Presidência da República
Secretaria-Geral
Subchefia para Assuntos Jurídicos

DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020

Aprova a Estratégia Nacional de Segurança Cibernética.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, **caput**, inciso VI, alínea "a", da Constituição,

DECRETA:

Art. 1º Fica aprovada a Estratégia Nacional de Segurança Cibernética - E-Ciber, conforme o disposto no inciso I do art. 6º do Decreto nº 9.637, de 26 de dezembro de 2018, na forma do Anexo a este Decreto.

Parágrafo único. A E-Ciber será publicada no sítio eletrônico do Gabinete de Segurança Institucional da Presidência da República.

Art. 2º Caberá aos órgãos e entidades da administração pública federal, no âmbito de suas competências, as gestões que possibilitem à implementação das ações estratégicas previstas na E-Ciber.

Art. 3º Este Decreto entra em vigor na data de sua publicação.

Brasília, 5 de fevereiro de 2020; 199º da Independência e 132º da República.

JAIR MESSIAS BOLSONARO
Augusto Heleno Ribeiro Pereira

Este texto não substitui o publicado no DOU de 6.2.2020.

ANEXO

ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA

A presente Estratégia Nacional de Segurança Cibernética - E-Ciber é orientação manifesta do Governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e terá validade no quadriênio 2020-2023.

1. CONSIDERAÇÕES PRELIMINARES

1.1. SUMÁRIO EXECUTIVO

Em 2015, o Governo federal deu publicidade à Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal[1], com validade até 2018, como um importante instrumento de apoio ao planejamento dos órgãos e entidades do Governo, cujo objetivo foi de melhorar a segurança e a resiliência das infraestruturas críticas e dos serviços públicos nacionais. Esse documento impulsionou as discussões sobre o tema no âmbito da Administração Pública federal, e também em outros setores da sociedade.

O Decreto nº 9.637, de 26 de dezembro de 2018[2], que instituiu a Política Nacional de Segurança da Informação e dispõe sobre princípios, objetivos, instrumentos, atribuições e competências de segurança da informação para os órgãos e entidades da Administração Pública federal, sob o prisma da governança, previu, para sua implementação, a elaboração da Estratégia Nacional de Segurança da Informação e dos Planos Nacionais. Em virtude da abrangência da Segurança da Informação o Decreto nº 9.637, de 2018, indicou, em seu art. 6º, que a Estratégia Nacional de Segurança da Informação seja construída em módulos, a fim de contemplar a segurança cibernética, a defesa cibernética, a segurança das infraestruturas críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados.

Em cumprimento ao estabelecido na Política Nacional de Segurança da Informação, e considerada a Segurança Cibernética - Seg Ciber como a área mais crítica e atual a ser abordada, o Gabinete de Segurança Institucional da Presidência da República elegeu, em janeiro de 2019, a EstratégiaNacional de Segurança Cibernética - E-Ciber como primeiro módulo da Estratégia Nacional de Segurança da Informação, a seu cargo, a ser elaborada.

Desse modo, por coordenação do Gabinete de Segurança Institucional da Presidência da República, e com participação de mais de quarenta órgãos e entidades do Governo, além de instituições privadas e do setor acadêmico, que foram distribuídos em três subgrupos de trabalho, foi elaborada a presente E-Ciber, após trinta e uma reuniões e sete meses de estudos e de debates.

Por meio de metodologia **bottom up**, e com base nas conclusões dos subgrupos de trabalho, em avaliação comparativa - **benchmarking** sobre estratégias correlatas de outros países, e em cumprimento ao contido na Política Nacional de Segurança da Informação, chegou-se ao diagnóstico da segurança cibernética global e do Brasil. Em seguida, foram estabelecidos os objetivos estratégicos nacionais, e as respectivas ações estratégicas, segundo sete eixos de atuação, que demonstram à sociedade brasileira os pontos considerados relevantes para o País na área da segurança cibernética.

1.2. INTRODUÇÃO

A revolução digital está transformando profundamente nossa sociedade. Nas últimas duas décadas, bilhões de pessoas se beneficiaram do crescimento exponencial do acesso à internet, da rápida adoção dos recursos de tecnologia da informação e comunicação, e das oportunidades econômicas e sociais oriundas do ambiente digital.

Os rápidos avanços na área de tecnologia da informação e comunicação resultaram no uso intenso do espaço cibernético para as mais variadas atividades, inclusive a oferta de serviços por parte do Governo federal, em coerência com as tendências globais. Entretanto, novas e crescentes ameaças cibernéticas surgem na mesma proporção, e colocam em risco a administração pública e a sociedade.

Desse modo, proteger o espaço cibernético requer visão atenta e liderança para gerenciar mudanças contínuas, políticas, tecnológicas, educacionais, legais e internacionais. Nesse sentido, o Governo, a indústria, a academia e a sociedade em geral devem incentivar a inovação tecnológica e a adoção de tecnologias de ponta, e manter constante atenção à segurança nacional, à economia e à livre expressão.

Em nível superior aos debates sobre a segurança no espaço cibernético está a Segurança da Informação, área sistêmica, e diretamente relacionada à proteção de um conjunto de informações e ao valor que estas possuem para um indivíduo ou para uma organização. Desse modo, segundo o art. 2º do Decreto nº 9.637, de 2018, a Segurança da Informação abrange a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais, e tem como princípios fundamentais a confidencialidade, a integridade, a disponibilidade e a autenticidade.

Entende-se que os recursos tecnológicos empregados na segurança sistêmica devem apoiar políticas que garantam os princípios fundamentais da autenticidade e da integridade dos dados, e prover mecanismos para proteção da legitimidade contra sua alteração ou eliminação não autorizada. Do mesmo modo, as informações coletadas, processadas e armazenadas na infraestrutura de tecnologia da informação e comunicação devem ser acessíveis apenas a pessoas, a processos ou a entidades autorizadas, a fim de garantir a confidencialidade das informações. Adicionalmente, os recursos de tecnologia da informação e comunicação devem prover disponibilidade permanente e apoiar de forma contínua todos os acessos autorizados.

A E-Ciber, além de preencher importante lacuna no arcabouço normativo nacional sobre segurança cibernética, estabelece ações com vistas a modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e de indivíduos sobre o assunto. Em primeiro lugar, verifica-se que há boas iniciativas gerenciais nessa área, entretanto, mostram-se fragmentadas e pontuais, o que dificulta a convergência de esforços no setor. Em segundo, nota-se a falta de um alinhamento normativo, estratégico e operacional, o que frequentemente gera retrabalho ou resulta na constituição de forças-

tarefas para ações pontuais, que prejudicam a absorção de lições aprendidas e colocam em risco a eficácia prolongada dessas ações. Em terceiro, vê-se a existência de diferentes níveis de maturidade da sociedade em segurança cibernética, o que resulta em percepções variadas sobre a real importância do tema.

Após a presente parte introdutória, discorre-se sobre a metodologia adotada nas linhas de análise, que tiveram por base o estudo de dois conjuntos de eixos temáticos: os de proteção e segurança, e os denominados transformadores. Aborda-se, ainda, como os subgrupos de trabalho se estruturaram, de acordo com os temas propostos.

Na Parte I, apresenta-se um diagnóstico da segurança cibernética, baseado no cenário internacional e o no cenário nacional, com especial atenção às ameaças, aos ataques e às vulnerabilidades cibernéticas, e ao modo como esses elementos impactam a sociedade e as instituições.

Os eixos temáticos são apresentados separadamente na Parte II. Primeiro, abordam-se os relativos à proteção e à segurança: governança da Segurança cibernética nacional, o universo conectado e seguro e a proteção estratégica. Depois, analisam-se aqueles que, por sua natureza, são chamados de Transformadores: a dimensão normativa; a pesquisa, desenvolvimento e inovação; a dimensão internacional e parcerias estratégicas; e a educação.

Em virtude da análise diagnóstica e do estudo dos eixos temáticos, apresentam-se os objetivos estratégicos e, em seguida, as ações estratégicas, elaboradas com o fim de atingir os objetivos especificados. Por meio dessas ações, para cuja realização recomenda-se a elaboração de planos, apontam-se valiosas direções, capazes de conduzir a sociedade e as instituições a um ambiente próspero, resiliente e seguro, como condição ideal para o crescimento econômico e para o desenvolvimento social.

Por fim, é importante ressaltar que no decorrer da apresentação da Estratégia são mencionados diversos termos relacionados não apenas à segurança cibernética, mas também ao grande campo de estudos da segurança da informação. Com o propósito de esclarecê-los, caso necessário, recomenda-se a consulta ao Glossário de Segurança da Informação, publicado pela Portaria nº 93, de 26 de setembro de 2019, do Gabinete de Segurança Institucional da Presidência da República [3].

Em decorrência da presente Estratégia, recomenda-se que cada órgão do setor público e do setor privado, planeje e realize gestões no sentido de colocar em prática os aspectos que lhe cabem e que estão estabelecidos nas ações estratégicas, em um esforço conjunto e dedicado, em prol do pleno alcance dos objetivos estratégicos do País, no crítico e atual tema da segurança cibernética nacional.

1.3. METODOLOGIA ADOTADA

A Estratégia é resultado de trabalho realizado por representantes de órgãos públicos, de entidades privadas, e do meio acadêmico, que participaram de uma série de reuniões técnicas, para debater vários aspectos da segurança cibernética. Ao considerar a vasta gama de assuntos, esses representantes foram divididos em três subgrupos, constituídos do seguinte modo:

- Subgrupo 1 - governança cibernética, dimensão normativa, pesquisa, desenvolvimento e inovação, educação, dimensão internacional e parcerias estratégicas.;

- Subgrupo 2 - confiança digital e prevenção e mitigação de ameaças cibernéticas; e

- Subgrupo 3 - proteção estratégica - proteção do Governo e proteção às infraestruturas.

Foram realizadas trinta e uma reuniões dos subgrupos, com a participação efetiva de todos esses representantes de notável saber, o que possibilitou o intercâmbio de conhecimentos e de ideias, e que contribuíram de forma decisiva para estabelecer a concepção estratégica.

Com o fim de estruturar os debates, o trabalho seguiu quatro etapas:

Primeira - Diagnóstico - levantamento e mapeamento de iniciativas, atores relacionados e ações existentes;

Segunda - Debates dos subgrupos - reuniões semanais com os atores relacionados e convidados de notório saber;

Terceira - Consulta pública - disponibilização do documento na internet para contribuições e ampla participação da sociedade em geral; e

Quarta - Aprovação e publicação - finalização da proposta e submissão à aprovação presidencial.

Adicionalmente, foi considerado o modelo de maturidade da capacidade em segurança cibernética [4], que define cinco dimensões:

- política e estratégia de segurança cibernética;

- cultura cibernética e de sociedade;

- educação, de treinamento e de habilidades em segurança cibernética;

- marcos legais e regulatórios; e

- padrões, organizações e tecnologias.

Essas dimensões, por sua transversalidade, abrangem as extensas áreas que devem ser consideradas no aumento da capacidade em segurança cibernética. Ao considerar as cinco dimensões do modelo, chegou-se à estrutura de sete eixos de atuação da Estratégia, anteriormente citados, que mantém relação direta com o modelo de maturidade da capacidade em segurança cibernética.

Os eixos temáticos da E-Ciber foram considerados de forma transversal, e podem ser descritos como:

- Eixos de Proteção e Segurança:

- governança da segurança cibernética nacional;

- universo conectado e seguro: prevenção e mitigação de ameaças cibernéticas; e

- proteção estratégica; e

- Eixos Transformadores:

- dimensão normativa;

- dimensão internacional e parcerias estratégicas;

- pesquisa, desenvolvimento e inovação; e

- educação.

A metodologia acima descrita permitiu o levantamento de informações relevantes, que resultaram numa concepção estratégica nacional sistêmica.

As conclusões finais desse trabalho resultaram numa primeira versão da E-Ciber, que foi disponibilizada para participação da sociedade em forma de consulta pública, lançada via internet em 10 de setembro de 2019, disponibilizada por vinte por dias consecutivos e acessada por quarenta e um participantes. Desse total, houve a participação de trinta e um indivíduos e de dez organizações públicas e privadas que enviaram cento e sessenta e seis contribuições. Após análise de todas as contribuições recebidas, chegou-se à presente versão aprovada pelo Excelentíssimo Senhor Presidente da República.

1.4. CONCEPÇÃO ESTRATÉGICA

Da análise dos Eixos Temáticos constantes na Parte II, chegou-se à presente concepção, que resulta da interação entre os mencionados eixos, a visão, e os objetivos estratégicos, em uma abordagem que culminou nas ações estratégicas nacionais.

2. A ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA

2.1. VISÃO PARA O BRASIL

Tornar-se país de excelência em segurança cibernética.

2.2. OBJETIVOS ESTRATÉGICOS

No intuito de atender à visão proposta, na concepção dos objetivos estratégicos foram considerados os parâmetros estabelecidos na Política Nacional de Segurança da Informação: o estágio de maturidade e as necessidades do País em segurança cibernética e os aspectos relativos ao ecossistema digital, no âmbito nacional e internacional.

Desse modo, estes objetivos estratégicos visam a nortear as ações estratégicas do País em segurança cibernética, e representam macrodiretrizes basilares para que o setor público, o setor produtivo e a sociedade possam usufruir de um espaço cibernético resiliente, confiável, inclusivo e seguro. São os objetivos estratégicos:

1. Tornar o Brasil mais próspero e confiável no ambiente digital;

2. Aumentar a resiliência brasileira às ameaças cibernéticas; e

3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional.

2.3. AÇÕES ESTRATÉGICAS

Em virtude dos aspectos abordados na Parte I - Diagnóstico, e das considerações realizadas sobre a situação da segurança cibernética nacional na Parte II - Análise dos Eixos Temáticos, estabeleceram-se dez ações estratégicas.

Enfatiza-se ser absolutamente fundamental que cada órgão do setor público e do setor privado identifique, planeje e execute as ações de sua competência, para que o País torne realidade os rumos materializados por cada ação estratégica.

2.3.1.Fortalecer as ações de governança cibernética

Fortalecer as ações de governança em segurança cibernética, por parte do setor público e do setor privado, que contemplem iniciativas relacionadas à gestão de pessoas, ao atendimento aos requisitos de segurança cibernética e à gestão dos ativos de informação. Dentre as ações que podem ser adotadas nesse sentido, mencionam-se:

- realizar fóruns de governança;

- criar controles para o tratamento de informações com restrição de acesso;

- estabelecer requisitos mínimos de segurança cibernética nas contratações pelos órgãos públicos;

- implantar programas e projetos sobre governança cibernética;

- adotar, além dos normativos de governança emitidos pelo Gabinete de Segurança Institucional da Presidência da República, normas, padrões e modelos de governança reconhecidos mundialmente;

- adotar, a indústria, padrões internacionais no desenvolvimento de novos produtos desde sua concepção(**privacy/security by design and default**);

- recomendar a adoção de soluções nacionais de criptografia, observada, para tanto, a legislação específica;

- intensificar o combate à pirataria de **software**;

- adotar soluções de segurança cibernética que abordem iniciativas integradoras;

- designar o gestor de segurança da informação;

- recomendar a certificação em segurança cibernética, conforme padrões internacionais; e

- ampliar o uso do certificado digital.

2.3.2. Estabelecer um modelo centralizado de governança no âmbito nacional

Estabelecer um modelo centralizado de governança para o País, por meio da criação de um sistema nacional de segurança cibernética, com as seguintes atribuições:

- promover a coordenação dos diversos atores relacionados com a segurança cibernética, além da esfera federal;

- promover a análise conjunta dos desafios enfrentados no combate aos crimes cibernéticos;

- auxiliar na formulação de políticas públicas;

- criar um conselho nacional de segurança cibernética;

- criar grupos de debate sobre segurança cibernética, em diferentes setores, sob coordenação do Gabinete de Segurança Institucional da Presidência da República, para fomentar discussões sobre o tema, por meio de mecanismos informais de participação;

- estabelecer rotina de verificações de conformidade em segurança cibernética, internamente, nos órgãos públicos e nas entidades privadas; e

- permitir a convergência dos esforços e de iniciativas, e atuar de forma complementar para receber denúncias, apurar incidentes e promover a conscientização e a educação da sociedade quanto ao tema. Para viabilizar a sua implementação, ficará a cargo do Gabinete de Segurança Institucional da Presidência da República a coordenação da segurança cibernética em âmbito nacional, que possibilite a atuação de modo amplo, cooperativo, participativo, e alinhado com as ações de defesa cibernética, a cargo do Ministério da Defesa.

2.3.3. Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade

Promover um ambiente participativo, colaborativo e seguro, entre as organizações públicas, as instituições privadas, a academia e a sociedade, por meio do acompanhamento contínuo e proativo das ameaças e dos ataques cibernéticos, com o objetivo de:

- estimular o compartilhamento de informações sobre incidentes e vulnerabilidades cibernéticas;

- realizar exercícios cibernéticos com participação de múltiplos atores;

- estabelecer mecanismos que permitam a interação e o compartilhamento de informações em diferentes níveis;

- fortalecer o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov e mantê-lo atualizado em pessoal e material;

- ressaltar o papel dos Centros de Tratamento e Resposta a Incidentes Cibernéticos - CSIRTs nacionais;

- aperfeiçoar a infraestrutura nacional de investigação de crimes cibernéticos;

- incentivar a criação e a atuação de equipe de tratamento e resposta aos incidentes cibernéticos - ETIRs, com ênfase no uso de tecnologias emergentes;

- emitir alertas e recomendações; e

- estimular o uso de recursos criptográficos, no âmbito da sociedade em geral, para comunicação de assuntos considerados sensíveis.

