2020

White paper series
Edición 9

_ EDUCACIÓN EN _ CIBERSEGURIDAD

Planificación del futuro mediante el desarrollo de la fuerza laboral

OEA Más derechos para más gente | aws

EDUCACIÓN EN **CIBERSEGURIDAD**

Planificación del futuro mediante el desarrollo de la fuerza laboral

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

CRÉDITOS

Luis Almagro
Secretario General
Organización de los Estados Americanos (OEA)

Equipo Técnico de la OEA
Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Gabriela Montes de Oca Fehr
Babara Marchiori de Assis
Rolando Ramirez

Equipo Técnico de AWS
Abby Daniell
Melanie Kaplan
Jordana Siegel

_ EDUCACIÓN EN _
CIBERSEGURIDAD
Planificación del futuro mediante
el desarrollo de la fuerza laboral

ÍNDICE DE CONTENIDO

EDUCACIÓN EN **CIBERSEGURIDAD**

Planificación del futuro mediante
el desarrollo de la fuerza laboral

¿Qué se propone este documento?

Dado el aumento continuo del número de actividades maliciosas en el ciberespacio, es evidente que una fuerza laboral capacitada en ciberseguridad es una necesidad. Las habilidades indispensables de dicha fuerza laboral incluyen la capacidad de diseñar y operar, de manera óptima, aplicaciones y sistemas que puedan identificar y responder a las amenazas cibernéticas, así como la capacidad de diseñar políticas públicas efectivas para contrarrestar esas amenazas. Los desafíos futuros de la fuerza laboral en ciberseguridad solo pueden abordarse fomentando carreras en ciberseguridad. La disparidad entre la oferta y la demanda de profesionales cualificados en ciberseguridad requiere una acción inmediata para capacitar a los expertos actuales mientras se formulan políticas para educar a la próxima generación de profesionales en ciberseguridad. Sin políticas para mejorar las habilidades en ciberseguridad de la fuerza laboral, un país no disfrutará plenamente de los beneficios de la economía digital. Este documento describe los pasos para diseñar un plan de acción para la educación en ciberseguridad que incluya mecanismos para integrar la educación en ciberseguridad al establecimiento de políticas y planes de estudios y así para superar la escasez de habilidades en ciberseguridad en América Latina y el Caribe. También ofrece un conjunto de iniciativas y mecanismos a nivel nacional para generar interés en carreras en ciberseguridad.

_ EDUCACIÓN EN _
CIBERSEGURIDAD

Planificación del futuro mediante
el desarrollo de la fuerza laboral

¿Por qué es importante la educación en ciberseguridad en América Latina?

La Cuarta Revolución Industrial está impulsada por una mayor interconectividad en el mundo (Schwab, 2016, pág. 3). América Latina ha adoptado rápidamente los servicios digitales habilitados por la computación en la nube, los dispositivos móviles y las redes de banda ancha, lo que ha permitido que haya una transformación más profunda en los Gobiernos y las empresas, incluida la incorporación del procesamiento de datos para la toma de decisiones integrada y eficaz por parte de quienes se encargan de la formulación de políticas. A pesar de haberse adoptado estas tecnologías en América Latina, el nuevo panorama también ha transformado la naturaleza y las operaciones delincuenciales. En América Latina y el Caribe, se ha estimado el costo del ciberdelito entre US$15 mil millones y US$30 mil millones en 2017; es decir, entre el 0,28 % y el 0,57 % del PIB de la región (Lewis, 2018, pág. 7). Los países de la región no solo son un blanco de ataques en línea, sino también una fuente activa de ellos (Lewis, 2018, pág. 20). El aumento de los riesgos cibernéticos está obligando a las empresas y a los Gobiernos a integrar la ciberseguridad en sus procesos, en la adquisición de tecnología y en la selección de personal.

A pesar de estas amenazas, sigue habiendo una escasez global de profesionales en ciberseguridad, y se estima que el déficit asciende a unos 4,07 millones de personas. Solo en la región de América Latina, este déficit es de aproximadamente 600 000 personas ((ISC)², 2019, pág. 8). Esta cifra representa un aumento significativo en comparación con 2018, cuando la escasez se estimó en unos 136 000 profesionales ((ISC)², 2018, pág. 4). Tanto las empresas medianas como las grandes demandan un gran número de profesionales de la ciberseguridad, lo que requiere una fuerza laboral preparada para diseñar, construir y operar las tecnologías más recientes, principalmente a nivel técnico (Foro Económico Mundial, 2015, pág. 20).

_ EDUCACIÓN EN _
CIBERSEGURIDAD

Planificación del futuro mediante
el desarrollo de la fuerza laboral

Educación en ciberseguridad

En América Latina y el Caribe, la demanda de una fuerza laboral capacitada en ciberseguridad ha aumentado, especialmente en las empresas medianas ((ISC)2, 2019). Según el informe de 2019 de (ISC)2, es probable que los profesionales en ciberseguridad tengan al menos una licenciatura o un pregrado, y un poco más de un tercio, una maestría o un doctorado/posdoctorado. Mientras que la mayoría obtienen títulos en informática y ciencias de la información (40%), otros obtienen títulos ajenos a las tecnologías de la información, como ingeniería (19%) y administración (10%). Por lo que toca a la región, el informe detalla que las empresas reclutan personal directamente de las instituciones educativas y de proveedores de seguridad. La realidad es que la gran mayoría de los profesionales en ciberseguridad no se iniciaron en este ramo, sino que siguieron otra trayectoria profesional, y muchos incluso se iniciaron en campos ajenos a las tecnologías de la información. Los responsables de la formulación de políticas deben adoptar una visión nacional por lo que toca a la educación en ciberseguridad de modo que se pueda generar un flujo de profesionales en ciberseguridad, además de pensar estratégicamente sobre cómo posicionar la educación en ciberseguridad en el marco nacional de ciberseguridad.

El pilar de la educación

Se han creado numerosas herramientas para ayudar a evaluar el estado de la capacidad en ciberseguridad de un país. Dos ejemplos son el Modelo de Madurez de Capacidades de Ciberseguridad para las Naciones (Cybersecurity Capacity Maturity Model for Nations, CMM) y el Índice Mundial de Ciberseguridad (IMC). Estas herramientas enfatizan la importancia de la educación en las capacidades en ciberseguridad de una nación y consideran la educación en ciberseguridad como un pilar clave de cualquier estrategia nacional.

El CMM, creado por el Global Cyber Security Capacity Centre (GCSCC)[1], es un estándar que evalúa el estado nacional de las capacidades en ciberseguridad en un país. Contiene una sección dedicada a la educación, la capacitación y las habilidades en ciberseguridad que señalan a la educación en ciberseguridad como un pilar clave que debe ser considerado por los responsables de la formulación de políticas al evaluar la capacidad en ciberseguridad a través de la capacidad, la calidad y la aceptación de las ofertas educativas y de capacitación para varios grupos, incluidos los representantes gubernamentales, el sector privado y la población en su conjunto (Cybersecurity Capacity Portal, 2020). Esta sección se divide en tres componentes principales: (1) sensibilización de los ciudadanos, (2) marco para la educación y (3) marco para la formación profesional. Mientras que el primero se centra en la existencia de campañas de concienciación para un público general, el segundo se

1. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0

refiere a programas acreditados a nivel universitario, iniciativas de investigación y desarrollo y un plan de estudios nacional en ciberseguridad. El tercer componente destaca la importancia de las certificaciones y los programas de capacitación en ciberseguridad como apoyo al desarrollo de habilidades con el paso del tiempo.

Asimismo, en el informe correspondiente a 2018 del IMC, creado por la Unión Internacional de Telecomunicaciones (UIT)[2], se destaca la importancia de combinar diferentes enfoques, técnicas y herramientas para cerrar la brecha educativa en ciberseguridad. Al igual que el CMM, el IMC tiene indicadores similares en el pilar "Creación de capacidad", que incluye campañas de concientización pública, el marco para la certificación y acreditación de los profesionales de la ciberseguridad; cursos de formación profesional en ciberseguridad, programas educativos o planes de estudio en ciberseguridad; inversión en programas de investigación y desarrollo en ciberseguridad y mecanismos de incentivos e industria local de ciberseguridad (UIT, 2019, pág. 8). Ambos modelos también destacan la importancia de los programas educativos, que pueden influir en el cambio social y el crecimiento económico.

