Revisão Da Capacidade De Cibersegurança

República Federativa do Brasil

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

GSI-PR

GREAT for PARTNERSHIP

OEA

Mais direitos para mais pessoas

Revisão da Capacidade de Cibersegurança

República Federativa do Brasil

Agradecimentos

Esta publicação foi possível graças à colaboração de muitas pessoas e instituições. Por este motivo, a Secretaria do Comitê Interamericano contra o Terrorismo da Organização dos Estados Americanos (CICTE / OEA), o Centro de Capacidade Global de Segurança Cibernética da Universidade de Oxford, o Departamento de Segurança da Informação - DSI do Escritório da Segurança Institucional da Presidência da República do Brasil, e o Governo do Reino Unido agradece às seguintes instituições por terem participado do processo de preparação e lançamento deste relatório.

Ministério da Defesa

Agência Brasileira de Inteligência (Abin)

Centro de Defesa Cibernética (CDCIBER)

Exército do Brasil (CIE)

Polícia Federal do Brasil

Ministério Público Federal

Superior Tribunal de Justiça

Minitério de Justiça

Ministério Ciência e Tecnologia

Agência Nacional de Telecomunicações (ANATEL)

Ministério das Relações Exteriores

Ministério da Educação

Ministério do Trabalho e Emprego

Ministério do Planejamento, Orçamento e Gestão

Ministério da Fazenda

Ministério da Saúde

Ministério dos Transportes
Ministério de Minas e Energia
Corregedoria-Geral da União (CGU)

Tribunal de Contas da União (TCU)

Banco Central do Brasil

Ministério da Indústria, Comércio Exterior e Serviços

Núcleo de Informação e Coordenação do Ponto BR (NIC.BR)

Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR.BR)

Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil (CERT.Br)

Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa (CAIS /RNP)

Centro de Coordenação para Tratamento de Incidentes de Redes do Exército Brasileiro (CCTIR / EB)

Centro de Tratamento de Incidentes de Rede Força Aérea Brasileira (CTIR.FAB)

Grupo de Resposta a Incidentes de Segurança em Computadores da CAIXA (CSIRT / CAIXA)

Grupos de Resposta a Incidentes de Segurança em Computadores do Banco do Brasil (CSIRT / BB)

Grupo de Resposta a Ataques do SERPRO (GRA / SERPRO)

Grupo de Resposta a Incidentes de Segurança Computacional da Câmara dos Deputados (GRIS / Correios)

CSIRT / CETRA (MPOG)
GATI (CADE, DPF, DPRF, DPU e FUNAI)

Grupo de Respostas a Incidentes de Segurança em Computadores Câmara dos Depútados (GRIS CD)

Rede-Rio de Computadores (CEO/Rede Rio)

Grupo de Respostas a Incidentes de Segurança do Grupo Abril (GRIS ABRIL)

Banco Caixa Geral

Banco do Brasil

Telecomunicações Brasileiras (Telebras)

Sumário

GESTÃO DE DOCUMENTOS

Pesquisadores responsáveis (2018):
Doutor Ioannis Agrafiotis, Doutora Eva Nagyfejeo, Doutora Maria Bada

Pesquisadores responsáveis (2019):
Doutor Andraz Kastelic

Revisado por:
Professor William Dutton, Professor Michael Goldsmith,
Professor Basie von Solms

Aprovado por:
Professor Michael Goldsmith

Versão	Data	Notas
1	3 de agosto de 2018	Primeiro esboço para a Diretoria Técnica
2	16 de agosto de 2018	Segundo esboço revisado pela Diretoria Técnica
3	11 de setembro de 2018	Terceiro esboço revisado pela OEA
4	3 de julho de 2019	Primeiro esboço revisado após o seminário de validação
5	21 de abril de 2020	Segundo esboço revisado apresentado à OEA após o seminário de validação
6	18 de maio de 2020	Terceira versão apresentada à OEA
7	5 de junho de 2020	Versão final apresentada à OEA

LISTA DE SIGLAS

ABIN
Agência Brasileira de Inteligência

ANATEL
Agência Nacional de Telecomunicações

CA
Autoridade Certificadora

CEPESC
Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações

CERT
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança

CGSIC
Comitê Gestor de Segurança da Informação e Comunicação

IC
Infraestrutura Crítica

CICTE
Comitê Interamericano contra o Terrorismo

CISM
Gerente Certificado de Segurança da Informação

CISSP
Certificado Profissional de Segurança de Sistemas de Informação

CMM
Modelo de Maturidade da Capacidade

CMU CERT
Equipe de Resposta a Emergências Informáticas da Universidade Carnegie Mellon

CNPJ
Cadastro Nacional de Pessoa Jurídica

CoE
Conselho da Europa

CPF
Cadastro de Pessoas Físicas

C-PROC
Escritório do Programa de Crime Cibernético do Conselho da Europa

CSIRT
Equipe de Resposta a Incidentes de Segurança Cibernética

CTIR Gov
Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo

DDOS
Ataque de Negação de Serviço Distribuído

ECA
Estatuto da Criança e do Adolescente

FIRST
Fórum de Resposta a Incidentes e Equipes de Segurança

FPA
Administração Pública Federal

GCSCC
Centro Global de Capacidade de Segurança Cibernética

GSI
Gabinete de Segurança Institucional

ICT
Tecnologias da Informação e das Comunicações

IDS
Sistemas de Detecção de Invasão

ISP
Provedor de Serviços de Internet

KPI
Indicador Chave de Desempenho

LACNIC
Registro de Endereços de Internet para a América Latina e o Caribe

NGO
Organização não governamental

NIST
Instituto Nacional de Normas e Tecnologia

OAS
Organização dos Estados Americanos

RNP
Rede Nacional de Ensino e Pesquisa

SENAC
Serviço Nacional de Aprendizagem Comercial

SERPRO
Serviço Federal de Processamento de Dados

SIAFI
Sistema Integrado de Administração Financeira do Governo Federal

SIEM
Gerenciamento de Eventos e Informações de Segurança

SME
Pequenas e médias empresas

SPED
Sistema Público de Escrituração Digital

SSH
Secure Shell

STIX
Expressão Estruturada de Informações sobre Ameaças

TCU
Tribunal de Contas da União

TLP
Protocolos Semáforos

URCC
Unidade de Repressão a Crimes Cibernéticos

RESUMO EXECUTIVO

O Centro Global de Capacidade de Segurança Cibernética (GCSCC ou " Centro") procedeu a uma análise da maturidade da capacidade de segurança cibernética no Brasil, a convite da Secretaria do Comitê Interamericano contra o Terrorismo (CICTE), com o qual estabeleceu cooperação, por intermédio de seu programa de segurança cibernética, da Organização dos Estados Americanos (OEA). O objetivo dessa análise era levar o Governo a entender sua capacidade de segurança cibernética, com o intuito de priorizar estrategicamente o investimento em capacidade de segurança cibernética.

Em 19 e 20 de março de 2018, as seguintes partes interessadas participaram de mesas-redondas de consulta: justiça criminal, cumprimento da lei, comunidade de defesa, funcionários de tecnologia da informação e representantes de entidades do setor público, proprietários de infraestrutura crítica, formuladores de políticas, equipes de resposta a emergências informáticas, funcionários de tecnologia da informação do setor privado (incluindo instituições financeiras), empresas de telecomunicações, o setor bancário e parceiros internacionais.

Os pesquisadores do GCSCC visitaram Brasília novamente, um ano depois, para validar os resultados de 2018 e para atualizar adequadamente o projeto de relatório de análise da capacidade de segurança cibernética. A metodologia de coleta de dados, utilizada em março de 2019, foi semelhante à metodologia utilizada no ano anterior. As partes interessadas que participaram das entrevistas do grupo de discussão incluíram representantes do setor acadêmico, operadores da infraestrutura crítica nacional, fornecedores de serviços de telecomunicações e outras entidades do setor privado, ministérios do governo, o Poder Judiciário, encarregados do cumprimento da lei, a comunidade de defesa, o setor financeiro, equipes de resposta a emergências informáticas (CERTs), a mídia, o setor privado e a sociedade civil.

Tanto em 2018 quanto em 2019, as consultas foram realizadas utilizando o Modelo de Maturidade em Capacitação (CMM), do Centro, que estabelece cinco dimensões da capacidade de segurança cibernética:

- Política e estratégia de segurança cibernética
- Cultura cibernética e sociedade
- Educação, treinamento e competências em segurança cibernética
- Estruturas jurídicas e regulamentares
- Normas, organizações e tecnologias

Cada dimensão é composta por uma série de fatores que descrevem o significado de possuir capacidade de segurança cibernética. Cada fator apresenta uma série de aspectos, e para cada aspecto há indicadores que descrevem passos e ações que, uma vez observados, definem o estágio de maturidade desse aspecto. Os estágios de maturidade são cinco, abrangendo do estágio inicial ao estágio dinâmico. O estágio inicial pressupõe uma abordagem ad hoc da capacidade, enquanto o estágio dinâmico representa uma abordagem estratégica e a capacidade de adaptação dinâmica ou de mudança em resposta a considerações ambientais. Mais detalhes sobre as definições de cada estágio em todas as dimensões constam do documento do CMM.[1]

A Figura 1 (abaixo) mostra uma representação geral da capacidade de segurança cibernética do Brasil e ilustra as estimativas de maturidade em cada dimensão. Cada dimensão representa um quinto do gráfico, com os cinco estágios de maturidade para cada fator estendendo-se para fora do centro do gráfico; o 'inicial' é o mais próximo do centro do gráfico e o 'dinâmico' é colocado no perímetro.

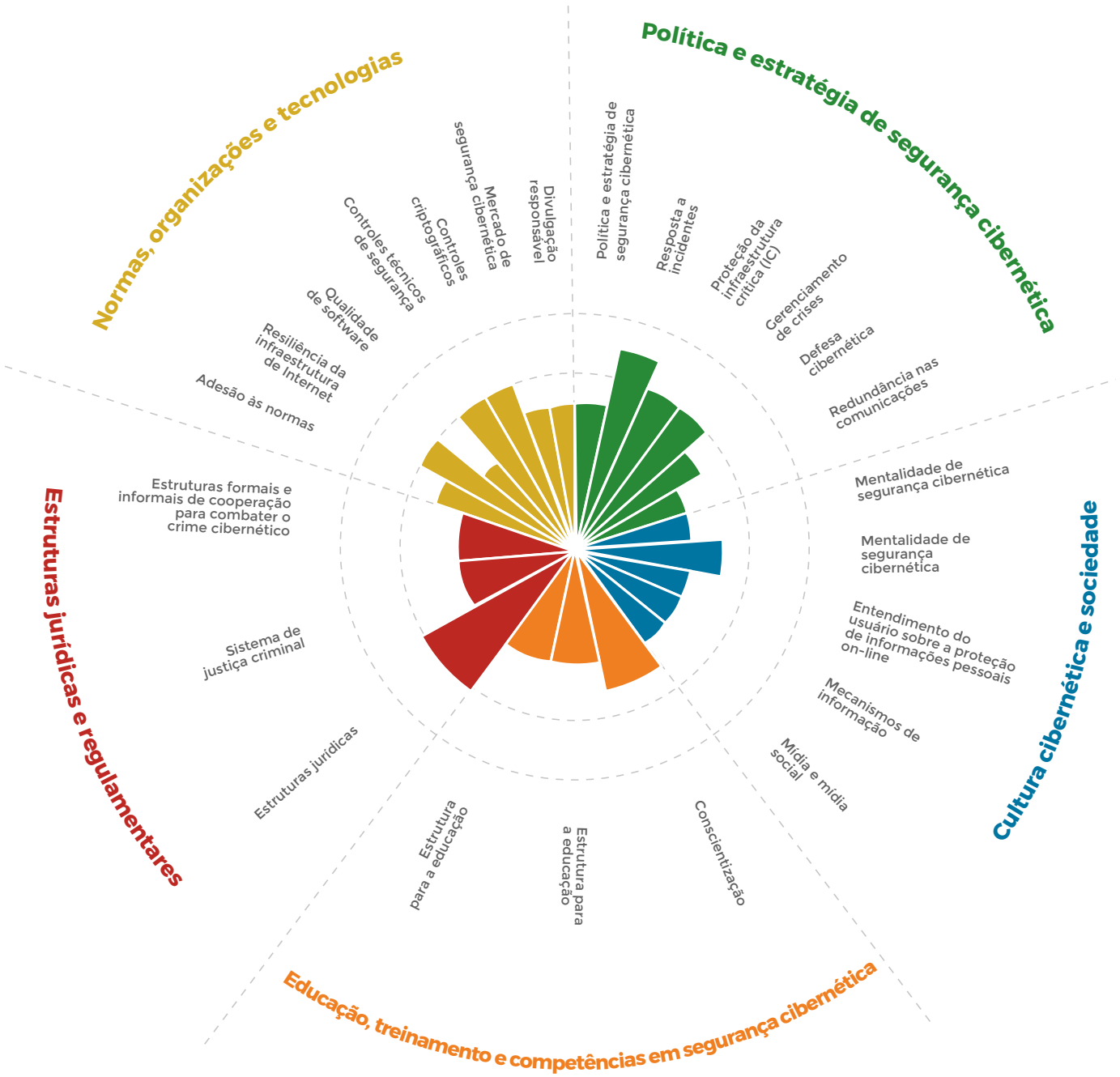


Figura 1: *Representação geral da capacidade de segurança cibernética no Brasil*

Política e estratégia de segurança cibernética

No momento da análise, em março de 2018, não havia nenhum documento oficial nacional de segurança cibernética com instruções sobre como estabelecer a coordenação entre os principais atores governamentais e não governamentais da segurança cibernética. A inexistência de colaboração entre as instituições governamentais e o setor privado e a "fragmentação das respostas" foram potencialmente abordadas com a Estratégia (2015-2018).[2] A Estratégia visava detalhar as diretrizes estratégicas para a segurança da informação e das comunicações e coordenar esses esforços entre os vários atores envolvidos, a fim de reduzir os riscos aos quais as organizações e a sociedade estão expostas. A estratégia teve como centro a Administração Pública Federal, com os críticos destacando a ausência de uma autoridade central para implementar essa abordagem sistemática e de múltiplos atores, bem como a inexistência de organizações da sociedade civil, de partes interessadas na Internet e do público em geral desde a elaboração da estratégia. Quanto à organização do programa de segurança cibernética, os participantes expressaram sua preferência por um modelo descentralizado, em que os setores comerciais fossem supervisionados pelas agências reguladoras existentes, com uma nova agência nacional criada para coordenar os esforços.

Após a validação das entrevistas do grupo de discussão, realizadas em março de 2019, foi confirmado que a Estratégia Nacional de Segurança Cibernética (Decreto Federal n° 10.222) foi finalmente aprovada em fevereiro de 2020.[3] De acordo com fontes governamentais, o decreto se concentra em dez ações estratégicas que devem orientar a Administração Pública Federal no desenvolvimento de suas próprias ações quanto à segurança cibernética.

Quanto à resposta a incidentes, as Equipes de Resposta a Incidentes de Segurança Cibernética (CSIRTs)[4] são muitas, desde entidades governamentais até entidades do setor privado e instalações acadêmicas. Dependendo do papel de uma CERT, essas entidades podem estar envolvidas exclusivamente na gestão da segurança dos sistemas ou na aplicação de diretrizes de segurança cibernética, ou ser responsáveis pela coordenação de esforços entre as autoridades nacionais e os âmbitos locais. A CERT nacional (CERT.br) é um órgão certificado pelo Fórum de Resposta a Incidentes e Equipes de Segurança (FIRST), cabendo-lhe a responsabilidade pelo processamento de relatórios de incidentes para o setor privado.[5] O Centro de Treinamento e Resposta a Incidentes Cibernéticos de Governo da Administração Pública Federal (CTIR Gov) oferece respostas a incidentes para a Administração Pública Federal, enquanto as CERTs são dedicadas a setores específicos e partes interessadas em infraestrutura crítica (IC). Também foi criada uma CERT militar para proteger as redes militares. Todas essas instituições têm diretrizes e papéis claros quanto à resposta a incidentes; o CERT.br mantém o cadastro de incidentes nacionais e publica anualmente dados estatísticos de ameaças e incidentes. Todas as CERTs apresentam relatórios por meio dos canais oficiais ao CERT.br. Sistemas automatizados em conformidade com normas internacionais, como o Expressão Estruturada de Informações sobre Ameaças (STIX) e os Protocolos Semáforos (TLP), garantem o compartilhamento da inteligência de ameaças com as CERTs que colaboram com o CERT.br. As ações jurídicas em curso visam a racionalizar o compartilhamento da inteligência de ameaças entre todas as CERTs, uma vez que nem todas

as partes interessadas privadas da IC têm direito a receber inteligência de ameaças. Como o leque de partes interessadas em IC vem se expandindo, há necessidade de maior participação das instituições de pesquisa.

A maturidade da capacidade do Brasil de proteger a infraestrutura crítica varia entre operadores públicos e privados de IC. Todas as instituições federais são obrigadas a realizar avaliações de risco cibernético, que são atualizadas anualmente com base nas lições aprendidas com os principais eventos. As partes interessadas da IC pública incluem empresas de telecomunicações, transporte, energia e instituições financeiras, todas em cooperação e coordenação mediante canais formais de comunicação com o Ministério da Defesa. Existem políticas e procedimentos claramente definidos a serem seguidos por todas as instituições públicas, com base nas informações prestadas pela ferramenta de conscientização situacional do CERT.br. O acesso a esses protocolos é concedido à Polícia Federal e aos serviços de inteligência para aumentar a cooperação entre as partes interessadas da IC. Hoje, o setor privado não é considerado parte da IC do país. Uma vez que o Brasil promoveu a privatização em setores críticos, como o financeiro, é imperativa uma revisão da lista de partes interessadas na IC, a fim de considerar as instituições privadas. As instituições privadas não são obrigadas a informar o Governo sobre incidentes graves, têm acesso restrito à inteligência de ameaças e ignoram as avaliações de risco e os processos implantados pelo governo para os operadores públicos de IC. Portanto, as instituições privadas precisam desenvolver suas próprias avaliações de risco e políticas de segurança internas, cuja eficácia dependerá de seu grau de maturidade. A maioria dos participantes instou o governo a criar um mecanismo de identificação do nível de maturidade da governança de TI, tanto no setor público quanto no privado, um protocolo de comunicação para distribuir alertas aos setores público e privado e uma iniciativa para avaliar as normas e os padrões aplicados por organizações privadas e públicas.

Na última década, o Brasil sediou uma série de eventos importantes e, como se esperava, o país experimentou uma série de ataques cibernéticos durante esses eventos. Os processos de tratamento de incidentes durante esses eventos mostraram que organizações críticas para a defesa cibernética são capazes de colaborar e mitigar efetivamente o impacto de tais ataques. As organizações que participaram do gerenciamento de crises tinham papéis claros, havia protocolos transparentes sobre como divulgar informações e notificar incidentes a instâncias superiores e diretrizes específicas sobre a proteção dos sistemas. Entretanto, os processos de gerenciamento de crise foram personalizados para esses eventos específicos. A experiência e as lições aprendidas nesses eventos deveriam alicerçar os esforços atuais no gerenciamento de crises. Os protocolos de gerenciamento de crises devem ser projetados e uma rede de organizações públicas e privadas criada para administrar as crises. Treinamento e exercícios sobre eventos simulados de crise foram sugeridos como a maneira ideal de validar protocolos de comunicação, aumentar a conscientização sobre a segurança cibernética e testar processos de tratamento de incidentes. Para essa finalidade, os participantes mencionaram o exercício Guardião Cibernético, que utiliza planejamento de alto nível para desenhar cenários e plataformas de simulação para operações cibernéticas que possam emular sistemas críticos dos setores financeiro, nuclear e público.

Quanto à governança da segurança cibernética, o governo brasileiro atribuiu a esfera política e estratégica ao Gabinete de Segurança Institucional da Presidência da República (GSI), e os procedimentos estratégicos, operacionais e de defesa cibernética ao Ministério da Defesa. Nos últimos anos, a área militar foi reestruturada para atender às necessidades de um sistema democrático em evolução, com foco em ameaças transfronteiriças emergentes e eventos de segurança interna. Há um documento oficial sobre defesa cibernética, publicado em 2012, além de diretrizes sobre políticas de segurança cibernética. As forças armadas operam uma CERT e ministram treinamento relacionado a gestão de risco e resposta a incidentes. Os participantes sugeriram que as forças armadas detêm capacidade tanto ofensiva quanto defensiva, e se centram no aprimoramento

das medidas defensivas. Salientaram que as forças armadas implantam sistemas que proporcionam consciência situacional e se encarregam, proativamente, da defesa de ataques de negação de serviço distribuídos (DDoS) ou da vandalização de sites. Há laboratórios para analisar software malicioso e um número significativo de funcionários em treinamento para executar essas tarefas.

Não foi possível obter uma visão ampla sobre a redundância nas comunicações no decorrer da análise do CMM. Os participantes sugeriram que o setor público conta com recursos de resposta a emergências conectados à estratégia nacional e sua rede de comunicação de emergência dispõe dos recursos apropriados para avaliar os protocolos de redundância em vigor, avaliar os sistemas redundantes, executar exercícios e realizar simulacros de comunicação. Existem diversos centros de crise designados em locais geograficamente dispersos para garantir a participação de todas as partes interessadas em caso de emergência. Em forte contraste, o setor privado é negligenciado e excluído desses planos, com exceção das CERTs privadas.

Cultura de segurança cibernética e sociedade

No tocante à dimensão cultura de segurança cibernética e sociedade, o Governo reconheceu a necessidade de priorizar a segurança cibernética em todas as suas instituições. Além disso, aspectos dos processos governamentais e estruturas institucionais foram projetados em resposta aos riscos de segurança cibernética, mas as iniciativas são encontradas principalmente nas principais agências. Em geral, os participantes observaram que a cultura de segurança no Brasil varia entre diferentes partes do país e diferentes setores do governo e da economia. Uma questão percebida pelos participantes foi que as estruturas governamentais são muito complexas. Portanto, quando se trata da avaliação da maturidade do setor público, é possível identificar diferentes estágios em diferentes departamentos. Outra preocupação suscitada pelos participantes foi a inexistência de um mecanismo de coordenação para identificar o nível de maturidade no governo e em todos os seus setores.

As principais empresas líderes do setor privado começaram a priorizar uma mentalidade de segurança cibernética, mediante a identificação de práticas de alto risco. Os setores financeiro e de TI estão mais avançados em segurança cibernética; por serem alvos mais frequentes, investem mais em segurança cibernética. Os participantes nos informaram que desde que os bancos nacionais começaram a tomar medidas de segurança proativas, os criminosos têm se concentrado cada vez mais nos bancos regionais e nas pequenas e médias empresas (PMEs). Uma proporção limitada, mas crescente, de usuários da Internet no Brasil começou a priorizar mais a segurança cibernética; por exemplo, por meio da identificação de riscos e ameaças. A sociedade como um todo ainda carece de uma mentalidade de segurança cibernética; ainda que estejam cientes dos riscos da segurança cibernética, os usuários, muitas vezes, deixam de agir de maneira adequada nas suas práticas cotidianas. Foi mencionado que é comum que até mesmo especialistas em TI, que têm consciência dos riscos, cliquem em e-mails de phishing, ou compartilhem informações sensíveis em sites de mídia social como o Facebook.

Em geral, os participantes acreditam que apenas uma pequena proporção de usuários da Internet avalia criticamente o que veem ou recebem on-line. Da mesma forma, poucos acreditam que os usuários finais têm a capacidade de usar a Internet de forma segura e de se protegerem on-line.

De maneira genérica, há um grande incentivo para que as empresas prestem serviços on-line. A prestação de serviços de comércio eletrônico vem crescendo e aumentou desde 2017. Em 2017, o Brasil (a Polícia Federal do Brasil) e a Europol assinaram um acordo estratégico para aumentar a cooperação no combate a atividades criminosas transfronteiriças, que poderia ser considerada uma operação conjunta formal. Uma proporção crescente de usuários confia no uso seguro dos serviços de comércio eletrônico. O Ministério da Justiça criou uma secretaria dedicada aos direitos do consumidor e ao comércio eletrônico.

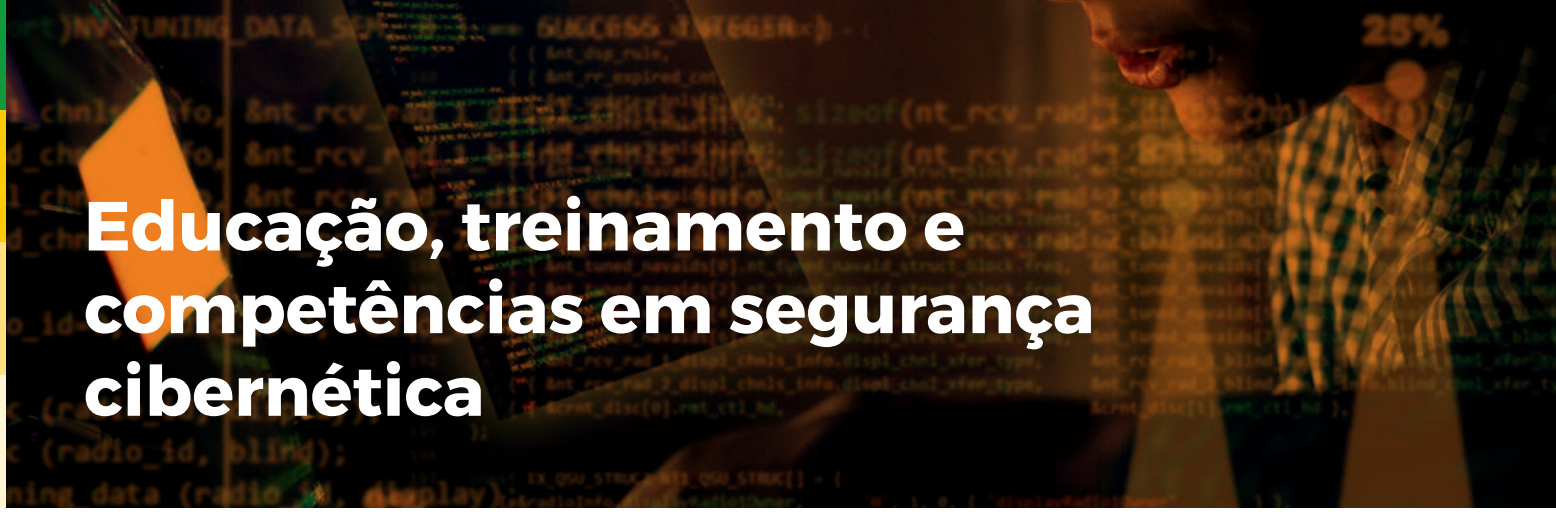
Os serviços de governo eletrônico também se desenvolveram e uma proporção crescente dos usuários confia no uso seguro desses serviços. Serviços como os que enviam declarações de Imposto de Renda e prestam informações sobre a Previdência Social e compras governamentais estão disponíveis via Internet desde 1998.

Observa-se que um número crescente de usuários e interessados dos setores público e privado tem conhecimento geral sobre o tratamento dado às informações pessoais on-line e emprega boas práticas (proativas) de segurança cibernética para proteger suas informações pessoais on-line. As regulamentações de dados pessoais ora em discussão na UE não estão alinhadas com aquelas que vêm sendo discutidas no Brasil. Já foram iniciadas as discussões sobre o enfoque do Brasil para a proteção de informações pessoais e sobre o equilíbrio entre segurança e privacidade, mas isso ainda não resultou em ações ou políticas concretas.

No Brasil, os setores tanto público quanto privado oferecem alguns canais para notificar incidentes on-line, mas esses canais não estão bem coordenados e geralmente são utilizados de forma ad hoc. Foram estabelecidos mecanismos de informação, que são utilizados com frequência, para que os usuários denunciem crimes relacionados à Internet. O SaferNet Brasil[6] presta informações sobre segurança na Internet e os recursos para registrar queixas por meio de seu site. A SaferNet Brasil é uma organização sem fins lucrativos, criada em 2005. Além disso, a Polícia Federal[7] tem uma página exclusiva para o registro de denúncias em seu site, as quais também podem ser enviadas para um endereço de e-mail privativo. O conteúdo ilegal on-line pode ser denunciado por intermédio da linha telefônica de ajuda ao combate da pornografia infantil e adolescente,[8] disponibilizada pelo Governo.