2.3.4. Elevar o nível de proteção do Governo

Elevar o nível de proteção do Governo, por meio de ações no campo cibernético, a exemplo de:

- incluir requisitos de segurança cibernética nas contratações estabelecidas pelos órgãos e entidades do Governo;

- aperfeiçoar e incentivar o uso dos dispositivos de comunicação segura do Governo;

- aperfeiçoar e manter atualizados os sistemas informacionais, as infraestruturas e os sistemas de comunicação dos órgãos públicos, em relação aos requisitos de segurança cibernética;

- recomendar que os órgãos públicos possuam cópias de segurança atualizadas e segregadas de forma automática em local protegido;

- elaborar requisitos específicos de segurança cibernética relativos ao uso de **endpoints** nas organizações públicas, aqui entendidos, em suma, como equipamentos finais conectados a um terminal de alguma rede ou a algum sistema de comunicação;

- incluir, nas políticas de segurança cibernética, requisitos relativos à gestão da cadeia de suprimentos;

- incluir requisitos de segurança cibernética nos processos de desestatização, no que envolver serviços essenciais; e

- monitorar a implementação dos requisitos mínimos de segurança cibernética pelos fornecedores que integram a cadeia de suprimentos.

2.3.5. Elevar o nível de proteção das Infraestruturas Críticas Nacionais

Proporcionar às infraestruturas críticas, maior resiliência que possibilite a contínua prestação de serviços essenciais, por meio das seguintes ações:

- promover a interação entre as agências reguladoras de infraestruturas críticas para tratar de temas relativos à segurança cibernética;

- estimular a adoção de ações de segurança cibernética pelas infraestruturas críticas;

- incentivar que essas organizações implementem políticas de segurança cibernética, que contemplem, dentre outros aspectos, métricas, mecanismos de avaliação, e de revisão periódica;

- incentivar a constituição de ETIRs;

- estímular que as infraestruturas críticas notifiquem o CTIR Gov dos incidentes cibernéticos; e

- incentivar a participação das infraestruturas críticas em exercícios cibernéticos.

2.3.6. Aprimorar o arcabouço legal sobre segurança cibernética

Para aprimorar o arcabouço legal sobre segurança cibernética, revisar e atualizar os normativos existentes, abordar novas temáticas e elaborar novos instrumentos. Nesse sentido, podem ser adotadas as seguintes ações como:

- identificar e abordar temas ausentes na legislaçãovigente;

- realizar esforços no sentido de incluir, no Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, novas tipificações de crimes cibernéticos;

- elaborar normativos sobre tecnologias emergentes;

- criar políticas de incentivo para contratação de mão de obra especializada em segurança cibernética;

- definir requisitos de segurança cibernética nos programas de trabalho remoto; e

- elaborar, sob coordenação do Gabinete de Segurança Institucional da Presidência da República, um anteprojeto de lei sobre segurança cibernética, com diretrizes que irão proporcionar alinhamento macroestratégico ao setor e contribuir de forma decisiva para elevar a segurança das organizações e dos cidadãos.

2.3.7. Incentivar a concepção de soluções inovadoras em segurança cibernética

Buscar o alinhamento entre os projetos acadêmicos e as necessidades da área produtiva, de modo a incentivar a pesquisa e o desenvolvimento de soluções em segurança cibernética, que tragam a necessária inovação aos produtos nacionais nessa área crítica, atual e imprescindível. Dentre as ações a serem consideradas, pode-se mencionar:

- propor a inclusão da segurança cibernética nos programas de fomento à pesquisa;

- incentivar a criação de centros de pesquisa e desenvolvimento em segurança cibernética no âmbito do Poder Executivo federal e no setor privado;

- viabilizar investimentos em pesquisas, por meio dos fundos públicos e privados;

- criar programas de incentivo ao desenvolvimento de soluções de segurança cibernética;

- estimular a criação de **startups** na área de segurança cibernética;

- estimular o desenvolvimento e a inovação de soluções de segurança cibernética nas tecnologias emergentes;

- incentivar a adoção de padrões globais de tecnologia, que permitirá a interoperabilidade em escala internacional;

- incentivar o desenvolvimento de competências e de soluções em criptografia;

- estimular o prosseguimento das pesquisas sobre o uso de inteligência espectral; e

- estabelecer requisitos mínimos de segurança cibernética que assegurem o uso pleno, responsável e seguro da tecnologia de quinta geração de conexão móvel - 5G.

2.3.8. Ampliar a cooperação internacional do Brasil em Segurança cibernética

Ampliar a cooperação do Brasil, em segurança cibernética, com o maior número possível de países, de forma transparente, e reforçar a posição do País na constante busca pela paz e pela segurança internacional, conforme a tradição da diplomacia nacional baseada nos princípios estabelecidos no art. 4º da Constituição. Para viabilizar esse intento, podem ser adotadas as seguintes medidas:

- estimular a cooperação internacional em segurança cibernética;

- incentivar as discussões sobre segurança cibernética nos organismos, nos fóruns e nos grupos internacionais dos quais o Brasil é membro;

- ampliar o relacionamento internacional com os países da América Latina;

- promover eventos e exercícios internacionais sobre segurança cibernética;

- participar de eventos internacionais de interesse para o País;

- ampliar os acordos de cooperação em segurança cibernética;

- ampliar o uso de mecanismos internacionais de combate aos crimes cibernéticos;

- estimular a participação do País em iniciativas futuras de estruturação normativa, como as relativas à criação de padrões de segurança em tecnologias emergentes, e

- identificar, estimular e aproveitar novas oportunidades comerciais em segurança cibernética.

2.3.9. Ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade

Ampliar parcerias, entre os diversos setores da sociedade, com vistas a elevar, de modo geral, o nível de segurança cibernética. Visualiza-se a efetiva cooperação do setor produtivo com a academia, por meio de recursos financeiros e materiais, e conforme apresentadas suas necessidades, investir na formação de universitários. Dentre as ações possíveis, destacam-se:

- ampliar a cooperação entre Governo, academia e iniciativa privada para promover a implementação da E-Ciber;

- manter um ambiente colaborativo que permita o estudo e a ampla utilização das tecnologias emergentes;

- estabelecer parcerias para incentivar o setor privado a investir em medidas de segurança cibernética;

- incentivar a realização de reuniões com atores destacados em segurança cibernética;

- estimular a instituição, caso necessário, de grupos de trabalho e de fóruns sobre segurança cibernética;

- incentivar a criação de mecanismos de compartilhamento de informações sobre riscos cibernéticos; e

- realizar parcerias entre a União, os Estados, o Distrito Federal, os Municípios, o Ministério Público e a academia, para a implantação de programas, projetos e ações em segurança cibernética, que alcancem a toda a sociedade.

2.3.10. Elevar o nível de maturidade da sociedade em segurança cibernética

Elevar o nível de maturidade em segurança cibernética da sociedade, com o fim de ensejar a compreensão das ameaças e dos riscos no espaço cibernético, e possibilitar às pessoas o uso adequado e oportuno de procedimentos e de ferramentas em prol da utilização segura do ambiente digital. Nesse sentido, identificam-se como iniciativas:

- incentivar os órgãos públicos e empresas privadas para que realizem campanhas de conscientização internas;

- realizar ações de conscientização da população;

- criar políticas públicas que promovam a conscientização da sociedade sobre segurança cibernética;

- propor a inclusão da segurança cibernética, por intermédio de suas competências básicas, e do uso ético da informação na educação básica - educação infantil, ensino fundamental e ensino médio;

- estimular a criação de cursos de nível superior em segurança cibernética;

- propor a criação de programas de incentivo para graduação e pós-graduação no Brasil e no exterior em segurança cibernética;

- fomentar a pesquisa e o desenvolvimento em segurança cibernética;

- criar programas de capacitação continuada para profissionais do setor público e do setor privado;

- incentivar a formação de profissionais para atuar no combate aos crimes cibernéticos;

- realizar eventos de capacitação em segurança cibernética;

- incentivo à participação em fóruns e eventos nacionais e internacionais em segurança cibernética;

- aperfeiçoar mecanismos de integração, de colaboração e de incentivos entre universidades, institutos, centros de pesquisa e setor privado em relação à segurança cibernética;

- incentivar exercícios de simulação em segurança cibernética; e

- promover a gestão de conhecimento de segurança cibernética, em articulação com os principais atores da área, a fim de otimizar a identificação, a seleção e o emprego de talentos.

PARTE I

DIAGNÓSTICO

Em 2018, mais da metade da população mundial utilizou a internet (quatro bilhões e cem milhões de usuários, o que representa cinquenta e quatro por cento da população mundial), sendo noventa e três por cento dos acessos a redes sociais realizados via dispositivos móveis[5]. De acordo com estimativa do portal statista.com, haverá mais de trinta bilhões de dispositivos de internet das coisas (IoT, do inglês **Internet of Things**) conectados em 2020.

Esse cenário de progressiva conectividade, em que milhares de equipamentos têm acesso simultâneo a redes de dados e à internet, oferece aos usuários grande variedade de serviços **online**, e proporcionam ao cidadão conforto e comodidade na vida diária.

Entretanto, ao tempo em que o crescimento dessa conectividade resulta em benefícios aos usuários, também traz, consigo, vasta gama de vulnerabilidades cibernéticas, que ensejam ameaças e ataques que podem causar prejuízos de toda ordem, com diferentes níveis de impacto para pessoas e para instituições.

Em termos financeiros, considerando ataques cibernéticos, estimam-se, por ano, perdas globais de US$ 600.000.000.000,00 (seiscentos bilhões de dólares)[6]. O Relatório de 2019 do Fundo Monetário Internacional destacou que, em todas as economias, a diretriz é a implementação de ações que fortaleçam a resiliência, ao tempo em que elege, como necessária, a busca por maior cooperação multilateral para gerenciar os riscos em segurança cibernética[7].

A digitalização quase total dos modelos de negócios tornou a economia global mais eficiente e dinâmica, e também mais vulnerável a ataques cibernéticos. A variedade e a complexidade das ameaças colocam em risco a imprescindível confiança no mundo digital, fator chave para as atividades **online**. Esse cenário leva a crescentes investimentos conjuntos entre Governos e setores produtivos. Em consequência, estima-se que, em 2020, o mercado de segurança cibernética mundial seja avaliado em US$ 151.000.000.000,00 (cento e cinquenta e um bilhões de dólares)[8]. A título de comparação, vê-se que, atualmente, o mercado brasileiro de segurança cibernética movimenta perto de US$ 2.000.000.000,00 (dois bilhões de dólares) por ano com a venda de **softwares**, **hardwares** e serviços[9].

Destaca-se, a seguir, o caso brasileiro. O relatório sobre o **ranking** de tecnologia da informação e comunicação da Organização das Nações Unidas - ONU analisa o índice de desenvolvimento mundial em tecnologias da informação e sua aplicação nos avanços da internet. Estuda, ainda, como as modernas tecnologias irão permitir inovações e transformar “de modo fundamental” negócios, Governos e sociedades. No **ranking** regional das Américas, o Brasil está apenas em décimo lugar, atrás de países como Barbados, Bahamas, Argentina e Chile. Segundo o relatório, no entanto, o Brasil é um dos maiores mercados de telecomunicações da região. A expectativa é que a qualidade e a cobertura dos serviços melhorem “significativamente” nos próximos anos[10].

O risco para a economia brasileira, gerado pela intrusão em computadores e pela disseminação de códigos maliciosos praticados pelo crime organizado já é uma realidade, conforme se vê pelos dados a seguir, referentes à conectividade do Governo, do setor privado e dos cidadãos, aos índices globais e aos crimes cibernéticos[(11)]:

- O Brasil ocupa o 66º lugar no **ranking** da Organização das Nações Unidas - ONU de tecnologia da informação e comunicação [1];

- Apenas 11% dos órgãos federais têm bom nível em governança de TI[2];

- O Brasil ocupa o 70º lugar no **Global Security Index**, da UIT[3];

- 74,9% dos domicílios (116 milhões de pessoas) com acesso à internet[4];

- 98% das empresas utilizam a internet[5];

- 100% dos órgãos federais e estaduais utilizam a internet[6];

- Em 2017, foram setenta milhões e quatrocentas mil vítimas de crimes cibernéticos[7];

- Em 2018, 89% dos executivos foram vítimas de fraudes cibernéticas[8];

- As questões de segurança desestimulam o comércio eletrônico[9];

- Em 2017, os crimes cibernéticos resultaram em US$ 22.500.000.000,00 (vinte e dois bilhões e quinhentos milhões de dólares) de prejuízo[10]; e

- O Brasil é o 2º com maior prejuízo com ataques cibernéticos[11].

Segundo o Relatório da “**Internet Organised Crime Threat Assessment** - IOCTA”[12], de 2018, da Agência da União Europeia para a Cooperação Policial - Europol, “a falta de legislação adequada sobre crimes cibernéticos fez com que o Brasil fosse o alvo número um e a principal fonte de ataques **online** na América

Latina; 54% dos ataques cibernéticos reportados no Brasil supostamente são originários de dentro do país". O documento prossegue afirmando que, "de modo semelhante aos EUA, o Brasil é um dos principais hospedeiros de sites de **phishing**, com alguns relatos colocando o Brasil como uma das dez maiores fontes mundiais de ataques cibernéticos".

Verifica-se, ainda, que o número de ataques cibernéticos praticamente dobrou no Brasil em 2018 em relação a 2017. Segundo informações do laboratório especializado em segurança cibernética da PSafe[13], foram detectados cento e vinte milhões e setecentos mil ataques no primeiro semestre de 2018. Esse número representa um crescimento de 95,9% em relação ao mesmo período do ano anterior. Nos últimos três meses de 2018, foram registrados sessenta e três milhões e oitocentos mil **links** maliciosos, um aumento de 12% em relação ao início daquele ano, sendo campeões de golpes os **links** de aplicativos de mensagens como WhatsApp. Ao todo, 57,4% dos ataques foram realizados por meio de **phishing**, enquanto que, em segundo, ficaram os golpes com publicidade suspeita, que somaram 19,2% dos casos.

A pesquisa **Cyber Review** 2019 da consultoria JLT[14], realizada com 200 empresas brasileiras de médio e de grande portes, apontou que 55,4% dessas empresas são totalmente dependentes do uso de tecnologia em suas atividades e que outras 35% podem ter paralizações severas diante de um problema relacionado à tecnologia. Outros dados relevantes da pesquisa são destacados a seguir:

- 80% dos entrevistados avaliaram que um incidente cibernético causaria um impacto operacional com reflexos em toda a empresa;

- 29% já avaliaram financeiramente o que esse impacto resultaria às suas organizações;

- 34% das empresas que responderam à pesquisa relataram ter sofrido algum tipo de incidente cibernético nos últimos doze meses;

- 29% das empresas que sofreram ataques tiveram impactos operacionais;

- 27,8% tiveram altos custos de reconstrução sistêmica; e

- 4% sofreram impactos de reputação frente aos clientes.

Os dados dessa pesquisa demonstram que as empresas brasileiras, principalmente aquelas consideradas como infraestruturas críticas, precisam considerar a segurança cibernética como ação prioritária de investimentos, elaborar planos de gestão de riscos e de tratamento e resposta a incidentes, assim como planejar orçamento adequado para combater os incidentes de segurança. Em mais da metade das empresas ouvidas no levantamento da **Tempest/EZ-Security**[15], o orçamento anual de segurança da informação representa até 2% do faturamento anual. Em 34,5% dessas empresas, esse percentual não ultrapassa 1%, de acordo com a mesma pesquisa.

Um ataque cibernético de grande envergadura, caso não seja adequadamente tratado, pode afetar profundamente a reputação da organização, ocasionar perda de receitas, levar a prejuízos operacionais com a paralização dos serviços, resultar em perda de informações e ainda levar à aplicação de sanções legais e administrativas.

Dessa forma, é importante que as organizações, públicas ou privadas, estabeleçam políticas e procedimentos de segurança cibernética que sejam periodicamente revisados, atendam à evolução tecnológica, ao aperfeiçoamento de processos e à necessidade de capacitação contínua e estruturada para todos os colaboradores, por meio de programas de capacitação e de treinamento. De acordo com a pesquisa **JLT CyberView** 2019, 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.

Na última década, não somente no Brasil, mas em vários países, verificou-se um aumento significativo na quantidade de serviços prestados ao cidadão por meio da internet. Dentre os diversos serviços destacam-se: o cadastramentos, a obtenção de certidões negativas, o pagamento de tributos, a segunda via de documentos e consultas, os quais são prestados em plataformas **online** no âmbito federal, no estadual e no municipal.

Iniciativas como a Política de Governança Digital - Decreto nº 8.638, de 15 de janeiro de 2016, a recente Estratégia Brasileira para a Transformação Digital - E-Digital - Decreto nº 9.319, de 21 de março de 2018[16] e a governança no compartilhamento de dados - Decreto nº 10.046, de 9 de outubro de 2019, evidenciam o forte processo de digitalização do Governo federal e os parâmetros que o embasam ao longo de sua implantação.

Acrescenta-se que essas iniciativas, com ênfase na mudança tecnológica, significam, para o sistema financeiro, a adoção dos processos denominados 4D: a democratização, a digitalização, a desburocratização e a desmonetização[17], que irão favorecer o conceito de **Open Insurance**[18], no qual, em relação ao mercado financeiro, os dados bancários vão passar a pertencer aos clientes e não às instituições financeiras.