Estos modelos e índices de madurez de la ciberseguridad demuestran que la educación también debe ocupar un lugar destacado en la estrategia nacional de ciberseguridad de un país. En América Latina, los Gobiernos de Argentina, Brasil, Chile, Colombia, Costa Rica, Guatemala, México, Panamá, Paraguay y República Dominicana han publicado o actualizado sus estrategias nacionales de ciberseguridad. Estas estrategias abarcan un marco de creación de capacidades y líneas de acción para fortalecer la educación en ciberseguridad a nivel nacional. Por ejemplo, los dos primeros objetivos de la estrategia nacional de Argentina se centran en la concienciación y la educación en ciberseguridad[3]. Cuatro de los siete objetivos de la Política Nacional de Seguridad de la Información de Brasil se relacionan con la investigación y desarrollo, la creación de capacidades de la fuerza laboral, el desarrollo de habilidades y una cultura de seguridad de la información[4]. Asimismo, los marcos nacionales de ciberseguridad de Chile[5] y Colombia[6] abarcan la educación como una característica clave para mejorar la madurez de la ciberseguridad y también identifican acciones específicas a realizar, establecen un cronograma y determinan los responsables de esas acciones. Los planes de acción de educación en ciberseguridad pueden fortalecer y orientar las políticas de ciberseguridad para manejar las deficiencias en las fuerzas laborales y sistemas educativos de cada país.

Al momento de dar los últimos toques a este documento, la COVID-19 se había convertido en una pandemia y cambió la educación en todo el mundo. Los ministerios y departamentos de educación federales, estatales y provinciales se movilizaron rápidamente para migrar su contenido educativo a la nube a fin de garantizar que millones de estudiantes y docentes tuvieran acceso ininterrumpido a la enseñanza a distancia. Las universidades públicas y privadas, las escuelas técnicas y las escuelas de primaria y secundaria hicieron lo mismo. El aprendizaje a distancia se generalizó cada vez más y, con ello, la necesidad de hacer frente a los problemas de ciberseguridad en la conectividad para permitir el aprendizaje. Los ejercicios de formación en línea y los mecanismos de apoyo a docentes y estudiantes en educación en ciberseguridad son ahora una prioridad mayor en la adaptación a la enseñanza virtual.

---

2. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

3. Argentina (2019). Estrategia Nacional de Ciberseguridad. Disponible en: http://www.enre.gov.ar/web/bibliotd.nsf/203df3042bad9c40032578f6004ed613/1e2bd1ba24f72e9b03258408003abee3/$FILE/anexo%201.pdf.

4. Brasil (2018). Política Nacional de Segurança da Informação. Disponible en:

http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Decreto/D9637.htm.

Elaboración de un plan de acción para la educación en ciberseguridad

El plan de acción para la educación en ciberseguridad, que aquí se propone, ha de servir de modelo para que la formulación de políticas públicas eficaces encaminadas a fortalecer las estrategias nacionales de ciberseguridad y desarrollar la fuerza laboral en ciberseguridad.

El siguiente diagrama muestra cómo se integra un plan de acción para la educación en ciberseguridad con los objetivos generales de la estrategia nacional de ciberseguridad como una línea de acción específica para abordar el pilar educativo.

Estrategia nacional de ciberseguridad

Plan de acción para la educación en ciberseguridad

El desarrollo de un plan de acción para la educación en ciberseguridad debe considerar:

1. Establecimiento de metas
2. Integración de las partes interesadas al plan
3. Establecimiento de objetivos y parámetros
4. Creación de un esquema de implementación.
5. Identificación de los recursos necesarios para la implementación del plan

La Iniciativa Nacional para la Educación en Ciberseguridad (National Initiative for Cybersecurity Education, NICE)[5], dirigida por el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST) en los Estados Unidos, es un ejemplo de una iniciativa que los responsables de la formulación de políticas pueden emular para desarrollar un plan de acción para la educación en ciberseguridad. La iniciativa NICE funciona como una alianza entre el Gobierno, el sector privado y la sociedad civil para afrontar la escasez de fuerza laboral, mediante la mejora de la capacidad del país para encarar los desafíos actuales y futuros en materia de ciberseguridad. Teniendo en cuenta la naturaleza multidisciplinaria de la ciberseguridad y las recomendaciones clave recibidas de los sectores académico, privado y gubernamental, la iniciativa NICE define claramente los roles y funciones de las partes interesadas en la mejora de las capacidades de seguridad cibernética en los Estados Unidos (NIST, 2017, págs. 1-2). Desde agosto de 2020, el NIST está realizando una consulta pública para actualizar la iniciativa NICE y prevé lanzar una nueva versión en noviembre de 2020[6].

A través de esta iniciativa, el NIST ofrece a los responsables de la formulación de políticas ejemplos sobre la importancia de adaptar las actividades de ciberseguridad a cada etapa del ciclo de desarrollo de la fuerza laboral. Los países pueden utilizar esta iniciativa como una guía para que las empresas desarrollen programas educativos y de capacitación en ciberseguridad adaptados a su propio entorno. La iniciativa NICE es la única en el mundo que busca estandarizar los roles requeridos en la fuerza laboral de ciberseguridad, abarcando roles técnicos y no técnicos. Países como Australia, Singapur y Japón han utilizado la iniciativa NICE como base para la creación de sus propios programas y lo han difundido en sus sectores público, privado y académico. En la actualidad, ningún país de América Latina y el Caribe ha adoptado formalmente esta iniciativa.

Las siguientes secciones describen los cinco pasos críticos para la creación de un plan de acción para la educación en ciberseguridad, teniendo como modelo la iniciativa NICE. La primera sección, ***Establecimiento de metas***, describe las metas específicas que definirán los resultados a largo plazo del plan de acción. La segunda sección, I***ntegración de las partes interesadas al plan de acción para la educación en ciberseguridad***, presenta la importancia de identificar adecuadamente a los actores que participarán en el diseño e implementación del plan de acción. La tercera sección, ***Establecimiento de objetivos y parámetros***, se refiere a la importancia de seleccionar objetivos mensurables y aplicables al contexto en el que se implementará el plan de acción. La cuarta sección, ***Implementación de un plan de educación en ciberseguridad***, identifica acciones detalladas que se pueden incorporar en cada etapa de la educación y del ciclo de desarrollo de la fuerza laboral. Por último, la sección ***Recomendaciones pragmáticas*** incluye una lista completa de recomendaciones para hacer realidad el plan de educación en ciberseguridad.

5. Véanse los detalles en el anexo

6. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-draft-revision

Establecimiento de metas

En las etapas iniciales del diseño de un plan de acción para la educación en ciberseguridad, los responsables de la formulación de políticas deben seleccionar un número limitado de metas y considerar el contexto social y económico del país y así estructurar un plan de acción exitoso. Al seleccionar unos cuantos objetivos relevantes y alcanzables, podrán definir mejor ese plan de acción.

Para ser eficaz, un plan de acción para la educación en ciberseguridad debe centrarse en: (a) abordar la escasez de educación y habilidades en ciberseguridad, y (b) crear conciencia sobre las brechas en la ciberseguridad y sobre la importancia de este campo. Por ejemplo, la iniciativa NICE describe tres metas para abordar la escasez de la oferta educativa y habilidades en ciberseguridad. No son excluyentes, pero si lo suficientemente amplias y detalladas, y pueden ser de utilidad a la hora de adaptar las metas específicas que se pretende lograr.

1. Acelerar el aprendizaje y el desarrollo de habilidades: describe la importancia de crear conciencia sobre la necesidad de la educación en ciberseguridad entre los actores públicos y privados. Específicamente, recomienda la participación de trabajadores desplazados que podrían estar disponibles para desempeñar roles de ciberseguridad, así como experimentar con el uso de programas cooperativos de educación donde las personas puedan convertirse en parte de la fuerza laboral y devengar un salario mientras aprenden las habilidades necesarias.

2. Fomentar una comunidad de aprendizaje diversa: busca garantizar que la educación en ciberseguridad enfatice el aprendizaje continuo, siga siendo mensurable e incorpore la diversidad. Para promover la diversidad, la iniciativa NICE recomienda instar a los miembros de minorías insuficientemente representadas a que aprovechen las oportunidades de aprendizaje sobre ciberseguridad. Esta meta también alienta a los sectores público y privado a inspirar la conciencia de la carrera en seguridad cibernética, comenzando en el nivel de la escuela primaria, para facilitar el desarrollo de itinerarios académicos.

3. Orientar el desarrollo profesional y la planificación de la fuerza laboral: especifica la necesidad de apoyar a los empleadores en la contratación, retención y desarrollo continuo de su fuerza laboral. Aboga por medidas tales como auxiliar a los profesionales de recursos humanos a desarrollar herramientas para ayudar a los gerentes y analizar las fuentes de datos para lograr un reclutamiento específico.

Los encargados de la formulación de políticas deben tomar en cuenta las opiniones de aquellos involucrados directa e indirectamente en la creación e implementación de un plan de acción para la educación en ciberseguridad. Al involucrar a las partes interesadas en este proceso, los responsables de la formulación de políticas pueden reforzar la eficacia de la estrategia y lograr las metas establecidas. La siguiente sección ofrece una descripción general sobre cómo identificar e involucrar mejor a las partes interesadas.

