2018

White paper series
Edición 3

OPORTUNIDADES Y DESAFÍOS — PARA LAS **PYMES** EN EL — CONTEXTO DE UNA MAYOR ADOPCIÓN DE LAS TIC

OEA Más derechos para más gente

aws

OPORTUNIDADES Y DESAFÍOS — PARA LAS **PYMES** EN EL — CONTEXTO DE UNA MAYOR ADOPCIÓN DE LAS TICs

CRÉDITOS

Luis Almagro

Secretario General
Organización de los Estados Americanos (OEA)

Equipo técnico de OEA

Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Nathalia Foditsch
Kerry-Ann Barrett
Bárbara Marchiori de Assis
Gonzalo García-Belenguer
Mariana Cardona

Equipo técnico de AWS

Min Hyun
Michael South
Maria Saab

OPORTUNIDADES Y DESAFÍOS — PARA LAS **PYMES** EN EL — CONTEXTO DE UNA MAYOR ADOPCIÓN DE LAS TICs

CONTENIDO

OPORTUNIDADES Y DESAFÍOS — PARA LAS **PYMES** EN EL — CONTEXTO DE UNA MAYOR ADOPCIÓN DE LAS TICs

Resumen Ejecutivo

Empresas de diferentes tamaños y sectores están dependiendo cada vez más de las Tecnologías de la Información y la Comunicación (TIC), y esto ha sido clave para la innovación, la productividad y el crecimiento. A pesar de los innumerables beneficios y oportunidades, surgen retos cuando se adoptan las TICs, y las pequeñas y medianas empresas (PYME) generalmente enfrentan mayores desafíos que las que encaran las compañías más grandes. El tener una infraestructura de TIC pobre, no saber cómo abordar adecuadamente las complejas amenazas de seguridad cibernética, o subestimar la importancia de la protección de los datos personales son ejemplos de los desafíos para las PYME. Este libro blanco pretende, por consiguiente, describir brevemente algunas de las dificultades que sufren las PYME al adoptar, cada vez más, las TIC. También atiende reparos cruciales relacionadas con la protección y privacidad de los datos personales, y la importancia de realizar algunos cambios institucionales que permitan la creación de una cultura "consciente de la seguridad". También explica los diferentes roles que desempeñan los gobiernos como posibilitadores de un ecosistema saludable, como cuando se usan las normas de contratación como un medio para fomentar la adopción de estándares de seguridad cibernética, o cuando se promueven gestiones de creación de capacidades centradas en las PYME. Por último, en los penúltimos párrafos se describen algunas medidas sencillas que pueden tomar las PYME cuando se trata de fortalecer su preparación para la seguridad cibernética.

1 OPORTUNIDADES Y DESAFÍOS PARA LAS PYME EN EL CONTEXTO DE UNA MAYOR ADOPCIÓN DE LAS TICs

Existen pequeñas y medianas empresas (PYME) en todas partes en las Américas. Se trata tanto de la panadería de su barrio, la tienda de bicicletas de propiedad familiar, el proveedor local de Internet, como de la empresa de diseño de software. Son reconocidas por su impacto positivo en las sociedades y se consideran "esenciales para lograr una globalización y un crecimiento más incluyentes" (OCDE, 2017, p.5), ya que han demostrado ser fundamentales para el desarrollo social y económico de los países. Las nuevas empresas (startups), organizaciones "formadas para buscar un modelo comercial repetible y escalable" (Blank, 2010), también se han vuelto populares en las Américas con el transcurso de los años[1]. Si bien pueden variar las contribuciones de tales emprendimientos entre empresas, países y sectores, diferentes estudios sugieren que son fundamentales para aliviar la pobreza y crear empleos (por ejemplo Deijl et al., 2013; Lopez-Acevedo & Tan, 2011).

Este mayor papel de las PYME se basa en gran medida en su creciente dependencia de Internet y las Tecnologías de la Información y la Comunicación (TIC), que les permiten aprovechar la economía mundial, así como fortalecer los procesos, la eficiencia e innovar. De hecho, las startup dependen en gran medida de las TICs, que representan nuevos modelos de creación de conocimiento, innovación y promoción de una cultura empresarial. Las nuevas empresas en América Latina, por ejemplo, han atraído inversiones que se han más que duplicado en los últimos cinco años, aunque estas cifras son aún más bajas que las encontradas en otras regiones emergentes globales (Ruvolo, 2018). Un ejemplo del crecimiento del uso de las TICs por parte de estas organizaciones es el aumento desenfrenado de las startup de nuevas tecnologías financieras (Fintech) en los países de América Latina y el Caribe[2] en los últimos años. En la actualidad hay cientos en la región, haciendo uso de plataformas en línea e impulsando el acceso a crédito de otras PYME (BID y Finnovista, 2017)[3].