Em virtude desse processo, e em consonância com iniciativas mais avançadas já adotadas, por exemplo, pelos países da União Europeia, consubstanciadas em relatórios como o **eGovernment Benchmark** 2018[19], ressalta-se a importância de instrumentos normativos adequados à realidade brasileira que, de fato, contribuam para a proteção dos sistemas e de redes governamentais, uma vez que os serviços apoiados nesses recursos não podem sofrer interrupções, vazamento de dados ou serem alvos de outras ações danosas.

Em ataques cibernéticos recentes, grupos de **hackers** têm considerado sistemas de governo como alvos compensadores, no intuito de provocar diferentes impactos, como: o potencial dano à imagem do Governo perante seu público interno e perante a comunidade internacional, o descrédito da população nos serviços públicos, a desconfiança de investidores internacionais na capacidade da administração pública em proteger seus próprios sistemas, a desconfiança nos processos eleitorais, e o descontentamento da população com relação à administração pública.

Além da proteção do próprio Governo, outro ponto crítico refere-se à proteção cibernética das empresas representantes das infraestruturas críticas. A título de compreensão, podemos conceituá-las como as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional. Essas empresas precisam ter uma abordagem consistente e evolutiva em segurança cibernética para identificar e avaliar vulnerabilidades, e gerenciar o risco de ameaças, ao observar , por exemplo, as cinco funções previstas na estrutura de segurança cibernética do **National Institute of Standards and Technology** - NIST, que são: Identificar, Proteger, Detectar, Responder e Restaurar[20].

Avalia-se que os principais tipos de ameaças contra essas organizações são ataques de **phishing**, negação de serviço em larga escala, vazamentos de informações privadas, espionagem e terrorismo cibernéticos e a interrupção de serviços.

A necessidade de proteção dessas empresas está crescendo em relevância. À medida que as infraestruturas de informação e de comunicação se tornam globalmente interligadas, tornam-se alvo de **malwares**, **hackers**, **hacktivistas** e de operações estatais adversas. Além disso, a interconectividade global de algumas infraestruturas críticas significa que uma parte vulnerável pode se tornar o elo mais fraco e, portanto, um risco para outras nações.

PARTE II

ANÁLISE DOS EIXOS TEMÁTICOS

Com vistas a auxiliar a formulação das ações estratégicas, foram analisados, primeiramente, os eixos temáticos que pertencem à área de proteção e de segurança, que são: a governança da segurança cibernética nacional, o universo subconectado e seguro, a prevenção e mitigação de ameaças cibernéticas, e a proteção estratégica. Em seguida, foram abordados os eixos temáticos transformadores, assim denominados pelo potencial que possuem em modificar, de forma decisiva e estruturante, os temas por eles influenciados. São eles: a dimensão normativa, a pesquisa, desenvolvimento e inovação, a dimensão internacional e parcerias estratégicas, e a educação.

1. EIXOS TEMÁTICOS: PROTEÇÃO E SEGURANÇA

1.1. Governança da Segurança Cibernética Nacional

Na análise deste eixo temático, serão abordados aspectos relativos a mecanismos e medidas passíveis de adoção em prol da governança cibernética, a metodologia de gestão de riscos, a confiança e segurança no uso do certificado digital, a implantação de modelo centralizado de coordenação da segurança cibernética nacional, e o monitoramento do cenário cibernético.

Com relação aos mecanismos e às medidas em prol da governança cibernética, analisa-se, inicialmente, a concepção de governança. Nota-se que esse conjunto de processos de gestão, em qualquer área, é de vital importância para alinhar o planejamento de uma organização às suas ações estratégicas, otimizar o emprego de recursos, elevar a qualidade dos serviços prestados e permitir a condução exitosa de projetos e de processos. Em segurança cibernética, esse aspecto adquire especial relevância, em virtude da profusão de atores relacionados ao tema, da capilaridade e da transversalidade do assunto em diferentes áreas da sociedade, e da multilateralidade de ações previstas e em andamento.

Nesse sentido, a governança cibernética abrange o desenvolvimento e a aplicação de princípios comuns, de normas, de procedimentos e de programas que moldam a evolução e o uso das ferramentas digitais.

A segurança da informação é obtida através da implementação de controles, de processos, de políticas e de procedimentos, que juntos fortalecem os objetivos de negócio com a minimização dos seus riscos, e a promoção da segurança da organização (NBR ISO/IEC 17799:2005).

Abordam-se, ainda, ações voltadas à comunicação de ataques cibernéticos e de ações maliciosas, ao fortalecimento da capacidade institucional dos órgãos públicos em segurança cibernética, aos mecanismos de liderança, aos manuais de boas práticas, aos requisitos mínimos e às recomendações, ao monitoramento de políticas públicas, à gestão de riscos, ao atendimento dos interesses da sociedade, à custódia de dados por órgãos públicos e aos certificados em segurança cibernética, além das ações voltadas a outras temáticas.

Para subsidiar e orientar a análise dos eixos temáticos de proteção e segurança, foram considerados os seguintes aspectos:

- confiança da população nos serviços públicos **online**;

- garantia, pela administração pública, de que seus órgãos protegem suas redes e sistemas, conforme a legislação sobre o tema;

- investimento governamental na prestação de serviços digitais;

- atendimento das normas de segurança cibernética, pelos fornecedores de bens e de serviços aos órgãos de governo; e

- necessidade de informações atualizadas que subsidiem a política governamental atual, o planejamento de novas diretrizes e a futura concepção de programas.

A governança na área cibernética está relacionada às ações, aos mecanismos e às medidas a serem adotados com o fim de simplificar e modernizar a gestão dos recursos humanos, financeiros e materiais, e acompanhar o desempenho e avaliar os resultados dos esforços empreendidos nesse campo.

Essa governança visa incorporar elevados padrões de conduta em segurança cibernética, e orientar as ações de agentes públicos e de agentes privados, ao considerar o papel que exercem em suas organizações, conforme a finalidade e a natureza de seu negócio.

Inclui, ainda, o planejamento voltado à execução de programas, de projetos e de processos, e o estabelecimento de diretrizes que irão nortear a gestão de riscos. Nesse contexto, orienta pessoas e organizações quanto à observância das normas, dos requisitos e dos procedimentos existentes em segurança cibernética.

Segundo o Decreto nº 9.203, de 22 de novembro de 2017, em seu art. 17[21], tem-se que “a alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional”.

Nesse contexto, ressalta-se a importância de as empresas, que produzem ou comercializam serviços no campo da segurança cibernética, adotarem padrões nacionais e internacionais no desenvolvimento de novas soluções, desde a sua concepção, o que é internacionalmente conhecido pelos termos **privacy by design and default** e **security by design and default**. Para tanto, destaca-se o papel do Estado em garantir às empresas a flexibilidade para continuar a criar mecanismos de aperfeiçoamento, com o uso de tecnologia de ponta para garantir a segurança de seus produtos, serviços e soluções e, assim, proteger seus usuários.

Visualiza-se que a governança cibernética, considerada em âmbito nacional, orienta os direitos, as obrigações e as responsabilidades dos diversos segmentos da sociedade, e leva os órgãos públicos e as organizações privadas a priorizarem o uso seguro do espaço cibernético.

Nesse sentido, verifica-se a importância de as instituições implementarem programas de segurança cibernética, com uso de modelos reconhecidos, que proporcionem um adequado diagnóstico do estágio em que se encontram, que identifiquem os pontos mais vulneráveis de seus sistemas, as ameaças

cibernéticas mais prováveis, e os maiores fatores de risco que considerem a adoção das proteções adequadas, os mecanismos de detecção de ataques, as metodologias de resposta a incidentes e os procedimentos de restauração do ecossistema informático.

Com relação à definição de papéis e de responsabilidades, vê-se que o cidadão brasileiro precisa elevar sua participação no ecossistema digital, não somente por meio do uso das tecnologias, porém, principalmente, no combate aos crimes cibernéticos, à chamada pirataria de **software**[22] e às ações maliciosas, ao reportar, por meio dos canais específicos de denúncia, todos os ilícitos cibernéticos de que for vítima.

No que tange à gestão de riscos, verifica-se que é um dos principais pontos de sustentação da governança cibernética, uma vez que indica a adoção de melhores políticas e metodologias, o que permite gerir, de forma otimizada, os limites aceitáveis de risco. Essa gestão resume-se aos princípios, aos objetivos, às estruturas, às competências e aos processos necessários para se conhecer as vulnerabilidades, e assim permitir que sejam tratadas de modo eficaz, sendo, portanto, uma ferramenta que permite a cada instituição, dentre outros benefícios, ter a perfeita dimensão de seus pontos críticos e dos ativos mais relevantes a proteger.

Em 13 de outubro de 2008, o Gabinete de Segurança Institucional da Presidência da República publicou a Norma Complementar nº 02/IN01/DSIC/GSI/PR, que dispõe sobre a metodologia de gestão de segurança da informação e dá orientações acerca de definição de riscos, de procedimentos para identificar os riscos e seus níveis aceitáveis, da análise de impactos e de probabilidades e de opções de tratamento dos riscos. Adicionalmente, em 15 de fevereiro de 2013, o Gabinete de Segurança Institucional da Presidência da República publicou a Norma Complementar nº 04/IN01/DSIC/GSI/PR, que estabelece diretrizes para o processo de gestão de riscos de segurança da informação e comunicações nos órgãos ou entidades da Administração Pública federal, direta e indireta. Essa norma faculta que cada órgão ou entidade pública adote uma metodologia de gestão de riscos de segurança da informação que atenda aos objetivos, às diretrizes gerais e ao escopo definido, e que contemple, no mínimo, os critérios de avaliação e de aceitação do risco.

Com o tempo, verificou-se que cada instituição adota metodologias e arcabouços internacionais diferentes, que, dentre outras coisas, fornecem: políticas de orientação de segurança, recomendações de boas práticas e guia para auxiliar as empresas na avaliação e no aprimoramento dos seus sistemas de controle interno, o que inclui a avaliação de riscos.

A adoção desses arcabouços de forma distinta entre os órgãos e entidades públicas e empresas do setor privado, dificulta a análise do grau de maturidade em segurança cibernética do País de forma geral, uma vez que os critérios e requisitos de cada normativo não são os mesmos, so que torna necessário padronizar as melhores práticas e permitir que mesmo pequenas organizações possam adotar medidas eficientes para a proteção de suas informações. Desse modo, destacam-se a avaliação e a gestão de risco em segurança cibernética como fatores chaves para a proteção do espaço cibernético, dos serviços e das informações nele existentes.

Entretanto, verificou-se que a adoção de padrões únicos e excludentes de governança não produziriam necessariamente resultados positivos, ao considerar a transversalidade e a capilaridade das ações de segurança cibernética nas instituições públicas e privadas e na sociedade em geral. Ressalta-se, ainda, que políticas de governança cibernética devem corresponder a processos contínuos que façam parte da cultura de entidades públicas e privadas.

Em consequência, no contexto mais amplo de governança, recomenda-se, como patamar inicial, a observância das normas emitidas pelo Gabinete de Segurança Institucional da Presidência da República. Entretanto, sabe-se que essas normas não são exaustivas, e devem ser consultadas e, quando pertinentes, também adotadas as normas correlatas da Organização Internacional para Padronização (ISO, do inglês **International Organization for Standardization**), além de outros padrões metodológicos, tais como o **Control Objectives for Information and related Technolog** - COBIT[23], o **National Institute of Standards and Technology** - NIST[24] e o discorrido pelo **Center for Internet Security** - CIS[25]. Desse modo, encorajam-se as empresas a adotarem medidas customizadas de segurança e ferramentas para tratar os riscos enfrentados pelo seu modelo de negócio específico.

A observância desses padrões pelos diferentes atores nacionais, para a elaboração de seus normativos em segurança cibernética, mostra-se relevante, uma vez que fornecem estruturas amplamente avaliadas e baseadas em consenso para definir e implementar abordagens eficazes para a segurança cibernética que possam ir ao encontro de desafios comuns, e assim possibilitar colaboração e interoperabilidade.

As ações de governança devem, ainda, de acordo com o contexto de cada instituição, contemplar conceitos de segurança cibernética que abordem iniciativas integradoras e que permitam a macro gestão de diversos ativos e de diferentes tecnologias, como uma plataforma SOAR - **Security Orchestration Automation and Response**, que consiste em um conjunto de soluções[26] de **softwares** compatíveis que permitem que uma organização colete dados sobre ameaças de segurança de várias fontes.

Uma plataforma SOAR inclui uma série de recursos[27] de gestão de segurança, análise e relatórios que utilizam dados legíveis de múltiplas fontes para oferecer relatórios, análises e funções de automatização de fluxos de trabalho para diversas equipes de segurança, e oferecemr a inteligência que as soluções pontuais, como SIEM (**software**[28] de gerenciamento de informações e eventos de segurança) - soluções de resposta a incidentes e escaneamento de vulnerabilidades, não oferecem. Portanto, a partir de soluções como o SOAR, espera-se responder adequadamente a eventos de segurança, e a aprimorar a eficácia das operações no cenário digital.

Uma plataforma SOAR pode, portanto, gerenciar diversos recursos[29], como por exemplo: os dispositivos portáteis, os sistemas de proteção de **endpoints**, os servidores, a segurança de e-mail, os roteadores, os **switches**, os sistemas de **Wireless**, os pontos de acesso, os **firewalls**, os sistemas de arquivos, os servidores DNS (**Domain Name System**), os protocolos DHCP (**Dynamic Host Configuration Protocol**), os IDS (**Intrusion Detection System**), os IPS (**Intrusion Prevention System**) e as soluções SIEM.

Por oportuno, entende-se que a certificação de produtos e de soluções em segurança cibernética é um objetivo a ser perseguido, ao considerar a complexidade dos equipamentos e das ferramentas computacionais, que exigem elevado grau de especialização e de recursos tecnológicos à disposição, e de organismos estruturados e equipados para conduzi-la. Destaca-se que, antes de fomentar e desenvolver uma certificação própria, recomenda-se buscar alavancar os mecanismos de certificação existentes, para evitar a criação de barreiras comerciais.

Entretanto, é crescente o entendimento, no meio produtivo, de que a certificação de produtos - mais especificamente, de equipamentos - não se mostra algo simples, uma vez que a certificação ocorre sobre o tipo, o modelo e o **firmware** de um equipamento, o que impede sua atualização de **firmware** ou que o fabricante disponibilize **patches** de segurança, sob pena de levar o produto a perder a certiticação inicial.

Outro aspecto a considerar quando se aborda proteção e segurança no ambiente cibernético é a confiança proporcionada pelo certificado digital, que pode ser compreendido como uma identidade eletrônica segura para pessoas ou organizações, e com autenticidade garantida por uma criptografia complexa. Com ele, é possível garantir de forma inequívoca a identidade de um indivíduo ou de uma instituição, sem uma apresentação presencial[30].

O certificado digital garante a confidencialidade, a autenticidade, e a comprovação de autoria em transações eletrônicas assinadas por meio de sua utilização.

Esse recurso é muito relevante e incentiva a padronização das práticas de validação e de autenticação, uma vez que diversos certificados possuem aceitação internacional. Assim, a adoção da certificação digital deve ser incentivada. Destaca-se que o seu uso em documentos públicos (carteira de identidade, título de eleitor ecadastro de pessoa física), pode ser uma forma de propagar um ambiente de acesso mais seguro e confiável.

No Brasil, a certificação digital foi introduzida em 2001. Dentre os pioneiros em sua utilização, destacam-se o Banco Central do Brasil, por meio do Sistema de Pagamentos Brasileiro - SPB, e a Receita Federal do Brasil, que a utilizou em serviços como o Centro Virtual de Atendimento ao Contribuinte - e-CAC, e para a emissão da Nota Fiscal Eletrônica - NF-e, que colabora para otimização dos processos e possibilita um maior controle para reduzir fraudes e sonegação fiscal.

O judiciário brasileiro também utiliza extensivamente a certificação, desde a edição do Diário da Justiça em formato eletrônico até o peticionamento eletrônico disponível em vários tribunais. São várias as aplicações que fazem uso do certificado digital ICP-Brasil, e possibilitam confiança e segurança digital.

De acordo com o Instituto Nacional de Tecnologia da Informação, até abril de 2019, a emissão de certificados superou 35,6% do número registrado no mesmo período de 2018. Entretanto, do total de emissões em 2019, os certificados emitidos para pessoa física representaram somente 8,4%, enquanto que, para pessoa jurídica, representaram 45,9%[31].

Hoje, praticamente, todas as pessoas jurídicas possuem ao menos um certificado digital. Entretanto, a certificação digital ainda não é amplamente utilizada nas corporações, em virtude de certas dificuldades, como a elevada quantidade de processos para emissão dos certificados, o alto custo para o cidadão e o baixo número de unidades certificadoras por habitante. A fim de solucionar essas questões, o Governo federal vem adotando ações para otimizar os processos visando à sua obtenção, com o propósito de expandir significativamente a oferta desse recurso. Todavia, há que se ter o devido cuidado de, em nome da celeridade e da disseminação da certificação digital, não fragilizar as medidas de segurança relativas à sua concessão, que levem ao comprometimento desse valioso recurso.

Com relação ao estudo do modelo mais adequado para coordenação das ações de segurança cibernética, é importante destacar que a gestão dessas ações envolve múltiplos atores. Tanto no âmbito nacional, quanto no internacional, uma mobilização efetiva para a consolidação da segurança cibernética, como

vital para o desenvolvimento da sociedade brasileira, terá mais sucesso por meio de assertiva coordenação política, que inclua o setor privado e a sociedade.

