CÓMO PROMUEVEN LOS ESTADOS LA CIBERSEGURIDAD DE LAS PYMES

Olda Bustillos Ortega
Directora de la Escuela de Ingeniería Informática de la Universidad Internacional de las Américas, San José Costa Rica

Javier Rojas Segura
Docente Investigador de la Escuela de Ingeniería Informática de la Universidad Internacional de las Américas, San José Costa Rica

Resumen

La tecnología ha producido cambios en la sociedad, lo cual ha forjado la evolución de nuestra especie. Actualmente la digitalización ha dado lugar al uso exponencial de tecnologías de la información y la comunicación, generando consecuentemente un aumento en el riesgo de ciberataques, que amenazan la cadena de suministros global, siendo las pequeñas y medianas empresas y su ecosistema las más afectados por la escasez de recursos para proteger la integridad, confidencialidad y disponibilidad de sus activos de información.

Incrementar la concientización general en ciberseguridad eleva la inmunidad global a los ciberataques, por lo que el objetivo es investigar como 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.*

Abstract

Technology has produced changes in society, which has forged the evolution of our species. Currently, digitalization has given rise to the exponential use of information and communication technologies, consequently determining an increase in the risk of cyberattacks, which threaten the global supply chain, with small and medium-sized companies and their ecosystems being the most affected by the lack of resources to protect the integrity, confidentiality, and availability of its information assets.

Increasing awareness of cybersecurity raises global immunity to cyberattacks, so the purpose is to investigate how the governments of some countries support the cybersecurity of small and medium-sized companies, highlighting international best practices and identifying areas for improvement in the 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 support in managing cyber risk, in cooperation with academia to 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 WEF (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 de COVID-19 el gran aumento del teletrabajo y las ventas *online*, sin la adecuada protección ante los virus informáticos o *malware*, colocaron sobre la mesa la vulnerabilidad existente (Ballestero, 2020). Desde el inicio de la pandemia, 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, en donde 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 resultado de 35 ataques cibernéticos por segundo, figurando 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, causando tal magnitud de daño 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 para 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 generando 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).

Para la Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2021) 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 representan 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. Es por ello que 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 ella misma, sino para toda la cadena de suministros.

Tal como lo revela el Gobierno de Japón (2021), las PYMES se enfrentan a una carencia particularmente grave de talento en ciberseguridad, por lo que el gobierno debe de ser responsable 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 el fortalecimiento de la ciberseguridad de las PYMEs.

2. Revisión de Literatura

La seguridad de la información se ha convertido en una tendencia a nivel 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 afecta al bienestar digital de la sociedad, de las organizaciones y de los países accediendo a datos privados tanto a nivel personal como organizacional (Zuñiga & 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 esta 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, con la finalidad de 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, originalmente de la UE, y 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, estableciendo 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 60 países a nivel mundial los que se han incorporado al tratado (Estévez, 2020). En Latinoamérica, además de Costa Rica quien 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 fomenta la creación de capacidad sostenibles a largo plazo en la lucha contra el ciberdelito. Apoyando a los sistemas de justicia penal de los Estados miembros y brindando asistencia técnica en la generación de capacidades para la prevención. Además, 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), tiene como función 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 de investigación y divulgación, beneficiando 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, el CCDCOE (s. f.) 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.

La agencia especializada de la Organización de las Naciones Unidas para las tecnologías de la información y las comunicaciones (TIC) es la ITU, misma que está formada y mejorada por el trabajo de una amplia gama de expertos y colaboradores dentro de los países y otras

organizaciones internacionales. Una de sus iniciativas es Índice de Ciberseguridad Global (GCI) en cuya Tabla 1 se presentan los resultados para Latinoamérica y el Caribe.

