

XII CONFERENCIA REDLAS

**Red Latinoamericana y del Caribe
para la Investigación en Servicios**



**Integración regional
en servicios**

CÓMO PROMUEVEN LOS ESTADOS LA CIBERSEGURIDAD DE LAS PYMES

MSc. Olda Bustillos Ortega

Universidad Internacional de las Américas

Dr. Cand. Javier Rojas Segura

Universidad Internacional de las Américas

San José, Costa Rica



Justificación

La tecnología ha producido cambios en la sociedad, lo cual ha forjado la evolución de nuestra especie.

La digitalización ha dado lugar al uso exponencial de TICs, generando consecuentemente un aumento en el riesgo de ciberataques, que amenazan la cadena de suministros global.

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 (WEF 2019)

Desde el inicio de la pandemia, los ciberataques han aumentado (Díaz, 2021)

Las PYMEs son el objetivo de la gran mayoría de ataques cibernéticos (Ponsard et al., 2019)

Justificación


En 2021, LATAM hubo 728 MM de intentos de infección (35 por segundo), 24% + que en 2020 (Deutsche Welle, 2021).

De los ataques que resultan efectivos y causan daños mayores, el 40% recae en las PYMEs, en muchos casos no se recuperan (Díaz, 2022)

En las PYMEs se generan 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 & Rojas, 2022).

La falta de capacidad de respuesta ante un ataque por parte de las PYMEs es un problema no solo para ella misma, sino para toda la cadena de suministros (Orellana, 2020).



Investigar cómo los gobiernos de diversos países apoyan a las PYMEs para asegurar la integridad, confidencialidad y disponibilidad de sus activos de información.

Las PYMES se enfrentan a una carencia grave de talento en ciberseguridad. El gobierno debe de ser responsable de proporcionar conocimientos y redes que sean útiles para aplicar prácticas de ayuda mutua, mediante la construcción de un ecosistema y la promoción de la colaboración entre la industria y la Academia (Gobierno de Japón, 2021).

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.

Convenio de Budapest (2001). + 60 países



Programa Mundial sobre Ciberdelincuencia - ONU

Agencia de la Unión Europea para la Ciberseguridad (ENISA)

Programa de Seguridad Cibernética - OEA

Centro de Excelencia de Ciberdefensa Cooperativa - OTAN

Unión Internacional en Telecomunicaciones (ITU) ONU

Índice de Ciberseguridad Global (GCI)

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

País	Nota	Posición
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
Belize	10.29	28
Grenada	9.41	29
Nicaragua	9	30
Haití	6.4	31
Dominica	4.2	32
Honduras	2.2	33