Segundo relatório da Comissão Parlamentar de Inquérito da Espionagem[32], a distribuição e o trato dos assuntos relacionados à segurança cibernética no País, não tem colaborado para que o Governo possua uma visão geral do assunto, o que dificulta a execução de ações mais eficazes nesse campo. Isso ocorre porque cada órgão público adota definições, critérios e diferentes ações para a proteção do ambiente digital, sem compartilhar informações, boas práticas e as soluções adotadas para cada incidente cibernético.

Nesse sentido, a criação de um sistema que reúna todos os atores estatais e não estatais sob a égide da segurança cibernética, poderá contribuir para o necessário alinhamento estratégico, doutrinário e operacional nas ações concernentes a esse campo, e cabe ao Governo federal incentivar a discussão de alternativas que levem ao fortalecimento institucional da segurança cibernética brasileira. Nesse contexto, é importante que se conceda a um órgão governamental a responsabilidade de orientar o tema em âmbito nacional, organizá-lo, e propor medidas e regulamentos, com a participação de representantes de todos os setores da sociedade. Faz-se exceção, apenas, aos aspectos relacionados à defesa e à guerra cibernéticas, que estão a cargo do Ministério da Defesa, o que de modo algum impede a necessária interação, nesse viés, entre as áreas de segurança e de defesa.

O modelo centralizado de gestão em segurança cibernética apresenta-se como alternativa viável e eficaz, e foi adotado por países como Estados Unidos da América, Reino Unido, Portugal, França, Índia, Malásia, Singapura, Coréia do Sul e Japão. A experiência desses países demonstra que a criação de estruturas centrais para condução desse tema, com autoridade para estabelecer regulamentos e ações específicas, apresenta bons resultados para a coordenação e a consolidação da segurança cibernética como assunto de Estado, promove sinergia entre Governo, setor privado, sociedade e academia, e evidencia o caráter estratégico da proteção do espaço cibernético.

No caso brasileiro, ao consider o Governo federal, destaca-se a atuação do Gabinete de Segurança Institucional da Presidência da República que, desde 2006, por meio do Departamento de Segurança da Informação, estuda e elabora diversos normativos, que consistem em Instruções Gerais, Normas Complementares, Estratégias e Política, no âmbito da Administração Pública federal, ao reunir, desde então, vasta experiência com relação a diversas áreas da segurança da informação, especialmente no que tange à segurança cibernética.

Desse modo, não se vislumbra a necessidade da criação de novos e dispendiosos organismos governamentais, sendo suficiente redimensionar a atual estrutura do Gabinete de Segurança Institucional da Presidência da República, de forma a lhe possibilitar a atuação em âmbito nacional. Portanto, urge a necessidade de uma lei que regule as ações de segurança cibernética, que especifique atribuições, que aponte mecanismos de diálogo com a sociedade e que torne possível, ao Gabinete de Segurança Institucional da Presidência da República, com a participação de representantes de todos os entes nacionais, exercer o papel de macro coordenador estratégico, ao proporcionar alinhamento às ações de segurança cibernética e ao contribuir para a evolução de todo o País nesse campo, de forma convergente e estruturada. Conclui-se, ainda, ser necessário e urgente que o Governo federal priorize a aplicação de recursos na área da segurança cibernética.

Outrossim, conforme mencionado no parágrafo anterior, devem ser considerados mecanismos que viabilizem a participação da sociedade. Dentre os instrumentos possíveis, esta Estratégiarecomenda a criação de um conselho nacional de segurança cibernética, que congregue diversos atores estatais e não estatais, com o objetivo de pensar a segurança cibernética sob um prisma abrangente, inclusivo, moderno e com ênfase nas reais necessidades nacionais.

Além desse conselho, como estímulo ao debate sobre o tema, a E-Ciber incentiva a criação de diversos grupos de debate, sob coordenação do Gabinete de Segurança Institucional da Presidência da República, de modo a se garantir o envolvimento de profissionais com conhecimentos setoriais e especialidades relevantes para uma melhor compreensão dos desafios a serem dirigidos aos vários setores de acordo com realidades específicas.

No tocante ao monitoramento do cenário cibernético, observa-se a necessidade da verificação contínua da eficácia dos instrumentos normativos, o que passa, necessariamente, por seu monitoramento e por sua constante avaliação. Avaliações que produzem resultados confiáveis permitem o aprimoramento de políticas e justificam investimentos ou economia de recursos, já que evidenciam se os resultados esperados são alcançados e se os recursos são utilizados de modo eficiente. Conforme as diretrizes de governança pública estabelecidas no Decreto nº 9.203, de 2017[33], vê-se a importância de igualmente prever métricas e indicadores que permitam, no futuro, o monitoramento das ações, dos programas e dos projetos voltados à segurança cibernética, de modo a se obter contínua eficácia na gestão das ações referentes a essa área.

Dentro dessa perspectiva, ressaltam-se três vertentes importantes: a medição da eficácia e da eficiência dos centros de tratamento e resposta aos incidentes computacionais, a elaboração de indicadores para medir o desempenho do País em segurança cibernética e o estabelecimento de rotina de

verificações de conformidade em segurança cibernética dentro dos órgãos públicos e das entidades privadas, por eles conduzidas, de modo que seja possível estabelecer a correta relação entre os aspectos técnicos detecnologia da informação, como análise de vulnerabilidades, relatórios técnicos de ameaças e relação de soluções em tecnologia, com os aspectos de negócio, como continuidade dos serviços prestados, riscos à imagem e processos de tomada de decisão. Entende-se, portanto, a verificação de conformidade como um processo natural, baseada em programas estabelecidos pelas próprias entidades públicas e privadas, que visa ao aprimoramento contínuo dos sistemas voltados à segurança cibernética.

Destaca-se que as verificações de conformidade devem ser planejadas com moderação, e devem ser baseadas em princípios de razoabilidade, para que não levem as instituições públicas e privadas a empregarem tempo e grande soma de recursos em procedimentos excessivos de conformidade, em detrimento de seu uso para lidar com ameaças cibernéticas.

1.2. Universo conectado e seguro: prevenção e mitigação de ameaças cibernéticas

O processo de preparação do País rumo à nova economia digital, experimentará forte impacto de variadas tecnologias, como internet das coisas, computação quântica, inteligência artificial, aprendizado de máquina, ciência cognitiva, robótica, biotecnologia, nanotecnologia ou geração de telefonia 5G. Para prover sustentação a esse processo, são necessárias ações que permitam sua viabilização de forma segura e resiliente.

Para fazer face a esse desafio, este eixo da E-Ciber versará sobre a gestão de incidentes computacionais, que envolve detecção, triagem, análise e resposta a esses incidentes.

As atividades preventivas baseadas nas avaliações de riscos podem reduzir o crescente número de incidentes cibernéticos, entretanto, não podem evitá-los totalmente. Portanto, é necessário um recurso de resposta para detectá-los com rapidez, minimizar a perda e a destruição que podem causar, atenuar os pontos fracos explorados e restaurar os serviços de tecnologia da informação e comunicação, sempre considerando que o acompanhamento das ameaças à segurança cibernética devem ter natureza global.

Nesse contexto, destaca-se a relevância de recursos e de mecanismos que permitam a interação e o compartilhamento de informações em diferentes níveis, entre instituições públicas e privadas, e entre essas e organizações internacionais, que possuam experiência no acompanhamento de tendências de ameaças e de ataques cibernéticos, de forma a consider os impactos regionais, multilaterais e globais da ocorrência de incidentes no ambiente digital.

É de amplo conhecimento que toda organização, pública ou privada, deve possuir uma equipe de tratamento e resposta aos incidentes cibernéticos - ETIR, também conhecida pela sigla - CSIRT, de **Computer Security Incident Response Team**. Essa equipe deve ser capacitada, e deve dispor de ferramentas computacionais adequadas às suas necessidades, e de sistemas baseados em tecnologias emergentes, condizentes com os padrões internacionais. Atualmente, o Brasil possui oito tipos de centros de tratamento e resposta aos incidentes cibernéticos, de acordo com sua atuação:

- Centros de Responsabilidade Nacional - CERT.br e CTIR Gov.

- Centros de Coordenação Internacional - CERT/**Coordination Center**, FedCirc e FIRST.

- CSIRTs de Infraestruturas Críticas - Energia - CSIRTCemig - Financeiro - CSIRTs do BB, da Caixa, do BASA, do BNB, do BRB e do BANESE - Telecom - CTIR/DATAPREV, GRA/SERPRO e CSIRT PRODESP.

- CSIRTs de Provedores - CSIRT Locaweb e CSIRT HP.

- CSIRTs Corporativos - CERT-RS, SEGTIC UFRJ e CSIRT Unicamp.

- CSIRTs Acadêmicos - CAIS/RNP, CEO/RedeRio, CERT-RS, CERT.Bahia, CSIRT POP-MG, CSIRT Unicamp, CSIRT USP, GSR/INPE, GRC/UNESP, NARIS/UFRN e TRI/UFRGS.

- CSIRTs do Poder Público - Executivo - CTIR Gov, Legislativo - GRIS-CD e Judiciário - GATI, CLRI e TRF-3.

- CSIRTs Militares - Marinha - CTIM, Exército - CCTIR/EB e Aeronáutica - CTIR.FAB.

Esses centros atuam em constante comunicação, e mantêm registros de incidentes nacionais, para avaliação de dados estatísticos referentes às ameaças e a esses incidentes. Os atuais esforços concentram-se em simplificar o compartilhamento de informações entre todos os CSIRTs, uma vez que o número de atores do Governo e do setor privado está-se ampliando, ao lado dos crescentes desafios no campo cibernético.

O Brasil possui dois centros de tratamento e resposta de responsabilidade nacional. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br[34], é o responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à internet no País, mais voltado às redes comerciais e de instituições privadas. Com atribuição similar, porém voltado às redes governamentais, existe o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov[35]. Hoje, os serviços fornecidos pelo CTIR Gov incluem, basicamente: a notificação de incidentes, a análise de incidentes, o suporte à resposta a incidentes, a coordenação na resposta a incidentes, a distribuição de alertas, de recomendações e de estatísticas e a cooperação com outras ETIRs.

Como exemplo de Alerta expedido pelo CTIR Gov, tem-se o Alerta nº 03/2019 - **Malware Silex** em dispositivos IoT, documento que pode ser encontrado no sítio desse Centro.

Para exercer suas funções, o CTIR Gov possui mecanismos que monitoram vulnerabilidades, adulterações e indisponibilidade de sítios, anúncios de vazamento de informações, e que verificam redes sociais abertas. Além disso, atua em cooperação com órgãos parceiros em segurança cibernética, ao integrar uma rede internacional de CSIRTs, com forte atuação na análise de possíveis ações massivas.

Destaca-se que o trabalho de um CSIRT pode ser aprimorado mediante pesquisas e consultas a padrões globais, o que pode facilitar a comunicação entre outros analistas de incidentes, operadores detecnologia da informação, fabricantes de equipamentos detecnologia da informação, e demais representantes da iniciativa privada e do meio acadêmico. Neste sentido, modelos como o descrito pela **Common Vulnerabilities and Exposures** - CVE[36], podem ser de grande utilidade.

Nesse contexto, considera-se essencial adotar ações que permitam o acompanhamento contínuo e proativo das ameaças e dos ataques cibernéticos, e que possibilitem o estabelecimento de meios de comunicação adequados com grupos internos e externos à própria organização. Canais de comunicação podem ser ampliados, também, em âmbito internacional, por meio da participação em foros como os seguintes:

- FIRST: Forum of Incident Response and Security Teams

- Criação: 1990.

- Membros: quatrocentos e oitenta e três CSIRTs, em noventa e dois países, participantes de todos os setores.

- APWG: Antiphising Working Group

- Criação: 2003.

- Membros: mais de duas mil organizações, participantes de todos os setores, incluindo organizações internacionais.

- M3AAWG: Messaging, Mobile, Malware Anti-Abuse working Group

- criação: 2004.

- Membros: mais de duzentos CSIRTs, pertencentes ao setor industrial.

- LAC-AAWG: Latin America and Caribbean Anti-Abuse Working Group

- Criação: 2017

- Membros: Comunidade da internet em geral.

Com o fim de demonstrar a ação do CTIR Gov diante das notificações recebidas, conforme o relatório dos incidentes reportados e confirmados por aquele Centro, de 2011 a 2018, tem-se que, dentre as notificações recebidas, 26,23% correspondem a abuso de sítio, 20,04% correspondem a vazamento e 15,95% correspondem a fraude, sendo essas as maiores categorias de incidentes.

Nesse sentido, segundo publicação do CERT.br, foram recebidas, em 2018, mil e setenta e cinco notificações de máquinas comprometidas. Esse total foi 168% maior em relação ao recebido em 2017. Mais de 98% das notificações foram referentes a servidores **web** que tiveram suas páginas desfiguradas[37]. Entretanto, como os casos são relatados de forma voluntária, é provável que o número real de incidentes seja muito maior, já que os incidentes cibernéticos direcionados a usuários são, em maior parte, relacionados a fraudes.

No atual cenário de ameaças cibernéticas, é provável que as organizações experimentem o mesmo tipo de ataque, o que ressalta a importância das informações sobre fato, sobre o tratamento realizado e sobre as lições aprendidas. Nesse contexto, visa-se à atuação conjunta em prol da segurança cibernética, e considera-se de suma importância a criação de um ambiente colaborativo, do qual participem a administração pública, o setor privado, a academia e a sociedade em geral.

Um exemplo de ação colaborativa é o exercício Guardião Cibernético, organizado anualmente pelo Comando de Defesa Cibernética, em parceria com oGabinete de Segurança Institucional da Presidência da República. A atividade consiste em treinamento de ações de proteção cibernética, por meio da cooperação entre Forças Armadas, órgãos parceiros e representantes das infraestruturas críticas, ao adotar técnicas virtuais de simulação e práticas de gestão de incidentes. O exercício emprega gabinetes de crise das áreas de tecnologia da informação e comunicação, de comunicação social, jurídica e da alta administração dos participantes, que são levados a apresentar soluções para os eventos cibernéticos com impacto nas organizações, incluindo o nível decisório-gerencial (gestão de crise) e o nível técnico (resposta a incidentes) das empresas e de órgãos de governo.

Outra abordagem nesse contexto, com o objetivo de promover um ambiente colaborativo, participativo e seguro, pode ser a implementação de uma plataforma de compartilhamento de ameaças ou de tendências cibernéticas, onde o intercâmbio de informações ocorra de maneira padronizada, rápida e segura.

Destaca-se que o compartilhamento de informações é uma forma de evidenciar a parceria estratégica entre os principais atores interessados em segurança cibernética, de todos os setores da sociedade. Desse modo, aqueles atores responsáveis pela exploração e pelo gerenciamento de infraestruturas críticas - sejam eles órgãos da administração pública ou empresas do setor privado - possuem melhores condições de compartilhamento de informações que possam auxiliar na mitigação de riscos, na análise de ameaças e no estudo de vulnerabilidades emergentes, enquanto que os órgãos públicos especializados em segurança cibernética, possuem condições de fornecer informações primordiais sobre aspectos relacionados ao **status** da segurança nacional.

O País necessita, ainda, fortalecer e aperfeiçoar seus órgãos de governo que tratam das ameaças e que combatem os crimes cibernéticos. Uma vez que o CTIR Gov é o órgão central do governo que coordena e realiza ações destinadas à gestão de incidentes computacionais, recomenda-se outorgar a esse órgão atuação em âmbito nacional, e que deve ser fortalecido. Na mesma direção, recomenda-se aperfeiçoar a estrutura nacional de investigação de crimes cibernéticos.

Atualmente, a comunicação pode ser alvo de interceptação ilegal que, de forma pontual, pode não ser evitada pelas políticas de segurança cibernética adotadas tanto pelas prestadoras de serviços de telecomunicações quanto por parte de outros atores, e promovida por agentes com diferentes intenções, como busca de informações, assédio a pessoas com determinado perfil ou tentativa de prejudicar a realização de algum projeto, entre outras razões. Assim, a comunicação digital pode ser monitorada ou interceptada, das seguintes formas:

- dispositivos pessoais ou organizacionais, infectados com **malware** ou monitorados diretamente;

- roteador **wi-fi**, infectado com **malware** ou controlado por terceiros;

- provedores de internet infectados, seja por intenções próprias ou de terceiros;

- ponte de rede nacional (**gateway**), independente de localização do interceptado;

- cabos com derivação para desvio das comunicações;

- **website** do serviço utilizado; e

- qualquer um dos serviços que armazena ou roteia sua comunicação.

Embora algumas recomendações sobre segurança digital sejam adaptadas a uma ferramenta, a uma tecnologia de rede ou a um meio de comunicação específico, outras recomendações são universais. Nesse aspecto, recomenda-se estabelecer protocolos e requisitos referentes à prevenção, ao monitoramento, ao tratamento, e à resposta aos incidentes computacionais, voltados principalmente às equipes especializadas que tratam das ameaças cibernéticas.

Além disso, orienta-se a mitigar os riscos, considerado os detalhes do ambiente, de forma a manter os dispositivos atualizados,e a evitar códigos maliciosos, atentar-se aos ataques de **phishing**, preferir serviços confiáveis, criar senhas fortes, utilizar criptografia e compartilhar essas práticas com aqueles agentes relacionados no processo da comunicação. Considera-se, ainda, que o uso adequado de recursos criptográficos comprovadamente habilita uma camada de segurança adicional de extrema relevância para atingir os níveis desejados de proteção de dados em repouso ou em trânsito.

