir dentro de las organizaciones, sino que, con sus características propias y sus diferencias, deben comprenderse entre ellas y complementarse.

Gráfica 10.
Fuerza laboral por edad



Fuente: (ISACA, 2022)

Gráfica 11.
Representación por generaciones



Fuente: (ISACA, 2021)

Actualmente, los principales sectores que demandan profesionales de ciberseguridad son el sector TIC, el sector financiero y asegurador y el sector de telecomunicaciones. La contratación en el sector público también representa una mayor cuota de mercado durante los últimos años.

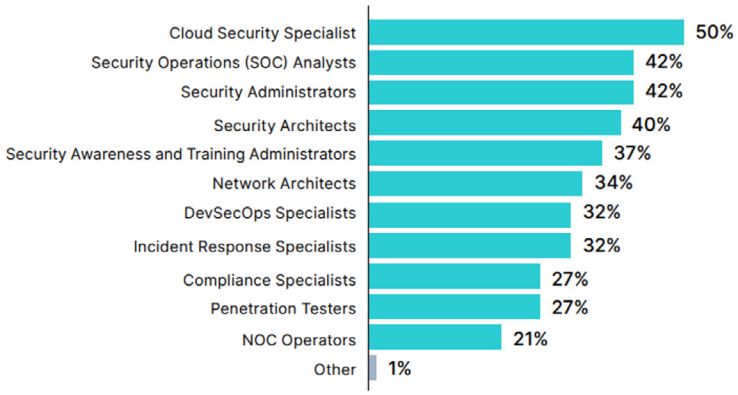
Gráfica 12.
Porcentaje de anuncios de trabajo para principales roles cibernéticos provenientes de sectores específicos en el Reino Unido

Nota: A partir de 8.426 publicaciones de empleo cibernético de enero a diciembre de 2021. Fuente: (DCMS & IPSOS, 2022.

40 Se destaca que la mayoría (35%) son personas entre los 35 y 44 años. Se resalta que esta situación puede impactar la fuerza laboral en ciberseguridad ya que, según (Cook, 2021), los empleados entre 30 y 45 años han impulsado el fenómeno de la *Gran Renuncia*, ya que han tenido el mayor aumento en las tasas de renuncia en Estados Unidos, con un aumento promedio de más del 20% entre 2020 y 2021.

Existe una gama amplia de roles y especialidades (especialistas, analistas, entre otros) de ciberseguridad demandados en el mercado laboral[41]. Se destaca, por ejemplo, los siguientes roles solicitados por empleadores dentro del mercado laboral de ciberseguridad de los Estados Unidos: analista de ciberseguridad, desarrollador de software, consultor de ciberseguridad, entre otros.

Gráfica 13.
Principales roles de trabajo en ciberseguridad solicitados



Fuente: (FORTINET, 2022)

Gráfica 14.
Principales roles de trabajo en ciberseguridad solicitados en Estados Unidos

Nota: Dato de septiembre de 2022
Fuente: (CyberSeek, 2022)

Los principales requisitos de habilidades blandas (en inglés, soft skills) en descripciones de puestos de ciberseguridad en el Reino Unido son: habilidades comunicacionales, pensamiento creativo, resolución de problemas, trabajo en equipo y atención a los detalles. Según (MichaelPage, 2022), el top 5 de las habilidades blandas más requeridas en 2022 en América Latina y el Caribe son: adaptabilidad, pensamiento creativo, trabajo en equipo, inteligencia emocional y resiliencia.

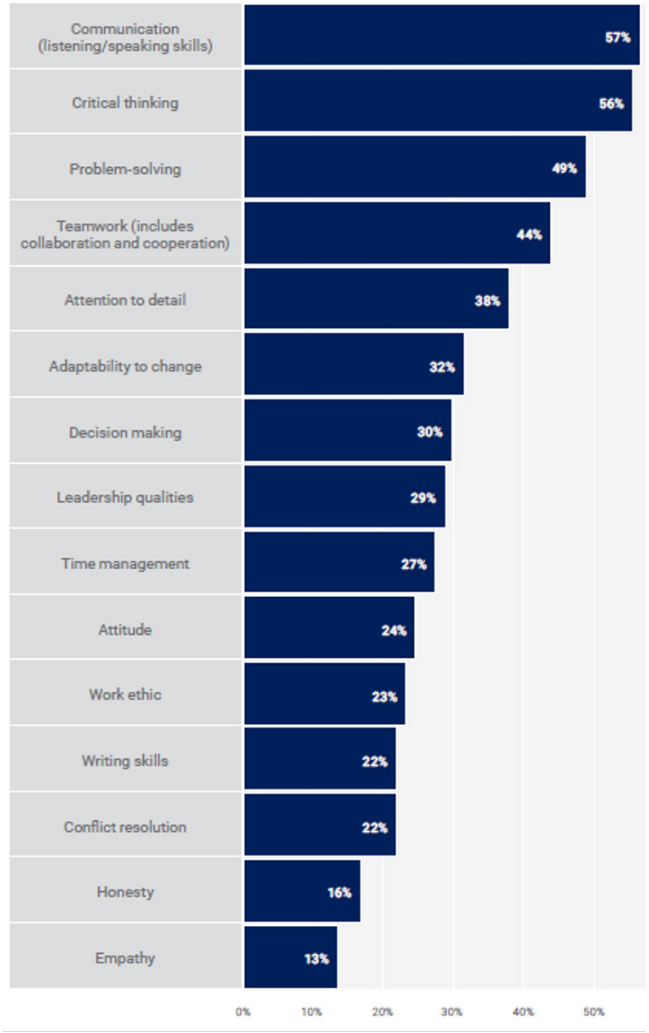
Gráfica 15.
Principales atributos requeridos para personal de ciberseguridad

Fuente: (ISC2, 2021)

41 Según (CyberSeek, 2022), en los Estados Unidos existen 714.548 ofertas de trabajo en línea para puestos relacionados con ciberseguridad desde mayo de 2021 hasta abril de 2022. Según (DCMS & IPSOS, 2022), entre enero de 2021 y diciembre de 2021 hubo 153.192 ofertas de empleo en ciberseguridad en el Reino Unido.

Gráfica 16.

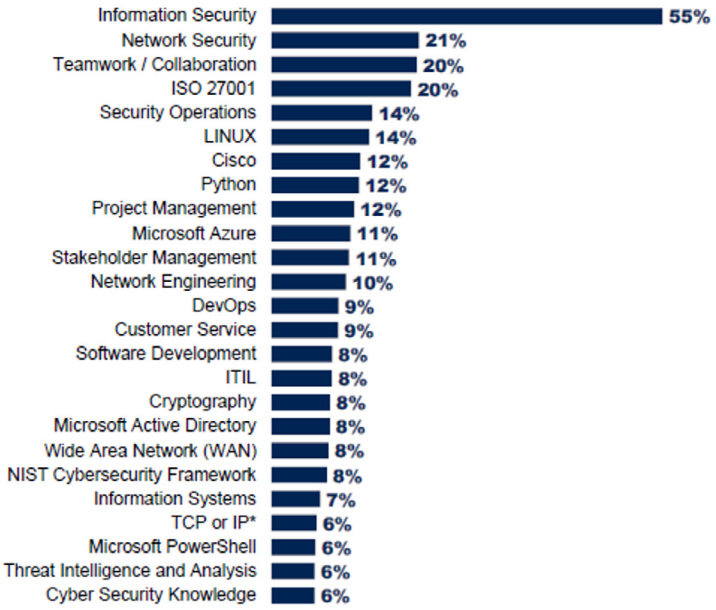
Principales habilidades blandas para roles de trabajo cibernéticos en el sector de ciberseguridad



Fuente: (ISACA, 2022)

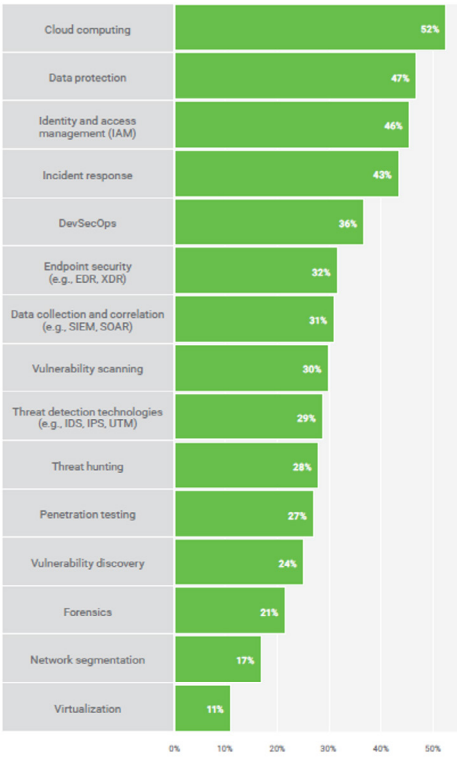
Los principales requisitos de habilidades técnicas en descripciones de puestos de ciberseguridad en el Reino Unido son: habilidades de seguridad de la información, habilidades de seguridad de redes y habilidades en torno a estándares, como la ISO 27001 (el estándar internacional de seguridad de la información). Otras áreas de habilidades técnicas requeridas en profesionales de ciberseguridad en el mercado laboral incluyen: computación en la nube (en inglés, cloud computing), desarrollo, seguridad y operaciones (en inglés, DevSecOps), gestión de riesgos y controles técnicos, conocimiento de sistemas operativos y virtualización, criptografía y programación.

Gráfica 17.
Principales habilidades técnicas solicitadas para principales roles de trabajo cibernéticos en el Reino Unido



Nota: A partir de 35.103 publicaciones de trabajos cibernéticos de enero a diciembre de 2021 que solicitan al menos una habilidad específica
Fuente: (DCMS & IPSOS, 2022)

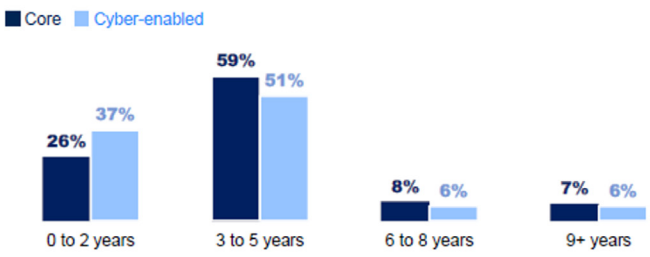
Gráfica 18.
Principales habilidades técnicas para roles de trabajo cibernéticos en el sector de ciberseguridad



Fuente: (ISACA, 2022)

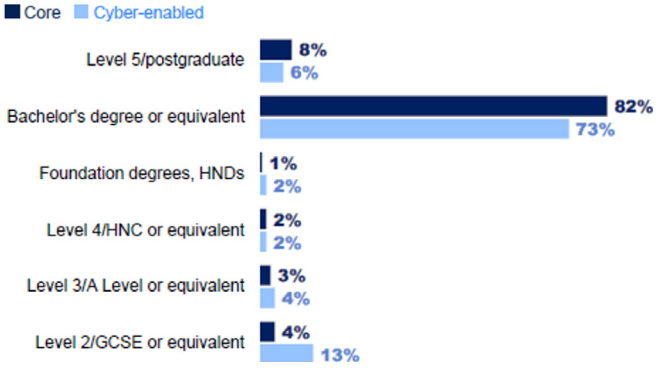
Durante los últimos años, las organizaciones buscan profesionales para roles de trabajo en ciberseguridad con 3 a 5 años de experiencia seguidos de solicitantes de nivel inicial con grado de licenciatura o equivalente.

Gráfica 19.
Niveles de experiencia mínima solicitados para roles de trabajo cibernéticos en el Reino Unido (principales y relacionados)



Nota: A partir de 31.307 publicaciones de trabajos cibernéticos (principales y relacionados) de enero a diciembre de 2021
Fuente: (DCMS & IPSOS, 2022)

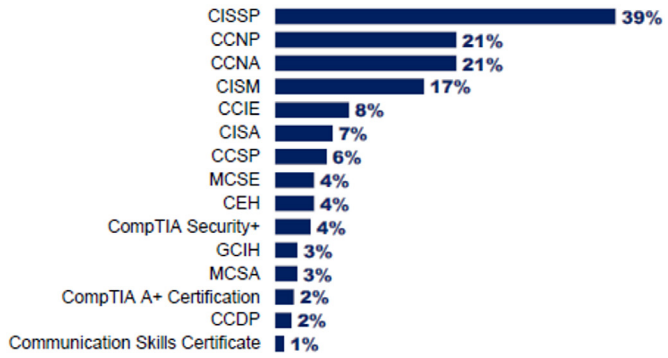
Gráfica 20.
Niveles mínimos de educación solicitados para roles de trabajo cibernéticos en el Reino Unido (principales y relacionados)



Nota: A partir de 30.472 publicaciones de trabajos cibernéticos (principales y relacionados) de enero a diciembre de 2021
Fuente: (DCMS & IPSOS, 2022)

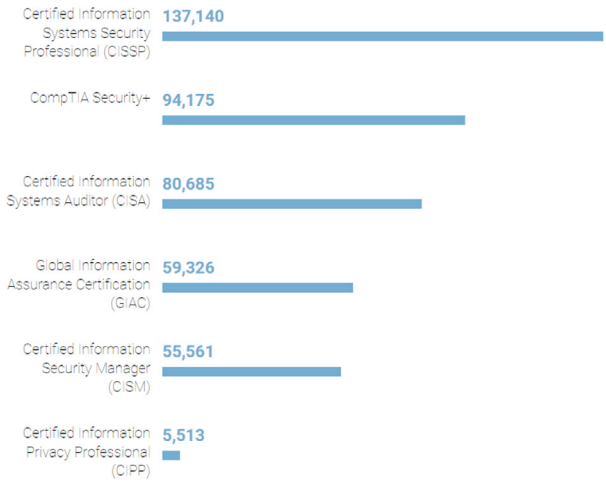
Adicionalmente, se resalta la importancia de que la oferta laboral cuente con certificaciones en tecnología de la información y seguridad de la información. Se destaca que el certificado *Certified Information Systems Security Professional (CISSP)* es la principal certificación solicitada para principales roles cibernéticos a nivel global. En el Reino Unido, las certificaciones de *Cisco Certified Network* también continúan teniendo una gran demanda, por ejemplo, Cisco Certified Network Professionals (CCNP) y Cisco Certified Network Associates (CCNA). En el mercado laboral de Estados Unidos, se valoran las certificaciones CompTIA Security+ y aquellas de la Asociación de Auditoría y Control de Sistemas de Información (en inglés, Information Systems Audit and Control Association -ISACA-) como la Certified Information Systems Auditor (CISA) y la Certified Information Security Manager (CISM).