Todos os incidentes podem ser relatados à polícia, enquanto os que não são claramente classificados são encaminhados ao CTIR Gov e posteriormente classificados antes de serem encaminhados às instituições apropriadas. De modo geral, os participantes salientaram que os cidadãos no Brasil carecem de uma cultura de denúncia. Além disso, não foi possível identificar se os mecanismos de denúncia instituídos pelos setores público e privado são utilizados rotineiramente ou com que frequência são utilizados.

A cobertura da mídia sobre segurança cibernética no Brasil é ad hoc, com prestação limitada de informações e reportagens esporádicas sobre questões específicas que as pessoas enfrentam on-line, como pornografia infantil on-line ou assédio virtual. Além disso, os participantes mencionaram que a discussão sobre segurança cibernética nas mídias sociais é limitada. Geralmente, a mídia ignora os detalhes técnicos dos incidentes de segurança cibernética e frequentemente oferece orientações e conselhos possivelmente incorretos sobre o comportamento on-line seguro.



Educação, treinamento e competências em segurança cibernética

Ainda não foi criado um programa nacional de conscientização sobre segurança cibernética, liderado por uma organização específica (de qualquer setor) que aborde uma ampla gama de dados demográficos.

Por causa da ausência de participantes da sociedade civil, não foi possível obter uma imagem clara das iniciativas existentes voltadas para aumentar a conscientização sobre segurança cibernética.

No decorrer da análise, o órgão de conscientização mais importante reconhecido pelos participantes foi a SaferNet Brasil, uma ONG criada em 2005.[9] Essa ONG tem estabelecido parcerias únicas com o Ministério da Justiça, a Polícia Federal e a Secretaria de Direitos Humanos do Gabinete do Presidente da República e existe para "proteger os direitos humanos e servir como linha direta, linha de ajuda e nodo de conscientização no Brasil".[10]

O Comitê Gestor da Internet no Brasil (www.cgi.br) – um conselho de diversas pessoas interessadas, criado pela Portaria Interministerial 147, de 31 de maio de 1995 – é a principal instituição responsável pela promoção das normas de segurança das tecnologias da informação e das comunicações (TIC) e das melhores práticas da Internet.[11] O Comitê executa suas atividades por intermédio do Núcleo de Informação e Coordenação do Ponto BR (NIC.br) (http://nic.br/quem-somos/).[12] Com base em pesquisa documental, o NIC.br implementa diversas iniciativas, como o Antispam.br[13] (http://www.antispam.br/) e o InternetSegura.br[14] (https://www.Internetsegura.br/), dois portais que visam conscientizar crianças e pais sobre spam, e que divulgam materiais sobre a segurança na Internet.

Quanto à conscientização sobre segurança cibernética para executivos, os participantes reconheceram que os níveis são frequentemente baixos entre os membros da gestão da empresa, que precisam aprender como os riscos de segurança cibernética afetam a organização. Além disso, os executivos não são obrigados a participar do treinamento em segurança cibernética, embora esse treinamento seja considerado uma boa prática.

Devido à falta de participação do setor acadêmico, não foi possível obter uma imagem clara sobre a educação em segurança cibernética no Brasil. Portanto, as informações prestadas são baseadas em pesquisa documental.

Os principais atores governamentais e industriais identificaram a necessidade de aprimorar a educação em segurança cibernética nas escolas e universidades.

O Ministério da Educação estabelece o currículo nacional de cursos e requisitos e normas relacionados à segurança cibernética, mas a decisão sobre o nível de desenvolvimento desse currículo nacional cabe às universidades. O currículo não é regulamentado por uma agência central. A análise não informou se há um orçamento nacional separado destinado à educação em segurança cibernética. Os debates do grupo de discussão tampouco esclareceram até que ponto existe cooperação entre o setor privado e as universidades. Há pronta disponibilidade de educadores qualificados em segurança cibernética, porquanto são oferecidos, no Brasil, cursos especializados em informática em nível universitário.

A necessidade de formar profissionais em segurança cibernética foi reconhecida pelo Governo. Com base em pesquisa documental, o Comitê Gestor da Internet no Brasil (CGI.br) (ver D 3.1) coordena os esforços de treinamento por meio da CERT.br, do Portal de Melhores Práticas (BCP.nic.br) e do CGSIC. Os participantes declararam que a maioria dos profissionais do setor público obtém qualificações profissionais de TI no exterior e recebe certificados de TIC, como o Certificado Profissional de Segurança de Sistemas de Informação (CISSP) e o de Gerente Certificado de Segurança da Informação (CISM), autorizados por instituições internacionais (Consórcio Internacional de Certificação de Sistemas de Informação (ISC)2 e ISACA®).

A rede COBIT - Objetivos de Controle de Informação e Tecnologia Relacionada - tem sido aceita como "uma norma de facto para boas práticas em todo o Brasil, em organizações privadas, públicas e governamentais".[15]

Estruturas jurídicas e regulamentares

O Brasil carece de uma estrutura regulamentar abrangente que considere expressamente a segurança cibernética. A despeito dos esforços envidados por introduzir regulamentação mediante uma estrutura legislativa vinculante, a legislação sobre segurança cibernética no Brasil continua em desenvolvimento. Entretanto, foram adotadas várias diretrizes oficiais ou "leis não vinculantes" que dizem respeito às questões de segurança cibernética.

A Lei de Crimes Cibernéticos (Lei n°. 12.737/2012),[16] também conhecida como "Lei Carolina Dieckmann", e o Marco Civil da Internet no Brasil (Lei n°. 12.965/2014)[17] são consideradas as peças de legislação mais relevantes e substantivas em vigor. Elas procuram abordar formalmente os crimes cibernéticos e proporcionar competências processuais ao lidar com provas eletrônicas.

O Marco Civil da Internet (Lei n° 12.965/2014) foi desenvolvido mediante um processo de consulta com múltiplos interessados, a fim de regulamentar o uso da Internet no Brasil, estabelecendo princípios, garantias, direitos e deveres para os usuários da Internet.

Na fase das análises, em março de 2018 e março de 2019, o Brasil não dispunha de uma lei específica de proteção de dados ou de privacidade, porém se baseava em várias disposições estabelecidas na Constituição Federal,[18] no Código Penal Brasileiro,[19] no Código de Proteção ao Consumidor[20] e no Marco Civil da Internet para a proteção da privacidade na Internet.

Uma legislação abrangente para a proteção de crianças on-line foi aprovada e aplicada. O Artigo 241-D do Estatuto da Criança e do Adolescente (ECA) define o aliciamento on-line e estabelece uma pena de um a três anos de prisão.[21] Alguns participantes criticaram essa pena, por eles qualificada como muito branda, e manifestaram preocupação com a falta de legislação comparável para criminalizar o assédio virtual, o envio de mensagem sexual e o acesso a imagens de pornografia infantil ou o download dessas imagens.

Atualmente, o Brasil também carece de legislação que considere expressamente as ameaças cibernéticas à propriedade intelectual (PI). Uma exceção é a Lei de Direitos Autorais (Lei n° 9.610/1998),[22] que garante a proteção de qualquer tipo de produto intelectual, independentemente de ter sido registrado ou publicado.[23]

Em dezembro de 2019, o Brasil iniciou o processo de adesão à Convenção de Budapeste, como observador.[24]

A autoridade reguladora para os crimes cibernéticos é o Ministério da Justiça e Segurança Pública.[25] De acordo com o Artigo 10, Item V, da Lei n°. 13.844/2019, cabe ao Gabinete de Segurança Institucional da Presidência da República a responsabilidade por outras questões de segurança cibernética.[26]

A Unidade de Combate a Crimes Cibernéticos da Polícia Federal (URCC), sediada em Brasília, é o principal agente de cumprimento da lei encarregado de combater o crime cibernético e, portanto, desempenha um papel operacional fundamental na perseguição dos criminosos cibernéticos, tanto dentro como fora das fronteiras do Brasil.[27]

Com base em entrevistas de acompanhamento, a competência dos promotores e juízes para considerar casos de crimes cibernéticos e casos que envolvam prova digital foi considerada pelos participantes demasiadamente ad hoc e não institucionalizada. Por exemplo, não há tribunais especiais para lidar com casos de crime cibernético, nem treinamento especializado para juízes sobre esse crime. Contudo, os juízes participam do treinamento realizado para promotores federais.

As autoridades no Brasil reconheceram a necessidade de melhorar os mecanismos informais e formais de cooperação, em âmbito tanto interno como transfronteiriço, mas esses mecanismos continuam sendo ad hoc. Em especial, os entrevistados disseram que a cooperação na luta contra o crime cibernético é uma área com muitas dificuldades, sobretudo no plano internacional.

Entre os diversos canais de cooperação internacional disponíveis, a INTERPOL, a Ameripol e a Europol foram descritas como os mais importantes para promover a cooperação transfronteiriça e o intercâmbio de informações.

Normas, organizações e tecnologias

A elaboração, adoção e auditoria das normas de segurança cibernética variam significativamente entre os setores público e privado. No que diz respeito do setor público, existem regras estritas que foram convertidas em normas desde 2001 e que se aplicam à Administração Federal. Um sistema de auditoria foi implementado e todos os órgãos federais são obrigados a designar uma unidade para realizar a auditoria. Além disso, existe um escritório de controle geral encarregado de elaborar normas e monitorar o progresso de todos os departamentos na implementação dessas normas. Quanto ao setor privado, os participantes disseram que a taxa de adoção varia entre setores, sendo as empresas financeiras e de comunicação eletrônica as pioneiras nessa área. Alguns setores, como o das comunicações eletrônicas e finanças, têm alguns requisitos obrigatórios de segurança; contudo, na maioria dos casos, a força motriz para a adesão às normas são a demanda do mercado e as necessidades comerciais. A ISO 27001 é a estrutura mais frequentemente adotada, sendo também considerada a estrutura de segurança cibernética do Instituto Nacional de Normas e Tecnologia (NIST). Com foco nas normas de desenvolvimento e aquisição de software, diretrizes específicas foram implementadas para o setor público, mas não é claro em que medida essas diretrizes se relacionam à segurança cibernética. Os participantes reconheceram a necessidade de que uma autoridade de segurança estabeleça normas em todos os setores (não apenas na Administração Federal) e promova a adesão a essas normas.

Os participantes da análise sugeriram que a infraestrutura da Internet no Brasil é muito resiliente. No Brasil, os provedores de serviços de Internet públicos e privados (ISPs) são muitos, com diferentes graus de qualidade, serviços e preços. Existem regulamentações impostas pela Associação Brasileira de Internet (Abranet), mas não foi possível entrevistar pessoas do setor de telecomunicações em nossa análise. Segundo nossa pesquisa documental, existem mais de 25 nodos de interconexão da Internet (IXPs), que são mantidos por um projeto abrangente chamado IX.br. O número de IXPs garante um ambiente atraente de inovação e conectividade com a Internet, aumentando, ao mesmo tempo, a resiliência da infraestrutura da Internet.

A qualidade do software varia significativamente no setor público, dependendo de as organizações fazerem ou não parte da Administração Federal. Há um estoque de software seguro para a Administração Federal, e as redes são monitoradas em busca de malware. A aplicação de patches em software desatualizado é automática, e Indicadores de Desempenho Chave (KPIs) foram implementados para avaliar a eficácia dos mecanismos de aplicação de patches. Os governos estaduais não dispõem de um estoque de software seguro, e a aplicação de patches não é implementada consistentemente. No

tocante ao setor privado, a qualidade do software depende do tamanho da organização, sendo as mais maduras as corporações nos setores de finanças e telecomunicações.

A adoção de controles técnicos de segurança no Brasil varia entre os setores e organizações. Os participantes sugeriram que a adoção e implementação de controles em órgãos governamentais é muito avançada na Administração Federal, mas elementar e incoerentemente promovida nos governos estaduais, devido a restrições financeiras, recursos humanos limitados e falta de estrutura organizacional apropriada. Há uma estratégia para a implementação de controles no Governo Federal, que inclui um modelo detalhado para avaliar a maturidade das organizações, mas o Governo Federal não controla os estados e municípios. No setor privado, entende-se que as organizações bem estabelecidas adotam controles técnicos adequados adaptados às suas redes. Os controles de segmentação de redes e ferramentas de monitoramento são evidentes nesse setor, assim como o uso de Sistemas de Detecção de Invasão (IDS) e outras ferramentas de Gerenciamento de Eventos e Informações de Segurança (SIEM). Organizações específicas criaram uma CERT para monitorar suas redes. É particularmente preocupante, no entanto, que as organizações do setor privado não sejam obrigadas a partilhar informações sobre incidentes com o CERT.br e não possam receber inteligência de ameaças.

O Brasil estabeleceu normas técnicas para o credenciamento de autoridades de certificação (CAs) e autoridades de registro (RAs), e realiza auditorias para a Root CA e seus prestadores de serviços. Os participantes salientaram que existem requisitos muito rigorosos tanto para as Root CAs (Nível 5) como para as CAs que lidam com a Infraestrutura de Chaves Públicas (PKI). No Governo Federal, a Agência Brasileira de Inteligência (ABIN) é o centro de credenciamento para criptografia e dispõe regras específicas sobre como as informações classificadas devem ser transmitidas, como é usado o protocolo de comunicação de informações sensíveis (PGP) e como os dados devem ser armazenados e processados. No tocante ao setor privado, foram feitas observações semelhantes. A criptografia é considerada principalmente para sistemas críticos, tanto para dados em trânsito quanto para dados em repouso. Não conseguimos obter uma imagem clara quanto à oferta, pelos provedores de serviços de Internet, de conexões Secure Shell (SSH) entre servidores e navegadores.

Existe uma ampla gama de produtos de software de segurança cibernética desenvolvidos internamente pelo setor público, bem como por empresas privadas, que chegam a exportar essas tecnologias para outros países. Do mesmo modo, a dependência de tecnologias estrangeiras de segurança cibernética é menor. Segundo os participantes, a prevalência de hackers no Brasil tem resultado em uma demanda cada vez maior de produtos de segurança cibernética. Para atender a essa demanda, as empresas locais desenvolvem e oferecem soluções e software nacionais de segurança. Um fator importante para o mercado interno estabelecido é a falta de legislação para proteger a PI; a ameaça de roubo de PI faz com que as organizações estrangeiras relutem em vender suas soluções de software. O mercado de seguro cibernético oferece uma gama de apólices, cuja demanda, por parte das organizações, vem aumentando. Em geral, as apólices detalham as situações em que o seguro é válido e, em uma nota positiva, especificam as políticas às quais as organizações devem aderir para que possam ser seguradas.

Uma estrutura de divulgação de vulnerabilidade foi implantada para o Governo Federal. As organizações estabeleceram processos formais para divulgação automática de informações, e o CERT.br recebe essas informações e prepara extensos relatórios sobre como fazer frente a incidentes. Por outro lado, as organizações privadas estão excluídas do intercâmbio de inteligência de ameaças do Governo. Além disso, não são obrigadas a relatar incidentes, de modo que tendem a ocultar os problemas por elas detectados. Considerando o fato de o Brasil ter começado a privatizar partes críticas da infraestrutura nacional, os participantes instaram o Governo a reconhecer o papel relevante das organizações privadas na estratégia nacional de segurança cibernética e a conceder-lhes acesso à inteligência de ameaças. Há vários meios para que os cidadãos relatem incidentes, por meio das polícias dos estados ou de páginas eletrônicas. Quanto ao setor financeiro, os bancos, em particular, oferecem canais exclusivos de comunicação para que os clientes denunciem fraudes on-line.

Reflexões adicionais

Esta foi a vigésima terceira análise de país apoiada diretamente pelo Centro Global de Capacidade de Segurança Cibernética (GCSCC), de Oxford. Essa análise visa a colaborar com o Governo do Brasil no conhecimento da amplitude e da profundidade da capacidade de segurança cibernética do país. Este relatório sugere uma série de passos específicos mediante os quais a capacidade de segurança cibernética do Brasil pode atingir maiores níveis de maturidade, podendo, desse modo, contribuir para fomentar a colaboração entre organizações privadas e estatais que fazem parte da IC.

Revisão da Capacidade de Cibersegurança

República Federativa do Brasil

INTRODUÇÃO

A convite da OEA, o GCSCC procedeu a uma análise da capacidade de segurança cibernética do Brasil. Essa análise teve por objetivo permitir ao Brasil determinar áreas de capacidade nas quais o Governo pudesse investir estrategicamente, com o intuito de melhorar sua posição nacional em segurança cibernética.

Em 19 e 20 de março de 2018, as partes interessadas dos diferentes setores participaram de um processo de consulta de três dias. Entrevistas virtuais também foram conduzidas em uma fase posterior. Os dados coletados em 2018 foram validados mediante um processo similar em março de 2019.

- **Entidades do setor público**
  - Gabinete de Segurança Institucional da Presidência (GSI)
  - Centro de Treinamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov)
  - Ministério da Defesa
  - Agência Brasileira de Inteligência (ABIN)
  - Agência Nacional de Telecomunicações (ANATEL)
  - Ministério dos Transportes, Portos e Aviação Civil
  - Ministério da Fazenda
  - Serviço Federal de Processamento de Dados (SERPRO)
  - Empresa de Tecnologia e Informações da Previdência Social (DATAPREV)
  - Centro de Defesa Cibernética (CDCiber)
  - Marinha do Brasil
  - Rede Nacional de Ensino e Pesquisa (RNP)
- **Setor da justiça penal**
  - Polícia Federal
  - Ministério Público
- **Setor financeiro**
  - Caixa Econômica Federal
  - Proprietários de infraestrutura crítica
  - Confederação Nacional da Indústria (CNI)
  - Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação

- **Setor Privado**

  - Opice Blum Advogados Associados (escritório de advocacia)

  - Bialer Falsetti Associados (escritório de advocacia)

  - IBM

  - Concordia Public Affairs Strategies

  - Apura Cybersecurity Intelligence

Dimensões da Capacidade de Segurança Cibernética

As consultas foram baseadas no Modelo de Maturidade da Capacidade (CMM) do GCSCC,[28] que é composto de cinco dimensões distintas de capacidade de segurança cibernética.

Cada dimensão consiste em um conjunto de fatores que descrevem e definem o que significa possuir capacidade de segurança cibernética na respectiva dimensão. A tabela abaixo mostra as cinco dimensões, juntamente com os fatores que as compõem.

Dimensão 1 **Política e estratégia de segurança cibernética**	**D1.1** Estratégia Nacional de Segurança Cibernética **D 1.2** Resposta a incidentes **D 1.3** Proteção da infraestrutura crítica (IC) **D 1.4** Gerenciamento de crises **D 1.5** Defesa cibernética **D 1.6** Redundância nas comunicações

Dimensão 2 **Cultura cibernética e sociedade**	**D2.1** Mentalidade de segurança cibernética **D 2.2** Confiança na Internet **D 2.3** Entendimento do usuário sobre a proteção de informações pessoais on-line **D 2.4** Mecanismos de informação **D 2.5** Mídia e mídia social
Dimensão 3 **Educação, treinamento e competências em segurança cibernética**	**D3.1** Conscientização **D3.2** Estrutura para a educação **D3.3** Estrutura para a formação profissional
Dimensão 4 **Estruturas jurídicas e regulamentares**	**D4.1** Estruturas jurídicas **D4.2** Sistema de justiça criminal **D4.3** Estruturas formais e informais de cooperação para combater o crime cibernético
Dimensão 5 **Normas, organizações e tecnologias**	**D5.1** Adesão às normas **D 5.2** Resiliência da infraestrutura da Internet **D 5.3** Qualidade do software **D 5.4** Controles técnicos de segurança **D 5.5** Controles criptográficos **D 5.6** Mercado de segurança cibernética **D 5.7** Divulgação responsável

Estágio de Maturidade da Capacidade de Segurança Cibernética

Cada dimensão é composta de uma série de fatores, que descrevem o que significa possuir capacidade de segurança cibernética. Cada fator apresenta uma série de aspectos e para cada aspecto existem indicadores, que descrevem etapas e ações que, assim que observadas, definem o estágio de maturidade desse aspecto específico. Existem cinco estágios de maturidade, do estágio inicial ao estágio dinâmico. O estágio inicial implica uma abordagem ad hoc da capacidade, enquanto o estágio dinâmico traduz uma abordagem estratégica e a capacidade de se adaptar ou mudar dinamicamente em relação às questões ambientais. Os cinco estágios são definidos a seguir.

- **Inicio:** nesse estágio não existe maturidade cibernética, ou ela é de natureza embrionária. Talvez haja discussões iniciais sobre a construção de capacidade de segurança cibernética, mas nenhuma ação concreta foi tomada. Não há evidência observável de capacidade de segurança cibernética nesse estágio.

- **Formativo:** alguns aspectos começaram a crescer e a ser formulados, mas podem ser ad hoc, desorganizados, mal definidos – ou simplesmente novos. No entanto, evidências desses aspecto podem ser claramente demonstradas.

- **Estabelecido:** os indicadores do aspecto foram implantados e funcionam. Entretanto, falta uma consideração bem pensada sobre a relativa alocação de recursos. Poucas decisões compensatórias foram tomadas sobre o investimento relativo a esse aspecto, mas o aspecto é funcional e definido.

- **Estratégico:** nesse estágio, houve escolhas sobre que indicadores do aspecto são importantes, e quais são menos importantes para a organização ou Estado em particular. O aspecto estratégico reflete o fato de que essas escolhas foram condicionadas às circunstâncias particulares do Estado ou organização.

- **Dinâmico:** nesse estágio, existem mecanismos claros em vigor para alterar a estratégia, dependendo das circunstâncias predominantes, tais como a sofisticação tecnológica do ambiente de ameaça, um conflito global ou uma mudança significativa em uma área de preocupação (por exemplo, crime cibernético ou privacidade). As organizações dinâmicas desenvolveram métodos para mudar estratégias em andamento. A rápida tomada de decisões, a realocação de recursos e o monitoramento constante do ambiente em mudança são características desse estágio.

A atribuição das fases de maturidade baseia-se nas evidências coletadas, incluindo a visão geral ou a média das contas apresentadas pelas partes interessadas, a pesquisa documental realizada e o julgamento profissional do pessoal de pesquisa do GCSCC. Usando a metodologia do GCSCC, conforme se descreve abaixo, este relatório apresenta os resultados da análise da capacidade de segurança cibernética do Brasil e, na conclusão, recomendações sobre os próximos passos que podem ser considerados para melhorar a capacidade de segurança cibernética do país.

Metodologia - Medição da Maturidade

No decorrer da análise no país, dimensões específicas são discutidas com grupos relevantes de partes interessadas. Espera-se que cada grupo de interessados atenda a uma ou duas dimensões do CMM, dependendo de sua especialização. Por exemplo, o setor acadêmico, a sociedade civil e os grupos de governança da Internet seriam todos convidados a discutir tanto a Dimensão 2 como a Dimensão 3 do CMM.

Com o intuito de determinar o nível de maturidade, cada aspecto reúne um conjunto de indicadores correspondentes aos cinco estágios de maturidade. Para que as partes interessadas apresentem evidências sobre quantos indicadores foram implementados por uma nação, e determinem o nível de maturidade de cada aspecto do modelo, um método consensual é usado para conduzir os debates nas sessões. Nos grupos de discussão, os pesquisadores utilizam perguntas semiestruturadas para orientar as discussões em torno dos indicadores. No decorrer desses debates, as partes interessadas devem ser capazes de apresentar ou apontar provas a respeito da implementação de indicadores, com vistas a minimizar as respostas subjetivas. Caso não seja possível apresentar provas para todos os indicadores em um só estágio, essa nação, por conseguinte, ainda não atingiu esse estágio de maturidade.

O CMM utiliza uma metodologia de grupos de discussão, pois oferece um conjunto de dados mais rico em comparação com outras abordagens qualitativas.[29] Assim como as entrevistas, os grupos de discussão são uma metodologia interativa com a vantagem de que, durante o processo de coleta de dados e informações, podem surgir diversos pontos de vista e conceitos. É parte fundamental do método que, em vez de fazer perguntas a cada entrevistado, os pesquisadores promovam um debate entre os participantes, encorajando-os a adotar, defender ou criticar diferentes perspectivas.[30] É nessa interação e tensão que reside a vantagem sobre outras metodologias, propiciando que os participantes cheguem a consenso e melhor compreendam as práticas e a capacidade de segurança cibernética a serem alcançadas.[31]

Com o consentimento prévio dos participantes, todas as sessões são gravadas e transcritas. A análise de conteúdo é uma metodologia sistemática de pesquisa utilizada para analisar dados qualitativos e é aplicada aos dados gerados pelos grupos de discussão.[32] A análise de conteúdo visa a projetar "inferências replicáveis e válidas dos textos para o contexto de seu uso".[33]

As abordagens para a análise de conteúdo são três. A primeira é a abordagem indutiva, baseada na "codificação aberta", o que significa que as categorias ou temas são criados livremente pelo pesquisador. Na codificação aberta, os títulos e notas são escritos nas transcrições enquanto são lidas, e diferentes categorias são criadas para incluir notas semelhantes que capturam o mesmo aspecto do fenômeno em estudo.[34] O processo é repetido e as notas e títulos são lidos novamente. O próximo passo é classificar as categorias em grupos. O objetivo é fundir possíveis categorias que compartilham o mesmo significado.[35] Dey explica que esse processo categoriza os dados como "dados associados".[36]

A segunda abordagem é a "análise dedutiva do conteúdo", que requer a existência prévia de uma teoria para alicerçar o processo de classificação. Essa abordagem é mais estruturada do que o método indutivo, e a codificação inicial é moldada pelas principais características e variáveis da estrutura teórica.

No processo de codificação, trechos são atribuídos a categorias e os resultados são definidos pela teoria ou por pesquisas anteriores. Porém, pode haver categorias novas que contradigam ou enriqueçam uma teoria específica. Portanto, se as abordagens dedutivas forem seguidas estritamente, essas categorias novas que oferecem uma perspectiva refinada podem ser ignoradas. É por isso que a equipe de pesquisa do GCSCC escolhe uma abordagem mista na análise de nossos dados, que é uma mistura das abordagens dedutiva e indutiva.

Após a realização de uma análise no país, os dados coletados durante as consultas com as partes interessadas e as notas tomadas nas sessões são usados para definir os estágios de maturidade para cada fator do CMM. O GCSCC adota uma abordagem mista para analisar os dados do grupo de discussão e usa os indicadores do CMM como critério para uma análise dedutiva. Os trechos que não se encaixam em nenhum tema são analisados mais detalhadamente na busca de questões adicionais que os participantes possam ter suscitado ou para adaptar nossas recomendações.

Em vários casos, durante a elaboração de um relatório, é necessária uma pesquisa documental visando validar e verificar os resultados. Por exemplo, as partes interessadas podem nem sempre estar cientes dos desenvolvimentos recentes em seu país, como, por exemplo, se o país assinou uma convenção sobre proteção de dados pessoais. As fontes que podem prestar mais informações podem ser os sites oficiais do Governo ou dos ministérios, relatórios anuais de organizações internacionais, sites de universidades etc.

Para cada dimensão, são apresentadas recomendações para os próximos passos a serem dados para que o país aumente sua capacidade. Caso a capacidade de um país para um determinado aspecto esteja em uma fase de formação de maturidade, então, examinando o CMM, os indicadores que ajudarão o país a passar para o próximo estágio podem ser facilmente identificados. As recomendações também podem decorrer de discussões com as partes interessadas e entre elas.

Usando a metodologia CMM do GCSCC, este relatório apresenta os resultados da análise da capacidade de segurança cibernética do Brasil, realizada em março de 2018 e março de 2019. Os dados coletados em 2019 e 2020 são marcados em azul. Cada seção do relatório é encerrada com recomendações sobre os próximos passos que podem ser considerados para melhorar a capacidade de segurança cibernética no país. As recomendações foram revisadas e levemente editadas, levando em conta os resultados do seminário de validação de 2019.

Revisão da Capacidade de Cibersegurança

República Federativa do Brasil

CONTEXTO DA SEGURANÇA CIBERNÉTICA NO BRASIL

A porcentagem de indivíduos que utilizam a Internet no Brasil cresceu rapidamente na última década. Especificamente, em 2017, 67% da população usava a Internet.[37]

Esse aumento levou o Brasil à sexagésima sexta posição no ranking do Índice Global de Desenvolvimento das TIC, da União Internacional de Telecomunicações (UIT).[38] Além disso, de acordo com o relatório do Fórum Econômico Mundial[39] (2017-2018), o Brasil melhorou muito no desenvolvimento da infraestrutura de TIC. Após dois anos de queda no crescimento do PIB e piora das condições macroeconômicas, o Brasil melhorou ligeiramente este ano, controlando de novo a inflação e os déficits do governo. O maior progresso do Brasil surge no pilar da inovação, com recuperação em muitos dos indicadores, o que mostra maior capacidade de inovação, maior colaboração indústria-universidade-empresa, maior qualidade de pesquisa e cientistas e engenheiros mais bem treinados.

