2018

White paper series
Publicação 3

OPORTUNIDADES E DESAFIOS — PARA AS **PMEs** NO — CONTEXTO DE UMA MAIOR ADOÇÃO DAS TIC

OEA | Mais direitos para mais pessoas

aws

OPORTUNIDADES E DESAFIOS — PARA AS **PME** NO — CONTEXTO DE UMA MAIOR **ADOÇÃO DAS TIC**

CRÉDITOS

Luis Almagro

Secretário Geral
Organização dos Estados Americanos (OEA)

Equipe Técnica da OEA

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

Equipe técnica da AWS

Min Hyun
Michael South
Maria Saab

OPORTUNIDADES E DESAFIOS — PARA AS **PME** NO — CONTEXTO DE UMA MAIOR **ADOÇÃO DAS TIC**

CONTEÚDO

1 OPORTUNIDADES E DESAFIOS PARA AS PME NO CONTEXTO DE UMA MAIOR ADOÇÃO DAS TIC 8

2 AS PMES, A PROTEÇÃO DOS DADOS PESSOAIS E A PRIVACIDADE DE DADOS 10

11 QUADRO #1: "Privacidade desde o design"

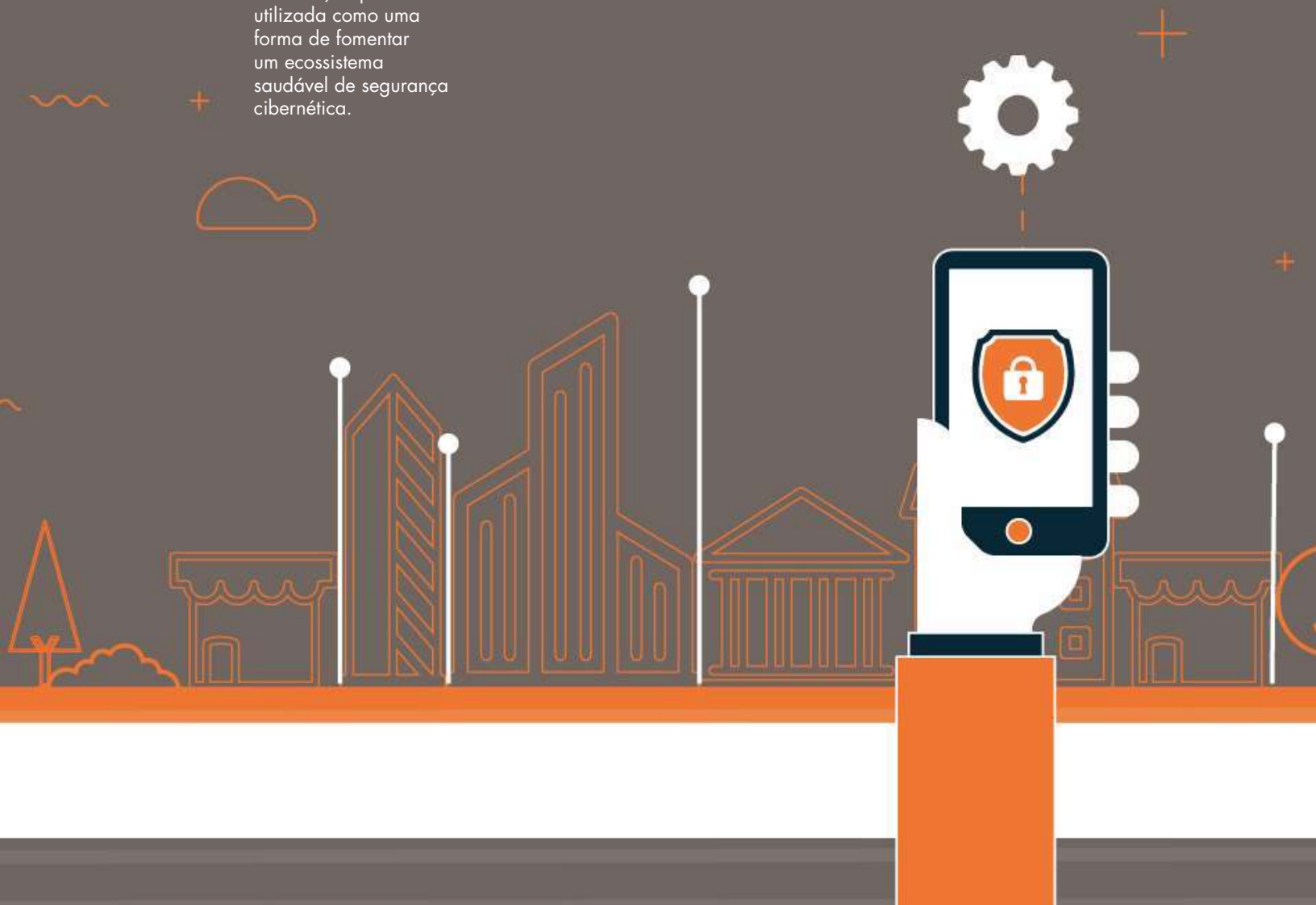
3 AS PMES E A CONSCIENTIZAÇÃO A RESPEITO DE SEGURANÇA CIBERNÉTICA 12

4 O PAPEL DO GOVERNO NA PROMOÇÃO DE UM ECOSSISTEMA DE SEGURANÇA CIBERNÉTICA SAUDÁVEL PARA AS PMES 14

5 MEDIDAS ATIVAS QUE AS PME PODEM ADOTAR PARA REFORÇAR SUA SEGURANÇA CIBERNÉTICA 17

6 REFERÊNCIAS 18

14 QUADRO #2: A contratação pública utilizada como uma forma de fomentar um ecossistema saudável de segurança cibernética.



OPORTUNIDADES E DESAFIOS — PARA AS **PME** NO — CONTEXTO DE UMA MAIOR **ADOÇÃO DAS TIC**

RESUMO EXECUTIVO

Empresas de portes e setores diversos estão dependendo cada vez mais das Tecnologias da Informação e Comunicação (TIC), e isto tem sido fundamental para a inovação, produtividade e crescimento. Apesar dos inúmeros benefícios e oportunidades, desafios surgem quando da adoção das TIC, e as pequenas e médias empresas (PMEs) geralmente enfrentam desafios maiores que os enfrentados pelas grandes companhias. Contar com uma infraestrutura de TIC desatualizada, não saber como abordar adequadamente as complexas ameaças de segurança cibernética, ou subestimar a importância da proteção dos dados pessoais são exemplos de desafios para as PME.

Considerando tais desafios, este documento oficial pretende descrever brevemente algumas das dificuldades que as PMEs experimentam ao adotar, cada vez mais, as TIC. Também trata de dificuldades cruciais relacionadas com a proteção e privacidade dos dados pessoais e a importância de se fazer algumas alterações institucionais que permitam a criação de uma cultura "consciente de segurança". Ademais, explica os diferentes papeis desempenhados