1.3. Proteção Estratégica

Na análise deste eixo temático, serão abordados aspectos relativos à proteção cibernética do Governo e à proteção cibernética das infraestruturas críticas.

O País encontra-se em pleno processo de digitalização de serviços públicos, o que confere progressiva criticidade às redes e aos sistemas de governo, que apoiam a prestação desses serviços ao cidadão. Observa-se o mesmo processo com relação às estruturas de comunicação entre os entes governamentais, cujo nível de proteção deve ser adequado e proporcional à sua relevância.

Para dar suporte efetivo à E-Digital e ao mesmo tempo conferir proteção cibernética aos sistemas de gestão e aos sistemas utilizados pelas repartições públicas, é necessário reduzir a vulnerabilidade das organizações governamentais contra qualquer tipo de ameaça cibernética, ao proporcionar à administração pública níveis adequados de segurança e de resiliência contra ataques cibernéticos.

Uma vez que a mitigação de ataques envolve a articulação de diferentes atores no âmbito nacional e, por vezes, no âmbito internacional, cresce em relevância a necessidade de ações a curto, médio e longo prazo para enfrentar esses ataques de forma eficaz, de forma a considerar que podem ser realizados por países, grupos ou indivíduos,que buscam interesses políticos, vantagens econômicas ou mesmo prejudicar a prestação de serviços essenciais à sociedade, causando danos de toda ordem.

O Brasil carece de ações de capacitação que alcancem diferentes esferas de governo, ao tempo em que necessita dedicar atenção especial à proteção das infraestruturas críticas nacionais. Faz-se mister, ainda, especificar ações que protejam a estrutura relacionada à internet, como grandes servidores, pontos de troca de tráfego e **datacenters**, uma vez que proporcionam o funcionamento dos setores críticos da rede.

Em relação à proteção das redes e dos sistemas governamentais, em virtude da crescente integração de serviços, de bases de dados e de plataformas digitais, nota-se o aumento das vulnerabilidades, que podem ser exploradas por **hackers**. Nesse sentido, destaca-se que o Governo deve empregar recursos para que a segurança cibernética seja implementada e adequada à proteção de suas estruturas computacionais, para que a prestação de serviços ao cidadão não sofra solução de continuidade. Ressalta-se que esses recursos devem compor um conjunto estruturado de investimentos em conhecimento, em políticas, em profissionais e em tecnologias, dentre outros.

Nesse contexto, as informações custodiadas por órgãos públicos revestem-se de caráter sensível, pelo potencial de impacto negativo na prestação de serviços à população, em caso de comprometimento. Com relação a essas informações, recomenda-se que os órgãos públicos possuam cópias de segurança frequentemente atualizadas, segregadas de forma automática e armazenadas em local protegido. Essa prática objetiva restringir os ataques maliciosos ao ambiente produtivo original, e diminuir os riscos de sequestro de dados, de perdas financeiras, de impactos negativos à imagem, e de descontinuidade dos serviços por prazos inaceitáveis.

Os dispositivos móveis funcionais, conectados à internet e utilizados com frequência por autoridades públicas, podem ser alvos de ilícitos cibernéticos, e merecem atenção, especialmente no caso dos órgãos que permitem, em suas políticas de segurança, a utilização desses equipamentos na modalidade conhecida como BYOD, sigla de **Bring Your Own Device** ou traga seu próprio dispositivo, em que o administrador do sistema permite a conexão, à rede do órgão, de um equipamento particular.

Nesse ponto, considera-se vital a segurança de **endpoints**, nome pelo qual são conhecidos, na área de rede de computadores, os dispositivos finais[38] que estão conectados em um terminal de rede. Trata-se, portanto, de qualquer dispositivo que esteja conectado em uma rede, interna ou externa.

O moderno e ágil fluxo de informações em uma organização exige rápida resposta, que nem sempre vem de uma estação de trabalho - um **desk** - corporativo, já que podem vir de **smartphones**, **notebooks** ou **tablets** conectados à rede corporativa. Por isso, esses **endpoints** devem ser escopo de um conjunto de medidas que visem bloqueá-los contra ameaças cibernéticas e mantê-los livres de ataques. Ao bloquear os terminais de rede[39], a segurança de **endpoint** impede que brechas e vulnerabilidades dos dispositivos conectados sejam utilizadas por **hackers** para invadir e roubar dados corporativos.

A preocupação e as ações de proteção voltadas aos **endpoints** são plenamente justificáveis, dado o crescimento de ameaças cibernéticas sobre eles. Segundo o AVTEST, mais de nove milhões de novos casos de **malware** são observados por mês[40], tendo por alvo não apenas os sistemas **Windows®**, mas também[41] o **macOS®**, o **Linux** e o **Android®**.

Outro ponto que se tem destacado dentre as preocupações de segurança cibernética do Governo refere-se aos ataques sofisticados e direcionados às cadeias de suprimentos. Um ataque à cadeia de suprimentos (**Supply Chain Attack**, em Inglês), ocorre quando há infiltração em um sistema por meio de um fornecedor, de uma empresa parceira ou de um provedor externo com acesso a sistemas e a dados. Esse tipo de ataque, em geral, causa perdas financeiras e reflete negativamente na imagem dos fornecedores,de forma a levar à perda de confiança e à afetar profundamente os negócios.

Nesse sentido, recomenda-se o estabelecimento de requisitos mínimos de segurança cibernética em contratos por parte dos órgãos e entidades do Governo, o que exerceria dupla função: a primeira, de aprimorar a segurança cibernética do setor público e, a segunda, de incentivar uma segurança mais efetiva em todo o mercado, que para comercializar com o Governo, deverá atentar para esses requisitos na prestação de serviços e na venda de equipamentos.

Na elaboração dos instrumentos contratuais, recomenda-se que os entes governamentais, no estabelecimento desses requisitos, assegurem que sejam orientados para o mercado, coerentes com o universo privado nacional e alinhados aos padrões internacionalmente conhecidos.

A proteção às infraestruturas críticas, por sua relevância, merece abordagem específica. No Brasil, essas organizações a serem protegidas, escopo desta Estratégia, são as pertencentes ao setor de Telecomunicações, ao setor de Transportes, ao setor de Energia, ao setor de Água e ao setor Financeiro.

Não obstante o setor de Saúde não tenha sido contemplado no rol de infraestruturas críticas, podemos considerá-lo em âmbito análogo, uma vez que suas instituições representantes prestam serviços essenciais à sociedade. A elas, portanto, consideramos válidas e adequadas as mesmas recomendações sobre segurança cibernética dedicadas aos outros cinco setores abordados por estaEstratégia.

De modo semelhante destaca-se a relevância estratégica da indústria farmacêutica, e o impacto que ataques cibernéticos bem sucedidos podem causar sobre ela e sobre a sociedade brasileira. Segundo o Portal CSO[42], as organizações farmacêuticas são alvos preferenciais para o crime cibernético, principalmente em virtude da possibilidade de obtenção de propriedade intelectual relacionada aos processos de negócios, que podem fornecer lucrativa vantagem competitiva.

O Decreto nº 9.573, de 22 de novembro de 2018[43], aprovou a Política Nacional de Segurança das Infraestruturas Críticas Nacionais. Essa Política visa garantir a segurança e a resiliência das infraestruturas críticas do País e a continuidade da prestação de seus serviços. Nesse sentido, estabelece o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas, a Estratégia Nacional de Segurança de Infraestruturas Críticas e o Plano Nacional de Segurança de Infraestruturas Críticas. Em seus princípios, a mencionada Política aponta a importância da prevenção e da precaução, com base em análise de riscos, que reflete na necessidade da adoção de procedimentos de segurança em todas as suas vertentes, inclusive na de segurança cibernética. Essa, em muitos casos, é considerada vital para o pleno funcionamento das infraestruturas críticas e como garantia de prestação adequada dos serviços para toda a sociedade brasileira.

Em 2018, os riscos dos ataques cibernéticos cresceram significativamente, em especial as violações de informações acessadas por fornecedores terceirizados e o furto de informações (informações pessoais identificáveis, propriedade intelectual e segredos comerciais). Segundo o estudo “2018 **Cost of Data Breach Study: Global Overview**”[44], realizado pela IBM em parceria com o Instituto Ponemon, observou-se, em 2018, um aumento de 350% em ataques de **ransomware**, verificou-se uma expansão de 250% em ataques de **spoofing** ou de comprometimento de e-mail comercial e constatou-se um acréscimo de 70% em ataques de **spear-phishing** nas empresas de modo geral. O custo médio de uma violação de dados cibernéticos aumentou de US$ 3.620.000,00 (três milhões seiscentos e vinte mil dólares) em 2017 para US$ 3.860.000,00 (três milhões oitocentos e sessenta mil dólares) em 2018. No Brasil, o custo médio de uma violação chegou a US$ 1.240.000,00 (um milhão duzentos e quarenta mil dólares).

As ameaças cibernéticas acima descritas têm o escopo de alcançar grande número de organizações, inclusive as representantes das infraestruturas críticas, que, por prestarem serviços essenciais à sociedade, possuem elevado nível de criticidade. Por isso, essas organizações necessitam de meios para identificar, proteger, detectar, avaliar, responder, recuperar e assim gerenciar o risco das ameaças cibernéticas, e também de ferramentas de automação de segurança que usam inteligência artificial e aprendizado de máquina, que permitam analisar, identificar e conter os ataques cibernéticos.

Os principais tipos de ameaças contra as infraestruturas críticas são ataques de **phishing**, negação de serviço em larga escala, vazamentos de informações privadas ou institucionais, espionagem cibernética e a interrupção de serviços. Nesse contexto, ressalta-se que a quantidade e a pluralidade de dispositivos e aplicações, especialmente os pertencentes à categoria de IoT, apresentam-se como um desafio para as infraestruturas críticas, considerada a necessidade de equilíbrio entre segurança, privacidade e o não confinamento de recursos para garantia do fomento ao ambiente de inovação.

Verifica-se, ainda, que em todas as abordagens de gerenciamento de riscos cibernéticos, em sistemas ou em funções críticas, existem indicações do uso de criptografia, que contém as devidas recomendações de onde, quando, e como deve ser aplicada.

É mencionado em muitas estratégias nacionais de segurança cibernética que ataques às infraestruturas críticas estão entre as maiores ameaças à segurança nacional, considerado que grande parte das economias nacionais está, de modo crescente, dependente de sistemas de informação de setores essenciais, baseados em controles automatizados.

Portanto, a proteção de infraestruturas críticas contra ameaças cibernéticas em evolução requer uma abordagem ampla, como: realizar o acompanhamento de assuntos pertinentes a essas organizações, com prioridade aos que se referem à avaliação de riscos, planejar, coordenar e desenvolver ações de segurança cibernética e definir normativos e requisitos metodológicos para a implementação de ações de segurança cibernética.

No decorrer da elaboração da Estratégia, foi observado que:

- não há, no Brasil, um arcabouço autóctone e abrangente de segurança cibernética que contribua para o fortalecimento da resiliência cibernética nacional;

- os códigos, as normas, os padrões e as orientações em vigor evoluíram com o desenvolvimento de projetos, de ferramentas e de práticas relacionadas à segurança cibernética, mas não foram absorvidos de modo adequado pelas entidades públicas e privadas;

- os recursos de segurança cibernética evoluíram;

- é necessário aumentar a articulação entre os representantes das infraestruturas críticas;

- é importante estabelecer modelos que permitam compreender o risco cibernético para a prestação de serviços e avaliar o custo de uma ocorrência; e

- é necessário incentivar essas organizações críticas a criarem uma cultura de segurança cibernética.

Um dos setores das infraestruturas críticas que possui normativos estabelecidos aos seus entes regulados com ações específicas para proteção cibernética é o setor financeiro. Publicadas pelo Banco Central do Brasil, a Resolução nº 4.658, de 26 de abril de 2018[45], voltada para instituições financeiras, trata da política de segurança cibernética a ser observada por aquelas instituições. Além disso, dispõe sobre as premissas de contratação de serviços de computação em nuvem e de processamento e armazenamento de dados. Muito embora as instituições de pagamento não integrem o Sistema Financeiro Nacional, não sendo consideradas como infraestruturas críticas, vale destacar a Circular nº 3.909, de 16 de agosto de 2018[46], específica para essas instituições, que aborda interessantes aspectos de segurança cibernética.

Um dos aspectos de grande relevância para as infraestruturas críticas é a continuidade de negócios. Quanto a esse tópico, o Banco Central do Brasil exige que essas organizações devem definir: o tratamento para os incidentes relevantes, os procedimentos no caso da interrupção dos serviços relevantes contratados e os cenários de incidentes a serem considerados nos testes.

Por meio de ação conjunta entre Governo e os diversos operadores de infraestruturas críticas, será possível proteger o espaço cibernético no qual estes estão inseridos. Além disso, verifica-se a relevância do papel das agências reguladoras no estímulo à adoção de procedimentos de segurança cibernética, por parte de seus entes regulados, como por exemplo:

- criação de uma estrutura de governança de segurança cibernética nas empresas de infraestruturas críticas, com o estabelecimento de manuais, de diretrizes, de classificações e de procedimentos para tratamento de incidentes, e de regras de segurança aplicáveis a todos os funcionários, terceirizados e fornecedores;

- inserção de planos anuais de auditoria externa em segurança cibernética;

- adoção de práticas e de requisitos de segurança cibernética no desenvolvimento de novos produtos, programas, projetos e ações;

- criação de CSIRTs por empresa e por setor, com mecanismos de colaboração e de troca de informações entre eles.

- capacitação contínua de seus colaboradores em todos os níveis;

- notificação ao CTIR Gov, no menor prazo possível, sobre a ocorrência de incidentes cibernéticos;

- comunicação aos consumidores em caso de incidente que comprometa a segurança de seus dados, nos termos da legislação em vigor;

- promoção de campanhas de conscientização sobre a importância de atitudes e de cuidados por parte dos usuários;

- exigência de que fornecedores de equipamentos, de programas computacionais e de serviços adotem os níveis de segurança cibernética recomendados pelos organismos de padronização nacionais e internacionais; e

- previsão de elaboração de planos de resposta a incidentes e de recuperação dos ambientes críticos que podem ser impactados pelos incidentes cibernéticos.

No que tange, ainda, ao **modus operandi** dos procedimentos de segurança cibernética, aspectos técnicos e operacionais relacionados ao tema poderão ser tratados de forma mais detalhada pelas agências reguladoras com apoio doGabinete de Segurança Institucional da Presidência da República, por meio de grupos de trabalho constituídos por representantes do Governo, da iniciativa privada, da academia e da sociedade em geral, de forma a ensejar, por exemplo, a elaboração de manuais operacionais e de procedimentos específicos de segurança cibernética.

Por fim, recomenda-se aos gestores das infraestruturas críticas que, ao elaborar suas políticas de segurança cibernética, contemplem, dentre outras, as seguintes ideias:

- foco nos resultados de segurança;

- uso de estrutura flexível e baseada em análise de riscos;

- ênfase na continuidade de seus serviços;

- alinhamento da segurança crítica com os padrões nacionais e internacionalmente reconhecidos; e

- garantia de que os processos de certificação sejam equilibrados, transparentes e com base em padrões nacionais e internacionais.

2. EIXOS TEMÁTICOS: TRANSFORMADORES

2.1. Dimensão Normativa

O aumento vertiginoso do número de usuários da internet e a forte expansão do comércio **online** expandiram as possibilidades de ações maliciosas e ilícitas, e ensejaram o cometimento de infrações penais conhecidas como crimes cibernéticos ou crimes virtuais. Esses delitos vão desde crimes que ofendem a honra da pessoa, como calúnia, difamação, injúria e **bullying**, até crimes que violam a privacidade do cidadão ou atentam contra seu patrimônio.

Atualmente, com o uso intenso da rede mundial de computadores, tais crimes expandem-se com rapidez. Há que se reconhecer as iniciativas e os esforços realizados até o momento, que resultaram na aprovação de leis importantes para o País, como a Lei nº 12.965, de 23 de abril de 2014[47], conhecida como Marco Civil da Internet e a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais - LGPD[48], entretanto, o nível de articulação e de normatização das instituições brasileiras nos temas relacionados à segurança cibernética ainda é tímido, e exigem esforço adicional.

Estabelecer normas e eventuais leis que rejam o espaço cibernético é sempre um desafio significativo, em razão do rápido desenvolvimento da tecnologia da informação e comunicação e dos sistemas de controle. Nesse sentido, é fundamental a ação coordenada entre as organizações governamentais e a sociedade em geral para prosseguir nos avanços legislativos sobre o tema.

Duas leis relacionadas aos crimes na internet foram sancionadas em 2012, que alteraram o Decerto-Lei nº 2848 de 1940 - Código Penal, que tipificou e estabeleceu penas para certas condutas delituosas cometidas no mundo digital.

A primeira é a Lei dos Crimes Cibernéticos - Lei nº 12.737, de 30 de novembro de 2012[49], conhecida como "Lei Carolina Dieckmann", que tipifica atos como a invasão de computadores - **hacking**, o roubo de senhas, a violação dos dados de usuários e a divulgação de informações privadas (fotos, mensagens, etc). A segunda é a Lei nº 12.735, de 30 de novembro de 2012[50], que determina a instalação de delegacias especializadas para o combate aos crimes digitais.

