COMO DEMOCRATIZAR O ACESSO DE MICRO E PEQUENAS EMPRESAS BRASILEIRAS A RESILIÊNCIA CIBERNÉTICA?

Larissa de Freitas Querino e
Ricardo Gonzaga Martins de Araújo

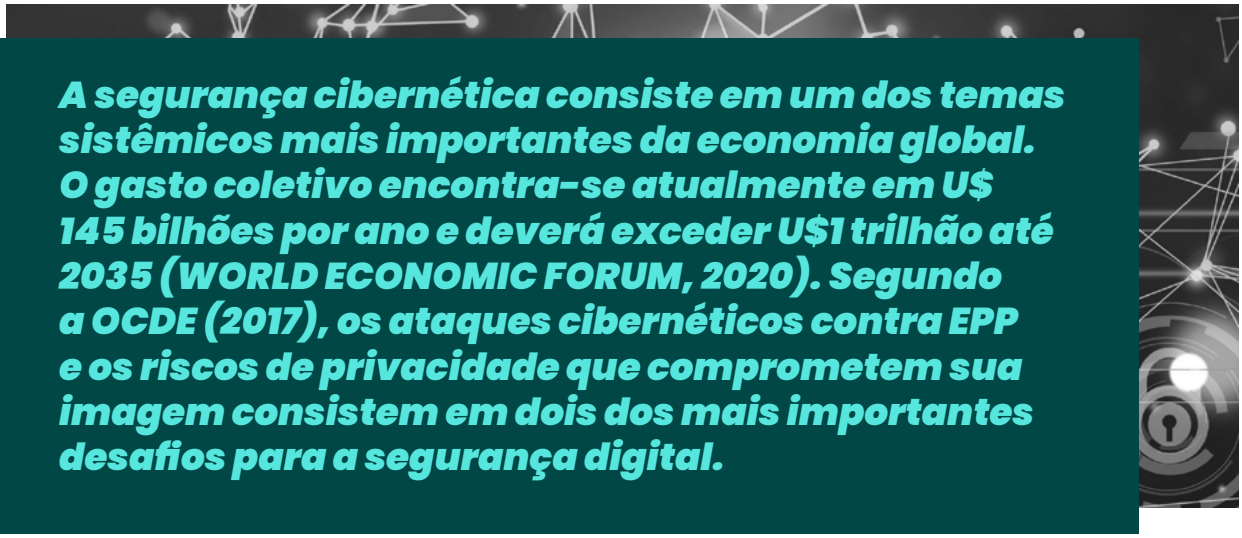
INTRODUÇÃO

O presente artigo procura discutir a importância da conscientização de micro e pequenas empresas acerca dos riscos cibernéticos e de privacidade para o setor produtivo, bem como as formas de democratização do acesso de microempresas (ME) e de empresas de pequeno porte (EPP) brasileiras a soluções – tecnológicas, de capacitação de recursos humanos e de gestão – que promovam o aumento da resiliência cibernética.

Conforme a OCDE (2017), ME e EPP são estruturas críticas para o crescimento econômico, uma vez que promovem competição e inovação, além de contribuir para a criação de empregos. Esses perfis de empresas enfrentam desafios distintos na gestão de segurança digital e de riscos de privacidade, que são prejudiciais para sua imagem. Por outro lado, as ME e EPP, conscientes do risco cibernético, podem demonstrar práticas robustas de gestão de segurança e privacidade digital e ter vantagens competitivas na busca de oportunidades de parcerias com organizações maiores.

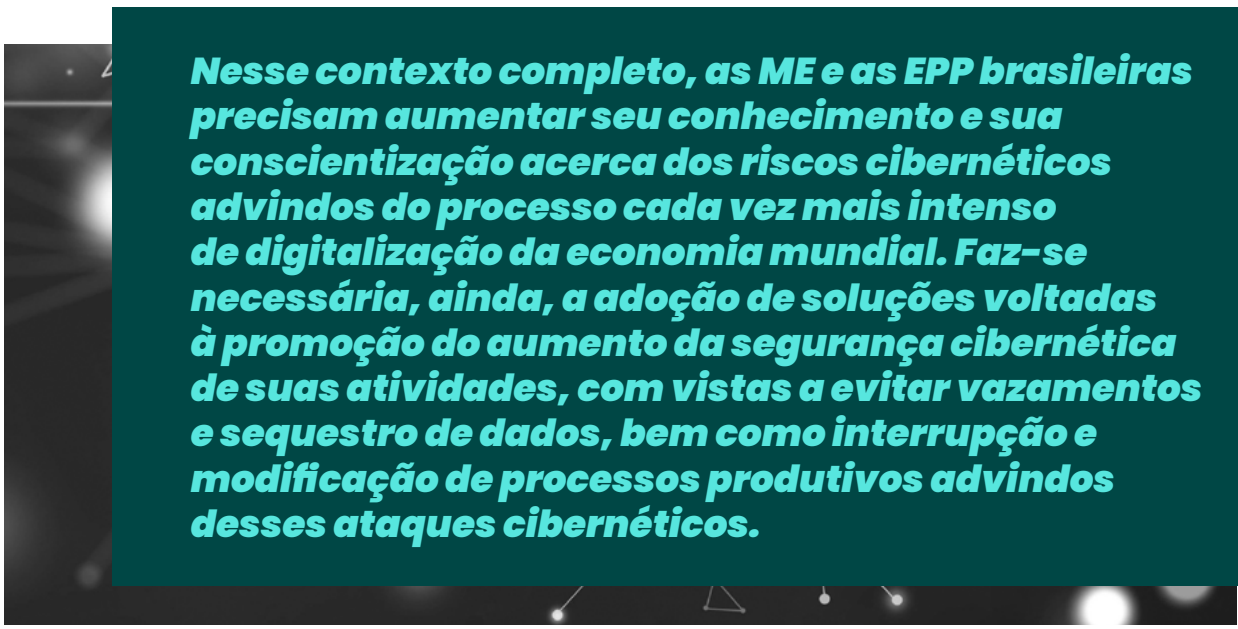
O processo de transformação digital da economia e da sociedade em nível mundial promove o aumento substantivo da utilização de redes interligadas de computadores e a transferência da gestão de processos produtivos para tais redes. Dessa forma, empresas, governos e cidadãos estão cada vez mais expostos a ataques em suas redes – caracterizados por sua sofisticação, especificidade e continuidade. Tais ataques impactam significativamente atividades sociais e econômicas.