pelos governos como fomentadores de um ecossistema saudável, como quando do uso das normas de contratação como meio de fomento à adoção de padrões de segurança cibernética, ou da promoção de capacitação focada nas PMEs. Por último, nos penúltimos parágrafos são descritas algumas medidas simples para as PMEs no que se refere a sua preparação para a segurança cibernética.

1 OPORTUNIDADES E DESAFIOS PARA AS PME NO CONTEXTO DE UMA MAIOR ADOÇÃO DAS TIC

Existem pequenas e médias empresas (PMEs) em todos os lugares das Américas. Trata-se, por exemplo, da padaria do seu bairro, da loja de bicicletas de propriedade familiar, do provedor de serviço de Internet local, ou da empresa de design de software. PMEs reconhecidas por seu impacto positivo nas sociedades e consideradas "essenciais para a obtenção de uma globalização e de um crescimento mais inclusivo" (OCDE, 2017, p.5), já que comprovaram serem fundamentais para o desenvolvimento social e econômico dos países. Outro tipo de empresas, as startups, que são organizações "que buscam um modelo de negócios replicável e escalável" (Blank, 2010), também se tornaram populares nas Américas no decorrer dos anos[1]. Embora as contribuições de tais empreendimentos possam variar entre empresas, países e setores, diferentes estudos sugerem que são fundamentais para aliviar a pobreza e gerar empregos (Veja, por exemplo, Deijl et al, 2013; Lopez-Acevedo & Tan, 2011).

Este importante papel exercido pelas PMEs está baseado, em grande medida, em sua crescente dependência da Internet e das Tecnologias da Informação e Comunicação (TICs), que lhes permitem aproveitar a economia mundial, bem como fortalecer os processos, a eficiência e a inovação. As startups, principalmente, se apoiam bastante nas TICs, trazendo novos modelos de criação de conhecimento e de cultura empresarial.

Na América Latina, por exemplo, as startups atraíram investimentos que mais que dobraram nos últimos cinco anos, embora essas cifras sejam ainda mais baixas que as verificadas em outras regiões emergentes no mundo (Ruvolo, 2018). Um exemplo do crescimento do uso das TIC por parte destas organizações é o notável aumento das startups de novas tecnologias financeiras (Fintech) nos países da América Latina e Caribe[2] nos últimos anos. Atualmente há centenas na região, fazendo uso de plataformas online e provendo acesso a crédito às PMEs (BID y Finnovista, 2017)[3].