A pesar de desempeñar tal papel mayor, las PYME enfrentan desafíos específicos cuando se comparan con empresas más grandes, tales como mayores obstáculos para la innovación y el acceso a redes de investigación y esquemas de patentes (Zuniga et al., 2016). Los retos relacionados con el acceso a instrumentos financieros también se han planteado en diferentes estudios (OCDE, 2017; Zuniga et al., 2016). De hecho, la deficiente "infraestructura de TIC impide que las PYME operen de manera eficiente y accedan a mercados internacionales a costos competitivos" (OCDE, 2017, p.12). Pero lo que se ve afectada no es solo la competitividad y la eficiencia cuando no están instaladas la infraestructura, las habilidades y el gobierno correctos. La cuestión de la seguridad también es

[1] Si bien las PYME y las nuevas empresas no son lo mismo, ya que tienen diferencias como los métodos de financiación y la escalabilidad, ambos modelos son más pequeños que las empresas más grandes y pueden tener desafíos similares relacionados con la seguridad cibernética, la protección de la privacidad y datos. Por lo tanto, el término "PYME" se usa indistintamente en este documento.
[2] Unos ejemplos de segmentos populares de Fintech son: plataformas financieras alternativas; soluciones de pago; gestión financiera empresarial; y gestión financiera personal. Brasil, México, Argentina, Colombia y Chile son los países de la región con más empresas Fintech (BID y Finnovista, 2017).
[3] Como lo señala Cathles (2014), en los países de América Latina y el Caribe hay una falta de "indicadores de emprendimiento oportunos sobre la demografía empresarial" (p.22), ya que solo se puede encontrar "información parcial sobre el emprendimiento" (p.24) en la región.

importante y ha llamado mucho la atención en los últimos años, ya que han sido muy frecuentes los ataques cibernéticos a las PYME. Estas podrían enfrentar pérdidas, con mayores costos per cápita, si se las compara con empresas más grandes. Hay que tener en cuenta que muchas PYME aún no están bien informadas sobre cómo abordar el problema (Zec & Kajtazi, 2015).

Con el transcurso de los años, los desafíos que enfrentan las compañías en la lucha contra los riesgos cibernéticos han cambiado a medida que han evolucionado los tipos de riesgos. En la primera década del nuevo milenio, las organizaciones enfrentaron desafíos como los programas espía (spyware) y la detección de "suplantación de identidad (phishing) automática", así como la detección de sitios intermediarios de derivación (proxy bypass websites), pero ahora son comunes retos más complejos como la detección de suplantación de identidad dirigido a un objetivo (spear phishing) (Symantec, 2018). Amenazas más audaces como el secuestro de archivos a cambio de un rescate (ransomware) incluso pueden infectar la organización e introducir mecanismos de limpieza para cubrir sus huellas (Bitdefender, 2017, p.2). De hecho, de acuerdo con PwC (2018), la mayor preocupación de los directores generales en Estados Unidos es enfrentar las amenazas cibernéticas.

Además del aumento en complejidad de las amenazas, la seguridad cibernética debe analizarse desde diferentes dimensiones. Se ha establecido una amplia variedad de definiciones de la seguridad cibernética, pero muchas de estas no son integrales y tampoco tan interdisciplinarias como deberían ser (Craigen et al., 2014). Como se explica brevemente a continuación, con el transcurso de los años, ha evolucionado la comprensión de la seguridad cibernética, y ahora no solo incluye las actividades y violaciones puramente técnicas, sino también diferentes tipos de aprovechamientos y usos de datos no autorizados. De hecho, la protección de los datos personales y la privacidad de los datos[4] también son parte del desafío para la mayoría de los tipos de negocios.

[4] Diferentes marcos regulatorios tratan los "datos personales" de manera diferente de otros tipos de datos. Si bien el concepto no se ha aplicado por igual en todos los países, generalmente se refiere a los datos que permiten identificar personalmente a una persona.

LAS PYME, LA PROTECCIÓN DE LOS DATOS PERSONALES Y LA PRIVACIDAD DE DATOS

2

Desde cuando se revelaron las actividades de vigilancia internacional a países extranjeros[5] en 2013, varios países de la región comenzaron a analizar o a crear marcos de políticas destinadas a proteger los datos personales y la privacidad, y ha aumentado la conciencia relacionada con los riesgos cibernéticos (Maciel et al., 2016). Por lo tanto, la seguridad puede entenderse de manera más amplia, abarcando también aspectos relacionados con la protección de datos, y las PYME deben comprender cómo se deben recopilar, almacenar, extraer, usar y proteger los datos.

La legislación relacionada con la protección de los datos personales y la privacidad no es nueva en las Américas, ya que han existido en diferentes países de la región por más de treinta años (Cerda, 2012). Sin embargo, en operación hay diferentes marcos, con diferentes niveles de madurez. Por ejemplo, la mayoría de los países de las Américas no cuentan con una autoridad de protección de datos personales, y los únicos países de las Américas que son signatarios de la "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" son Argentina, México y Uruguay[6]. Dado este escenario, no existe un nivel mínimo de estándares de protección de datos o privacidad que deba garantizarse en todos los países de las Américas. Sin embargo, esto no significa que las PYME no deban tomar en serio la protección de los datos personales y la privacidad, ni en mayor medida la seguridad cibernética. De hecho, al contar con un nivel sólido de protección, las PYME crean ventajas competitivas y se fortalece la confianza.

