Recibido: 31/1/2023 / Aceptado: 14/4/2023
doi: https://doi.org/10.26439/interfases2023.n017.6246

Cómo promueven los Estados la ciberseguridad de las pymes

Olda Bustillos Ortega
obustillos@uia.ac.cr
https://orcid.org/0000-0003-2822-3428
Escuela de Ingeniería Informática de la Universidad Internacional de las Américas, Costa Rica

Javier Rojas Segura
jrojass@uia.ac.cr
https://orcid.org/0000-0002-0488-4056
Escuela de Ingeniería Informática de la Universidad Internacional de las Américas, Costa Rica

RESUMEN

La tecnología ha producido cambios en la sociedad que han forjado la evolución de nuestra especie. Actualmente, la digitalización ha dado lugar al uso exponencial de tecnologías de la información y la comunicación, lo que ha generado un aumento en el riesgo de ciberataques que amenazan la cadena de suministros global. Los más afectados son las pequeñas y medianas empresas y su ecosistema, por la escasez de recursos para proteger la integridad, confidencialidad y disponibilidad de sus activos de información. Aumentar la concientización general en ciberseguridad eleva la inmunidad global a los ciberataques, por lo que el objetivo de este trabajo es investigar cómo los gobiernos de diversos países apoyan a la ciberseguridad de las pequeñas y medianas empresas, resaltando las mejores prácticas internacionales e identificando áreas de mejora en el desarrollo de capacidades para gobiernos, formuladores de políticas, expertos en seguridad cibernética y académicos. La ciberseguridad debe abordarse con un enfoque interdisciplinario y holístico, con aplicación multilateral, ya que las pequeñas y medianas empresas necesitan el apoyo del gobierno en la gestión del riesgo cibernético, en cooperación con la academia para construir una cultura de ciberseguridad.

PALABRAS CLAVE: ciberseguridad, pymes, gobierno, academia

HOW STATES PROMOTE CYBERSECURITY FOR SMEs

ABSTRACT

Digitalization has increased the exponential use of information and communication technologies, consequently increasing the risk of cyberattacks, which threaten the global supply chain. Small and medium-sized companies and their ecosystems are the most affected by the lack of resources to protect their information assets' integrity, confidentiality, and availability. Increasing awareness of cybersecurity helps reinforce global immunity to cyberattacks. This article investigates how some countries' governments support the cybersecurity of small and medium-sized companies, highlights the best international practices, and identifies areas for improvement in capacity building for governments, policymakers, cyber security experts, and academics. Cybersecurity must be addressed with an interdisciplinary and holistic approach, with a multilateral application, since small and medium-sized companies need government and academic support to manage cyber risk and build a culture of cybersecurity.

KEYWORDS: cybersecurity, SMEs, government, academia

1. INTRODUCCIÓN

El riesgo de ciberseguridad ha atraído una atención considerable en las últimas décadas (Xu & Hua, 2019). Según el Foro Económico Mundial (2019), el fraude de datos y los ataques cibernéticos se encuentran entre las amenazas más graves del planeta, junto al cambio climático y las tensiones geopolíticas. Durante la pandemia del COVID-19, la expansión del teletrabajo y las ventas en línea, sin la adecuada protección ante los virus informáticos o *malware*, colocaron sobre la mesa la vulnerabilidad existente (Ballestero, 2020). Desde el inicio de la crisis sanitaria, los ciberataques han aumentado (Díaz, 2021); en la actualidad, los ataques de *phishing*, ingeniería social y *ransomware* están evolucionando y cada día son más especializados, por lo que su impacto mayormente negativo abarca más usuarios en cualquier tipo de empresa (Ramírez & González, 2020). No obstante, las pequeñas y medianas empresas (pymes) son el objetivo de la gran mayoría de ataques cibernéticos (Ponsard et al., 2019).

En los primeros ocho meses del año 2021, en la región de América Latina hubo 728 millones de intentos de infección, lo cual representa un promedio de 35 ataques cibernéticos por segundo y un aumento de 24 % en relación con el mismo período del año anterior (Deutsche Welle, 2021). Díaz (2022) estima que, de los ataques que resultan efectivos y causan daños mayores, el 40 % recae en las pymes, y el daño es de tal magnitud que en muchos casos no se recuperan. Concurren diversos factores que amenazan la seguridad de información de las pymes y, por lo general, el presupuesto destinado a proteger y resguardar la información de las redes de internet externas no es el adecuado (Inoguchi & Macha, 2017). La inversión en ciberseguridad pasa a un segundo plano por no ser parte de la misión de las empresas; la necesidad solo se hace presente al momento de ser víctimas de ataques cibernéticos, lo que genera respuestas reactivas y no proactivas (Florez Martinez & Rentería Mosquera, 2020). La ciberseguridad es percibida por las pymes como excesivamente compleja y onerosa, por lo que se requieren soluciones económicas, efectivas y accesibles (Bustillos Ortega & Rojas Segura, 2022).