A economia do Brasil é uma das maiores da América Latina, representando 40% do PIB da região.[40] De acordo com o relatório "Visão Geral do Mercado Digital: Brasil" do Governo do Reino Unido,[41] a segurança cibernética vem se tornando um dos maiores mercados no domínio das TIC, em virtude da escalada das ameaças cibernéticas no país.

Os investimentos em banda larga são importantes, e buscam prover cobertura de banda larga em 95% dos municípios até 2018. Oportunidades de 4,5G e 5G com empresas de telecomunicações também existem.

Na última década, o Brasil testemunhou um grande aumento no acesso à Internet e a assinaturas de telefonia móvel, com mais da metade de sua população de 200 milhões de pessoas on-line em 2018. Uma série de fatores relacionados às melhorias no desenvolvimento social e econômico do Brasil impulsionam essas tendências. Não surpreende que o empoderamento digital também seja acompanhado de desafios adicionais, que vão do protesto em massa ao crime organizado. A natureza complexa e multifacetada da "ameaça cibernética" - e a forma como ela é interpretada no Brasil - tem desempenhado um papel significativo na formação da governança cibernética e da arquitetura de segurança cibernética do país.[42]

RELATÓRIO DA ANÁLISE

Visão geral

Nesta seção, figura uma representação geral da capacidade de segurança cibernética no Brasil. A Figura 2, abaixo, apresenta as estimativas de maturidade em cada dimensão. Cada dimensão representa um quinto do gráfico, com os cinco estágios de maturidade para cada fator estendendo-se a partir do centro do gráfico; o "inicial" é o mais próximo do centro do gráfico e o "dinâmico" está localizado no perímetro.

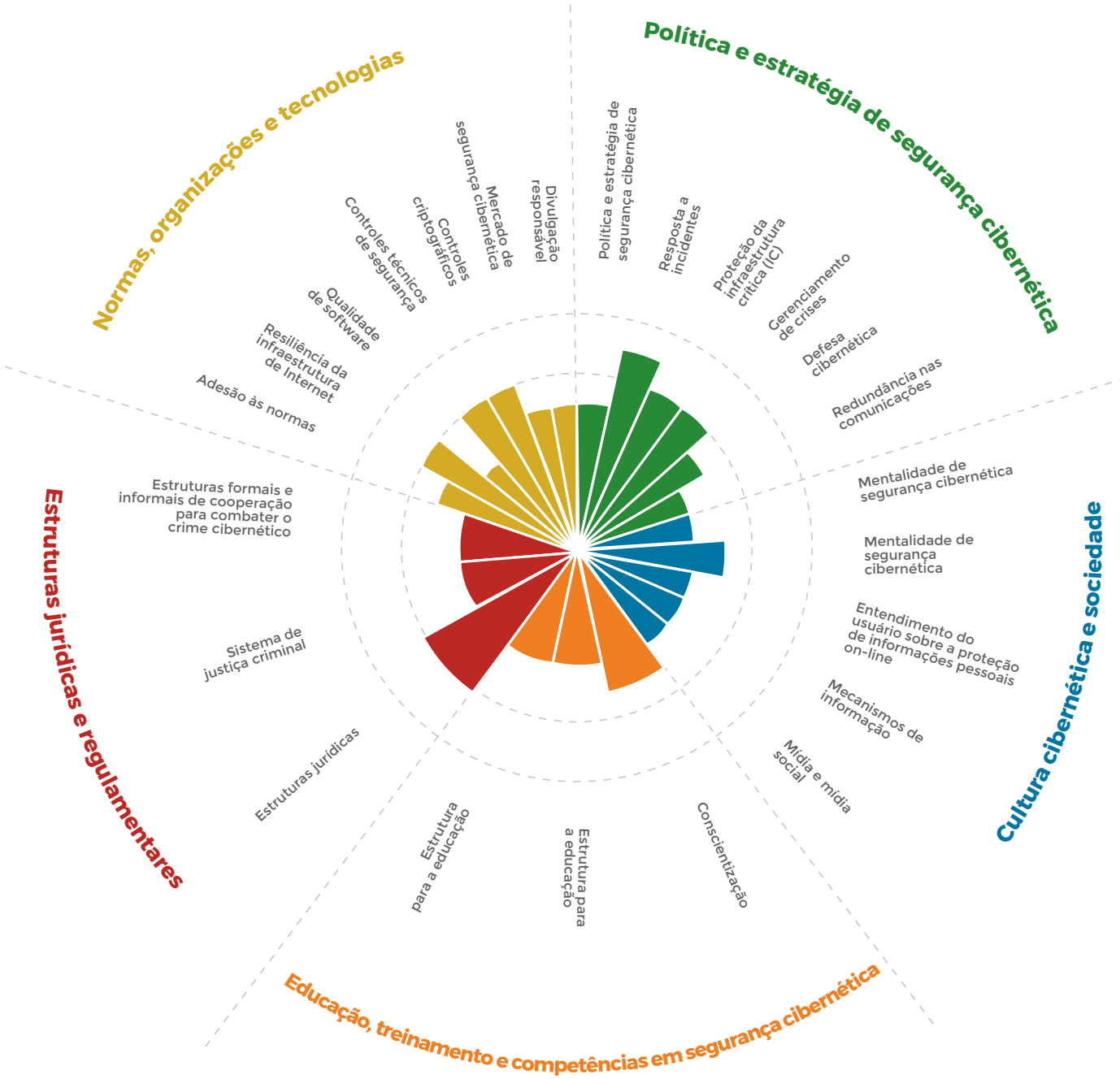


***Figura 2:** Representação geral da capacidade de segurança cibernética no Brasil*

Dimensão 1

POLÍTICA E ESTRATÉGIA DE SEGURANÇA CIBERNÉTICA

Os fatores da Dimensão 1 medem a capacidade do Brasil de desenvolver e proporcionar políticas e estratégias de segurança cibernética e aumentar a resiliência de segurança cibernética, por meio de melhorias na resposta a incidentes, no gerenciamento de crises, na redundância e na capacidade de proteção da infraestrutura crítica. A dimensão também inclui considerações para alerta precoce, dissuasão, defesa e recuperação, e considera uma política eficaz no avanço da capacidade nacional de defesa cibernética e de resiliência, propiciando o acesso efetivo ao ciberespaço, que é cada vez mais vital para o governo, as empresas internacionais e a sociedade em geral.

D 1.1 - Estratégia Nacional de Segurança Cibernética

A estratégia de segurança cibernética é essencial para a incorporação de uma agenda de segurança cibernética a todo o governo, uma vez que ajuda a priorizar a segurança cibernética como importante área de política, determina responsabilidades e mandatos dos principais atores governamentais e não governamentais de segurança cibernética e direciona a alocação de recursos para as questões e prioridades de segurança cibernética novas e existentes

Estágio:Formativo – Estabelecido

Os processos de apoio ao desenvolvimento de uma estratégia de segurança cibernética foram iniciados no Brasil em 2010 com o "Plano Brasil 2022",[43] documento que descreve o plano estratégico do Brasil até 2022. A digitalização da economia, a liberdade de expressão na Internet e a proteção do direito de acesso público à Internet foram objetivos fundamentais do plano, cujo sucesso dependia do desenvolvimento de uma estratégia de segurança cibernética. A primeira tentativa dessa estratégia foi o Livro Verde sobre Segurança Cibernética no Brasil,[44] documento aprovado pelo Governo, que ofereceu orientações ao Estado sobre questões relacionadas à segurança cibernética. A necessidade de uma estratégia de segurança cibernética também foi destacada na Estratégia Nacional de Defesa, do Ministério da Defesa,[45] onde o ciberespaço é reconhecido como elemento fundamental da função militar brasileira. Apesar da importância do ciberespaço, a estratégia de defesa não se deteve em como integrar a segurança cibernética a uma estratégia nacional. O ponto culminante dessas duas iniciativas foi a Estratégia,[46] uma instância mais ampla de planejamento estratégico para o Governo do Brasil. Apesar de todos esses esforços, na ocasião da análise, em março de 2018, não havia documento oficial nacional algum de segurança cibernética aprovado pelo Congresso Nacional, que detalhasse como estabelecer a coordenação entre os principais atores governamentais e não governamentais da segurança cibernética.

A falta de colaboração entre as instituições governamentais e o setor privado e a "fragmentação das respostas" foram potencialmente consideradas na Estratégia (2015- 2018).[46] O objetivo da Estratégia era propor as diretrizes estratégicas para a segurança da informação e das comunicações e coordenar esses esforços entre os vários atores engajados, com o intuito de mitigar os riscos a que as organizações e a sociedade estão expostas.[47] A Estratégia estabeleceu os princípios fundamentais a serem seguidos, objetivos estratégicos claros (entre outros, educação do pessoal e conscientização sobre questões de segurança cibernética, institucionalização de políticas de segurança cibernética, pesquisa e inovação em tecnologias de segurança cibernética e fortes controles de segurança para as partes interessadas na infraestrutura crítica), ações para alcançar esses objetivos e as instituições

incumbidas da execução dessas ações em prazos predeterminados. A estratégia focalizou a Administração Pública Federal do Brasil, que abrange 29 Ministérios, 6.000 órgãos públicos, mais de 1.000.000 de funcionários, 320 redes digitais e 12.000.000 de páginas eletrônicas.[48] Os críticos da estratégia destacaram a ausência de uma autoridade central para implementar essa abordagem tão sistemática e de múltiplas partes interessadas.[49]

Por ocasião da análise, em março de 2018, os participantes explicaram que a comunidade cibernética, subordinada ao Ministério da Defesa, era a entidade responsável pela segurança cibernética na Administração Pública Federal, razão pela qual um grupo interministerial interno de mais de 15 ministérios, com a assistência de um comitê técnico composto por membros do Gabinete de Segurança Institucional, foi incumbido de redigir a Estratégia. O documento foi enviado a 98 organizações, incluindo membros do meio acadêmico, das confederações nacionais, das entidades do setor financeiro, das partes interessadas da IC, das empresas de engenharia de software e dos ISPs privados. De acordo com os participantes, mais de 200 reuniões e eventos foram realizados até o momento para aperfeiçoar ainda mais o documento antes de encaminhá-lo ao Parlamento para aprovação. Vale notar que em nossa análise não foi possível comprovar a participação de organizações privadas com pessoas que trabalham no setor privado.

Os críticos, entretanto, enfatizaram a ausência de organizações da sociedade civil, de atores da Internet e do público em geral nesse grupo de diversas partes interessadas.49 No decorrer de nossa análise, os participantes destacaram ainda mais a ausência de organizações do setor privado que deveriam ser consideradas parte da IC, mas que, no momento, são negligenciadas pela Administração Pública Federal. Os rápidos desdobramentos em governança eletrônica, cidades inteligentes e soluções inovadoras em TIC no Brasil criaram as bases para discussões frutíferas e colaboração entre uma ampla gama de interessados, incluindo organizações de direitos civis, o setor privado e o governo. Hoje, o debate sobre questões relacionadas à segurança cibernética envolve funcionários governamentais, as forças armadas, instituições de aplicação da lei, um grupo de instituições privadas, ICs públicas e um pequeno número de instituições acadêmicas. Os participantes sugeriram que a ampliação do leque de atores que participam da formação da estratégia nacional de segurança cibernética, incluindo a sociedade civil e organizações privadas, assegurará à comunidade que a estratégia oferece uma abordagem equilibrada da segurança cibernética e ajudará a aliviar o medo de não incluir e proteger os direitos humanos e civis.

No que diz respeito à organização do programa de segurança cibernética, os participantes expressaram sua preferência por um modelo descentralizado, em que os setores comerciais sejam supervisionados pelas agências reguladoras existentes, com uma nova agência nacional criada para coordenar os esforços. Os participantes sugeriram que o modelo proposto é inspirado na abordagem da UE, onde a Agência Europeia para a Segurança das Redes e da Informação (ENISA) desempenha o papel central de unificar e coordenar os esforços em todos os países. A opinião dos participantes levou em conta a estrutura atual do Brasil, onde existem vários estados autônomos, mas a Administração Pública Federal é responsável pelos processos críticos em todos os estados. Os participantes salientaram que a dimensão do país dificulta a coordenação entre os estados e que a chave para uma estratégia de sucesso é aumentar a colaboração entre todos os atores públicos, federais e privados relevantes, sem centralizar responsabilidades e iniciativas.

Finalmente, a estratégia nacional de segurança cibernética dispõe uma estrutura genérica de ações críticas para implementar os principais objetivos. No entanto, como os participantes explicaram, essa estrutura confere às autoridades o mandato para projetar ações e fixar os prazos para os objetivos principais. Isso se deve ao fato de que a estratégia em si deve ser concisa

e ser votada pelo Congresso, e de que não será atualizada regularmente. Uma estratégia mais elaborada, com ações específicas, exigiria mais articulação política.

Resultados do processo de validação realizado em março de 2019

Durante as entrevistas de validação do grupo de discussão, conduzidas em março de 2019, os participantes informaram os pesquisadores sobre a Política Nacional de Segurança da Informação publicada em forma de Decreto Presidencial (No. 9.637), em dezembro de 2018.[50] A política serviu de base para a Estratégia Nacional de Segurança Cibernética, publicada em 2020.[51] O projeto da Estratégia Nacional de Segurança Cibernética foi elaborado com base na Política Nacional de Segurança da Informação. Essa política prometia um processo de elaboração[52] inclusivo com a participação de grande número de interessados; [53] o setor privado já foi, aparentemente, consultado.

Informações prestadas pelo Governo em 2020

Após as entrevistas de validação do grupo de discussão, realizadas em março de 2019, a Estratégia Nacional de Segurança Cibernética (Decreto Federal n° 10.222) foi finalmente adotada, em fevereiro de 2020.[54] O Decreto "estabelece um modelo centralizado de governança no âmbito nacional, para [...] promover a coordenação dos diversos atores relacionados com a segurança cibernética; [...] criar um conselho nacional de segurança cibernética"; [...] e "estabelecer rotina de verificações de conformidade em segurança cibernética, internamente nos órgãos públicos e nas entidades privadas".[55] Além disso, dispõe-se a notificação de incidentes cibernéticos contra a infraestrutura crítica ao Centro de Treinamento e Resposta a Incidentes Cibernéticos de Governo.[56] De acordo com fontes governamentais, a Estratégia focaliza dez ações estratégicas que devem orientar a Administração Pública Federal na formulação de suas próprias ações quanto à segurança cibernética. Os novos desdobramentos (desde 2018) com relação à estratégia de segurança cibernética do Brasil apontam para um estágio de maturidade "formativo a estabelecido".

Da mesma forma, foi esclarecido que, de acordo com o Artigo 10 da Lei n° 13.844 (junho de 2019), a coordenação e supervisão da atividade de segurança da informação no âmbito da Administração Pública Federal cabe ao Gabinete de Segurança Institucional da Presidência da República,[57] ao passo que as ações de defesa cibernética estarão sujeitas ao Ministério da Defesa.

D 1.2 - Resposta a Incidentes

Esse fator aborda a capacidade do Governo de identificar e determinar sistematicamente as características dos incidentes em âmbito nacional e analisa a capacidade do Governo de organizar, coordenar e operacionalizar a resposta aos incidentes.

Estágio: Estabelecido – Estratégico

Há um grande número de Equipes de Resposta a Incidentes de Segurança Cibernética (CSIRTs), de entidades governamentais a instituições privadas e acadêmicas. A Figura 3: Número de CERTs no Brasil ilustra a distribuição geográfica das CERTs no Brasil. Dependendo do papel de uma CERT, essas entidades podem estar envolvidas exclusivamente na gestão da segurança dos sistemas, fazendo cumprir as diretrizes de segurança cibernética ou sendo responsáveis pela coordenação de esforços entre as autoridades nacionais e locais. As iniciativas de serviços de Internet são coordenadas pelo CGI.br e seu órgão executivo, o NIC.br. Essas duas autoridades supervisionam as operações do CERT.br nacional, que é certificado pelo FIRST e é responsável pelo gerenciamento de relatórios de incidentes para o setor privado. Outra instituição, o CTIR Gov, também age como CSIRT em âmbito nacional, oferecendo resposta a incidentes para a Administração Pública Federal, enquanto outras CERTs se dedicam a setores específicos e a interessados da IC. Finalmente, existe um CERT militar que protege as redes militares.

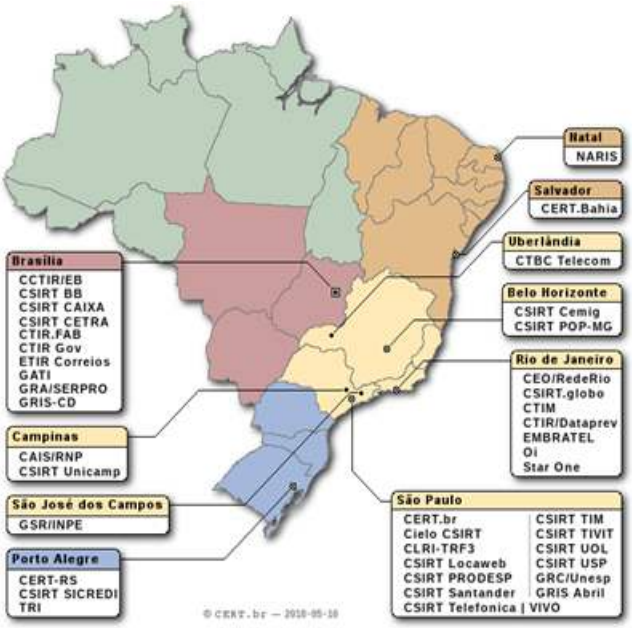


Figura 3: *Número de CERTs no Brasil*[58]

Todas essas instituições têm diretrizes e papéis claros no tocante à resposta a incidentes, e sua maturidade nesse fator se encontra no nível estabelecido, com a presença de determinados indicadores do nível estratégico. O CERT.br mantém o registro de incidentes nacionais e publica anualmente dados estatísticos de ameaças e incidentes. Da mesma forma, o CTIR Gov executa essas mesmas atividades para a Administração Pública Federal, dispondo também alertas e recomendações em seu site (https://www.ctir.gov.br/). Os esquemas de classificação usados no tratamento de incidentes são constantemente atualizados para capturar novos ataques e partilhar mais eficientemente o conhecimento adquirido com esses ataques. Além disso, todos os incidentes são automaticamente incorporados a um banco de dados de suporte de software de

inteligência empresarial (BI). Como sugeriram os participantes, esse software utiliza visualizações para permitir que os altos funcionários tenham acesso às informações relevantes "com apenas um clique". Os participantes mencionaram que quando acontece um incidente nacional, tanto o setor público quanto o privado estão envolvidos nos procedimentos de resposta. A ABIN, que é a agência de inteligência, também presta apoio, assim como a Polícia Federal.

Todas as CERTs apresentam relatórios ao CERT.br, por meio dos canais oficiais. Sistemas automatizados que seguem normas internacionais, como o STIX e os Protocolos Semáforos (TLP), garantem o intercâmbio da inteligência de ameaças com as CERTs que colaboram com a CERT nacional. Esses sistemas também facilitam a comunicação com as CERTs internacionais. Contudo, os participantes mencionaram que, por razões burocráticas, o uso do e-mail é preferido para trocas não oficiais de inteligência de ameaças com parceiros internacionais. O CERT.br é membro da comunidade FIRST e frequentemente participa de eventos organizados pela FIRST e pela OEA.
Apesar dos sistemas automatizados implementados, os participantes sugeriram que o tempo de resposta a partir do recebimento da inteligência, da compreensão da informação e da respectiva ação poderia ser melhorado se os funcionários da CERT participassem de eventos e colaborassem mais estreitamente para fomentar a confiança. Os esforços legislativos atuais concentram-se na racionalização do intercâmbio da inteligência de ameaças entre todas as CERTs, uma vez que nem todos os participantes privados da IC têm direito a receber inteligência de ameaças. Como o leque de partes interessadas da IC vem se ampliando e o intercâmbio de informações confiáveis tem se tornado mais complexo, há necessidade de maior participação das instituições de pesquisa. Existem iniciativas que têm por objetivo proporcionar às CERTs melhor conhecimento da situação, com inteligência artificial utilizada por várias ferramentas para oferecer percepções baseadas na correlação de eventos.

Quanto às CERTs públicas, cada uma delas é encarregada de criar uma equipe técnica para lidar com incidentes, além de receber instruções e políticas claras sobre como responder a diferentes situações. Também têm sido estabelecidos códigos de conduta e procedimentos específicos para preservar e armazenar provas. Existem sistemas inovadores para identificar atividades de hacking, buscar conversas na Internet escura, prevenir ataques de páginas eletrônicas e capturar, em tempo real, nas mídias sociais, conteúdos pertinentes a ataques em evolução. Finalmente, dois grandes projetos financiados pelo CERT nacional visam a aumentar a capacidade de detecção de incidentes, correlação de eventos e análise de tendências (um projeto de "honeypots distribuídos"), e obter detalhes da atividade de spam ("SpamPots"). Para as necessidades desses projetos, o CERT.br criou honeypots em mais de dez países, e frequentemente produz relatórios e publicações acadêmicas em que os dados são analisados.

O SERPRO, uma das maiores empresas estatais de serviços de TI no Brasil, opera uma CERT que institucionalizou os procedimentos de resposta a incidentes, com uma equipe responsável pela coordenação em nível de rede, uma equipe encarregada de realizar testes de penetração e outra que projeta o robustecimento da rede. Existem laboratórios de última geração para análise de malware e sistemas para desinfetar redes, para agir proativamente antecipando eventos e prever vulnerabilidades. Além disso, existem processos internos para análise de risco e modelos de maturidade para indicar a eficácia do gerenciamento de um incidente. O SERPRO também mantém uma linha telefônica direta que liga vários órgãos governamentais. Além disso, foram criados um grupo de e-mail para autoridades da administração pública e um grupo de discussão onde os incidentes são analisados. Finalmente, a inteligência de atividades de hacking é reunida por especialistas do SERPRO que se infiltraram em fóruns de hackers em todo o mundo.

No tocante à educação, há uma ampla gama de cursos oferecidos pelas CERTs, bem como uma série de campanhas de conscientização que visam a informar os cidadãos. O CERT.br oferece programas de treinamento profissional certificados pelo CMU CERT, e metodologias propostas pelo FIRST. Há ainda um portal para promover as melhores práticas para os administradores de sistemas[59] e um guia sobre como os usuários da Internet podem se proteger on-line.[60] O SERPRO também oferece seminários de melhores práticas e cursos técnicos para analistas de CERT e realiza eventos semanais para informar os usuários sobre ameaças recentes e notícias falsas.

Resultados do processo de validação realizado em março de 2019

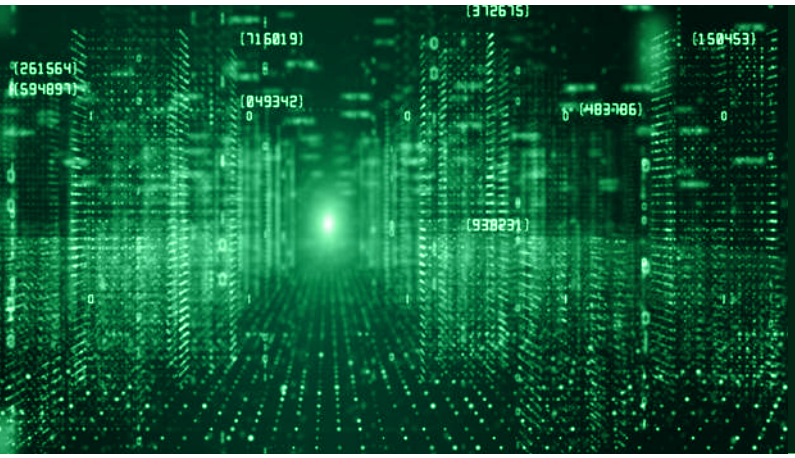
O Brasil optou por uma estrutura descentralizada de capacidade de resposta a incidentes. O papel de coordenação entre as 42 CERTs[61] no Brasil é confiado ao CERT.br,[62] este último responsável também pela coordenação das atividades internacionais de resposta a incidentes.[63]

Além disso, cabe ao CERT.br a responsabilidade de assegurar a cooperação entre os membros da rede nacional de CERTs. Desse modo, o CERT.br auxilia as CERTs recém-criadas a desenvolver sua capacidade de gerenciamento de incidentes, mediante diversas reuniões, treinamentos e exposições em conferências. Também organiza o Fórum Brasileiro de CSIRTs anual e cursos especializados (por exemplo, "Visão geral da criação e gestão de CSIRTs", "Fundamentos do Gerenciamento de Incidentes", "Gerenciamento Avançado de Incidentes para Pessoal Técnico" etc.), tanto no Brasil[64] como no exterior.[65] O envolvimento internacional do CERT.br também inclui sua parceria com o Software Engineering Institute (CMI CERT), da Universidade Carnegie Mellon, e o Grupo de Trabalho Anti-Phishing, além de seu papel de coordenador do projeto SpamPots, coletando e analisando dados sobre o abuso da infraestrutura da Internet por parte de spammers a partir de sensores de honeypot de baixa interação em 11 países.[66]

Informações prestadas pelo Governo em 2020

Após as entrevistas de validação do grupo de discussão, realizadas em março de 2019, ficou claro que o Brasil dispõe de mais de uma CSIRT para suas operações nacionais: CTIR Gov. e CERT.br. A CTIR Gov coordena as atividades relacionadas à prevenção, tratamento e resposta a incidentes cibernéticos relacionados às CSIRTs da Administração Pública Federal. Além disso, cada entidade da Administração Pública Federal deve ter sua própria CSIRT e seu próprio órgão de TI responsável por essa interferência. O CTIR Gov, sendo uma CSIRT de responsabilidade nacional, também gere as solicitações de cooperação internacional em incidentes cibernéticos. O CERT.br, por outro lado, é um órgão certificado pelo FIRST, e é encarregado do setor privado. Cumpre salientar que, em virtude da natureza colaborativa do trabalho, na prática, os limites de competência entre as CSIRTs não são rígidos, com vistas a evitar comprometer a prevenção, o tratamento e a resposta a incidentes cibernéticos.

D 1.3 - Proteção da Infraestrutura Crítica (Ic)



Esse fator analisa a capacidade do governo de identificar os ativos de CI e os riscos a eles inerentes, de se envolver no planejamento de respostas e na proteção de ativos críticos, de promover a interação de qualidade com os proprietários de ativos de CI e de permitir uma prática abrangente de gerenciamento de risco geral, incluindo o planejamento de respostas.

Estágio: Estabelecido

A maturidade da capacidade do Brasil de proteger a infraestrutura crítica é diferente entre os atores públicos e privados da IC. Os participantes sugeriram que para os segmentos operados por entidades públicas da IC, o Gabinete de Segurança Institucional da Presidência (GSI), em colaboração com o Ministério da Defesa, mantém uma lista detalhada dos ativos da IC e realiza auditorias regularmente. As avaliações de risco consideram o impacto dos ataques aos ativos de IC na defesa nacional. Todas as instituições federais são obrigadas a realizar avaliações internas de risco cibernético, que são atualizadas anualmente com base nas lições aprendidas de grandes incidentes.[67] Foi informado que a página eletrônica do Departamento de Segurança da Informação (DSI) do GSI (http://dsic.planalto.gov.br) também reúne toda a legislação nacional relativa à segurança da informação. As partes interessadas da IC pública incluem empresas de telecomunicações, transporte e energia, e instituições financeiras, todas operando e coordenando por meio de canais formais de comunicação com o Ministério da Defesa. Há políticas e procedimentos claramente definidos em vigor, que devem ser seguidos por todas as instituições públicas, com base nas informações prestadas pela ferramenta nacional de conhecimento situacional da CERT. O acesso a essas informações é concedido à Polícia Federal e aos serviços de inteligência, com vistas a aumentar a cooperação e o gerenciamento de incidentes entre as partes interessadas da IC. Todos os protocolos, procedimentos e avaliações de risco são examinados anualmente por um grupo de trabalho de defesa cibernética. Esse grupo conta com chefes de informação (CIOs) em nível de gerência, bem como com membros técnicos, e identificou processos sobre como incorporar as lições aprendidas para aprimorar os protocolos e sistemas atualmente em vigor. Os participantes comentaram sobre o oximoro de que as lições aprendidas sejam baseadas em grandes incidentes, que ajudaram a aperfeiçoar significativamente os protocolos atuais: a falta de um incidente importante nos últimos dois anos tem dificultado o aperfeiçoamento constante desses protocolos.