Integración de las partes interesadas al plan de acción para la educación en ciberseguridad

La colaboración de múltiples partes interesadas durante la formulación e implementación de un plan de acción para la educación en ciberseguridad es esencial. Durante la fase de formulación, la alianza entre el Gobierno, el sector privado y la sociedad civil ayuda a evaluar las necesidades actuales de la fuerza laboral e identificar iniciativas relevantes que ya están en marcha en la educación primaria y postsecundaria.

Los Gobiernos de América Latina y el Caribe podrían comenzar identificando a las partes interesadas clave de la industria, el sector académico y la sociedad civil e invitarlos a participar en el proceso de formulación del plan de acción para la educación en ciberseguridad. Con este fin, es vital comunicarles claramente lo siguiente a las partes interesadas: (1) las metas y el alcance del plan de acción para la educación en ciberseguridad; (2) el cronograma, los objetivos intermedios y los resultados concretos del proceso de formulación, y (3) los mecanismos para la toma de decisiones durante el proceso de formulación (por ejemplo, cómo se aprobará el plan de acción y cómo se considerarán, analizarán y, en última instancia, incorporarán en él los comentarios y aportes de las diferentes partes interesadas). Los responsables de la formulación de políticas podrían involucrar a las partes interesadas mediante la creación de comités, la organización de talleres y la realización de consultas públicas, entre otros mecanismos. Los países que desarrollaron sus estrategias nacionales de ciberseguridad mediante procesos en los que participaron múltiples partes interesadas también podrían aplicar esa experiencia a la formulación de su plan de acción para la educación en ciberseguridad[7].

Además, para implementar un plan de acción nacional de educación en ciberseguridad, los responsables de la formulación de políticas deberían considerar la creación de un comité o comisión integrado por entidades gubernamentales para coordinar la implementación de políticas educativas, así como mesas de trabajo abiertas a contribuciones y recomendaciones de varios sectores. El caso de la iniciativa NICE ofrece un buen ejemplo de mecanismos de coordinación, como es el caso de su Consejo de Coordinación Interagencial y el grupo de trabajo. El primero reúne a las entidades gubernamentales que lideran la implementación del plan de acción y el segundo tiene como objetivo reunir a representantes de diferentes sectores. Ambas estructuras deben tenerse en cuenta a la hora de implementar un plan de acción nacional para la educación en ciberseguridad. Cabe destacar que muchos países de América Latina y el Caribe han desarrollado un modelo similar para la implementación de sus estrategias nacionales de ciberseguridad[8], y han optado por la creación de comités o comisiones integradas por entidades gubernamentales, así como grupos de trabajo que invitan a representantes de otros sectores a participar voluntariamente. Este modelo de gobernanza podría replicarse para respaldar cualquier plan de acción nacional para la educación en ciberseguridad.

7. Los documentos que describen cómo se podría emplear la modalidad de múltiples partes interesadas en el desarrollo de estrategias nacionales de ciberseguridad son un buen comienzo a la hora de formular un marco nacional de educación en ciberseguridad. (Véanse los informes de Global Partners Digital, como por ejemplo, "Framework for Multistakeholder Cyber Policy Development" y "Multistakeholder Approaches to National Cybersecurity Strategy Development".)

8. Por ejemplo, Chile ha creado el Comité Interministerial de Ciberseguridad, integrado por varias entidades gubernamentales. El Comité puede invitar a representantes de instituciones académicas, la sociedad civil y el sector privado a participar en sus reuniones. Asimismo, Paraguay ha creado una Comisión Nacional de Ciberseguridad con miembros gubernamentales. Y se pueden crear grupos con múltiples partes interesadas para definir temas específicos.

Sector privado

El sector privado es un actor y aliado decisivo en la implementación de un plan de acción nacional para la educación en ciberseguridad. Al tener un papel de liderazgo en el impulso al desarrollo tecnológico, el sector privado es consciente de las necesidades de la industria y también puede proporcionar herramientas para capacitar a la fuerza laboral, así como recursos para mejorar la distribución de la oferta educativa.

Además de las estructuras de gobernanza, las alianzas público-privadas-académicas también juegan un papel importante en un plan de acción para la educación en ciberseguridad. Las instituciones educativas públicas y privadas pueden aprovechar la experiencia del sector privado, incluidas las empresas de tecnología, para mejorar el contenido, la eficacia y garantizar la sostenibilidad general de la educación en ciberseguridad. Facilitar estas alianzas puede permitir el acceso de un mayor número de estudiantes a recursos y oportunidades.

Por ejemplo, la iniciativa Educate Cloud Degree de Amazon Web Services (AWS) ayuda a "bajar de la nuble" los planes de estudio existentes de las instituciones participantes, y otorga títulos y certificados con una especialización o concentración en computación en la nube. En Brasil y Colombia, tanto el Servicio Nacional de Capacitación Industrial (SENAI)[9] como el Servicio Nacional de Aprendizaje (SENA)[10] se han asociado con AWS para brindar capacitación a estudiantes en inteligencia artificial, Internet de las cosas y computación en la nube, que incluye herramientas y módulos sobre ciberseguridad. Gracias a esta alianza, SENAI y SENA han brindado capacitación a 3 000 y 10 000 estudiantes en 2019, respectivamente. Asimismo, el Gobierno de Argentina también se asoció con AWS, y les ha ofrecido a sus ciudadanos el programa AWS Educate a través del portal del Ministerio de Modernización, además de un plan de estudios de computación en la nube, con módulos de ciberseguridad, a 28 instituciones educativas del país[11].

De igual forma, CISCO y Trend Micro brindan recursos para ayudar a estudiantes e instituciones de nivel postsecundario. La CISCO Networking Academy, por ejemplo, ofrece aprendizaje en línea y presencial sobre muchos temas tecnológicos, incluida la ciberseguridad, que también está disponible en portugués y español[12]. Trend Micro, a través del programa Cybersecurity Education for Universities[13], ofrece capacitación para profesores universitarios, brinda asistencia para reforzar el plan de estudios de ciberseguridad y ofrece seminarios técnicos y seminarios web a estudiantes y profesores.

9. https://noticias.portaldaindustria.com.br/noticias/educacao/senai-e-amazon-web-services-se-unem-para-incentivar-a-educacao-no-brasil/

10. https://aws.amazon.com/blogs/publicsector/president-of-colombia-joins-aws-in-bogota-talks-innovation-across-the-region/

14. https://aws.amazon.com/es/blogs/aws-spanish/aws-announces-amazon-cloudfront-edge-location-in-argentina/

12. https://www.netacad.com/

13. https://www.trendmicro.com/en_us/initiative-education/cybersecurity-education-universities.html

Instituciones educativas

Instituciones educativas, tales como de universidades, centros de investigación y otras instituciones académicas, suelen albergar a múltiples expertos que, a través de su labor en investigación, continúan promoviendo el campo de la ciberseguridad. La integración de los académicos en alianzas público-privadas-académicas puede ayudar a lograr una visión objetiva, científica y equilibrada en la formulación de políticas. Las instituciones educativas suelen ser fuente de innovación y avance en tecnología.

La Universidad de Oxford, a través del Global Cyber Security Capacity Centre (GCSCC), se ha convertido en un centro de investigación internacional líder en temas de ciberseguridad dedicado a promover el alcance, el ritmo, la calidad y el impacto de la ciberseguridad. La universidad y el GCSCC han unido fuerzas con organizaciones tales como la OEA y el Banco Interamericano de Desarrollo para brindar modelos para una evaluación objetiva sobre el estado de la ciberseguridad en la región. La primera de estas alianzas tuvo lugar en 2016 con la publicación Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? (2016)[14]. Esta publicación ha permitido que los responsables de la formulación de políticas y las partes interesadas del sector privado puedan identificar el avance que ha logrado cada país en materia de ciberseguridad, además de destacar áreas clave de participación y apoyo necesarios para alcanzar un mayor nivel de madurez.

La integración del sector académico debería ser un incentivo para que los responsables de la formulación de políticas aprovechen la asesoría y datos disponibles para delinear políticas efectivas que puedan asegurar la inclusión de los principios de ciberseguridad en la educación. Más importante aún es que estas son entidades primordiales que deben recibir apoyo financiero para continuar con su trabajo en innovación y promoción de la labor en ciberseguridad y educación.

Sociedad civil

La sociedad civil y muchas asociaciones de seguridad de la información (por ejemplo, (ISC)^2, CompTIA, ISACA y SANS) han desarrollado programas de educación en ciberseguridad que podrían ayudar a los Gobiernos a aprovechar las habilidades de ciberseguridad en diferentes instituciones y regiones del país. Además, en proyectos orientados a mejorar la educación y la empleabilidad de los jóvenes, las alianzas público-privadas tienden a ser neutrales y tener una duración definida y, a menudo, involucran a la sociedad civil (BID, 2018, pág. 4). Las organizaciones sin fines de lucro ayudan a los Gobiernos y actores del sector privado en el monitoreo y la rendición de cuentas de estos proyectos y aseguran que se cumplan los objetivos. Además, las organizaciones no gubernamentales, las comunidades y las instituciones académicas también encajan necesariamente en esta ecuación, al aportar sus propias ventajas comparativas, su voz y su posicionamiento (WEF, 2014, pág. 11). Además, en América Latina es más probable que las organizaciones contraten profesionales en ciberseguridad de instituciones académicas ((ISC)^2, 2019, pág. 27), lo que acentúa la importancia de las alianzas público-privadas-sociedad civil para mejorar las habilidades y el conocimiento de los profesionales de la ciberseguridad de la región.