Imagem: AdobeStock.com



A segurança cibernética consiste em um dos temas sistêmicos mais importantes da economia global. O gasto coletivo encontra-se atualmente em U$ 145 bilhões por ano e deverá exceder U$1 trilhão até 2035 (WORLD ECONOMIC FORUM, 2020). Segundo a OCDE (2017), os ataques cibernéticos contra EPP e os riscos de privacidade que comprometem sua imagem consistem em dois dos mais importantes desafios para a segurança digital.

Ademais, a Lei Geral de Proteção de Dados (Lei 13.709/2018), em vigor desde agosto de 2021, objetiva assegurar que os dados pessoais sejam tratados de forma a proteger a liberdade, a privacidade e o livre desenvolvimento das pessoas. Essa lei traz impactos significativos nas áreas jurídica, administrativa e de segurança da informação das organizações, uma vez que determina que empresas e órgãos públicos adaptem as formas de coletar, armazenar e utilizar os mencionados dados.



Nesse contexto completo, as ME e as EPP brasileiras precisam aumentar seu conhecimento e sua conscientização acerca dos riscos cibernéticos advindos do processo cada vez mais intenso de digitalização da economia mundial. Faz-se necessária, ainda, a adoção de soluções voltadas à promoção do aumento da segurança cibernética de suas atividades, com vistas a evitar vazamentos e sequestro de dados, bem como interrupção e modificação de processos produtivos advindos desses ataques cibernéticos.

A fim de contextualizar o presente artigo, tomaremos a seguir algumas definições ou compreensões acerca de conceitos a serem abordados, a saber, ataques cibernéticos e resiliência cibernética . Conforme a Accenture (2019), ataques cibernéticos consistem em atividades maliciosas conduzidas contra organizações, por meio de sua infraestrutura de Tecnologia da Informação, via redes internas, externas ou a internet. Incluem, ainda, ataques contra sistemas de controle industrial.

Já a resiliência cibernética pode ser entendida como a habilidade de sistemas cibernéticos de antecipar, de continuar a operar corretamente, de recuperar-se, de evoluir e de adaptar-se diante de ameaças cibernéticas (BODEAU et al, 2015). O termo remete à preparação e à adaptação às mudanças de condições, além das capacidades de resistência e de recuperação rápida diante de ataques cibernéticos. Dessa forma, pressupõem-se a manutenção de nível aceitável de serviço diante de várias falhas e desafios à operação normal (BODEAU et al, 2015).

Presso (2020)[1] define resiliência cibernética como

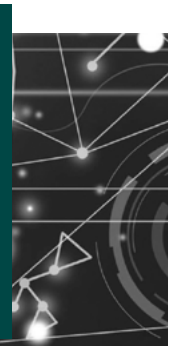
> *"um conjunto de métodos, práticas recomendadas e tecnologias que atenuam os riscos nos processos e fluxos de trabalho de negócios, a fim de proteger a organização. Devem abordar ameaças externas (hackers) e internas (funcionários mal-intencionados ou negligentes)".*

Essa resiliência nas empresas abrange o tripé tecnologia, pessoas e processos de governança, assim como define como lidar com um ataque, como manter os negócios operacionais durante a violação e a rapidez da evolução e do preparo para um eventual próximo incidente.

Portanto, o aumento da resiliência cibernética abrange fatores ligados à adoção de soluções de segurança da informação nas empresas, à qualificação constante de profissionais dedicados à segurança cibernética, à sensibilização e ao engajamento dos demais perfis profissionais da empresa, à adoção de processos de gestão interna para monitoramento de riscos e à definição de protocolo de respostas a incidentes.

Dessa forma, faz-se necessário despertar a consciência de pequenas empresas de todos os setores econômicos acerca dos riscos e dos potenciais impactos em seus negócios advindos de ataques cibernéticos que visam o roubo, o vazamento de dados e a interrupção de atividades.

É necessário também desenvolver a capacidade dessas empresas em lidar com os riscos dos ataques, por meio da democratização do acesso a soluções de prevenção, de detecção e de resposta a incidentes cibernéticos, assim como conscientizar sobre o uso ético e responsável de dados.