Gráfica 21.
Principales certificaciones solicitadas para principales roles cibernéticos en Reino Unido



Nota: A partir de 11.086 publicaciones de empleo cibernético de enero a diciembre de 2021
Fuente: (DCMS & IPSOS, 2022)

Gráfica 22.
Principales certificaciones solicitadas para principales roles cibernéticos en Estados Unidos



Nota: Dato de septiembre de 2022
Fuente: (CyberSeek, 2022)

Cuadro 1.
Principales Certificaciones de Tecnología de la Información y Seguridad de la Información

Proveedor		Certificación	Certificación
(ISC)²	CISSP	Certified Information Systems Security Professional	USD 749
ISACA	CISA	Certified Information Systems Auditor	USD 575 miembros ISACA, USD 760 no miembros
ISACA	CISM	Certified Information Security Manager	USD 575 miembros ISACA, USD 760 no miembros
CompTIA	Security+	CompTIA Security+	USD 381
EC-Council	CEH	Certified Ethical Hacker	USD 950 a USD 1.199, dependiendo de lugar
GIAC	GSEC	GIAC Security Essentials Certification	USD 2.499
(ISC)²	SSCP	Systems Security Certified Practitioner	USD 249
CompTIA	CASP+	CompTIA Advanced Security Practitioner	USD 480
GIAC	GCIH	GIAC Certified Incident Handler	USD 2.499
Offensive Security	OSCP	Offensive Security Certified Professional	USD 999 a USD 5.499

Fuente: Coursera (2022)[42] y ComputerScienceMS (2022)[43]

42 https://www.coursera.org/articles/popular-cybersecurity-certifications
43 https://computersciencems.com/resources/cyber-security/best-cybersecurity-certifications/

3.3. LOS PRINCIPALES DESAFÍOS

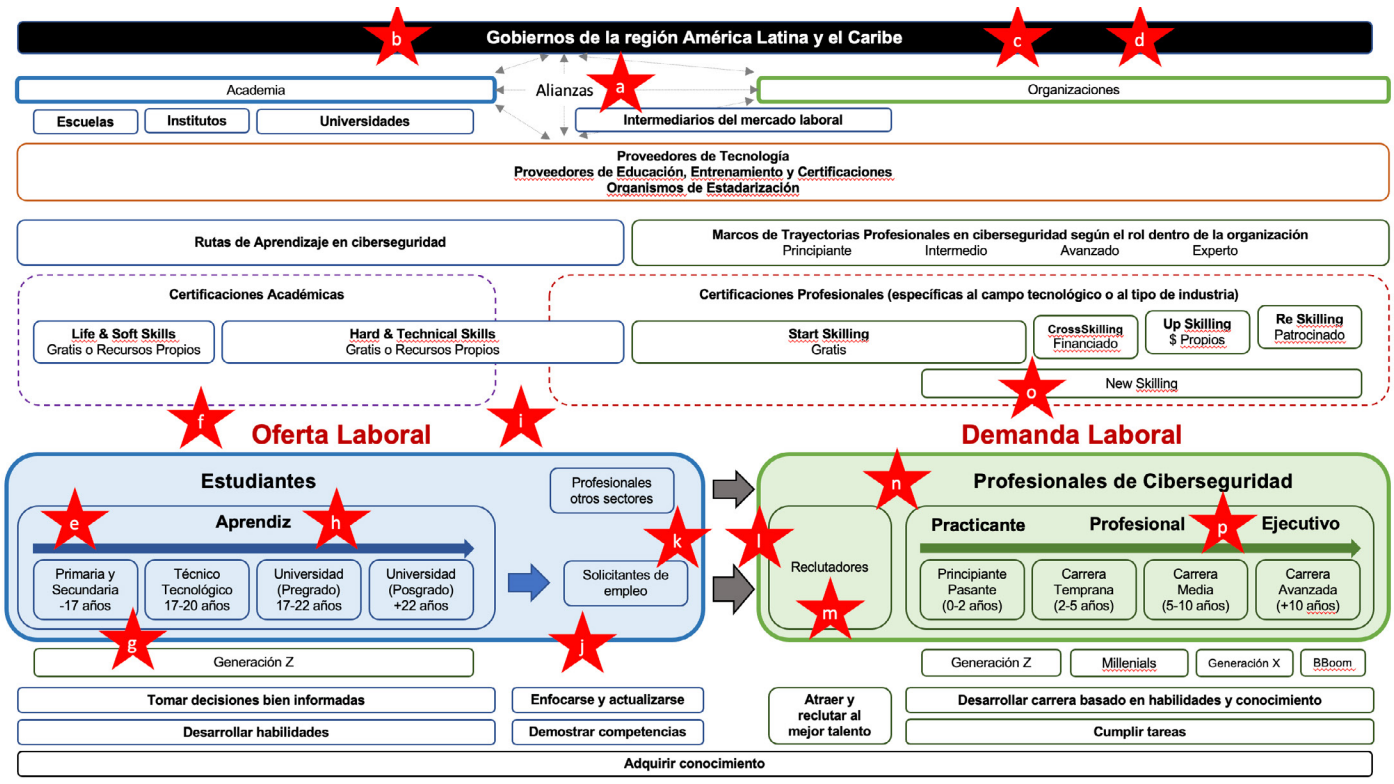
Las habilidades y capacidades sólidas en ciberseguridad son un motor clave de la actividad económica en la región América Latina y el Caribe y son fundamentales para su prosperidad futura. La escasez tanto de profesionales de ciberseguridad como de habilidades de este talento humano puede ser causada por una combinación única de desafíos para la región, en donde se estima que actualmente se puede necesitar entre 515.000 y 701.000 profesionales adicionales para posiciones técnicas y no técnicas. Por lo tanto, se identifica que la región enfrenta el siguiente problema:

> ***La demanda de profesionales de ciberseguridad en América Latina y el Caribe continúa superando la oferta, lo que resulta en una creciente brecha (escasez) en la fuerza laboral de ciberseguridad.*** *Esos puestos vacantes en las organizaciones públicas y privadas pueden derivar en amenazas, ataques e incidentes cibernéticos, con graves consecuencias de tipo económico o social, y pueden dejar a los países de la región mal preparados para enfrentar conflictos en el ciberespacio.*

Los desafíos en el mercado laboral de ciberseguridad, en torno a este problema, pueden ser identificados tanto por el lado de la oferta laboral como por el lado de la demanda laboral. A continuación, se identifican algunos grandes desafíos que afrontan los países de la región.

Gráfica 23.

Representación esquemática de los desafíos en el mercado laboral de ciberseguridad en la región



Fuente: Elaboración propia

Se identifican los siguientes desafíos para los gobiernos de la región:

A Esfuerzos aislados para el desarrollo de fuerza laboral y la promoción de alianzas nacionales e internacionales

B Débil marco regulatorio y articulación institucional

C Insuficiente información estratégica a nivel nacional para la toma de decisiones

D Insuficiente sensibilización y divulgación sobre recursos, herramientas e información para el desarrollo de la fuerza laboral en ciberseguridad

Por el lado de la oferta laboral de ciberseguridad, se identifican los siguientes desafíos:

E Insuficiente desarrollo de vocaciones STEM y bajas habilidades digitales en las niñas y en los niños de la región

F Bajo / moderado dominio del inglés en la región

G Falta de conciencia y educación en ciberseguridad en edades tempranas

H Desconocimiento de la oferta educativa por parte de los estudiantes

I Desconexión entre la educación, la formación y la industria

J Desconocimiento de las rutas de aprendizaje por parte de los solicitantes de empleo

K Débil entendimiento de la definición de la profesión en ciberseguridad

Por el lado de la demanda laboral de ciberseguridad, se identifican los siguientes desafíos:

L Inexistencia de un lenguaje común entre la demanda y la oferta laborales

M Preferencia de la experiencia sobre las calificaciones en las organizaciones

N Rezago en diversidad, equidad e inclusión en la fuerza laboral

O Dificultades para el acceso a los marcos de trayectorias profesionales

P Débiles programas de retención en las organizaciones

04

ANÁLISIS PARA EL DESARROLLO DE LA FUERZA LABORAL EN LA REGIÓN

A pesar de los esfuerzos de los países en la región América Latina y el Caribe, una cantidad sustancial de puestos vacantes de ciberseguridad siguen sin cubrirse porque las organizaciones no pueden encontrar los talentos adecuados. En respuesta a esta situación, los sistemas educativos en la región han comenzado a movilizarse, con un gran número de instituciones y entidades educativas creando y lanzando nuevos títulos y cursos de ciberseguridad. De igual manera, los *Proveedores de Educación, Entrenamiento y Certificaciones* y los *Proveedores de Tecnología* fortalecen sus herramientas, recursos y contenidos para desarrollar capacidades y habilidades de profesionales de la actual fuerza laboral de ciberseguridad.

No obstante, la escasez de habilidades en ciberseguridad en la región genera impactos en el mercado laboral y seguirá siendo grave a mediano plazo. Para desarrollar defensas cibernéticas fuertes, la región necesita construir y desarrollar una fuerza laboral en ciberseguridad más diversa con más y mejores habilidades técnicas y no técnicas. Mejorar el equilibrio de género también ayudará a que esta fuerza laboral crezca y madure. Estrechar los vínculos entre las competencias ofrecidas por los sistemas educativos y las necesidades del mercado laboral es una prioridad para el cierre de brechas de capital humano en ciberseguridad.

Por tal razón, a continuación, se presentan consideraciones tanto por el lado de la oferta laboral como por el lado de la demanda laboral de profesionales de ciberseguridad con el fin de que el ecosistema de ciberseguridad trabaje integralmente en el desarrollo de la fuerza laboral en la región. Para cada desafío identificado se hace un análisis en tres (3) partes: una descripción de la importancia del tema que aborda el desafío, unos soportes o evidencias de la situación actual a nivel global o regional y una descripción de buenas prácticas para abordar el desafío. Adicionalmente, se presentan algunas consideraciones para los gobiernos de América Latina y el Caribe.

4.1. DESDE LA OFERTA LABORAL

La nueva generación de estudiantes y de profesionales de otros sectores necesita habilidades personales y profesionales para prepararse para las oportunidades actuales y futuras del mercado laboral de ciberseguridad.

Del análisis de los desafíos identificados por el lado de la oferta laboral de ciberseguridad, a continuación, se presentan consideraciones con el fin de:

- Incrementar las vocaciones científicas en la población infantil y juvenil de la región
- Fortalecer el dominio del inglés en la región
- Concientizar y sensibilizar en ciberseguridad durante la edad temprana
- Promover el acceso a la oferta educativa
- Conectar la educación con la formación y la industria
- Promover el acceso a las rutas de aprendizaje
- Aclarar la definición de la profesión en ciberseguridad

Incrementar las vocaciones científicas en la población infantil y juvenil de la región

Relevancia

El desarrollo de la fuerza laboral en ciberseguridad debe comenzar en las escuelas primarias y secundarias. Cuantas más escuelas alienten a los estudiantes a considerar una carrera en ciberseguridad y cuanto más fomenten las habilidades tempranas, mayor será la calidad de los estudiantes en el sistema de educación terciaria. Esto significa que las escuelas deben poner mayor énfasis en el desarrollo de habilidades de ciberseguridad en los programas curriculares y extracurriculares como caminos hacia la educación superior. Las habilidades aprendidas en la educación STEM son las mismas habilidades requeridas para una carrera en ciberseguridad. Prácticamente todos los roles en el mercado laboral de ciberseguridad requieren habilidades relacionadas con STEM. A medida que más trabajadores con habilidades basadas en STEM ingresan a la fuerza laboral de ciberseguridad, es probable que las empresas y otras organizaciones vean menos ataques cibernéticos exitosos y experimenten menos daños económicos por esos ataques (WICKR, 2021).

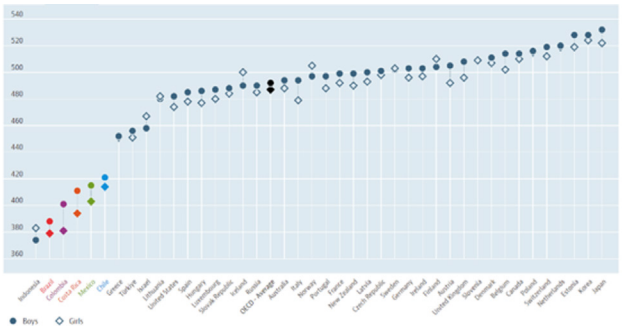
Retos

En América Latina y el Caribe existe una insuficiente formación en áreas del conocimiento de STEM al nivel de educación básica, media y secundaria. Los resultados de la última medición de PISA confirman que, en promedio, los estudiantes de 15 años de la región están tres (3) años atrasados en lectura, matemáticas y ciencias con respecto a un estudiante en un país de la OCDE. También se aprecia una brecha de género en el desarrollo de competencias en STEM (World Bank, 2019). Adicionalmente, tan solo el 2,68% de los matriculados en el nivel de educación superior en la región corresponde a estudiantes en áreas relacionadas con matemáticas, ciencias, y estadística. Lo anterior resulta problemático al compararlo con el promedio de los países de la OCDE, en cuyos casos, las matrículas en áreas relacionadas con las mismas áreas del conocimiento alcanzaron el 6,24% (DNP, 2022).

Algunas cifras

Gráfica 24.

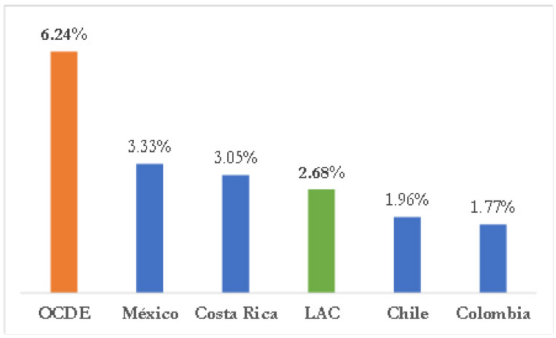
Rendimiento (puntuación media) en competencias matemáticas discriminado entre niños y niñas a partir de PISA 2018



Fuente: (OECD, 2022)

Gráfica 25.

Proporción de matriculados en programas universitarios en áreas STEM



Fuente: (DNP, 2022)

Buenas prácticas

La educación STEM es un esfuerzo global para mejorar las habilidades científicas, tecnológicas, de ingeniería y matemáticas de niños y jóvenes. Cada país del mundo tiene un enfoque diferente para implementarlo, algunos lo están integrando en sus políticas educativas, otros lo están implementando a través de organizaciones externas. La *Estrategia de Educación de Estonia (2021-2035)*[44] hace énfasis en las habilidades STEM que crean más valor agregado para mejorar la formación continua y las oportunidades de readiestramiento, incluido el aprendizaje basado en el trabajo. Singapur ha incorporado el *Programa de Aprendizaje Aplicado STEM (ALP)*[45] en sus escuelas secundarias en conjunto con STEM Inc, una unidad del Centro de Ciencias de Singapur. La educación STEAM integrada en Corea del Sur es un enfoque para preparar una fuerza laboral STEM de calidad y ciudadanos alfabetizados para una sociedad altamente tecnológica mediante la integración de la ciencia, la tecnología, la ingeniería, las artes y las matemáticas en la educación (Kang, 2019). La OEA ofrece en la región la *Diplomatura en Educación STEM-STEAM*[46] a docentes y agentes educativos para fortalecer el diseño e implementación de prácticas, proyectos o programas en educación STEM. Colombia ha lanzado el *Programa Ruta STEM 2022*[47] por que busca el fortalecimiento de capacidades de 5.000 profesores y 100.000 estudiantes de educación básica y media del país en tecnología, ciencia, ingeniería y matemáticas.