Os participantes relataram que, no momento, o setor privado não é considerado parte da IC do país. Uma vez que o Brasil aprovou a privatização em setores críticos como o financeiro, é imperativa uma revisão da lista de participantes da IC para considerar instituições privadas. As instituições privadas não são obrigadas a informar

o Governo sobre um incidente grave, têm acesso restrito à inteligência de ameaças e ignoram as avaliações de risco e os processos que o governo tem implementado para as infraestruturas críticas públicas. Portanto, precisam desenvolver suas próprias avaliações internas de risco e políticas de segurança, cuja eficácia dependerá do grau de sua maturidade. As organizações bem estabelecidas dispõem de recursos para desenvolver suas políticas internas de segurança cibernética, mas os participantes expressaram preocupação com a capacidade das PMEs e da maioria das organizações do setor privado em geral.

Um exemplo característico de uma parte interessada importante negligenciada é o SERPRO, que atualmente não é considerado parte da infraestrutura crítica. Como os participantes observaram, todas as avaliações de risco são realizadas de uma perspectiva empresarial e não consideram o impacto na defesa nacional. Existem indicadores e medidas internas para o tratamento de incidentes do SERPRO, que são corporativos ou relacionados a seus clientes do Governo. Relatórios de incidentes com conteúdo confidencial são entregues aos clientes. Indicadores de desempenho foram estabelecidos para mostrar a eficácia dos processos, tais como o número de incidentes administrados, o número de incidentes categorizados e os considerados fora do prazo de aceitação. Quando o SERPRO decide que as ameaças em curso podem afetar a empresa, e caso exista a possibilidade de que esse incidente afete serviços ou bens do Governo, dispõe de políticas e instruções claras sobre como comunicar esses eventos às autoridades governamentais e à Polícia Federal. Em 2010, o SERPRO elaborou um livro detalhando estratégias e políticas sobre proteção da infraestrutura crítica, que não são seguidas na prática. Apesar dos processos claros do SERPRO sobre como relatar incidentes e protocolos para lidar com situações e prestar assistência a organizações privadas que deviam ser consideradas parte da IC, como as instituições financeiras, os participantes destacaram que a segurança das informações é como a higiene e, portanto, não pode ser implementada isoladamente. As infraestruturas críticas públicas, embora avançadas em maturidade, serão influenciadas por ataques contra instituições privadas mais frágeis. Portanto, apesar das claras diferenças de competência e capacidade cibernética entre os setores público e privado, é importante que as instituições aperfeiçoem sua coordenação, de modo a aumentar a maturidade no setor privado.

A maioria dos participantes instou o governo a criar um mecanismo para identificar o nível de maturidade na governança de TI, tanto no setor público quanto no privado, um protocolo de comunicação para distribuir alertas entre os setores público e privado e uma iniciativa para avaliar as normas e padrões das organizações privadas e públicas. Contudo, reconheceram que no esboço da estratégia nacional essas questões são provavelmente abordadas. Ações específicas foram implementadas para identificar ativos da infraestrutura crítica no setor privado e para criar canais formais de comunicação entre todas as partes interessadas da infraestrutura crítica.

Finalmente, os participantes gostariam de ter a oportunidade de colaborar estreitamente com outros países e de impor responsabilidade aos governos estrangeiros pelos danos que seus hackers causam ao Brasil. Essa é a razão pela qual as CERTs brasileiras se empenham em identificar vulnerabilidades globalmente. Nossas discussões de análise destacaram que uma cooperação mais estreita com a OEA, mediante a criação de uma plataforma de inteligência de ameaças entre os países que dela são membros, deveria ser o próximo passo. O maior obstáculo para uma inteligência de ameaças mais ampla entre os países é a falta de confiança entre eles. A revelação das vulnerabilidades das redes nacionais a outros países torna-se inteligência que poderia ser potencialmente posta em prática. Portanto, um protocolo de troca de informações que não crie desconforto aos países precisa ser acordado, a fim de fomentar a confiança na comunidade da OEA.

Resultados do processo de validação realizado em março de 2019

Em novembro de 2018, o Brasil publicou sua Política Nacional de Segurança de Infraestruturas Críticas, que estabelece as bases da Estratégia Nacional de Segurança de Infraestruturas Críticas e do Plano Nacional de Segurança de Infraestruturas Críticas.[68] Os participantes das entrevistas do grupo de discussão para validação da análise do CMM de 2019 destacaram que a presidência da federação promoveu alguma priorização dentro da infraestrutura nacional crítica, com base em sua vulnerabilidade e impacto, embora isso não pareça se refletir na documentação oficial. Entretanto, entende-se que esses documentos, delineando uma direção estratégica nacional para a proteção da infraestrutura crítica, oferecerão uma abordagem mais inclusiva e, portanto, considerarão as questões relativas à exclusão de operadores privados de infraestrutura crítica, observadas na análise do CMM em 2018.

De fato, já foram observados alguns desenvolvimentos no sentido de uma abordagem inclusiva da proteção da infraestrutura crítica. Os exercícios Guardião Cibernético, mencionados na seção seguinte deste relatório, envolveram não apenas o Governo e as forças armadas, mas também vários operadores privados de infraestrutura crítica. Os participantes das entrevistas de validação do CMM salientaram o "imenso valor" dessas oportunidades de articulação entre o Governo e os operadores privados de infraestrutura crítica.

D 1.4 - Gerenciamento de Crises

Esse fator aborda o planejamento de gerenciamento de crises e considera a realização de avaliações especializadas de necessidades, exercícios de treinamento e simulações que produzem resultados escaláveis para o desenvolvimento de políticas e a tomada de decisões estratégicas. Mediante técnicas qualitativas e quantitativas, os processos de avaliação de segurança cibernética visam a produzir resultados estruturados e mensuráveis que exigiriam recomendações dos formuladores de políticas e outras partes interessadas e fundamentariam a implementação de estratégias nacionais, além das alocações orçamentárias.

Estágio: Estabelecido

Na última década, o Brasil sediou uma série de eventos importantes, entre eles os Jogos Pan-Americanos, em 2007; a visita do Papa ,em 2013; a Copa do Mundo da FIFA, em 2014; e os Jogos Olímpicos, em 2016. A segurança cibernética foi um elemento crítico para o gerenciamento de crises nesses eventos, e mais de 40 organizações (incluindo a Rio CERT, o SERPRO, a CERT nacional e o CTIR Gov) foram responsáveis pelo tratamento e redução de incidentes. O Centro de Defesa Cibernética (CDCiber), unidade encarregada da coordenação dos aspectos estratégicos e operacionais da arquitetura de defesa cibernética do Brasil, supervisionou os procedimentos de gerenciamento de crises durante esses grandes eventos, em coordenação com o Ministério da Defesa e o GSI.

Conforme se previa, o Brasil experimentou diversos problemas de segurança cibernética no decurso desses grandes eventos. Dois dos incidentes mais significativos foram múltiplos ataques de DDOS que variaram de 300GB por segundo a 1TB por segundo, e um incidente de sabotagem que destruiu o cabo que garantia o acesso à Internet da rede da Copa do Mundo da FIFA. Todos os eventos foram conduzidos eficientemente e o retorno à atividade normal foi alcançado conforme o acordo de nível de serviço aprovado. Os participantes esclareceram que os processos de tratamento de incidentes durante esses eventos mostraram que as organizações críticas para a defesa cibernética são capazes de colaborar e efetivamente reduzir o impacto desses ataques. As organizações que participaram do gerenciamento de crises tinham papéis claros, havia protocolos transparentes sobre como divulgar informações e relatar incidentes a instâncias superiores, e diretrizes específicas sobre a proteção de sistemas. Entretanto, os processos de gerenciamento de crises foram adaptados a esses eventos específicos.

Os participantes expressaram a opinião de que os grandes eventos obrigaram as organizações a cooperar, e ajudaram a fomentar a confiança da comunidade de segurança cibernética do Brasil. Como exemplo da relevância da confiança no intercâmbio da inteligência de ameaças, os participantes mencionaram o ataque WannaCry, cujo impacto na maioria das organizações no Brasil foi mínimo. Isso se deve ao fato de as

organizações terem partilhado informações rapidamente com seus parceiros de confiança, emitindo alertas e especificando detalhes sobre as respostas, que foram considerados confiáveis e que todos podiam executar.

No decorrer da análise, os participantes sugeriram que a experiência e as lições aprendidas com esses eventos deveriam fundamentar os esforços atuais no gerenciamento de crises. Os protocolos de gerenciamento de crise devem ser projetados e uma rede de organizações públicas e privadas criada para atender aos principais eventos. Treinamento e exercícios sobre eventos simulados de crise foram sugeridos como a melhor maneira de validar protocolos de comunicação, aumentar a conscientização sobre segurança cibernética e testar processos de tratamento de incidentes. Nesse sentido, os participantes mencionaram o exercício Guardião Cibernético, que utiliza planejamento de alto nível para elaborar cenários e plataformas de simulação para operações cibernéticas que possam emular sistemas críticos dos setores financeiro, nuclear e público.

Os exercícios de situação de crise ocorrem frequentemente e envolvem principalmente sistemas militares e governamentais. Esses exercícios são também combinados com simulações físicas. Os participantes mencionaram que em breve será realizado um exercício que incluirá o setor financeiro e os sistemas nucleares. Também salientaram que mais organizações precisam participar desses exercícios, incluindo a sociedade civil.

Resultados do processo de validação realizado em março de 2019

Em 2019, o seminário de validação confirmou em grande parte os resultados do relatório CMM de 2018.

D 1.5 - Defesa Cibernética

Esse fator examina a capacidade do governo de projetar e implementar uma estratégia de defesa cibernética e liderar a implementação dessa estratégia, inclusive por meio de uma organização de defesa cibernética específica. O fator também analisa o nível de coordenação entre vários atores dos setores público e privado, em resposta a ataques maliciosos a sistemas de informação estratégicos e à infraestrutura nacional crítica.

Estágio: Formativo – Estabelecido

No tocante à governança da segurança cibernética, o governo brasileiro atribuiu o nível político e estratégico ao GSI, e os procedimentos estratégicos, operacionais e de defesa cibernética ao Ministério da Defesa. Nos últimos anos, a área militar foi reestruturada para atender às necessidades de um sistema democrático em evolução, com ênfase em ameaças transfronteiriças emergentes e eventos de segurança interna. De acordo com fontes secundárias, as forças armadas são consideradas as instituições nacionais mais confiáveis e têm sido incumbidas do gerenciamento de crises de grandes eventos civis.[69] Desse modo, as Forças Armadas receberam verbas governamentais para liderar o desenvolvimento da capacidade de segurança cibernética da nação.

Um documento oficial de defesa cibernética foi publicado em 2012 fixando as diretrizes de políticas de segurança cibernética.[45]Os militares operam uma CERT e oferecem treinamento em gerenciamento de risco e resposta a incidentes. Há uma unidade exclusiva especializada em planejar e realizar operações cibernéticas.[70] A mesma unidade é responsável pela coordenação com o Ministério do Interior, bem como com os serviços de inteligência, a Polícia Federal e o SERPRO, por meio de canais formais e bem estabelecidos de comunicação.

Os participantes sugeriram que as forças armadas detêm capacidade tanto ofensiva quanto defensiva, e se centram no aprimoramento das medidas defensivas. Salientaram que as forças armadas implantam sistemas que proporcionam consciência situacional e defendem proativamente de ataques de DDOS e vandalização de sites. Há laboratórios para analisar software malicioso, e um número significativo de funcionários em treinamento para executar essas tarefas. Há ferramentas implementadas, como o BI, para facilitar as avaliações de riscos cibernéticos e analisar os resultados. Por último, exercícios cibernéticos são realizados com frequência e, para a próxima edição, os militares convidarão as organizações privadas para participar.

Resultados do processo de validação realizado em março de 2019

Em 2019, o Brasil ainda não dispunha de uma estratégia específica para a defesa cibernética; quando for adotada, um dos principais elementos da Estratégia Nacional de Segurança da Informação será a defesa cibernética.[71] Diretrizes estratégicas para a defesa cibernética já vêm sendo elaboradas pelo Ministério da Defesa, e as futuras consultas incluirão, segundo informações, o setor privado. Diretrizes estratégicas relevantes estão atualmente definidas, resumidamente, na Estratégia Nacional de Defesa.[72]

D 1.6 - Redundância nas Comunicações

Este fator analisa a capacidade do governo de identificar e mapear a redundância digital e as comunicações redundantes entre as partes interessadas. A redundância digital prevê um sistema de segurança cibernética no qual um backup adequado irá proteger contra a duplicação e falha de qualquer componente. A maioria desses backups terá a forma de redes digitais isoladas (de sistemas de linha principal), porém prontamente disponíveis, mas algumas podem ser não digitais (p.ex., backup de uma rede de comunicações digitais com uma rede de comunicações via rádio).

Estágio: Formativo

Não foi possível obter uma visão ampla sobre a redundância nas comunicações no decorrer da análise do CMM. Os participantes sugeriram que o setor público possui recursos de resposta a emergências conectados à rede de comunicação de emergências da estratégia nacional. Recursos apropriados estão disponíveis para avaliar os protocolos atuais de redundância, para testar sistemas redundantes, realizar exercícios e executar práticas de comunicação. Vários centros de crise são designados em locais geográficos dispersos para garantir a participação de todas as partes interessadas no caso de uma emergência. Em forte contraste, o setor privado é negligenciado e excluído desses planos, com exceção de um pequeno número de CERTs privadas.

Como os participantes salientaram, existem sistemas telefônicos seguros entre a CERT nacional e a CSIRT, e normas internacionais são seguidas para o uso de e-mail e outros métodos como procedimentos de redundância para comunicação. Entretanto, a ausência do setor privado da rede de comunicação de emergência é ainda um problema. É importante obter um quadro holístico da maturidade das partes interessadas da IC privada que apoiam processos críticos nas redes nacionais de comunicação. É necessário definir os requisitos para que os ISPs disponham de recursos de resposta a emergências redundantes e realizem com frequência testes de stress para disponibilidade de rede.

Resultados do processo de validação realizado em março de 2019

Desde 2018, a situação no Brasil não mudou drasticamente. Segundo um participante do seminário de validação de análise do CMM de 2019, “o Brasil ainda precisa fazer mais para definir medidas adequadas de redundância das comunicações”.

Recomendações

Com base nas informações apresentadas no decorrer da análise da maturidade da política e da estratégia de segurança cibernética, o GCSCC desenvolveu o seguinte conjunto de recomendações para consideração do Governo do Brasil. Essas recomendações propõem orientações e passos, com vistas a aumentar a capacidade existente de segurança cibernética, de acordo com as considerações do CMM do Centro. As recomendações são formuladas especificamente para cada fator.

ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA

R 1.1
Preparar uma complementação do documento da estratégia, compatível com os objetivos nacionais e as prioridades de risco, para sugerir diretrizes aplicáveis com a métrica respectiva, para monitorar o andamento da implementação da estratégia.

R 1.2
Assegurar que as partes interessadas envolvidas na concepção da estratégia nacional de segurança cibernética incorporem organizações do setor privado que devem fazer parte da IC (especialmente de finanças, energia, telecomunicações, transportes, o SERPRO, Empresa de Tecnologia e Informações da Previdência Social (Dataprev), PMEs, sociedade civil, setor acadêmico e parceiros internacionais.

R 1.3
Aprimorar a colaboração com a OEA e desenvolver uma taxonomia comum para a segurança cibernética.

R 1.4
Assegurar que as normas de segurança da informação desenvolvidas pela Administração Pública Federal sejam as normas mínimas a serem adotadas pelas autoridades públicas do Estado, e que sua implementação seja incluída nos programas nacionais de estratégia de segurança cibernética.

Resposta a incidentes

R 1.5
Criar um banco de dados nacional central de inteligência de incidentes que reuna informações sobre incidentes de todos os setores. Designar CERTs para cada setor crítico (isto é, finanças, telecomunicações, governo, forças armadas, petróleo e gás etc.) incumbidas da divulgação das informações adaptadas às necessidades do setor respectivo.

R 1.6
Identificar organizações do setor privado que sejam fundamentais para a segurança cibernética nacional e autorizar que tenham acesso às informações compartilhadas pela CERT nacional.

R 1.7
Obter consenso entre as partes interessadas (particularmente do setor privado) sobre arquitetura, interfaces e normas para a troca de informações. As normas comuns promovidas, por exemplo, pela UE e pelos Estados Unidos, são STIX e TAXII. As partes interessadas devem incluir os setores privado e público, bem como a comunidade de segurança cibernética, em âmbito nacional, regional e internacional.

R 1.8
Estabelecer métricas para monitorar e avaliar a eficácia de todas as CERTs. Além disso, aumentar a colaboração entre a OEA, as CERTs regionais e outros organismos internacionais.

R 1.9
Estabelecer treinamento regular para os funcionários de todas as CERTs e projetar métricas para avaliar os resultados desse treinamento. Os cursos oferecidos pela CERT nacional, a CERT militar e o SERPRO podem fundamentar o treinamento para as demais CERTs.

R 1.10
Identificar e documentar os principais processos de resposta a incidentes, destacando quando e como diferentes ministérios, o governo estadual e as organizações privadas devem ser envolvidas.

Proteção da infraestrutura crítica (IC)

R 1.11
Desenvolver e realizar uma avaliação nacional de risco, com vistas a identificar as partes interessadas e as ameaças nacionais da IC, com destaque específico para as organizações do setor privado.

R 1.12
Elaborar e divulgar uma lista de ativos da IC, com prioridades identificadas com base no risco, que inclua ativos do setor privado.

R 1.13
Estabelecer um mecanismo para a divulgação regular de vulnerabilidades e intercâmbio de informações entre os proprietários de ativos privados e públicos da IC e o Governo. Estabelecer uma comunicação regular entre os níveis tático, executivo e estratégico, quanto às práticas de risco cibernético, e encorajar a comunicação entre os operadores da IC.

R 1.14
Identificar estratégias de comunicação interna e externa da IC, com pontos de contato claros, que incluam o setor privado.

R 1.15
Estabelecer procedimentos e processos de proteção de informações e gerenciamento de riscos no âmbito da IC, apoiados por soluções técnicas adequadas de segurança, que fundamentem o desenvolvimento de um plano de resposta a incidentes cibernéticos.

R 1.16
Estabelecer procedimentos comuns para medir e avaliar a capacidade dos proprietários de ativos da IC de detectar e identificar ameaças cibernéticas, bem como a elas responder e delas se recuperar.

R 1.17
Determinar a concepção e implementação de avaliações de risco cibernético, apropriadas e regulares, por todas as partes interessadas da IC, e identificar as informações necessárias a serem partilhadas. Projetar avaliações de risco cibernético para todas as partes interessadas da IC, com base na abordagem de avaliação de risco nacional.

R 1.18
Incumbir os reguladores de cada setor de dispor a divulgação de incidentes. Estabelecer limites para a divulgação de incidentes após consultas com organizações privadas e públicas dos respectivos setores.

Gerenciamento de crises

R 1.19
Projetar um cenário de crise realista, de alto nível, para fundamentar um plano para testar fluxos de informação, tomada de decisões e investimento de recursos em âmbito nacional.

R 1.20
Desenvolver objetivos e indicadores chave de desempenho (PKI), específicos, mensuráveis, atingíveis, relevantes e com calendário definido (SMART), para orientar as decisões no gerenciamento de crises.

R 1.21
Assegurar que os resultados da avaliação dos dois exercícios do Guardião Cibernético anteriores sirvam de base para o investimento futuro na capacidade nacional de segurança cibernética, e que os resultados sejam avaliados em relação às boas práticas internacionais de gerenciamento de crises.

R 1.22
Preparar relatórios personalizados e específicos do setor sobre os exercícios de gerenciamento de crise para cada parte interessada.

Defesa cibernética

R 1.23
Garantir o desenvolvimento de um componente de defesa cibernética na estratégia de segurança nacional, o qual deve considerar as ameaças à segurança nacional que possam surgir do ciberespaço.

R 1.24
Avaliar e determinar os requisitos de capacidade de defesa cibernética e envolver as partes interessadas dos setores público e privado. Realizar análises contínuas do panorama de ameaças em evolução na segurança cibernética, a fim de garantir que as políticas de defesa cibernética continuem atendendo aos objetivos de segurança nacional.

R 1.25
Projetar exercícios cibernéticos nacionais que impliquem uma série de organizações do setor privado.

Redundância nas comunicações

R 1.26
Testar a interoperabilidade e a função dos ativos de resposta a emergências em cenários de comunicação negociados, para fundamentar investimentos estratégicos em ativos de resposta a emergências futuras. Assegurar que o setor privado seja considerado participante chave no plano de resposta a emergências.

R 1.27
Estabelecer um processo, envolvendo todas as partes interessadas relevantes, para identificar as lacunas e sobreposições nas comunicações de ativos de resposta a emergências e as responsabilidades das autoridades.

R 1.28
Estabelecer um processo, envolvendo todas as partes interessadas relevantes, para identificar as lacunas e sobreposições nas comunicações de ativos de resposta a emergências e as responsabilidades das autoridades.

R 1.29
Estabelecer canais de comunicação entre as funções de resposta a emergências, as áreas geográficas de responsabilidade, as equipes de emergência públicas e privadas, e as autoridades de comando. Criar atividades de extensão e educação para protocolos de comunicações redundantes adaptados às funções e responsabilidades de cada organização no plano de resposta a emergências.

R 1.30
Incluir elementos cibernéticos nos exercícios existentes de emergência e crise, e identificar métricas para avaliar o sucesso do exercício. Avaliar os exercícios e introduzir os resultados no processo de tomada de decisão.

Dimensão 2

CULTURA CIBERNÉTICA E SOCIEDADE

As estratégias e políticas de segurança cibernética de vanguarda envolvem uma grande variedade de atores, incluindo os usuários da Internet. O tempo em que a implementação da segurança cibernética era confiada formalmente aos especialistas chegou ao fim com o advento da Internet. Todos os envolvidos com a Internet e tecnologias correlatas, como as mídias sociais, precisam entender o papel que podem desempenhar na proteção de dados sensíveis e pessoais, ao usar as mídias e recursos digitais. Essa dimensão destaca a centralidade dos usuários na consecução da segurança cibernética, mas procura evitar as tendências convencionais de culpar os usuários pelos problemas de segurança cibernética. Em vez disso, um aspecto importante da cultura de segurança cibernética e sociedade é a conscientização entre os especialistas em segurança cibernética de que precisam construir sistemas e programas para os usuários – sistemas que possam ser usados facilmente e incorporados às práticas cotidianas on-line.

Essa dimensão analisa elementos importantes de uma cultura responsável de segurança cibernética e sociedade , tais como a compreensão dos riscos cibernéticos por todos os atores, o desenvolvimento de um nível avançado de confiança nos serviços da Internet, de governo eletrônico e de comércio eletrônico, e o entendimento por parte dos usuários sobre como proteger informações pessoais on-line. Essa dimensão também implica a existência de mecanismos de responsabilização, tais como canais para que os usuários denunciem ameaças à segurança cibernética. Essa dimensão analisa ainda o papel da mídia e das mídias sociais e sua contribuição para moldar os valores, atitudes e comportamentos de segurança cibernética.

D 2.1 - Mentalidade de Segurança Cibernética

Esse fator avalia o grau em que a segurança cibernética é priorizada e incorporada aos valores, atitudes e práticas do Governo, do setor privado e dos usuários em toda a sociedade. Uma mentalidade de segurança cibernética consiste em valores, atitudes e práticas, incluindo hábitos, de usuários individuais, especialistas e outros atores do ecossistema de segurança cibernética, que aumentam a resiliência dos usuários diante de ameaças a sua segurança on-line.

Estágio: Formativo

O Governo reconheceu a necessidade de priorização da segurança cibernética em todas as suas instituições. Do mesmo modo, aspectos dos processos governamentais e das estruturas institucionais foram projetados em resposta aos riscos de segurança cibernética, mas são localizados principalmente em agências líderes específicas.

Em geral, os participantes observaram que a cultura de segurança no Brasil varia entre as diferentes zonas do país e os diferentes setores do governo, das empresas e da indústria. Todos os ministérios têm funcionários certificados pelo CISSP e, da mesma forma, diferentes agências cobrem as necessidades de gerenciamento de TIC e estabelecem requisitos de software.

O Gabinete do Presidente da República tem seu próprio escritório de TI que fornece tudo, de software a computadores pessoais, com suporte administrativo centralizado. Como os participantes mencionaram, no governo federal, os recursos são alocados para o treinamento de funcionários que administram questões de segurança, para esforços voltados para o cumprimento de obrigações com a ISACA e estruturas como a ISO 270001, e para o cumprimento das melhores práticas relacionadas à segurança da informação identificadas pelo governo. Além disso, um sistema de auditoria vem sendo aplicado no âmbito do governo federal. Todas as agências mantêm um departamento responsável pela auditoria. Em 2017, foi executado um programa de visitas de auditoria, para avaliar o nível de maturidade em 40 agências diferentes.

Os participantes se mostraram preocupados com a complexidade da estrutura governamental no Brasil. De acordo com a atual avaliação de maturidade do setor público, reconhece-se que haverá diferentes estágios de maturidade nos diferentes departamentos e entre eles. Entretanto, o controle ou a influência do governo federal nos governos estaduais e municipais são limitados.

Outra preocupação suscitada pelos participantes é a inexistência de um mecanismo de coordenação para identificar e considerar as inadequações de maturidade no governo. Como sugeriram, falta um protocolo para a distribuição de alertas, similar aos usados pelas CERT, além de ser necessário um canal de comunicação integrado, para avaliar as normas e os padrões implementados.

O DSI é o Departamento de Segurança da Informação, e pode administrar a segurança da informação para o setor público em geral. No entanto, existem departamentos

governamentais independentes e conjuntos de diretrizes independentes. Como exemplos, os participantes mencionaram, entre outros, o Serviço Federal de Processamento de Dados, o SERPRO,[73] unidade da administração pública responsável pela prestação de serviços de TI para o Ministério da Fazenda. Os regulamentos e normas são obrigatórios para o SERPRO porque ele pertence ao Governo. Entretanto, as agências estaduais não são obrigadas a seguir essas regras, o que cria a necessidade de o governo federal persuadir as agências estaduais e locais a adotar iniciativas de segurança cibernética.

Empresas líderes do setor privado começaram a priorizar mais uma mentalidade de segurança cibernética, mediante a identificação de práticas de alto risco. Os participantes salientaram que, entre as barreiras para o desenvolvimento de uma esfera digital, se encontram o alto custo de implantação e a falta de clareza quanto ao retorno do investimento, bem como a falta de normas e regulamentos bem compreendidos, a carência de normas técnicas e a necessidade de educação e treinamento nessa área.

Os setores financeiro e de TI estão relativamente mais avançados em segurança cibernética, pelo fato de serem alvos frequentes de ataques, o que faz com que invistam mais em segurança cibernética e possam mostrar a outras agências como adotar práticas mais seguras. Os participantes relataram que desde que os bancos centrais começaram a tomar medidas de segurança proativas, os criminosos cibernéticos têm se concentrado mais nos bancos regionais e nas PMEs.

Uma proporção limitada, mas crescente, de usuários da Internet começou a conferir maior prioridade à segurança cibernética, tornando-se, por exemplo, mais consciente dos riscos e ameaças. A sociedade como um todo ainda carece de uma mentalidade de segurança cibernética. Os usuários da Internet podem estar cada vez mais conscientes dos riscos da segurança cibernética, porém raramente agem da maneira devida em suas práticas cotidianas. Mencionaram que é comum que até mesmo os especialistas em TI, que são supostamente os mais conscientes dos riscos, cliquem em e-mails de phishing, ou partilhem informações sensíveis em sites de mídia social, como o Facebook. Em distritos de baixa renda, os cidadãos tendem a depender do uso de telefones celulares para se conectarem à Internet, apesar de o Governo disponibilizar satélites para essas comunidades para conexão à Internet. É muito importante que essas comunidades aumentem a conscientização dos riscos.

Em geral, os participantes salientaram a necessidade de maior conscientização e educação em todos os níveis, em todos os setores.

Resultados do processo de validação realizado em março de 2019

Em 2019, os entrevistados observaram que houve algum progresso na maturidade da mentalidade de segurança cibernética em relação ao ano anterior. Apesar disso, alguns argumentaram que os problemas com phishing e outros incidentes cibernéticos similares persistem, mostrando que as boas práticas de segurança cibernética não são amplamente empregadas por funcionários do Governo.