La Agencia de la Unión Europea para la Ciberseguridad (2021) señala que las pymes son la columna vertebral de la economía, representan el 99 % de todas las empresas de la Unión Europea (UE) y emplean a unos 100 millones de personas. También producen más de la mitad del producto interno bruto (PIB) de Europa y desempeñan un papel clave en la creación de valor en todos los sectores de la economía. Por ello, la falta de capacidad de respuesta ante un ataque cibernético por parte de la gerencia de las pymes es un problema (Orellana, 2020) no solo para ellas mismas, sino también para toda la cadena de suministros.

Tal como revela el Gobierno de Japón (2021), las pymes se enfrentan a una carencia particularmente grave de talento en ciberseguridad, por lo que los gobiernos deben ser responsables de proporcionar conocimientos y redes que sean útiles para aplicar

prácticas a través de iniciativas de ayuda mutua, mediante la construcción de un ecosistema y la promoción de la colaboración entre la industria y las instituciones educativas. La seguridad debe abordarse holísticamente, no solo desde el punto de vista de la tecnología en sí, sino de todo el conjunto que hace posible su funcionamiento (Díaz, 2022).

El objetivo de este artículo es investigar cómo los gobiernos de diversos países apoyan a las pymes para asegurar la integridad, confidencialidad y disponibilidad de sus activos de información. Esto nos lleva a preguntarnos si para promover la ciberseguridad de las pymes es necesaria la cooperación entre la academia y el gobierno.

Este estudio es una herramienta útil para resaltar las mejores prácticas internacionales e identificar áreas de mejora en el desarrollo de capacidades para gobiernos, formuladores de políticas, expertos en seguridad cibernética y académicos, en cuanto al fortalecimiento de la ciberseguridad de las pymes.

2. REVISIÓN DE LITERATURA

La seguridad de la información se ha convertido en una tendencia global debido a la significativa y relevante importancia que tiene la información para toda empresa y al incremento de amenazas en los últimos tiempos (Morales et al., 2020). La seguridad cibernética contribuye al bienestar digital de la sociedad, de las organizaciones y de los países, pues impide que cualquiera acceda a datos privados tanto personales como organizacionales (Peralta Zuñiga & Aguilar Valarezo, 2021). Por lo anterior, es clave la cooperación internacional en la lucha global contra el flagelo de los delitos cibernéticos, dado el carácter transfronterizo que este puede llegar a tener (Estévez, 2020).

2.1 Convenio de Budapest

El Convenio sobre la Ciberdelincuencia, o Convenio de Budapest, como se le conoce, fue creado en el 2001 por el Consejo de Europa (COE, por sus siglas en inglés), con la participación activa de los gobiernos involucrados, para combatir los delitos informáticos (Díaz, 2022). Es un tratado internacional pionero, instituido con el fin de resguardar a la sociedad frente a los delitos informáticos y los delitos en internet.

Este tratado incluye la creación de la legislación adecuada, el perfeccionamiento de técnicas de investigación y el incremento de la cooperación internacional para la protección de la información. Este convenio es referente, en principio, de la UE, pero se ha extendido a varios países para la emanación de legislación moderna y efectiva en la protección contra el delito cibernético (Díaz, 2021). Se convirtió en el único instrumento internacional vinculante, siendo el referente para que los Estados desarrollen leyes nacionales contra el crimen cibernético, pues estableció que aquellos que no son miembros del COE y que no hubiesen sido parte de la elaboración del tratado pudiesen

incorporarse por invitación. Actualmente, son más de sesenta países a nivel mundial los que se han incorporado al tratado (Estévez, 2020). En Latinoamérica, además de Costa Rica, que fue el país 56 en adherirse a este convenio (Paris, 2017), también forman parte Panamá, República Dominicana, Colombia, Perú, Chile, Argentina y Paraguay. Esto magnifica a una perspectiva global el horizonte de colaboración, dada la aceptación de la normativa de la UE y la observación implícita de otras normas mundiales a partir de la interrelación de la UE con otras regiones del planeta (Díaz, 2022).

2.2 Programa Mundial sobre Ciberdelincuencia

Este programa de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) fomenta la creación de capacidad sostenible a largo plazo en la lucha contra el ciberdelito, para lo cual apoya a los sistemas de justicia penal de los Estados miembros y brinda asistencia técnica en la generación de capacidades para la prevención. Además, promueve la concientización, así como la cooperación internacional y la recopilación de datos, la investigación y el estudio de los delitos cibernéticos. En el 2015, lanzó el repositorio de delitos cibernéticos, una base de datos central de legislación, jurisprudencia y lecciones aprendidas sobre delitos cibernéticos y pruebas electrónicas. El repositorio de delitos informáticos tiene como objetivo ayudar a los países en sus esfuerzos por prevenir y enjuiciar eficazmente a los delincuentes cibernéticos (Díaz, 2022).