Nos termos da E-digital: "é oportuno para o Brasil estabelecer um marco legal, protegendo direitos dos cidadãos e conferindo segurança jurídica para investimentos na economia digital. Há, contudo, normas legais e infralegais que atualmente tratam da questão em âmbito setorial, como: Código de Defesa do Consumidor, que resguarda os dados pessoais de consumidores; a Lei de Acesso à Informação que protege os dados pessoais e ao mesmo tempo em que promove a transparência do poder público; a Lei do Cadastro Positivo, que salvaguarda os dados pessoais no âmbito de análise de crédito; entre outras"

A Lei nº 12.965, de 2014 - Marco Civil da Internet, regula o uso da internet no Brasil por meio da previsão de princípios, de garantias, de direitos e de deveres para quem utiliza a rede mundial de computadores, e de diretrizes para a atuação do Estado, protegendo os dados pessoais e a privacidade dos usuários no ambiente **online**, o que é tratado, de modo mais direto e assertivo, pela LGPD. Apesar de abrangente e moderno, o intenso avanço da tecnologia e o consequente redesenho das relações humanas no espaço cibernético enseja análises periódicas desse valioso instrumento legal, no intuito de sempre preservar seus nobres pilares democráticos de liberdade de expressão e de livre trânsito de opiniões.

A publicação, em agosto de 2018, da LGPD mencionada, reforçou a necessidade das organizações em realizar investimentos em sua estrutura e em adotar políticas internas que atendam as exigências de segurança voltadas ao tratamento dos dados pessoais.

A outra frente de trabalho refere-se aos instrumentos normativos de competência do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, direcionados aos órgãos da Administração Pública federal, que visam ao aperfeiçoamento e à atualização das diretrizes operacionais e dos requisitos relativos ao tema. Após a criação do então Departamento de Segurança da Informação e Comunicações, em 2006, o Gabinete de Segurança Institucional da Presidência da República dedicou-se intensamente à temática. Como resultado, desde 2008, foram publicadas três Instruções Gerais e vinte e duas Normas Complementares[51], de forma a contemplar os assuntos relacionados à Segurança da Informação. Devido às características evolutivas do tema, tais instrumentos necessitam de apreciação e de revisão constantes.

Em 26 de dezembro de 2018, foi publicada a Política Nacional de Segurança da Informação, por meio do Decreto nº 9.637, de 2018, que dispõe sobre princípios, objetivos, instrumentos, atribuições e competências de segurança da informação para os órgãos e entidades da Administração Pública federal, sob o prisma da governança. Não obstante seja um instrumento significativo, recomenda-se a elaboração de uma lei específica sobre Segurança Cibernética, capaz de dar diretrizes específicas para o setor cibernético nacional, e que inclua os Poderes da União, dos Estados, do Distrito Federal, dos Municípios, o setor privado e a sociedade em geral.

Uma lei se destinaria a disciplinar diversos aspectos da dimensão nacional da segurança cibernética, uma vez que todo o arcabouço normativo existente é insuficiente para o adequado enfrentamento do tema pelo País. Essa insuficiência decorre da natureza infralegal dos instrumentos existentes, e faz com que se restrinjam à Administração Pública federal, de forma a não se aplicar, desse modo, aos demais entes do Poder Público, e a não contemplar, ainda, o setor produtivo, dentre os quais, os fornecedores de serviços essenciais, e a sociedade em geral.

Além disso, destaca-se que a segurança cibernética apresenta novo paradigma em termos de segurança para o Estado, uma vez que todos os atores nacionais possuem vulnerabilidades que podem ser exploradas por uma ameaça cibernética que adquira grande repercussão, de forma a colocar em risco até mesmo a estabilidade das instituições nacionais.

Um dos grandes desafios em termos de segurança cibernética é que ela precisa ser compreendida de uma forma holística e multissetorial, não sendo adequado abordá-la de forma restrita aos órgãos governamentais, sem o devido engajamento do setor privado e sem um olhar para o usuário final de todas as

tecnologias que utilizam o espaço cibernético.

Nesse sentido, uma lei sobre segurança cibernética teria o condão de alinhar ações de governança e de conformidade nesse tema, a partir de um patamar único, ao vincular os diversos atores nacionais aos princípios e regramentos propostos. A economia digital, a inserção do Brasil na Indústria 4.0 e o alcance dos Objetivos de Desenvolvimento Sustentável[52] elegidos pelas Organização das Nações Unidas, exigem que o País tenha condições de construir a confiança e a segurança necessárias para o desenvolvimento nacional na era da informação.

Sob essa ótica, indicam-se ações que aprimorem o arcabouço legal da segurança cibernética nacional, por acreditar que essa iniciativa poderá proporcionar o necessário alinhamento estratégico e normativo às ações do País nessa área, de forma a ressaltar que deve ser atribuída especial atenção às políticas em segurança cibernética voltadas ao setor produtivo, as quais, pela natural força advinda do mercado, tendem a ser mais bem-sucedidas que aquelas dedicadas exclusivamente às ações do setor público e à fiscalização regulatória.

Recomenda-se, ainda, no sentido de permitir a elaboração de instrumentos com a maior legitimidade possível, a criação de mecanismos que ensejem a participação da iniciativa privada e da academia para troca de experiências, para exploração de práticas internacionais, para discussão de padrões e de melhores práticas no tema e apoio às decisões da entidade central.

2.2. Pesquisa, Desenvolvimento e Inovação

As últimas décadas foram marcadas por intensas transformações e por impactante revolução tecnológica, que promoveram importantes mudanças no cotidiano das pessoas, especialmente no que se refere às formas de comunicação, de interação e de acesso às informações. Nesse sentido, o avanço tecnológico evidenciou a relevância do incentivo à pesquisa e à inovação em prol do desenvolvimento, e demonstrou o papel essencial dessas áreas para a sociedade.

O papel que o Governo deve desempenhar nesse cenário também se torna relevante, para que o País prossiga em um crescimento econômico guiado pela inovação, de modo inclusivo e sustentável. Nesse contexto, as iniciativas de Pesquisa, Desenvolvimento e Inovação - PD&I, na área de segurança cibernética, necessitam de maior prioridade, com o fim de obter maior investimento, mais pesquisadores capacitados na área, e novos projetos, aos moldes de outros países, de forma a contemplar, inclusive, a criptologia como matéria de extrema relevância a ser incorporada em projetos de pesquisa e de inovação em âmbito nacional.

O foco deste eixo é incentivar a busca de soluções de segurança no ambiente digital, em linha com o E-Digital, de 2018. Cidades inteligentes, que utilizam amplamente tecnologias provenientes da IoT, e integração de sistemas de governo, que utilizam recursos de **BigData**, por exemplo, precisam ter, no centro dos debates, a preocupação com a segurança cibernética.

A E-Digital estimula a PD&I, e a modernização de uma estrutura produtiva, em áreas como: de microeletrônica, em particular, em ações que visem à capacitação em **design house**, de sensores, de automação e robótica, de supercomputador, de inteligência artificial, de **BigData** e **analytics**, de redes de alto desempenho, de criptografia, de redes móveis de quinta geração - 5G e de computação em nuvem.

Recomenda-se, nesse sentido, o investimento na busca de soluções inovadoras em novos tipos de criptografia, de forma a considerar seu potencial variado de aplicabilidade e seu valor estratégico para a segurança da informação e para a segurança cibernética do País.

O Brasil possui um cenário diversificado no que tange à pesquisa e ao desenvolvimento em tecnologia. Identificam-se centros de excelência altamente capacitados e reconhecidos por suas atividades, mas que produzem pouca inovação ou tecnologia aplicável ao ambiente cibernético. É preciso que o País disponha de uma indústria de segurança cibernética inovadora, apoiada por pesquisas e por produções científicas de alto nível, capaz de reter talentos que possam contribuir com a indústria nacional e realimentar o ciclo de produção do conhecimento.

Verifica-se uma dissonância entre os projetos conduzidos pelas universidades públicas e privadas e as necessidades em soluções de segurança cibernética por parte do setor produtivo. Esse quadro demonstra a necessidade de diálogo mais estreito e eficaz entre o setor empresarial e a academia, para que haja convergência de esforços e de projetos que impactem a sociedade de forma positiva e construtiva.

Nesse sentido, recomenda-se o estabelecimento de parcerias com o Ministério da Educação, visando à implementação de programas de incentivo ao desenvolvimento de capacidades em segurança cibernética para estudantes da educação básica, com o objetivo de identificar talentos, e orienta-se que as universidades desenvolvam projetos em alinhamento com as necessidades do setor produtivo.

A aproximação dos programas de mestrado e doutorado não só em computação aplicada, mas em outras áreas do conhecimento, pode ser uma via eficaz para formação, aprimoramento e qualificação de pessoal interessado no tema, além de geração de conhecimento.

No contexto da inovação, a E-Ciber incentiva a adoção de padrões globais e voluntários de tecnologia, que permitirá a interoperabilidade em escala internacional e, por consequência, irá assegurar que não só as organizações localizadas no Brasil como também aquelas fora do País possam adotar nossas práticas e processos, de modo a servir de modelo para a cooperação internacional no fortalecimento da segurança cibernética. Ressalta-se, portanto, que políticas públicas nesse tema contemplem a relevância de se aproveitar avanços e tecnologias globais, para garantir, de todas as formas, a utilização das melhores ferramentas disponíveis para a segurança cibernética.

Um dos indicadores usados para medir o desempenho de um país quanto à inovação tecnológica é o ranking **World Competitiveness Yearbook** da escola de negócios **IMD Foundation Board**[53]. Na versão de 2019, o Brasil ocupou o quinquagésimo nono lugar mundial de sessenta e três posições. A pesquisa indica que o Brasil vem perdendo posições nesse indicador de inovação tecnológica desde 2010, quando apareceu no trigésimo oitavo lugar. Em 2011, caiu para o quadragésimo quarto lugar. Em 2012, já havia perdido mais duas posições no **ranking** e, na última edição, caiu mais quinze posições.

No que tange ao uso dos fundos, o maior é o Fundo Nacional de Desenvolvimento Científico e Tecnológico - FNDCT[54], criado formalmente em 1969, com o objetivo de apoiar financeiramente programas e projetos prioritários de desenvolvimento científico e tecnológico nacionais. Os recursos do FNDCT são utilizados para apoiar atividades de inovação e pesquisa em empresas e instituições científicas e tecnológicas, entretanto, não há foco específico para projetos em segurança cibernética. Nessa perspectiva, considera-se como relevante o uso desse e de outros fundos para incentivar programas e ações de inovação em segurança cibernética.

No atual cenário de inovação e revolução tecnológica, as empresas que surgem com base tecnológica - **startups** desempenham papel de relevância como principais fontes de inovação. A percepção de seu potencial inovador incentivou diversos países a estabelecerem ampla gama de programas de apoio a **startups** e a pequenas e médias empresas, solução que o Brasil deve seguir e incentivar.

A propósito, nesse contexto, ressalta de importância o prosseguimento das pesquisas sobre o uso de inteligência espectral, em virtude do fato de sensores empregados em redes IoT, **drones**, **smartphones**, dispositivos GPS e em roteadores sem fio poderem sofrer ações maliciosas no espectro de radiofrequência com sérios impactos na privacidade e até mesmo na segurança de pessoas e de infraestruturas críticas. Entende-se como inteligência espectral o uso e a análise do espectro de radiofrequência em sistemas de comunicação sem fio[55].

No que tange, ainda, ao eixo Pesquisa e Desenvolvimento, destaca-se a importância de considerar os aspectos de segurança cibernética relacionados à tecnologia das redes 5G, uma vez que representa uma revolução nas comunicações de dados, no potencial de emprego de equipamentos de IoT e na prestação de novos e disruptivos serviços que necessitam de redes com latência muito reduzida para sua operacionalização, implementação, efetivação e resiliência. Nesse contexto, a E-Ciber recomenda que devem ser considerados, na comercialização de equipamentos 5G, requisitos mínimos de segurança cibernética que assegurem o uso pleno, responsável e seguro dessa tecnologia em prol do desenvolvimento da sociedade e das instituições nacionais.

2.3. Dimensão Internacional e Parcerias Estratégicas

O Brasil experimenta o fenômeno da quarta revolução industrial, onde as tecnologias ganham maior integração, o mundo físico e o ambiente virtual alcançam elevado grau de interação, e os dispositivos de IoT proliferam em apoio aos processos produtivos. Essa automação tende, naturalmente, a aumentar a competitividade e a produtividade do setor industrial.

A denominada Indústria 4.0, portanto, traz grandes possibilidades de ganhos de produtividade para o setor industrial por meio do emprego de novas tecnologias, como IoT, robótica avançada, impressão 3D, **BigData**, computação em nuvem, inteligência artificial e sistemas de simulação virtual. Além disso, a combinação entre as tecnologias enseja novas possibilidades, novos negócios e soluções, de forma a transpor fronteiras e de eliminar distâncias. Para melhor visualização dessas tecnologias, tem-se uma lista delas, trazida pela Agência Mais[56]:

- Robótica Avançada: ramo educacional e tecnológico que engloba computadores, robôs e computação que fazem parte de circuitos integrados;

- BigData - análise e interpretação de grandes volumes de dados variados;

- Impressão 3D - forma de tecnologia de fabricação aditiva onde um modelo tridimensional é criado por sucessivas camadas de material;

- Computação em Nuvem - possibilidade de acessar arquivos e de executar diferentes tarefas pela internet sem a necessidade de instalar aplicativos, por exemplo;

- Inteligência artificial - ramo da informática que visa criar máquinas com inteligência similiar à humana;

- Simulação Virtual - sistemas capazes de simular o comportamento dos equipamentos que se deseja reproduzir; e

- Internet da Coisas - revolução tecnológica que tem por objetivo conectar itens usados no dia a dia das pessoas à rede mundial de computadores.

Motivado por esse fenômeno, observa-se a crescente incorporação de tecnologias digitais nas diversas atividades cotidianas, como, por exemplo, os aplicativos para marcar consultas ou realizar operações bancárias, os carros autônomos, o controle de máquinas e produtos por meio de sensores ou qualquer outra tecnologia que otimize a realização de atividades, em termos de custos financeiros e de tempo, de forma a corroborar, enfim, para o processo de digitalização da economia.

Com a economia digitalizada, surgem oportunidades de negócios no âmbito nacional e no internacional. Entretanto, também despontam novas formas de crimes e de ações maliciosas. O crime cibernético é um fenômeno de dimensão global, geralmente com múltiplas conexões territoriais. Em virtude dessas características, é impossível a um país atuar sozinho no combate aos crimes no ambiente cibernético. Nesse sentido, abre-se espaço para a busca por maior integração internacional, especialmente entre as forças policiais, os investigadores, os órgãos de justiça e os demais atores relacionados às investigações criminais no ambiente digital. Em todas essas ações, deve-se manter um ambiente colaborativo que permita o estudo e a ampla utilização das tecnologias emergentes.

Ressalta-se que a segurança cibernética é assunto global em que se faz primordial a interação entre diversos atores da comunidade internacional para a construção de um ambiente digital seguro e confiável. Nesse sentido, recomenda-se que o País adote diretrizes que, por meio de medidas de construção de confiança, visem à cooperação interestatal, ao intercâmbio intenso de informações, à transparência, à previsibilidade de ações, à reafirmação da paz internacional e à estabilidade, de modo a corroborar para reduzir o risco da escalada de incidentes cibernéticos em âmbito global.

No âmbito internacional, em relação ao tema cibernético, o País deve continuar a se orientar pelos princípios constitucionais brasileiros, pelos valores fundamentais de nossa sociedade - como o respeito à democracia e aos direitos humanos - pela ênfase ao multilateralismo, pelo respeito ao direito internacional, pela vocação para o diálogo e pela solução pacífica de controvérsias, passando pela identificação de novas oportunidades comerciais. A existência de normativos como a Lei nº 12.965, de 2014 - Marco Civil da Internet, e a Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais, aliada às políticas de desenvolvimento da internet brasileira, reforçam a atuação do País nos foros internacionais de discussão da tecnologia da informação e comunicação e, em especial, a segurança cibernética.

Ao observar o cenário internacional, verifica-se a necessidade urgente de cooperação entre os países para mitigar ameaças como: os crimes cibernéticos, os ataques cibernéticos às infraestruturas críticas, a espionagem cibernética, a interceptação de dados em massa e as operações ofensivas destinadas a projetar poder pela aplicação indevida e desproporcional de força em tempo de paz. Nesse sentido, é preciso reforçar a atuação brasileira na elaboração e na revisão dos instrumentos internacionais relativos à segurança cibernética, ao estimular debates e incentivar a cooperação internacional no tema. Identifica-se, ainda, a necessidade de maior integração entre o Brasil e os países da América Latina, sendo o País um importante condutor regional.

Ressalta-se que o País pretende buscar acordos bilaterais de cooperação em segurança cibernética com o maior número possível de países, como demonstração de nosso intuito em estabelecer, nesse campo, relações que sejam adequadas, profícuas, construtivas e transparentes. Considera-se, portanto, que parcerias estratégicas são fundamentais, e devem, sempre, ser pautadas em princípios como confiança, capacidade agregadora, e contribuição efetiva, de forma a proporcionar oportunidade para que outros atores, além dos integrantes do Poder Público, possam também contribuir.

A cooperação internacional, portanto, deve ser viabilizada por meio de ações que assegurem seu desenvolvimento e sua contínua implementação, e deve contemplar, dentre outras, o compartilhamento de informações (**benchmarking**, conhecimento tecnológico, doutrina, análise de ameaças, compartilhamento de inteligência cibernética, avaliação de crises cibernéticas de vulto) e a celebração de instrumentos sobre o tema.