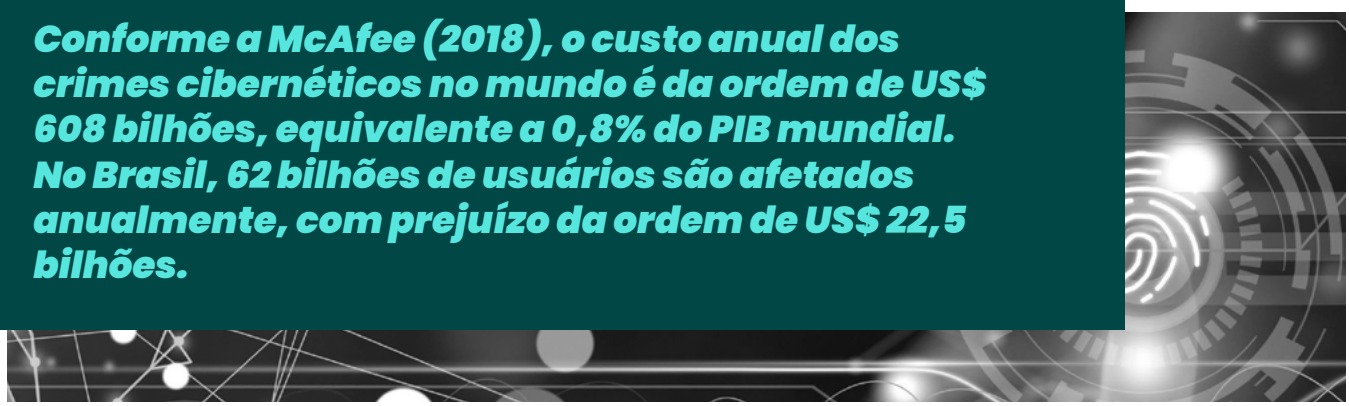
O CENÁRIO ATUAL DAS AMEAÇAS CIBERNÉTICAS NO BRASIL E NO MUNDO VERSUS A REALIDADE DAS PEQUENAS EMPRESAS

Segundo a OCDE (2017), os maiores desafios de segurança digital que afetam as atividades econômicas e digitais consistem em ataques cibernéticos contra pequenas empresas, que interrompem ou impedem atividades econômicas e sociais, bem como espionagem e crimes cibernéticos que envolvem o roubo de propriedade intelectual digital e de ativos.

Nos últimos anos, houve mudança real na escala e no escopo desses riscos cibernéticos, no que diz respeito à segurança digital e à privacidade. Tal situação impõe impactos significativos em atividades sociais e econômicas, uma vez que incidentes de segurança digital podem afetar a reputação, as finanças e os ativos intelectuais e físicos de uma empresa ou organização, pois podem gerar a queda de sua competitividade, de sua capacidade de inovar e de modificar sua posição no mercado (OCDE, 2017).

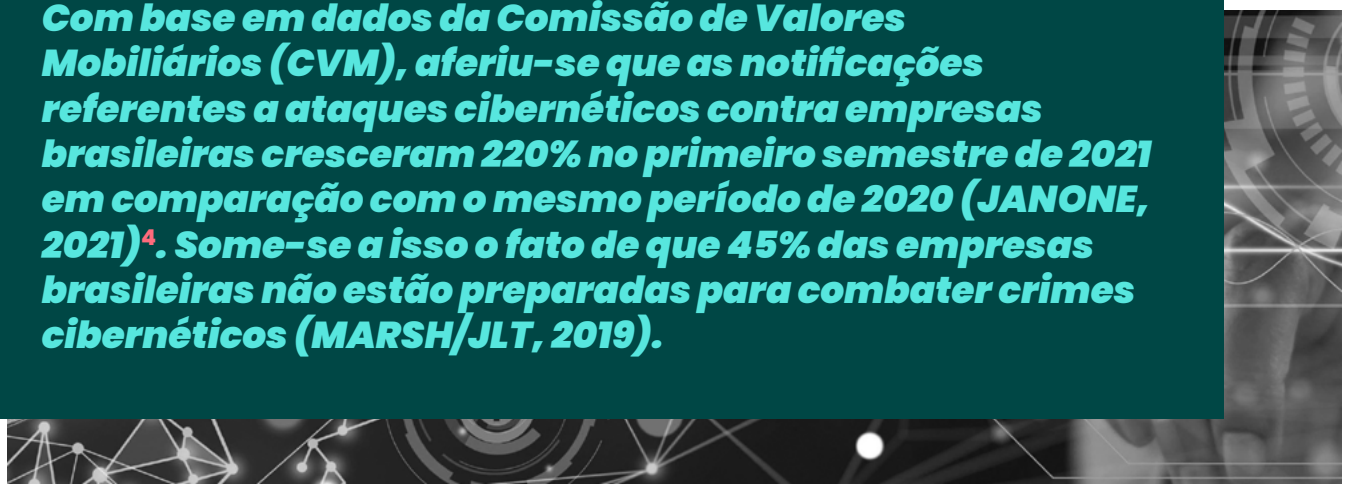
De acordo com a Kaspersky, somente em abril de 2020, o Brasil foi alvo de mais de 60% dos ataques identificados pela companhia na América Latina. Em seguida vem a Colômbia, com 11,9 milhões de ataques, o México (9,3 milhões), o Chile (4,3 milhões), o Peru (3,6 milhões) e a Argentina (2,6 milhões) (ROLFINI, 2020)[2].