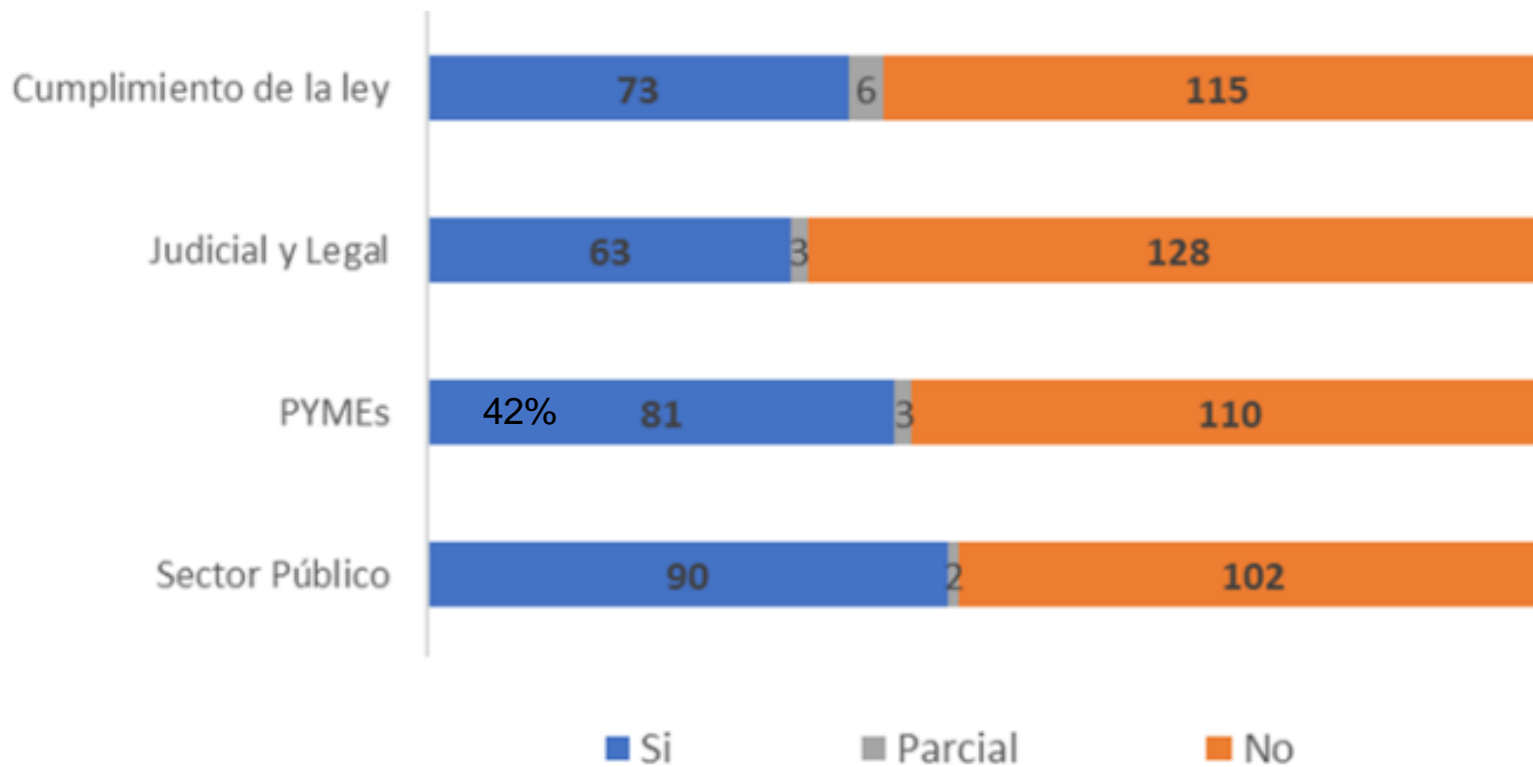


Número de países con campañas de concientización sobre ciberseguridad dirigidas a PYMEs, sector privado y agencias gubernamentales