44 https://www.hm.ee/sites/default/files/haridusvaldkonna_arengukava_2035_kinnittaud_vv_eng.pdf
45 https://www.science.edu.sg/stem-inc/about-us/about-stem-inc
46 https://www.oas.org/en/scholarships/professionaldev/Courses_2022/Anuncio-PDSP-Educacion_STEM-STEAM.pdf
47 https://www.mineducacion.gov.co/portal/salaprensa/Noticias/410966:Gobierno-nacional-lanza-Ruta-Stem-2022-para-fortalecer-las-capacidades-de-docentes-y-estudiantes-del-pais-en-tecnologia-ciencia-ingenieria-y-matematicas

Fortalecer el dominio del inglés en la región

Relevancia

Actualmente, el inglés es el idioma predeterminado en negocios internacionales, diplomacia, entretenimiento, ciencia, tecnología y, en particular, en ciberseguridad. El inglés es el idioma más utilizado en el mundo tanto por hablantes nativos como no nativos. Se estima que 1,45 billones de personas (18,2% de la población total) hablan inglés, mientras que 548 millones aprox. (6,9% del total) hablan español y 258 millones aprox. (3,2%) hablan portugués (ETHNOLOGUE, 2022). Además, el inglés sigue siendo el idioma más utilizado en Internet en 2022 siendo utilizado por el 60,4% de todos los sitios web cuyo idioma de contenido se conocen, mientras que el español tan solo representa un 4,1% de los sitios web en Internet (W3TECHS, 2022). En el mundo de la programación informática y en la industria de software, el inglés parece ser la *lingua franca*.[48] La mayoría de los códigos nuevos generalmente son desarrollados por personas que hablan inglés. El idioma más usado en las principales certificaciones académicas y profesionales de Tecnología de la Información y Seguridad de la Información es el inglés.

Retos

Según (EF, 2022), Centroamérica y Sudamérica han mejorado considerablemente su nivel de inglés en la última década no obstante en 2022 el dominio del inglés continúa siendo muy bajo para México y Haití y bajo para Colombia, Ecuador, Panamá, Venezuela y Nicaragua. Además, la región cuenta con la diferencia de calificación por edades más amplia del mundo. Las calificaciones de los jóvenes en la región han caído significativamente desde 2020. Los cierres de los centros educativos durante la pandemia parecen ser la causa más probable. Finalmente, en 2022 el nivel de inglés de los hombres ha aumentado y el de las mujeres ha disminuido ligeramente. Los hombres han obtenido mejores calificaciones que las mujeres en la región.

Algunas cifras

Cuadro 2.
Relevancia del idioma inglés a nivel global

Lenguajes hablados	Sitios WEB por idioma *	Población por idioma **	Usuarios de Internet por idioma ***
Inglés	60.4%	18.2%	25.9%
Ruso	5.4%	3.2%	2.5%
Español	4.1%	6.9%	7.9%
Aleman	3.4%	1.7%	2.0%
Frances	3.1%	3.4%	3.3%
Japonés	2.8%	1.6%	2.6%
Chino	1.8%	14.0%	19.4%
Otros	19.0%	51.1%	36.4%
Total	**100.0%**	**100.0%**	**100.0%**

Fuente: Elaboración propia a partir de * (W3TECHS, 2022), ** (ETHNOLOGUE, 2022), * (INTERNETWORLDSTATS, 2022)**

Gráfica 26.
Ranking de dominio de inglés en la región

Fuente: (EF, 2022)

Buenas prácticas

Una persona bilingüe, que habla español e inglés, puede entender a 1 de cada 3 personas que se conectan a Internet actualmente (un 25,9% de usuarios de internet hablan inglés y un 7,9% hablan español). Como caso de buenas prácticas, Argentina ha implementado diferentes iniciativas y leyes para mejorar la enseñanza de idiomas en las escuelas (Ley de Educación Nacional, Núcleos de Aprendizajes Prioritarios -NAP- y programas como la Jornada Ampliada en Buenos Aires)[49]. Para lograr estos objetivos, se ha desarrollado un sistema de formación de los docentes de idiomas en metodologías comunicativas. En Costa Rica, se destaca lo dispuesto tanto en la Directriz de Bilingüismo[50] como en la Política Educativa de Promoción de Idiomas[51] que destacan la importancia del aprendizaje de una segunda lengua como herramienta indispensable para la formación, el desempeño, el desarrollo personal y profesional de la ciudadanía; planteando mejorar la enseñanza del inglés aplicándola desde el nivel de educación preescolar.

48 https://preply.com/en/blog/b2b-english-for-software-engineers-developers-and-programmers/#:~:text=So%2C%20how%20important%20is%20English,will%20still%20be%20in%20English.
49 https://www.ambito.com/informacion-general/ranking/la-argentina-es-el-pais-mejor-dominio-del-ingles-america-latina-n5149683
50 Directriz N° DM-0004-2-2019 y Circular DVM-AC-004-2020 del Ministerio de Educación Pública de Costa Rica en donde se establecen disposiciones para implementar la enseñanza del inglés en el nivel de Educación Preescolar.
51 http://cse.go.cr/sites/default/files/acuerdos/politica_educativa_para_la_promocion_de_idiomas.pdf

Concientizar y sensibilizar en ciberseguridad durante la edad temprana

Relevancia

La población menor a 15 años en América Latina y el Caribe representa el 24% de la población total mientras que en Norte América es el 18% y en Europa es el 16%. Para el desarrollo de la fuerza laboral en la región es fundamental concientizar y sensibilizar en ciberseguridad durante la edad temprana. Los ataques cibernéticos continúan dirigidos a todo tipo de organizaciones, incluidas las escuelas, ya que los estudiantes y el personal traen dispositivos conectados desde casa y comparten información a través de sus redes. Concientizar y sensibilizar a los estudiantes a temprana edad sobre los riesgos que enfrentan en línea es importante, pero también lo es ofrecerles la oportunidad de aprender sobre ciberseguridad a un nivel más profundo, permitiéndoles tener habilidades cibernéticas de por vida. Es imperante cerrar la creciente brecha en la conciencia y las habilidades de ciberseguridad entre los jóvenes estudiantes al garantizar que se convierta en un área temática crítica para la educación.

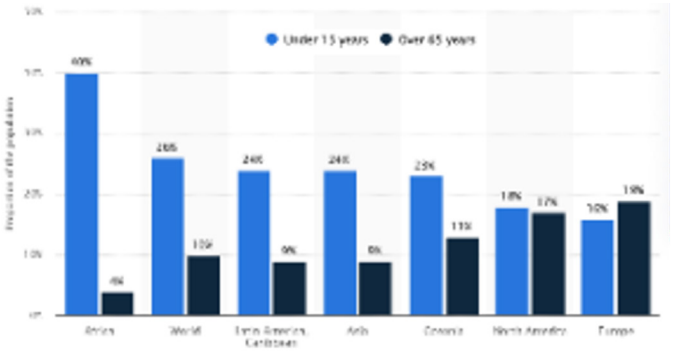
Retos

Generalmente, en las escuelas y otros tipos de instituciones educativas y vocacionales preuniversitarias, el contenido relacionado con riesgos de ciberseguridad está agregado como parte de un área temática tecnológica, como informática/ciencias de la computación/TIC/tecnología (digital), y contenido agregado a una variedad de materias no tecnológicas. Según (GFCE, 2022), en la educación a edad temprana tiende a haber una falta de habilidades prácticas de ciberseguridad, una falta de mentalidad de ciberseguridad, una falta de suficiente cobertura de conjunto de habilidades incorporadas, hacia una carrera profesional relacionada con la ciberseguridad y se percibe una falta general de interés y conciencia entre los niños en el desarrollo de habilidades cibernéticas y ciberseguridad como una carrera potencial.

Algunas cifras

Gráfica 27.
Población mundial menor a 15 años y mayor a 65 años

Fuente: STATISTA (2022)[52]



Buenas prácticas

Dentro de los contextos internacionales y multinacionales, existe una oferta amplia de contenido educativo en ciberseguridad (a través de programas, directrices e iniciativas) dentro de un contexto preuniversitario. Por ejemplo, se destaca el programa *Child Online Protection (COP)*[53] de la Unión Internacional de Telecomunicaciones -UIT- dirigido a niños, padres y educadores, la industria y los formuladores de política. También el contenido que provee la Agencia de la Unión Europea para la Ciberseguridad (en inglés, European Union Agency for Cybersecurity -ENISA-) enfocado, por una parte, a la concientización y sensibilización en torno a la ciberseguridad[54]. La Organización Europea de Seguridad Cibernética (ECSO) desarrolla la iniciativa *Youth4Cyber*[55] que tiene como objetivo educar y sensibilizar a los jóvenes (de 6 a 26 años) sobre la ciberseguridad. También se destaca el contenido del Foro Global sobre Experiencia Cibernética (en inglés, Global Forum on Cyber Expertise -GFCE-)[56], donde se comparten las mejores prácticas y desarrolla iniciativas para mejorar la capacidad cibernética. A nivel nacional, se destaca el programa *SG Cyber Youth* en Singapur dirigido por la Agencia de Ciberseguridad de Singapur (en inglés, Cyber Security Agengy of Singapore -CSA-) para guiar a niños y jóvenes (especialmente aquellos en escuelas secundarias) hacia una carrera profesional en ciberseguridad, con el apoyo de la academia, la comunidad y la industria. También, el Programa de Asistencia para la Educación y Capacitación en Ciberseguridad[57] de Estados Unidos (en inglés, Cybersecurity Education and Training Assistance Program -CETAP-) para apoyar la educación en ciberseguridad en las aulas K-12[58] a través del desarrollo de planes de estudio de ciberseguridad y capacitación de instructores.

52 https://www.statista.com/statistics/265759/world-population-by-age-and-region/#:~:text=Globally%2C%20about%2026%20percent%20of%20the%20world%20is,19%20percent%20being%20over%2065%20years%20of%20age.
53 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx y https://www.itu-cop-guidelines.com/
54 https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport
55 https://www.ecs-org.eu/initiatives/youth4cyber
56 https://thegfce.org/working-groups/working-group-d/
57 https://niccs.cisa.gov/education-training/cybersecurity-teachers
58 K–12 ("k al doce" o "k hasta doce") es la designación utilizada en algunos sistemas educativos para la escolarización primaria y secundaria.

Promover el acceso a la oferta educativa

Relevancia

La educación superior ofrece una gama considerable de contenidos, cursos, módulos y oportunidades para explorar la ciberseguridad tanto a nivel de pregrado como de posgrado. Las universidades e institutos de educación superior amplían rápidamente su oferta de programas de ciberseguridad otorgando títulos específicos o títulos como especialización o maestrías en TI, TIC y seguridad de la información. Dado que la demanda de profesionales de la ciberseguridad ha crecido en los últimos años, la educación superior también ha respondido mediante la provisión de: i) cursos de ciberseguridad dedicados, ii) cursos generales de informática o computación con uno o más módulos en ciberseguridad y iii) cursos no técnicos con módulos en ciberseguridad. Además, los cursos multidisciplinarios son cada vez más comunes.

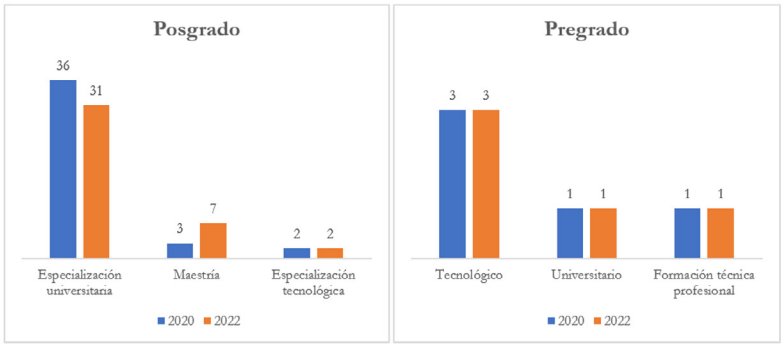
Retos

Aunque existen esfuerzos aislados en varios países[59], en la región no existe la suficiente oferta educativa para generar competencias y capacidades adecuadas en ciberseguridad[60]. La demanda de educación en ciberseguridad por parte de los estudiantes postsecundarios no aumenta lo suficientemente rápido. Además, la demanda de habilidades en ciberseguridad en los sectores de la industria también dificulta que la academia atraiga académicos, investigadores y profesores, con conocimiento, experiencia práctica, antecedentes de investigación y aspiraciones académicas. Existen también dificultades para atraer y retener a profesores calificados en ciberseguridad, en gran parte porque este tipo de profesionales de alta calidad exigen salarios superiores al promedio. Los proveedores de educación terciaria deben garantizar que la ciberseguridad se considere una opción de estudio deseable para atraer a los mejores y más motivados estudiantes.

Algunas cifras

Gráfica 28.
Evolución del número de programas de educación superior relacionadas con Ciberseguridad y Seguridad de la Información en Colombia

Fuente: Datos de 2020 (DNP, 2020) y Datos de 2022[61] (MINEDUCACION, 2022)



Buenas prácticas

Con el fin de promover la oferta educativa, se destacan iniciativas regionales para el desarrollo de habilidades de ciberseguridad como CYBERHEAD[62] de ENISA, convirtiéndose en la mayor base de datos validada de educación superior en ciberseguridad (123 programas en 25 países) y principal punto de referencia para todos los ciudadanos de dicha región que buscan mejorar sus conocimientos y habilidades en ciberseguridad. En el Reino Unido, el Centro Nacional de Seguridad Cibernética (en inglés, National Cyber Security Centre -NCSC-) ha certificado varios títulos a nivel de licenciatura y maestría bajo el programa de títulos certificados. También ha apoyado el desarrollo de Centros Académicos de Excelencia en Investigación en Ciberseguridad (ACE-CSR) y Centros Académicos de Excelencia en Educación en Ciberseguridad (ACE-CSE). En Singapur, se destaca la existencia de diversos programas dirigidos a jóvenes, en especial el programa *SG Cyber Youth*[63] que los guía para iniciar en ciberseguridad, con el apoyo de la academia, la comunidad y la industria. Una iniciativa clave es el *Youth Cyber Exploration Programme*[64] que presenta a los estudiantes de nivel secundario los fundamentos de la ciberseguridad y cultiva su interés en una carrera de ciberseguridad. El *Cybersecurity Career Mentoring Programme (CCMP)* también brinda orientación profesional y apoyo de mentores de la industria. Otras iniciativas en Singapur incluyen el *Student Volunteer & Recognition Programme (SVRP)* y el *Cybersecurity Learning Journeys*. También el programa *SG Cyber Olympians* con el fin de ser preparados bajo el a través de sesiones de lucha cibernética, entrenamiento más profundo y competencias internacionales.