Todas las partes interesadas deben apoyar el desarrollo de una fuerza laboral cualificada en ciberseguridad, ya que esos diferentes actores desempeñan roles únicos en diferentes instancias del ciclo educativo. Las siguientes secciones presentan algunos ejemplos en los que el sector público, el sector privado y la sociedad civil pueden participar en lograr la concienciación acerca de la ciberseguridad y de la preparación de la fuerza laboral que se necesita para ir cerrando la brecha.

14. https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Establecimiento de objetivos y parámetros

Objetivos mensurables y parámetros apropiados para evaluar continuamente el avance y hacer recomendaciones para su mejora resultan ser de gran ayuda en el diseño de un plan de acción para la educación en ciberseguridad efectivo y específico. Sin embargo, para que funcionen correctamente, los objetivos deben ser específicos, mensurables, precisos, confiables y oportunos.

Los Gobiernos también podrían considerar el uso de indicadores de insumos (es decir, relacionados con los recursos requeridos, como la formación de docentes y la pedagogía en el aula), indicadores de resultados (es decir, que se refieren al impacto de la actividad realizada, por ejemplo, conocimientos y habilidades de los estudiantes), indicadores educativos y socioeconómicos nacionales, como tasas de matrícula educativa, e indicadores de costos (es decir, la comparación de los resultados de una iniciativa con sus costos a través de un análisis de costo-beneficio, por ejemplo) (Wagner et al., 2005, págs. 21-30).

Los responsables de la formulación de políticas también podrían tener en cuenta la posibilidad de adaptar los indicadores de la tecnología de la información y las comunicaciones (TIC) para medir el impacto de la educación en ciberseguridad. Por ejemplo, la Asociación sobre la Medición de las TIC para el Desarrollo[15], de la Unión Internacional de Telecomunicaciones, consiste en una lista de indicadores, acordados a través de un proceso de consulta de múltiples partes interesadas, para las TIC en la educación, que podrían ajustarse y luego usarse para evaluar la implementación general de un plan de acción nacional para la educación en ciberseguridad. Algunos indicadores nacionales incluyen, por ejemplo:

- La proporción de escuelas primarias y secundarias con programas educativos en ciberseguridad
- La proporción de estudiantes de nivel postsecundaria matriculados en cursos relacionados con la ciberseguridad
- La proporción de educadores cualificados en ciberseguridad en las escuelas[16]

Los Gobiernos y otras partes interesadas deben considerar no solo depender de herramientas tradicionales (como encuestas específicas) para medir el impacto, sino también deben explorar otras fuentes de datos (OCDE, 2019, pág. 18). Por ejemplo, gracias al avance tecnológico, los responsables de la formulación de políticas pueden combinar diferentes fuentes de datos, identificar correlaciones e incluso realizar análisis predictivos.

15. https://www.itu.int/en/ITU-D/Statistics/Pages/intlcoop/partnership/default.aspx

16. Indicadores preparados a partir de la lista básica de indicadores de TIC de la Alianza para la medición de las TIC para el desarrollo, disponible en https://www.itu.int/en/ITU-D/Statistics/Pages/coreindicators/default.aspx.

Implementación de un plan de educación en ciberseguridad

Esta sección presenta información sobre los aspectos críticos que se deben tener en cuenta en la implementación de un plan de acción para la educación en ciberseguridad en cada fase del ciclo de vida del desarrollo de la fuerza laboral, así como las mejores prácticas que se han establecido en todo el mundo.

Educación primaria y secundaria: educar a la próxima generación

La iniciativa NICE es un buen ejemplo de cómo diseñar un plan de educación para los niveles de primaria a secundaria. El Plan nacional de implementación de educación en ciberseguridad para los niveles de primaria a secundaria[17] tiene como finalidad: (1) alentar a los estudiantes a participar en actividades relacionadas con la ciberseguridad; (2) ayudar a educadores a incorporar conceptos de ciberseguridad en las clases y, por último, (3) ayudar a los estudiantes de los niveles primaria y secundaria a identificar oportunidades profesionales en el campo de la ciberseguridad. Además, este plan también fomenta la participación de la comunidad en la creación de una campaña de concientización sobre la carrera en ciberseguridad, dirigida a educadores, estudiantes, padres, administradores y consejeros. Estos objetivos son un excelente ejemplo de los derroteros que pueden plantearse los Gobiernos a la hora de educar a la próxima generación de profesionales en ciberseguridad.

Para ayudar a los estudiantes en los niveles de primaria a secundaria, el National Integrated Cyber Education Research Center (NICERC)[18], en los Estados Unidos, ofrece planes de estudio gratuitos para que los educadores integren conceptos de seguridad cibernética en la formación en el aula y también brinda oportunidades de desarrollo profesional para los maestros.

Para educar a la fuerza laboral de la próxima generación, los responsables de la formulación de políticas deben considerar el diseño de un plan de acción específico con actividades para educadores y estudiantes. Para los educadores, la capacitación debe generar recursos y herramientas innovadoras que los maestros puedan incluir en sus clases para captar la atención de los estudiantes. Para los estudiantes de primaria y secundaria, es esencial considerar las inquietudes sobre seguridad, las posibles carreras profesionales y cómo aprovechar los juegos y los concursos. Los Gobiernos también deben considerar la posibilidad de asociarse con el sector privado, organizaciones sin fines de lucro y universidades para formular e implementar iniciativas educativas. Se podrían utilizar muchas herramientas para educar a los niños sobre la ciberseguridad, que van desde la adaptación de los planes de estudio —o el desarrollo de otros nuevos— hasta los concursos ofrecidos por el sector privado.

Caso de estudio

AWS se ha asociado con Code.org, una organización sin fines de lucro dedicada a ampliar el acceso a la informática en las escuelas y aumentar la participación de las mujeres y las minorías insuficientemente representadas. Esta organización cuenta con el apoyo de AWS y su visión es que todos los estudiantes de todas las escuelas tengan la oportunidad de aprender ciencias de la computación, de la misma forma que estudian biología, química o álgebra. Específicamente, AWS respalda el sitio web de Code.org todo el año y le ayuda a mejorar su capacidad de escalamiento para apoyar a millones de maestros y estudiantes en más de 180 países durante la Hour of Code, una campaña anual en la que participa el 15 % de los estudiantes de todo el mundo en actividades de introducción a la codificación, con una hora de duración. Además, Code.org

17. https://www.nist.gov/sites/default/files/documents/2017/04/26/nice_k12_implementation_plan.pdf
18. https://nicerc.org/student/

guarda celosamente millones de registros de estudiantes y los protege contra ataques cibernéticos con programas tales como AWS Infrastructure Event Management, AWS Shield Advanced, AWS WAF – Web Application Firewall y AWS GuardDuty. En los últimos tres años, miles de empleados de Amazon se han ofrecido como voluntarios en Hour of Code en salones de clase en ciudades como San Miguel (Chile) y Ciudad del Cabo (Sudáfrica). En 2019, los empleados de Amazon encabezaron 280 eventos en más de 20 países y 160 ciudades.

Nivel postsecundaria y capacitación laboral

Durante esta fase de su educación, los estudiantes suelen dar su primer paso importante hacia una carrera en ciberseguridad. En el nivel postsecundaria, la educación en ciberseguridad podría ofrecerse tanto a estudiantes que buscan trabajos técnicos como a aquellos que buscan carreras en campos no técnicos, como derecho, política pública, administración, defensa y milicia. Muchos de los profesionales de la ciberseguridad de hoy en día no tienen antecedentes en tecnologías de la información, y el 30% de ellos proviene de áreas tales como administración, mercadotecnia, finanzas, contabilidad y milicia. En América Latina, el 18% de los profesionales de la ciberseguridad comenzaron en carreras no técnicas ((ICS)2, 2017, pág. 5).

Muchos programas de ciencias de la computación e ingeniería no han sido actualizados conforme a los cambios provocados por la Cuarta Revolución Industrial, y su modernización podría ser uno de los primeros pasos en ese proceso. Asimismo, los cursos en ciberseguridad deben formar parte de los programas de ingeniería de software y ciencias de la computación a fin de garantizar que los desarrolladores incorporen la seguridad en el proceso de desarrollo.