Representantes do setor privado relataram que a principal questão entre seus funcionários é a falta de conscientização sobre a segurança cibernética, especialmente a relacionada à proteção de dados pessoais. Os pesquisadores ouviram durante uma das entrevistas de grupo em março de 2019 que "as pessoas partilham tudo on-line". No entanto, a mentalidade de segurança cibernética no setor privado continua aumentando, e um número crescente de empresas faz da mentalidade de segurança cibernética uma prioridade.

Observações semelhantes podem ser feitas sobre a mentalidade de segurança cibernética entre os usuários da Internet. Embora a mentalidade de segurança cibernética na sociedade brasileira ainda seja limitada e as pessoas regularmente desconsiderem as boas práticas, especialmente quando se trata de partilhar conteúdo pessoal on-line, fontes secundárias informam que uma proporção limitada de usuários de Internet de fato confere prioridade à segurança cibernética no cotidiano. Por exemplo, quase metade dos internautas brasileiros evita clicar em links não solicitados em mensagens e mais de um terço deles faz uso das configurações de privacidade oferecidas por várias plataformas on-line. Além disso, quase metade dos internautas brasileiros usa software antivírus, embora apenas um quarto deles mude suas senhas regularmente.[74]

D 2.2 - Confiança na Internet

Esse fator analisa o nível de confiança dos usuários no uso de serviços on-line em geral e de serviços de governo eletrônico e comércio eletrônico em particular.

Estágio: Formativo – Estabelecido

Em geral, os participantes acreditam que uma pequena proporção de usuários da Internet avalia criticamente o que veem ou recebem on-line. Da mesma forma, poucos acreditam ter a capacidade de usar a Internet e de se proteger on-line. Além disso, uma proporção limitada de usuários confia na segurança da Internet e não sabe como determinar a legitimidade de um site.

Os serviços de governo eletrônico foram desenvolvidos, e uma proporção crescente de usuários confia na segurança desses serviços. Contudo, possíveis violações nos serviços de governo eletrônico estão sendo identificadas, reconhecidas e divulgadas de forma ad hoc.

Atualmente, o governo brasileiro oferece vários serviços governamentais aos cidadãos, entre eles os abaixo enumerados.[75]

- Receita Federal – serviços de cobrança do imposto de renda, situação fiscal do contribuinte, registro do Cadastro de Pessoas Físicas (CPF) e do Cadastro Nacional da Pessoa Jurídica (CNPJ), e declarações, entre outros.

- Polícia Federal – serviços como pedidos de passaporte, declarações de registros criminais e apoio a adoções internacionais, entre outros.

- Sistema Integrado de Administração Financeira do Governo Federal (SIAFI) – interesses vinculados ao Tesouro Nacional, como a provisão de gastos públicos.

- Poupa Tempo (Estado de São Paulo) – acesso a informações sobre serviços públicos, tais como solicitação de documentos e abertura e encerramento de empresas.

• Projeto OntoJuris – prestação de informações sobre legislação na área de direitos de propriedade intelectual, direitos do consumidor e direito eletrônico.

• Projeto OntoJuris – prestação de informações sobre legislação na área de direitos de propriedade intelectual, direitos do consumidor e direito eletrônico.

Serviços como o envio da Declaração de Imposto de Renda, informações sobre previdência social e compras governamentais estão disponíveis via Internet desde 1998, mas, são, em grande parte, prestação de informações versus prestação de serviços. No ano 2000, a Política de Governo Eletrônico foi definida e instituída, e o Programa Sociedade da Informação foi lançado, desse modo consolidando e divulgando estratégias de governo eletrônico, a importância social da inclusão digital, assim como ações relacionadas à tecnologia da informação no país, como a elaboração de diretrizes e estruturas jurídicas no país para serviços de governo eletrônico (Scartezini, 2004).

Uma proporção crescente de usuários confia no uso seguro dos serviços de comércio eletrônico. Há, no Ministério da Justiça, uma secretaria dedicada aos direitos do consumidor e ao comércio eletrônico. A legislação brasileira inclui disposições sobre comércio eletrônico (Código de Proteção do Consumidor – Lei n° 8.078/1990; Decreto n° 8.771/2016, que regulamenta o Marco Civil da Internet no Brasil ou Lei da Internet (Lei n° 12.965/2012), ver D 4.1). Portanto, nessa área, os impostos altos sobre o comércio eletrônico não se referem ao comércio nacional, mas ao comércio internacional.

Em geral, há um grande incentivo para que as empresas prestem serviços on-line. A prestação de serviços de comércio eletrônico vem crescendo e aumentou desde 2017. Nesse ano, o Brasil (a Polícia Federal do Brasil) e a Europol assinaram um acordo estratégico para expandir a cooperação no combate a atividades criminosas transfronteiriças, o que se poderia considerar uma cooperação formal. As empresas tendem cada vez mais a investir em serviços de comércio eletrônico já totalmente estabelecidos. As soluções de segurança são atualizadas e sistemas de pagamento confiáveis, disponibilizados. Contudo, os participantes destacaram que ainda existem desafios à segurança cibernética e à proteção dos dados dos usuários, tais como o vazamento de dados de cartões de crédito decorrentes de ataques cibernéticos.

O setor bancário organiza campanhas de conscientização e presta informações on-line aos usuários, com relação a sua segurança. Por exemplo, o Banco do Brasil[76] e o Banco Itaú[77] oferecem dicas de segurança para os clientes. Embora haja investimentos em serviços de comércio eletrônico e os participantes acreditem em um aumento no uso de serviços de comércio eletrônico, os hackers parecem estar na vanguarda.

Resultados do processo de validação realizado em março de 2019

Em maio de 2018, o Governo publicou a versão revisada da Estratégia de Governança Digital: Transformação digital - Cidadania e governo,[78] que, entre outros aspectos, abrange questões de segurança cibernética no contexto dos serviços de governo eletrônico. A estratégia inclui vários princípios aplicáveis de governança digital – um deles, a segurança cibernética – que são promovidos por várias entidades governamentais e mantém uma página eletrônica exclusiva.[79] A promoção dos princípios provavelmente contribuiu para o fato de que, de acordo com a pesquisa da OCDE de 2018, 94% das organizações do setor público têm conhecimento da Estratégia de Governança Digital.[80]

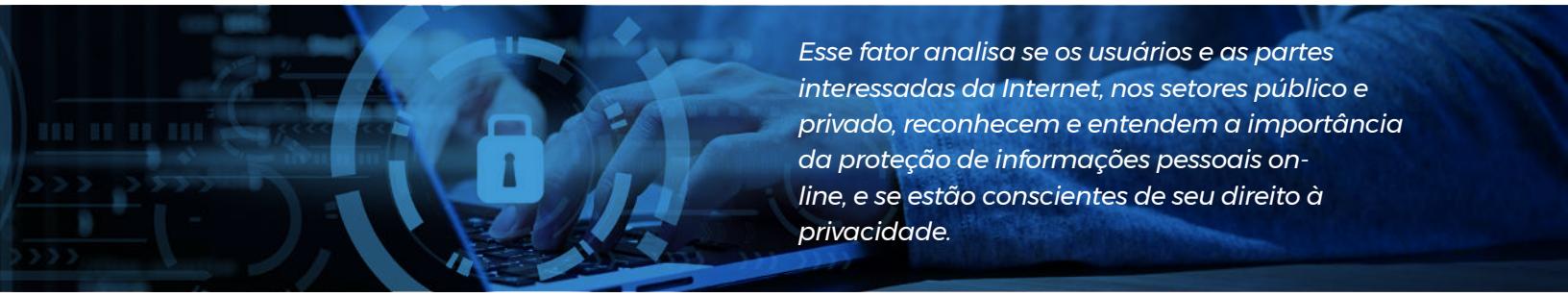
Os usuários, assim como o Governo, estão cientes da importância de serviços de governo eletrônico seguros.[81] identificação, a notificação e a análise de violações se inserem no mandato do CTIR Gov; exemplos de alertas públicos relacionados à insegurança dos serviços eletrônicos do Governo estão disponíveis on-line.[82] De acordo com o estudo oficial mais recente, publicado em 2018, 64% (número em crescimento) de todos os brasileiros com mais de 16 anos de idade

utilizam os serviços eletrônicos do Governo. Metade deles não citaram a preocupação com privacidade e segurança como a principal razão de sua abstinência.[83]

Em 2019, a maioria dos sites de comércio eletrônico oferecia termos e condições de uso facilmente acessíveis.[84] A maioria deles também utilizava conexão criptografada entre o usuário e seus servidores, e oferecia uma ampla gama de opções de pagamento seguro.[85] A segurança e a confiança foram promovidas pelos provedores de comércio eletrônico mediante a grande exibição de protocolos de segurança disponíveis para os usuários. O Governo também foi dinâmico na promoção da confiança por meio da publicação de dicas de segurança para compradores on-line.[86]

Uma proporção crescente de brasileiros usa os serviços de comércio eletrônico. Em 2018, 33% dos entrevistados no estudo do Centro para a Inovação da Governança Internacional informou que fazem compras on-line pelo menos duas vezes por mês, em comparação com 23% em 2017. Um quarto dos que não fazem compras on-line argumentou que isso se deve ao fato de não confiarem nas compras on-line (embora isso não se deva apenas à falta de confiança na segurança das plataformas de compras on-line.[87]

D 2.3 - Entendimento do Usuário Sobre a Proteção de Informações Pessoais On-line



Esse fator analisa se os usuários e as partes interessadas da Internet, nos setores público e privado, reconhecem e entendem a importância da proteção de informações pessoais on-line, e se estão conscientes de seu direito à privacidade.

Estágio: Formativo

Os usuários e as partes interessadas dos setores público e privado têm conhecimento geral sobre como as informações pessoais são tratadas on-line e empregam boas práticas (proativas) de segurança cibernética para a proteção das informações pessoais on-line.

A Lei Geral de Proteção de Dados Pessoais foi aprovada pelo Brasil em julho de 2018.[88] Além disso, muitos escritórios de advocacia no Brasil começaram a criar divisões especializadas em proteção de dados, enquanto empresas privadas e organizações sem fins lucrativos organizam eventos sobre proteção de dados.

Além disso, algumas disposições em outras estruturas legislativas consideram essa questão (ver D 4.1). Por exemplo, as partes interessadas mencionaram que, no Brasil, é comum que as pessoas sejam solicitadas a declarar suas informações pessoais tanto offline como on-line. De acordo com os participantes, os

brasileiros estão acostumados a abrir mão de sua privacidade, embora se tenha conhecimento de grandes bancos de dados que foram alvo de importantes episódios de vazamento e de uso indevido de eventos de dados.

Além de um recibo, um consumidor no Brasil receberá uma fatura com um número e um código de barras que terá que digitalizar por meio de seu telefone celular. Essa prática causou alguns incidentes no passado. Quando, por exemplo, um malware chamado boware visou usuários do comércio eletrônico, ele mudou o código de barras da fatura de forma a permitir fraudes.
Com relação às PMEs, as partes interessadas mencionaram que existe a necessidade de prepará-las para essas atividades fraudulentas. Nesse sentido, o Governo tomou medidas para aumentar a conscientização sobre a privacidade dos dados e a proteção de informações pessoais on-line (ver D 3.1).

No ano passado, exercícios internos de phishing foram realizados e foi desenvolvida uma análise interna do nível de conscientização, com o intuito de entender como aumentar esse nível de conscientização em âmbito nacional. Os esforços por aumentar a conscientização são contínuos, mediante a divulgação de folhetos sobre a proteção de senhas e a necessidade de backups, por exemplo, e a definição do mês de outubro como o mês da segurança, realizando palestras e outros eventos, e produzindo uma série de vídeos, áudios e materiais informativos escritos. Essas iniciativas vêm sendo desenvolvidas com base no pensamento de que o usuário deve ser capaz de seguir as instruções dadas.

Resultados do processo de validação realizado em março de 2019

Embora seja difícil dizer que a maturidade do fator mudou desde a análise do CMM, em 2018, cumpre observar que, em agosto de 2018, o Brasil promulgou a Lei Geral de Proteção de Dados (Lei Federal n° 13.709/2018). Os participantes das entrevistas do grupo de discussão de 2019 expressaram insatisfação com o fato de essa lei não entrar em vigor até agosto de 2020.

D 2.4 - Mecanismos de Informação

Esse fator explora a existência de mecanismos de informação que funcionam como canais para os usuários denunciarem crimes de Internet, como fraude, assédio virtual, abuso infantil, roubo de identidade, violação de privacidade e segurança, e outros incidentes.

Estágio: Formativo

Foram estabelecidos mecanismos de informação para que os usuários denunciem crimes relacionados à Internet, os quais são utilizados regularmente. A SaferNet Brasil[89] presta informações sobre segurança na Internet e dispõe espaço para reclamações em seu site. A SaferNet Brasil, organização sem fins lucrativos criada em 2005, é um órgão único da sociedade civil no Brasil. Os acordos formais que mantém com o Ministério da Justiça, a Polícia Federal e a Secretaria de Direitos Humanos no Gabinete do Presidente da República permitem que receba e processe relatórios provenientes do público. Seu serviço de linha direta on-line pode ser usado para relatar conteúdos anonimamente.

Além disso, figura no site da Polícia Federal[90] uma página exclusiva para denúncias, que também podem ser feitas pelo endereço de e-mail (denuncia.ddh@dpf.gov.br). A pornografia infantil e adolescente[91] pode ser denunciada pela linha de ajuda criada pelo Governo.

No Brasil, em geral, existem diferentes canais para relatar incidentes. Para incidentes como pornografia infantil, deve-se enviar um e-mail à polícia, enquanto para incidentes de fraude as denúncias devem feitas por meio do banco respectivo. Todos os incidentes são denunciados à polícia, enquanto aqueles não claramente classificados são enviados ao CTIR Gov Brasil para categorização, antes do encaminhamento às instituições competentes. Por exemplo, caso o crime cibernético seja cometido contra um cidadão, o incidente será tratado pela Polícia Civil do estado onde mora esse cidadão. Caso o crime atinja empresas públicas federais, como a Caixa[92] ou o Banco Central do Brasil,[93] o órgão competente será a Polícia Federal.

Em geral, os participantes ressaltaram que os cidadãos no Brasil não têm uma cultura de informação. Não foi possível identificar se existem programas para promover o uso dos mecanismos existentes estabelecidos pelos setores público e privado.

Os incidentes mais comuns que os usuários enfrentam são crimes financeiros, como fraudes on-line. Quanto a esses incidentes, caberá à Federação de Bancos tomar medidas. O CTIR Gov Brasil participa das reuniões mensais e da troca de informações também na área financeira. Também o Governo vem buscando maneiras de tornar obrigatória a comunicação de incidentes para o setor privado.

Resultados do processo de validação realizado em março de 2019

Em 2019, o seminário de validação confirmou em grande parte os resultados do relatório CMM de 2018.

D 2.5 Mídia e Mídia Social

Esse fator analisa se a segurança cibernética é um assunto comum em toda a grande mídia e um tema de amplo debate nas mídias sociais. Esse aspecto também considera o papel da mídia na transmissão de informações sobre segurança cibernética ao público, desse modo moldando seus valores, atitudes e comportamentos online.

Estágio: Formativo

A cobertura da segurança cibernética na mídia brasileira é adhoc, com informações e reportagens limitadas sobre questões específicas que as pessoas enfrentam on-line, como a proteção à criança on-line. Um exemplo de cobertura da segurança cibernética pela mídia social é a do Facebook:[94] O Facebook criou, em 2016, um "centro" para prevenir o assédio virtual no Brasil, em parceria com o UNICEF e a Safernet. Os participantes mencionaram também que há pouca discussão sobre a segurança cibernética nas mídias sociais. Existem grupos sem fins lucrativos que debatem a questão das mídias sociais no Brasil. No entanto, alguém teria de se interessar por esse tema para receber essas informações. Normalmente, os casos de incidentes cibernéticos são comunicados pela imprensa, pela televisão, pelo rádio e pela mídia digital, e também se divulga orientação.

Entretanto, as partes interessadas salientaram que nenhum incidente grave teve impacto na infraestrutura crítica nacional no Brasil, que pudesse levar a uma cobertura mais ampla da mídia e da mídia social.

Resultados do processo de validação realizado em março de 2019

Resultados do processo de validação realizado em março de 2019

Recomendações

Com base nas consultas, as seguintes recomendações são formuladas para consideração, no que diz respeito à maturidade da cultura cibernética e sociedade. Essas recomendações visam a mostrar os próximos passos que poderão ser seguidos para aprimorar a capacidade atual de segurança cibernética, de acordo com as considerações do CMM do Centro.

Mentalidade de segurança cibernética

R 2.1
Intensificar os esforços em todos os níveis do Governo, especialmente junto aos funcionários públicos, e do setor privado para empregar boas práticas (proativas) de segurança cibernética. Projetar sistemas que permitam aos usuários em toda a sociedade inserir práticas seguras mais facilmente em seu uso cotidiano da Internet e dos serviços on-line.

R 2.2
Desenvolver programas coordenados de treinamento para funcionários do setor público.

R 2.3
Promover cooperação intersetorial e intercâmbio de informações sobre riscos de segurança cibernética e rotina de melhores práticas entre organizações dos setores público e privado.

R 2.4
Identificar grupos vulneráveis e comportamentos de alto risco em toda a sociedade, para fundamentar campanhas de conscientização específicas e coordenadas.

Confiança na internet

R 2.5
Estabelecer programas de ISP para promover a confiança em seus serviços, com base em medidas de eficácia desses programas.

R 2.6
Implementar mecanismos de realimentação, para garantir que os serviços eletrônicos sejam continuamente aprimorados, desse modo reforçando a confiança entre os usuários.

R 2.7
Empregar processos de coleta de informações dos usuários nas agências governamentais, de forma a garantir uma gestão eficiente do conteúdo on-line.

Entendimento do usuário sobre a proteção de informações pessoais on-line

R 2.8
Promover a compreensão da proteção de informações pessoais on-line entre os usuários, além do desenvolvimento de suas competências para gerenciar sua privacidade on-line.

R 2.9
Incentivar um debate público sobre a proteção de informações pessoais e sobre o equilíbrio entre segurança e privacidade, com vistas a embasar a formulação de políticas.

R 2.10
Promover o cumprimento das normas da Internet que protegem o anonimato dos usuários.

R 2.11
Desenvolver políticas de consentimento do usuário destinadas a notificar práticas sobre a coleta, uso ou divulgação de informações pessoais sensíveis.

Mecanismos de informação

R 2.12
Desenvolver programas para promover a utilização, pelos setores público e privado, dos mecanismos de informação em vigor para a denúncia de fraude digital, assédio virtual, abuso infantil on-line, roubo de identidade, violação de privacidade e segurança e outros incidentes.

R 2.13
Incentivar as diferentes partes interessadas (setores público e privado, polícia, CERT) a coordenar os mecanismos de informação e suas funções e responsabilidades, e a colaborar e partilhar boas práticas para aprimorar os mecanismos.

R 2.14
Utilizar métricas de eficácia para todos os mecanismos existentes e garantir que contribuam para a melhoria desses mecanismos.

Mídia e mídia social

R 2.15
Incentivar os provedores de mídia e mídia social a estender a respectiva cobertura, indo além da cobertura de ameaças, e a se concentrar em informar o público sobre medidas de segurança cibernética proativas e implementáveis, bem como sobre impactos econômicos e sociais.

R 2.16
Encorajar um debate frequente sobre segurança cibernética nas redes sociais.

R2.17
Assegurar que o debate na mídia e na grande mídia, e as atitudes expressas, fundamentem a formulação de políticas.

Dimensão 3

EDUCAÇÃO, TREINAMENTO E COMPETÊNCIAS EM SEGURANÇA CIBERNÉTICA

Essa dimensão analisa a disponibilidade de programas de conscientização sobre segurança cibernética, tanto para o público quanto para os executivos. Além disso, avalia a disponibilidade, a qualidade e a aceitação de ofertas educacionais e de treinamento para diversos grupos de interesse do governo, do setor privado e da população como um todo.

D 3.1 - Conscientização

Esse fator se centra na prevalência e na elaboração de programas que conscientizam sobre os riscos e ameaças da segurança cibernética, bem como na forma de enfrentá-los, tanto para o público em geral quanto para a gerência executiva.

Estágio: Formativo – Estabelecido

Estabelece-se um programa nacional de conscientização da segurança cibernética, liderado por uma organização específica (de qualquer setor) e que considera uma ampla gama de dados demográficos.

Devido à participação limitada da sociedade civil, não foi possível obter uma imagem clara das iniciativas de conscientização sobre segurança cibernética.

No decorrer da análise, o órgão de conscientização mais importante reconhecido pelos participantes foi a SaferNet Brasil, uma ONG criada em 2005.[95] A SaferNet Brasil tem firmado parcerias únicas com o Ministério da Justiça, a Polícia Federal e

a Secretaria de Direitos Humanos do Gabinete do Presidente da República, que lhe permitem proteger os direitos humanos e servir como linha direta, linha de ajuda e nodo de conscientização no Brasil.[96] Administra uma linha de assistência, que recebe reclamações anônimas sobre crimes e violações dos direitos humanos na Internet.[97] Além disso, a SaferNet participa da organização de campanhas de conscientização por meio de instituições educacionais em todo o Brasil.[98] Em 2008, a SaferNet estendeu a cooperação a empresas de tecnologia, como o Google, mediante a celebração de um acordo de cooperação que permite o monitoramento e o rastreamento de crimes de pornografia infantil.[99]

O Comitê Gestor da Internet no Brasil (www.cgi.br) – um conselho de diversas partes interessadas, criado pela Portaria Interministerial 147, de 31 de maio de 1995 – é a principal instituição responsável pela promoção de normas de segurança de TIC e melhores práticas na Internet,[100] e executa suas atividades por intermédio do Núcleo de Informação e Coordenação do Ponto BR (NIC.br) (http://nic.br/quem-somos/).[101] Com base em pesquisa documental, o NIC.br implementa diversas iniciativas, como a Antispam.br[102] (http://www.antispam.br/)[103] e a InternetSegura.br (https://www.Internetsegura.br/), ambos portais dedicados à conscientização de pais e filhos sobre spam, mediante a divulgação de materiais sobre segurança na Internet. Além disso, a CERT.br, em colaboração com o CGI.br e o NIC.br, vem promovendo e divulgando materiais de conscientização (e-books, slides) para o público (https://cartilha.cert.br/), mas especialmente desenhado para professores e crianças, com temas como redes sociais, senhas, dispositivos móveis e comércio eletrônico.[104](Para mais informações sobre os projetos do NIC.br relacionados à capacitação profissional, ver D 3.3). Um dos participantes mencionou que existem algumas atividades internas de conscientização para o pessoal administrativo das instituições federais, mas que não estão disponíveis ao público. Alguns participantes observaram que atividades de conscientização focadas no uso seguro da Internet, e destinadas às escolas públicas e privadas, foram realizadas entre 2009 e 2013. Aduziu-se que, em 2015, o Ministério Público Federal lançou um projeto denominado Ministério Público Federal pela Educação Digital nas Escolas, para realizar workshops nas universidades (para 200 professores e alunos) e distribuir folhetos e materiais.[105] Após o workshop, os professores foram incentivados a levar os materiais distribuídos pelo Ministério Público Federal e a formular comentários por meio do site da SaferNet. Em 2018, os mesmos workshops foram ministrados nas universidades, mas dirigidos a profissionais e psicólogos.

Com relação à conscientização dos executivos sobre segurança cibernética, os participantes reconheceram que a alta administração muitas vezes não tem consciência de como os riscos da segurança cibernética afetam suas organizações, e precisa ser informada sobre o assunto. Por exemplo, na Federação das Indústrias do Estado de São Paulo (FIESP), existe um departamento de segurança que orienta o debate sobre segurança cibernética.[106] Além disso, a Brasscom (Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação) organiza eventos cibernéticos para promover o setor de TIC junto às autoridades públicas e clientes públicos e privados.[107] Isso não envolve a participação das principais organizações internacionais, instituições financeiras e empresas de telecomunicações, nas quais as implicações estratégicas da segurança cibernética são prioridade. Algumas iniciativas de conscientização foram disponibilizadas para os conselhos de administração, mas carecem de programas específicos. Além disso, os executivos não são obrigados a participar de treinamentos sobre segurança cibernética, embora isso seja considerado uma boa prática. De acordo com o modelo para empresas públicas ou estatais, o Governo nomeia os diretores e exige que dois dos executivos nomeados sejam da empresa. Um dos participantes destacou que, normalmente, no caso de empresas de tecnologia, os dirigentes selecionados não têm conhecimento prévio de como essa empresa funciona. Isso muitas vezes leva a má administração, uma vez que o executivo é nomeado com base em filiações políticas. Entretanto, uma das empresas públicas

de tecnologia vem planejando estabelecer regras internas para retificar esse procedimento, e os membros do conselho nomeados são selecionados com base em seus conhecimentos e experiência de segurança cibernética. Aduziu-se que a política de segurança da empresa estatal está diretamente ligada ao Gabinete do Presidente da República, para prestar apoio e oferecer diretrizes aos principais dirigentes.

Além disso, os participantes destacaram a importância de distinguir as empresas de TI das empresas de segurança da informação no Brasil, já que, em sua opinião, as empresas não falam a mesma língua. Uma empresa de TI está mais comprometida com a satisfação e fidelidade do cliente, mas acontece o contrário com uma empresa de segurança da informação, razão pela qual são tomadas medidas diferentes para preencher a lacuna entre os objetivos comerciais e a segurança de TI. Muitas vezes, quando a nova gestão assume, o pessoal de TI tem que se adaptar aos aspectos mais avançados da empresa. Isso significa que cursos de treinamento internos de conscientização são oferecidos à nova direção executiva (por exemplo, para esclarecer a importância da segurança cibernética e das normas de segurança da informação). Um dos participantes revelou que em sua empresa há 24 normas de segurança e quatro procedimentos para orientar esses processos.

Um dos desdobramentos após a avaliação de março de 2018 foi a introdução da Política Nacional de Segurança da Informação (Decreto Presidencial No 9.637), em dezembro de 2018; o decreto estabelece que é responsabilidade do Gabinete de Segurança Institucional da Presidência da República "elaborar e implementar programas sobre segurança da informação destinados à conscientização e à capacitação dos servidores públicos federais e da sociedade."[108] Não é claro, portanto, até que ponto as atividades de conscientização conduzidas pelo Gabinete de Segurança Institucional da Presidência da República se sobrepõem às atividades de conscientização do NIC.br.[109]

Resultados do processo de validação realizado em março de 2019

Em 2019, representantes do setor acadêmico participaram do seminário de validação e confirmaram em grande parte os resultados do relatório da CMM de 2018.

D 3.2 Estrutura para a Educação

Esse fator considera a importância da oferta de educação de alta qualidade em segurança cibernética e a existência de educadores qualificados. Também analisa a necessidade de melhorar a educação em segurança cibernética em âmbito nacional e institucional, e a colaboração entre o Governo e a indústria, com vistas a garantir que os investimentos educacionais atendam às necessidades do ambiente de segurança cibernética em todos os setores.

Estágio: Formativo

Devido à ausência de participação do setor acadêmico, não foi possível obter uma imagem clara sobre a educação em segurança cibernética no Brasil. Portanto, as informações abaixo são baseadas em pesquisa documental.

A necessidade de melhorar a educação em segurança cibernética nas escolas e universidades foi identificada pelos principais atores governamentais e industriais.

O Ministério da Educação (MEC) estabelece o currículo nacional de cursos e requisitos e normas relacionados à segurança cibernética, mas a decisão sobre o nível de desenvolvimento desse currículo nacional cabe às universidades. O currículo não é regulamentado por uma agência central. O Ministério da Educação organiza um Catálogo Nacional dos Cursos Superiores de Tecnologia, que estabelece os requisitos para a criação de programas relacionados à segurança cibernética, tais como defesa cibernética e segurança da informação.[110] O catálogo apresenta a carga mínima de trabalho e a infraestrutura recomendada para cada curso.[111] A análise não revelou a existência de orçamento nacional distinto alocado à educação em segurança cibernética. Da mesma forma, não ficou claro, a partir dos debates do grupo de discussão, até que ponto existe cooperação entre o setor privado e as universidades.