59 Se destaca, por ejemplo, el Directorio de la Oferta Académica 2022 del *Cyber-Security Hub* de la ciudad de Córdoba en Argentina (https://corlab.cordoba.gob.ar/wp-content/uploads/2022/09/oferta-educativa-ciberseguridad-cordoba.pdf)
60 Por ejemplo, según (DNP, 2020) se *"evidencia que la oferta de programas educativos relacionados con seguridad digital es baja en el nivel de académico pregrado"* en Colombia.
61 Se destaca la actual oferta de programas de maestría en Colombia, tales como: Maestría en gestión y seguridad de la información, Maestría en seguridad digital, Maestría en seguridad de la información, Maestría en seguridad informática y de las comunicaciones, Maestría en ciberseguridad e informática forense o Maestría en ciberseguridad y ciberdefensa.
62 https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/
63 https://www.cyberyouth.sg/
64 https://www.csa.gov.sg/ycep

Conectar la educación con la formación y la industria

Relevancia

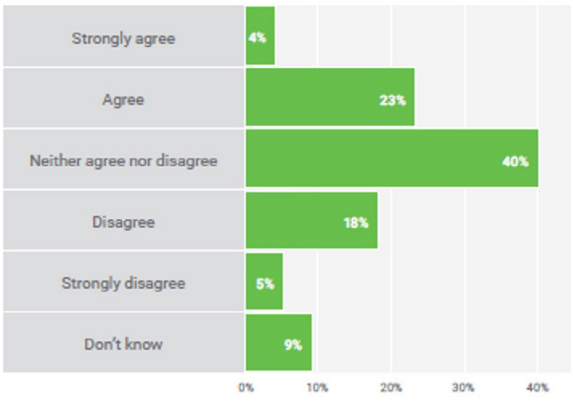
El desarrollo de planes de estudio y programas de educación superior y continua es de gran importancia cuando se trata de mitigar la escasez laboral y la brecha de habilidades en ciberseguridad, ya que alientan a los estudiantes a seguir temas de ciberseguridad, mejoran las capacidades operativas de la potencial nueva fuerza laboral y promover y fomentar las relaciones entre la academia y la industria, así como alinear la formación en ciberseguridad con las necesidades reales de la industria. Los planes de estudio deben ser multidisciplinarios, ya que los estudiantes y profesionales necesitan comprender una variedad de áreas de conocimiento de ciberseguridad, que van desde temas más técnicos hasta aspectos sociales y legales. Adicionalmente, los planes y programas deben priorizar la formación práctica frente a la basada en la teoría.

Retos

En los países de la región no se aprecia la existencia de marcos específicos para definir planes de estudios estandarizados y ampliamente concertados y alineados con la industria. No se aprecia la existencia de alianzas entre la industria y la academia con el fin de generar guías o lineamientos curriculares de alcance nacional en torno a los programas de pregrado o posgrado relacionados con la ciberseguridad o la seguridad de la información. Es necesario que de estas alianzas surja periódicamente un conjunto de áreas temáticas básicas con sus prácticas asociadas en ciberseguridad en las que se espera que todos los estudiantes sean competentes al final de la educación secundaria y terciaria. Esta situación puede generar un impacto en la entrada de los estudiantes a la fuerza laboral.

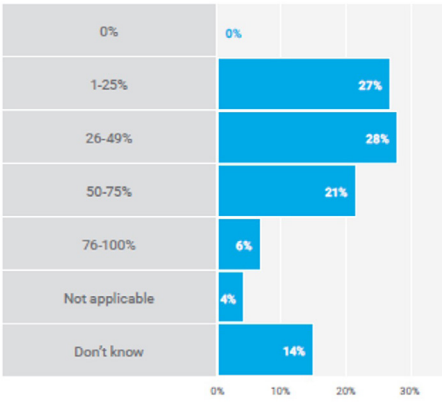
Algunas cifras

Gráfica 29.
¿Están los recién graduados universitarios en ciberseguridad bien preparados para los desafíos de ciberseguridad en su organización?



Fuente: (ISACA, 2022)

Gráfica 30.
% de solicitantes de ciberseguridad que están bien calificados para la posición a la que aplican



Fuente: (ISACA, 2022)

Buenas prácticas

Existen algunas iniciativas con el fin de aportar a crear marcos específicos o un conjunto estandarizado de pautas a seguir por los países frente a la educación preuniversitaria y la universitaria. Respecto a la educación preuniversitaria se destaca la iniciativa *Informática para todos*[65] y su *"Marco del plan de estudios de informática para la escuela"*[66] lanzado en 2022 convirtiéndose en un buen ejemplo de cómo las diferentes partes interesadas en varios países pueden trabajar juntas para producir planes de estudio y pautas más estandarizados y ampliamente adoptados. Respecto a la educación universitaria se destaca la experiencia en Estados Unidos en donde existen varios esfuerzos de colaboración público-privado destacando a la Fuerza de Tarea Conjunta (en inglés, Joint Task Force -JTF-) sobre Educación en Seguridad Cibernética que desde el año 2015 trabaja en desarrollar una guía curricular que alinee los programas académicos de ciberseguridad a nivel de pregrado con las necesidades de la industria. En específico, se destaca también el proyecto *Cyber2yr2020*[67] que se enfoca en las pautas del plan de estudios para los programas de ciberseguridad, incluidos programas de grado asociado orientados a la carrera y que deben alinearse con el marco de la fuerza laboral de ciberseguridad de la Iniciativa Nacional para la Educación en Ciberseguridad (en inglés, National Initiative for Cybersecurity Education -NICE-) del NIST.

65 https://www.informaticsforall.org/
66 https://www.informaticsforall.org/wp-content/uploads/2022/03/Informatics-Reference-Framework-for-School-release-February-2022.pdf
67 http://ccecc.acm.org/files/publications/Cyber2yr2020.pdf

Promover el acceso a las rutas de aprendizaje

Relevancia

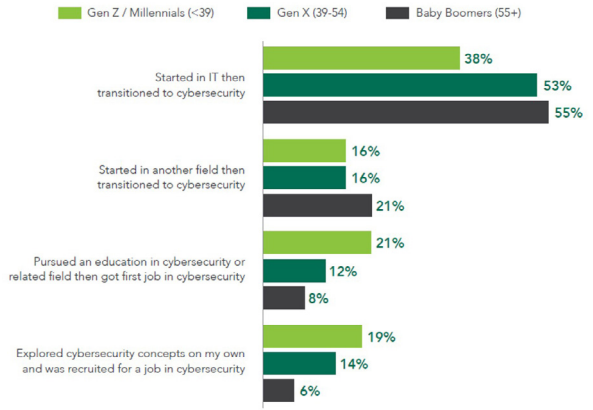
Tener una base sólida de conocimientos y habilidades es de suma importancia en el mercado laboral de ciberseguridad. Esto incluye habilidades blandas, como la comunicación verbal y escrita, y habilidades técnicas validadas a través de certificaciones académicas o profesionales. Los estudiantes y profesionales de otros sectores que se convertirán en solicitantes de empleo pueden desarrollar estas habilidades y competencias mediante rutas de aprendizaje enfocados especialmente para niveles principiantes o practicantes dentro de las organizaciones. Tanto los *Proveedores de Educación, Entrenamiento y Certificaciones* como los *Proveedores de Tecnología* son actores claves para cerrar brechas entre la demanda y la oferta en habilidades de ciberseguridad. Estas rutas, que comprenden cursos prácticos que enseñan habilidades comerciales y tecnológicas, permiten demostrar las habilidades a los posibles empleadores. Se destacan programas académicos de certificación en ciberseguridad para estudiantes que ya hayan obtenido un título en un campo relacionado y buscan cambiar de carrera, o para los estudiantes que desean explorar cómo sería prepararse para una carrera en ciberseguridad antes de comprometerse con una carrera más larga.

Retos

Iniciar y adelantar una carrera en ciberseguridad no es tan sencillo como otras profesiones más tradicionales. En los países de la región es importante generar más interés en los estudiantes y solicitantes de empleo con el fin de incursionar en las rutas de aprendizaje a su propio ritmo. Puede existir incapacidad de los actores involucrados para alentar a más estudiantes a ingresar a caminos académicos que se asocian más fácilmente con un trabajo de ciberseguridad. Otro problema es que las habilidades requeridas están cambiando a un ritmo más rápido de lo habitual dentro de los campos de tecnología avanzada, debido a los cambios introducidos por la nueva tecnología digital y la rápida digitalización de la sociedad.

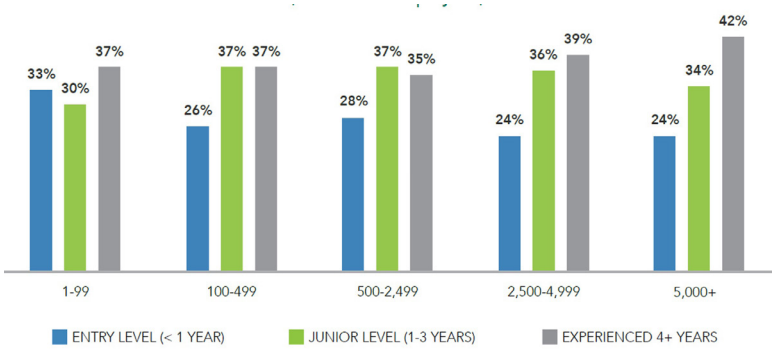
Algunas cifras

Gráfica 31.
Rutas hacia carreras en ciberseguridad



Fuente: (ISC2, 2021)

Gráfica 32.
Composición del equipo de ciberseguridad por nivel de experiencia por tamaño de la organización



Fuente: (ISC2, 2022b)

Buenas prácticas

En el mercado laboral existen actores claves que impulsan desde el lado de la oferta laboral rutas de aprendizaje. Los *Proveedores de Educación, Entrenamiento y Certificaciones* y los *Proveedores de Tecnología* ofrecen contenidos de todo nivel de complejidad para desarrollar capacidades y habilidades. Existe una gran cantidad de cursos en el mercado bajo plataformas MOOC[68] dirigidos estudiantes y profesionales. Ejemplo de este tipo de plataformas son: Coursera (https://www.coursera.org/), LinkedIn Learning (https://www.lynda.com/), edX (http://www.edx.org/), PluralSight (https://www.pluralsight.com/), Cybrary (https://www.cybrary.it/), Udacity (https://www.udacity.com/), Udemy (https://www.udemy.com/), MiriadaX (https://miriadax.net/) o Cyberwiser (https://www.cyberwiser.eu/). También se destacan plataformas que ofrecen *Proveedores de Tecnología* para iniciar rutas de aprendizaje tales como la *Cisco Networking Academy* desarrollando *Skills for All*[69], una plataforma gratuita y móvil que ofrece experiencias de aprendizaje al ritmo de cada individuo, para impulsar un futuro inclusivo para todos, incluyendo el *Cybersecurity Learning Pathway*[70].

68 El término MOOC es el acrónimo del término en inglés *Massive Open Online Courses*, es decir, se refiere a cursos online abiertos, tanto gratuitos como de pago, que son accesibles a un número masivo de alumnos.
69 https://skillsforall.com/
70 Al estar alineado con la nueva certificación de *Certiport Information Technology (IT) Specialist Cybersecurity*, los alumnos pueden desempeñar roles como técnico de ciberseguridad, analista junior de ciberseguridad y soporte de help desk. Así mismo, los egresados pueden aprovechar el programa de *Talent Bridge* de CISCO y utilizar el motor de búsqueda de empleo que incluye oportunidades en más de 725 socios empleadores en 70 países.

Aclarar la definición de la profesión en ciberseguridad

Relevancia

El rol de los profesionales en ciberseguridad está en constante evolución y, por lo tanto, es difícil de definir la profesión en ciberseguridad. Adicionalmente, la taxonomía en torno a la ciberseguridad puede ser confusa y las rutas hacia y a través de las carreras de ciberseguridad pueden ser difíciles de recorrer. Es importante que los países aborden este tema para garantizar que haya una profesión de ciberseguridad estructurada y sostenible. El lenguaje técnico y los acrónimos que se usan a menudo pueden hacer que este desafío sea particularmente pronunciado para aquellos estudiantes o solicitantes de empleo que son nuevos o no están familiarizados con la ciberseguridad. El panorama profesional actual también es complejo para las organizaciones profesionales existentes y los *Proveedores de Educación, Entrenamiento y Certificaciones*, que a menudo no pueden articular la equivalencia de sus ofertas en ausencia de un marco técnico común. La ciberseguridad se reconoce cada vez más como un tema altamente interdisciplinario, que abarca áreas de conocimiento como la gestión y la gobernanza de riesgos, las leyes y regulaciones cibernéticas, los factores humanos, la protección de la privacidad y derechos en línea y comportamientos adversarios (GFCE, 2022).

Retos

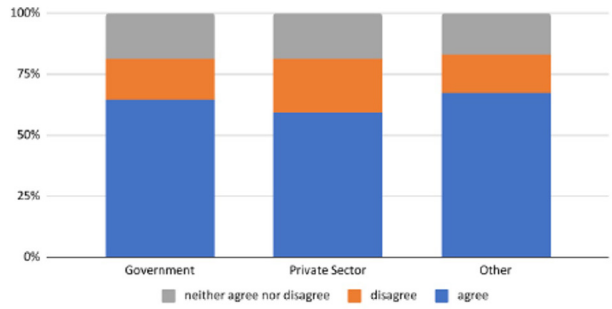
En la región, la seguridad informática y la seguridad de la información son términos que aún se confunden con el término ciberseguridad. Esto también genera confusión ente los estudiantes y solicitantes de empleo en relación con el alcance en las tareas y habilidades que deben poseer para cumplir requisitos o perfiles al buscar empleo. Según (GFCE, 2022), más de la mitad de las partes interesadas encuestadas en un estudio sobre el desarrollo de la ciberseguridad como profesión a nivel global mencionan que no está clara la definición de la profesión y esta respuesta fue prácticamente la misma en todos los grupos de partes interesadas y fue ligeramente superior entre los encuestados de países desarrollados.

Algunas cifras

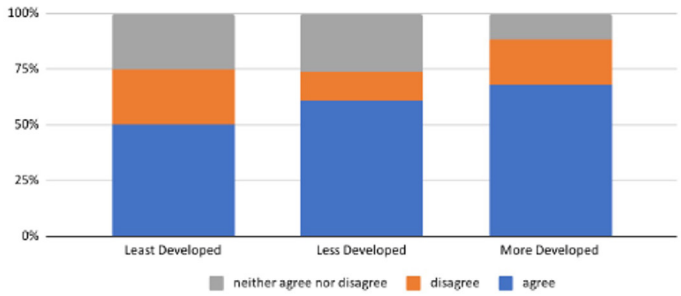
Gráfica 33.

Percepción frente a la definición de la profesión en ciberseguridad

(¿Hasta qué punto está de acuerdo con que la definición de profesional de ciberseguridad no es clara?)



Fuente: (GFCE, 2022)



Fuente: (GFCE, 2022)

Buenas prácticas

En el Reino Unido, el *UK Cyber Security Council y el Cyber Security Body Of Knowledge (CyBOK)*[71] han establecido una categorización[72] de los roles en ciberseguridad. El CyBOK es un recurso único, que proporciona un cuerpo de conocimientos de base que abarca la amplitud y profundidad de la ciberseguridad abarcando una amplia gama de disciplinas. Por ejemplo, según (DCMS & IPSOS, 2022), los roles más demandados en ciberseguridad en Reino Unido son ingenieros de seguridad (35%), analistas de seguridad (18%), gerentes de seguridad (14%), arquitectos de seguridad (11%) y consultores de seguridad (9%). Existen iniciativas para temas específicos, por ejemplo, Singapur ha emitido un *Marco de Competencias de Ciberseguridad de Tecnología Operacional* (CSA, 2021) que proporciona la base para atraer y desarrollar talento para el emergente sector de ciberseguridad OT en Singapur y brinda orientación sobre las competencias para equipar a los profesionales en el desempeño de sus trabajos en los sectores de la industria de OT. También existen iniciativas como el (ISC)^2 CBK[73] (en inglés, Body of Knowledge) que es un compendio desarrollado por pares de lo que un profesional competente en ciberseguridad debe saber, incluidas las habilidades, técnicas y prácticas que se emplean de forma rutinaria y establece un marco común de términos y principios de seguridad de la información que permite a los profesionales de ciberseguridad y de TI/TIC de todo el mundo discutir, debatir y resolver asuntos relacionados con la profesión con un entendimiento, una taxonomía y un léxico comunes.