No solo puede verse afectada la confianza por una mala gestión de la protección y privacidad de los datos personales, sino que incluso podría verse afectado el ciclo de ventas o podrían producirse pérdidas financieras en caso de violación. Según CISCO (2018), el ciclo de ventas de las empresas puede verse profundamente afectado por las inquietudes sobre la privacidad de los datos del consumidor. A su vez, las organizaciones que se consideran "maduras en materia de privacidad" tienen menos probabilidades de tener retrasos en su ciclo de ventas o pérdidas por violación de datos. Además, se encontró que las empresas con un modelo de organización de privacidad híbrida (en comparación con un modelo centralizado o descentralizado) tenían menos probabilidades de enfrentar retrasos en las ventas (CISCO, 2018). Como podemos ver, las PYME también deben intentar crear un modelo de gobernanza que genere impactos positivos en los temas relacionados con la seguridad cibernética.

Además de la gobernanza de la empresa, los productos y servicios mismos pueden idearse de modo que cuenten con protecciones "desde el diseño", un concepto amplio que incluye diferentes aspectos, como se explica en el recuadro a continuación.

[5] Estas revelaciones mostraron que Estados Unidos había vigilado países extranjeros. De hecho, las revelaciones mostraron que "la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) y otras agencias estadounidenses de aplicación de la ley y seguridad nacional han utilizado disposiciones de la Ley de Vigilancia de Inteligencia Extranjera (FISA, por sus siglas en inglés) y la Ley Patriotica de Estados Unidos (USA PATRIOT Act) para obtener datos electrónicos de terceros" (Castro, 2013, p.1). Clarke et al. (2013) argumentaron que "las inquietudes extranjeras sobre la vigilancia estadounidense pueden reducir directamente la participación de mercado de las empresas de tecnología con sede en EE. UU. Además pueden tener un efecto indirecto para la justificación de medidas proteccionistas" (p. 212).

[6] Consulte el "Cuadro de firmas y ratificaciones del Tratado 108", disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=wWwV2sLp

RECUADRO #1 Privacidad desde el diseño

El concepto de "privacidad desde el diseño" existe desde hace varios años y es clave para la seguridad de los datos. En general, se refiere a incorporar la privacidad en las tecnologías de la información, las prácticas comerciales y las infraestructuras en red, como una funcionalidad central, desde su gestación -que significa incluir la privacidad desde el principio- intencionalmente, con previsión (Cavoukian, 2012, p. 39).

Los propietarios de negocios pueden poner en práctica este concepto de diferentes maneras, incluido el desarrollo de software que incorpora requisitos de privacidad tales como la minimización de la recopilación de datos, el uso de procesos de desidentificación o el uso de "cifrado por defecto"[7] (Cavoukian, 2012). Debido a la gran cantidad de datos que las PYME pueden recopilar, extraer y almacenar, la implementación de protecciones de privacidad es más importante que nunca, pero también más difícil que nunca. Por ejemplo, varios modelos de negocio se basan en "grandes datos" y "migas de pan digitales que van quedando atrás por el uso de tecnologías por parte del usuario y que más tarde se vuelven a usar para analizarlos" (D'Acquisto et al., 2015, p.22). Por esta razón, minimizar la recopilación de datos y proteger los datos personales mientras se permite que los datos se transformen, usen y analicen de forma que sean útiles y valiosos para los sectores público y privado son un desafío importante.

Algunos marcos regulatorios contienen reglas relacionadas expresamente con "privacidad desde el diseño". El Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), por ejemplo, que entró en vigor en la Unión Europea en 2018, ha establecido expectativas sobre la "privacidad desde el diseño" y también afirma que "por defecto, solo se deben procesar los datos personales que sean necesarios para cada propósito específico de procesamiento"[8]. De hecho, tales requisitos deberán seguirse cuando las empresas estén celebrando contratos públicos, según se describe más adelante en este documento.

A pesar del hecho de que el aumento de la protección de la seguridad cibernética y de la privacidad se hayan vuelto medidas progresivamente importantes en los últimos años, no todas las PYME son plenamente conscientes de los beneficios de implementarlas, o a veces carecen de recursos y capacidades para hacerlo.

[7] Consulte el estudio de caso "Using Encryption by Default" de New America Foundation, disponible en https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-1-using-transit-encryption-default/

[8] Artículo 25, numeral 2, GDPR: "El responsable del tratamiento aplicará las medidas técnicas y organizacionales apropiadas para garantizar que, por defecto, solo se procesen los datos personales que sean necesarios para cada fin específico del procesamiento. Esa obligación se aplica a la cantidad de datos personales recopilados, el alcance de su procesamiento, el período de su almacenamiento y su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles sin la intervención de la persona a un número indefinido de personas naturales".