Apesar de desempenharem esse importante papel, as PMEs enfrentam desafios específicos quando comparadas com empresas maiores, tais como, maiores obstáculos para a inovação e acesso a redes de pesquisa e de patenteamento (Zuniga et al., 2016). Os desafios relativos ao acesso a instrumentos financeiros também foram apresentados em distintos estudos (OCDE, 2017; Zuniga et al, 2016). De fato, a deficiente "infraestrutura de TICs impede que as PMEs operem de forma eficiente e tenham acesso a mercados internacionais a custos competitivos" (OCDE, 2017, p.12). Mas não é só a competitividade e a eficiência que são afetadas quando não estão instaladas a infraestrutura, as capacidades e administração corretas. A questão da segurança também é importante e tem chamado muito a atenção nos últimos anos, já que os ataques

[1] Embora os conceitos de PMEs e de startups não sejam equivalentes, já que existem diferenças quanto a métodos de financiamento e à escalabilidade, ambos os modelos se tratam de empresas menores que as grandes empresas e que podem enfrentar desafios semelhantes relacionados com a segurança cibernética, a proteção da privacidade e dados. Portanto, neste documento o termo "PME" é utilizado indistintamente.
[2] Alguns exemplos de segmentos populares de Fintech são: plataformas financeiras alternativas; soluções de pagamento; gestão financeira empresarial; e gestão financeira pessoal. O Brasil, o México, a Argentina, a Colômbia e o Chile são os países da região com mais empresas Fintech (BID e Finnovista, 2017).
[3] Como indica Cathles (2014), nos países da América Latina e do Caribe há uma falta de "indicadores de empreendimento oportunos sobre a demografia empresarial" (p.22), já que só é possível encontrar "informação parcial sobre o empreendimento" (p.24) na região.

cibernéticos às PMEs têm sido muito frequentes, e que estas enfrentam perdas com maiores custos per capita, se comparados aos enfrentados por empresas maiores. Há de se considerar, ainda, que muitas PMEs ainda não estão bem informadas sobre como enfrentar o problema (Zec & Kajtazi, 2015).

Com o transcurso dos anos, os desafios enfrentados pelas companhias na luta contra os riscos cibernéticos mudaram à medida que os tipos de risco evoluíam. Na primeira década do novo milênio, as organizações enfrentaram desafios como os programas-espião (spyware) e a detecção de usurpação de identidade (phishing), bem como a detecção de sites intermediários de derivação (proxy bypass websites), mas agora são comuns desafios mais complexos, como a detecção de usurpação de identidade direcionada a um objetivo (spear phishing) (Symantec, 2018). Ameaças mais audazes, como o sequestro de arquivos em troca de um resgate (ransomware), podem até infectar a organização e introduzir mecanismos de limpeza pra esconder as evidências deixadas (Bitdefender, 2017, p.2). De fato, de acordo com a PwC (2018), a maior preocupação dos diretores gerais nos Estados Unidos é enfrentar ameaças cibernéticas.

Além do aumento na complexidade das ameaças, a segurança cibernética deve ser analisada desde diferentes aspectos. Foi estabelecida uma ampla variedade de definições da segurança cibernética, mas muitas delas não são completas e, tampouco tão interdisciplinares como deveriam ser (Craigen et al, 2014). Como explicado brevemente a seguir, com o decorrer dos anos a compreensão da segurança cibernética evoluiu, e agora não só inclui atividades e violações puramente técnicas, mas também diferentes tipos de aproveitamento e uso de dados não autorizados. De fato, a proteção dos dados pessoais e a privacidade dos dados[4] também são parte do desafio para a maioria dos tipos de negócios.

[4] Distintos marcos regulatórios tratam os "dados pessoais" de forma diferente à de outros tipos de dados. Embora o conceito não tenha sendo aplicado igualmente em todos os países, geralmente se refere a dados que permitem identificar individualmente uma pessoa.

AS PMES, A PROTEÇÃO DOS DADOS PESSOAIS E A PRIVACIDADE DE DADOS

2

Desde que foram reveladas as atividades de vigilância internacional a países estrangeiros[5] em 2013, vários países das Américas começaram a analisar ou criar marcos de políticas destinadas a proteger os dados pessoais e a privacidade, e a consciência relacionada aos riscos cibernéticos vem aumentado (Maciel et al, 2016). De fato, a segurança pode ser entendida de maneira mais ampla, abrangendo também aspectos relacionados com a proteção de dados, e as PME precisam entender como os dados devem ser recopilados, armazenados, extraídos, utilizados e protegidos.