71 https://www.cybok.org/

72 Por ejemplo, según (DCMS & IPSOS, 2022) la fuerza laboral del sector cibernético en el Reino Unido trabaja en roles o especialidades particulares: Un rol de ciberseguridad generalista (26 %), Gobierno de seguridad, riesgo, cumplimiento y legal (14 %), Seguridad de red (redes y firewalls) (11 %), Arquitectura de seguridad (11 %), Gestión de incidentes, respuesta y recuperación (10 %), operaciones de seguridad (por ejemplo, detección de intrusos) (9 %), seguridad del sistema (sistemas operativos y parches) (9 %) y pruebas de penetración (8 %).

73 https://www.isc2.org/Certifications/CBK

4.2. DESDE LA DEMANDA LABORAL

Las organizaciones se han vuelto cada vez más dependientes de la tecnología y proteger los sistemas, las redes y los datos contra los ciberataques es más difícil que nunca, ya que se necesitan aún más tecnologías y procesos de seguridad para trabajar en conjunto. Por lo tanto, las organizaciones necesitan que su fuerza laboral de ciberseguridad sea más grande y tenga una gama de habilidades más amplia que nunca.

Del análisis de los desafíos identificados por el lado de la demanda laboral de ciberseguridad, a continuación, se presentan consideraciones con el fin de:

- Garantizar que la demanda y la oferta hablen un lenguaje común
- Ajustar los requisitos de contratación para atraer el mejor talento
- Promover la diversidad, equidad e inclusión en la fuerza laboral
- Impulsar los marcos de trayectorias profesionales
- Retener a la fuerza laboral

Garantizar que la demanda y la oferta hablen un lenguaje común

Relevancia

A medida que el mercado laboral de ciberseguridad madura se ha generado una necesidad local y regional de un léxico común para describir y organizar la fuerza laboral de ciberseguridad. Es importante que los países cuenten con marcos de trabajo que generen una comprensión común de los roles, competencias, habilidades y conocimientos utilizados por y para las personas, los empleadores y los *Proveedores de Educación, Entrenamiento y Certificaciones*, con el fin de abordar la escasez de habilidades en ciberseguridad. Además, ayuda a facilitar aún más el reconocimiento de habilidades relacionadas con la ciberseguridad, impulsar el empleo y la empleabilidad en puestos relacionados con la ciberseguridad. Estos marcos de trabajo, que en varios países se convierten en estándares, proporcionan orientación sobre qué roles implementar en la organización para lograr tareas de ciberseguridad necesarias y también formas de identificar los talentos adecuados mediante la formulación de descripciones de puestos adecuadas que identifiquen correctamente las calificaciones y deberes correctos que se pueden asignar a cada rol.

Retos

En la región no se aprecian esfuerzos de estandarización en torno a la ciberseguridad, en términos de cómo se definen y describen los roles de ciberseguridad y las habilidades asociadas a dichos roles y cómo se capacita a la fuerza laboral. La falta de estándares unificados para el conocimiento, la competencia y las habilidades que los estudiantes deben desarrollar para satisfacer las necesidades y que las organizaciones deben tener en cuenta al momento de crear sus perfiles para búsqueda de talento puede generar ineficiencias en el mercado laboral de ciberseguridad impactando la transacción entre vendedores y consumidores de este mercado.

Algunas cifras

Gráfica 34.
Beneficios del Marco Europeo de Habilidades en Ciberseguridad

Fuente: (ENISA, 2022)

Buenas prácticas

Una buena práctica en las Américas es el marco de la fuerza laboral de ciberseguridad de la Iniciativa Nacional para la Educación en Ciberseguridad (en inglés, National Initiative for Cybersecurity Education -NICE-) del NIST que proporciona a los empleadores, empleados, educadores, estudiantes y proveedores de capacitación en los Estados Unidos un lenguaje común para definir el trabajo de ciberseguridad. Al definir la fuerza laboral de ciberseguridad y usar terminología estándar, la academia y los empleadores pueden sincronizar la educación, el reclutamiento y el desarrollo para establecer una fuente de talento sólida y mantener una fuerza laboral altamente calificada. Por ejemplo, la *Iniciativa Nacional de Carreras y Estudios en Ciberseguridad* ha desarrollado la herramienta *Cyber Career Pathways Tool*[74], basada en el marco NICE, que describe la fuerza de trabajo describiendo en detalle los atributos principales entre cada uno de 52 roles de trabajo[75] definidos en ciberseguridad. Otra buena práctica es el desarrollo de un *Marco Europeo de Habilidades en Ciberseguridad*[76] por parte de ENISA. Australia ha desarrollado un *Marco de Habilidades Cibernéticas*[77] que permite la contratación específica de especialistas cibernéticos, proporciona una vía de desarrollo para el personal cibernético actual y futuro y alinea las habilidades, el conocimiento y los atributos con los estándares nacionales e internacionales de la industria.

74 Adicionalmente NIST ha expedido documentación (Draft NISTIR 8193) sobre indicadores de capacidad destinados a ayudar a las organizaciones a determinar si un trabajador de ciberseguridad puede desempeñar un rol de trabajo en ciberseguridad. Los indicadores de capacidad son educación recomendada, certificación, capacitación, aprendizaje experiencial y aprendizaje continuo que podría indicar una mayor capacidad para desempeñar un rol de trabajo determinado.
75 https://niccs.cisa.gov/about-niccs/workforce-framework-cybersecurity-nice-framework-work-roles
76 https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework
77 https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework

Ajustar los requisitos de contratación para atraer el mejor talento

Relevancia

Los procesos de contratación son métodos paso a paso para encontrar, reclutar y contratar nuevos empleados. Un buen proceso de contratación ayuda a atraer y retener empleados de alta calidad en la fuerza laboral de ciberseguridad. Los elementos específicos de un proceso de contratación son únicos para cada organización. Los gerentes de contratación se basan en una amplia gama de tácticas y recursos para contratar todo el personal de nivel inicial y junior. Si bien las empresas de reclutamiento y los organismos de certificación ocupan un lugar destacado en todos los países, los aprendizajes y las pasantías son más populares en el Reino Unido y la India (ISC2, 2022b).

Retos

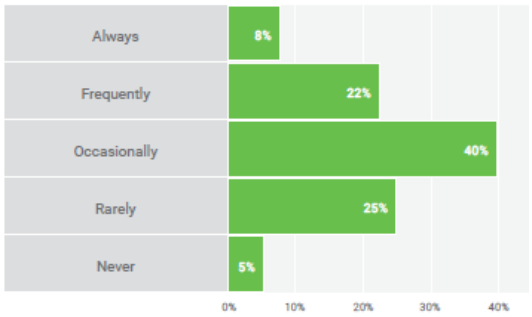
La contratación de talento para roles en ciberseguridad sigue siendo un desafío para muchas organizaciones. Se continúa apreciando problemas de comunicación entre los gerentes de organizaciones y sus áreas de recursos humanos (ISACA, 2022). Además, las especificaciones del trabajo son diferentes si las organizaciones operan fuera de la industria de la ciberseguridad. También existen altas expectativas que los empleadores tienen sobre el nivel de habilidad de los candidatos. En muchas ocasiones, las organizaciones buscan profesionales de ciberseguridad para trabajos de nivel de entrada, sin embargo, sin saberlo, están pidiendo varios años de experiencia[78]. Además, las suposiciones por parte de algunos empleadores de que los candidatos deben tener un cierto título académico o certificación para calificar para un trabajo o rol de ciberseguridad o que las promociones deben basarse en el tiempo en el servicio en lugar de las competencias son obstáculos para atraer el mejor talento. Otros problemas son que algunas veces se pide talento que no se necesita y que los empleadores a menudo descartan a personas que carecen de credenciales formales a pesar de la evidencia de adquirir conocimientos y habilidades en ciberseguridad. Según (DCMS & IPSOS, 2022), los agentes de reclutamiento en Reino Unido dicen que comúnmente veían especificaciones de trabajo mal escritas, que intentaban reclutar múltiples roles en uno, no reflejaban los requisitos reales para el rol que se ofrecía o minimizaban beneficios importantes como la capacitación.

Algunas cifras

Gráfica 35.

Comprensión de las necesidades de contratación por recursos humanos

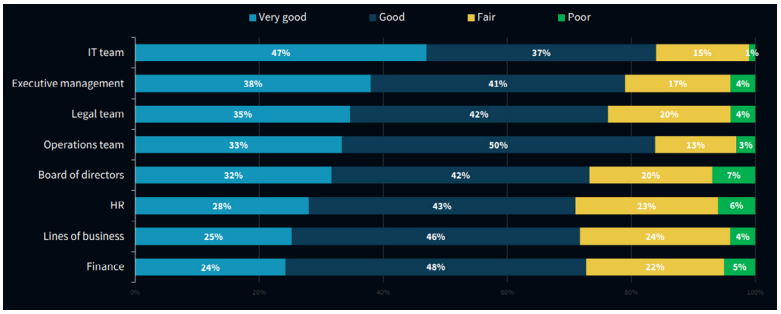
¿Con qué frecuencia siente que su departamento de recursos humanos comprende completamente sus necesidades de contratación de ciberseguridad para preseleccionar adecuadamente a los candidatos?



Fuente: (ISACA, 2022)

Gráfica 36.

Estado de la relación entre la ciberseguridad y otras organizaciones funcionales



Fuente: (ESG, 2021)

Buenas prácticas

Las descripciones de puestos deben ser una responsabilidad compartida. Es importante mejorar continuamente la relación entre las áreas de ciberseguridad con el área de Recursos Humanos para crear descripciones de trabajo realistas para roles de nivel inicial y junior que establezcan expectativas claras para nuevos empleados y empleadores (ISC2, 2022b). Es importante crear publicaciones de trabajo que sean atractivas para aquellos que están saliendo de programas de capacitación y educación en ciberseguridad o que se han desarrollado por sí mismos. Las organizaciones deben redefinir los requisitos mínimos para obtener un puesto de trabajo básico en ciberseguridad y aceptar canales de formación no tradicionales. CISCO ha desarrollado un motor de emparejamiento *Talent Bridge*[79] que automatiza la conexión entre los estudiantes de *Cisco Networking Academy* y una red de partners en todo el mundo, sin costo alguno para empleadores o estudiantes. Dicho motor hace coincidir las calificaciones de los estudiantes con las necesidades de los empleadores, facilitando a los gerentes de contratación identificar rápidamente a los principales candidatos.

78 Por ejemplo, una de las certificaciones más solicitadas es la CISSP que exige que los candidatos aprueben el examen y tengan al menos cinco años de experiencia laboral remunerada acumulada en dos o más de los ocho dominios del ISC2. Al solicitar esta certificación, los empleadores en realidad requieren cinco años de experiencia para un puesto de nivel de entrada.

79 https://www.netacad.com/es/careers/matching-engine

Promover la diversidad, equidad e inclusión en la fuerza laboral

Relevancia

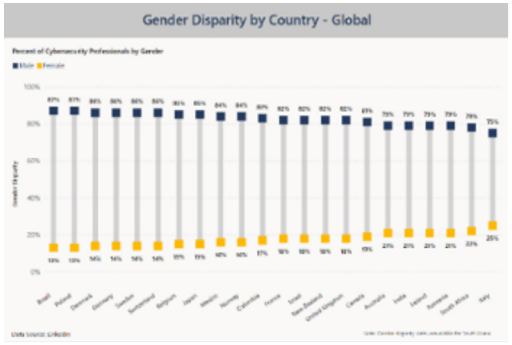
Según (FORTINET, 2022), el desafío actual en el mercado laboral no es solo contratar a más personas, sino también construir equipos más capaces y diversos. Si bien las empresas necesitan talento calificado para una variedad de roles diferentes, el 89% de las empresas globales también tienen objetivos de diversidad explícitos como parte de su plan de contratación. Un equipo de ciberseguridad más diverso es un mejor equipo de ciberseguridad, ya que en este campo multidisciplinario las diferentes perspectivas son críticas. Cuando las amenazas cambian todos los días, los diversos puntos de vista de la fuerza laboral ayudan a contrarrestar al aportar nuevas ideas a las situaciones. En este sentido, hay países como el Reino Unido donde la fuerza laboral del sector cibernético se ha vuelto más diversa en los últimos 3 años, en términos de la cantidad de mujeres y minorías étnicas que trabajan en roles cibernéticos[80].

Retos

Según el último informe del centro de políticas tecnológicas digitales de ASPEN, los grupos subrepresentados como los profesionales afroamericanos (9%), hispanos (4%) y asiáticos (8%) constituyen un porcentaje cada vez más bajo de la industria. En este mismo sentido, las mujeres constituyen el 51% de la población, pero solo representan el 24% de la fuerza laboral de ciberseguridad (ASPENDIGITAL, 2021). Según (FORTINET, 2022), a nivel mundial, el 70% de los gerentes de TI ven la contratación de mujeres y nuevos graduados como uno de los tres principales desafíos. A pesar de que las organizaciones en América Latina (93%) y América del Norte (90%) tienen objetivos de diversidad establecidos, probablemente como resultado de mayores dificultades para reclutar de estas poblaciones.

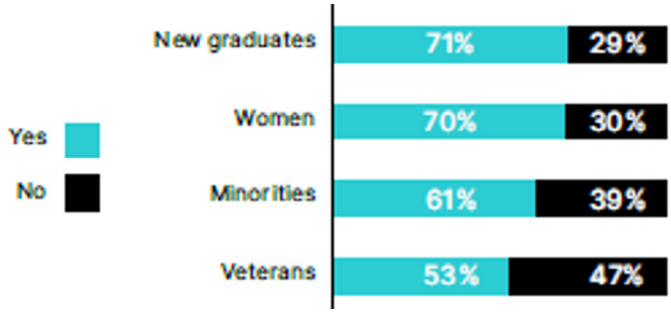
Algunas cifras

Gráfica 37.
Disparidad de género en ciberseguridad



Fuente: (MICROSOFT, 2022)

Gráfica 38.
¿Es la contratación de estas poblaciones uno de los tres principales desafíos de su organización?



Fuente: (FORTINET, 2022)

Buenas prácticas

En el Reino Unido se resalta la importancia de contar con defensores para el reclutamiento cibernético diverso, dentro de las organizaciones y en toda la industria, para ayudar a cambiar la cultura entre los empleadores y crear conciencia sobre las necesidades de los diversos candidatos (DCMS & IPSOS, 2022). Otra buena práctica en las organizaciones es agregar lenguaje inclusivo en las descripciones de puestos que indique explícitamente el interés en grupos minoritarios como personas de color y miembros de la comunidad LGBTQIA+[81]. Estas prácticas fomentan entornos acogedores para la fuerza laboral y el desarrollo personal y profesional del talento en ciberseguridad. Singapur tiene iniciativas como SG Cyber Women[82], dirigida a aprovechar el grupo de talentos subrepresentados y a mujeres, desde edades tan tempranas como la educación terciaria, a unirse a la profesión de ciberseguridad abundan en ese terreno. A nivel regional, CISCO ofrece actualmente una capacitación gratuita en tres (3) fases a toda la comunidad de mujeres chilenas bajo el *Programa educacional de ciberseguridad Chilenas Conectadas y Seguras*[83] buscando acelerar la transformación digital y la inclusión de género en Chile. También se destaca WOMCY[84], iniciativa que busca aumentar la diversidad en ciberseguridad en la región América Latina y el Caribe minimizando la brecha de conocimiento y aumentando las oportunidades de las mujeres en la industria de la ciberseguridad.