Conforme a McAfee (2018), o custo anual dos crimes cibernéticos no mundo é da ordem de US$ 608 bilhões, equivalente a 0,8% do PIB mundial. No Brasil, 62 bilhões de usuários são afetados anualmente, com prejuízo da ordem de US$ 22,5 bilhões.



O relatório *Midyear Cybersecurity Roundup* também identificou aumento das ameaças cibernéticas no Brasil no primeiro semestre de 2020, em especial devido à pandemia de coronavírus. Durante o primeiro semestre de 2020, o Brasil foi o oitavo país que mais recebeu ameaças por e-mail com temas relacionados ao novo SARS-CoV-2. No total, foram 132 mil mensagens eletrônicas com arquivos maliciosos. Ademais, houve aumento do risco para as empresas devido a falhas de segurança criadas por uma força de trabalho em grande parte remota (TREND MICRO, 2020)[3].

Com base em dados da Comissão de Valores Mobiliários (CVM), aferiu-se que as notificações referentes a ataques cibernéticos contra empresas brasileiras cresceram 220% no primeiro semestre de 2021 em comparação com o mesmo período de 2020 (JANONE, 2021)[4]. Some-se a isso o fato de que 45% das empresas brasileiras não estão preparadas para combater crimes cibernéticos (MARSH/JLT, 2019).

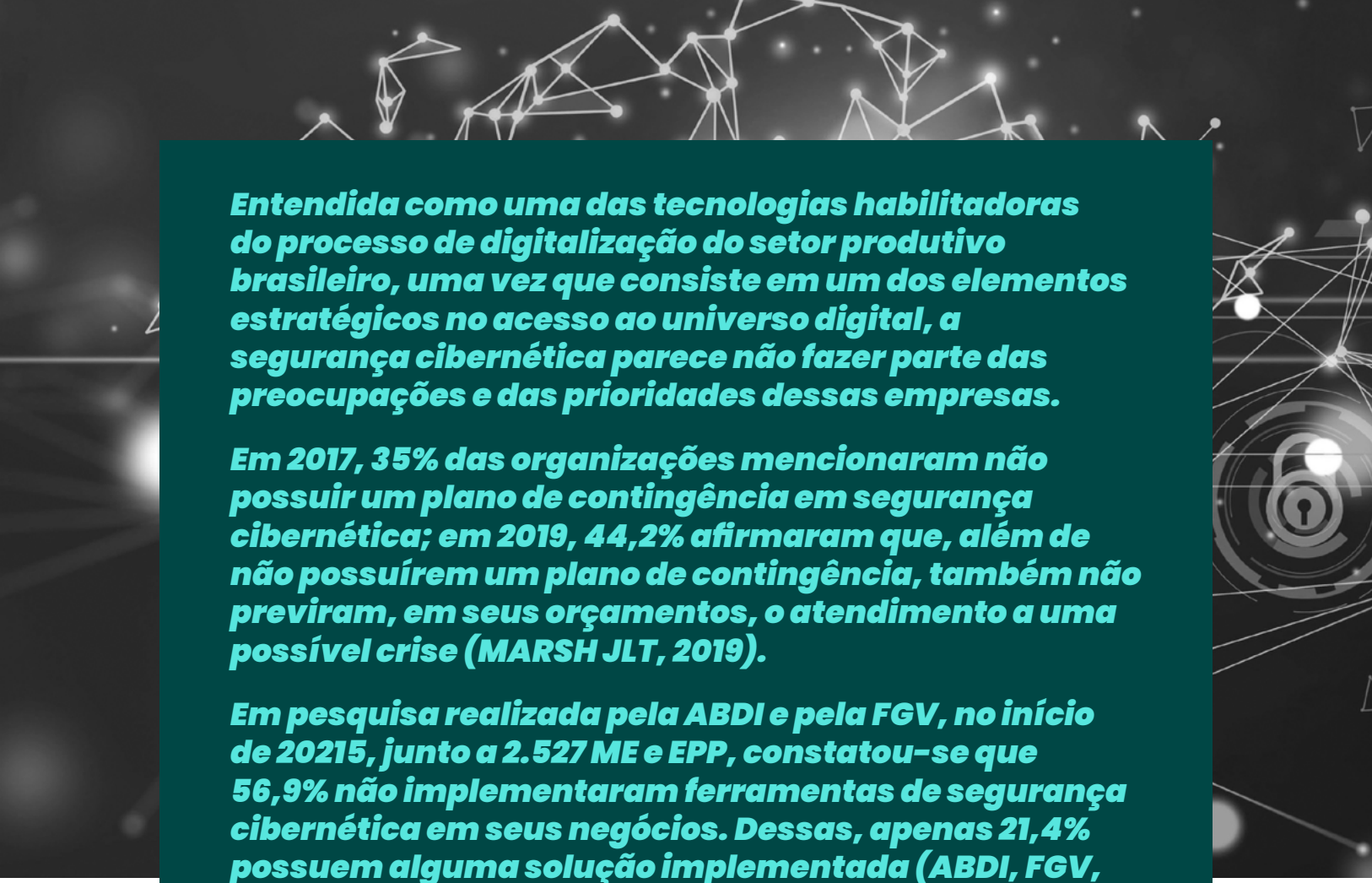


As quase cinco milhões de microempresas (ME) e empresas de pequeno porte (EPP) brasileiras correspondem a 98,5% do total de empresas privadas no Brasil, respondem por 27% do PIB e proporcionam 54% do total de empregos formais brasileiros (SEBRAE, 2018).