Tabla 1

Índice de Ciberseguridad Global para Latinoamérica y el Caribe

País	Nota	Posición
Brasil	96.6	1
México	81.68	2
Uruguay	75.15	3
República Dominicana	75.07	4
Chile	68.83	5
Costa Rica	67.45	6
Colombia	63.72	7
Cuba	58.76	8
Paraguay	57.09	9
Perú	55.67	10
Argentina	50.12	11
Panamá	34.11	12
Jamaica	32.53	13
Surinam	31.2	14
Guyana	28.11	15
Venezuela	27.06	16
Ecuador	26.3	17
Trinidad and Tobago	22.18	18
Barbados	16.89	19
Bolivia	16.14	20
Antigua and Barbuda	15.62	21
Bahamas	13.37	22
El Salvador	13.3	23
Guatemala	13.13	24
Saint Kitts and Nevis	12.44	25
Saint Vincent and the Grenadines	12.18	26
Saint Lucia	10.96	27
Belice	10.29	28
Grenada	9.41	29
Nicaragua	9	30
Haití	6.4	31
Dominica	4.2	32
Honduras	2.2	33

Nota. Adaptada de Global Cybersecurity Index 2020. International Telecommunication Union, U.N. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

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 de COVID-19, analizó la capacidad de las PYMEs dentro de la UE para hacer frente a los desafíos de ciberseguridad planteados por la pandemia 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 Foro Económico Mundial (WEF, 2022) a 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 las cadenas de suministro 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 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 ciberdelicuentes para efectuar sus ataques (Zuñiga & 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 (ACSC, 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 de 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, representan el 99% del parque empresarial empleando a unos 100 millones de colaboradores, además aportan más de la mitad del PIB de la UE y juegan un papel clave en la creación de valor en todos los sectores de la economía europea (ENISA, 2021).

3. Metodología

Acorde a la Unión Internacional de Telecomunicaciones (ITU, 2022), los países deben abordar sus fortalezas y debilidades en ciberseguridad, aprovechando sus ventajas competitivas para promover su capacidad cibernética. El GCI puede apoyar a los países a iniciar este proceso. Sin embargo, para progresar los países deben de 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 lo que, mediante un enfoque cualitativo con alcance exploratorio, se propone investigar como los gobiernos de diversos países apoyan a las PYMEs para asegurar la integridad, confidencialidad y disponibilidad de sus activos de información, siguiendo las siguientes etapas:

3.1. Investigación

Se procedió en esta etapa 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 tales como Google Académico, ProQuest Digital Disertation and 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. Así como fuentes primarias de informes de instituciones a cargo de promover la ciberseguridad de las empresas.

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 la adaptación de la redacción alineado al propósito del artículo.

3.3. Revisión por expertos

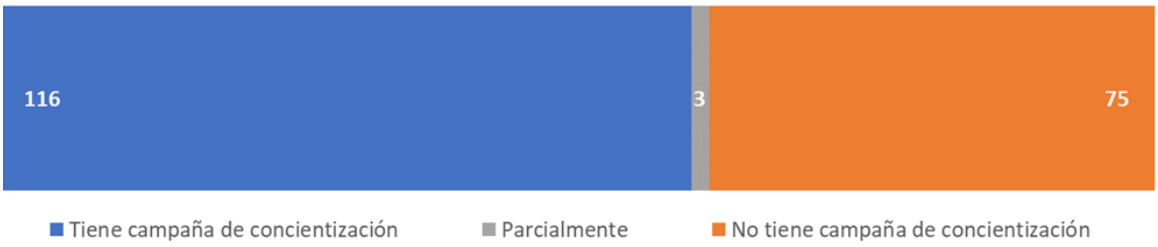
La datos recopilados y adaptados fueron sometidos al criterio de expertos para seleccionar la información relevante para el objetivo de estudio.

4. Acciones para promover la ciberseguridad de las PYMEs

Una de las iniciativas de ITU es el GCI, del cual uno de sus puntos clave es “Medir el desarrollo de capacidades: Desarrollando capacidades en ciberseguridad”, mismo que 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 gubernamental.