SENSIBILIZACIÓN DE LA SEGURIDAD CIBERNÉTICA Y LAS PYME

3

El nivel de conocimiento y preparación con respecto a la seguridad cibernética y la privacidad varía ampliamente según la PYME. Mientras que es posible que algunas hayan entendido y adoptado las medidas para proteger sus recursos y capacidades implementadas, otras tal vez no hayan implementado ninguna. De hecho, parte de esta problemática se debe a la falta de "cultura de seguridad", definida como "actitudes, creencias y percepciones compartidas por los miembros del grupo, que definen normas y valores que, a su vez, determinan la forma en que actúan y reaccionan respecto al riesgo y al sistema de control de riesgos" (Lopes y Oliveira, 2014, p. 278). La falta de una cultura de seguridad puede resultar en que entre las PYME haya una comprensión limitada de la seguridad, y estas tienden a implementar medidas que protegen las capas físicas y lógicas de sus redes pero subestiman el componente humano, como capacitar a los empleados y supervisar el cumplimiento (Lopes and Oliveira, 2014).

Si se necesita fortalecer la cultura de seguridad entre las PYME, ¿qué se debe hacer al respecto? Un tema importante es, sin duda, crear conciencia y capacitar a los empleados. Beyer et. al. (2015) plantean que "actualmente, la seguridad no forma parte de los contratos psicológicos en la mayoría de las organizaciones" (p.8) y explican algunos de los puntos clave relacionados con las campañas de sensibilización, como la eliminación de tareas de seguridad que no son realistas, el enfoque en lograr cambios de comportamiento y hacer que los empleados participen progresivamente. El aspecto humano de la seguridad cibernética no debe subestimarse, por lo tanto, y estas son algunas de las maneras en que se puede fortalecer. Un estudio empírico que intentó comprender los aspectos organizativos, tecnológicos y psicológicos de la seguridad cibernética en las PYME encontró que una gran mayoría de los empleados (dos tercios) no informaron sobre sus errores a sus superiores (Zec & Kajtazi, 2015)[9]. Además, la "ausencia de políticas cibernéticas internas en las PYME" y las "bajas inversiones financieras" también fueron factores que pusieron a las PYME en una posición vulnerable (Zec y Kajtazi, 2015, p.237). En otro estudio empírico, Burgurcu et al. (2010) descubrieron que se puede mejorar la seguridad de la información si se crea una cultura "consciente de la seguridad" al interior de la organización, y que recompensas como reconocer la "confiabilidad, reputación y buena imagen" (p. 544) de los empleados que cumplen con las reglas de seguridad pueden tener un impacto positivo en la forma en que los empleados perciben el beneficio de dicho cumplimiento, mejorando sus comportamientos y actitudes. Dado que los empleados perciben las gestiones de cumplimiento como fastidiosas, se podría mitigar esta apreciación por medio de la asignación de una cantidad de tiempo ininterrumpida, a los empleados en sus rutinas, a gestiones de concientización y cumplimiento, y simplificación de procedimientos (Bulgurcu et al., 2010; Lopes y Oliveira, 2014). Además, se podrían incluir desarrollos tecnológicos que permitan que algunas tareas se automaticen fácilmente, algo que las PYME también deberían considerar al evaluar las opciones.

[9] Si bien muchos de ellos podrían no tener la intención de ocultar sus errores, parece que el aspecto humano de las organizaciones es importante cuando se evalúan las vulnerabilidades de las empresas. Zec y Kajtazi (2015) también sugirieron que deberían tenerse en cuenta los rasgos de personalidad cuando se seleccionen profesionales para asumir roles relacionados con la seguridad de la información (por ejemplo, proponen que aquellos con mayor "propensión a la culpa" deberían ser mejores en tener segura a la compañía)

Según PwC (2018), el número de miembros de la Junta que supervisa los riesgos de seguridad y privacidad es menos de un tercio, una realidad que se espera que cambie, dado que las inquietudes sobre seguridad y privacidad tienen un impacto directo en los resultados y, por consiguiente, en la rentabilidad de las empresas. Por otra parte, la contratación de un ejecutivo cuyo principal deber es ser responsable de supervisar la privacidad y la seguridad en la empresa es una tendencia que ahora se encuentra comúnmente en las grandes organizaciones. De hecho, dos tercios de las compañías "Fortune 1000" ya han asignado un "Director de datos" o "Director de privacidad", aunque hay evidente confusión y desacuerdo sobre la autoridad y la importancia de sus roles (NewVantage Partners, 2018, p.8). La existencia de dicho profesional, también conocido como "Director de información" (CIO), todavía no es una tendencia extendida en organizaciones más pequeñas (PwC, 2018), pero es probable que este escenario cambie a medida que más organizaciones se familiaricen con los desafíos y oportunidades que llegan con las nuevas tecnologías.

Como se demostró anteriormente, cada organización individual es responsable de su negocio, así como de asegurar los datos que acumula, almacena y usa. No obstante, los gobiernos también pueden ser clave en el fomento de un ecosistema propicio para la seguridad. Dicha función se describe brevemente a continuación.