A legislação relacionada com a proteção dos dados pessoais e privacidade não é nova nas Américas, já que existe em diversos países da região há mais de trinta anos (Cerda, 2012). No entanto, há em operação diferentes marcos, com diferentes níveis de maturidade. Por exemplo, a maioria dos países das Américas ainda não conta com uma autoridade de proteção aos dados pessoais, e os únicos países das Américas signatários do "Convênio para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal" são a Argentina, o México e o Uruguai[6]. Dado este cenário, não existe um nível mínimo de padrões de proteção de dados ou privacidade que deva ser garantido em todos os países das Américas. Entretanto, isto não significa que as PME não devam levar o tema a sério. De fato, contando com um nível sólido de proteção as PME criam vantagens competitivas e a confiança é fortalecida.

Não apenas a confiança pode ser afetada por uma má gestão da proteção e privacidade dos dados pessoais, como também o ciclo de vendas poderia ser afetado, ou perdas financeiras poderiam ocorrer em caso de violação. De acordo com a CISCO (2018), o ciclo de vendas das empresas pode ser profundamente afetado por problemas relacionados à privacidade dos dados do consumidor. Por sua vez, as organizações que se consideram "maduras em matéria de privacidade" têm menos probabilidades de sofrer atrasos em seu ciclo de vendas ou perdas por violação de dados. Ademais, verificou-se que empresas com um modelo organizacional híbrido de privacidade (em comparação com um modelo centralizado ou descentralizado) tinham menos probabilidades de enfrentar atrasos em vendas (CISCO, 2018). Como podemos ver, as PME também devem tentar criar um modelo de governança que gere impactos positivos em temas relacionados à segurança cibernética.

Além da governança da empresa, os próprios produtos e serviços podem ser idealizados contendo proteções de privacidade desde a sua concepção, o que se costuma chamar de "privacy by design", um conceito amplo que inclui diversos aspectos, como explicado no quadro abaixo:

[5] Estas revelações mostraram que os Estados Unidos haviam vigiado países estrangeiros. De fato, as revelações mostraram que "a Agência de Segurança Nacional (NSA, por suas siglas em inglês) e outras agências estadunidenses de aplicação da lei e segurança nacional utilizaram disposições da Lei de Vigilância de Inteligência Estrangeira (FISA, por suas siglas em inglês) e a Lei Patriótica dos Estados Unidos (USA PATRIOT Act) para obter dados eletrônicos de terceiros" (Castro, 2013, p.1). Clarke et al. (2013) argumentaram que "as inquietudes estrangeiras sobre a vigilância estadunidense podem reduzir diretamente a participação de mercado das empresas de tecnologia com sede nos Estados Unidos. Ademais, podem ter um efeito indireto para justificação de medidas protecionistas" (p. 212).

[6] Consulte o "Quadro de assinaturas e ratificações do Tratado 108", disponível em https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=wWwV2sLp

QUADRO #1 Privacidade desde o design

o conceito de "privacy by design" existe há vários anos e é fundamental para a segurança dos dados. Em geral, se refere à "incorporação da privacidade nas tecnologias da informação, práticas comerciais e infraestruturas em rede, como uma funcionalidade central, desde sua concepção - que significa incluir a privacidade desde o princípio-intencionalmente, como prevenção" (Cavoukian, 2012, p. 39).

Os proprietários de negócios podem colocar em prática este conceito de diversas maneiras, incluído o desenvolvimento de software que incorpore requisitos de privacidade, tais como, a minimização da coleta de dados, o uso de processos de desidentificação ou a utilização de "criptografia padrão"[7] (Cavoukian, 2012). Devido à grande quantidade de dados que podem ser coletados, extraídos e armazenados pelas PMEs, a implementação de proteções de privacidade é mais importante que nunca, mas também é mais difícil que nunca. Por exemplo, vários modelos de negócio se baseiam em "big data" e "rastros digitais que vão ficando para trás pela utilização de tecnologias por parte do usuário e que mais tarde são usadas novamente para analisá-los" (D'Acquisto et al, 2015, p.22). Por esta razão, é um desafio importante minimizar a coleta de dados e proteger os dados pessoais enquanto se permite que os dados sejam transformados, usados e analisados de forma que sejam úteis e valiosos para os setores público e privado.

Alguns marcos regulatórios contêm regras relacionadas expressamente com "privacy by design". O Regulamento Geral de Proteção de Dados (GDPR, por suas siglas em inglês), por exemplo, que entrou em vigor na União Europeia em 2018, estabeleceu expectativas sobre o tema e também afirma que "por padrão, só devem ser processados os dados pessoais necessários a cada propósito específico de processamento"[8]. De fato, tais requisitos deverão ser seguidos quando as empresas estiverem celebrando contratos públicos, conforme descrito mais adiante neste documento.