Figura 1

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

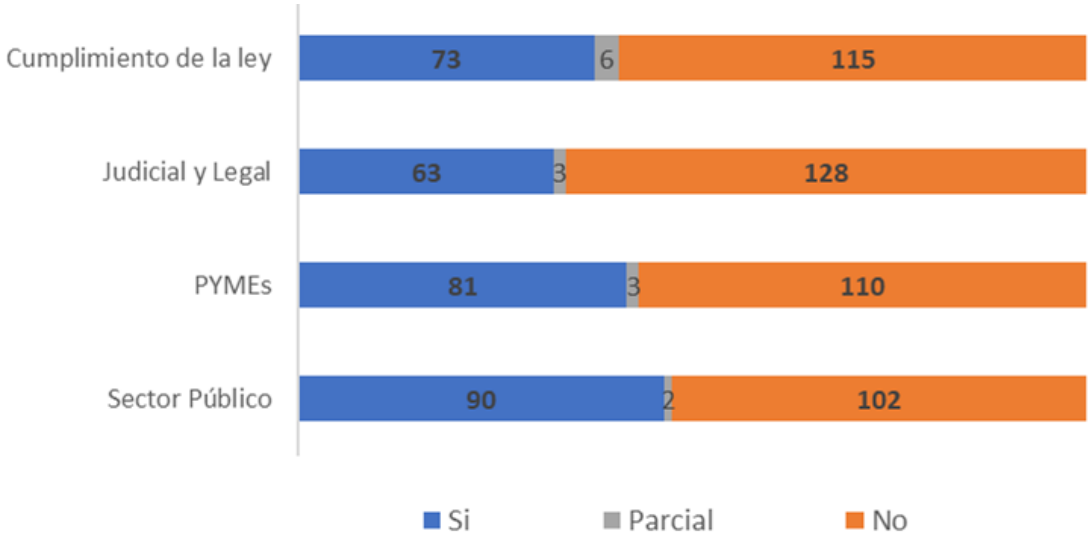


Nota. Adaptada de Global Cybersecurity Index 2020 (p. 16). International Telecommunication Union, U.N. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

Al segregar este indicador por áreas, tal como se muestra en la figura 2, la cantidad de países que tienen campañas de concientización en ciberseguridad específicos para PYMEs disminuye a 42%.

Figura 2

Número de países con programas formación específicos en ciberseguridad



Nota. Adaptada de Global Cybersecurity Index 2020 (p. 17). International Telecommunication Union, U.N. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

A continuación, se detallan el caso de cinco países de diferentes regiones, que han tomado acciones concretas 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 suministro completa, donde las PYMEs, pueden no tener los medios adecuados, por lo tanto, pueden ser objeto de ataques cibernéticos.

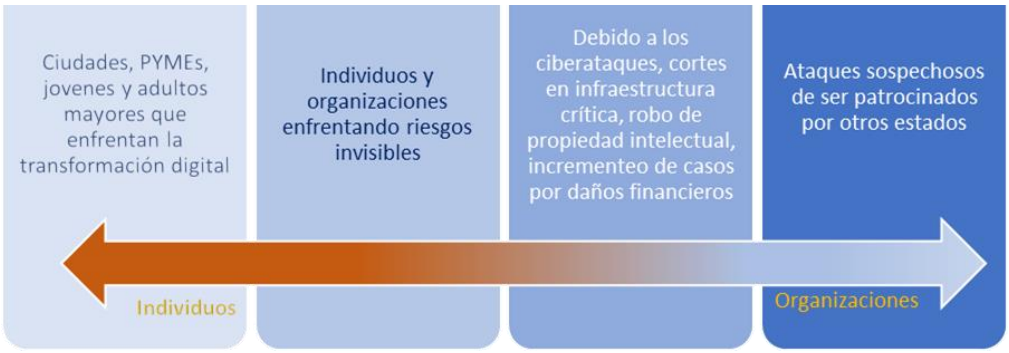
Según el Centro para la Cooperación Industrial UE-Japón (2022), este es uno de los países líderes en la aplicación comercial de las TIC desde principios de la década de 1980, pero hoy en día es considerado uno de los países más débiles entre las 15 potencias mundiales en lo que respecta a la ciberseguridad. Japón tiene algunas fortalezas potenciales en algunas categorías, pero debilidades significativas en otras. En la última década, Japón realizó esfuerzos y actualmente tiene un enfoque desarrollado para la gobernanza del ciberespacio. La década de 2020 fue importante para Japón, ya que el mundo entró en una era de nueva normalidad y sociedad digital. Es en este contexto donde las empresas se ven obligadas a responder a la pandemia, 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. Construyendo 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 integrando recursos humanos a las empresas, o fomentando las competencias y desarrollando soluciones de seguridad regional, sino también mediante subsidios destinados a las PYMEs para contrarrestar su falta de recursos. Buscando con esto 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 (como se muestra en 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 participan 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 en diversas formas de felicidad.

Figura 3

Propuesta de ciberseguridad para todos, sin dejar a nadie atrás.