2.3 Programa de Seguridad Cibernética

Este programa es impulsado por el Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos (OEA). Su función es proveer iniciativas de investigación, fortalecimiento de la capacidad técnica y desarrollo de políticas de seguridad cibernética en el continente americano. Esta acción se enfocó en tres pilares: desarrollo de políticas, desarrollo de capacidades (incluyendo capacitación y ejercicios cibernéticos), así como investigación y divulgación. Beneficia a todos los Estados miembros de la OEA.

2.4 Otros organismos internacionales

En el año 2008, la Organización del Tratado del Atlántico Norte (OTAN) creó el Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE, por sus siglas en inglés), un centro de investigación y capacitación que se encarga de la educación, la consulta, las lecciones aprendidas, la investigación y el desarrollo de la defensa del ciberespacio (Díaz, 2022). Además, según su página web (https://ccdcoe.org/), combina el conocimiento de la industria y la academia de los países miembros y aliados para realizar investigación científica y tecnológica en nuevas tecnologías, como 5G. Organiza la Conferencia Internacional sobre Conflictos Cibernéticos, llamada CyCon 2023, buscando desarrollar investigación

científica sobre el conflicto cibernético y las tecnologías asociadas en general, así como su papel en tiempos de paz, en la crisis y el conflicto.

Otro ente regional importante es la Agencia de la Unión Europea para la Ciberseguridad (ENISA), un ente especializado en el conocimiento para la seguridad del ciberespacio europeo (Díaz, 2022). Esta agencia, en respuesta a la pandemia del COVID-19, analizó la capacidad de las pymes dentro de la UE para hacer frente a los desafíos de ciberseguridad planteados por la crisis sanitaria y determinar las buenas prácticas para abordar esos desafíos. En este informe, ENISA (2021) proporciona consejos sobre ciberseguridad, pero también propuestas de acciones que los Estados miembros deberían considerar para ayudar a las pymes a mejorar su postura en materia de ciberseguridad.

2.5 Ciberseguridad de las pymes

En una investigación realizada por el WEF (2022) entre líderes cibernéticos de 20 países, el 88 % de los encuestados indicaron estar preocupados por la resiliencia cibernética de las pymes en su ecosistema, considerándolas como una amenaza clave para la cadena de suministros global. En línea con esta preocupación, el Gobierno de Japón (2021), en su estrategia de ciberseguridad, planteó una cooperación en un consorcio liderado por la industria, establecido con el objetivo de mejorar la ciberseguridad de la cadena de suministros completa, incluidas las pymes.

Garnacho (2018) en su investigación halló evidencia de que las pymes españolas ven la seguridad cibernética como un gasto antes que una inversión. Un sinnúmero de pymes cree que invertir en ciberseguridad es un gasto innecesario (Zuña Macancela et al., 2019). Estas empresas no hacen un adecuado balance del costo-beneficio, lo que incrementa la confianza de los ciberdelincuentes para efectuar sus ataques (Peralta Zuñiga & Aguilar Valarezo, 2021).

El intercambio de información sobre ciberdelincuencia es fundamental para que las pymes entiendan mejor los riesgos a los que se enfrentan (ENISA, 2021). Un incidente de seguridad cibernética puede tener impactos devastadores en una pequeña empresa (Gobierno Australiano & Centro Australiano de Seguridad Cibernética, 2021). Para el Gobierno de Japón (2021), las pymes afrontan un déficit particularmente grave de talento humano en seguridad, por lo que el gobierno y la academia deben proporcionar conocimientos y redes que sean útiles para aplicar prácticas a través de iniciativas de ayuda mutua.

La columna vertebral de la economía de la UE son las pymes, pues representan el 99 % del parque empresarial y emplean a unos 100 millones de colaboradores; además, aportan más de la mitad del PIB de la UE y cumplen un papel clave en la creación de valor en todos los sectores de la economía europea (ENISA, 2021).

3. METODOLOGÍA

La Unión Internacional de Telecomunicaciones (ITU, 2022) sostiene que los países deben abordar sus fortalezas y debilidades en ciberseguridad, aprovechando sus ventajas competitivas para promover su capacidad cibernética. El Índice de Ciberseguridad Global (GCI) puede apoyar a los países en iniciar este proceso. Sin embargo, para progresar, los países deben considerar mejorar la capacidad de ciberseguridad de las pymes y fomentar la participación regular de todas las partes interesadas relevantes en ciberseguridad, incluida la academia, el sector privado y la sociedad civil. Por eso, mediante un enfoque cualitativo con alcance exploratorio, se propone investigar cómo los gobiernos de diversos países apoyan a las pymes para asegurar la integridad, confidencialidad y disponibilidad de sus activos de información, de acuerdo con las siguientes etapas:

3.1 Investigación

En esta etapa, se procedió a investigar y recopilar las propuestas y planes concretos de apoyo de diversos gobiernos a la seguridad cibernética de las pymes, consultando bases de datos como Google Académico, ProQuest Digital Dissertation & Theses, IEEE Xplore. Se examinaron diversos trabajos de investigación, tesis, así como buenas prácticas y tendencias en ciberseguridad (WEF, 2022).