80 Según (DCMS & IPSOS, 2022), existe evidencia de que la fuerza laboral del sector cibernético en el Reino Unido se ha vuelto más diversa en los últimos 3 años, tanto en términos de género (22 % son mujeres, frente a 15 % en 2020) como de origen étnico (25 % son de minorías étnicas, frente a 16 % en 2020). La fuerza laboral senior (típicamente con 6 o más años de experiencia) tiende a ser un poco menos diversa que aquellos en roles más jóvenes, en términos de género, etnia y estado de discapacidad. Por ejemplo, solo el 13 por ciento de los puestos de alto nivel están ocupados por mujeres. Ha habido un aumento en los esfuerzos para reclutar personas con condiciones neurodiversas (23% de los empleadores del sector cibernético han realizado cambios para este grupo frente al 15% en 2021). Sin embargo, sigue siendo una minoría que hace adaptaciones para animar a cualquiera de estos diversos grupos a aplicar.
81 El término LGBTQIA+ es el acrónimo de términos en inglés Lesbian, Gay, Bisexual, Transgender, Intersex, Queer/Questioning, Asexual.
82 https://www.csa.gov.sg/programmes/sgcybertalent/sgcyberwomen
83 https://www.cisco.com/c/m/es_cl/cda/chilenas-conectadas-y-seguras.html
84 https://womcy.org/

Impulsar los marcos de trayectorias profesionales

Relevancia

Hay muchas oportunidades para que los trabajadores comiencen y avancen en sus carreras dentro de la ciberseguridad dentro de las organizaciones. Debido a que los empleados en roles de ciberseguridad valoran los trabajos que les permiten crecer y desarrollarse, los empleadores que no pueden ofrecer salarios generosos aún pueden competir por el talento al ofrecer marcos de trayectorias profesionales que demuestren crecimiento y potencial de aprendizaje. Estos marcos ayudan a los profesionales de ciberseguridad a prepararse para trabajos clave dentro de la organización, para oportunidades de transición comunes entre ellos y para conocer información detallada sobre los salarios, las credenciales y los conjuntos de habilidades asociados con cada rol de ciberseguridad. Estos marcos generalmente son secuencias bien articuladas de ofertas educativas y de formación y servicios de apoyo que ayudan a los profesionales a progresar en su carrera en una industria u ocupación particular.

Retos

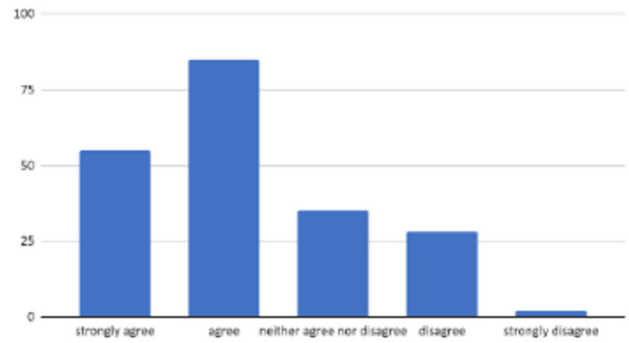
Según (DCMS & IPSOS, 2022), un poco más de 6 de cada 10 empresas cibernéticas (63%) en el Reino Unido informan que emplean personal que tiene o está trabajando para obtener calificaciones relacionadas con la ciberseguridad (es decir, en educación superior, aprendizaje u otra capacitación certificada)[85]. Por otra parte, los precios de suscripción para algunas asociaciones profesionales, así como los precios de algunos programas en los marcos de trayectorias profesionales pueden ser más altos que el salario mensual promedio de algunos profesionales de ciberseguridad en países en desarrollo (GFCE, 2022). Adicionalmente, dos tercios de las partes interesadas encuestadas en un estudio sobre el desarrollo de la ciberseguridad como profesión a nivel global estuvieron de acuerdo en que las trayectorias profesionales de la ciberseguridad no están claras y, de ellos, la mayoría pensó que esta falta de claridad desalentaba a las personas a unirse o permanecer en la profesión de la ciberseguridad. Esta opinión fue más fuerte en las personas que trabajan en el gobierno (6%) y menos fuerte en las personas que trabajan en el sector privado (40%) (GFCE, 2022).

Algunas cifras

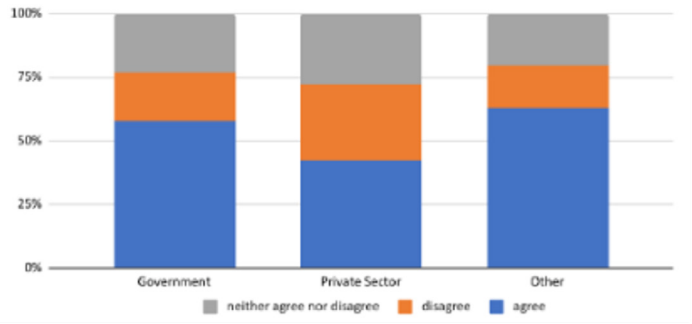
Gráfica 39.

Percepción frente a los marcos de trayectorias profesionales

¿Hasta qué punto está de acuerdo con que los marcos de trayectorias profesionales no son claros?



Fuente: (GFCE, 2022)



Fuente: (GFCE, 2022)

Buenas prácticas

El sitio web interactivo Cyberseek.org[86] contiene varias herramientas diseñadas para ayudar a los profesionales a planear rutas profesionales que muestra trabajos clave de ciberseguridad, oportunidades de transición comunes entre ellos e información detallada sobre los salarios, las credenciales y los conjuntos de habilidades asociados con cada rol. Por ejemplo, la *Iniciativa Nacional de Carreras y Estudios en Ciberseguridad* ha desarrollado la herramienta *Career Pathway Roadmap*[87], una forma interactiva para que los profesionales que trabajan (cibernéticos y no cibernéticos), los empleadores exploren y construyan su propia hoja de ruta profesional en los 52 roles laborales diferentes del Marco NICE. El apoyo a las trayectorias profesionales y la creación de valor económico y laboral a largo plazo necesitan programas de readiestramiento a través del aprendizaje transformacional. Muchos proveedores de certificaciones profesionales brindan trayectorias profesionales a seguir, y cada credencial representa un nivel diferente de experiencia. Se destacan Proveedores de Certificaciones como (ISC)2 (https://www.isc2.org/), CompTIA (https://www.comptia.org/), ISACA (https://www.isaca.org/), GIAC (https://www.giac.org/), EC-Council (https://www.eccouncil.org/) y SANS (https://www.sans.org/).

85 La certificación solicitada con más frecuencia por los empleadores cibernéticos es la de *Profesional Certificado en Seguridad de Sistemas de Información (CISSP)*, que se encuentraron en el 39% de las ofertas de trabajo en línea en 2021 que solicitaron una certificación específica. Las certificaciones *Cisco Certified Network Professional* y *Cisco Certified Network Associate* también tuvieron una gran demanda en el Reino Unido, con el 21% de las ofertas de trabajo solicitando cada una de estas.

86 https://www.cyberseek.org/pathway.html

87 https://niccs.cisa.gov/workforce-development/career-pathway-roadmap

Retener a la fuerza laboral

Relevancia

Las áreas de recursos humanos en las organizaciones deben implementar estrategias de desarrollo de la fuerza laboral de ciberseguridad para satisfacer las demandas actuales y futuras de la fuerza laboral. Cuando hay una falta de profesionales calificados, las organizaciones deben innovar para hacer crecer su fuerza laboral. Para que las empresas se protejan de manera confiable a largo plazo, lo más importante que pueden hacer es concentrarse en retener a sus mejores empleados. Según (WEF, 2022), la retención y el equilibrio entre el trabajo y la vida también son factores que amplifican la escasez de talento, encontrando que el 6% de los ciber líderes expresan que en sus organizaciones faltan personas y habilidades críticas, el 6% depende de terceros y recursos externos, el 37 % tiene las personas y las habilidades que necesita hoy y el 47% tienen brechas de capacitación y habilidades en algunas áreas. Las organizaciones deben mejorar su capacidad para retener a las personas haciendo posible que los empleados mejoren sus habilidades, se certifiquen y continúen con su desarrollo profesional.

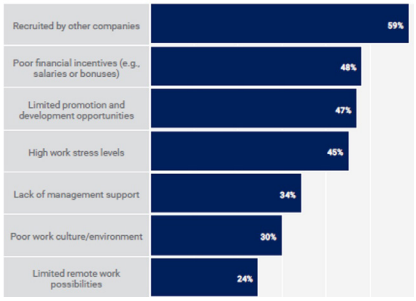
Retos

Existen varios problemas en las organizaciones para retener el talento de la fuerza laboral en ciberseguridad. La incapacidad de adquirir y retener el talento en ciberseguridad necesario para abordar los retos actuales es un factor limitante clave tanto para el sector privado como para el público. Existe una falta de programas de formación suficiente y adecuada para los empleados, especialmente en las PYMES. Además, este segmento afronta riesgos debido a la existencia de formación en ciberseguridad de baja calidad en el mercado de formación externo ya que la mayoría de las organizaciones compran capacitación principalmente en función del costo y la velocidad, sin reconocer inicialmente el valor de los cursos más largos[88]. Según (LinkedIn, 2022), actualmente las organizaciones deben priorizar el éxito personal de los empleados a través del desarrollo profesional. Según (ISACA, 2022), el 60% de las respuestas de la encuesta apuntan a la dificultad para retener el talento en empresas del sector de ciberseguridad, siendo las principales causas el reclutamiento por otras empresas, los bajos incentivos y la limitada promoción.

Algunas cifras

Gráfica 40.

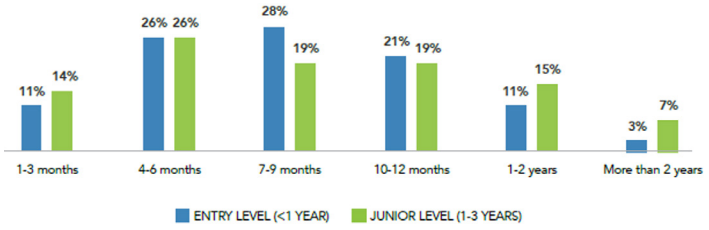
Principales causas de renuncia de los profesionales de ciberseguridad



Fuente: (ISACA, 2022)

Gráfica 41.

¿Cuánto tiempo lleva capacitar al personal de nivel inicial y junior?



Fuente: (ISC2, 2022b)

Buenas prácticas

Las organizaciones deben implementar estrategias innovadoras para retener a la fuerza laboral y al talento, combinando varios incentivos como el salario, la formación, la reputación y las oportunidades de progresar. Según (MERCER, 2022), las organizaciones deben considerar diferentes estructuras de recompensas para diferentes modelos de trabajo, por ejemplo, un cambio hacia el pago basado en habilidades es una solución. También menciona que se deben considerar las notables diferencias generacionales[89], por ejemplo, la Generación X y los Baby Boomers valoran más el sentido de pertenencia mientras que los Millennials valoran más las oportunidades para aprender nuevas habilidades. Según (ISC2, 2022b), las tutorías, las certificaciones y la orientación profesional se encuentran entre las herramientas y los recursos que los participantes del estudio ofrecen para ayudar a los recién llegados a adquirir experiencia, desarrollar sus habilidades y lograr nuevos hitos profesionales. Según (ESG, 2021), algunas acciones que la organización podría tomar para retener la fuerza laboral y abordar el impacto de la escasez de habilidades en ciberseguridad son aumentar el compromiso con la formación, aumentar los niveles de compensación, ofrecer incentivos como el pago de certificaciones y la participación en eventos, crear/mejorar programas de prácticas en ciberseguridad.

88 Según (DCMS & IPSOS, 2022), esto había incentivado la entrada en el mercado de cursos de formación de baja calidad, lo que a su vez había dificultado que las organizaciones distinguieran entre una buena y una mala formación. En este informe también se menciona que las universidades y los proveedores de educación superior también habían sesgado el mercado en esta dirección, al favorecer cursos cortos impartidos externamente que tenían altas tasas de aprobación. Un indicador de esto fue la amplia brecha en los cargos entre los proveedores de capacitación más baratos y caros.

89 Un ejemplo de esto se aprecia en el reporte de *Tendencias de selección globales de 2022* (LinkedIn, 2022), en donde el 66% de personas de la Generación Z que respondieron su encuesta global menciona que le gustaría ver más inversión en salud mental y bienestar para mejorar la cultura empresarial, mientras que el 51% de Millenials, el 41% de la Generación X y tan sólo el 31% de Baby Boomers apoyan dicha idea.

05

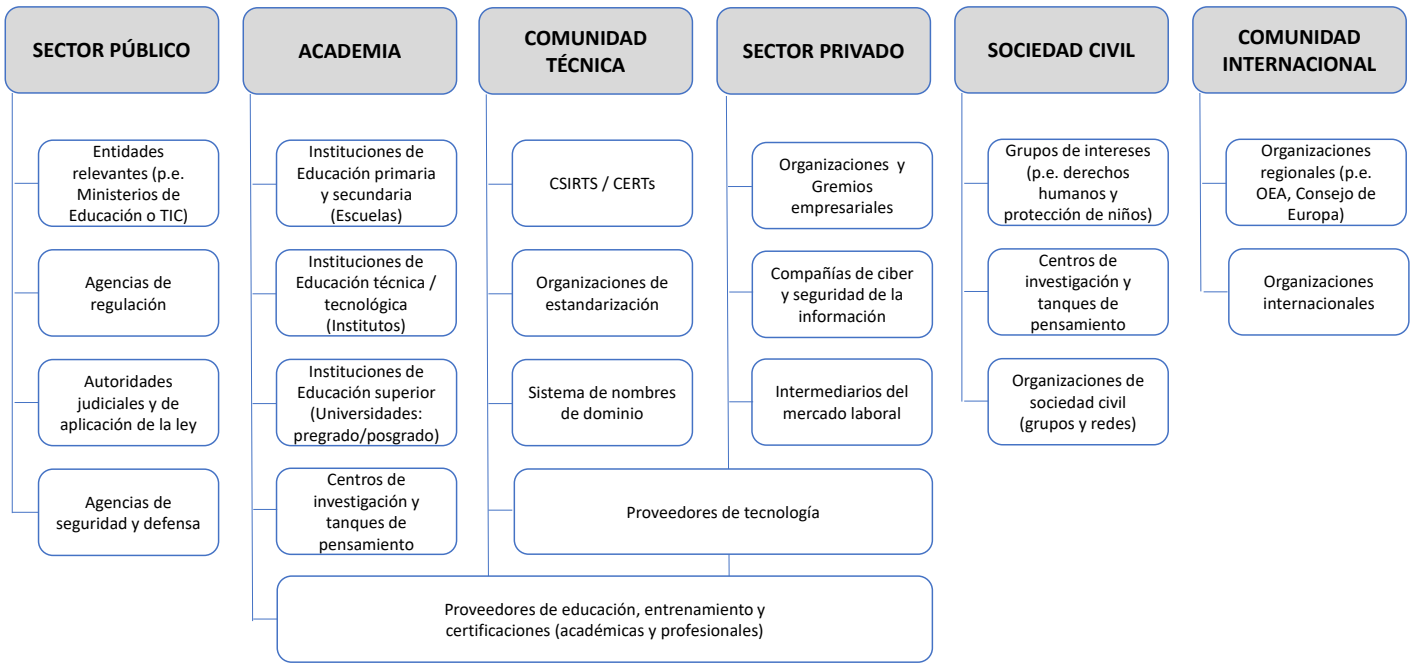
LAS MÚLTIPLES PARTES INTERESADAS EN LA REGIÓN DEBEN PASAR A LA ACCIÓN

Las condiciones actuales del mercado laboral de ciberseguridad y los desafíos analizados exigen en los países de América Latina y el Caribe, por una parte, que se desarrollen y apliquen nuevos caminos en la educación y formación para la provisión de un mayor número de solicitantes de empleo en ciberseguridad con las habilidades necesarias y, por otra, que se invierta en estrategias innovadoras de reclutamiento, capacitación y entrenamiento de la actual fuerza laboral por parte de las organizaciones.