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

4.2. Australia

El Centro Australiano para la Ciber Seguridad (2020) es muy consciente 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 las más de 2 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 muestra las barreras que experimentan las PYMEs australianas para implementar buenas prácticas de ciberseguridad.

Figura 4

Barreras para implementar buenas prácticas en ciberseguridad

Nota. Adaptada de Centro Australiano para la Ciber Seguridad. (2020). Ciber Seguridad y Pequeños Negocios Australianos. https://www.cyber.gov.au/sites/default/files/2021-05/Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results%20-%2020201130.pdf

Por esta razón Gobierno Australiano (2021) creó 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. La Guía para la Ciber Seguridad de las PYMEs, explica cuáles son las principales ciberamenazas (*malware, phishing y ramsomware*), así como las consideraciones del software a tener en cuenta (actualizaciones automáticas, copias de seguridad y autenticaciones multifactor), incluyendo un capítulo dedicado a las personas y los procedimientos (controles de acceso, claves y capacitación). Paralelamente crearon guías relativas a software y tecnologías específicas, detallando el paso a paso para aquellas PYMEs con la intensión de profundizar en la ciberseguridad. Así como 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, busca 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 Unión Europea

El Centro para la Seguridad Cibernética de Bélgica en colaboración con la Coalición de Seguridad Cibernética para las PYMEs, creó en 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 concejos más avanzados ayudaban con técnicas de mayor protección (Bruycker & Darville, 2017).

Por su parte la Agencia de la Unión Europea para la Ciberseguridad (ENISA) que fue creada en 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. En respuesta a la pandemia de COVID-19, ENISA (2021) analizó la capacidad de las PYMEs dentro de la UE para hacer frente a los desafíos de ciberseguridad planteados por la pandemia y determinar las buenas prácticas para abordar esos desafíos. 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 materia de ciberseguridad. 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 COVID-19, siguiendo con entrevistas específicas con participantes seleccionados. La investigación 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 disponibilidad de especialistas en ciberseguridad de las TICs, la falta de pautas adecuadas dirigido al sector PYME, y bajo apoyo gerencial. Finalmente ENISA (2021) creó una guía que proporciona a las PYMEs 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 la ciberseguridad.

4.4. Estados Unidos de América

Por un lado tenemos a la agencia federal de Ciberseguridad e Infraestructura (CISA por sus siglas en inglés) creada en 2018 por otro a la Alianza Nacional de Ciberseguridad (NCSA), que es una organización sin fines de lucro, con la misión de crear un mundo más seguro e interconectado. Interactuando con las familias, organizaciones intermedias y hasta las *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 (NCSA, 2022).

Cyber Essentials de 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, dirigiéndose a el 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 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 a 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 que recursos se necesitan para recuperarse después de un ataque.

4.5. Costa Rica

En junio del 2017, se generó la Estrategia Nacional de Ciberseguridad (ENC) de Costa Rica, liderado 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 de 2022 a más de 25 instituciones públicas, se ha presentado 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. Siendo un ambicioso proyecto país en su alcance, reflejando las mejores prácticas existentes a nivel internacional en esta materia. Propone crear una Agencia Nacional de Ciberseguridad, como dependencia adscrita al MICITT (Paris, 2022).

Siendo estos 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. En la Estrategia Nacional de Ciberseguridad 2023-2027 el país continúa avanzando para promover actividades de investigación y desarrollo en el ámbito de la ciberseguridad, en colaboración con la academia y la industria para generar nuevas soluciones y enfoques para enfrentar incidentes y promover los sistemas de información (ENC, 2023) de las empresas y el gobierno.

5. Discusión

Acorde a 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). Tal como 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. Particularmente, el país podría acceder a la Industrial 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 del país, es posible que los países deban apoyar a otros gobiernos menos capacitados para abordar los desafíos de ciberseguridad, como 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, 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. Donde el capital humano debe ser 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 el paso uno que los estados deberían considerar (Díaz, 2021). Particularmente en Latinoamérica, tenemos una propensión a minimizar la exposición al riesgo, aún más al riesgo tecnológico, esto podría tener su causa en la falta de conocimiento de las actividades delictivas que las tecnologías actuales facilitan (Díaz, 2022). Tal como lo recomienda 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 TICs, podría 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 de COVID-19 es que los problemas de acción colectiva como la salud o la ciberseguridad deben abordarse con un enfoque interdisciplinario y holístico. Por lo que 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 el *e-commerce* transfronterizo y las cadenas de suministro global. En este periodo 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 posicionar a las PYMEs en la ruta evolutiva de una fase de concientización del riesgo a la construcción de una cultura de ciberseguridad, asegurando la integridad, confidencialidad y disponibilidad de sus activos de información, para la continuidad del negocio.