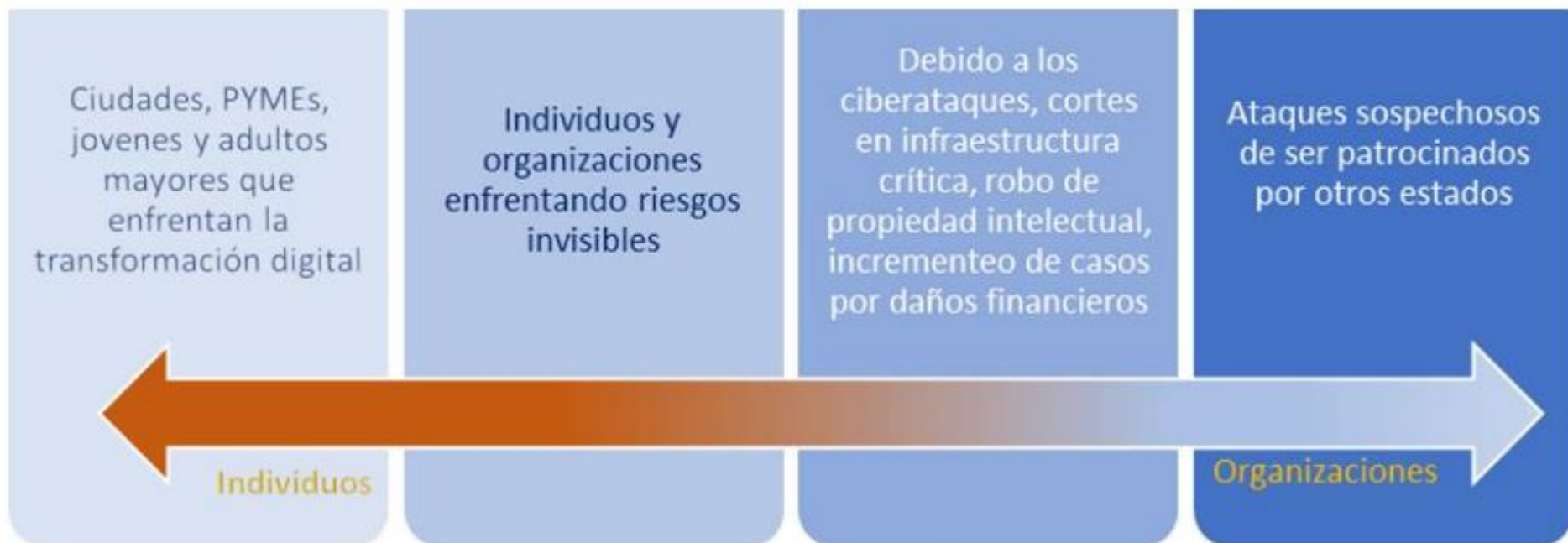



Nota. Adaptada de Global Cybersecurity Index 2020 (p. 16). International Telecommunication Union, U.N. <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E>.

Número de países con programas formación específicos en ciberseguridad



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





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.**

Barreras para implementar buenas prácticas en ciberseguridad

NO TENER STAFF DE TI DEDICADO

La ciberseguridad debe competir por tiempo y recursos entre múltiples necesidades

PLANIFICACION Y RESPUESTA


Las empresas necesitan planificar y responder mejor a los incidentes cibernéticos


COMPLEJIDAD Y AUTOEFICACIA

Los dueños de las PYMEs no logran identificar las debilidades en las prácticas de seguridad, no saben por donde empezar

SUBESTIMAR EL RIESGO

Las PYMEs necesitan comprender mejor el riesgo e impacto de un incidente cibernético y no subestimar su periodo de recuperación.

- 
- La Guía para la Ciber Seguridad de las PYMEs, explica cuáles son las principales ciberamenazas (*malware, phishing y ransomware*)
 - 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).
 - 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

- 
- 2016 Guía para la Ciberseguridad de las PYMEs, basada en aportes y mejores prácticas de entidades públicas y privadas.
 - 2021 Desarrollaron Guía 12 temas básicos y avanzados sobre ciberseguridad, desde involucrar a la dirección hasta un plan de continuidad del negocio en caso de un incidente.

- 
- Ciberseguridad e Infraestructura (CISA), agencia federal - 2018.

Cyber Essentials (2021), guía para que los líderes de las PYMEs y agencias gubernamentales pequeñas y locales, para que desarrollen una comprensión práctica.

- Alianza Nacional de Ciberseguridad (NCSA) sin fines de lucro

Crear un mundo más seguro e interconectado. Interactuando con las familias, PYMEs 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.**

Cyber Secure My Business (2022) Talleres interactivos y fáciles de entender, hasta como recuperarse de un ataque.



- Estrategia Nacional de Ciberseguridad 2017

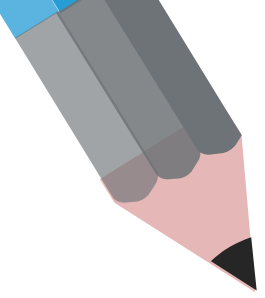
Campañas de concientización y formación a PYMEs, protección digital como deber del usuario.

- Proyecto de Ley de Ciberseguridad 2022.

Un ambicioso proyecto país en su alcance, reflejando las mejores prácticas existentes a nivel internacional en esta materia.

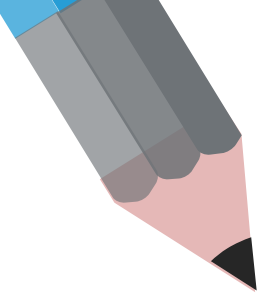
- Estrategia Nacional de Ciberseguridad 2023-2027

Promueven actividades de investigación y desarrollo en el ámbito de la ciberseguridad, en colaboración con la academia y la industria.



Conclusiones

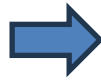
- Un aprendizaje trascendental producto de la pandemia de COVID-19 es que **los problemas de acción colectiva** como la salud o la ciberseguridad **deben abordarse con un enfoque interdisciplinario y holístico.**
- Los países que llevan la delantera deben apoyar a los menos desarrollados, ya que los 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.



Conclusiones

- 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.

Concientización del Riesgo



Cultura de Ciberseguridad