Por otro lado, se analizaron acuerdos y convenios de cooperación internacional en la lucha global contra la ciberdelincuencia, para comprender los esfuerzos regionales y en el concierto de las naciones sobre el apoyo en la ciberseguridad de las pymes.

3.2 Adaptación de la información recopilada

Luego de identificar los datos de interés para la investigación, se procedió en los casos requeridos a su traducción, extracción de contenido de documentos y artículos, así como a la adaptación de la redacción al propósito del artículo.

3.3 Revisión por expertos

Los datos recopilados y adaptados fueron sometidos al criterio de expertos para seleccionar la información relevante para el objetivo de estudio.

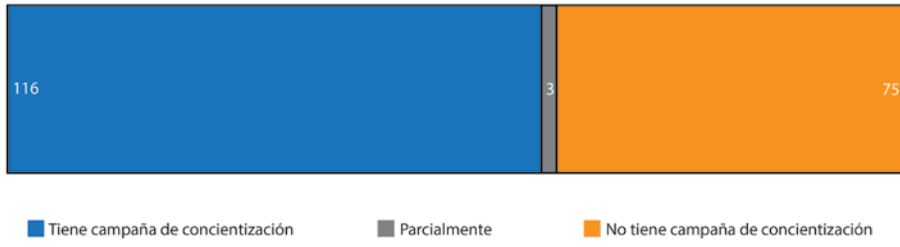
4. ACCIONES PARA PROMOVER LA CIBERSEGURIDAD DE LAS PYMES

La Unión Internacional de Telecomunicaciones (ITU) es la agencia especializada de la Organización de las Naciones Unidas para las tecnologías de la información y las comunicaciones (TIC). Está formada por una amplia gama de expertos y colaboradores dentro de los países y otras organizaciones internacionales. Una de sus iniciativas es el GCI, uno de cuyos puntos clave es "Medir el desarrollo de capacidades: desarrollando capacidades

en ciberseguridad", el cual contiene el subíndice denominado "Incrementando atención en las pymes, el sector privado y la conciencia cibernética del gobierno", donde se muestra que el 60 % de los países (como se muestra en la Figura 1) tienen una campaña de concientización sobre seguridad dirigida a las pymes, el sector privado y/o a las agencias gubernamentales.

Figura 1

Número de países con campañas de concientización sobre ciberseguridad dirigidas a pymes, sector privado y agencias gubernamentales

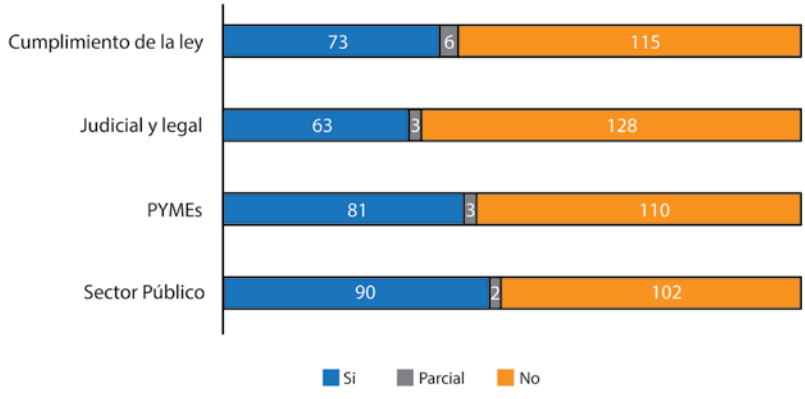


Nota. Adaptado de *Global Cybersecurity Index 2020* (p. 16), por Unión Internacional de Telecomunicaciones, 2022 (https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E).

Al segregar este indicador por áreas, tal como se muestra en la Figura 2, la cantidad de países que tienen programas de formación específicos sobre ciberseguridad disminuye a 42 %.

Figura 2

Número de países con programas de formación específicos en ciberseguridad



Nota. Adaptado de *Global Cybersecurity Index 2020* (p. 17), por Unión Internacional de Telecomunicaciones, 2022 (https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E).

A continuación, se describen las acciones concretas que han tomado cinco países de diferentes regiones para promover la ciberseguridad de las pymes.

4.1 Japón

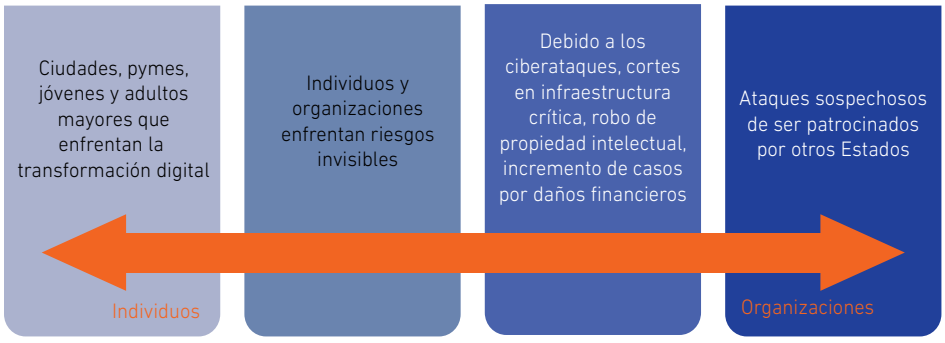
Dado que los ataques cibernéticos recientes se han vuelto cada vez más complejos y sofisticados, el Gobierno de Japón (2021) entiende que se deben tomar medidas de seguridad considerando la cadena de suministros completa, donde las pymes pueden no tener los medios adecuados y, por lo tanto, pueden ser objeto de ataques cibernéticos.