EL PAPEL DEL GOBIERNO EN LA PROMOCIÓN DE UN ECOSISTEMA DE SEGURIDAD CIBERNÉTICA SALUDABLE PARA LAS PYME

4

El sector privado "actúa como un laboratorio para identificar, desarrollar e implementar las mejores prácticas de seguridad cibernética que se aprovechan para la formulación de políticas nacionales e internacionales" (Shackelford et al., 2015, p.360). Las PYME, aunque forman parte de este grupo, podrían no tener todos los recursos técnicos, humanos y financieros necesarios para comprender a cabalidad las medidas de seguridad cibernética y privacidad que necesitan adoptar, implementar y usar. Por esta razón, existe un papel que deben desempeñar los gobiernos de las Américas para apoyar la creación de un ecosistema de seguridad cibernética saludable para las PYME.

Como lo demuestra Mazzucato (2013), es un error suponer que el estado no desempeña un papel en el avance de las tecnologías, ya que algunas de las principales empresas de tecnología se han beneficiado en gran medida de las políticas gubernamentales dirigidas a permitir que se tomaran riesgos. Ella destacó el papel de las políticas descentralizadas y "orientadas a la misión", como las que llevaron a la creación de tecnologías como Internet, la World Wide Web, la tecnología de comunicación celular y el GPS que también se desarrollaron con el apoyo de fondos públicos (Mazzucato, 2013). El tema de la seguridad trae consigo nuevos desafíos para los gobiernos, que ahora enfrentan el reto no solo de fomentar la creación y adopción de tales tecnologías, sino también de apoyar un ecosistema saludable que priorice las necesidades de seguridad cibernética. La sensibilización sobre el tema, la creación de capacidades y otras intervenciones más directas, como el establecimiento de normas mínimas de seguridad para la seguridad cibernética en la contratación pública, son algunas de las formas en que se juega este papel, como se describe brevemente a continuación.

Las gestiones de contratación pública se han utilizado como una forma de fomentar la justicia social y el cambio social por décadas (McCrudden 2006 y 2007). Un ejemplo es el aumento en la disponibilidad de dispositivos accesibles fomentados a través de la contratación pública, que se ha realizado en diferentes países como Estados Unidos, Japón, Canadá y el Reino Unido y ha tenido un impacto positivo en las personas con discapacidad (Tibben y Astbrink, 2012). Con la seguridad cibernética no es diferente, ya que algunos países han establecido reglas encaminadas a garantizar que la contratación pública respete los requisitos mínimos relacionados con la seguridad cibernética.

RECUADRO #2 La contratación pública se utiliza como una forma de fomentar un ecosistema de seguridad cibernética saludable.

El Reglamento General de Protección de Datos (GDPR), que entró recientemente en vigencia en Europa como se describió anteriormente, es un ejemplo de un marco que incluye reglas relacionadas con contratos gubernamentales que involucran el procesamiento de datos personales. Debido a esto, "los organismos gubernamentales deberán revisar y llevar a cabo la diligencia debida sobre los contratos existentes y futuros bajo los cuales se procesa la información personal" (Tucker, 2018).

En Estados Unidos, algunas de las reglamentaciones relacionadas con los requisitos de seguridad cibernética en la contratación pública se han probado incluso a nivel administrativo. El Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) ha establecido, por ejemplo, que "los requisitos de seguridad se aplican a todos los componentes de los sistemas no federales y organizaciones que procesan, almacenan o transmiten información controlada no clasificada o que brindan protección de seguridad para dichos componentes", requisitos que están "destinados a ser utilizados por agencias federales en vehículos contractuales u otros acuerdos establecidos entre esas agencias y organizaciones no federales" (SP 800-171 Rev. 1)[10]. Reynolds (2018) señala que tales reglas incluso han sido impugnadas a nivel administrativo, ya que la Oficina para la Responsabilidad Gubernamental de EE. UU. ha emitido dos decisiones relacionadas con la aplicación de dichas reglas. De hecho, se espera que haya "más agencias que incorporen explícitamente requisitos de seguridad cibernética en convocatorias" y "oferentes que no demuestren un cumplimiento total podrán ser descalificados por ser técnicamente inaceptables o bajados de categoría en la evaluación" (Reynolds, 2018).

En algunos casos, razones de seguridad justifican la contratación directa en contratación pública de acuerdo con los marcos legales y regulatorios en diferentes países de las Américas. Algunos ejemplos son Argentina, Bolivia, Brasil, Chile, Costa Rica, Guyana, Honduras, Jamaica, Panamá y Perú, donde las consideraciones de seguridad son "circunstancias especiales" que podrían "hacer que un proceso competitivo sea una imposibilidad práctica" (Benavides et al., 2016, p 48). Con seguridad cibernética podría no ser diferente, y es posible predecir ocasiones en las que podría justificarse la contratación

[7] NIST. SP 800-171 Rev. 1 https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

directa de empresas, ya que los beneficios de mantener un nivel de referencia de seguridad cibernética podrían superar las reducciones de costos de productos y servicios que no tienen en cuenta la seguridad cibernética. Si bien las PYME deben esforzarse por cumplir con los estándares de seguridad cibernética[11], los gobiernos deberían apoyarlos para que tomen las medidas correctas. Se podrían desarrollar o modificar las normas de contratación pública para ofrecer incentivos a las PYME que optan por adoptar y cumplir dichas normas. Además, se podría desarrollar un enfoque escalonado en el que se les solicite a las empresas de diferentes tamaños que cumplan con diferentes niveles de seguridad cibernética para evitar sobrecargar a las empresas más pequeñas.