Nesse sentido, a E-Ciber recomenda a participação do País em esforços internacionais para elaboração de procedimentos operacionais padrão a serem utilizados para o compartilhamento de informações e de respostas a grandes crises transnacionais, e incentivar a participação de entidades públicas e privadas em exercícios regionais e internacionais como forma de apoiar a cooperação com parceiros estratégicos.

Com relação aos atos internacionais relacionados ao tratamento da informação classificada, o Gabinete de Segurança Institucional da Presidência da República tem a competência de conduzir as negociações, em articulação com o Ministério das Relações Exteriores. Atualmente, o Gabinete de Segurança Institucional da Presidência da República acompanha dezenas de acordos para troca e proteção mútua de informação classificada.

Ainda com relação aos acordos bilaterais, o Brasil deve estimular a negociação de tratados de assistência jurídica mútua (ou MLATs, **Mutual Legal Assistance Treaty**) a fim de melhor combater o crime cibernético quando se expande além de nossas fronteiras.

Na busca desse engajamento internacional, é essencial que o Brasil participe de iniciativas de estruturação normartiva futura, como as relativas à criação de padrões que guiarão a segurança em tecnologias emergentes, como as redes de comunicação 5G, a inteligência artificial e a internet das coisas. Desse modo, o País terá melhores condições de trabalhar e de influenciar esses padrões, ao reconhecer que consistem em desafios internacionais.

É fato que a integração e a cooperação entre administração pública, setor privado e sociedade, em diversas áreas, costuma trazer resultados benéficos, e contribui para elevar a confiança do cidadão nas instituições públicas e privadas e aprimora a relação entre esses atores. Na área da segurança cibernética essa relação é essencial, uma vez que, como o tema é transversal, os melhores resultados somente serão alcançados se todos agirem de forma coordenada, sempre cientes de que nenhum ator poderá, de forma isolada, enfrentar com todos os desafios impostos pelas novas tecnologias. Nesse sentido, são necessárias responsabilidades bem definidas, e cabe ao Governo o papel central de coordenação desse complexo ecossistema, ao direcionar os esforços em prol do bem-estar da sociedade.

A necessidade de estabelecer e consolidar parcerias estratégicas no ambiente cibernético torna-se ainda mais evidente ao se constatar que grande parte das infraestruturas críticas estão sob responsabilidade do setor privado, o que reforça a necessidade de propósitos comuns, em segurança cibernética, entre Governo, empresas privadas, academia e a sociedade em geral.

No Brasil, os processos de coordenação entre os distintos atores do ambiente cibernético, até o momento, compõem um amplo leque de arranjos nem sempre institucionalizados e perenes, e nem atrelados a mecanismos convencionais de regulação[57]. Soma-se a esse fato a existência de grande quantidade de instituições que lidam direta ou indiretamente com a segurança cibernética, o que traz grandes desafios de cooperação e de coordenação para o Estado brasileiro. Portanto, recomenda-se a criação de canais de comunicação apropriados, a fim de que seja ouvido e contemplado o maior número de segmentos da sociedade brasileira quando da elaboração, da implementação e da promoção de políticas públicas relativas à segurança cibernética.

É importante ressaltar que as parcerias no campo cibernético tendem a se consolidar se forem baseadas na confiança, em interesses e em objetivos comuns, onde os planos de ação sejam construídos em conjunto, e onde os mecanismos de coordenação sejam eficazes. Diante disso, cresce em relevância a realização de reuniões com atores destacados em segurança cibernética e a instituição, caso necessário, de grupos de trabalho e de fóruns sobre o tema.

Portanto, como a segurança cibernética é de extrema importância para o poder público e para as instituições privadas, entende-se como relevante a criação de um mecanismo de compartilhamento de informações sobre riscos cibernéticos, com o fim de contribuir para a identificação, o gerenciamento e a mitigação de riscos. Essa contínua troca de conhecimento irá auxiliar organizações a evitar, a avaliar e a gerenciar riscos corretamente, além de viabilizar uma abordagem coordenada mais eficaz e eficiente.

2.4. Educação

Construir uma sociedade conectada tem sido um desafio para o Estado brasileiro. Contudo, graças à modernização tecnológica e à expansão das redes de telecomunicações, que resultaram em um rápido e massivo acesso à internet por parte de milhões de brasileiros, conforme abordado no item Diagnóstico, hoje 98% da população possui acesso às redes móveis e 60% dos domicílios têm acesso por meio da rede fixa. Entretanto, essa realidade trouxe uma série de novas preocupações, especialmente com relação às vulnerabilidades e às ameaças cibernéticas.

Como consequência do maior acesso às redes digitais, e em virtude da pouca maturidade em segurança cibernética, o Brasil ocupa lugar de destaque no **ranking** dos países que mais recebem ataques cibernéticos. A falta de cultura em segurança cibernética, de habilitação e de conhecimento nesse tema de grande

número de brasileiros conectados ao mundo digital mostra que a nossa sociedade não está preparada para o uso das ferramentas digitais com os cuidados adequados relativos à segurança cibernética.

Nesse contexto, destaca-se a importância da alfabetização digital, ou **digital literacy**, conceito que, segundo a **Western Sidney University**[58], significa "possuir as habilidades necessárias para viver, aprender e trabalhar em uma sociedade em que a comunicação e o acesso à informação ocorrem cada vez mais por meio de tecnologias digitais, como plataformas da Internet, mídias sociais e dispositivos móveis". Esse esforço de educação digital, que passa pela inclusão tecnológica, visa a preencher imensa lacuna entre os usuários atuais dessas tecnologias e os pertencentes ao grupo dos chamados "nativos digitais", expressão criada em 2001, por Marc Prensky[59], especialista estadunidense em educação, que usou o termo para se referir a todos os nascidos após 1980, cujo desenvolvimento biológico e social se deu em contato direto com a tecnologia.

Dessa forma, recomenda-se desenvolver uma cultura de segurança cibernética, por meio da educação, que alcance todos os setores da sociedade e níveis de ensino, a fim de prevenir incidentes e proporcionar o uso responsável das tecnologias, por ser um dos fatores chaves para o desenvolvimento do País.

A educação em segurança cibernética é concebida em três formas de atuação, em grau crescente de especialização de conteúdo, e em grau decrescente de abrangência da sociedade, conforme o que segue:

- Capacitação - profissionais da área ou com funções que requerem competências na área;

- Formação - parcela da sociedade que se encontra nos bancos escolares; e

- Conscientização - sociedade e seus setores.

A conscientização é obtida por meio de ações direcionadas a sensibilizar setores específicos da sociedade, ou esta como um todo. Num foco mais restrito, a formação abrange o ensino de segurança cibernética direcionado à parcela da sociedade que se encontra na educação infantil, no ensino fundamental, no ensino médio e no ensino superior. Por fim, a capacitação engloba a educação, na modalidade profissional e tecnológica, destinada ao ensino continuado para profissionais da área, ou para aqueles cujo cargo ou função requeira conhecimentos técnicos mais profundos e especializados de segurança cibernética. A capacitação é a forma de atuação mais especializada e pode ser realizada por intermédio de treinamentos de curta duração, certificações de segurança, dentre outros meios.

No que diz respeito à implementação dessas três vertentes de educação em segurança cibernética, a responsabilidade deve ser compartilhada entre órgãos de Estado, setor educacional, serviços sociais do comércio e da indústria, e sistemas nacionais de aprendizagem. Cabe ressaltar que, para isso, há uma série de recursos educacionais disponíveis, conforme vê-se a seguir:

- Capacitação - os Planos de Capacitação para professores, gestores e especialistas e os Bancos de Talentos;

- Formação - a Criação de cursos e a Inserção do tema nos currículos escolares;

- Conscientização - os Planos de Conscientização nas escolas e instituições, os Portais de boas práticas e as Campanhas educativas.

No contexto da conscientização, incentiva-se a concepção de políticas públicas, que levem à consciência situacional ante o atual cenário de ameaças cibernéticas, e estimulem o comportamento responsável e seguro por parte dos usuários da internet.

As ações de conscientização tornaram-se ferramenta essencial para mudanças de comportamento relativas ao ambiente cibernético, e são relevantes, à medida que levam os indivíduos a perceber, em sua rotina pessoal ou profissional, quais atitudes precisam ser corrigidas no mundo digital.

Como exemplo, tem-se a realização, em todo mês de outubro, do **National Cybersecurity Awareness Month** - Mês Nacional de Conscientização em Segurança Cibernética, que é um esforço colaborativo entre o Governo dos Estados Unidos da América e a indústria para aumentar a conscientização sobre a importância da segurança cibernética e garantir que todos os norte-americanos tenham os recursos necessários para estarem mais seguros **online**.

A conscientização deve atingir amplas audiências, dentre usuários individuais e corporativos, de crianças a idosos. Deve ainda ser contínua, criativa e motivadora, a fim de concentrar a atenção do público-alvo, para mudança de comportamento favorável ao ambiente cibernético, sendo importante a promoção de ações periódicas, junto à sociedade, com o objetivo do uso seguro e responsável dos recursos de tecnologia da informação e comunicação, e à proteção contra riscos típicos no espaço cibernético.

Um programa de conscientização pode incluir as seguintes tarefas:

- definir o alvo da campanha de conscientização;

- desenvolver mecanismos para alcançar esse público-alvo;

- identificar problemas comportamentais comuns que afetam o público-alvo ou que ele deve conhecer;

- aprimorar o conteúdo de sites governamentais, principalmente os mais acessados, com material relacionado à segurança cibernética; e

- considerar a tradução do material para outros idiomas.

Orienta-se fortalecer programas de treinamento e de educação em segurança cibernética. Tal sugestão constitui uma demanda atual por parte de organizações públicas e privadas. Segundo o **Center for Strategic and International Studies**, estima-se que existam de um a dois milhões de empregos não preenchidos em todo o mundo na área de segurança cibernética[60].

O rápido avanço tecnológico, acompanhado da transformação digital proposta para a sociedade moderna, tornou imprescindível o desenvolvimento de ações educacionais e pedagógicas para a formação em prol do uso criterioso, seguro e responsável das tecnologias. Nesse sentido, considera-se que a prioridade de investimentos em programas de educação relacionados à segurança cibernética é um pilar essencial para reduzir os riscos às empresas e à sociedade.

No contexto da formação, a abordagem da segurança cibernética nas escolas brasileiras ainda é muito incipiente, quando não, inexistente. No âmbito da educação superior, a segurança cibernética, como disciplina ou programa de estudo, ainda é de difícil acesso aos alunos. A segurança cibernética, em geral, não é um tópico acadêmico isolado, mas parte do currículo do curso de graduação de Ciência da Computação, sendo um tema em constante mudança, que requer treinamento e educação constantes. Entretanto, ressalta-se que já existem iniciativas de ensino em áreas correlatas à segurança cibernética, como a recente criação do curso superior de Tecnologia em Defesa Cibernética, no Catálogo Nacional de Cursos Superiores de Tecnologia.

Nesse sentido, segundo o **McAfee Reporter**, “o aprendizado contínuo é vital para reter talentos em segurança cibernética. Embora os empregadores possam ser cautelosos em investir em programas de treinamento caros que tornam os funcionários mais atraentes no mercado de talentos, nossa pesquisa mostra que a ausência desse treinamento é muitas vezes um fator significativo nas decisões das pessoas em buscar emprego alternativo”.

Atualmente, universidades e instituições não formam especialistas suficientes em segurança cibernética para atender às crescentes necessidades do setor; entretanto, o tema tornou-se de tamanha relevância que não pode permanecer restrito àquelas entidades, mas deve ser de conhecimento e de domínio de todos os níveis de ensino.

Recomenda-se que se dê ênfase em segurança cibernética nos currículos de cursos técnicos, particularmente naqueles que envolvam desenvolvimento de **softwares**, nos níveis de ensino médio e de ensino superior, e nos currículos da modalidade de ensino “educação tecnológica e formação profissional”[61].

No contexto da capacitação em segurança cibernética, a situação não é diferente. Pesquisa realizada em 2018, pela **ManpowerGroup**[62], empresa líder mundial em soluções inovadoras de força de trabalho, com aproximadamente quarenta mil empregadores de quarenta e três países, mostra que quase a metade deles (45%) tem dificuldade para encontrar pessoas qualificadas, inclusive, no segmento de segurança cibernética. Entre os empregadores brasileiros, 34% afirmam ter dificuldade em recrutar talentos. A era digital tem transformado os modelos de trabalho, que passam a exigir novas habilidades.

As maiores dificuldades das empresas no processo de contratação no Brasil são a ausência de habilidades técnicas (33%), seguida pela falta de experiência (23%) e pela carência de habilidades interpessoais (19%). A primeira tem a ver com as lacunas educacionais brasileiras. A segunda se relaciona com a resistência de recrutadores de dar oportunidade a novatos. E a terceira relaciona-se a competências comportamentais, que não são inatas, sendo possível

desenvolvê-las. Tais dificuldades para a contratação demonstram o descompasso existente entre a situação dos profissionais existentes e as necessidades do mercado de trabalho.

Apesar dos esforços educacionais empreendidos até o momento no campoda tecnologia da informação e comunicação, verifica-se que têm sido insuficientes diante da demanda nacional. “Segundo estudo divulgado pela Brasscom - Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação, o mercado de tecnologia no Brasil precisará de aproximadamente 70 mil profissionais ao ano até 2024, número que poderá representar um déficit de 260 mil pessoas qualificadas no período”[63].

Acrescenta o estudo que hoje, no País, “o setor de TIC - tecnologia da informação e comunicação é responsável por 845 mil empregos e forma 46 mil alunos por ano com perfil tecnológico no ensino superior”. O relatório afirma, ainda, que “as especializações mais requisitadas e que precisam de mão de obra imediata são as de desenvolvedores **web** e **mobile**, computação em nuvem, ciências de dados, segurança cibernética e inteligência artificial”.

Verifica-se que o setor privado se concentra com intensidade no desenvolvimento da força de trabalho, mas necessita do apoio do Estado na formação da força de trabalho futura. Para tanto, recomendam-se ações governamentais no sentido de proporcionar maiores oportunidades de treinamento e de formação para profissionais de tecnologia da informação e de segurança cibernética, para melhorar a capacitação necessária à implantação das múltiplas tecnologias e soluções digitais. Esse objetivo pode ser alcançado, por exemplo, por meio de parcerias com universidades para o desenvolvimento dos currículos de segurança cibernética; de treinamentos na área, mediante seminários e **workshops**; e da criação de programas voltados para as áreas internacionalmente conhecidas como de STEM - **Science**, **Technology**, **Engineering and Mathematics**[64].

Não obstante o cenário cibernético atual, as empresas continuam a sofrer com a falta de profissionais melhor qualificados e com a retenção de seus talentos, de acordo com o estudo **State of Cybersecurity**: 2019, da associação global de tecnologia da informação, segurança e auditoria cibernética - ISACA[65], divulgado no início de 2019. Segundo a pesquisa, manter os profissionais de segurança cibernética é muito difícil, e a formação e as certificações promovidas e custeadas pelo empregador não são suficientes para garantir a retenção. Os profissionais de segurança cibernética estão migrando com maior frequência de seus empregos para aqueles que oferecem remunerações maiores, perspectivas de progressão na carreira e percepção de ambientes de trabalho mais saudáveis.

Por fim, segundo a pesquisa da ISACA, as empresas implementam várias estratégias para reter profissionais de segurança cibernética, dentre elas, o fornecimento de treinamento adicional. Cinquenta e sete por cento dos entrevistados indicam que suas empresas investem em mais treinamento, como incentivo para que seus funcionários nelas permaneçam.

Como as previsões para 2020 indicam que as pequenas e médias empresas são o próximo alvo dos ataques cibernéticos, ressalta-se a necessidade de ações de conscientização. O primeiro passo é o reconhecimento, por parte das empresas, que seus dados não estão 100% seguros. Isso significa que ataques, redução da produtividade e prejuízos podem ser evitados, se houver mudança de atitude. O assunto é comum, tanto que conceitos como o **Zero Trust**, refletidos em maior rigidez no acesso à rede, na inspeção e no registro de tráfego, têm sido discutidos e aplicados no meio corporativo.

A tendência é que os crimes cibernéticos ocorram com maior frequência no nicho das pequenas e médias empresas, porque, em geral, essas empresas não adotam as devidas medidas e ações preventivas. Como, frequentemente, empresas menores são fornecedoras de serviços das maiores, isso torna as menores um canal de conexão para grandes organizações, que possibilitam ataques por infiltração.

Nesse sentido, ressalta-se a importância da conscientização de gestores, tanto do setor público quanto do setor privado, sobre segurança cibernética, uma vez que, em sua maioria, decidem a alocação de recursos e o tempo destinado aos projetos definidos como prioritários. Essa iniciativa cresce de importância com a premente conformidade de entidades públicas e privadas à recente Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais, que evidencia a necessidade de que tais instituições invistam em programas de capacitação sobre proteção e privacidade desses dados.

Recomenda-se, nesse contexto, o incentivo às iniciativas para aumentar o interesse e o acesso à educação em ciências da computação para alunos da educação básica, com possibilidade de expansão de parcerias público-privadas, repensar a educação profissional e treinar mais professores para qualificá-los adequadamente no tema.

Identifica-se, também, a necessidade de desenvolvimento de programas de treinamento em segurança cibernética, para os trabalhadores do setor público e do setor privado, para que possam aprimorar seus conhecimento e desenvolver novas habilidades nessa área.