Según el Centro para la Cooperación Industrial UE-Japón (2022), este es uno de los países líderes en la aplicación comercial de las TIC desde principios de la década de 1980, pero hoy en día es considerado uno de los países más débiles entre las 15 potencias mundiales en lo que respecta a la ciberseguridad. Japón tiene algunas fortalezas potenciales en algunas categorías, pero debilidades significativas en otras. En la última década, ha realizado esfuerzos y ahora tiene un enfoque desarrollado para la gobernanza del ciberespacio. La década del 2020 fue importante para Japón, ya que el mundo entró en una era de nueva normalidad y sociedad digital. En este contexto, las empresas se vieron obligadas a responder a la pandemia con la innovación de los modelos de negocio, los cambios de patrones de empleo y estilos de trabajo, que desarrollan una estrategia país, donde el Gobierno de Japón (2021) promueve la transformación digital con ciberseguridad. Para ello, ha construido comunidades locales basadas en el concepto de ayuda mutua entre el gobierno, la empresa y la academia, no solo a través de asesorías con expertos, o ha integrado recursos humanos a las empresas, o ha fomentado las competencias y desarrollado soluciones de seguridad regional; igualmente, brinda subsidios a las pymes para contrarrestar su falta de recursos. Con esto busca fortalecer la ciberseguridad de toda la cadena de suministros, hasta sus eslabones más débiles.

La idea del Gobierno de Japón (2021), con su estrategia "Ciberseguridad para todos", es que nadie se quede atrás (véase la Figura 3). Todas las partes interesadas deben ser conscientes de forma independiente de su propio papel y participar en la ciberseguridad, ya que, a medida que avanza la transformación digital, una gama más amplia de personas, empresas e instituciones participa del ciberespacio. La sociedad y la economía de Japón deben lograr la transformación digital acompañada de varios cambios innovadores para lograr la visión de crear una sociedad donde las personas puedan elegir los servicios que se adapten a sus necesidades y, mediante el uso de la tecnología digital, puedan realizarse diversas formas de felicidad.

Figura 3

Propuesta de "Ciberseguridad para todos"



Nota. Adaptado de *Cybersecurity for All* (p. 12), por Gobierno de Japón, 2021 (https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf).

4.2 Australia

El Gobierno Australiano y el Centro Australiano de Seguridad Cibernética (2020) son muy conscientes de la escala creciente y el impacto de la actividad cibernética maliciosa. Sus datos indican que el 62 % de las pymes han experimentado un incidente de ciberseguridad. Además, casi la mitad de ellas calificaron su comprensión de la seguridad cibernética como promedio o por debajo del promedio y tenían prácticas de seguridad cibernética deficientes. Para los más de dos millones de pymes australianas, las acciones de estos actores maliciosos pueden ser dañinas y algunas empresas podrían no recuperarse de ese golpe. En la Figura 4, se muestran las barreras que experimentan las pymes australianas para implementar buenas prácticas de ciberseguridad.

Figura 4

Barreras para implementar buenas prácticas en ciberseguridad

Nota. Adaptado de *Cyber Security and Australian Small Businesses*, por Gobierno Australiano y Centro Australiano de Seguridad Cibernética, 2020 (https://www.cyber.gov.au/sites/default/files/2021-05/Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results%20-%20 20201130.pdf).

Por esta razón, el Gobierno Australiano y el Centro Australiano de Seguridad Cibernética (2020) crearon una guía escrita en lenguaje claro, con acciones simples, diseñada específicamente para que las pequeñas empresas entiendan, tomen medidas y aumenten su resiliencia en seguridad cibernética contra las amenazas en constante evolución. Esta guía explica cuáles son las principales ciberamenazas (*malware, phishing y ransomware*), así como las consideraciones del *software* necesarias (actualizaciones automáticas, copias de seguridad y autenticaciones multifactor); incluye también un capítulo dedicado a las personas y los procedimientos (controles de acceso, claves y capacitación). Paralelamente, elaboraron guías relativas a *software* y tecnologías específicas, que detallan el paso a paso para las pymes con la intención de profundizar en la ciberseguridad; y también guías con acciones de corto plazo (*quick wins*) que se pueden implementar de manera rápida, sencilla y económica, en temas de actualizaciones, dispositivos portátiles y sitios web. En síntesis, buscan enseñar a las pymes a protegerse ellas mismas de los incidentes de ciberseguridad más comunes, ya que un ataque puede tener un impacto devastador para este tipo de empresas.