Las respuestas educativas deben considerar la inclusión de cursos más interdisciplinarios, así como planes de estudio dinámicos y que respondan a las necesidades del entorno en que se ofrecen, a fin de mantenerse al día con los avances tecnológicos (Gleason, 2018, pág. 223). Por ejemplo, se necesitan profesionales con conocimientos tanto del sector de la salud como de la ciberseguridad. En consecuencia, algunas universidades han comenzado a ofrecer programas educativos que combinan políticas de salud y ciberseguridad[19].

Después de los programas de pregrado, los estudiantes tienen la opción de especializarse en ciberseguridad a nivel de posgrado. Existe un buen número de programas de posgrado en ciberseguridad, con grados de maestría e investigación en campos que van desde la informática hasta política y gestión. De hecho, algunos países de América Latina ofrecen estudios de posgrado en ciberseguridad, como el Instituto Tecnológico y de Estudios Superiores de Monterrey (México)[20] y la Escuela Superior de Guerra (Colombia)[21].

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) creó un catálogo de los grados relevantes en ciberseguridad en sus estados miembros, incluidos programas de pregrado y posgrado[22]. Además de ayudar a los estudiantes a tomar decisiones informadas sobre sus programas de ciberseguridad, al crear un catálogo educativo en ciberseguridad, los Gobiernos pueden tener una mejor idea de la disponibilidad de programas de educación superior en esta área.

19. Por ejemplo, la Universidad de Sydney ofrece una maestría en seguridad sanitaria. Véase: https://sydney.edu.au/courses/courses/pc/master-of-health-security.html.

20. https://maestriasydiplomados.tec.mx/posgrados/maestria-en-ciberseguridad

21. https://ciber.esdegue.edu.co/course/index.php?categoryid=6

22. https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities

Los Gobiernos pueden desempeñar un papel esencial en la promoción de la disponibilidad y la calidad de los programas de educación superior en ciberseguridad al establecer un estándar para una buena educación en ciberseguridad a nivel nacional. Por ejemplo, el National Cybersecurity Center (NCSC) certifica títulos de licenciatura y maestría en ciberseguridad en el Reino Unido[23]. Esto ayuda a los estudiantes a tomar decisiones informadas sobre su educación postsecundaria y los empleadores pueden contratar personas mejor cualificadas.

Programas de formación laboral en ciberseguridad

Los estudiantes pueden involucrarse en la seguridad cibernética después de la escuela secundaria a través de programas de formación laboral. En concreto, los programas centrados en técnicas emergentes como el aprendizaje automático y la inteligencia artificial son fundamentales para el futuro de la fuerza laboral, ya que estas tecnologías estarán presentes en casi todos los productos de software nuevos y se han convertido en una prioridad de inversión para los directores de información[24]. Según una encuesta realizada entre 800 expertos y ejecutivos de alta tecnología, para 2025 habrá una amplia integración de la tecnología de inteligencia artificial y, como tal, de roles y trabajos en inteligencia artificial en diferentes partes de las empresas. Al mismo tiempo, muchas empresas de seguridad de alta tecnología están interesadas en desarrollar programas de formación laboral que combinen ciberseguridad e inteligencia artificial[25].

Muchos programas de formación laboral en América Latina ya han comenzado a capacitar a estudiantes en ciberseguridad; tal es el caso de los programas ya mencionados anteriormente del SENAI (Brasil) y el SENA (Colombia). Del mismo modo, la National Research Foundation (Singapur), por ejemplo, creó un programa nacional de inteligencia artificial (conocido como AI Singapur), que incluye un programa de formación laboral en inteligencia artificia[26] para preparar el talento local en esta área. En Alemania[27] y Corea del Sur[28], los Gobiernos han estado aplicando un modelo de prácticas de educación dual, que combina la formación práctica a través de alianzas con empleadores, en paralelo con la educación tradicional (Deloitte, 2018b, pág. 23). Este sistema de prácticas de doble aprendizaje puede ser un gran mecanismo para facilitar la contratación por parte de empresas de tecnología que tienen alta demanda de trabajadores cualificados.

Formación continua y certificaciones

Los avances tecnológicos y el panorama cambiante de las amenazas a la ciberseguridad requieren una mejora y actualización continua. Ya no es una opción, ahora la educación continua es una necesidad para los trabajadores del siglo XXI. Los cursos de capacitación de corta duración y en línea ayudan a llenar rápidamente las lagunas en conocimientos y habilidades. En América Latina, existen algunas oportunidades de capacitación de corta duración, tanto presenciales como en línea. También hay muchas oportunidades de becas financiadas por Gobiernos, el sector privado y organizaciones internacionales como la OEA.

---

23. https://www.ncsc.gov.uk/information/ncsc-certified-degrees

24. Gartner (julio de 2017). Gartner says AI technology will be in almost every new software product by 2020. Disponible solo en inglés en: https://www.gartner.com/en/newsroom/press-releases/2017-07-18-gartner-says-ai-technologies-will-be-in-almost-every-new-software-product-by-2020.

25. American Association of Community Colleges (enero de 2019). Developing Apprenticeships for cybersecurity. Disponible solo en inglés en: http://www.ccdaily.com/2019/01/developing-apprenticeships-cybersecurity/.

26. On peut obtenir plus d'information à l'adresse internet https://www.aisingapore.org/industryinnovation/aiap/.

27. https://www.make-it-in-germany.com/en/study-training/training/vocational/system/

28. http://ncee.org/what-we-do/center-on-international-education-benchmarking/top-performing-countries/south-korea-overview/south-korea-school-to-work-transition/

Por ejemplo, el Instituto Nacional de Ciberseguridad de España (INCIBE) y la OEA organizan el Cybersecurity Summer Bootcamp cada año en León (España). Este es un programa, con una duración de dos semanas y que se imparte en español, para técnicos, profesionales del orden público e interesados en el desarrollo de estrategias nacionales de ciberseguridad[29]. La OEA otorga becas a profesionales de América Latina y el Caribe para que cubran los costos de su asistencia al Summer Bootcamp. Este programa se está convirtiendo en una iniciativa líder en ciberseguridad y en 2019 contó con la asistencia de más de 100 profesionales de América Latina gracias a las becas otorgadas por la OEA. Del mismo modo, la Florida International University ofrece un programa de certificación en liderazgo en ciberseguridad, de dos días de duración, respaldado por la OEA[30]. En 2020 el Cybersecurity Summer Bootcamp se transformó en un evento virtual en el que participaron más de 800 estudiantes de ochenta países.

Muchas empresas también brindan oportunidades de capacitación y certificación con módulos de ciberseguridad, como AWS[31], Microsoft[32] y CISCO[33]. Aunque un título de educación superior es una indicación de que se cuenta con un mayor conocimiento en ciberseguridad, es posible que los empleadores consideren que una certificación sea una mejor manera de adquirir habilidades en esta área (McAfee, 2017, pág. 4). De hecho, la formación y la certificación en ciberseguridad pueden proporcionar experiencia práctica en áreas de ciberseguridad (Catota; Morgan; Sicker, 2019). Además, las certificaciones pueden tener un impacto directo en las expectativas salariales. El salario promedio de los profesionales de la ciberseguridad con los correspondientes certificados es más alto que el promedio de los que no lo tienen. Mientras que los primeros ganan unos US$21 000 anuales, los segundos ganan un promedio de aproximadamente US$16 000 en América Latina ((ISC)², 2019, pág. 17).

La formación continua y la certificación son un mecanismo tan importante para promover la adaptabilidad de una fuerza laboral de ciberseguridad que la iniciativa NICE creó el Grupo de Trabajo de Capacitación y Certificación. Este grupo desarrolló una matriz de los puestos de trabajo existentes en ciberseguridad con certificaciones vinculadas a la iniciativa NICE[34]. Entre las certificaciones en ciberseguridad reconocidas se incluyen las siguientes:

- Certified Ethical Hacker (CEH), ofrecido por el International Council of E-Commerce Consultants (EC-Council)[35]
- Certified Information Security Manager (CISM), ofrecido por ISACA[36]
- CompTIA Security+[37]
- Certified Information Systems Security Professionals (CISSP), ofrecido por (ISC)² [38]
- Sans GIAC Security Essentials (GSEC)[39]
- NIST Cybersecurity Framework (NCSF), Foundation and Practitioner[40]
- Certified Computer Security Incident Handler (CERT), ofrecido por la Carnegie Mellon University.[41]

29. https://www.incibe.es/en/summer-bootcamp
30. https://gordoninstitute.fiu.edu/executive-education/cls/
31. https://www.aws.training/
32. https://www.microsoft.com/en-us/learning/default.aspx
33. https://www.cisco.com/c/en/us/training-events/training-certifications.html
34. https://www.nist.gov/itl/applied-cybersecurity/nice/illustrative-mapping-certifications-nice-framework
35. https://cert.eccouncil.org/application-process-eligibility.html
36. http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx
37. https://certification.comptia.org/certifications/security
38. https://www.isc2.org/Certifications/CISSP
39. https://www.giac.org/certification/security-essentials-gsec
40. https://niccs.us-cert.gov/training/search/itsm-solutions-llc/nist-cybersecurity-framework-boot-camp-foundation-practitioner
41. https://www.sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=14324

Las oportunidades continuas de capacitación y certificaciones les permiten a los profesionales mantenerse actualizados y llenar cualquier brecha de conocimiento rápidamente.