Mais de 45% das ME e das EPP concentram-se nas atividades de Comércio e mais de 33% atuam no setor de Serviços. As atividades do comércio varejista em que mais predominam mais as ME e EPP consistem em artigos de vestuário, produtos alimentícios, lanchonetes, restaurantes, acessórios para veículos automotores, materiais de construção, equipamentos de informática, produtos farmacêuticos e bebidas. Já as atividades de serviços concentram-se em transporte rodoviário e de cargas, contabilidade, escritório e apoio administrativo, manutenção e reparação mecânica de veículos, consultoria em gestão empresarial, atividade médica restrita a consultas, preparação de documentos e apoio administrativo, serviços de engenharia e cabeleireiro e manicure (SEBRAE, 2018).

No contexto atual de ameaças cibernéticas crescentes, a Estratégia Nacional de Segurança Cibernética – E-Ciber, aprovada pelo Decreto Nº 10.222/20 – pontua a importância de as organizações públicas e privadas estabelecerem políticas e procedimentos de segurança cibernética periodicamente revisados e de atenderem à evolução tecnológica, ao aperfeiçoamento de processos e à necessidade de capacitação contínua e estruturada para todos os colaboradores (GOVERNO FEDERAL, 2020).

No entanto, o cenário atual nas microempresas (ME) e nas empresas de pequeno porte (EPP) brasileiras parece não observar a realidade imposta pelos riscos cibernéticos, tampouco as recomendações da E-Ciber.



Entendida como uma das tecnologias habilitadoras do processo de digitalização do setor produtivo brasileiro, uma vez que consiste em um dos elementos estratégicos no acesso ao universo digital, a segurança cibernética parece não fazer parte das preocupações e das prioridades dessas empresas.

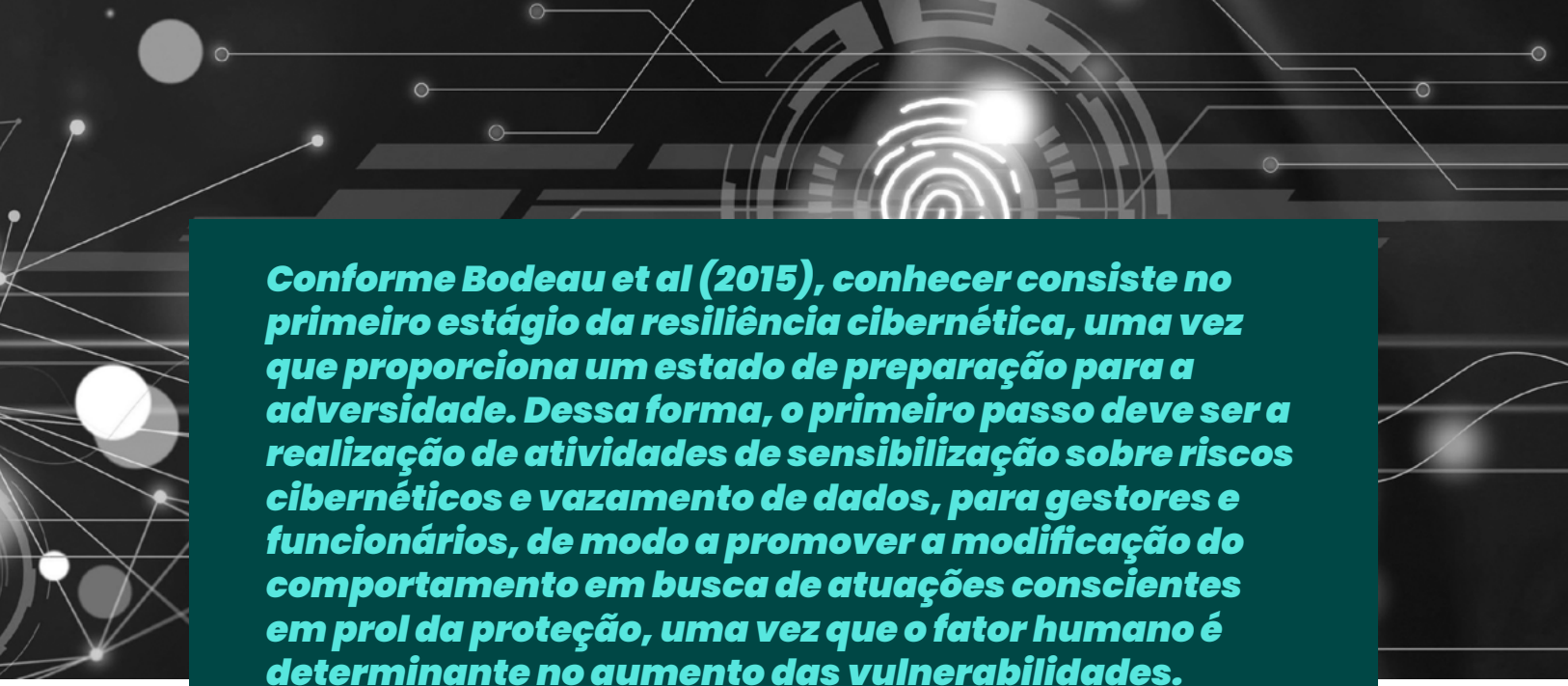
Em 2017, 35% das organizações mencionaram não possuir um plano de contingência em segurança cibernética; em 2019, 44,2% afirmaram que, além de não possuírem um plano de contingência, também não previram, em seus orçamentos, o atendimento a uma possível crise (MARSH JLT, 2019).