4.3 Bélgica y la Unión Europea

El Centro de Ciberseguridad de Bélgica, en colaboración con la Coalición de Seguridad Cibernética para las Pymes, creó en el 2016 una guía de ciberseguridad para pymes, basada en aportes y mejores prácticas de entidades públicas y privadas. Desarrollaron una lista de 12 temas básicos y avanzados sobre ciberseguridad, que iban desde involucrar a la dirección hasta tener un plan de continuidad del negocio en caso de un incidente. Las recomendaciones básicas ayudaban a las pymes a evitar las trampas más comunes y proteger la información más valiosa, mientras que las prácticas y consejos más avanzados apoyaban con técnicas de mayor protección (Bruycker & Darville, 2017).

Por su parte, la ENISA, que fue creada en el 2004 con el objetivo de alcanzar un elevado nivel común de ciberseguridad en toda Europa a través del intercambio de conocimientos, el desarrollo de capacidades y la sensibilización, analizó la capacidad de las pymes en la UE para hacer frente a los desafíos de ciberseguridad planteados por la pandemia del COVID-19 y determinar las buenas prácticas para abordar esos desafíos (ENISA, 2021). Este informe proporciona consejos sobre ciberseguridad, pero también propuestas de acciones que los Estados miembros deberían considerar para ayudar a las pymes a mejorar su postura en esta materia. Esta investigación se complementó con una encuesta de dos meses de duración, en la que 249 pymes europeas compartieron sus comentarios sobre su estado de seguridad digital y preparación para crisis como la pandemia del COVID-19, así como con entrevistas específicas a participantes seleccionados. De esta manera, se identificó que los mayores desafíos para las pymes son la poca conciencia de las amenazas que plantea para su negocio una ciberseguridad deficiente, los costos de implementar medidas de ciberseguridad —a menudo combinados con la falta de presupuesto dedicado—, la poca disponibilidad de especialistas en ciberseguridad de las TIC, la inexistencia de pautas adecuadas dirigidas al sector de las pymes, y el bajo apoyo gerencial. Finalmente, la ENISA (2021) creó una guía que proporciona a este sector 12 pasos prácticos de alto nivel sobre cómo proteger mejor los sistemas y sus negocios, tales como proteger la red mediante *firewall*, proteger las copias de seguridad, impartir formación adecuada y desarrollar una buena cultura de ciberseguridad.

4.4 Estados Unidos de América

Estados Unidos cuenta con la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA, por sus siglas en inglés), creada en el 2018; y con la Alianza Nacional de Ciberseguridad (NCSA), que es una organización sin fines de lucro que tiene la misión de crear un mundo más seguro e interconectado. Para ello, interactúa con las familias, organizaciones intermedias y hasta con las empresas de la lista Fortune 500, con el objetivo de hacer que la ciberseguridad sea más fácil y accesible, para disfrutar de los beneficios de la tecnología sin preocupaciones, como indica en su página web (https://staysafeonline.org).

Cyber Essentials Starter Kit (CISA, 2021) es una guía para que los líderes de las pymes, así como los líderes de las agencias gubernamentales pequeñas y locales, desarrollen una comprensión práctica de dónde comenzar a implementar las prácticas de ciberseguridad. Se dirige al líder o la dirección, los usuarios o colaboradores, los sistemas (activos y aplicaciones), el lugar de trabajo, los datos y la forma de responder ante una crisis.

Por su parte, la NCSA (2022) creó el programa *Cyber Secure My Business*, que ayuda a las pymes a aprender a ser más seguras y protegidas en línea, mediante una serie de talleres altamente interactivos y fáciles de entender para educar a la comunidad pyme en identificar y proteger sus activos informáticos, detectar cuando algo ha salido mal, responder rápidamente para minimizar el impacto e implementar un plan de acción, así como conocer los recursos que se necesitan para recuperarse después de un ataque.

3.5 Costa Rica

En junio del 2017, se creó la Estrategia Nacional de Ciberseguridad de Costa Rica, liderada por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). Uno de sus objetivos era desarrollar o implementar campañas de concientización y de formación en ciberseguridad que fomenten la responsabilidad de la protección digital como un deber de todos los usuarios de las tecnologías digitales, desarrollando foros de intercambio de información y conversatorios sobre temas de ciberseguridad, específicamente para las pymes.

Luego de los ciberataques perpetrados por un grupo criminal en abril y junio del 2022 a más de 25 instituciones públicas, se presentó un nuevo proyecto de ley en la Asamblea Legislativa (2022) denominado Ley de Ciberseguridad, que procura dotar a Costa Rica del andamiaje regulatorio indispensable para que el país se prepare adecuadamente a futuro con herramientas e infraestructura. Es un ambicioso proyecto país en su alcance, pues refleja las mejores prácticas existentes a nivel internacional en esta materia. Propone crear una Agencia Nacional de Ciberseguridad como dependencia adscrita al MICITT (Paris, 2022).

Estos son los pasos iniciales que Costa Rica está dando en el tema de ciberseguridad. Los planes de gobierno apuntan hacia una integración de esfuerzos particularmente en el sector público para establecer escenarios propicios para el desarrollo de estas normativas.