Investigación y desarrollo en ciberseguridad

La experiencia en investigación puede ayudar a los Gobiernos y a la industria en la formulación de soluciones innovadoras a la hora de enfrentar los desafíos en ciberseguridad actuales y futuros y de identificar las habilidades necesarias para optimizar los planes de capacitación. La investigación puede realizarse de diferentes formas, por ejemplo: (1) programas de doctorado enfocados en estudios de ciberseguridad, (2) centros de excelencia de investigación en ciberseguridad y (3) programas específicos de investigación y desarrollo a través de convenios entre instituciones académicas y la industria/Gobierno, entre otros.

Por ejemplo, la Oficina del Primer Ministro de Singapur lanzó el Programa Nacional de Investigación y Desarrollo en Ciberseguridad, que busca fortalecer la resiliencia y preparación de la infraestructura cibernética crítica. Entre sus iniciativas se encuentran el National Cybersecurity R&D Laboratory (NCL) y el Cybersecurity Consortium Research Grants, así como becas para estudios de posgrado. Para ilustrar la forma en que estos programas fomentan la educación en ciberseguridad, el NCL estableció recientemente una alianza con Singapore University of Technology y Design's iTrust Labs para ofrecer experimentos y servicios integrados para apoyar a las entidades gubernamentales, las instituciones académicas y la industria en sus investigaciones en tecnología de operaciones y tecnologías de la información en ciberseguridad, evaluaciones de tecnología y capacitación[42].

Otro ejemplo es el National Cybersecurity Center of Excellence (NCCoE) en los Estados Unidos. El NCCoE es parte del NIST y consiste en un centro colaborativo donde las empresas, entidades gubernamentales e instituciones académicas trabajan juntas para hacer frente a los problemas de ciberseguridad más apremiantes de las empresas. Esta alianza público-privada permite la creación de soluciones prácticas de ciberseguridad para industrias específicas, así como para desafíos tecnológicos amplios e intersectoriales[43]. El NCCoE está realizando proyectos tales como Transport Layer Security (TLS), Server Certificate Management, Mobile Device Security, Data Security Projects, entre otros[44].

Bajo el liderazgo de los Gobiernos y con una visión nacional para la investigación y desarrollo en ciberseguridad, las partes interesadas (universidades, industria, sociedad civil y Gobierno) pueden unirse para colaborar en investigaciones y herramientas para resolver las más apremiantes necesidades de ciberseguridad de los países. Se pueden crear centros de investigación y desarrollo cuando las partes interesadas de diferentes sectores unen esfuerzos.

42. https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme

43. https://www.nccoe.nist.gov/about-the-center

44. thttps://www.nccoe.nist.gov/projects

Fomento de una cultura de ciberseguridad

Hoy día, gran parte de nuestra vida personal y profesional se desarrolla en línea. Todos los ciudadanos, incluso aquellos que no siguen una carrera en el campo de la ciberseguridad, necesitan un nivel de competencia en seguridad para proteger sus datos personales y los de la entidad para la que trabajan. Según un informe McKinsey, el error humano es una de las principales causas de las filtraciones de datos en las empresas: el 50% de las filtraciones de datos entre 2012 y 2017 tenían un componente de amenaza interna (McKinsey, 2018, pág. 3). Los profesionales de todas las trayectorias profesionales pueden y deben aprender las mejores prácticas en ciberseguridad.

El ***Kit de herramientas para la campaña de concientización*** en materia de ciberseguridad de la OEA recomienda que este tipo de campañas sean simples y fáciles, y que se evite utilizar detalles técnicos[45]. Los mensajes de concientización sobre ciberseguridad deben enmarcarse de manera positiva para que la gente se anime a tomar medidas para protegerse (OEA, 2016, pág. 14). Los Gobiernos deberían considerar la posibilidad de realizar encuestas sobre la forma en que los jóvenes utilizan la tecnología y qué saben sobre seguridad y privacidad en línea. Hay una serie de herramientas que podrían aplicarse para crear conciencia sobre la seguridad cibernética, como asambleas escolares, concursos, lecciones en el aula, material informativo disponible en sitios web, campañas de redes sociales y otros.

Las alianzas entre el Gobierno, la industria y la sociedad civil también pueden contribuir a crear conciencia sobre la seguridad cibernética. La campaña ***STOP.THINK.CONNECT***[46] fue creada por la National Cybersecurity Alliance (NCSA) y el Anti-Phishing Working Group (APWG) en colaboración con empresas privadas, organizaciones sin fines de lucro y organizaciones gubernamentales. En 2014, la OEA reconoció octubre como el Mes de la Concientización sobre la Ciberseguridad y, desde entonces, lo ha celebrado todos los años. La OEA también ha alentado a sus Estados Miembros a que redoblen sus esfuerzos tendientes al diseño de políticas nacionales en materia de ciberseguridad y a que se unan a STOP.THINK.CONNECT "en el establecimiento de una unidad coordinada y unificada en todo el mundo para crear conciencia pública sobre la seguridad cibernética"[47].

En América Latina, el Gobierno de Chile lanzó una campaña nacional de concientización sobre ciberseguridad, que incluye varias recomendaciones para el público en general y los trabajadores en oficinas[48]. Asimismo, la campaña nacional de concientización sobre ciberseguridad de Colombia, EnTIConfío, brinda información y recursos a una amplia audiencia, particularmente a los niños[49]. Países como Argentina, México, Panamá y Uruguay, por nombrar algunos, han creado sus propias campañas de concientización con la finalidad de contribuir a la resiliencia de la sociedad en materia cibernética.

45. https://www.sites.oas.org/cyber/Documents/2015%20OEA%20-%20Ciberseguridad%20Kit%20de%20Herramientas%20para%20la%20Campa%C3%B1a%20de%20Concientizaci%C3%B3n%20(Espa%C3%B1ol).pdf

46. https://www.stopthinkconnect.org/

47. OAS (octubre de 2014). "OEA se une al reconocimiento de octubre como el 'mes de concienciación de la Seguridad Cibernética'". Disponible en https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-474/14.

48. https://www.concienciadigital.gob.cl/

49. https://www.enticconfio.gov.co/

Recomendaciones prácticas

Esta sección ofrece un resumen de las diferentes herramientas y programas que podrían desarrollar los responsables de la formulación de políticas y los educadores en América Latina y el Caribe para mejorar los conocimientos y habilidades de la actual fuerza laboral de la región y alcanzar las metas y objetivos de un plan para la educación en ciberseguridad.

Conferencias y debates en el aula

Clases innovadoras y dinámicas sobre ciberseguridad que fomenten la discusión de conceptos básicos e introduzcan conceptos más complejos durante el ciclo educativo ayudarán a preparar a los estudiantes para el trabajo. Los educadores podrían introducir conceptos de ciberseguridad en sus clases u organizar talleres específicos sobre algún tema. Por ejemplo, la OEA, en alianza con Citi Foundation, desarrolló el programa "Creando una trayectoria profesional en seguridad digital, Pathways2Progress" que consiste en un curso técnico en seguridad digital (con una duración de 48 horas) para estudiantes universitarios de 17 a 25 años. El INCIBE también organiza las jornadas "Espacios de ciberseguridad", que consisten en un curso técnico práctico (de tres horas de duración) para grupos de entre 20 y 30 alumnos, de entre 16 y 18 años. Estos son algunos ejemplos de cursos que ayudan a animar a los jóvenes a seguir una carrera en ciberseguridad.

Ferias universitarias

Deben fomentarse las ferias universitarias y las campañas informativas sobre una trayectoria profesional en ciberseguridad, ya que la mayoría de los estudiantes del nivel secundario no tienen acceso a cursos relacionados con ciberseguridad, ni conocen las oportunidades de empleo en este campo en muchos países de América Latina (Catota; Morgan; Sicker, 2019). Debe invitarse a las ferias universitarias no solo a los estudiantes, sino también a los padres, ya que éstos pueden ayudar a sus hijos a elegir una trayectoria profesional. Por ejemplo, la iniciativa NICE en los Estados Unidos organiza "NICE K-12 Cybersecurity Education Conference, que reúne a educadores, profesionales, investigadores, organizaciones sin fines de lucro y estudiantes para debatir sobre posibles estrategias para crear conciencia sobre las trayectorias profesionales en ciberseguridad.

Capacitación y laboratorios en línea

Existe una serie de programas en línea y seminarios web que ofrecen un sin número de clases en ciberseguridad para diversas audiencias y en diversos niveles. En muchos países de América Latina, las personas se conectan a Internet a través de laboratorios públicos de innovación, y estos laboratorios podrían ofrecer capacitación en línea. Los Gobiernos deberían combinar sus proyectos de acceso a las tecnologías de la información y la comunicación con la formación en línea sobre ciberseguridad.