Em pesquisa realizada pela ABDI e pela FGV, no início de 20215, junto a 2.527 ME e EPP, constatou-se que 56,9% não implementaram ferramentas de segurança cibernética em seus negócios. Dessas, apenas 21,4% possuem alguma solução implementada (ABDI, FGV, 2021).

A DEMOCRATIZAÇÃO DO ACESSO A SOLUÇÕES VOLTADAS PARA O AUMENTO DA RESILIÊNCIA CIBERNÉTICA DE PEQUENAS EMPRESAS BRASILEIRAS

As prioridades de ME e EPP no Brasil encontram-se voltadas para a adoção de boas práticas digitais com foco em captação, engajamento e conexão de clientes, com menor interesse na adoção de soluções de segurança cibernética nos negócios. Essa negligência na adoção de medidas de segurança da informação adequadas em suas prioridades de negócios traz como consequência uma maior fragilidade frente a ataques cibernéticos.

Com vistas a reduzir essa fragilidade, a questão relevante consiste em como democratizar o acesso e a utilização de soluções cibernéticas para o aumento da resiliência nos pequenos negócios.



Conforme Bodeau et al (2015), conhecer consiste no primeiro estágio da resiliência cibernética, uma vez que proporciona um estado de preparação para a adversidade. Dessa forma, o primeiro passo deve ser a realização de atividades de sensibilização sobre riscos cibernéticos e vazamento de dados, para gestores e funcionários, de modo a promover a modificação do comportamento em busca de atuações conscientes em prol da proteção, uma vez que o fator humano é determinante no aumento das vulnerabilidades.

A conscientização sobre riscos cibernéticos e o entendimento claro sobre as necessidades digitais da empresa tornam-se indispensáveis para o aumento de sua capacidade de promover a proteção de suas operações, mesmo para empresas de pequeno porte, pois podem mitigar certos riscos de ataques cibernéticos, despertar para necessidade de intervenções de segurança cibernética e promover real aumento de resiliência cibernética.

De maneira prática, o conhecimento e a adoção de comportamentos simples podem mitigar significativamente os riscos cibernéticos de ME e EPP, a saber:

- Cuidados com a segurança da senha;
- Uso de Token;
- Cuidados com e-mails suspeitos/falsos;
- Instalação de barreiras tipo antivírus e *firewall*;
- Definição de regras de sites proibidos e habilitados;
- Autenticação (controle de acesso) baseada em 2 fatores;
- Atualização automática de sistema operacional e outros softwares;
- Cuidado com downloads de arquivos e programas;
- Cuidado com acesso a links recebidos em mídias sociais e e-mails;
- Estabelecimento de procedimentos e condutas para os funcionários;
- Gerenciamento de identidade e acesso de usuários.

Já as ações de resistência e de recuperação de ataques cibernéticos requerem maiores investimentos, tanto técnicos quanto financeiros. Faz-se necessária a oferta de consultorias que avaliem o patamar de digitalização da empresa, analisem sua realidade, realizem a gestão do risco cibernético e a identificação das vulnerabilidades do negócio, promovam o acesso e a adoção de ferramentas de segurança cibernética adequadas e específicas para a necessidade da empresa.

A demonstração dos prejuízos em situação de ataque, a compreensão clara das principais ameaças a sistemas operacionais, o conhecimento sobre os tipos e as formas de ataque mais frequentes, a adoção das tecnologias adequadas, o planejamento para mitigação de ameaças e a criptografia de dados são parte de estrutura de aumento de resiliência cibernética para a promoção da continuidade de realização das funções essenciais da organização e de seus negócios, apesar das adversidades resultantes de ataques cibernéticos.

Ademais, estratégias para a promoção da segurança cibernética nos negócios podem ser estimuladas pelo governo junto ao setor produtivo, conforme preconizado pela OCDE (2017) e pela Estratégia Nacional de Segurança Cibernética (BRASIL, 2018). Apresentam-se, a seguir, algumas dessas estratégias:

- ***Capacitação e desenvolvimento de habilidades profissionais, por meio da ampliação de cursos técnicos e acadêmicos sobre o tema.***
- ***Estímulo ao desenvolvimento de projetos de pesquisa e desenvolvimento voltados às necessidades de segurança do setor produtivo.***
- ***Promoção de incentivos fiscais para empresas que invistam em segurança da informação.***
- ***Definição de critérios técnicos mínimos de segurança cibernética a serem adotados por empresas e organizações que façam negócios com o governo.***
- ***Estímulo à criação de startups na área de segurança cibernética.***