Apesar do fato de que o aumento da proteção da segurança cibernética e da privacidade se tornaram medidas progressivamente importantes nos últimos anos, nem todas as PMEs têm plena consciência dos benefícios de implementá-las, ou às vezes carecem de recursos e capacidades para fazê-lo.

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

[8] Artigo 25, numeral 2, GDPR: "O responsável pelo tratamento aplicará as medidas técnicas e organizacionais adequadas para garantir que, por padrão, sejam processados apenas os dados pessoais necessários para cada finalidade específica do processamento. Essa obrigação é aplicada à quantidade de dados pessoais recopilados, abrangência de seu processamento, período de armazenamento e sua acessibilidade. Em particular, tais medidas garantirão que, por padrão, os dados pessoais não sejam acessíveis sem a intervenção da pessoa a um número indefinido de pessoas naturais".

AS PMES E A CONSCIENTIZAÇÃO A RESPEITO DE SEGURANÇA CIBERNÉTICA

3

O nível de conhecimento e preparação em relação à segurança cibernética e à privacidade varia amplamente conforme a PME. Enquanto é possível que algumas tenham entendido e adotado as medidas para proteger seus recursos e capacidades implementadas, outras talvez não tenham implementado nenhuma. De fato, parte desta problemática se deve à falta de "cultura de segurança", definida como "atitudes, crenças e percepções compartilhadas pelos membros do grupo, que definem normas e valores que, por sua vez, determinam a forma em que atuam e reagem em relação ao risco e ao sistema de controle de riscos" (Lopes y Oliveira, 2014, p. 278). A falta de uma cultura de segurança pode resultar que entre as PMEs exista uma compreensão limitada acerca da segurança e elas implementem medidas de proteção a camadas físicas e lógicas de suas redes, mas subestimem o componente humano, como o treinamento dos empregados e a supervisão do cumprimento às regras de segurança estabelecidas (Lopes e Oliveira, 2014).

Se for necessário fortalecer a cultura de segurança entre as PMEs, o que deve ser feito a respeito? Um tema importante é, sem dúvida, criar consciência e treinar os empregados. Beyer et al. (2015) propõem que "atualmente, a segurança não faz parte dos contratos psicológicos na maioria das organizações" (p.8) e explicam alguns dos pontos-chave relacionados com as campanhas de sensibilização, como a eliminação de tarefas de segurança que não são realistas, o enfoque para obter mudanças de comportamento e como fazer que os empregados participem mais ativamente. O aspecto humano da segurança cibernética não deve, portanto, ser subestimado, e há maneiras por meio das quais ele pode ser fortalecido. Um estudo empírico que pretendeu compreender os aspectos organizacionais, tecnológicos e psicológicos da segurança cibernética nas PMEs detectou que uma grande maioria dos empregados (dois terços) não informaram seus superiores a respeito de seus erros (Zec & Kajtazi, 2015)[9].

Além disso, a "ausência de políticas cibernéticas internas nas PME" e os "baixos investimentos financeiros" também foram fatores que colocaram as PME em uma posição vulnerável (Zec y Kajtazi, 2015, p.237). Em outro estudo empírico, Burgurcu et al (2010) verificaram que é possível melhorar a segurança da informação quando se cria uma cultura "consciente da segurança" dentro da organização, e que recompensas como o reconhecimento da "confiabilidade, reputação e boa imagem" (p. 544) dos empregados que cumprem as regras de segurança podem ter um impacto positivo na forma em que eles percebem o beneficio de tal cumprimento, melhorando seus comportamentos e atitudes. Dado que os empregados percebem as gestões de cumprimento como enfadonhas, seria possível mitigar esta percepção através da atribuição de um período de tempo ininterrupto aos empregados, dentro de suas rotinas, para gestões de conscientização e cumprimento, e simplificação de procedimentos

[9] Embora muitos deles poderiam não ter a intenção de ocultar seus erros, parece que o aspecto humano das organizações é importante quando avaliadas as vulnerabilidades das empresas. Zec y Kajtazi (2015) também sugeriram que deveriam ser considerados os traços de personalidade quando se da seleção de profissionais para assumirem funções relacionadas com a segurança da informação (por exemplo, propõem que aqueles com maior "propensão à culpa" deveriam ser melhores em manter a companhia segura)

(Bulgurcu et al, 2010; Lopes y Oliveira, 2014). Além disso, poderiam ser incluídos desenvolvimentos tecnológicos que permitam que algumas tarefas sejam automatizadas facilmente, algo que as PME também deveriam considerar ao avaliar as opções.