Dados da Organização para a Cooperação e Desenvolvimento Econômico - OCDE revelam que até 2021 haverá três milhões e quinhentas mil vagas não preenchidas no mercado de trabalho de segurança cibernética em todo o mundo. No Brasil, a pesquisa da Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação - Brasscom estima que, até 2024, o mercado demandará quatrocentos e vinte mil profissionais da área de tecnologia da informação e comunicação, sendo que quarenta e cinco mil especificamente para o segmento de segurança cibernética. Tais números levam ao entendimento de que a maior deficiência no combate aos crimes cibernéticos não será de ordem tecnológica mas, sim, da falta de recursos humanos.

Uma recente pesquisa realizada pelo **Center for Strategic and International Studies** - CSIS[66], com tomadores de decisões de tecnologias da informação de oito países, revelou que 82% dos empregadores relatam uma falta de habilidades de seus empregados no tema de segurança cibernética, e 71% acreditam que essa lacuna de talentos causa danos diretos às suas organizações.

No Brasil, as seguintes lacunas foram identificadas:

- poucos profissionais especializados em segurança cibernética;

- baixa conscientização dos usuários; e

- poucos programas educacionais focados na área.

O combate aos ataques cibernéticos exige profissionais continuamente capacitados. Nesse sentido, urge a necessidade de um programa de capacitação de abrangência nacional destinado à formação técnica e ao aprimoramento de recursos humanos com vistas a fortalecer a segurança cibernética nos órgãos de governo e nas empresas privadas. Nesse contexto, as instituições públicas devem buscar a articulação e o fortalecimento na área de segurança cibernética, por meio de ações colaborativas e de parcerias com o setor privado, com a academia e com o terceiro setor, no País e no exterior, para estimular o contínuo desenvolvimento de massa crítica e de talentos. Visualiza-se como uma das alternativas possíveis, a disponibilização de treinamentos gratuitos em segurança cibernética em plataformas virtuais de governo.

O investimento em capacitação de profissionais de segurança - gestores, analistas e mesmo operadores - objetiva a adoção não apenas de uma atitude preventiva ou reativa diante de ameaças e de incidentes cibernéticos, mas também de uma atitude consultiva, o que resultará em maior confiança por parte das áreas finalísticas de suas instituições, e em menor resistência, em caso de recomendações.

Verifica-se, ainda, que em geral as equipes de segurança enfrentam uma disparidade entre a disponibilidade de mão de obra qualificada e a sofisticação das ameaças, sendo de suma importância o investimento na capacitação de profissionais para que possam, de modo eficaz, enfrentar esses constantes desafios.

Por fim, a efetividade do desenvolvimento de uma cultura de segurança cibernética por intermédio da conscientização, formação e capacitação depende de uma gestão de conhecimento bem estruturada, a fim de dar continuidade a todos os processos envolvidos, formar profissionais no estado-da-arte e em função da dinâmica do surgimento e da obsolescência das competências de segurança cibernética.

REFERÊNCIAS

1. BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Estratégia de Segurança da Informação e Comunicações e de Segurança cibernética da Administração Pública Federal, 2015-2018. Versão 1.0. Disponível em: <http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf>. Acesso em maio de 2019.

2. BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Casa Civil, Subchefia para Assuntos Jurídicos, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm>. Acesso em maio de 2019.

3. BRASIL. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 93, de 26 de setembro de 2019. Aprova o Glossário de Segurança da Informação. Disponível em: <http://www.in.gov.br/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Acesso em outubro de 2019.

4. MODELO DE MATURIDADE DA CAPACIDADE DE CIBERSEGURANÇA (CMM). CARNEGIE-MELLON UNIVERSITY. Disponível em: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5887>. Acesso em maio de 2019.

5. REPORT “DIGITAL IN 2018. WE ARE SOCIAL. HOOTSUITE. Disponível em: < https://hootsuite.com/pt/pages/digital-in-2018> Acesso em maio de 2019.

6. *THE COST OF CYBERCRIME*. INTERNET SOCIETY. Disponível em: <https://www.internetsociety.org/blog/2018/02/the-cost-of-cybercrime/>. Acesso em maio de 2019.

7. *WORLD ECONOMIC OUTLOOK REPORTS.* INTERNATIONAL MONETARY FUND. Disponível em: <https://www.imf.org/en/Publications/WEO/Issues/2019/03/28/world-economic-outlook-april-2019>. Acesso em maio de 2019.

8. *GLOBAL DIGITAL POPULATION AS OF JULY 2019 (IN MILLIONS)*. STATISTA. Disponível em: <https://www.statista.com/statistics/617136/digital-population-worldwide/>. Acesso em maio de 2019.

9. *TEMPEST, EMPRESA DE SEGURANÇA DIGITAL, COMPRA INTEGRADORA EZ-SECURITY*. VALOR ECONÔMICO. Disponível em: <https://www.valor.com.br/empresas/5313593/tempest-empresa-de-seguranca-digital-compra-integradora-ez-security>. Acesso em maio de 2019.

10. *BRASIL OCUPA 66º LUGAR EM RANKING DA ONU DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO*. NAÇÕES UNIDAS - BRASIL. Disponível em: <https://nacoesunidas.org/brasil-ocupa-66o-lugar-em-ranking-da-onu-de-tecnologia-de-informacao-e-comunicacao> Acesso em junho de 2019.

11. Referências das fontes utilizadas para compor o cenário descrito no Anexo I - Diagnóstico:

(1) *MEASURING THE INFORMATION SOCIETY REPORT 2017.* ITU. Disponível em: <https://www.itu.int/en/ITUD/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf>. Acesso em junho de 2019.

(2) BRASIL. Tribunal de Contas da União. Relatório de levantamento Governança de Tecnologia da Informação (TI) na Administração Pública Federal (APF). TC 008.127/2016-6. Disponível em: <https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/perfil-de-governanca-de-ti/>. Acesso em junho de 2019.

(3) *GLOBAL CYBERSECURITY INDEX 2018.* ITU. Disponível em: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>. Acesso em junho de 2019.

(4) *PNAD CONTÍNUA TIC 2017*. PNAD. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais>. Acesso em junho de 2019.

(5) *PESQUISA TIC EMPRESAS 2017.* CETIC.BR. Disponível em: <https://www.cetic.br/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nas-empresas-brasileiras-tic-empresas-2017/>. Acesso em junho de 2019.

(6) *PESQUISA TIC EMPRESAS 2017.* CETIC.BR. Disponível em: <https://cetic.br/tics/governo/2017/orgaos/>. Acesso em junho de 2019.

(7) *NORTON LIFELOCK CYBER SAFETY INSIGHTS REPORT 2018.* NORTON SECURITY. Disponível em: <2018 Norton LifeLock Cyber Safety Insights Report>. Acesso em junho de 2019.

(8) *8 A CADA 10 EXECUTIVOS JÁ ENFRENTARAM FRAUDES CIBERNÉTICAS*. IT FORUM 365. Disponível em: <https://itforum365.com.br/8-cada-10-executivos-ja-enfrentaram-fraudes-ciberneticas/> Acesso em junho de 2019.

(9) *PESQUISA TIC EMPRESAS 2017.* CETIC.BR. Disponível em: <https://www.cetic.br/media/docs/publicacoes/2/10522920190604-TIC-EMPRESAS-2017-ed-rev.pdf>. Acesso em junho de 2019.

(10) *NORTON CYBER SAFETY INSIGHTS REPORT, 2017.* NORTON SECURITY. Disponível em: <https://us.norton.com/cyber-security-insights-2017> Acesso em junho de 2019.

(11) *NORTON CYBER SAFETY INSIGHTS REPORT, 2017.* NORTON SECURITY. Disponível em: <https://us.norton.com/cyber-security-insights-2017> Acesso em junho de 2019.

12. *INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2018.* EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION, EUROPOL. Disponível em: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018> Acesso em junho de 2019.

13. *RELATÓRIO DA SEGURANÇA DIGITAL NO BRASIL,* 2018. PSAFE. Disponível em: <https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf.>. Acesso em junho de 2019.

14. *CYBER REVIEW 2019*. JLT BRASIL. Disponível em: <http://www.brasil.jlt.com/midia/noticias-e-releases/2019/04/nova-edicao-cyber-view-2019>. Acesso em junho de 2019.

15. *TEMPEST APRESENTA PRIMEIRO ESTUDO DO MERCADO BRASILEIRO DE CIBERSEGURANÇA*. CRYPTO ID. TEMPEST/EZ-SECURITY. Disponível em: <https://cryptoid.com.br/pesquisas-seguranca-da-informacao-e-ciberseguranca/tempest-apresenta-primeiro-estudo-do-mercado-brasileiro-de-ciberseguranca/>. Acesso em junho de 2019.

16. BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. Estratégia Brasileira para a Transformação Digital (E-Digital). MCTIC. Disponível em: <http://www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf>. Acesso em julho de 2019.

17. BC QUER CRIAR CONDIÇÕES PARA O REAL SER LIVREMENTE NEGOCIADO NO EXTERIOR. EXAME. Disponível em: <https://exame.abril.com.br/seu-dinheiro/bc-quer-criar-condicoes-para-o-real-ser-livremente-negociado-no-exterior/>. Acesso em outubro de 2019.

18. Open Insurance chega ao mercado brasileiro. IBRACOR. Disponível em: http://ibracor.org.br/todas-noticias/-/asset_publisher/oEWZ8S1DqA47/content/open-insurance-chega-ao-mercado-brasileiro. Acesso em outubro de 2019.

19. *EGOVERNMENT BENCHMARK 2018.* EUROPEAN COMMISSION. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2018-digital-efforts-european-countries-are-visibly-paying>. Acesso em junho de 2019.

20. CYBERSECURITY FRAMEWORK. NIST. Disponível em: <https://www.nist.gov/cyberframework/online-learning/five-functions>. Acesso em outuibro de 2019.

21. BRASIL. Decreto nº 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9203.htm>. Acesso em junho de 2019.

22. INFONOVA. Disponível em: < https://www.infonova.com.br/artigo/entenda-sobre-pirataria-de-software/>. Acesso em outubro de 2019.

23. ISACA. Disponível em: <http://www.isaca.org/COBIT/Pages/default.aspx>. Acesso em outubro de 2019.

24. NIST. Disponível em: <https://www.nist.gov/>. Acesso em outubro de 2019.

25. CIS. Disponível em: <https://www.cisecurity.org/>. Acesso em outubro de 2019.

26. ECOIT. Disponível em: https://ecoit.com.br/o-que-e-soar/. Acesso em outubro de 2019.

27. IBLISS. Disponível em: https://www.ibliss.digital/saiba-o-que-uma-plataforma-soar-pode-fazer-pelo-seu-negocio/>. Acesso em outubro de 2019.

28. TI FORENSE. Disponível em: <https://www.tiforense.com.br/o-que-e-um-siem/>. Acesso em outubro de 2019.

29. MUROYA, Leonardo. Apresentação “Trilha Cases & Lições”, Security Leaders 10 Anos, São Paulo, 29 Out 19.

30. *O QUE É UM CERTIFICADO DIGITAL?.* BRY TECNOLOGIA. Disponível em: <https://www.bry.com.br/blog/o-que-e-um-certificado-digital/>. Acesso em junho de 2019.

31. *NÚMEROS DA ICP-BRASIL EM ABRIL DE 2019*. ITI. Disponível em: <https://www.iti.gov.br/component/content/article?id=2590>. Acesso em julho de 2019.

32. BRASIL. CONGRESSO NACIONAL. Senado Federal. Comissão Parlamentar de Inquérito. CPI da Espionagem. Disponível em: <https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>. Acesso em julho de 2019.

33. BRASIL. Decreto nº 9.203, de 22 novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9203.htm>. Acesso em julho de 2019.

34. CERT.BR. Disponível em: < https://www.cert.br/>. Acesso em julho de 2019.

35. CTIR Gov. Disponível em: < https://www.ctir.gov.br/>. Acesso em julho de 2019.

36. COMMON VULNERABILITIESAND EXPOSURES. CVE. Disponível em: <https://cve.mitre.org/index.html>. Acesso em outubro de 2019.

37. *INCIDENTES REPORTADOS AO CERT.BR -- JANEIRO A DEZEMBRO DE 2018*. CERT.BR. Disponível em: <https://www.cert.br/stats/incidentes/2018-jan-dec/analise.html>. Acesso em julho de 2019.

38. HIGH SECURITY CENTER. HSC. Disponível em: <https://www.hscbrasil.com.br/seguranca-de-endpoint/>. Acesso em outubro de 2019.

39. CANAL COMSTOR. Disponível em: <https://blogbrasil.comstor.com/qual-a-importancia-de-uma-seguranca-de-endpoint>. Acesso em outubro de 2019.

40. AVTEST. Disponível em: <https://www.av-test.org/en/statistics/malware/>. Acesso em outubro de 2019.

41. SEGURANÇA DA REDE E DO ENDPOINT, PALO ALTO. Disponível em: <https://www.paloaltonetworks.com.br/resources/whitepapers/traps-and-ngfw-better-together>. Acesso em outubro de 2019.

42. CSO. UNITED STATES. Disponível em: <https://www.csoonline.com/article/3387981/stakes-of-security-especially-high-in-pharmaceutical-industry.html>. Acesso em outubro de 2019.

43. BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Casa Civil, Subchefia para Assuntos Jurídicos, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm>. Acesso em julho de 2019.

44. *PONEMOM REPORT 2018.* LEADCOMM. Disponível em: <https://leadcomm.com.br/portfolio_item/2018-ponemom-report/>. Acesso em julho de 2019.

45. BRASIL. Banco Central do Brasil. Resolução nº 4.658, de 26 de abril de 2018. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: <https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf>. Acesso em julho de 2019.

46. BRASIL. Banco Central do Brasil. Circular nº 3.909, de 16 de agosto de 2018. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: <http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/37402932/do1-2018-08-20-circular-n-3-909-de-16-de-agosto-de-2018-37402763>. Acesso em julho de 2019.

47. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em julho de 2019.

48. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em julho de 2019.

49. BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em

julho de 2019.

50. BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em julho de 2019.

51. BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação. Legislação. Disponível em: <http://dsic.planalto.gov.br/assuntos/editoria-c>. Acesso em julho de 2019.

52. NAÇÕES UNIDAS. BRASIL. Disponível em: <https://nacoesunidas.org/pos2015/agenda2030/>. Acesso em outubro de 2019.

53. *IMD WORLD COMPETITIVENESS RANKING 2019*. IMD. Disponível em: <https://www.imd.org/contentassets/6b85960f0d1b42a0a07ba59c49e828fb/one-year-change-vertical.pdf>. Acesso em julho de 2019.

54. MCTIC. FUNDO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO (FNDCT). Disponível em: < http://fndct.mcti.gov.br/>. Acesso em agosto de 2019.

55. PESQUISA FAPESP. Disponível em: https://revistapesquisa.fapesp.br/2018/01/16/inovacao-permanente/. Acesso em outubro de 2019.

56. *ALAGOAS: INDÚSTRIA 4.0 TAMBÉM SERÁ NECESSIDADE PARA PEQUENAS EMPRESAS*. AGÊNCIA DO RÁDIO MAIS. 05 Out 18. Disponível em: <https://www.agenciadoradio.com.br/noticias/alagoas-industria-4-0-tambem-sera-necessidade-para-pequenas-empresas-mrin180127>. Acesso em agosto de 2019.

57. HURIEL, LOUISE MARIE e LOBATO, LUISA. *Uma Estratégia para a Governança da Segurança Cibernética no Brasil*. Instituto Igarapé, Nota Estratégica 30, setembro 2018.

58. WESTERN SYDNEY UNIVERSITY. Disponível em: <https://www.westernsydney.edu.au/studysmart/home/digital_literacy/what_is_digital_literacy>. Acesso em outubro de 2019.

59. ROCKCONTENT. Disponível em: <https://comunidade.rockcontent.com/nativos-digitais/>. Acesso em outubro de 2019.

60. *HACKING THE SKILLS SHORTAGE. A STUDY OF THE INTERNATIONAL SHORTAGE IN CYBERSECURITY SKILLS*. MCAFEE/CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. Jul 2016. Disponível em: <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf>. Acesso em agosto de 2019.

61. BRASIL. PLANO NACIONAL DE EDUCAÇÃO. Lei nº 10.172, de 9 de janeiro de 2001. Aprova o Plano Nacional de Educação e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10172.htm>. Acesso em agosto de 2019.

62. *SKILLS REVOLUTION 2.0.* MANPOWERGROUP. Disponível em: <https://www.manpowergroup.com/wps/wcm/connect/59db87a7-16c6-490d-ae70-1bd7a322c240/Robots_Need_Not_Apply.pdf?MOD=AJPERES>. Acesso em agosto de 2019.

63. INFRA NEWS TELECOM. Disponível em: <https://infranewstelecom.com.br/brasil-precisa-formar-70-mil-profissionais-de-tecnologia-ao-ano-ate-2024/>. Acesso em outubro de 2019.

64. IT FORUM 365. Sisponível em: <https://www.itforum365.com.br/brasil-precisa-investir-em-areas-stem-para-nao-ficar-fora-do-mercado-de-trabalho-alerta-especialista/>. Acesso em outubro de 2019.

65. *STATE OF CYBERSECURITY: 2019.* ISACA. Disponível em: <https://www.isaca.org/info/state-of-cybersecurity-2019/index.html>. Acesso em agosto de 2019.

66. CSIS. Disponível em: <https://www.csis.org/>. Acesso em agosto de 2019.

*