Las plataformas como AWS Educate y CISCO Academy, mencionadas anteriormente, son buenos ejemplos de capacitación disponible en línea. Microsoft también ofrece un curso de ciberseguridad que tiene una duración de tres meses e inicia cada trimestre. Los cursos abiertos masivos en línea (mejor conocidos como MOOC) también se han convertido en una herramienta esencial para la creación de capacidades en ciberseguridad. Plataformas como Coursera, edX, Udacity y Pluralsight ofrecen muchos cursos e incluso maestrías de universidades reconocidas, disponibles en español.

En resumen, la capacitación y los laboratorios en línea son una opción interesante para los estudiantes de países donde la capacitación en ciberseguridad no está ampliamente disponible o tiene costos prohibitivos. A través de alianzas público-privadas, los Gobiernos nacionales y locales deben aprovechar la oportunidad de utilizar estas plataformas en línea para capacitar a su fuerza laboral en temas de ciberseguridad. La industria desarrolló muchas de estas plataformas en función de lo que buscan en un empleado.

Concursos/ludificación

Los concursos pueden contribuir a crear conciencia y fomentar el trabajo en equipo; además, ofrecen a los participantes la posibilidad de tratar de solucionar un incidente cibernético del mundo real en un entorno controlado, bajo la supervisión de expertos. Estas simulaciones pueden estructurarse de tal manera que se asemejen a los ataques del mundo real que enfrentan empresas o instituciones. Asimismo, son una oportunidad para que los competidores se relacionen y compartan información e incluso para fomentar la diversidad en el campo de la ciberseguridad.

En el Reino Unido, por ejemplo, el NCSC está organizando el concurso CyberFirst Girls Competition para niñas en el país. Este concurso tiene como objetivo alentar a la próxima generación de mujeres a seguir una carrera en el campo de la ciberseguridad. Asimismo, en América Latina, la OEA organiza el CyberWomen Challenge en alianza con Trend Micro, que establece equipos integrados exclusivamente por mujeres para mitigar eficazmente los ciberataques. Los juegos y pruebas en línea también son una forma interactiva de captar la atención del público en general para conocer buenas prácticas en ciberseguridad.

No son pocas las políticas que podrían promover la integración de la ciberseguridad en la educación. La implementación efectiva de políticas de educación en ciberseguridad puede dar lugar a una mayor priorización de la ciberseguridad en general. Como se ha destacado en este documento, el primer paso que deben tomar los responsables de la formulación de políticas es identificar la necesidad de integrar la ciberseguridad en la educación. Después de esto, es importante crear un plan de acción para la educación en ciberseguridad que agilice el proceso del establecimiento de metas, objetivos y parámetros. Una vez establecidos éstos, pueden optar por la integración de actores, como el sector privado, las instituciones académicas e incluso la sociedad civil a través de alianzas entre todos ellos. Estos actores liderarán diferentes actividades con el objetivo general de educar al público sobre la ciberseguridad y lograr que la población sea más consciente de la cibernética. Algunos ejemplos incluyen educar a aquellos en los niveles primario y secundario, alentar a los estudiantes a realizar estudios postsecundarios en ciberseguridad, postularse como aprendices en alguna empresa o institución, capacitarse continuamente y obtener certificaciones. También deben tenerse en cuenta las políticas a nivel micro, como conferencias en el aula, debates, ferias universitarias y laboratorios de capacitación para lograr una rápida integración.

Conclusión

Con el propósito de formular e implementar un plan de acción para la educación en ciberseguridad, los Gobiernos de América Latina y el Caribe deben coordinar sus esfuerzos con el sector privado, la sociedad civil y las instituciones académicas. La escasez de profesionales cualificados en ciberseguridad requiere una acción inmediata para capacitar a los actuales profesionales en ciberseguridad y educar a la próxima generación. Para cubrir el déficit en la fuerza laboral —que en América Latina asciende a 600 000 personas y llega a 4 millones en todo el mundo— los Gobiernos deben colaborar con el sector privado y las instituciones académicas para formular e implementar un plan de acción para la educación en ciberseguridad. Dicho plan debe guiar a los responsables de la formulación de políticas en el diseño de políticas públicas efectivas destinadas a fortalecer sus estrategias nacionales de ciberseguridad y desarrollar la fuerza laboral en esta área. Pueden también contribuir al desarrollo de una fuerza laboral en ciberseguridad más preparada y una población más consciente de la ciberseguridad. Los componentes clave de un plan de acción para la educación en ciberseguridad incluyen:

(1) metas claras y definidas para priorizar e integrar la educación en ciberseguridad en todos los niveles que orienten las acciones de los responsables de la formulación de políticas;

(2) múltiples partes interesadas; y

(3) mecanismos de seguimiento e indicadores que evalúen el avance hacia las metas que se hayan planteado.

Los responsables de la formulación de políticas tienen diversas herramientas a su disposición para implementar un plan de acción para la educación en ciberseguridad y pueden crear programas apropiados para la edad de los estudiantes y poder así fomentar la conciencia y la educación en ciberseguridad desde la escuela primaria hasta los profesionales interesados en la educación continua. Pueden organizar desde laboratorios en línea hasta concursos, juegos, ferias universitarias, conferencias y debates en el aula. Conforme crezcan los estudiantes en edad, pueden ofrecérseles pasantías en ciberseguridad, programas de posgrado, capacitación adicional y certificaciones.

La iniciativa NICE es un buen ejemplo de un plan para los niveles de primaria a secundaria. El National K-12 Cybersecurity Education Implementation Plan tiene como objetivo (1) alentar a los estudiantes a participar en actividades relacionadas con la ciberseguridad; (2) ayudar a los educadores a incorporar conceptos de ciberseguridad en las clases y, finalmente, (3) ayudar a los estudiantes de primaria y secundaria a identificar oportunidades profesionales en el campo de la ciberseguridad. La educación y el desarrollo de la fuerza laboral tienen muchas etapas; y la expansión de cualquier plan para la educación en ciberseguridad debe tener esto en cuenta. La educación desde el nivel primario hasta el postsecundario, los programas de educación continua y la investigación y desarrollo juegan un papel importante en la mejora de la fuerza laboral en ciberseguridad. Se podrían desarrollar varias herramientas para impulsar

la educación en ciberseguridad en cada etapa del ciclo de vida del desarrollo de la fuerza laboral. La creación de capacidades puede mejorarse a nivel nacional en todas las etapas de la educación y el desarrollo de la fuerza laboral al incluir componentes específicos de la educación en cibernética en cada instancia. Desde la educación de primaria a secundaria hasta la investigación y el desarrollo, todos pueden beneficiarse del fomento de habilidades en educación en cibernética tangibles y e intangibles.

Los países de América Latina podrán cosechar los beneficios de la Cuarta Revolución Industrial si invierten tanto en tecnología como en su gente. La innovación a través de nuevas oportunidades comerciales e interacciones sociales solo puede lograrse cuando la tecnología esté en manos de trabajadores cualificados. América Latina, al igual que todas las regiones del mundo, requiere una fuerza laboral que tenga el conocimiento y las habilidades para desarrollar y operar tecnologías emergentes y las que estén por venir, así como la capacidad para conservarlas.

Bibliografía

Banco Interamericano de Desarrollo (2016). La ruta hacia las Smart Cities. Migrando de una gestión tradicional a la ciudad inteligente. Disponible en: https://publications.iadb.org/publications/spanish/document/La-ruta-hacia-las-smart-cities-Migrando-de-una-gesti%C3%B3n-tradicional-a-la-ciudad-inteligente.pdf

Banco Interamericano de Desarrollo (2018). Factores de éxito y aprendizajes obtenidos de la formación de alianzas público-privadas. Disponible en:
https://publications.iadb.org/es/factores-de-exito-y-aprendizajes-obtenidos-de-la-formacion-de-alianzas-publico-privadas

Catota, F. E., Morgan, M.G. y Sicker, D. C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment, Journal of Cybersecurity, Vol. 5, No. 1. Disponible en: https://doi.org/10.1093/cybsec/tyz001.

Cybersecurity Ventures (2019). 2019 Official Annual Cybercrime Report. Disponible en:
https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Deloitte (2019). Tech Trends 2019. Disponible en:
https://www2.deloitte.com/content/dam/Deloitte/br/Documents/technology/DI_TechTrends2019.pdf

Deloitte (2018a). The jobs are here, but where are the people? Disponible en:
https://www2.deloitte.com/us/en/pages/manufacturing/articles/future-of-manufacturing-skills-gap-study.html

Deloitte (2018b). Preparing tomorrow's workforce for the Fourth Industrial Revolution. Disponible en:
https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-preparing-tomorrow-workforce-for-4IR.pdf.