De acordo com a PwC (2018), o número de de conselhos de diretores que supervisiona os riscos de segurança e privacidade é inferior a um terço, uma realidade que se espera que mude, dado que as inquietudes sobre segurança e privacidade têm um impacto direto nos resultados e, por conseguinte, na rentabilidade das empresas. Por outro lado, a contratação de um executivo cujo principal dever é responsabilizar-se pela supervisão da privacidade e da segurança da empresa é agora uma tendência observada nas grandes organizações. De fato, dois terços das companhias "Fortune 1000" já alocaram um "Chief Data Officer" ou "Chief Privacy Officer", embora haja evidente confusão e desacordo quanto à autoridade e importância de suas funções (NewVantage Partners, 2018, p.8). A existência de tal profissional, também conhecido como "Chief Information Officer" (CIO), ainda não é frequente em organizações menores (PwC, 2018), mas é provável que este cenário mude à medida que mais organizações se familiarizem com os desafios e oportunidades que chegam com as novas tecnologias.

Como demonstrado anteriormente, cada organização individual é responsável por seu negócio, bem como por assegurar os dados que colhe, armazena e utiliza. Não obstante, os governos também podem ser fundamentais no fomento de um ecossistema propício para a segurança. Tal função é brevemente descrita a seguir.

O PAPEL DO GOVERNO NA PROMOÇÃO DE UM ECOSSISTEMA DE SEGURANÇA CIBERNÉTICA SAUDÁVEL PARA AS PMES

4

O setor privado "atua como um laboratório para identificar, desenvolver e implementar as melhores práticas de segurança cibernética que são aproveitadas para a formulação de políticas nacionais e internacionais" (Shackelford et al, 2015, p.360). As PMEs, embora façam parte deste grupo, poderiam não dispor de todos os recursos técnicos, humanos e financeiros necessários para compreender completamente as medidas de segurança cibernética e privacidade que precisam adotar, implementar e utilizar. Por esta razão, existe um papel que os governos das Américas devem desempenhar para apoiar a criação de um ecossistema de segurança cibernética saudável para as PME.

Como demonstrado por Mazzucato (2013), é um erro supor que o estado não desempenha um papel no avanço das tecnologias, pois algumas das principais empresas de tecnologia se beneficiaram em grande medida das políticas governamentais dirigidas a permitir que assumissem riscos. Ela destacou o papel das políticas descentralizadas e "orientadas à missão", como as que levaram à criação de tecnologias como Internet, a World Wide Web, a tecnologia de comunicação celular e o GPS, que também foram desenvolvidos com o apoio dos fundos públicos (Mazzucato, 2013). O tema da segurança traz consigo novos desafios aos governos, que agora não apenas enfrentam o desafio de fomentar a criação e adoção de tais tecnologias, mas também o de apoiar um ecossistema saudável que priorize as necessidades de segurança cibernética. A sensibilização sobre o tema, a criação de capacidades e outras intervenções mais diretas, como o estabelecimento de normas mínimas de segurança cibernética na contratação pública, são algumas das formas em que desempenha este papel, como descrito brevemente a seguir.

Contratações públicas têm sido utilizadas como forma de fomentar a justiça social e a mudança social há décadas (McCrudden 2006 y 2007). Um exemplo é o aumento na disponibilidade de dispositivos acessíveis fomentados através da contratação pública, realizada em diversos países como os Estados Unidos, o Japão, o Canadá e o Reino Unido, que causaram um impacto positivo para pessoas com deficiência (Tibben y Astbrink, 2012). Com a segurança cibernética não é diferente, pois alguns países estabeleceram regras orientadas a garantir que a contratação pública respeite os requisitos mínimos relacionados de segurança cibernética.

QUADRO #2

A contratação pública utilizada como uma forma de fomentar um ecossistema saudável de segurança cibernética.

O Regulamento Geral de Proteção de Dados (GDPR) que recentemente entrou em vigor na Europa, como foi descrito anteriormente, é exemplo de um marco que inclui regras relacionadas com contratos governamentais que envolvem o processamento de dados pessoais. Devido a isto, "os organismos governamentais deverão revisar e realizar a due diligence dos contratos existentes e futuros sob os quais a informação pessoal é processada" (Tucker, 2018).