CONCLUSÃO

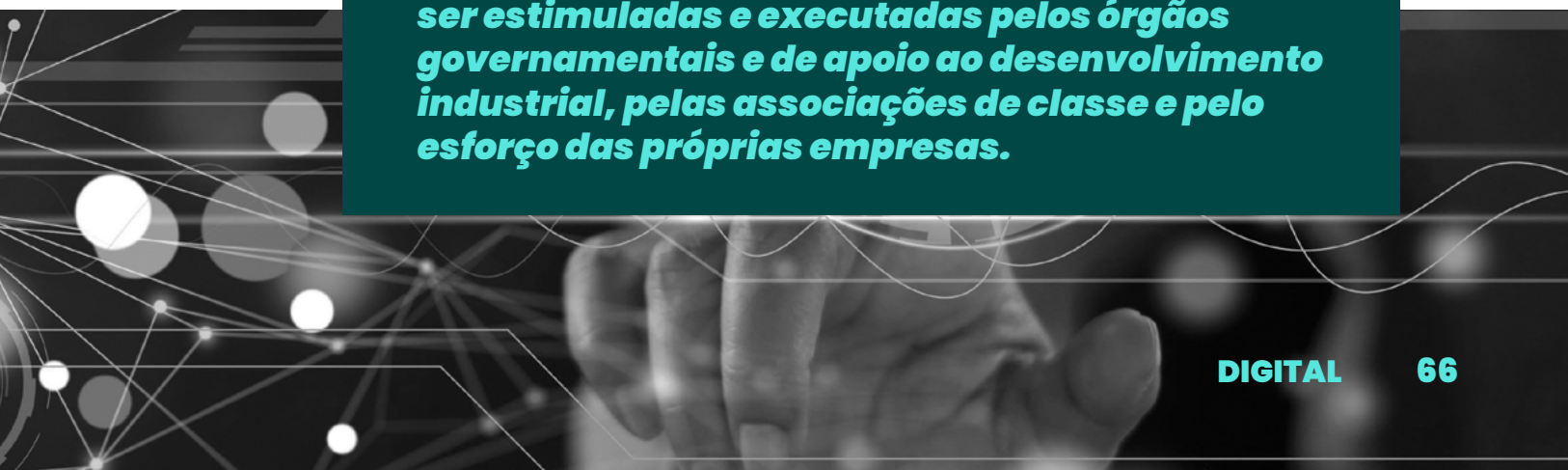
O aumento da velocidade do processo de digitalização da economia brasileira demanda a criação de ambiente propício para o aumento da maturidade digital do setor produtivo, por meio da remoção das barreiras externas que dificultam a adoção de tecnologias digitais pelas empresas. Nesse contexto, a promoção da segurança cibernética e da proteção de dados assumem papel fundamental no processo de tornar as empresas brasileiras mais digitais e, por consequência, mais produtivas.

É fato que, em um contexto de transformação digital da economia cada vez mais crescente, o setor produtivo estará cada vez mais vulnerável a ataques em suas redes, devido à aceleração da transição do modelo dos negócios, de analógico para digital. À medida que aumenta a digitalização dos processos produtivos, aumentam os riscos e a necessidade de implantar nas empresas, não importa o seu tamanho, soluções de segurança da informação, de forma a possibilitar o aumento de sua resiliência cibernética.

Adiciona-se a esse contexto a entrada em vigor da Lei de Proteção Geral de Dados – LPGD, que passou a exigir que empresas conectadas à internet promovam ações de prevenção e de contenção de ataques e de vazamento de dados. No entanto, a grande maioria das empresas brasileiras ainda não está sensibilizada e tampouco preparada para tal desafio.

Nesse contexto, tornam-se necessários esforços reais de democratização do acesso a soluções voltadas para o aumento da resiliência cibernética de ME e EPP brasileiras, com vistas a promover a conscientização e a adoção de estratégias de segurança para preparar empresas e aumentar sua confiança frente a potenciais ataques perpetrados via as infraestruturas de Tecnologia da Informação, de modo a reduzir suas vulnerabilidades.

Tais soluções devem concentrar-se no tripé necessário à redução dos impactos de ataques cibernéticos, a saber: de ordem tecnológica, de capacitação de recursos humanos e de gestão de pessoas e processos na empresa. E devem ser estimuladas e executadas pelos órgãos governamentais e de apoio ao desenvolvimento industrial, pelas associações de classe e pelo esforço das próprias empresas.



Atividades de conscientização e sensibilização sobre riscos cibernéticos para gestores e funcionários das pequenas empresas, oferta de consultorias que analisem a realidade da empresa e promovam o acesso e a implementação de ferramentas de segurança cibernética que modifiquem o comportamento dos funcionários, a sua capacitação na implementação de ferramentas de segurança cibernética são ações que devem ser adotadas de forma a se propagarem por todo o tecido econômico brasileiro.

A conscientização sobre riscos cibernéticos e o entendimento claro sobre as necessidades digitais da empresa tornam-se indispensáveis para o aumento na capacidade de promover a proteção das operações para as ME e as EPP. Nesse contexto, democratizar e promover o acesso e a utilização de soluções cibernéticas para o aumento da resiliência em seus negócios passam a ter um caráter primordial.

Com esse objetivo, a ABDI ampliará suas atividades voltadas para a capacitação de recursos humanos especializados em segurança cibernética, sensibilização a respeito de riscos cibernéticos e adoção de soluções tecnológicas em pequenos negócios.

A *Cyber Arena* promoverá, a partir de 2022, sensibilizações, para o público em geral, e capacitações para profissionais de TI, com a utilização de simulador hiper-realista de ataque e defesa cibernéticos, que consiste em ambiente virtualizado para treinamento, experimentação, avaliação de vulnerabilidades, trabalho em grupo, feedback em tempo real, experiências *on the job*, teste de novas ideias e solução de problemas cibernéticos, onde ataques cibernéticos são realizados em réplica de ambiente real de operação de uma organização, de maneira segura, controlada e confiável.