Referencias

ACSC. (2021). *Small Business Cyber Security Guide*. Centro Australiano para la Ciber Seguridad. https://www.cyber.gov.au/sites/default/files/2021-11/ACSC_Small_Business_Cyber_Security_Guide_V6.pdf

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—Global Cybersecurity Index 2020*. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Bruycker, Mi. de, & Darville, C. (2017). *Cyber Security Guide for SME, Foreword*. 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, 016*, Article 016. https://doi.org/10.26439/interfases2022.n016.6021

CCDCOE. (s. f.). *CCDCOE - El Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN es un centro multinacional e interdisciplinario de experiencia en defensa cibernética.* Recuperado 6 de octubre de 2022, de https://ccdcoe.org/

Centro Australiano para la Ciber Seguridad. (2020). *Ciber Seguridad y Pequeños Negocios Australianos*. https://www.cyber.gov.au/sites/default/files/2021-05/Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results%20-%2020201130.pdf

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

CISA. (2021). *Cyber Essentials Starter Kit*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf

Deutsche Welle. (2021, agosto 31). *Ciberataques aumentaron 24% en América latina este año | DW | 31.08.2021*. DW.COM. 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* (serie Desarrollo Productivo, N° 228). Comisión Económica para América Latina y el Caribe (CEPAL). https://repositorio.cepal.org/handle/11362/47240

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

ENC. (2023). Estrategia Nacional de Ciberseguridad de Costa Rica, 2023-2027. Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. https://www.micitt.go.cr/wp-content/uploads/2023/04/Estrategia-Nacional-de-Ciberseguridad-MICITT-2023-2027.pdf#:~:text=El%20objetivo%20es%20el%20de%20posicionar%20a%20Costa,las%20oportunidades%20que%20de%20este%20desarrollo%20pudieran%20surgir.

ENISA. (2021). *Cybersecurity for SMEs—Challenges and Recommendations*. The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Estévez, J. C. (2020, enero 6). 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*. https://dspace.tdea.edu.co/handle/tdea/1395

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

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

Proyecto de Ley de Ciberseguridad de Costa Rica, Expediente 23292, Asamblea Legislativa, Gaceta 172 Alcance 189 (2022). http://www.asamblea.go.cr/Centro_de_informacion/Consultas_SIL/SitePages/ConsultaProyectos.aspx

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

ITU. (2022). *Global Cybersecurity Index 2020* (p. 172). International Telecommunication Union, U.N. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

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. https://www.researchgate.net/publication/339956501_Implementacion_de_un_sistema_de_seguridad_perimetral_como_estrategia_de_seguridad_de_la_informacion

NCSA. (2022). *Cyber Secure My Business*. National Cybersecurity Alliance. https://staysafeonline.org/programs/cybersecure-my-business/

Orellana, F. D. (2020). *Cybersecurity Incident Response Capabilities in the Ecuadorian Small Business Sector: A Qualitative Study* [D.B.A.]. http://www.proquest.com/pqdtglobal/docview/2466034020/abstract/6BDCDD913D1D469EPQ/1

Paris, M. (2017, julio 14). Convenio de Budapest sobre Ciber delincuencia aprobado en Costa Rica. *Bonafide*. https://bonafide.cr/convenio-de-budapest/

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

Ponsard, C., Grandclaudon, J., & Bal, S. (2019). Survey and Lessons Learned on Raising SME Awareness about Cybersecurity. *ICISSP*, 558-563. https://doi.org/10.5220/0007574305580563

Ramírez, C., & González, J. C. (2020). *Guía de Controles y Buenas Prácticas de Ciberseguridad para MiPymes* [Tecnológico de Antioquia, Institución Universitaria]. https://dspace.tdea.edu.co/handle/tdea/1394

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.

WEF. (2019). *Global risks 2019: Insight report* (14th Edition). World Economic Forum. https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2019/January/ES-Global-Risks-Report-2019.pdf

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

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., 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. *Revista 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

Zuñiga, M. L. P., & Valarezo, D. N. A. (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