Nos Estados Unidos, algumas das regulamentações relacionadas com os requisitos de segurança cibernética na contratação pública foram provadas inclusive em nível administrativo. O Instituto Nacional de Padrões e Tecnologia (NIST, por suas siglas em inglês) estabeleceu, por exemplo, que "os requisitos de segurança são aplicados a todos os componentes dos sistemas não federais e organizações que processam, armazenam ou transmitem informação controlada não classificada que proporcionam proteção de segurança para tais componentes", requisitos que estão "destinados a serem utilizados por agências federais em veículos contratuais ou outros acordos estabelecidos entre essas agências e organizações não federais" (SP 800-171 Rev. 1)[10]. Reynolds (2018) indica que tais regras foram inclusive impugnadas em nível administrativo, pois a Agência da Responsabilidade Governamental dos EEUU emitiu duas decisões relacionadas com a aplicação de tais regras. De fato, espera-se que haja "mais agências que incorporem explicitamente requisitos de segurança cibernética em convocatórias" e "licitantes que não demonstrem um cumprimento total poderão ser desclassificados por serem tecnicamente inaceitáveis ou rebaixados de categoria na avaliação" (Reynolds, 2018).

Em alguns casos, razões de segurança justificam a contratação direta em contratação pública, de acordo com os marcos legais e regulatórios de diferentes países das Américas. Alguns exemplos são a Argentina, a Bolívia, o Brasil, o Chile, a Costa Rica, a Guiana, Honduras, a Jamaica, o Panamá e o Peru, onde as considerações de segurança são "circunstâncias especiais" que poderiam "fazer com que um processo competitivo seja uma impossibilidade prática" (Benavides et al, 2016, p 48). Com a

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

segurança cibernética poderia não ser diferente, e é possível prever ocasiões nas quais poderia ser justificada a contratação direta de empresas, já que os benefícios de manter um nível de referencia de segurança cibernética poderiam superar as reduções de custos de produtos e serviços que não levam em conta a segurança cibernética. Embora as PMEs devam esforçar-se para cumprir os padrões de segurança cibernética[11], os governos deveriam apoiá-las para que tomem as medidas corretas. Seria possível desenvolver ou modificar as normas de contratação pública para oferecer incentivos para que as PMEs optem por adotar e cumprir tais normas. Além disso, seria possível desenvolver um enfoque escalonado no qual se solicite às empresas de diversos portes que atendam diferentes níveis de segurança cibernética para evitar sobrecarregar as empresas menores.

O papel do governo também poderia implicar a criação de capacidades e esforços de conscientização, uma demanda que foi destacada em um estudo conjunto publicado pelo OEA, o Banco Interamericano de Desenvolvimento e o Ministério de Tecnologias da Informação e Comunicações da Colômbia em 2017 (OAS et al, 2017), bem como políticas correspondentes a intervenções mais diretas[12]. Os programas governamentais destinados a apoiar as PMEs já existem e estão demonstrando serem valiosos para apoiar um ecossistema favorável para estas empresas. Uma avaliação dos programas de apoio das PMEs em quatro países latino-americanos (Chile, Colômbia, México e Peru) verificou impactos positivos estatisticamente significativos de tais programas, especialmente em relação às vendas e ao desempenho empresarial (López-Acevedo y Tan, 2011). Por exemplo, a participação em programas dirigidos às PMEs no Chile, como programas de redes empresariais e programas de promoção de exportações, foi associada a melhoramentos positivos em curto e médio prazo, e na Colômbia, as PMEs que se beneficiaram de um fundo governamental foram positivamente impactadas quanto a exportações e investimento em pesquisa e devenvolvimento. (Lopez-Acevedo & Tan, 2011).

As políticas dirigidas aos esforços de desenvolvimento de capacidades também podem implicar o desenvolvimento de conteúdo e conhecimento, bem como de cursos e programas de treinamento que podem ser úteis para as PMEs. Tais conteúdos só podem ser desenvolvidos pelas autoridades públicas ou em associação com empresas privadas que contem com experiência em segurança cibernética. As iniciativas de criação de capacidade e conscientização podem estar dirigidas, por exemplo, para o desenvolvimento de ferramentas de sensibilização e para alinhar campanhas nacionais (GFCE, 2017)[13].

O papel do governo é extenso, como foi descrito anteriormente. Apesar de que os governos têm desempenhado um papel ativo e, em muitos casos, têm servido como um pilar fundamental para o sucesso das PMEs, ainda há muito por fazer. Tal cenário resulta ser especialmente acertado quando se considera que a adoção de novas tecnologias, em conjunto com o aumento na quantidade de dados recopilados, minados, armazenados e utilizados pelas empresas, vem crescendo a um ritmo exponencial.