5. DISCUSIÓN

Según los resultados del GCI, muchos países promulgaron nuevas leyes y reglamentos de seguridad cibernética para abordar áreas como la privacidad, el acceso no autorizado y la seguridad en línea (Bogdan-Martin, 2022). Este es el caso de Costa Rica y su nuevo proyecto de ley como producto de su visionaria vinculación al Convenio de Budapest. Dicho proyecto es indispensable para el país, es robusto y técnicamente sustentado; en caso de aprobarse,

sería pionero en nuestra región. En particular, el país podría acceder a la Industria 4.0 con las herramientas necesarias, comprometido con la seguridad y los derechos de la población en el ciberespacio. Esta legislación se enmarca en el contexto histórico vivido; si en el futuro Costa Rica vuelve a ser presa de un ciberataque a esta escala, será por negligencia de quienes no hayan asimilado las recientes lecciones (Asamblea Legislativa, 2022).

Más allá de trabajar juntos dentro de cada país, es posible que sea necesaria la cooperación entre gobiernos para que los menos capacitados puedan abordar los desafíos de ciberseguridad, por ejemplo, los países menos desarrollados (ITU, 2022). Tal como lo propone el Gobierno de Japón (2021) en su proyecto de ciberseguridad para todos, sin dejar a nadie rezagado, se debe contar con colaboración basada en la plena participación de la industria, la academia, los sectores públicos y privados, participando y promoviendo actividades de sensibilización fluidas y efectivas. El capital humano es el elemento primordial para la transformación cultural que requiere el paso hacia la ciberinmunidad; es por ello que la inclusión de contenidos cognitivos apropiados en los ámbitos educativos en todos los niveles puede ser una de las vías que los Estados podrían considerar (Díaz, 2021).

En especial en Latinoamérica, tenemos una propensión a minimizar la exposición al riesgo, aún más al riesgo tecnológico. La causa podría ser la falta de conocimiento de las actividades delictivas que las tecnologías actuales facilitan (Díaz, 2022). Tal como recomiendan Vergara-Romero et al. (2021) para desarrollar las habilidades necesarias, la gestión formativa, especialmente de la academia, debe utilizar la gama completa de formas de aprendizaje disponible. Desde proyectos especializados de extensión para pymes hasta promover a nivel universitario la oferta educativa especializada en ciberdefensa, así como revisar los contenidos curriculares actuales relacionados con las TIC, podrían ser una buena estrategia desde la gestión pública de cada país para contribuir a la sinergia regional (Díaz, 2021).

6. CONCLUSIONES

Un aprendizaje trascendental producto de la pandemia del COVID-19 es que los problemas de acción colectiva, como la salud o la ciberseguridad, deben abordarse con un enfoque interdisciplinario y holístico. Por eso, desde una perspectiva multilateral, los países que llevan la delantera deben apoyar a los menos desarrollados, ya que los ataques cibernéticos no respetan fronteras.

Las pymes desempeñan un papel importante como actores en la economía digital y las cadenas de suministro global. En este período de cambio hacia el comercio electrónico y la transformación digital de la sociedad como un todo, las pymes requieren soporte de los gobiernos en la gestión del riesgo cibernético. Debido a ello, es esencial la cooperación entre la academia y los gobiernos para posicionarlas en la ruta evolutiva desde una fase de concientización del riesgo hasta la construcción de una cultura

de ciberseguridad, asegurando la integridad, confidencialidad y disponibilidad de sus activos de información para la continuidad del negocio.

REFERENCIAS

Agencia de Ciberseguridad y Seguridad de Infraestructura. (2021). *Cyber Essentials Starter Kit*. https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf

Agencia de la Unión Europea para la Ciberseguridad. (2021). Cybersecurity for SMEs. Challenges and recommendations. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Asamblea Legislativa. (2022). Proyecto de Ley, Ley de Ciberseguridad de Costa Rica [Expediente N.° 23.292]. Diario oficial *La Gaceta*, *172*(Alcance 189). http://www.asamblea.go.cr/Centro_de_informacion/Consultas_SIL/SitePages/ConsultaProyectos.aspx

Ballestero, F. (2020). La ciberseguridad en tiempos difíciles. ¿Nos ocupamos de ella o nos preocupamos por ella? *Boletín Económico de ICE, Información Comercial Española*, *3122*, 39-48.