Há pronta disponibilidade de educadores qualificados em segurança cibernética, porquanto são oferecidos, no Brasil, cursos especializados de pós-graduação em segurança cibernética em nível universitário. Um dos participantes salientou que há laboratórios na maioria das universidades que oferecem cursos em ciência da computação. A Universidade de São Paulo oferece um bacharelado em Ciência da Computação, Física da Computação e Engenharia da Computação, bem como mestrados e doutorados em Ciência da Computação.[112] A Universidade Federal do ABC também oferece programas de mestrado e doutorado em Ciência da Computação, subordinados ao Programa de Pós-Graduação em Ciência da Computação.[113] As áreas de pesquisa abrangem Computação Aplicada e Científica, Fundamentos da Computação e Sistemas de Computação.[114]

Além das universidades privadas, a Rede Nacional de Ensino e Pesquisa (RNP) também oferece cursos de pós-graduação em segurança cibernética.[115] Além disso, todos os anos a RNP organiza o Dia Internacional da Segurança Informática (DISI), que é gratuito, aberto ao público e transmitido ao vivo.[116] O Serviço Nacional de Aprendizagem Comercial (SENAC), instituição privada sem fins lucrativos, oferece cursos de pós-graduação em defesa cibernética, a fim de apoiar esse setor em particular.[117]

De acordo com o relatório da Trend Micro sobre o crime cibernético clandestino no Brasil, a tendência de hackers é preocupante, pois "realmente oferecem tutoriais e cursos para aspirantes a criminosos cibernéticos por um alto preço (por exemplo, vídeos de treinamento, tutoriais do Skype)."[118]

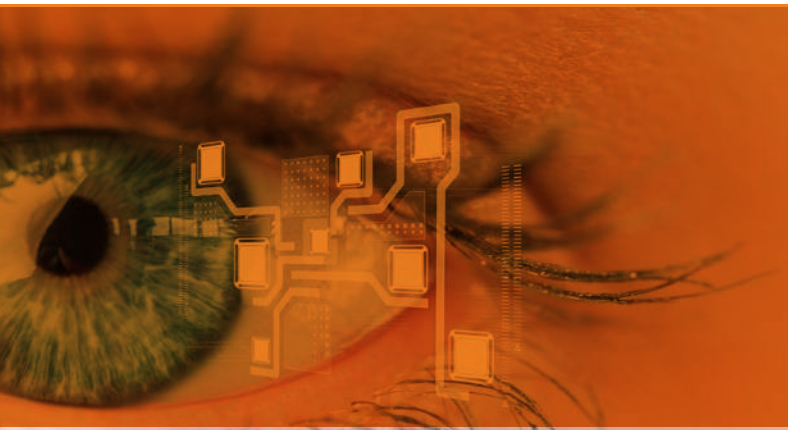
Atualmente, existe um debate nacional sobre que aspectos da segurança cibernética devem ser ensinados aos alunos do ensino fundamental e médio. O currículo atual faz uma pequena referência aos sistemas de TI, mas principalmente no contexto do uso da mídia digital e das tecnologias da informação para divulgar o conhecimento adquirido.[119]

Não foram prestadas informações sobre o envolvimento exato das partes interessadas no tocante à definição de prioridades para o programa de educação em segurança cibernética. Por ser esse tema ainda muito incipiente, as prioridades ainda não são discutidas, mas os procedimentos de implementação, sim.

Resultados do processo de validação realizado em março de 2019

Em 2019, representantes do setor acadêmico participaram do seminário de validação e confirmaram em grande parte os resultados do relatório da CMM de 2018.

D 3.3 - Estrutura para a Formação Profissional



Esse fator aborda a disponibilidade e a oferta de programas de treinamento em segurança cibernética, visando à criação de um quadro de profissionais em segurança cibernética. Esse fator também analisa o consumo do treinamento em segurança cibernética e a transferência horizontal e vertical do conhecimento em segurança cibernética nas organizações, e como isso se traduz em desenvolvimento contínuo de competências.

Estágio: Formativo

A necessidade de formar profissionais em segurança cibernética foi reconhecida pelo Governo.

Segundo pesquisa documental, o CGI.br (ver D 3.1) coordena os esforços de treinamento por meio do CERT.br, do Portal de Boas Práticas (BCP.nic.br) e do CGSIC. Por exemplo, o CERT.br, como parceiro CME CERT, está autorizado a oferecer programas de treinamento profissional, como os "Fundamentos do Tratamento de Incidentes", "Tratamento Avançado de Incidentes para Pessoal Técnico" e "Visão Geral da Criação e Gerenciamento de Equipes de Resposta a Incidentes de Segurança Informática".[120] Também o BCP.nic.br reúne um conjunto de boas práticas operacionais para administradores de sistemas.[121] O portal nacional é mantido por profissionais de diversas áreas do NIC.br, tais como o CERT.br,

o Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações (CEPTRO.br) e o Registro.br, em colaboração com especialistas de fora do NIC.br. [122]Além disso, o CGSIC oferece um curso de "Gestão de Segurança da Informação e Comunicações".[123]

Os participantes declararam que a maioria dos profissionais do setor público adquire qualificações profissionais de TI no exterior e recebe certificados de TIC, como o Certificado Profissional de Segurança de Sistemas de Informação (CISSP) e o de Gerente Certificado de Segurança da Informação (CISM). Quanto às acreditações técnicas, um dos participantes mencionou que o curso de medicina legal on-line oferecido pelo CERT.br é caro, mas vantajoso.[124]

Segundo pesquisa documental, o Comando de Defesa Cibernética (ComDCiber), no âmbito do Exército Brasileiro e em cooperação com a Escola Nacional de Defesa Cibernética, oferece a executivos civis e militares de recursos humanos o treinamento necessário para combater ataques cibernéticos de forma eficaz.[125] Do mesmo modo, instituições financeiras, como a Fundação Bradesco (um banco nacional), oferece cursos de segurança da informação.[126]

O COBIT tem sido aceito como "um padrão de facto para boas práticas em todo o Brasil, em organizações privadas, públicas e governamentais".[127] O Tribunal de Contas da União (TCU) realizou pesquisas, relatórios e iniciativas de auditoria sobre o uso e a aceitação da estrutura, e há um número crescente de cursos e certificações disponíveis de TI, tanto para profissionais quanto para servidores públicos.[128] Para complementar o COBIT, a ISO 27000 também é utilizada como referência. Cursos relacionados ao gerenciamento de informações são oferecidos na esfera do governo federal: quatro cursos ao longo de dois anos. O CISSP é a certificação mais renomada e reconhecida disponível, juntamente com o treinamento de resposta a incidentes oferecido pelo Instituto SANS.

Os participantes sugeriram que é grande a demanda por mais profissionais de segurança cibernética no Brasil. A maioria dos participantes confirmou que o consumo de cursos de segurança cibernética é alto e que as empresas privadas em geral treinam seu próprio pessoal internamente.

Resultados do processo de validação realizado em março de 2019

Em 2019, os participantes das entrevistas em grupo nos informaram sobre outros provedores de educação profissional (por exemplo, a Febraban, uma federação de bancos brasileiros),[129] porém não foi registrada mudança alguma na maturidade da capacidade de segurança cibernética do Brasil.

Recomendações

Após as informações apresentadas sobre a análise da maturidade da educação, do treinamento e das competências em segurança cibernética, o seguinte conjunto de recomendações é apresentado ao Brasil. Essas recomendações têm por objetivo oferecer assessoramento e sugerir as etapas a serem seguidas para o aprimoramento da atual capacidade de segurança cibernética, seguindo as considerações do CMM do Centro.

Conscientização

R 3.1
Nomear uma organização específica (por exemplo, a RNP) com mandato para desenvolver e implementar um programa nacional de conscientização sobre segurança cibernética. Coordenar e cooperar com as principais partes interessadas de todos os setores.

R 3.2
Desenvolver um programa especial de conscientização para os gerentes executivos dos setores público e privado, por ser esse grupo geralmente o árbitro final dos investimentos em segurança. O programa poderia ter por objetivo destacar a responsabilidade e a responsabilização dos dirigentes executivos e diretores de segurança cibernética.

R 3.3
Promover esforços de conscientização do gerenciamento de crises de segurança cibernética no nível executivo.

R 3.4
Promover a conscientização dos riscos e ameaças em todos os níveis do Governo.

R 3.5
Promulgar medidas de avaliação para estudar a eficácia dos programas de conscientização em um nível em que fundamentem campanhas futuras, levando em conta as lacunas ou falhas.

R 3.6
Promover discussões que destaquem o papel central e próprio das informações e da segurança cibernética em todas as empresas e operações de TI, considerando os riscos futuros.

Estrutura para a educação

R 3.7
Desenvolver programas educacionais de segurança cibernética para instrutores de segurança cibernética, a fim de garantir que pessoal qualificado esteja disponível para ministrar os cursos de segurança cibernética recém-criados.

R 3.8
Criar cursos de graduação e pós-graduação credenciados em segurança cibernética, além dos demais cursos de segurança cibernética existentes nas diversas universidades do Brasil.

R 3.9
Promover ações de universidades e outros órgãos para realizar seminários e palestras sobre questões de segurança cibernética, destinados a não especialistas.

R 3. 10
Incorporar cursos especializados em segurança cibernética a todos os cursos de informática nas universidades e oferecer cursos especializados em segurança cibernética nas universidades e outros órgãos de ensino superior.

R 3.11
Coletar e avaliar informações dos atuais alunos, com vistas a um maior desenvolvimento e aprimoramento das ofertas de cursos de segurança cibernética.

R 3.12
Criar iniciativas para fazer avançar a educação em segurança cibernética nos currículos das escolas de nível fundamental e médio.

R 3.13
Firmar parcerias para o desenvolvimento de interfaces de pesquisa, inovação e interação entre as universidades e o setor privado.

R 3.14 Assegurar a sustentabilidade dos programas de pesquisa.

R 3.15 Desenvolver métricas eficazes para garantir que os investimentos no aprimoramento da educação e das competências atendam às necessidades do ambiente de segurança cibernética.

R 3.16
Reunir estatísticas sobre a oferta e a demanda de profissionais graduados em segurança cibernética.

Estrutura para a formação profissional

R 3.17
Estabelecer programas de treinamento em segurança cibernética mais acessíveis e estruturados, com vistas ao desenvolvimento de competências para a construção de uma estrutura de profissionais específicos de segurança cibernética.

R 3.18
Estabelecer treinamento contínuo para funcionários de TI e funcionários em geral quanto a questões de segurança cibernética, em todos os setores.

R 3.19
Desenvolver métricas para avaliar a aceitação e o sucesso dos cursos de treinamento em segurança cibernética.

R 3.20
Criar um programa de intercâmbio de conhecimentos, visando a maior cooperação entre os provedores de treinamento e o meio acadêmico.

R 3.21
Garantir que certificação profissional de segurança seja oferecida, de maneira acessível, em todos os setores do país.

R 3.22
Desenvolver uma plataforma central para o intercâmbio de informações de treinamento para especialistas e criar um registro nacional de especialistas em segurança cibernética.

R 3.23
Estabelecer requisitos para o treinamento conjunto em segurança cibernética para os setores público e privado, e desenvolver plataformas de treinamento colaborativo.

R 3.24
Criar iniciativas para desenvolver uma abordagem rápida para a construção de capacidade cibernética.

R 3.25
Estabelecer iniciativas para promover a atratividade da profissão de segurança cibernética, com vistas a incentivar os empregadores a treinar os empregados para que se tornem profissionais de segurança cibernética.

R 3.26
Desenvolver um quadro de competências em segurança cibernética ou utilizar um quadro de competências existente no país para definir trajetórias de carreira claras para especialistas em segurança cibernética.

Revisão Da Capacidade De Cibersegurança

República Federativa do Brasil

Dimensão 4

ESTRUTURAS JURÍDICAS E REGULAMENTARES

Essa dimensão analisa a capacidade do Governo de elaborar e promulgar legislação nacional direta e indiretamente relacionada à segurança cibernética, com destaque especial para os temas de segurança das TIC, privacidade e proteção de dados, e outras questões relacionadas ao crime cibernético. A capacidade de fazer cumprir essa legislação é analisada mediante o cumprimento da lei, a ação penal e a capacidade dos tribunais. Essa dimensão também observa questões como as estruturas formais e informais de cooperação para combater o crime cibernético.

D 4.1 - Estruturas Jurídicas

Esse fator aborda a legislação e as estruturas regulamentares relacionadas à segurança cibernética, incluindo: estruturas legislativas de segurança das TIC; privacidade; liberdade de expressão e outros direitos humanos on-line; proteção de dados; proteção da criança; proteção do consumidor; propriedade intelectual; e legislação substantiva e processual sobre crimes cibernéticos.

Estágio: Estabelecido

No Brasil não há uma regulamentação abrangente que considere explicitamente a segurança cibernética. Apesar dos esforços por introduzir uma estrutura legislativa vinculante, a legislação sobre segurança cibernética no Brasil ainda se encontra em desenvolvimento. Como alternativa, foram adotadas várias diretrizes oficiais ou "leis não vinculantes" sobre questões de segurança cibernética.

As estruturas legislativas e as diretrizes mais relevantes relacionadas ao cenário da Internet no Brasil são:

- Lei de Crimes Cibernéticos (Lei n° 12.737/2012) (2012), também conhecida como "Lei Carolina Dieckmann";[130]
- Marco Civil da Internet (Lei n° 12.965) (2014); [131]
- Livro Verde sobre Segurança Cibernética no Brasil (2010);[132]
- Política Cibernética de Defesa (2012) Portaria No. 3.389; [133]
- Livro Branco sobre a Defesa Nacional (2012); [134]
- Estratégia Nacional de Defesa (2008); [135]
- Proteção da Infraestrutura Crítica de Informação e Comunicação (2010) [136]
- Anatel – Consulta Pública No. 21[137]

Legislação penal

Outras legislações sobre crimes cibernéticos são abordadas pelos seguintes instrumentos:

- Lei 8.137/1990, Art. 2
- Lei 9.296/1996, Art. 10
- Lei 11.829/2008
- Lei 8.069/1990, Art. 241
- Lei 9.504/1997
- Lei 12.735/2012, Art.4
- Lei 9.100/1995, Art. 67
- Lei 9.983/2000

Regulamentação e conformidade

Outros regulamentos relacionados à segurança cibernética são abordados pelos seguintes instrumentos:

- Portaria n°. 35/2009
- Decreto 3.505/2000
- Resolução n°. 614/2013, Art. 53
- Portaria n°. 45/2009
- Portaria n°. 34/2009
- Decreto 7.845/2012
- Resolução n°. 617/2013, Art. 47

(Adaptado de ITU, Perfil Cyberwellness, Brasil) [138]

A introdução de leis penais "de emergência" não é inédita na história do sistema jurídico brasileiro, particularmente quando os legisladores aprovam apressadamente essas leis, a fim de atender à demanda pública por justiça.[139]Da mesma forma, em 2012, a Lei de Crimes Cibernéticos[86] (Lei n° 12.737/2012), também conhecida não oficialmente como "Lei Carolina Dieckmann",[140] foi aprovada às pressas pelo Congresso e acrescentada ao Código Penal[141] para regulamentar o uso indevido de computadores. Os dois Artigos 154-A e 154-B que foram introduzidos referem-se a crimes cibernéticos, como invasão de computadores, uso indevido de dados de usuários ou eliminação de sites.

Invasão de dispositivo informático

> ***Artigo 154-A***
> *Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:*
>
> *Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.*

Ação penal

> ***Artigo 154-B.***
> *Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionarias de serviços públicos.*

O Artigo 154-A criminaliza a invasão de computadores e estabelece penas maiores se isso redundar em perda econômica e violação de dados.[142] No decorrer da análise, alguns participantes expressaram sua preocupação de que as penas sejam muito leves (três meses a um ano de prisão, além de multa). Esta é considerada uma atividade de baixo risco para o criminoso e incentiva o comportamento malicioso on-line.

O Artigo 154-B permite que a vítima decida se deve prosseguir com as acusações criminais, a não ser que o ataque tenha sido contra o Governo ou um órgão público.[143]

O Marco Civil da Internet[144] (Lei n° 12.965) foi desenvolvido por meio de um processo de consulta com diversas partes interessadas e com a participação da sociedade civil, ao longo de vários anos, e finalmente aprovado em 2014. A lei pretende regulamentar o uso da Internet no Brasil, mediante princípios, garantias, direitos e deveres para os usuários. A legislação considera diversas questões, incluindo a neutralidade da rede; a privacidade dos dados da Internet; a retenção de dados em relação à Internet; os direitos civis relacionados à Internet com obrigações para os usuários e provedores de serviços de Internet (ISPs); a liberdade de expressão, de manifestação e de comunicação.[146] Essa lei é, ademais, considerada pioneira na proteção dos direitos dos usuários da Internet e também limita de maneira estrita o acesso aos dados necessários para investigações.[146]

Em julho de 2018, o Brasil adotou a Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em fevereiro de 2020.[147] Do mesmo modo, o Brasil conta com várias disposições da Constituição Federal,[148] do Código Penal Brasileiro,[149] do Código de Defesa do Consumidor[150] e do Marco Civil da Internet no Brasil.

Marco Civil da Internet no Brasil

Seção II
Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

> ***Artigo 10.***
> *A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de*

comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

Artigo 11.
Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros..[151]

No decorrer da análise (março de 2018), muitos expressaram a necessidade de aprovação de um estatuto para a regulamentação da proteção de dados, o que finalmente ocorreu em julho de 2018.[152] O Marco Civil da Internet no Brasil aplica-se apenas a questões relacionadas à Internet.[153] Esse marco "protege dados pessoais (sem definir o que seria considerado dados pessoais), conteúdo de comunicação privada e registros de acesso, tanto para conexão à Internet quanto para aplicativos."[154] Além disso, de acordo com o Código Civil[155] Brasileiro, os diretores de uma organização podem ser responsabilizados em caso de negligência na proteção de redes e dados por parte da organização.[156] Apesar de a Lei Brasileira de Direitos Autorais[157] ter uma disposição específica sobre proteção de dados, refere-se apenas à proteção do titular.

O Projeto de Lei Geral de Proteção de Dados recentemente aprovado (o "Projeto de Lei") – inspirado no GDPR da UE – requer a criação de uma autoridade nacional de proteção de dados e a notificação de violações de dados à autoridade de proteção de dados.[158] Como não havia uma autoridade nacional de proteção de dados, as vítimas de violações de dados frequentemente apresentavam queixa contra um controlador de dados que poderia ser penalizado com base no Marco Civil da Internet no Brasil e na Lei Carolina Dieckmann, além de incorrer em responsabilidade civil.[159]

Pode-se considerar que o Brasil ocupa posição de vanguarda em direitos digitais, com a adoção do Marco Civil da Internet no Brasil (também chamado de Carta de Direitos da Internet no Brasil), em 2014, que pretende proteger a privacidade e os direitos de livre expressão on-line.[160] Ademais, em 2015, o Brasil "copatrocinou uma iniciativa no Conselho de Direitos Humanos das Nações Unidas para a criação de uma nova relatoria especial da ONU sobre o direito à privacidade."[161] Apesar da implementação dessa histórica estrutura legislativa, protegendo de forma abrangente os direitos humanos on-line, de acordo com a Human Rights Watch, houve algumas violações que ameaçaram o direito à privacidade no Brasil. Por exemplo, em 2015, as empresas de telefonia móvel receberam uma ordem judicial para bloquear temporariamente o WhatsApp (o serviço de mensagens do Facebook) por dois dias.[162] Em seguida, em 2016, um executivo do Facebook foi preso pela polícia federal porque a empresa negou às autoridades o acesso aos dados dos usuários.[163]

Legislação abrangente sobre a proteção de crianças on-line foi adotada e aplicada:

- Artigos 240* e 241A–E* da Lei 11.829/2008 que emendaram o Estatuto da Criança e do Adolescente – ECA (Lei N°. 8.069/90) em 2008; [164] [165]

- Artigos 218, 218A, 218B* do Código Penal, emendados e incorporados pela Lei N°. 12015/2009, em 2009 [166]

Além disso, "os Artigos 17, 18, 143 e 247 do Estatuto da Criança e do Adolescente estabelecem disposições para proteger a imagem e a reputação de crianças e adolescentes, punindo qualquer pessoa que os exponha de forma negativa ou lesiva".[167] O Artigo 241–D do ECA define o aliciamento on-line e impõe uma pena de um a três anos de prisão por esse crime.[168] Alguns participantes criticaram essa pena, por eles qualificada como muito branda, e manifestaram preocupação com a falta de legislação para criminalizar o assédio virtual, o envio de mensagem sexual e o acesso imagens de pornografia infantil ou o download dessas imagens. Da mesma forma, na legislação

brasileira, não é obrigatória a denúncia de suspeita de pornografia infantil aos ISPs, a não ser que recebam uma notificação oficial para negar o acesso a imagens de abuso infantil.[169] Além disso, a Convenção sobre os Direitos da Criança foi assinada e ratificada pelo Brasil, sem declarações ou reservas sobre os Artigos 16, 17(e) e 34(c).[170] Do mesmo modo, o Protocolo Facultativo à Convenção sobre os Direitos da Criança sobre a Venda de Crianças, Prostituição Infantil e Pornografia Infantil foi assinado e ratificado, sem declarações ou reservas sobre os Artigos 2o e 3o.[171]

O Brasil neste momento carece de legislação que considere explicitamente as ameaças cibernéticas à PI. Entretanto, a Lei de Direitos Autorais (Lei n° 9.610/1998)[172] garante a proteção de qualquer tipo de produto intelectual, independentemente de ser registrado ou publicado.[173] Além disso, a proteção da PI de um programa de computador é regulamentada pela Lei de Proteção da Propriedade Intelectual de Programa de Computador (Lei n° 9.609/1998).[174]

As empresas na Internet são regulamentadas pela Lei da Internet[175] (Lei n° 12.965/2014), o decreto que a regulamenta[176] (Decreto n° 8.771/2016) e o Código de Proteção ao Consumidor[177] (Lei n° 8.078/1990), que se aplica a todos os consumidores e fornecedores de serviços ou bens.[178] Os Escritórios de Proteção ao Consumidor são responsáveis pelos direitos dos consumidores. O Código de Proteção ao Consumidor garante o direito do indivíduo de "acessar todos os dados armazenados sobre si mesmo e solicitar alterações, correções e até mesmo sua eliminação de um banco de dados".[179] A falta de acesso do consumidor às informações a seu respeito está sujeita a uma pena de prisão ou a multa.[180] A Agência Nacional de Telecomunicações (Anatel) regulamenta o acesso à Internet e tem o poder de eliminar abusos e estabelecer diretrizes; por exemplo, a obrigação de notificar oportunamente os clientes sobre os preços cobrados.[181]

A Lei de Crimes Cibernéticos (Lei No. 12.737/2012)[86] e o Marco Civil da Internet no Brasil (Lei No. 12.965)[182] (2014) são consideradas as legislações substantivas mais relevantes atualmente em vigor para considerar formalmente os crimes cibernéticos e outorgar poderes processuais ao abordar provas eletrônicas (Figura 4).

Figura 4: *Linha do tempo da legislação de crimes cibernéticos no Brasil*

Alguns participantes salientaram que o problema não é a legislação propriamente dita, mas a aplicação e a capacidade de resposta. Apesar do debate político em andamento sobre essas questões, ainda há lacunas legislativas no processo de implementação, que o Brasil deve superar. Um participante observou que:

> *"Por exemplo, a Lei Carolina Dieckmann foi introduzida por causa do questionamento da mídia sobre o que aconteceu. Nós não temos o mesmo nível de compromisso. O progresso da legislação deve evoluir continuamente, no entanto, ainda está atrasado em relação aos criminosos cibernéticos. A mídia às vezes revela eventos cibernéticos, mas qual deveria ser a norma e a linha de pensamento ao legislar? Nós ainda não estamos no patamar almejado".*

Portanto, a falta de aplicação da legislação de crimes cibernéticos e as punições brandas tendem a incentivar os criminosos cibernéticos.

O phishing foi outra preocupação suscitada por um participante, pois não é penalizado no Brasil, e não é considerado atividade criminosa. O participante argumentou que muitos consideram o phishing apenas uma preparação – apontar uma arma de fogo para alguém, mas não usá-la. A discussão técnica na esfera jurídica é dificultada pelo desconhecimento das tecnologias de TI. Geralmente, os advogados não compreendem a gravidade dos casos (por exemplo, vazamento de informações ou fraude on-line) e, portanto, não acham que isso seja um problema.

O Brasil ainda não assinou a Convenção do Conselho da Europa (CoE) sobre Crimes Cibernéticos. Entretanto, alguns participantes ressaltaram a necessidade de o Brasil aderir à Convenção.

Resultados do processo de validação realizado em março de 2019

O panorama legislativo não mudou significativamente desde a análise do CMM de 2018. Mais uma vez, os participantes das entrevistas do grupo de discussão de 2019 salientaram a necessidade de o Brasil assinar a Convenção sobre Crimes Cibernéticos; algumas discussões internas ocorreram entre várias entidades do Governo. Em dezembro, após as entrevistas do grupo de discussão, em março de 2019, o Brasil iniciou o processo de adesão à Convenção de Budapeste, como observador.

Um acréscimo notável ao panorama legislativo brasileiro é a Lei Geral de Proteção de Dados, promulgada em agosto de 2018. Em dezembro de 2018, foi publicada a Medida Provisória n° 869/2018, que altera a Lei Geral de Proteção de Dados e cria a Autoridade Nacional de Proteção de Dados. De acordo com a referida alteração, a Lei de Proteção de Dados deverá entrar em vigor em agosto de 2020.

Da mesma forma, a Lei de Importunação Sexual (n° 13.718), que entrou em vigor em setembro de 2018 para alterar o Código Penal (Decreto-Lei n° 2.848, de 7 de dezembro de 1940), criminaliza a prática de ato libidinoso (não consensual) e a divulgação de cena de estupro, que anteriormente era apenas um delito criminal.[183] A nova lei prevê penas como a prisão de um a cinco anos.[184] Isso revoga as disposições da Lei das Contravenções Penais (Decreto-Lei n° 3.688, de 3 de outubro de 1941). A Lei de Importunação Sexual representa um avanço significativo no combate à pornografia de vingança que "inclui a divulgação de cena de sexo, nudez ou pornográficas, em forma de vídeo ou foto, sem o consentimento da vítima".[185]

Lei de Importunação Sexual (N°. 13.718)

Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia

Artigo. 218-C.
Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia:

Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.

Por último, mas não menos importante, os participantes das entrevistas do grupo de discussão de 2019 salientaram várias iniciativas destinadas a modernizar a legislação em vigor (incluindo a Lei de Crimes Cibernéticos) e a garantir que ela aborde adequadamente a segurança cibernética, embora nenhuma nova legislação relacionada à segurança cibernética esteja prevista para 2019.

D 4.2 - Sistema de Justiça Criminal

Esse fator estuda a capacidade dos órgãos de aplicação da lei de investigar crimes cibernéticos e a capacidade da acusação de apresentar casos de crimes cibernéticos e provas eletrônicas. Finalmente, esse fator aborda a capacidade do tribunal de presidir casos de crimes cibernéticos e aqueles que envolvam provas eletrônicas.

Estágio: Formativo

Em todo o sistema de justiça criminal, a capacidade se localiza entre o estágio inicial e formativo de maturidade no Brasil.

A principal autoridade reguladora, que implementa normas de segurança cibernética no Brasil, é o Ministério da Justiça, por intermédio do Ministério Público Federal e do Departamento de Polícia Federal.[186]

A URCC da Polícia Federal, com sede em Brasília, é o principal agente de cumprimento da lei encarregado do combate ao crime cibernético, desempenhando, portanto, papel operacional fundamental na perseguição dos criminosos cibernéticos, tanto dentro como fora das fronteiras do Brasil.[187] Entre suas competências, a unidade participa da investigação de fraudes eletrônicas (e-banking e fraudes com cartão de crédito), de redes criminosas de apoio ao abuso infantil on-line, do acesso não autorizado a sistemas e redes de TI e também da abordagem de crimes contra instituições públicas federais.[188] Foi reconhecido no decorrer da análise que a Polícia Federal tem um bom histórico no combate à fraude bancária e à pornografia infantil on-line.

Os participantes expressaram várias preocupações que a comunidade de cumprimento da lei enfrenta no tocante à aplicação das leis de crimes cibernéticos:

- falta de um nível adequado de treinamento e certificações em muitas das instituições necessárias para a condução de processos, uma vez que os policiais têm conhecimento limitado de TI; a oferta de conhecimentos básicos de TI é, portanto, essencial para o sucesso da investigação (por exemplo, treinamento em ISPs, análise de código malicioso e atribuição de crimes cibernéticos);

- falta de recursos técnicos e financeiros para o pessoal mal treinado;

- transferência frequente de policiais convidados a participar de treinamentos sobre crimes cibernéticos em Brasília para outros lugares, o que dificulta a manutenção de policiais em áreas específicas de crimes cibernéticos;

- diferentes níveis de competências entre as unidades de crimes cibernéticos da Polícia Federal e as da Polícia Civil (pequeno orçamento, falta de ferramentas forenses avançadas, falta de treinamento específico);

- falta de confiança entre as agências de cumprimento da lei e empresas privadas para a realização de investigações de crimes cibernéticos;

- inexistência de padronização na coleta de provas digitais e procedimentos forenses;

- competência limitada na coleta de inteligência cibernética;

- necessidade de esclarecer os papéis e responsabilidades dos atores institucionais, a fim de administrar o crime cibernético em uma estrutura federal complexa.