Se o cenário descrito anteriormente for compreendido, os governos têm a possibilidade de não só proteger as PMEs, mas de fomentar um ecossistema mais seguro, no qual é provável o surgimento da confiança e da prosperidade econômica. É possível concluir, portanto, que os setores privado e público têm um papel a desempenhar. De fato, cada PME também deveria fazer esforços concretos para criar um ecossistema seguro, e há medidas que estas podem tomar para fortalecer sua preparação para a segurança cibernética, algumas das quais estão descritas a seguir.

[11] As PME devem, por exemplo, examinar os requisitos estabelecidos pelas normas oficiais de segurança cibernética, como o Marco de Segurança Cibernética do Instituto Nacional de Padrões e Tecnologia (NIST); os relatórios de controle de organização de serviço (SOC, por suas siglas em inglês) e a norma da segurança cibernética da Organização Internacional de Normalização (ISO, por suas siglas em inglês). Cada uma possui características diferentes e correspondem a uma metodologia diferente.

[12] Alguns exemplos de tais esforços são os realizados pelo Departamento de Segurança Nacional dos Estados Unidos, como o "Mês nacional de conscientização sobre segurança cibernética", que "é uma campanha anual para a criação de consciência sobre a importância da segurança cibernética". STOP.THINK. CONNECT.™ é outro esforço de sensibilização liderado por uma coalizão de partes interessadas públicas e privadas, bem como algumas ONGs que ajudam "as pessoas a compreender não apenas os riscos que a Internet implica, mas também a importância de praticar um comportamento seguro online". Veja maiores informações em https://www.dhs.gov/national-cyber-security-awareness-month e em www.stopthinkconnect.org/.

[13] A "Agenda Global para a Criação de Capacidade Cibernética" de 2017, desenvolvida pelo Fórum Global em Perícia Cibernética (GFCE), identificou diferentes iniciativas relacionadas com a criação de capacidade e conscientização (GFCE, 2017)

MEDIDAS ATIVAS QUE AS PME PODEM ADOTAR PARA REFORÇAR SUA SEGURANÇA CIBERNÉTICA

5

Levando em conta os desafios e as oportunidades descritas anteriormente, as PMEs podem adotar diferentes medidas para fortalecer sua preparação para a segurança cibernética. A seguinte lista proporciona orientação sobre quais são algumas destas medidas importantes:

1. **Selecione um empregado que se encarregue de todos os aspectos relacionados com a privacidade e a proteção de dados e segurança cibernética.**
Se possível, esta pessoa deve estar completamente dedicada a estas tarefas. Se não houver possibilidade de tal compromisso devido a restrições orçamentárias, assegure-se de que uma pessoa seja responsável, pelo menos em tempo parcial, e treine-o(a) adequadamente. Um fator importante é selecionar uma pessoa com habilidades e personalidade adequadas, já que a função exige atenção e conhecimento cuidadosos;

2. **Crie uma cultura "consciente da segurança" dentro de sua PME.**
As políticas internas, as campanhas de sensibilização e os programas de desenvolvimento de capacidades são algumas das formas de atingir este objetivo. É possível criar diferentes programas para diferentes tipos de empregados, mas todos devem ter um nível mínimo de conhecimento dos problemas relacionados com a importância da segurança cibernética. Além disso, evite interromper ou sobrecarregar os empregados e dê a eles tempo suficiente para realizar estas sessões de treinamento;

3. **Elabore produtos e serviços integrados com proteção de privacidade e dados pessoais**
(leia mais acima sobre conceitos tais como "privacy by design"). Esta não é apenas uma prática socialmente responsável, mas também ajuda a evitar a potencial responsabilidade relacionada com a segurança e a privacidade. Além disso, as empresas que integram estes princípios em seus modelos de negócios, produtos e serviços têm vantagens competitivas que podem valer a pena.

4. **Busque recursos disponíveis, especialmente programas e políticas governamentais de apoio às PME**. Além disso, há muitos recursos disponíveis online que podem ser analisados cuidadosamente. Dada a natureza do tema, é necessário um esforço constante para atualização do conhecimento e habilidades;

5. **Adapte-se às normas oficiais de segurança cibernética, de proteção de dados e demais requisitos de contratação pública.** Se não existirem tais requisitos, informe aos legisladores e formuladores de políticas que estas devem ser implementadas. É de interesse de todos contar com um ecossistema empresarial e governamental saudável e seguro.

REFERÊNCIAS 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 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 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 E DESAFIOS — PARA AS **PME** NO — CONTEXTO DE UMA MAIOR **ADOÇÃO DAS TIC**

OPPORTUNITIES AND CHALLENGES FOR SMES IN THE CONTEXT OF INCREASED ADOPTION OF ICTS

OAS | More rights for more people

aws

White paper series

Issue 3

2018