El problema identificado relacionado con la escasez de mano de obra y de habilidades en ciberseguridad en la región puede ser afrontado logrando que las múltiples partes interesadas (sector público, academia, comunidad técnica, sector privado, sociedad civil y comunidad internacional) pasen a la acción. A nivel internacional, la práctica más común para resolver la problemática identificada es abordar de manera integral los desafíos en el mercado laboral de ciberseguridad mediante enfoques inclusivos y cooperativos que fomenten la participación de las múltiples partes interesadas en el ecosistema de ciberseguridad.

Gráfica 42.

Representación esquemática de las múltiples partes interesadas relacionadas con el desarrollo de la fuerza laboral de ciberseguridad[90]



Fuente: Elaboración propia

90 Esta gráfica ilustra los grupos de partes interesadas relevantes, incluida una lista no exhaustiva de partes interesadas potenciales en cada grupo. Es importante reconocer que cualquier agrupación de partes interesadas debe abordarse con flexibilidad y precaución, ya que las categorías y subcategorías pueden cambiar según el contexto local para cada país de la región y la autoidentificación de las partes interesadas. Como regla general, el marco para identificar a los actores relevantes debe ser tan amplio y flexible como sea necesario para que no restrinja la participación efectiva de los actores relevantes

5.1. RECOMENDACIONES PARA LOS GOBIERNOS DE LA REGIÓN

El problema de escasez de profesionales y de habilidades en ciberseguridad es un asunto de política multidimensional en el que participan múltiples partes interesadas y se ve agravada por muchos factores. Los gobiernos de la región juegan un papel fundamental para el desarrollo de la fuerza laboral con el fin de brindar a las personas educación, desarrollar habilidades y un mejor acceso al empleo y el avance en el mercado laboral para lograr el máximo crecimiento económico sostenible en general.

En primer lugar, se recomienda que los gobiernos desarrollen estrategias nacionales y planes de acción para el desarrollo de la fuerza laboral en ciberseguridad, adelantando al menos las siguientes acciones:

- Crear un modelo de gobernanza para la articulación y la armonización de las múltiples partes interesadas con el fin de fortalecer las capacidades del país en torno al desarrollo de la fuerza laboral de ciberseguridad.
- Desde el lado de la oferta laboral, elaborar e incluir un plan de acción para la educación en ciberseguridad[91], abordando los desafíos identificados más adelante.
- Desde el lado de la demanda laboral, elaborar e incluir un plan de acción para promover el reclutamiento, retención, capacitación y entrenamiento de la actual fuerza laboral de ciberseguridad, abordando los desafíos identificados más adelante.
- Financiar las estrategias nacionales y los planes de acción relacionadas con el desarrollo de la fuerza laboral de ciberseguridad.
- Crear hubs de habilidades y empleo / fondos (posibles esquemas de subsidios para segmentos específicos de la población).

En segundo lugar, los gobiernos deben establecer estructuras de liderazgo y coordinación a nivel nacional y regional, adelantando al menos las siguientes acciones:

- Convocar a todas las múltiples partes interesadas en altas instancias de decisión y en grupos de trabajo.
- Promover la máxima colaboración y cooperación entre las múltiples partes interesadas, teniendo en cuenta el rol y el grado de responsabilidad en la formación y desarrollo de la fuerza laboral.
- Promover el diálogo social y las alianzas entre las múltiples partes interesadas para el desarrollo de habilidades de la fuerza laboral.
- Facilitar la implementación de iniciativas regionales conjuntas para abordar la escasez laboral y la brecha de habilidades en ciberseguridad.
- Desarrollar ecosistemas para la formación en ciberseguridad que motive a los estudiantes y profesionales a desarrollar su carrera en ciberseguridad.

45 Ver la propuesta elaborada por el Programa de Ciberseguridad de la OEA y Amazon Web Services -AWS- en la Edición 9 del White Paper Series 2020 llamado *"Educación en Ciberseguridad - Planificación del futuro mediante el desarrollo de la fuerza laboral"* (OEA & AWS, 2020)

En tercer lugar, se presentan consideraciones con el fin de que los gobiernos aborden desafíos identificados de manera específica para el desarrollo de alianzas público-privadas, la actualización de marcos legislativos y regulatorios, la recopilación y evaluación continua de datos relacionada y la sensibilización y divulgación de recursos, herramientas e información para el desarrollo de la fuerza laboral en ciberseguridad.

1) Establecer estrategias para desarrollar alianzas público-privadas

El desarrollo de fuerza laboral en ciberseguridad depende de una estrecha coordinación entre los gobiernos, el sector privado y los proveedores de educación o formación. En particular, los gobiernos deben:

- Involucrar a los empleadores de las organizaciones en el lanzamiento de nuevos programas de capacitación.
- Actualizar los planes de estudios y la entrega de los programas existentes para mejorar los programas de aprendizaje en el trabajo a las necesidades del mercado laboral.
- Diseñar una estrategia integral de desarrollo de la fuerza laboral de ciberseguridad que no solo cubra políticas dirigidas al sistema de educación, capacitación y formación, sino que promueva el desarrollo de alianzas público-privadas.

2) Actualizar o adaptar marcos legislativos y regulatorios para promover el desarrollo de la fuerza laboral

En (OEA & BID, 2020) se resalta la importancia de que los países de la región América Latina y el Caribe cuenten con marcos legales y regulatorios efectivos con el fin de mejorar el nivel de madurez de capacidades de ciberseguridad. Dado que un marco legislativo establece la base mínima de comportamiento sobre la que se pueden construir más capacidades de ciberseguridad, el objetivo es que los países cuenten con legislación suficiente para armonizar las prácticas a nivel regional / internacional. Por lo tanto, los gobiernos deben:

- Adecuar, adaptar y/o armonizar el marco legal y regulatorio nacional en torno a la dinámica de la economía digital y sus incertidumbres inherentes, ya que en muchos casos dichos marcos nacionales son dispersos y están desactualizado en muchos ámbitos relacionados con la ciberseguridad, incluido aspectos que tienen relación con los desafíos identificados en el análisis del mercado laboral y que impactan el desarrollo de la fuerza laboral en la región.

3) Promover la recopilación y evaluación continua de datos del mercado laboral y de la fuerza laboral de ciberseguridad

En término generales, el personal que trabaja en desarrollo de la fuerza laboral cibernética carece de datos precisos para medir y comprender el impacto de diferentes esfuerzos e intervenciones de políticas en la fuerza laboral de ciberseguridad. Cerrar brechas en el mercado laboral de ciberseguridad requiere un conocimiento detallado de la fuerza laboral de ciberseguridad en los países de la región, por lo tanto, los gobiernos de la región deben:

- Impulsar la cooperación entre las múltiples partes interesadas para la recopilación y compartición de la información[92].

46 En Estados Unidos, se resalta la iniciativa CyberSeek que presenta a empleadores locales, educadores, consejeros de orientación y carrera, estudiantes, trabajadores actuales, legisladores y otras partes interesadas herramientas como: i) un mapa de calor interactivo que proporciona la situación instantánea y granular de la oferta y la demanda de trabajos de ciberseguridad a nivel estatal y de área metropolitana, ii) una propuesta de rutas profesionales que muestra trabajos clave de ciberseguridad, oportunidades de transición comunes entre ellos e información detallada sobre los salarios, las credenciales y los conjuntos de habilidades asociados con cada rol, y iii) una herramienta que informa sobre diferentes programas de educación y formación así como de proveedores de entrenamiento en el país.

- Promover la colaboración entre las múltiples partes interesadas para investigar y difundir los resultados sobre los factores que influyen en el impacto de la educación, la capacitación y el desarrollo de la fuerza laboral en ciberseguridad[93].

- Utilizar los resultados de la investigación para informar los programas y el diseño del currículo, fomentar oportunidades de aprendizaje continuo, impactar el éxito del alumno y garantizar un acceso equitativo.

- Establecer y mantener un directorio de programas y actividades de proyectos, iniciativas y recursos relacionados con la concientización, exploración, preparación, colocación, mantenimiento y tutoría de la carrera de ciberseguridad.

- Promover el análisis de las necesidades del mercado de la ciberseguridad y las tendencias relacionadas a través de la identificación de métricas que muestren el alcance del problema y las posibles medidas para hacerle frente.

4) Sensibilizar y divulgar sobre recursos, herramientas e información para el desarrollo de la fuerza laboral en ciberseguridad

En los países de la región es necesario que la población en general sea más consciente de su seguridad personal, pero también aumenta la conciencia de las oportunidades profesionales en ciberseguridad, lo que ayudaría a encaminar a los futuros profesionales de ciberseguridad hacia sus carreras. Los gobiernos deben:

- Sensibilizar y divulgar sobre recursos, herramientas e información para el desarrollo de la fuerza laboral de ciberseguridad para ayudar a las organizaciones a reclutar profesionales calificados de manera más eficiente y efectiva, y a proporcionar a esta fuerza laboral crítica descripciones de trabajo claras y oportunidades de desarrollo.

- Adoptar y promover el diseño y conformación de bases de datos de educación, especialmente del sector de educación superior, sobre ciberseguridad y bases de datos para promocionar la demanda laboral tanto en el sector privado como en el sector público.

- Trabajar con la industria para crear conciencia sobre las calificaciones, certificaciones, títulos y estándares de aprendizaje, llegando tanto a los empleadores como a los profesionales de la ciberseguridad (GFCE, 2022).

93 Se destaca la experiencia del Reino Unido adelantando encuestas, estudios y reportes detallados sobre el mercado laboral de ciberseguridad, los cuales reúne datos de las brechas y la escasez de habilidades a partir del análisis de la oferta laboral y de la demanda laboral de ciberseguridad. Este tipo de informes resaltan, por un lado, los desafíos de satisfacer las necesidades de contratación y formación de los empleadores, y por otro, la perspectiva de las personas que ingresan o están activas en el mercado laboral de ciberseguridad, ilustrando las dificultades que enfrentan para encontrar la carrera y las vías de capacitación adecuadas, y la creciente necesidad de un conjunto de habilidades holísticas en varios roles.

5.2. RECOMENDACIONES POR EL LADO DE LA OFERTA LABORAL

Con el fin de incrementar las vocaciones científicas en la población infantil y juvenil de la región, las entidades del sector público relacionadas junto con la academia (instituciones educación primaria y secundaria) deben:

- Evaluar y actualizar las políticas educativas nacionales que hacen énfasis en las habilidades STEM para docentes y estudiantes.
- Fomentar la alfabetización digital en la población infantil y juvenil promoviendo vocaciones científicas y énfasis STEM.
- Organizar eventos masivos para aprovechar el grupo de talentos e invertir en la creación de prácticas para el fortalecimiento de capacidades y habilidades STEM.

Con el fin de fortalecer el dominio del inglés en la región, las entidades del sector público relacionadas junto con la academia (instituciones educación primaria, secundaria y educación superior) deben:

- Evaluar y actualizar las políticas educativas nacionales de promoción de idiomas y de bilingüismo en marcha e identificar las dificultades clave que afectan las oportunidades para lograr un dominio del idioma inglés tanto en estudiantes como en profesores en los sistemas educativos de la región.
- Actualizar los programas y/o estrategias nacionales de bilingüismo incorporando el uso de nuevas tecnologías para el aprendizaje.
- Crear contenidos educativos complementarios relacionados con la gestión de riesgos de ciberseguridad en idioma inglés y capacitar a los estudiantes de educación básica y media, y a los estudiantes de educación superior.

Con el fin de concientizar y sensibilizar en ciberseguridad durante la edad temprana, las entidades del sector público relacionadas junto con la academia (instituciones educación primaria y secundaria) deben:

- Identificar y compartir prácticas efectivas para promover la conciencia de los niños y jóvenes y el descubrimiento de la carrera de ciberseguridad.
- Proporcionar información y herramientas sobre opciones profesionales relacionadas con la ciberseguridad a quienes influyen en las opciones profesionales (por ejemplo, profesores, consejeros escolares, entrenadores profesionales, mentores, padres o tutores).
- Sensibilizar sobre la privacidad y la ciberseguridad entre los usuarios de tecnologías, especialmente los usuarios jóvenes, a través de ejercicios masivos de capacitación y desarrollo de capacidades.

Con el fin de promover el acceso a la oferta educativa, las entidades del sector público relacionadas junto con la academia (instituciones de educación técnica / tecnológica y de educación superior) deben:

- Desarrollar y utilizar herramientas y recursos para identificar y atraer a las personas con más probabilidades de tener éxito en el mercado laboral.
- Diversificar y actualizar los planes de estudio de la educación básica, media y superior incluyendo contenidos de ciberseguridad.
- Promover y facilitar la accesibilidad a los programas académicos relacionados.
- Poner a disposición más becas y esfuerzos más activos centrados en la diversidad para aumentar inscripciones.
- Promover y fomentar materias específicas como criptografía, los planes de estudio de la educación básica, media y superior.

Con el fin de conectar la educación con la formación y la industria, el sector público, el sector privado, la comunidad técnica (organizaciones de estandarización) y la academia deben:

- Promover el uso de enfoques unificados relativos a las funciones, competencias, habilidades y conocimientos en ciberseguridad.
- Desarrollar currículos estandarizados que establezcan una taxonomía y un léxico común para la ciberseguridad para que las instituciones de educación alineen sus planes de estudios a los estándares establecidos.
- Integrar el conocimiento de la industria sobre ciberseguridad en los diversos cursos que componen la oferta académica para que la desconexión de la academia y de la industria pueda superarse gradualmente.
- Actualizar los contenidos de educación en ciberseguridad para aplicarse en ambos sectores: educación de alto nivel y en la industria relevante.
- Promover casos de uso creíbles en el mundo académico para el desarrollo de habilidades.
- Promover desafíos y competencias en el mundo empresarial para el desarrollo de habilidades en ciberseguridad.
- Promover una estrategia de certificación de títulos en ciberseguridad a nivel nacional.