El papel del gobierno también podría implicar la creación de capacidades y esfuerzos de concientización, una demanda que fue destacada en un estudio conjunto publicado por la OEA, el Banco Interamericano de Desarrollo y el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia en 2017 (OAS et al., 2017), así como las políticas correspondientes a intervenciones más directas[12]. Los programas gubernamentales destinados a apoyar a las PYME ya existen y han demostrado ser valiosos para apoyar un ecosistema favorable para las PYME. Una evaluación de los programas de apoyo a las PYME en cuatro países latinoamericanos (Chile, Colombia, México y Perú) encontró impactos positivos estadísticamente significativos de dichos programas, especialmente con respecto a las ventas y el desempeño empresarial (López-Acevedo y Tan, 2011). Por ejemplo, la participación en programas dirigidos a las PYME en Chile, como programas de redes empresariales y programas de promoción de exportaciones, se asoció con mejoras positivas en el corto y mediano plazo, y en Colombia, las PYME que se beneficiaron de un fondo gubernamental fueron impactadas positivamente en cuanto a exportaciones e inversión en I+D (Lopez-Acevedo & Tan, 2011). Las políticas dirigidas a los esfuerzos de desarrollo de capacidades también pueden implicar el desarrollo de contenido y conocimiento, así como de cursos y programas de capacitación que pueden ser útiles para las PYME. Dichos contenidos pueden ser desarrollados por las autoridades públicas solas o en asocio con empresas privadas que cuenten con experiencia en seguridad cibernética. Las iniciativas de creación de capacidad y concienciación pueden estar dirigidas, por ejemplo, a desarrollar herramientas de sensibilización y alinear campañas nacionales (GFCE, 2017)[13].

El papel del gobierno es extenso, como se describió anteriormente. A pesar de que los gobiernos han estado desempeñando un papel activo y, en muchos casos, han servido como un pilar fundamental para el éxito de las PYME, aún hay mucho por hacer. Tal escenario resulta especialmente cierto si se tiene en cuenta que la adopción de nuevas tecnologías, aunado a un aumento en cantidad de datos recopilados, minados, almacenados y utilizados por las empresas está creciendo a un ritmo exponencial.

Si se comprende el escenario descrito anteriormente, los gobiernos tienen la posibilidad no solo de proteger a las PYME, sino de fomentar un ecosistema más seguro, en el que es probable que surjan la confianza y la prosperidad económica. Es posible concluir, por lo tanto, que los sectores privado y público tienen un papel que desempeñar. De hecho, cada PYME también debería hacer esfuerzos concretos para crear un ecosistema seguro, y hay medidas que estas pueden tomar para fortalecer su preparación para la seguridad cibernética, algunas de las cuales se describen a continuación.

[11] Las PYME deben, por ejemplo, examinar los requisitos establecidos por las normas oficiales de seguridad cibernética, como el Marco de seguridad cibernética del Instituto Nacional de Estándares y Tecnología (NIST); los informes de control de organización de servicio (SOC, por sus siglas en inglés) y la norma de la seguridad cibernética de la Organización Internacional de Normalización (ISO, por sus siglas en inglés). Cada una tiene diferentes características y corresponde a una metodología diferente.

[12] Algunos ejemplos de tales esfuerzos son los realizados por el Departamento de Seguridad Nacional de Estados Unidos, como el "Mes nacional de concientización sobre seguridad cibernética", que "es una campaña anual para crear conciencia sobre la importancia de la seguridad cibernética". STOP.THINK. CONNECT.™ es otro esfuerzo de sensibilización liderado por una coalición de partes interesadas públicas y privadas, así como unas ONG que ayudan a "las personas a comprender no solo los riesgos que conlleva Internet, sino también la importancia de practicar un comportamiento seguro en línea". Consulte más información en https://www.dhs.gov/national-cyber-security-awareness-month y en www.stopthinkconnect.org/.

[13] La "Agenda Global para la Creación de Capacidad Cibernética" de 2017 desarrollada por el Foro Global sobre Experticia Cibernética (GFCE) ha identificado diferentes iniciativas relacionadas con la creación de capacidad y la concientización (GFCE, 2017)

MEDIDAS ACTIVAS QUE LAS PYME PUEDEN ADOPTAR PARA REFORZAR SU SEGURIDAD CIBERNÉTICA 5

Teniendo en cuenta los desafíos y las oportunidades descritas anteriormente, las PYME pueden adoptar diferentes medidas para fortalecer su preparación para la seguridad cibernética. La siguiente lista brinda orientación sobre cuáles son algunas de estas medidas importantes:

1. **Seleccione un empleado que se encargue de todos los aspectos relacionados con la privacidad y la protección de datos y la seguridad cibernética.**
Esta persona debe estar completamente dedicada a estas tareas, si es posible. Si tal compromiso no es posible debido a restricciones presupuestarias, asegúrese de que una persona sea responsable, al menos a tiempo parcial, y capacítelo/la adecuadamente. Un factor importante es seleccionar a una persona con habilidades y personalidad adecuadas, ya que el rol exige atención y conocimiento cuidadosos.