A URCC mantém acordos principalmente informais com as agências de cumprimento da lei dos 26 estados brasileiros, para realizar investigações de crimes cibernéticos na esfera subnacional. Foi destacado durante a análise que, como os policiais só têm conhecimento básico de TI, especialistas em crimes cibernéticos do exterior são frequentemente chamados para colaborar nas investigações. Aliás, a Academia Nacional de Polícia oferece cursos e treinamento on-line de segurança cibernética para policiais federais.

O Brasil possui um laboratório digital forense localizado no Instituto Nacional de Criminalística (INC), na Polícia Federal, em Brasília.[189] Além disso, cada estado no Brasil criou seu próprio laboratório de TI com funções específicas, como decifrar dados criptografados de um telefone. Caso falte ao laboratório de TI estadual alguma competência, mantém-se contato com a URCC ou uma organização privada. Os participantes descreveram como muito eficientes a cooperação e o intercâmbio operacional de informações entre a Polícia Federal e a Polícia Civil Estadual. Um dos participantes reconheceu que não há, na Polícia Federal, qualquer restrição que impeça a troca de informações. Não há uma estrutura formal de intercâmbio de informações entre a Polícia Federal e a Polícia Civil Estadual, e a cooperação se baseia na confiança. Quanto à troca de informações de segurança entre os órgãos responsáveis pelo cumprimento da lei, o Brasil segue um enfoque descendente.

De acordo com a lei brasileira, os ISPs são obrigados a cooperar com as autoridades governamentais ao receberem pedidos oficiais (por exemplo, ordem judicial, mandado de busca, intimações) e a divulgar os dados dos clientes.[190] Uma vez recebido um pedido de uma autoridade competente, um juiz pode emitir um mandado ou ordem para realizar uma investigação em virtude da violação da lei.[191] O Marco Civil da Internet no Brasil garante que as restrições legais não limitarão a capacidade dos agentes da lei de exercer suas funções e de acessar dados pessoais, quando tenham autoridade legal para fazê-lo.[192] Igualmente, de acordo com o Código Brasileiro de Telecomunicações, nos termos da Lei 9.296/96, "a interceptação de sistemas de comunicação telefônica e de tecnologia da informação dependerá de ordem de juiz – se houver suspeita de que o perpetrador cometeu um crime e não existe outra forma de produzir provas."[193]

No decorrer da análise de 2018, não foi possível obter uma imagem clara da capacidade dos promotores e juízes de conduzir casos de crimes cibernéticos e casos envolvendo provas digitais. Com base em entrevistas de acompanhamento, a capacidade dos promotores e juízes de lidar com casos de crimes cibernéticos e casos envolvendo provas digitais foi considerada pelos participantes como ad hoc e não institucionalizada. O Brasil tem atualmente 1.000 promotores federais e 2.400 promotores. Não há tribunais especiais para considerar casos de crimes cibernéticos, nem juízes especializados em crimes cibernéticos. Os juízes recebem apenas o treinamento realizado para os promotores federais.

Em 2011, foi criado um grupo de trabalho especial sobre crimes cibernéticos, composto por oito promotores federais.[194] Novos promotores e juízes federais (desde 2015) são elegíveis para participar desse grupo de trabalho, mas o grupo está disponível apenas uma vez por ano. Isso impacta negativamente a eficácia das instituições do cumprimento da lei para lidar com casos de crimes cibernéticos. Caso sejam apresentados ao tribunal, há possibilidade de que as investigações e processos sejam ineficazes e, portanto, haja falha na condenação. Também foi destacado na análise que, em âmbito estadual, o maior problema é que o promotor estadual muitas vezes não tem o conhecimento nem a capacidade para realizar investigações de crimes cibernéticos. Além disso, há dificuldades quando os promotores solicitam dados digitais dos ISPs, em parte pelo fato de que o Brasil não consegue passar para a versão 6 do Protocolo Internet (IPv6). Hoje, os ISPs estão operando com IPv4, o que é insuficiente porque não há endereços IP suficientes no acervo de endereços IPv4. Portanto, os ISPs compartilham o mesmo endereço IP entre muitas pessoas, o que torna muito difícil identificar o verdadeiro criminoso. Uma sugestão foi tentar instituir normas sobre o número de pessoas que podem ter o mesmo IP. No momento, no Brasil, os ISPs fornecem o mesmo endereço IP para 32 pessoas.

O Brasil participa regularmente de treinamentos em crimes cibernéticos no exterior, patrocinados por órgãos regionais como o CoE e a OEA. Por exemplo, o Escritório do Programa de Crimes Cibernéticos da Europa (C-PROC) prestou ao Brasil apoio em legislação, treinamento judicial e policial e em desenvolvimento institucional.[195] Em julho de 2018, os promotores federais foram convidados a participar da Conferência Octopus sobre Crimes Cibernéticos, em Estrasburgo.[196] Um dos participantes acrescentou que procuradores federais e estaduais são convidados a participar de reuniões sobre crimes cibernéticos com a OEA – o Grupo de Trabalho sobre Delito Cibernético das uniões de Ministros da Justiça ou de outros Ministros ou Procuradores-Gerais das Américas (REMJA), em Washington D.C., a cada dois anos.[197]

Em 2018, a Microsoft Brasil assinou um acordo de cooperação com o Ministério Público de São Paulo (MPSP) para oferecer um programa de treinamento em crimes digitais aos promotores públicos e outras iniciativas relacionadas ao combate do crime on-line.[198]

Resultados do processo de validação realizado em março de 2019

Além de reafirmar os resultados da revisão do CMM, os participantes das entrevistas do grupo de discussão de 2019 destacaram treinamentos recentes para o judiciário. Também informaram os pesquisadores sobre a existência de equipes especializadas de promotoria em certos estados federativos. Apesar disso, os participantes foram de opinião que o Brasil ainda não dispõe de procuradores e juízes treinados em número suficiente para entregar à justiça um número crescente de criminosos cibernéticos.

Informações prestadas pelo Governo em 2020

Segundo a pesquisa documental realizada após as entrevistas dos grupos de discussão de março de 2019, a autoridade reguladora para crimes cibernéticos é o Ministério da Justiça e

Segurança Pública.[199] De acordo com o Artigo 10, Item V, da Lei n° 13.844, cabe ao Gabinete de Segurança Institucional da Presidência da República a responsabilidade por outras questões de segurança cibernética.[200] Isso não difere muito dos resultados da revisão da CMM de 2018 e, portanto, não altera a maturidade da capacidade de segurança cibernética do Brasil.

D 4.3 - Estruturas Formais e Informais de Cooperação Para Combater o Crime Cibernético

Esse fator aborda a existência e o funcionamento de mecanismos formais e informais que permitem a cooperação entre atores nacionais e estrangeiros para evitar e combater o crime cibernético.

Estágio: Formativo

As autoridades brasileiras reconheceram a necessidade de melhorar os mecanismos tanto formais quanto informais de cooperação, em âmbito interno e transfronteiriço, mas esses mecanismos continuam sendo ad hoc. Os participantes mencionaram concretamente que a cooperação na luta contra o crime cibernético é uma área com grandes dificuldades, especialmente no plano internacional.

A cooperação formal existe tanto entre países quanto entre agências. Uma parceria com o CICTE é um bom exemplo de cooperação interestatal, ao facilitar uma troca de informações sobre segurança cibernética além das fronteiras do Brasil.[201] Além disso, o blog SegInfo serve como programa nacional de divulgação de informações relacionadas à segurança cibernética (por exemplo, avisos de vulnerabilidade, últimos eventos e projetos) no setor público.[202] O Brasil é membro da iniciativa ITU-IMPACT e também participou da Reunião Regional de CSIRTs da América Latina e do Caribe organizada pelo Registro de Endereços da Internet para a América Latina e o Caribe (LACNIC).[203] Além disso, o CERT.br é membro do FIRST desde 2002.[204]

Já foi estabelecida cooperação informal e voluntária com ISPs multinacionais, uma vez que os ISPs não têm qualquer responsabilidade legal e não são obrigados a responder a solicitações de aplicação da lei, salvo se receberem uma solicitação oficial (por exemplo, uma ordem judicial ou um mandado de busca). Atualmente, o Brasil vem desenvolvendo um acordo bilateral entre os ISPs e as instituições de aplicação da lei, que permite aos ISPs compartilhar dados diretamente com essas autoridades. Por exemplo, em maio de 2018, o Escritório Central Nacional da INTERPOL (NCB) em Brasília e o Banco do Brasil S/A celebraram um acordo de cooperação e troca de informações, com vistas a combater o

crime cibernético. "Essa parceria público-privada promoverá uma troca sistemática de dados relacionados às ameaças cibernéticas."[205]

Entre os vários canais de cooperação internacional disponíveis, os compromissos com a INTERPOL, a Ameripol e a Europol foram descritos como os caminhos mais importantes para facilitar a cooperação transfronteiriça e a troca de informações. Segundo pesquisa documental, a URCC é incumbida da coordenação de "todas as redes internacionais de aplicação da lei para facilitar a troca de informações e gerenciar protocolos operacionais".[206] No nível operacional, a troca de informações com órgãos policiais e tribunais estrangeiros foi descrita como eficaz, mas surgem problemas ao solicitar informações dos ISPs no exterior e de empresas privadas de Internet (como Facebook e Google) nos Estados Unidos, uma vez que raramente respondem e evitam cooperar com as instituições de aplicação da lei no Brasil. Em outras palavras, é mais fácil solicitaR informações a empresas sediadas no Brasil porque são obrigadas a cumprir a lei brasileira. Outra preocupação suscitada no decorrer da análise foi uma questão relativa aos Tratados de Assistência Jurídica Mútua (MLATs), por sua lentidão, que atrasa as investigações. Muitas vezes são necessários até dois anos para obter uma resposta a um pedido oficial dos Estados Unidos, uma vez que esse país dispõe de poucos promotores que trabalham com os MLATs de todo o mundo.

A INTERPOL Brasília tem acesso ao link de comunicação seguro da INTERPOL, I-24/7, um portal de acesso restrito à Internet que oferece à polícia de todo o país acesso instantâneo e automatizado aos bancos de dados criminais da INTERPOL.[207] A rede I-24/7 é considerada uma cooperação informal, porquanto é utilizada apenas para trocar informações para fins de inteligência e não para coletar provas. Em 2017, o Brasil (a Polícia Federal do Brasil) e a Europol assinaram um acordo estratégico para expandir a cooperação no combate a atividades criminosas transfronteiriças, que poderia ser considerada uma cooperação formal.[208]

Um dos participantes acrescentou que o treinamento em crimes cibernéticos e os eventos internacionais relacionados aos crimes cibernéticos servem como outra plataforma para criar confiança e conexões entre as diferentes partes interessadas, com o intuito de possibilitar pedidos informais de apoio para preservar dados ou obter informações para determinar o melhor caminho a seguir. O Governo está em processo de tomar medidas para colocar o Brasil em situação legislativa para finalmente ratificar a Convenção de Budapeste sobre Crimes Cibernéticos.

Resultados do processo de validação realizado em março de 2019

Mais uma vez, os participantes das entrevistas de validação do grupo de discussão de 2019 destacaram que a colaboração entre os ISPs e as autoridades responsáveis pelo cumprimento da lei está em andamento, mas alguns ISPs ainda se recusam a colaborar. Uma questão é exacerbada, inter alia, pelo grande número de ISPs no país, muitos dos quais não dispõem de pessoal específico de TI e dependem de consultores externos para lidar com questões de segurança cibernética.

A cooperação entre o CERT.br e o CTIR Gov, por outro lado, experimentou provável melhora. O mesmo foi afirmado pelos entrevistados em 2019 sobre a cooperação entre os vários níveis das entidades de aplicação da lei no país; os papéis e responsabilidades entre as agências de cumprimento da lei estaduais e federais são claros e as relações são supostamente funcionais. Todas essas entidades têm um ponto de contato designado 24 horas por dia, o que contribui para que os entrevistados da análise-validação de 2019 a tenham avaliado como "boa comunicação".

Recomendações

Com base nas informações apresentadas sobre a análise da maturidade da estrutura legislativa e regulamentar da segurança cibernética, propõe-se o seguinte grupo de recomendações para o Brasil. Essas recomendações visam a sugerir medidas e passos a serem seguidos para o aprimoramento da capacidade existente de segurança cibernética, tendo como fundamento as considerações do CMM do Centro.

Estruturas jurídicas

R 4.1
Considerar o estabelecimento de um processo periódico de revisão e aprimoramento das leis brasileiras relacionadas ao ciberespaço para abordar a dinâmica das ameaças à segurança cibernética (por exemplo, assédio virtual, envio de mensagem sexual e acesso a imagens de pornografia infantil ou o download dessas imagens).

R 4.2
Desenvolver novas disposições legislativas mediante processos de consulta de diversas partes interessadas sobre PI on-line e direitos humanos on-line.

R 4.3
Promulgar a ordem de entrada em vigor da legislação existente e designar órgãos para monitorar o cumprimento da lei de segurança cibernética e do crime cibernético.

R 4.4
Destinar recursos para garantir o pleno cumprimento das leis de segurança cibernética existentes e novas, e monitorar sua implementação.

R 4.5
Assegurar que, no caso de investigação transfronteiriça, a lei processual estipule as ações a serem executadas, a fim de investigar com sucesso os crimes cibernéticos.

R 4.6
Considerar o desenvolvimento de uma estratégia que abranja a segurança cibernética e os crimes cibernéticos e que também esclareça as funções e responsabilidades dos atores (CIRTs, instituições de cumprimento da lei, ministérios) envolvidos no tratamento da resposta a incidentes de segurança cibernéticas e investigações de crimes cibernéticos.

R 4.7
Adaptar e implementar disposições legais sobre comércio eletrônico, relativas a incidentes de crimes cibernéticos, tais como fraude on-line, spam e páginas de phishing.

R 4.8
Considerar o desenvolvimento de uma plataforma para o intercâmbio de provas eletrônicas entre as forças regionais de crime cibernético.

R 4.9
Melhorar a cooperação existente entre os ISPs e as instituições de aplicação da lei para a eliminação, dos sites, de conteúdo que viole os direitos autorais.

R 4.10
Rever e aplicar as disposições legislativas que obrigam os ISPs a prestar assistência técnica ao cumprimento da lei quando realizem vigilância eletrônica lícita.

R 4.11
Considerar a assinatura da Convenção de Budapeste do Conselho da Europa sobre crime cibernético.

Sistema de justiça criminal

R 4.12
Investir em capacidade de investigação avançada, com vistas a permitir a apuração de casos complexos de crime cibernético, com apoio em testes regulares e treinamento de investigadores.

R 4.13
Alocar recursos destinados a unidades de crimes cibernéticos totalmente operacionais, com base na tomada de decisões estratégicas, a fim de apoiar investigações, especialmente em âmbito estadual.

R 4.14
Estabelecer programas de capacitação institucional para juízes, promotores e pessoal policial (por exemplo, por intermédio da Ameripol, da Interpol, da Europol ou de outras organizações), com vistas a adquirir novas competências em TIC necessárias para investigações de crimes cibernéticos (por exemplo, coleta de provas digitais) e formas eficazes de fazer cumprir as leis cibernéticas.

R 4.15
Fortalecer a capacidade nacional de investigação de crimes informáticos, incluindo recursos humanos, processuais e tecnológicos, medidas de investigação completas e cadeia de custódia digital.

R 4.16
Construir um quadro de promotores e juízes especializados em casos de crimes cibernéticos e casos envolvendo provas eletrônicas.

R 4.17
Considerar o estabelecimento de normas para o treinamento de agentes de cumprimento da lei em crimes cibernéticos.

R 4.18
Destinar recursos humanos e tecnológicos suficientes para garantir procedimentos legais eficazes em casos de crimes cibernéticos.

R 4.19
Considerar a solicitação de estatísticas confiáveis e precisas sobre crimes cibernéticos à URCC da Polícia Federal e ao CERT.br, com vistas a melhor informar os tomadores de decisão sobre o atual cenário de ameaça de crimes cibernéticos no Brasil, ao desenvolver políticas e legislações para considerar esse assunto.

R 4.20
Considerar a criação de um Laboratório Nacional de Crimes Cibernéticos sob o patrocínio da URCC da Polícia Federal, para facilitar a investigação forense digital.

R 4.21
Estabelecer um mecanismo formal para permitir a troca de informações e boas práticas entre promotores e juízes, visando a assegurar o processamento eficiente e eficaz de casos de crimes cibernéticos.

R 4.22
Coletar e analisar, regularmente, estatísticas e tendências sobre investigações de crimes cibernéticos, sobre acusações por crimes cibernéticos e sobre condenações por crimes cibernéticos.

Estruturas formais e informais de cooperação para combater o crime cibernético

R 4.23
Fortalecer a cooperação internacional para combater o crime cibernético com base nas estruturas de assistência jurídica em vigor e aderir a outros acordos bilaterais ou internacionais.

R 4.24
Considerar a criação de uma Plataforma de Inteligência de Ameaças para a troca de informações em tempo real entre a URCC da Polícia Federal e o CERT (CERT.br).

R 4.25
Alocar recursos para apoiar a troca de informações entre os setores público e privado nacionais e melhorar a estrutura legislativa e os mecanismos de comunicação.

R 4.26
Aprimorar a cooperação entre o setor público e os bancos e outras instituições financeiras com relação ao compartilhamento de incidentes, visando a aumentar o nível de conscientização sobre segurança cibernética no Brasil.

R 4.27
Promover mecanismos informais de cooperação na polícia e nos sistemas de justiça criminal, e entre a polícia e terceiros, em âmbito tanto interno como transfronteiriço, em particular os ISPs.

R 4.28
Fortalecer os mecanismos de cooperação informal na polícia e nos sistemas de justiça criminal, e entre a polícia e terceiros, em âmbito tanto interno quanto transfronteiriço. Considerar os conhecimentos técnicos de outras áreas, como a cooperação anticorrupção.

Revisão Da Capacidade De Cibersegurança

República Federativa do Brasil

Dimensão 5

NORMAS, ORGANIZAÇÕES E TECNOLOGIAS

Essa dimensão aborda o uso eficaz e generalizado da tecnologia de segurança cibernética para proteger os indivíduos, as organizações e a infraestrutura nacional. Essa dimensão analisa especificamente a implementação de normas e boas práticas de segurança cibernética, a implantação de processos e controles e o desenvolvimento de tecnologias e produtos para reduzir os riscos de segurança cibernética.

D 5.1 - Adesão às Normas

Esse fator analisa a capacidade do Governo de projetar, adaptar e implementar normas e boas práticas de segurança cibernética, particularmente as relacionados a procedimentos de aquisição e desenvolvimento de software.

Estágio: Formativo – Estabelecido

O Brasil estabeleceu uma série de instituições que as organizações, tanto privadas quanto públicas, podem consultar para a certificação de normas, melhores práticas e diretrizes de TIC. Concretamente, a Associação Brasileira de Normas Técnicas (ABNT) proporciona as versões brasileiras das normas ISO IEC, como a ABNT NBR ISO/IEC 270001; o CEPESC, o Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, se encarrega do desenvolvimento de projetos relacionados à segurança das comunicações, incluindo a transferência de tecnologia; a CAIS RNP, apesar de ser a equipe de resposta a incidentes para as redes acadêmicas brasileiras, é incumbido da criação e

promoção de práticas de segurança para as redes em geral. Segundo fontes governamentais, existem instruções normativas e normas complementares elaboradas no Departamento de Segurança da Informação do GSI, que tratam da normalização da segurança da informação e da segurança cibernética no âmbito da Administração Pública Federal.

Os participantes sugeriram que a concepção, adoção e auditoria das normas de segurança cibernética variam significativamente entre os setores público e privado. Quanto ao setor público, existem regras rigorosas que foram convertidas em normas desde 2001, e que se aplicam à Administração Pública Federal.[209] Foi implementado um sistema de auditoria, e todas as agências federais são obrigadas a designar uma unidade dentro de sua organização para realizar auditorias. Além disso, um escritório de controle geral foi incumbido de elaborar normas e avaliar o progresso da respectiva implementação em todos os departamentos. Do mesmo modo, uma ferramenta de autoavaliação foi colocada à disposição dos departamentos para ajudá-los a se preparar para futuras auditorias. Finalmente, os participantes mencionaram que a Administração Pública Federal projetou um modelo de maturidade e visitou mais de 40 agências para estabelecer um quadro global de seu nível geral de maturidade. Em forte contraste, existem diferenças significativas de maturidade em organizações públicas de nível estadual. A principal razão é a ausência de um mecanismo para impor uma aplicação uniforme das políticas, bem como a carência de especialização e financiamento. Além disso, a falta de responsabilização dos funcionários que violam as políticas e a ausência de métricas para medir a conformidade contribuem para a má prática de segurança cibernética nos estados.

Casos interessantes são o SERPRO e a DATAPREV, duas empresas que não fazem parte da Administração Pública Federal, mas que prestam serviços essenciais ao governo brasileiro. Ambas aderem aos mais altos padrões internacionais, tendo a DATAPREV obtido a certificação Tier 4 para dois de seus centros de dados, enquanto o terceiro possui a certificação Tier 3.

No tocante ao setor privado, os participantes postularam que a taxa de adoção difere entre os setores, sendo as empresas financeiras e de comunicação eletrônica pioneiras nessa área. Alguns setores, como o de comunicações eletrônicas e finanças, têm alguns requisitos obrigatórios de segurança; contudo, na maioria dos casos, a força que impulsiona a adesão às normas é a demanda do mercado e a necessidade comercial. A ISO 27001 é a estrutura mais frequentemente adotada, sendo também considerada a estrutura de segurança cibernética do NIST.

Os participantes concordaram que o Banco Central pode impor exigências de segurança, mas não há nenhuma norma específica promovida pelo regulador. Há uma combinação de normas internacionais, tais como o Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS)[210] para segurança de dados imposto pela MasterCard[211] e pelo Visa,[212] que as empresas concordaram em seguir rigorosamente. Cumpre salientar que, no decorrer da análise, não tivemos a oportunidade de dialogar com instituições financeiras privadas, para confirmar essas conclusões.

A respeito das normas de desenvolvimento e aquisição de software, existem diretrizes específicas para o setor público, porém não é claro em que medida essas diretrizes estão relacionadas à segurança cibernética. Os participantes sugeriram que há exigências na Administração Pública Federal quanto à compra de equipamentos de segurança cibernética e ao desenvolvimento de software. Essas exigências são genéricas, e as organizações desenvolvem processos internos. Em geral, os participantes afirmaram que as diretrizes são eficazes e oferecem transparência. Não foi possível obter uma imagem clara do setor privado.

Os participantes reconheceram a necessidade de que uma autoridade de segurança estabeleça normas em todos os setores (não apenas na Administração Pública Federal) e promova a adesão a essas normas. Salientaram também a relevância da racionalização do processo de aquisição de software e hardware.

Foi ainda sugerido que as discussões com todas as partes interessadas e reguladores relevantes devem começar antes da adoção da Estratégia Nacional de Segurança Cibernética.

Resultados do processo de validação realizado em março de 2019

Em março de 2018, não havia normas nacionais de TIC para o setor bancário, o que foi informado em nosso relatório. Desde então, a situação mudou. De acordo com a resolução do Conselho Monetário Nacional Brasileiro, CMN 4.658, de 26 de abril de 2018,[213] todas as instituições financeiras no âmbito regulatório do Banco Central do Brasil tiveram de implantar uma política de segurança cibernética até 6 de maio de 2019, e deverão tomar medidas de acordo com as normas de segurança cibernética estabelecidas nessa resolução até o final de 2021. À parte isso, os entrevistados de 2019 não informaram sobre nenhuma nova norma de segurança cibernética.

D 5.2 - Resiliência da Infraestrutura de Internet

Esse fator aborda a existência de serviços e infraestrutura de Internet confiáveis no país, bem como de processos rigorosos de segurança nos setores público e privado. Analisa também o controle que o Governo pode ter sobre sua infraestrutura de Internet e a extensão em que as redes e sistemas são terceirizados.

Estágio: Estabelecido

Os participantes da análise sugeriram que a infraestrutura da Internet no Brasil é muito resiliente. Foi registrado um aumento constante no número de internautas nos últimos cinco anos. Hoje, a taxa de penetração da Internet no Brasil está acima de 67%.[214]

Há também um mercado significativo de Internet móvel, com mais de 81 milhões de usuários.[215] As vendas de comércio eletrônico vêm aumentando e hoje excedem US$ 20 bilhões, já que mais de 61 milhões de pessoas são compradores digitais, área em que o comércio móvel atinge uma taxa de penetração de 32%.

Essas estatísticas dispõem as bases para entender a maturidade da resiliência da infraestrutura da Internet e das normas de segurança de serviços eletrônicos oferecidos por organizações públicas e privadas. Os participantes sugeriram que é oferecida uma ampla gama de serviços de governo eletrônico, tais como a votação eletrônica. Observações semelhantes podem ser feitas para o setor privado, onde há uma abundância de serviços eletrônicos, cuja aceitação os participantes acreditam estar aumentando.

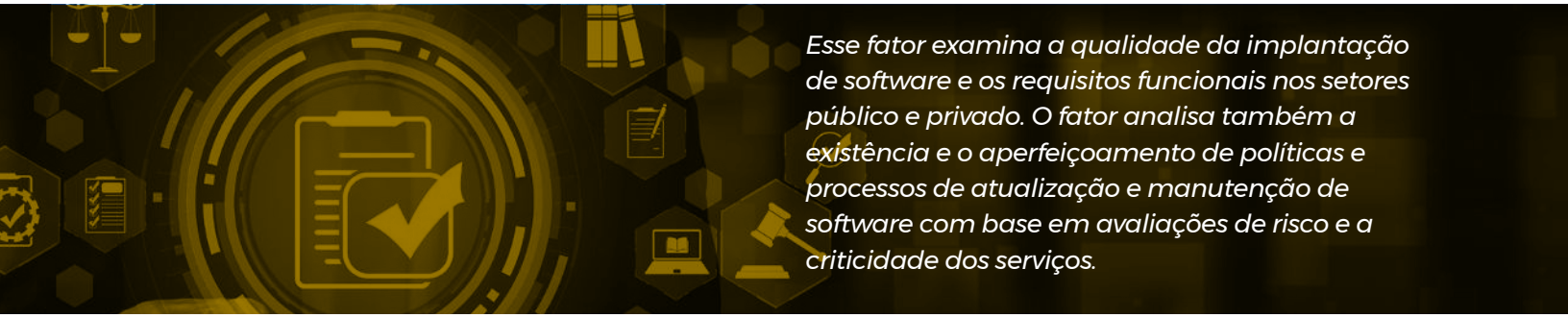
Existe uma grande variedade de ISPs públicos e privados no Brasil, com diferentes graus de qualidade, serviços e preços. A Abranet[216] tem imposto regulamentações, porém não foi possível entrevistar pessoas do setor de telecomunicações no decorrer de nossa análise. Segundo nossa pesquisa documental, há mais de 25 nodos de interconexão da Internet (IXPs), que são mantidos por um projeto global chamado IX.br. O número de IXs garante um ambiente atraente para inovação e conectividade com a Internet,

enquanto aumenta a resiliência da infraestrutura da Internet.[217] Vale notar que o projeto IX.br atinge uma produção máxima de 5.060GB por segundo, com uma média de 3.260GB por segundo para o Brasil, amplamente equivalente aos serviços oferecidos pelo provedor alemão DE-CIX, que são os mais altos do mundo.[218]

Resultados do processo de validação realizado em março de 2019

Além das informações coletadas no decorrer da análise, os participantes das entrevistas do grupo de análise e validação de 2019 informaram sobre as atividades do NIC.br para promover a resiliência da infraestrutura da Internet. Em particular, tomamos conhecimento da promoção das Normas de Acordo Mútuo para Segurança de Roteamento (MANRS), que têm por objetivo incentivar os operadores de rede e os nodos de interconexão da Internet a fomentar a resiliência na infraestrutura da Internet no Brasil.