ENISA (2019). Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity. Disponible en:
https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

ENISA (2015). Status of Privacy and NIS course curricula in Member States. Disponible en:
https://www.enisa.europa.eu/publications/status-of-privacy-and-nis-course-curricula-in-eu-member-states

Foro Económico Mundial (2014). Creating New Models: Innovative Public-Private Partnerships for Inclusive Development in Latin America. Disponible en:
http://www3.weforum.org/docs/GAC/2014/WEF_GAC_LatinAmerica_InnovativePublicPrivatePartnerships_Report_2014.pdf

Foro Económico Mundial (2015a). Bridging the Skills and Innovation Gap to Boost Productivity in Latin America. Disponible en:
https://www2.deloitte.com/content/dam/Deloitte/cr/Documents/finance/201501-Competitiveness_Lab_Latin_America_final.pdf

Foro Económico Mundial (2015b). Deep Shift: technology tipping points and societal impact. Disponible en:
http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

Gleason, N. W. (Ed.). (2018). Higher education in the era of the fourth industrial revolution. Singapore: Palgrave Macmillan.

Global Cyber Security Capacity Centre (2016). Cybersecurity Capacity Maturity Model for Nations (CMM) – Revised Edition. Disponible en: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf

IBM (2018). IBM X-Force Threat Intelligence Index 2018. Disponible en: https://www.ibm.com/downloads/cas/MKJOL3DG

(ISC)2 (2019). Strategies for Building and Growing Strong Cybersecurity Teams. (ISC)2 Cybersecurity Workforce Study, 2019. Disponible en: https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

(ISC)2 (2018). Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens. (ISC)2 Cybersecurity Study, 2018. Disponible en: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

(ISC)2 (2017). Global Information Security Workforce Study. Disponible en: https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

Kelly, K. (2016). The inevitable: understanding the 12 technological forces that will shape your future. New York, NY: Penguin Books.

Lewis, J. (2018). Economic Impact of Cybercrime – No Slowing Down. Disponible en: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-1940938

McAfee (2017). Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills. Disponible en: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

McKinsey & Company (2018). Insider Threat: The human element of cyberrisk. Disponible en: https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk.

National Cybersecurity Alliance (2017). Securing our Future: Cybersecurity and the Millennial Workforce. Disponible en: https://www.raytheon.com/sites/default/files/2017-12/2017_cyber_report_rev1.pdf

National Initiative for Cybersecurity Education (2017). National K-12 Cybersecurity Education Implementation Plan. Disponible en: https://www.nist.gov/sites/default/files/documents/2017/04/26/nice_k12_implementation_plan.pdf

National Institute of Standards and Technology (2017). NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Open Web Application Security Project (2016). Security by Design Principles. Disponible en: https://www.owasp.org/index.php/Security_by_Design_Principles

Organización de Cooperación y Desarrollo Económicos (2012). The Protection of Children Online: Recommendations of the OECD Council. Disponible en:

Organización de Cooperación y Desarrollo Económicos (2016). Startup América Latina 2016. Construyendo un futuro innovador. Disponible en: https://www.oecd.org/innovation/startup-america-latina-2016-9789264265141-es.htm

Organización de Cooperación y Desarrollo Económicos (2017). Perspectivas económicas de América Latina 2017. Juventud, competencias y emprendimiento. Disponible en: https://www.oecd.org/economy/perspectivas-economicas-de-america-latina-20725183.htm

Organización de Cooperación y Desarrollo Económicos (2019). Measuring Innovation in Education 2019: What has changed in the classroom? Disponible en:

Organización de los Estados Americanos (2016). Ciberseguridad. Kit de herramientas para la campaña de concientización. Disponible en: https://www.sites.oas.org/cyber/Documents/2015%20OEA%20-%20Ciberseguridad%20Kit%20de%20Herramientas%20para%20la%20Campa%C3%B1a%20de%20Concientizaci%C3%B3n%20(Espa%C3%B1ol).pdf

Ponemon Institute (2018). 2018 Cost of a Data Breach Study: Global Overview. Disponible en: https://www.ibm.com/downloads/cas/861MNWN2

Ponemon Institute (2019). Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection. Disponible en: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Schwab, K. (2016). The Fourth Industrial Revolution. New York, NY: Crown Business

Symantec (2018). Internet Security Threat Report. Disponible en: http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_

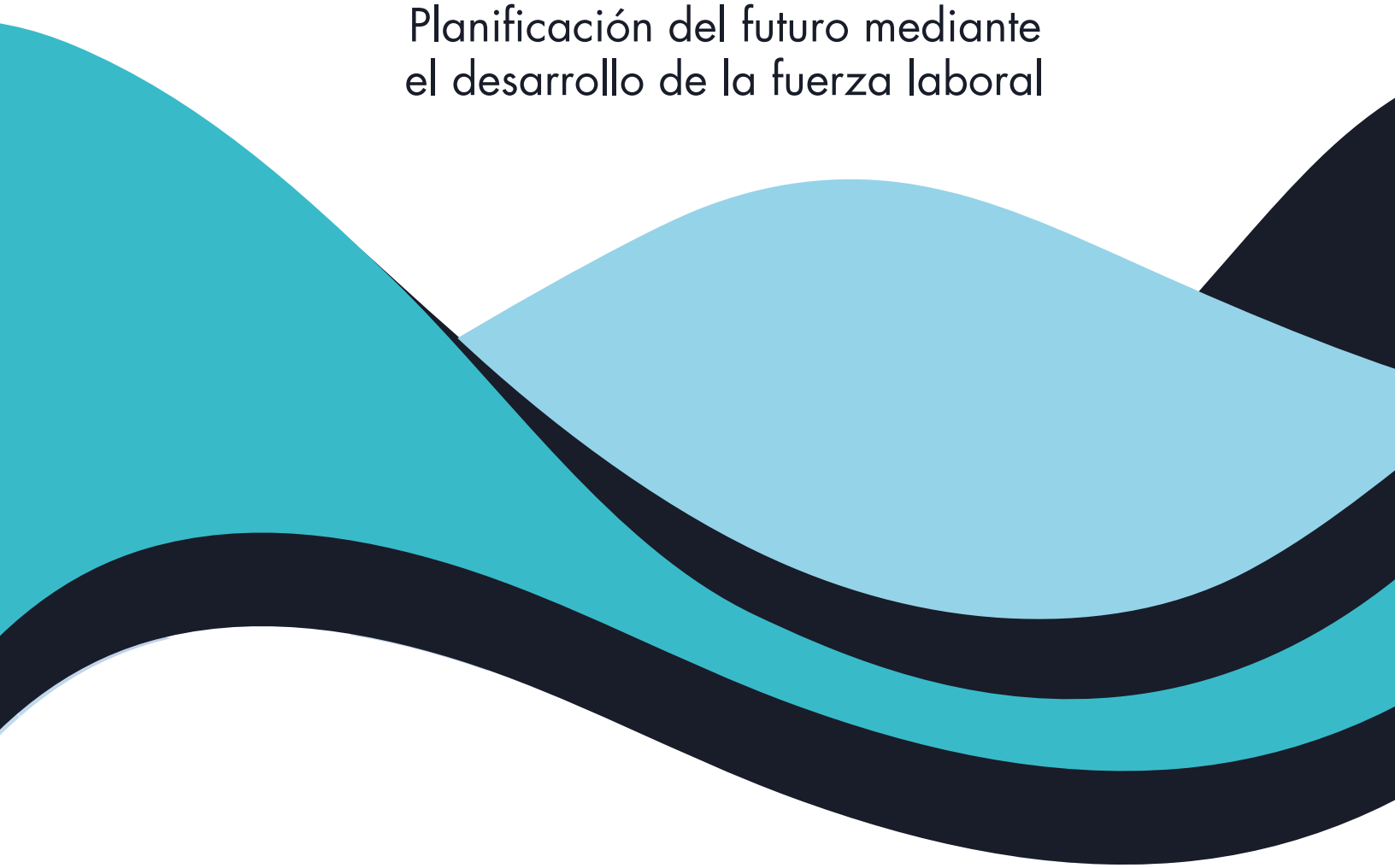
Symantec (2019). Internet Security Threat Report. Disponible en: https://img03.en25.com/Web/Symantec/%7Bdfc1cc41-2049-4a71-8bd8-12141bea65fd%7D_ISTR_24_2019_en.pdf

Unión Internacional de Telecomunicaciones (2019). Global Cybersecurity Index (GCI) 2018. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

Wagner, D. A., et al. (2005). Monitoring and evaluation of ICT in education projects: a handbook for developing countries. Washington, D. C.: InfoDev.

_ EDUCACIÓN EN _
CIBERSEGURIDAD

Planificación del futuro mediante el desarrollo de la fuerza laboral



CICTE01316E05

OEA Más derechos para más gente | aws

_ EDUCACIÓN EN _ CIBERSEGURIDAD

Planificación del futuro mediante el desarrollo de la fuerza laboral

White paper series
Edición 9

2020