Con el fin de promover el acceso a las rutas de aprendizaje, el sector público, el sector privado y la academia junto con los *Proveedores de educación, entrenamiento y certificaciones* y los *Proveedores de Tecnología* deben:

- Fomentar la democratización del conocimiento para el desarrollo de habilidades.
- Garantizar vías de articulación claras entre la escuela, la universidad, la industria y el mercado laboral de ciberseguridad.
- Aumentar la comprensión por parte de los estudiantes y solicitantes de empleo de las rutas de aprendizaje y de las certificaciones académicas.
- Trabajar para garantizar que los programas de grado académico y las certificaciones reconocidas por la industria midan de manera efectiva las competencias de ciberseguridad.
- Aumentar la inversión de los socios del sector privado en la fuerza laboral de ciberseguridad.

Con el fin de aclarar la definición de la profesión en ciberseguridad, el sector público, el sector privado y la academia junto con los *Proveedores de educación, entrenamiento y certificaciones*, los *Proveedores de Tecnología,* la Comunidad Técnica (Organismos de Estandarización) y la Comunidad Internacional deben:

- Impulsar iniciativas para la estandarización nacional (y si es posible, regional) para la generación de currículos y planes de estudios con el fin de establecer una definición del trabajo de ciberseguridad bajo un lenguaje común y la categorización de los roles en ciberseguridad.
- Impulsar el uso del lenguaje común y la categorización de los roles en ciberseguridad en la región América Latina y el Caribe.

5.3. RECOMENDACIONES POR EL LADO DE LA DEMANDA LABORAL

Con el fin de garantizar que la demanda y la oferta hablen un lenguaje común, el sector público, el sector privado y la academia junto con los *Proveedores de educación, entrenamiento y certificaciones*, los Proveedores de Tecnología, la Comunidad Técnica (Organismos de Estandarización) y la Comunidad Internacional deben:

- Elaborar marcos de trabajo para la generación de un léxico y lenguaje común para generar incentivos y promover la fuerza laboral de ciberseguridad.
- Dar claridad en las funciones, roles y responsabilidades para el desarrollo de la fuerza laboral de ciberseguridad.
- Utilizar nuevas tecnologías emergentes para aumentar las conexiones y el ajuste entre los empleadores y los solicitantes de empleo.

Con el fin de ajustar los requisitos de contratación para atraer el mejor talento, las entidades del sector público y las organizaciones del sector privado deben:

- Mejorar las capacidades para reclutar y contratar de manera efectiva el talento necesario para gestionar los riesgos relacionados con la ciberseguridad.
- Promover el establecimiento de más puestos de nivel de entrada y oportunidades que brinden vías para el crecimiento y el avance.
- Promover la comunicación entre las áreas de recursos humanos y las de ciberseguridad con el fin de concertar los perfiles requeridos por la organización.

Con el fin de promover la diversidad, equidad e inclusión en la fuerza laboral, el sector público, el sector privado, la academia, la comunidad técnica, la sociedad civil y comunidad internacional deben:

- Promover la diversidad en la fuerza laboral en todos los niveles, mejorar el equilibrio de género y crear programas teniendo en cuenta la diversificación de la fuerza laboral.
- Identificar y promover métodos de aprendizaje efectivos, prácticas y programas educativos que hagan crecer y desarrollen una fuerza laboral de ciberseguridad diversa e inclusiva.
- Garantizar la financiación para la formación, el perfeccionamiento y el reciclaje profesional, especialmente para las mujeres, los grupos desfavorecidos y los sectores más afectados.

Con el fin de impulsar los marcos de trayectorias profesionales, el sector público, el sector privado y la academia junto con los *Proveedores de educación, entrenamiento y certificaciones* y los *Proveedores de Tecnología* deben:

- Aumentar la accesibilidad y la asequibilidad a los marcos de trayectoria profesional en ciberseguridad.
- Ampliar los presupuestos en los esfuerzos existentes para el desarrollo de la fuerza laboral de ciberseguridad.
- Fomentar prácticas efectivas para volver a capacitar a los desempleados, subempleados, trabajadores titulares para prepararlos para carreras en ciberseguridad.
- Tomar medidas específicas para fomentar la oferta y la participación en programas de aprendizaje en el trabajo, incluidos las pasantías y las prácticas profesionales.
- Identificar, medir y difundir oportunidades exitosas de aprendizaje basado en el trabajo de ciberseguridad.
- Proporcionar motivación a las organizaciones a través de diversos mecanismos para desarrollar cursos y certificaciones internos, productos, marcos, etc.

Con el fin de retener a la fuerza laboral, las entidades del sector público y las organizaciones del sector privado deben:

- Identificar, atraer y reclutar al mejor talento disponible y retenerlo implementando estrategias innovadoras de capacitación y entrenamiento, tales como: i) Upskilling (procesos de aprendizaje de nuevas habilidades o de enseñar nuevas habilidades a los empleados), ii) Reskilling (procesos de capacitación a empleados en un conjunto completamente nuevo de habilidades para prepararlos para asumir un rol diferente dentro de la empresa), y iii) New Skilling (procesos de aprendizaje continuo para ayudar a desarrollar habilidades de alta demanda, ya sea que una persona esté tratando de mejorar las capacidades actuales o que necesite una actualización completa para desarrollar capacidades completamente nuevas).
- Fomentar programas de aprendizaje basados en el trabajo, incluidas pasantías y prácticas laborales.
- Proporcionar incentivos para convertir a los empleados de nivel inicial en talentos de mitad de carrera y talentos de carrera avanzada.
- Fomentar y permitir el desarrollo y la capacitación continuos de los empleados, incluidos los programas rotativos y de intercambio, para fomentar el mantenimiento del talento actual con diversas habilidades y experiencias.

06

REFERENCIAS BIBLIOGRÁFICAS

ASPENDIGITAL. (Septiembre de 2021). Diversity, Equity, and Inclusion in Cybersecurity. Obtenido de https://www.aspeninstitute.org/wp-content/uploads/2021/09/Diversity-Equity-and-Inclusion-in-Cybersecurity_9.921.pdf

BID. (2020). El futuro del trabajo en America Latina y el Caribe - Cual es el impacto de la automatizacion en el empleo y los salarios. Obtenido de https://publications.iadb.org/publications/spanish/document/El-futuro-del-trabajo-en-America-Latina-y-el-Caribe-Cual-es-el-impacto-de-la-automatizacion-en-el-empleo-y-los-salarios.pdf

BID. (2021). *El impacto de la automatización, más allá de las fronteras.* Obtenido de https://blogs.iadb.org/trabajo/es/el-impacto-de-la-automatizacion-mas-alla-de-las-fronteras/

BID, CEPAL & KAS. (2021). Recuperacion economica tras la pandemia COVID-19 - Empoderar a America Latina y el Caribe para un mejor aprovechamiento del comercio electronico y digital. Obtenido de https://publications.iadb.org/publications/spanish/document/Recuperacion-economica-tras-la-pandemia-COVID-19-empoderar-a-America-Latina-y-el-Caribe-para-un-mejor-aprovechamiento-del-comercio-electronico-y-digital.pdf

CISCO. (2022). *Employees are ready for hybrid work, are you? Cisco Global Hybrid Work Study 2022*. Obtenido de https://www.cisco.com/c/dam/m/en_us/solutions/global-hybrid-work-study/reports/cisco-global-hybrid-work-study-2022.pdf

Computer Science. (2022). Obtenido de Women in Computer Science: Getting Involved in STEM: https://www.computerscience.org/resources/women-in-computer-science/

Cook, I. (15 de Septiembre de 2021). *"Who Is Driving the Great Resignation?"*. (T. H. Review, Editor) Obtenido de https://hbr.org/2021/09/who-is-driving-the-great-resignation

CSA. (2021). Operational Technology Cybersecurity Competency Framework. Obtenido de https://www.csa.gov.sg/News/Publications/operational-technology-cybersecurity-competency-framework-(otccf)

CSES. (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development. Obtenido de https://www.gov.uk/government/publications/the-role-of-further-and-higher-education-in-cyber-security-skills

CyberSeek. (Agosto de 2022). *Cybersecurity supply/demand heat map.* Obtenido de https://www.cyberseek.org/heatmap.html

DCMS & IPSOS. (2022). Cyber security skills in the UK labour market 2022 - Findings report. Obtenido de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf

DELOITTE. (2020). Workforce development: Equipping the workforce for the future. Obtenido de https://www2.deloitte.com/us/en/pages/human-capital/articles/workforce-development-strategies.html

DNP. (2020). Política Nacional de Confianza y Seguridad Digital de Colombia (Documento CONPES 3995 de 2020). Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

DNP. (2022). Política Nacional de Ciencia, Tecnología e Innovación de Colombia 2022-2031 (Documento CONPES 4069 de 2022). Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%c3%b3micos/4069.pdf

ENISA. (2022). European Cybersecurity Skills Framework ECSF - Draft v0.5. Obtenido de https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf

ESG. (2021). ESG Infographic: the Life and Times of Cybersecurity Professionals 2021. Obtenido de https://www.esg-global.com/research/esg-infographic-the-life-and-times-of-cybersecurity-professionals-2021

FORBES. (31 de Julio de 2022). *The Future Of Work: More Hybrid, More Collaborative, More Automated.* Obtenido de https://www.forbes.com/sites/danielnewman/2022/07/31/the-future-of-work-more-hybrid-more-collaborative-more-automated/?sh=77896d589c46

FORTINET. (18 de Agosto de 2022). Obtenido de https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortinet-registro-137-mil-millones-de-intentos-de-ciberataques-e

FORTINET. (2022). 2022 Cybersecurity Skills Gap - Global Research Report. Obtenido de https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

GFCE. (Julio de 2022). Developing Cyber Security as a Profession - A Report by the Global Forum on Cyber Expertise. Obtenido de https://thegfce.org/wp-content/uploads/2022/08/GFCE-Report-Developing-Cyber-Security-as-a-Profession-July-2022-1.pdf

GFCE. (2022). Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people. Obtenido de https://thegfce.org/wp-content/uploads/2022/08/GFCE-report-20220731.pdf

GLOBAL PARTNERS DIGITAL. (2018). *Multistakeholder Approaches to National Cybersecurity Strategy Development*. Obtenido de Multistakeholder Approaches to National Cybersecurity Strategy Development: https://www.gp-digital.org/publication/multistakeholder-approaches-to-national-cybersecurity-strategy-development/

ILO. (11 de Agosto de 2022). *Global Employment Trends for Youth.* Obtenido de https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_853078/lang—en/index.htm

ILO. (2022). ILOSTAT. Obtenido de https://ilostat.ilo.org/es/data/

ISACA. (2022). State of Cybersecurity 2022. Obtenido de https://www.isaca.org/go/state-of-cybersecurity-2022

ISC2. (2021). Cybersecurity Workforce Study. Obtenido de https://www.isc2.org/Research/Workforce-Study

ISC2. (2022a). Cybersecurity Workforce Study. Obtenido de https://www.isc2.org/-/media/2A313135414E400FA0DBD364FD74961F.ashx

ISC2. (2022b). Best Practices for Hiring and Developing Entry and Junior-Level Cybersecurity Practitioners. Obtenido de https://www.isc2.org//-/media/ISC2/Research/2022/ISC2-Cybersecurity-Hiring-Managers-Guide.ashx

Kang, N. (2019). A review of the effect of integrated STEM or STEAM (science, technology, engineering, arts, and mathematics) education in South Korea. *Asia Pac. Sci. Educ*. doi: https://doi.org/10.1186/s41029-019-0034-y

LinkedIn. (2022). The Reinvention of Company Culture - Global Talent Trends 2022. Obtenido de https://business.linkedin.com/content/dam/me/business/en-us/talent-solutions-lodestone/body/pdf/global_talent_trends_2022.pdf

LinkedIn. (2022). The Transformation of L&D - Learning leads the way through the Great Reshuffle. Obtenido de https://learning.linkedin.com/content/dam/me/learning/en-us/pdfs/workplace-learning-report/LinkedIn-Learning_Workplace-Learning-Report-2022-EN.pdf

MERCER. (2022). Rise of the relatable organization - Global Talent Trends 2022 Study. Obtenido de https://www.mercer.com/our-thinking/career/global-talent-hr-trends.html

MichaelPage. (2022). Estudio de Perspectivas LATAM 2022. Obtenido de https://www.michaelpage.com.co/estudios-y-tendencias/perspectivas-2022

MICROSOFT. (23 de Marzo de 2022). *Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries.* Obtenido de https://blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries/

MINEDUCACION. (Septiembre de 2022). *Sistema Nacional de Información de la Educación Superior -SNIES-*. Obtenido de https://hecaa.mineducacion.gov.co/consultaspublicas/programas

NICCS. (2022). *Cyber Career Pathways Tool*. Obtenido de https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool

OEA & AWS. (2020). Educación en Ciberseguridad - Planificación del futuro mediante el desarrollo de la fuerza laboral. Obtenido de https://www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf

OEA & BID. (2020). Reporte de Ciberseguridad 2020 - Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe. Obtenido de https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

OEA & GPD. (2022). National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions. Obtenido de https://www.gp-digital.org/publication/national-cybersecurity-strategies-lessons-learned-and-reflections-from-the-americas-and-other-regions/

OECD. (2021). OECD Employment Outlook 2021: Navigating the COVID-19 Crissi and Recovery. Paris: OECD Publishing. Obtenido de https://read.oecd-ilibrary.org/employment/oecd-employment-outlook-2021_5a700c4b-en#page1

OECD. (2022). Obtenido de OECD Data - Mathematics performance (PISA): https://data.oecd.org/pisa/mathematics-performance-pisa.htm

OECD. (2022). *Supporting SME development in Latin America and the Caribbean.* Obtenido de https://www.oecd.org/latin-america/regional-programme/productivity/sme-development/

Oxford Martin School. (2022). *Oxford Institute of Populating Ageing.* Obtenido de https://www.oxfordmartin.ox.ac.uk/ageing/

RAND. (2014). Hackers Wanted: An Examination of the Cybersecurity. Obtenido de https://www.rand.org/pubs/research_reports/RR430.html

WEF. (2022). Global Cybersecurity Outlook 2022. Obtenido de https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

WEF. (2022). Global Gender Gap Report 2022. Obtenido de https://www.weforum.org/reports/global-gender-gap-report-2022/

WICKR. (18 de February de 2021). Obtenido de The Future of Cybersecurity Depends on STEM Education: https://wickr.com/the-future-of-cybersecurity-depends-on-stem-education/

World Bank. (2019). Obtenido de What are the main lessons from the latest results from PISA 2018 for Latin America?: https://blogs.worldbank.org/latinamerica/what-are-the-main-results-pisa-2018-latin-america

WORLD BANK. (2022). *Global Growth to Slow through 2023, Adding to Risk of 'Hard Landing' in Developing Economies.* Obtenido de https://www.worldbank.org/en/news/press-release/2022/01/11/global-recovery-economics-debt-commodity-inequality

2023

Reporte sobre el desarrollo de la

FUERZA LABORAL DE CIBERSEGURIDAD

en una era de escasez de talento y habilidades

OEA | Más derechos para más gente

Cybersecurity Innovation Councils

CISCO