Já o *Cyber Solutions* promoverá, por meio de consultorias especializadas e individualizadas, a avaliação da maturidade cibernética de empresas brasileiras, bem como o acesso e a adoção de soluções tecnológicas em segurança cibernética, com vistas à mitigação de riscos e de vulnerabilidades.

A ABDI proporá, ainda, o desenvolvimento de modelagem de alto nível para a aferição e análise de Índice de Resiliência Cibernética (IRCiber) para o setor produtivo. O objetivo consiste em medir a evolução e o aumento dessa resiliência ao longo do tempo, além de incorporar a gestão de riscos cibernéticos.

Larissa de Freitas Querino

Larissa de Freitas Querino é Mestre em Economia com habilitação em Economia da Defesa pela Universidade de Brasília. É bacharel em Relações Internacionais pela Universidade de Brasília, possui Maestría em Desenvolvimento Econômico pela Universidade Internacional de Andalucía, na Espanha e MBA em Gestão de Comércio Exterior e Negócios Internacionais pela Fundação Getúlio Vargas. É a especialista em Indústria de Defesa da Agência Brasileia de Desenvolvimento Industrial (ABDI) desde 2011, onde realiza atividades de estruturação, negociação e implementação de projetos e agendas de trabalho no setor de Defesa, junto a parceiros dos setores público e privado. Coordenou, dentre outras publicações sobre o tema na ABDI, os trabalhos para o desenvolvimento e a publicação do Mapeamento da Base Industrial de Defesa (2016). Atualmente lidera os projetos de Segurança Cibernética e do Uniforme Inteligente.

Ricardo Gonzaga Martins de Araújo

Profissional com mestrado Strictu-senso em Gestão de Pessoas – FEAD, Pós graduado em Finanças Empresariais – Fundação Getúlio Vargas, Pós graduado em Engenharia Econômica – FDC, Pós graduado em Engenharia da Qualidade – IETEC/MG, Graduado em Engenharia Eletrônica e de Telecomunicação – PUC/MG. Com mais de 35 anos de atuação nas áreas industrial, administrativa, financeira, contábil, tendo sido responsável por uma planta industrial e proprietário de microempresa, Ricardo tem experiência em articulação público-privado na Agência Brasileira de Desenvolvimento Industrial - ABDI para formulação e aplicação de políticas públicas.

Imagem: AdobeStock.com

NOTAS

1 Disponível em https://balipodo.com.br/o-que-e-resiliencia-cibernetica-blogs-do-opentext/. Acesso em 17 de agosto de 2021.

2 Disponível em https://olhardigital.com.br/2020/07/03/seguranca/cibercrime-ataques-no-brasil-aumentam-mais-de-300-com-a-pandemia/. Acesso em 11 de setembro de 2020.

3 Disponível em https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report. Acesso em 11 de setembro de 2020.

4 Disponível em https://www.cnnbrasil.com.br/business/2021/07/22/ataques-ciberneticos-a-empresas-brasileiras-crescem-220-no-1-semestre-de-2021. Acesso em 17 de agosto de 2021.

5 ABDI, FGV. Mapa da Digitalização das MPEs Brasileiras – Resumo Executivo. Brasília, junho de 2021.

REFERÊNCIAS

ABDI, FGV. Mapa da digitalização das MPEs brasileiras – Resumo Executivo. Brasília, junho de 2021.

ACCENTURY SECURITY. Ninth Annual Cost of Cybercrime Study. Unlocking the Value of Improved Cybersecurity Protection. Accenture, 2019

BODEAU, Deborah et al. Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques. The MITRE Corporation Bedford, MA: 2015.

BRASIL. Presidência da República. Decreto nº 10.222, de 05 de fevereiro de 2020. Estratégia Nacional de Segurança Cibernética.

BRASIL. Presidência da República. Lei 13.709/2018 - Lei Geral de Proteção de Dados (LGPD), de 14 de agosto de 2018.

JANONE, Lucas. Ataques cibernéticos a empresas brasileiras crescem 220% no 1º semestre de 2021. CNN Brasil. Disponível em https://www.cnnbrasil.com.br/business/2021/07/22/ataques-ciberneticos-a-empresas-brasileiras-crescem-220-no-1-semestre-de-2021. Acesso em: 17 agosto de 2021.

MCAFEE. Economic Impact of Cybercrime – No Slowing Down. Santa Clara: McAfee, 2018

MARSH JLT. Cyber View 2019: identificando oportunidades no mercado brasileiro. São Paulo: MARSH JLT, 2019.

OECD. Digital Economy Outlook 2017, Paris: OECD Publishing, 2017.

PRESSO, Luiz. O Que É Resiliência Cibernética? Balipodo. Disponível em https://balipodo.com.br/o-que-e-resiliencia-cibernetica-blogs-do-opentext/. Acesso em: 17 de agosto de 2021.

ROLFINI, Fabiana. Cibercrime: Ataques no Brasil Aumentam mais de 300% com a Pandemia. Olhar Digital. Disponível em https://olhardigital.com.br/2020/07/03/seguranca/cibercrime-ataques-no-brasil-aumentam-mais-de-300-com-a-pandemia/. Acesso em: 11 set. 2020.

TREND MICRO. Securing the Pandemic-Disrupted Workplace. Midyear Cybersecurity Report 2020. Disponível em https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report. Acesso em: 11 set. 2020.

WEF. Future Series: Cybersecurity, emerging technology and systemic risk. Insight Report, Novembro, 2020.