2. **Cree una cultura "consciente de la seguridad" al interior de su PYME.**
Las políticas internas, las campañas de sensibilización y los programas de desarrollo de capacidades son algunas de las formas de lograr este objetivo. Se pueden crear diferentes programas para diferentes tipos de empleados, pero todos deben tener un nivel mínimo de conocimiento de los problemas relacionados con la importancia de la seguridad cibernética. Además, evite interrumpir o sobrecargar a los empleados y deles suficiente tiempo para realizar estas sesiones de capacitación;

3. **Diseñe productos y servicios integrados con protección de privacidad y datos personales**
(lea más arriba sobre los conceptos de "privacidad desde el diseño" y "privacidad por defecto"). Esta no es solo una práctica socialmente responsable, sino que ayuda a evitar la responsabilidad potencial relacionada con la seguridad y la privacidad. Además, las empresas que tienen tales diseños integrados en sus negocios principales tienen ventajas competitivas que podrían dar sus frutos; have competitive advantages that might pay off;

4. **Busque recursos disponibles, especialmente las gestiones gubernamentales para apoyar las PYME.** Además, hay muchos recursos disponibles en línea que se pueden analizar cuidadosamente. Dada la naturaleza del tema, es necesario un esfuerzo constante para actualizar el conocimiento y las habilidades;

5. **Cumpla con las normas oficiales de seguridad cibernética y protección de datos y los requisitos de contratación pública.** Si no existen tales requisitos, comuníqueles a los legisladores y formuladores de políticas que estas deben implementarse. Es del interés de todos tener un ecosistema empresarial y gubernamental saludable y seguro.

REFERENCIAS 6

• Benavides, J. L., M'Causland Sánchez, M. C., Flórez Salazar, C., & Roca, M. E. (2016). Public Procurement in Latin America and the Caribbean and IDB-financed Projects - A Normative and Comparative Study. Inter-American Development Bank.

• Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M. A., & Passingham, N. (2015). Awareness is only the first step. A framework for progressive engagement of staff in cyber security. Retrieved from https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf

• Bitdefender. (2017). The Global Threat Landscape Report - 2017. Retrieved from https://download.bitdefender.com/resources/files/News/CaseStudies/study/181/Bitdefender-Business-2017-Whitepaper-threat-landscape-crea2186-en-EN-GenericUse.pdf

• Blank, S. (2010). What's A Startup? First Principles. Retrieved April 3, 2018, from https://steveblank.com/2010/01/25/whats-a-startup-first-principles/

• Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34, 523–548.

• Castro, D. (2013). How Much Will PRISM Cost the U.S. Cloud Computing Industry? (p. 9). ITIF. Retrieved from http://www2.itif.org/2013-cloud-computing-costs.pdf

• Cathles, A. (2014). Entrepreneurship Data for Latin America and the Caribbean -What Is There and What Is Missing? Inter-American Development Bank. Retrieved from https://publications.iadb.org/bitstream/handle/11319/6744/CTI_TN_Enterpreneurship_Data_for_Latin_America_and_the_Caribbean.pdf

• Cavoukian, A. (2012). Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices. Information and Privacy Commissioner of Ontario. Retrieved from http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf

• Cerda Silva, A. (2012). Protección de datos personales y prestación de servicios en línea en América Latina. In Hacia una Internet Libre de Censura: propuestas para América Latina I (Eduardo Bertoni). Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Facultad de Derecho de la Universidad de Palermo. Retrieved from http://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf

• CISCO. (2018). Privacy Maturity Benchmark Study. CISCO. Retrieved from https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/privacy-maturity-benchmark-study-2018.pdf

• Clarke, R., Morell, M., Stone, G., Sunstein, C., & Swire, P. (2013). Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. White House Review Group on Intelligence and Communications Technologies. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

• Cook, K. (2017). Effective Cyber Security Strategies for Small Businesses. Walden Dissertations and Doctoral Studies. Retrieved from http://scholarworks.waldenu.edu/dissertations/3871

• Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, (4(10)), 13–21.

• D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., Montjoye, Y.-A. de, & Bourka, A. (2015). Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. European Union Agency For Network And Information Security (ENISA).