Bogdan-Martin, D. (2022). Foreword. En Unión Internacional de Telecomunicaciones, *Global Cybersecurity Index 2020* (pp. iv-v). https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Bruycker, M., & Darville, C. (2017). *Cyber Security Guide for SME*. Centre for Cyber Security Belgium. https://ccb.belgium.be/en/document/guide-sme

Bustillos Ortega, O., & Rojas Segura, J. (2022). Protocolo básico de ciberseguridad para pymes. *Interfases*, *16*, 168-186. https://doi.org/10.26439/interfases2022.n016.6021

Centro para la Cooperación Industrial UE-Japón. (2022, febrero). *Cybersecurity*. https://www.eubusinessinjapan.eu/sectors/security/cybersecurity

Deutsche Welle. (2021, 31 de agosto). *Ciberataques aumentaron 24 % en América latina este año.* https://www.dw.com/es/ciberataques-aumentaron-24-en-am%C3%A9rica-latina-este-a%C3%B1o/a-59046424

Díaz, R. M. (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe*. Comisión Económica para América Latina y el Caribe, serie Desarrollo Productivo n.° 228. https://repositorio.cepal.org/handle/11362/47240

Díaz, R. M. (2022). *Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe*. Comisión Económica para América Latina y el Caribe, serie Documentos de Proyectos. https://repositorio.cepal.org/handle/11362/48065

Estévez, J. C. (2020, 6 de enero). En qué consiste el convenio de Budapest y cómo regula la ciberdelincuencia. *Think Big*. https://empresas.blogthinkbig.com/convenio-budapest-ciberdelincuencia/

Florez Martinez, J. L., & Rentería Mosquera, J. M. (2020). *Conocer el valor de la información (activo económico) para valorar la necesidad de la ciberseguridad* [Tesis de grado, Tecnológico de Antioquia, Institución Universitaria]. Repositorio Digital. https://dspace.tdea.edu.co/handle/tdea/1395

Foro Económico Mundial. (2019). *Informe de riesgos mundiales 2019* (14.ª ed.). https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2019/January/ES-Global-Risks-Report-2019.pdf

Foro Económico Mundial. (2022). *Global Cybersecurity Outlook 2022*. https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

Garnacho, A. R. (2018). Panorama actual de la ciberseguridad. *Economía Industrial*, *410*, 13-26.

Gobierno Australiano & Centro Australiano de Seguridad Cibernética. (2020). *Cyber security and Australian small businesses*. https://www.cyber.gov.au/sites/default/files/2021-05/Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results%20-%2020201130.pdf

Gobierno Australiano & Centro Australiano de Seguridad Cibernética. (2021). *Small Business Cyber Security Guide*. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/small-business-cyber-security/small-business-cyber-security-guide

Gobierno de Japón. (2021). *Cybersecurity for all*. https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf

Inoguchi, A., & Macha, E. L. (2017). *Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016* [Tesis de grado, Universidad San Ignacio de Loyola]. Repositorio Institucional. Universidad San Ignacio de Loyola. https://repositorio.usil.edu.pe/handle/usil/2810

Morales, F., Toapanta, S., & Toasa, R. M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *E27*, 553-565. http://www.risti.xyz/issues/ristie27.pdf

Orellana, F. D. (2020). *Cybersecurity incident response capabilities in the Ecuadorian small business sector: A qualitative study* [Tesis doctoral, Northcentral University]. ProQuest Dissertations Publishing. http://www.proquest.com/pqdtglobal/docview/2466034020/abstract/6BDCDD913D1D469EPQ/1

Paris, M. (2017, 14 de julio). Convenio de Budapest sobre ciberdelincuencia ya es ley en Costa Rica. *Bonafide*. https://bonafide.cr/convenio-de-budapest/

Paris, M. (2022, 25 de agosto). Ley de Ciberseguridad. *La República*. https://www.larepublica.net/noticia/ley-de-ciberseguridad

Peralta Zuñiga, M. L., & Aguilar Valarezo, D. N. (2021). La ciberseguridad y su concepción en las PYMES de Cuenca, Ecuador. *Contabilidad y Auditoría*, *53*, 99-126. https://ojs.econ.uba.ar//index.php/Contyaudit/article/view/2061

Ponsard, C., Grandclaudon, J., & Bal, S. (2019). Survey and lessons learned on raising SME awareness about cybersecurity. En *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP)* (pp. 558-563). https://doi.org/10.5220/0007574305580563

Ramírez, C., & González, J. C. (2020). *Guía de controles y buenas prácticas de ciberseguridad para MiPymes* [Tesis de grado, Tecnológico de Antioquia, Institución Universitaria]. Repositorio Digital. https://dspace.tdea.edu.co/handle/tdea/1394

Unión Internacional de Telecomunicaciones. (2022). *Global Cybersecurity Index 2020*. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Vergara-Romero, A., Sánchez, F. M., Sorhegui-Ortega, R., & Olalla-Hernández, A. (2021). Capital humano: actor central para la sostenibilidad organizacional. *Revista Venezolana de Gerencia*, *26*(93), 297-307.

Xu, M., & Hua, L. (2019). Cybersecurity insurance: Modeling and pricing. *North American Actuarial Journal*, *23*(2), 220-249. https://doi.org/10.1080/10920277.2019.1566076

Zuña Macancela, E. R., Arce Ramírez, Á. A., Romero Berrones, W. J., & Soledispa Baque, C. J. (2019). Análisis de la seguridad de la información en las PYMES de la ciudad de Milagro. *Universidad y Sociedad*, *11*(4), 487-492. http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2218-36202019000400487&lng=es&nrm=iso&tlng=en