• Deijl, C., de Kok, J., & Veldhuis-Van Essen, C. (2013). Is Small Still Beautiful? Literature Review of Recent Empirical Evidence on the Contribution of SMEs to Employment Creation. Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH. Retrieved from http://lup.lub.lu.se/record/cfac576e-a5c4-4802-b5f3-7989d9bffd46

• GFCE. (2017). Global Agenda for Cyber Capacity Building. Retrieved from https://www.thegfce.com/documents/publications/2017/11/20/gfce-global-agenda

• IDB, & Finnovista. (2017). Fintech: Innovations you may not know were from Latin America and the Caribbean. Inter-American Development Bank and Finnovista. Retrieved from https://publications.iadb.org/bitstream/handle/11319/8265/FINTECH-Innovations-You-May-Not-Know-are-from-latin-America-and-the-Caribbean.pdf?sequence=7&isAllowed=y

• Lopes, I., Oliveira, P. (2014). Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises. In. Rocha Á., Correia A., Tan F., Stroetmann K. (eds) New Perspectives in Information Systems and Technologies, Volume 1. Advances in Intelligent Systems and Computing, vol 275. Springer, Cham . Lopez-Acevedo, G., & Tan, H. W. (2011). Impact evaluation of small and medium enterprise programs in Latin America and the Caribbean (No. 61641) (pp. 1–146). The World Bank. Retrieved from http://documents.worldbank.org/curated/en/587801468183890334/Impact-evaluation-of-small-and-medium-enterprise-programs-in-Latin-America-and-the-Caribbean

• Maciel, M., Foditsch, N., Belli, L., & Castellon, N. (2016). Cybersecurity, Privacy and Trust: Trends in Latin America and the Caribbean. In 2016 Cybersecurity Report. OAS / IDB.

• Mazzucato, M. (2013). The Entrepreneurial State: Debunking Public vs. Private Sector Myths. Anthem.

• McCrudden, C. (2006). Corporate Social Responsibility and Public Procurement (SSRN Scholarly Paper). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=899686

• McCrudden, C. (2007). Buying Social Justice: Equality, Government Procurement, and Legal Change. Oxford University Press. Retrieved from http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199232420.001.0001/acprof-9780199232420

• NewVantage Partners, (NVP). (2018). Big Data Executive Survey 2018 - Executive Summary of Findings. Retrieved from http://newvantage.com/wp-content/uploads/2018/01/Big-Data-Executive-Survey-2018-Findings-1.pdf

• OAS, IDB, & MINTIC. (2017). Impact of Digital Security Incidents in Colombia 2017. Retrieved from http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

• OECD. (2017a). Active with Latin America and the Caribbean. Retrieved from http://www.oecd.org/global-relations/Active-with-Latin-America-and-the-Caribbean.pdf

• OECD. (2017b). Enhancing the Contributions of SMEs in a Global and Digitalised Economy (Meeting of the OECD Council at Ministerial Level). Paris. Retrieved from https://www.oecd.org/mcm/documents/C-MIN-2017-8-EN.pdf

• PwC. (2018). Revitalizing privacy and trust in a data-driven world - Key findings from The Global State of Information Security Survey 2018 (p. 23). Retrieved from https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf

• Reynolds, T. (2018, January). Top Five Government Contractor Cybersecurity Considerations for 2018. Retrieved from http://govcon.mofo.com/defense/top-five-government-contractor-cybersecurity-considerations-for-2018/

• Ruvolo, J. (2018, February 28). Global tech firms and investors are reshaping Latin America's startup environment. TechCrunch. Retrieved from http://social.techcrunch.com/2018/02/27/global-tech-firms-and-investors-are-reshaping-latin-americas-startup-environment/

• Shackelford, S., Fort, T. L., & Prenkert, J. D. (2015). How Businesses Can Promote Cyber Peace. University of Pennsylvania Journal of International Law, 36(2). https://doi.org/10.2139/ssrn.2393528

• Symantec. (2018). Rethinking Security for the Cloud GenerationWelcome to the Cloud Generation. Retrieved from https://www.symantec.com/theme/cloud-generation

• Tibben, W., & Astbrink, G. (2012). Government ICT Purchasing: What differences do accessibility criteria make for people with disabilities? University of Wollongong and GSA Information Consultants. Retrieved from http://accan.org.au/index.php?option=com_content&view=article&id=495:government-ict-purchasing-what-differences-do-accessibility-criteria-make-for-people-with-disabilities&catid=98:access-for-all&Itemid=234

• Tucker, I. (2018, January). Government procurement prepares for GDPR. Retrieved from https://www.lexology.com/library/detail.aspx?g=4cbf7ab3-2082-44d3-a41e-f2edc4537d48

• Zec, M., & Kajtazi, M. (2015). Examining how IT Professionals in SMEs Take Decisions About Implementing Cyber Security Strategy. In The European Conference on Information Systems Management; Reading (pp. 231–239). Reading, United Kingdom, Reading: Academic Conferences International Limited. Retrieved from https://search-proquest-com.proxyau.wrlc.org/docview/1776778140/abstract/1F1546EA8CF452FPQ/1

• Zuniga, P., Negri, F. de, Dutz, M., & Rauen, A. (2016). Conditions for Innovation in Brazil: a review of key issues and policy challenges. IPEA, (218), 110.

OPORTUNIDADES Y DESAFÍOS — PARA LAS **PYMES** EN EL — CONTEXTO DE UNA MAYOR ADOPCIÓN DE LAS TICs

OPORTUNIDADES Y DESAFÍOS — PARA LAS **PYMES** EN EL — CONTEXTO DE UNA MAYOR ADOPCIÓN DE LAS TIC

OEA Más derechos para más gente | aws

White paper series
Edición 3

2018