D 5.3 - Qualidade de Software



Esse fator examina a qualidade da implantação de software e os requisitos funcionais nos setores público e privado. O fator analisa também a existência e o aperfeiçoamento de políticas e processos de atualização e manutenção de software com base em avaliações de risco e a criticidade dos serviços.

Estágio: Formativo

A qualidade do software varia significativamente no setor público, dependendo de as organizações fazerem ou não parte da Administração Pública Federal. Há um estoque de software seguro para a Administração Pública Federal, e as redes são monitoradas em busca de malware. A aplicação de patches em software desatualizado é automática, e existem KPIs para avaliar a eficácia dos mecanismos de aplicação de patches. Além disso, todos os ministérios têm agências incumbidas do gerenciamento de TIC e do estabelecimento de requisitos relativos a software. Há um escritório exclusivo de TI que fornece soluções tanto de software quanto de hardware, centralizando o suporte administrativo. Os participantes sugeriram que as organizações no governo estadual não dispõem de um catálogo de software seguro e que a aplicação de patches não é consistente. Quanto ao setor privado, a qualidade do software depende em grande parte do porte da organização, sendo as corporações dos setores financeiro e de telecomunicações as mais maduras.

O desenvolvimento de software é uma prática comum tanto no setor público quanto no privado. Os participantes mencionaram que ferramentas de software internas são desenvolvidas para monitorar redes, classificar incidentes e proporcionar consciência situacional. A inteligência artificial e as técnicas de aprendizagem de máquina são utilizadas pelas organizações para deter, detectar e reduzir ataques cibernéticos.

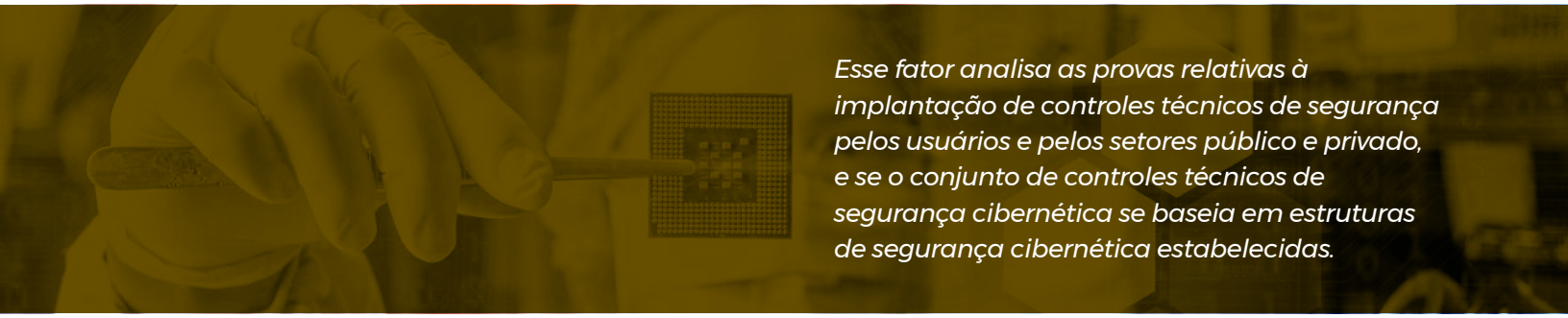
Como explicaram os participantes, a transferência de tecnologia é problemática no Brasil, devido à falta de legislação para estabelecer e proteger a

PI. Muitas organizações internacionais do setor de tecnologia hesitam, portanto, em fornecer soluções de software ao Brasil. Isso levou a um aumento na concepção de produtos domésticos de segurança cibernética. Não foi possível obter uma imagem clara sobre a testagem do software interno para validar as propriedades de segurança.

Resultados do processo de validação realizado em março de 2019

Durante o seminário de validação de 2019, os participantes acrescentaram que nem a indústria da aviação nem o setor financeiro[219] possui um catálogo de plataformas e aplicativos de software seguro, embora ambas as indústrias estejam alegadamente cientes da segurança no que diz respeito ao software em uso. Entretanto, devido a restrições orçamentárias, o software utilizado pelas instituições financeiras não é atualizado regularmente.

D 5.4 - Controles Técnicos de Segurança



Esse fator analisa as provas relativas à implantação de controles técnicos de segurança pelos usuários e pelos setores público e privado, e se o conjunto de controles técnicos de segurança cibernética se baseia em estruturas de segurança cibernética estabelecidas.

Estágio: Estabelecido

A adoção de controles técnicos de segurança no Brasil varia de acordo com os setores e as organizações. Os participantes sugeriram que a adoção e implementação de controles em órgãos governamentais é muito avançada na Administração Pública Federal, mas bastante elementar e inconsistentemente promovida nos governos estaduais, em virtude de restrições financeiras, recursos humanos limitados e inexistência de uma estrutura organizacional apropriada. A Constituição do Brasil, embora ampla, atualmente não prevê a segurança cibernética. Existe uma estratégia para a implementação de controles na Administração Pública Federal, que inclui um modelo detalhado para avaliar a maturidade das organizações, mas que não tem controle sobre os estados e municípios. Assim, controle técnico obrigatório algum para a Administração Pública Federal pode ser aplicado nos estados, nem os órgãos de auditoria podem monitorá-los com vistas a essa aplicação.

Os participantes mencionaram que existem 22 regras complementares que descrevem os controles técnicos para a Administração Pública Federal. Há redes descentralizadas protegidas por uma CERT, filtros e firewalls, sistemas de detecção de invasão (IDS) que utilizam inteligência artificial para determinar tendências, sistemas de backup, processos de resposta a incidentes e recuperação, e plataformas para compartilhar

a inteligência de ameaças com outras partes interessadas. Os participantes mencionaram o incidente wannacry como um exemplo em que, graças às plataformas de compartilhamento de inteligência de ameaças, foram capazes de trocar automaticamente informações sobre o malware, reajustar o endurecimento das redes e trocar patches e atualizações de software. Finalmente, métricas para todos os controles e avaliações de risco foram criadas e são aplicadas com frequência.

No setor privado, há um entendimento de que organizações bem estabelecidas adotam controles técnicos adequados adaptados às suas redes. Os controles de segmentação e ferramentas de monitoramento de redes são evidentes nesse setor, bem como o uso de IDSs e outras ferramentas de Gerenciamento de Informações e Eventos de Segurança (SIEM). Organizações específicas estabeleceram uma CERT para monitorar suas redes. Particularmente preocupante, entretanto, é o fato de que as organizações do setor privado não são obrigadas a compartilhar informações sobre incidentes com a CERT nacional e podem não receber informações sobre ameaças.

Em geral, o nível de compreensão e implantação dos controles de segurança nos setores privado e público é considerado pelos participantes como adequado. Contudo, não foram implantados mecanismos para avaliar a eficácia desses controles em organizações específicas, nem processos para recomendar melhorias adicionais. Os participantes concordaram que uma única autoridade deve ser responsável pelas decisões estratégicas sobre controles técnicos e deve promover a adoção de uma estrutura unificada como um conjunto mínimo de controles de segurança.

Resultados do processo de validação realizado em março de 2019

A pesquisa realizada em 2019 confirma em grande parte as evidências obtidas no decorrer da análise do CMM de 2018, o que foi posteriormente reforçado pelos resultados de pesquisa documental. Os dados do NIC.br[220] mostram que 93% das organizações do setor público no Brasil realizam backups de dados regularmente e 85% delas estabelecem controles físicos para impedir o acesso de pessoal não autorizado às instalações de computação.

D 5.5 - Controles Criptográficos

Esse fator analisa a implantação de técnicas criptográficas em todos os setores e usuários para a proteção de dados em repouso ou em trânsito, bem como a medida em que esses controles criptográficos atendem às normas e diretrizes internacionais e são mantidos atualizados.

Estágio: Estabelecido

A Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil) é a entidade responsável por garantir a autenticidade, a integridade e a validade jurídica dos documentos em formato eletrônico; apoiar aplicativos e aplicativos acreditados usando certificados digitais; e garantir transações eletrônicas seguras.[221] A ICP-Brasil compreende uma série de autoridades de certificação que prestam diferentes serviços, tais como uma Autoridade de Certificação Raiz (Root CA), autoridades de certificação (CAs) e autoridades de registro (RAs). A ICP Brasil estabeleceu normas técnicas para a acreditação de CAs e RAs, presta serviços de auditoria e supervisiona a Root CA e seus prestadores de serviços. Os participantes salientaram que requisitos muito rigorosos foram estabelecidos tanto para as ACs Raiz (Nível 5) quanto para as ACs que proveem a Infraestrutura de Chaves Públicas (PKI).

No governo federal, a ABIN, o centro de acreditação para criptografia, elabora regras específicas sobre como devem ser transmitidas as informações classificadas, define o protocolo de comunicação para informações sensíveis (com o uso de PGP) e orienta sobre a armazenagem dos dados. Com foco no DATAPREV, usam SSH para seus serviços e criptografam os dados em trânsito, mas não criptografam os dados nos repositórios. No DATAPREV, prevalece o uso de e-mails criptografados, o que tem criado problemas com a auditoria. Portanto, desestimula-se o uso de e-mails criptografados para informações não sensíveis. Os participantes mencionaram que existe uma chave mestra para decifrar informações para as auditorias. No tocante ao setor privado, observações semelhantes podem ser feitas. A criptografia é considerada principalmente para sistemas críticos, tanto para dados em trânsito quanto para dados em repouso. Não foi possível obter uma imagem clara quanto à oferta, pelos provedores de serviços de Internet, de conexões SSH entre servidores e navegadores.

Resultados do processo de validação realizado em março de 2019

A importância da criptografia foi reconhecida pelas autoridades federais, e seu uso é incentivado pela Política Nacional de Segurança da Informação adotada no final de 2018.[222] Os participantes das entrevistas do grupo de validação de 2019 observaram que essa política é voltada apenas para as instituições públicas federais, e que ser expandida a todos os setores, a fim de causar um impacto tangível na maturidade da capacidade de segurança cibernética do Brasil. Espera-se que isto dissemine o uso da criptografia, que, supostamente, ainda não é amplamente utilizada em todos os setores críticos.

D 5.6 - Mercado de Segurança Cibernética

Esse fator aborda a disponibilidade e o desenvolvimento de tecnologias de segurança cibernética e produtos de seguro competitivos.

Estágio: Formativo – Estabelecido

O mercado doméstico de tecnologias de segurança cibernética no Brasil se encontra em um nível de maturidade estabelecido. Existe uma ampla gama de produtos de software de segurança cibernética desenvolvidos internamente por empresas públicas e privadas. Os participantes mencionaram que algumas dessas tecnologias são exportadas e utilizadas por outros países. Da mesma forma, a dependência das tecnologias de segurança cibernética estrangeiras é menor. Segundo os participantes, a prevalência de hackers no Brasil tem resultado em uma demanda cada vez maior de produtos de segurança cibernética. Para atender a essa demanda, empresas locais desenvolvem e oferecem soluções para softwares de segurança nacional. Um fator importante para o mercado interno estabelecido é a falta de legislação para proteger a PI, o que faz com que as organizações estrangeiras relutem em implantar as soluções de software no Brasil, por medo de roubo de PI.

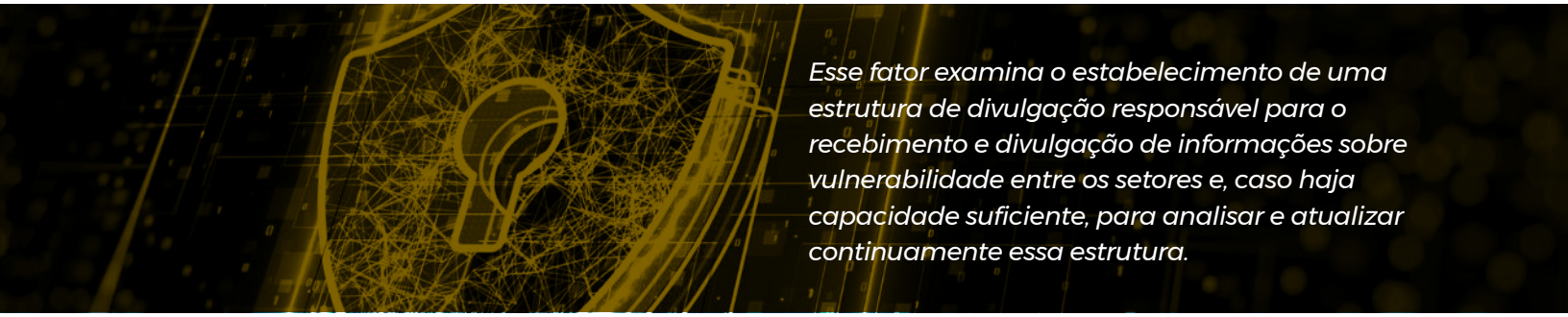
O mercado de seguros cibernéticos no Brasil acha-se no nível de maturidade formativo. Há uma variedade de apólices em oferta, e a demanda das organizações vem aumentando. Em geral, as apólices detalham as situações em que o seguro é válido e, em uma nota positiva, especificam as diretrizes de segurança a que as organizações devem aderir para serem seguradas. Um pequeno número de participantes observou que há cobertura em suas organizações para incidentes cibernéticos específicos.

Os participantes concordaram que é benéfico para todas as organizações obter um seguro cibernético já que, como sugeriram, o custo de até mesmo um incidente justifica a despesa. Além disso, destacaram que o apoio prestado nos incidentes e, especificamente, na análise forense é inestimável.

Resultados do processo de validação realizado em março de 2019

Em 2019, o seminário de validação confirmou em grande parte os resultados do relatório do CMM de 2018.

D 5.7 - Divulgação Responsável



Esse fator examina o estabelecimento de uma estrutura de divulgação responsável para o recebimento e divulgação de informações sobre vulnerabilidade entre os setores e, caso haja capacidade suficiente, para analisar e atualizar continuamente essa estrutura.

Estágio: Formativo – Estabelecido

Os participantes concluíram que a divulgação responsável varia entre os setores, com a Administração Pública Federal atingindo um grau de maturidade estabelecido, mediante a presença de alguns indicadores do nível estratégico. Em contraposição, os governos estaduais e o setor privado estão na fase formativa de maturidade.
Mais especificamente, uma estrutura de divulgação de vulnerabilidade foi implantada para a Administração Pública Federal. As organizações instituíram processos formais para divulgar informações automaticamente, e a CERT nacional recebe essas informações e prepara relatórios extensos sobre como abordar incidentes. Houve casos, como o evento wannacry, em que detalhes técnicos e patches foram oportunamente compartilhados com todas as partes interessadas relevantes, que puderam analisar automaticamente as informações e agir para proteger suas redes.

Por outro lado, as organizações privadas estão excluídas do intercâmbio de informações sobre inteligência de ameaças. Além disso, não são obrigadas a relatar incidentes, razão pela qual tendem a ocultar quaisquer problemas que detectem. Considerando o fato de que o Brasil começou a privatizar partes críticas da infraestrutura nacional, os participantes exortaram o Governo a reconhecer o importante papel desempenhado pelas organizações privadas na estratégia nacional de segurança cibernética e a elas conceder acesso aos sistemas de inteligência de ameaças.

Finalmente, vários meios para os cidadãos denunciarem incidentes foram criados, seja por meio da polícia estadual (cuja maturidade, no entanto, não é comparável à da Polícia Federal) ou de páginas eletrônicas. Canais exclusivos de comunicação foram criados no setor bancário para os clientes denunciarem fraudes on-line, e várias organizações públicas, como o SERPRO, oferecem orientações sobre como se defender de ameaças, por intermédio das mídias sociais, programas de rádio e jornais.

Recomendações

Com base nas informações prestadas na análise da maturidade das normas, organizações e tecnologias de segurança cibernética, o seguinte grupo de recomendações é apresentado ao Brasil. Essas recomendações visam a oferecer assessoramento a mostrar os passos a serem seguidos para o aprimoramento da capacidade existente de segurança cibernética, com base nas considerações do CMM do Centro.

Adesão às normas

R 5.1
Adotar uma linha de base acordada nacionalmente de normas e boas práticas de segurança cibernética nos setores público e privado, incluindo normas em aquisições e desenvolvimento de software.

R 5.2
Estabelecer ou designar uma instituição responsável pela implementação, auditoria e avaliação do sucesso das normas em todos os setores públicos e privados. Aplicar métricas para monitorar o cumprimento e estabelecer auditorias periódicas.

R 5.3
Promover debates sobre o uso das normas e boas práticas para enfrentar os riscos nas cadeias de abastecimento da IC, tanto por organizações governamentais quanto privadas. Identificar e ordenar as normas a que as IC devem aderir.

R 5.4
Identificar um conjunto mínimo de controles para todos os departamentos governamentais (incluindo o governo estadual), com base em avaliações anuais e inteligência de ameaças da CERT nacional, e estabelecer uma análise de controle para avaliar a eficácia dos controles e práticas atuais.

R 5.5
Estabelecer requisitos obrigatórios para a adesão às normas, designando agentes de segurança que serão incumbidos de sua implementação.

R5.6
Promulgar legislação que permita a aplicação de medidas disciplinares por violações de políticas.

R 5.7
Racionalizar orientações claras para a aquisição de hardware e software, considerando normas que atendam à segurança cibernética.

R 5.8
Promover a conscientização e a implementação de normas entre as PMEs.

R 5.9
Estabelecer a estrutura para avaliar a eficácia das normas para aquisição e desenvolvimento de software.

Resiliência da infraestrutura de internet

R 5.10
Melhorar a coordenação e a colaboração no tocante à resiliência da infraestrutura da Internet nos setores público e privado.

R 5.11
Realizar avaliações regulares dos processos, de acordo com normas e diretrizes internacionais, juntamente com a avaliação da segurança da infraestrutura de informação nacional e serviços críticos que impulsionam o investimento em novas tecnologias.

R 5.12
Identificar e mapear pontos potenciais de falha crítica na infraestrutura da Internet.

R 5.13
Estabelecer um sistema para administrar formalmente a infraestrutura nacional, com processos, papéis e responsabilidades documentados, e redundância adequada.

Qualidade de software

R 5.14
Desenvolver um catálogo de plataformas e aplicativos de software seguro nos setores público e privado.

R 5.15
Criar um inventário de software e aplicativos utilizados no setor público e na IC.

R 5.16
Desenvolver políticas e processos sobre atualizações e manutenção de software e aplicá-las nas ICs no setor público e privado.

R 5.17
Reunir e avaliar evidências de deficiências na qualidade de software em relação ao impacto dessas deficiências na usabilidade e no desempenho.

R 5.18
Estabelecer ou designar uma instituição para definir estrategicamente os requisitos comuns de qualidade e funcionalidade de software em todos os setores públicos e privados.

R 5.19
Monitorar e avaliar a qualidade do software utilizado nos setores público e privado.

Controles técnicos de segurança

R 5.20
Estabelecer treinamento frequente para funcionários de TI.

R 5.21
Incentivar os ISPs e bancos a oferecerem serviços de proteção contra malware e vírus.

R 5.22
Estabelecer métricas para medir a eficácia dos controles técnicos no setor público (incluindo o governo estadual) e aconselhar o setor privado a adotar essas métricas.

R 5.23
Desenvolver processos de reflexão sobre a adoção de controles mais técnicos baseados em metodologias de avaliação de riscos em todo o setor público.

R 5.24
Promover as melhores práticas em segurança cibernética para os usuários.

R 5.25
Designar uma autoridade que se encarregue das decisões estratégicas sobre controles técnicos, supervisione integralmente todas as redes, de ponta a ponta, e promova a adoção de uma estrutura unificada para os controles de segurança.

R 5.26
Instituir controles técnicos de segurança amplos e atualizados nos setores público e privado, monitorar sua eficácia e revisá-los regularmente.

R 5.27
Realizar regularmente testes de penetração para a proteção tanto do setor público como do privado.

Controles criptográficos

R 5.28
Incentivar o desenvolvimento e a divulgação de controles criptográficos em todos os setores e para todos os usuários, com vistas à proteção de dados em repouso e em trânsito, de acordo com as normas e diretrizes internacionais.

R 5.29
Conscientizar o público sobre serviços de comunicação seguros, tais como e-mails criptografados/assinados.

R 5.30
Considerar a criptografia dos dados em repouso nos centros de dados.

R 5.31
Estabelecer ou designar uma instituição responsável pela concepção de uma política para avaliar a implantação de controles criptográficos, de acordo com seus objetivos e prioridades, no setor público e privado.

Mercado de segurança cibernética

R 5.32
Estender a colaboração ao setor privado e ao meio acadêmico, em relação à pesquisa e desenvolvimento do avanço tecnológico da segurança cibernética.

R 5.33
Promover o intercâmbio de informações e melhores práticas entre as organizações, para analisar a possível cobertura de seguro.

Divulgação responsável

R 5.34
Desenvolver uma estrutura ou política responsável de divulgação de vulnerabilidade no setor público e promover sua adoção no setor privado, incluindo um prazo de divulgação, uma resolução programada e um relatório de reconhecimento.

R 5.35
Estabelecer ou designar uma instituição que se encarregue de supervisionar o processo de divulgação responsável e assegurar que as organizações não ocultem informações sobre vulnerabilidade.

R 5.36
Redesenhar o sistema atual, que facilita o intercâmbio da inteligência de ameaças entre os parceiros de infraestrutura crítica, com vistas a incluir o setor privado e o serviço civil. Promover o intercâmbio de inteligência de ameaças e incentivar as empresas privadas a participar ativamente.

R 5.37
Promover os mecanismos existentes de notificação de incidentes no setor público.

R 5.38
Definir patamares e requisitos de notificação para todos os setores. Essas exigências não devem considerar apenas a disponibilidade dos serviços, mas também a integridade e a confidencialidade dos dados.

R 5.39
Acordar instruções claras sobre como compartilhar informações, de maneira uniforme, em outros países da região da ALC (e não apenas), de maneira formal e estruturada.

Reflexões adicionais

Embora o nível de envolvimento das partes interessadas na análise fosse mais limitado do que almejávamos, o que limita a integralidade das provas em algumas áreas, a representação e a composição dos grupos de interessados foi, em geral, equilibrada e ampla.

A análise do CMM de 2018 foi a vigésima terceira análise de país que apoiamos diretamente.

O seminário de análise-validação de 2019 foi a primeira tentativa dos pesquisadores do GCSCC de buscar confirmação dos resultados iniciais da análise e pesquisar mudanças na maturidade da capacidade de segurança cibernética de uma nação. Embora não tenham sido detectadas grandes mudanças na maturidade, a atividade de validação é considerada útil.

Centro Global de Capacidade de Segurança Cibernética
Departamento de Informática, Universidade de Oxford
Wolfson Building, Oxford OX1 3QD,
Reino Unido

Tel.: +44 (0)1865 287434
E-mail: cybercapacity@cs.ox.ac.uk
Web: www.oxfordmartin.ox.ac.uk/cyber-security
Portal de Capacidade de Segurança Cibernética: www.sbs.ox.ac.uk/cybersecurity-capacity

Preparado e publicado pelo Programa de Segurança Cibernética do Comitê Interamericano contra Terrorismo (cybersecurity@oas.org).

Esta publicação foi possível graças ao apoio financeiro da UKFCO e seu Programa de Acesso Digital.

Referências

1. "Cybersecurity Capacity Maturity Model for Nations" (CMM), Edição revisada, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition (consultado em 25 fevereiro de 2018).

2. "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Publica Federal 2015-2018", Presidência da República Gabinete de Segurança Institucional Secretaria Executiva Departamento de Segurança da Informação e Comunicações, 2015, http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf (visitado em 29 de julho de 2018).

3. Estratégia Nacional de Segurança Cibernética, 2020, Decreto Federal No. 10.222, http://www.in.gov.br/web/dou/-/Decreto No10.222-de-5-de-fevereiro-de-2020-241828419 (visitado em 16 de abril de 2020).

4. Algumas são chamadas de CSIRTs e outras de CERTs.

5. "Das CERT.br", https://www.cert.br/about/ (visitado em 1 de junho de 2020).

6. http://www.inhope.org/gns/our-members/Brazil.aspx; http://new.safernet.org.br/ (visitado em 7 de maio de 2019).

7. http://www.pf.gov.br/ (visitado em 7 de maio de 2019).

8. www.disque100.gov.br (visitado em 7 de maio de 2019).

9. SaferNet Brazil, http://new.safernet.org.br/content/o-que-fazemos (visitado em 14 de julho de 2018).

10. INHOPE Association-SaferNet Brazil, https://www.inhope.org/EN/become-a-partner (visitado em 14 de julho de 2018).

11. CGI.br, https://www.cgi.br/about/ (visitado em 14 de julho de 2018).

12. Núcleo de Informação e Coordenação do Ponto BR (NIC.br), Disponível em https://www.nic.br/who-we-are/ (visitado em 14 de julho de 2018).

13. Antispam.br, http://www.antispam.br/ (visitado em 14 de julho de 2018).

14. InternetSegura.br, https://www.internetsegura.br/ (visitado em 14 de julho de 2018).

15. J. L. Marciano, "Applying COBIT in a Government Organization," ResearchGate, abril 2015, https://www.researchgate.net/publication/275638852 (visitado em 13 de julho de 2018).

16. Lei de Crimes Cibernéticos (Lei No. 12,737/2012), também chamada de "Lei Carolina Dieckmann", http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm (visitado em 14 de maio de 2018).

17. Marco Civil da Internet no Brasil, Lei 12.965, 23 de abril 2014, estabelece os princípios, garantias, direitos e deveres para o uso da Internet no Brasil - Brasília: Câmara dos Deputados, Edições Câmara, 2016 (Série legislação; No. 204), bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1 Marco Civil da Internet no Brasil em inglês (visitado em 14 de abril de 2018).

18. Constituição da República Federativa do Brasil, 1998, http://english.tse.jus.br/arquivos/federal-constitution (visitado em 14 de maio de 2018).

19. Código Penal 1940, Decreto-Lei No. 2.848, 7 de dezembro de 1940, http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm (visitado em 11 de maio de 2018).

20. Código de Defesa do Consumidor (Lei 8,078/1990) (1990), https://www.emergogroup.com/sites/default/files/file/lei_8.078_1990_consumer_protection_code.pdf (visitado em 14 de maio de 2018).

21. Janice K. Song, "Protecting Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying", World Bank, 2015; License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), https://www.icmec.org/wpcontent/uploads/2015/10/Protecting_Children_from_Cybercrime__Legislative_Responses_in_Asia_to_Fight_Child_Pornography__Online_Grooming__and_Cyberbullying_2015.pdf (visitado em 16 de junho de 2018).

22. Lei sobre direitos de autor e direitos conexos, 1998, (Lei No. 9.610), http://www.wipo.int/wipolex/en/text.jsp?file_id=125393 (visitado em 14 de junho de 2018).

23. Rafael Mendes Loureiro and Leonardo A F Palhares, "Cybersecurity - Brazil. Getting the Deal Through", Law Business Research Ltd., https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/ (visitado em 14 de junho de 2018).

24. Ministério das Relações Exteriores, Processo de Adesão à Convenção de Budapeste - Nota conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública, Nota 309, 2019, http://www.itamaraty.gov.br/en/press-releases/21149-accession-process-to-the-budapest-convention-joint-note-by-the-ministry-of-foreign-affairs-and-the-ministry-of-justice-and-public-security (visitado em 15 de abril de 2020).

25. Ministério da Justiça e Segurança Pública, o Ministério da Justiça e Segurança Pública coordena operação integrada contra abuso e exploração sexual cometidos pela Internet, 2019, https://www.justica.gov.br/news/collective-nitf-content-1553775485.52 (visitado em 15 de abril de 2020).

26. Lei No. 13,844, Junho 2019, que estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios, http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm (visitado em 15 de abril de 2020).

27. G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil: Threats and Responses", Strategic Paper, Igarape Institute, 2014, https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf (visitado em 14 de abril de 2018).

28. Ver Cybersecurity Capacity Maturity Model for Nations (CMM), Edição revisada, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition (visitado em 7 de maio de 2019).

29. Publicações relevantes: M. Williams, Making sense of social research (London: Sage Publications Ltd. 2003), doi: 10.4135/9781849209434; J. Knodel, "The design and analysis of focus group studies: A practical approach", in D. L. Morgan, Successful focus groups: Advancing the state of the art (SAGE Focus Editions 1993) 35–50; Thousand Oaks, CA: SAGE Publications Ltd., doi: 10.4135/9781483349008; R. A. Krueger, and M. A. Casey, Focus groups: A practical guide for applied research (London: Sage Publications Ltd. 2009).

30. Publicações relevantes: J. Kitzinger, "The methodology of focus groups: the importance of interaction between research participants", Sociology of Health & Illness, 16(1) (1994), 103–121; J. Kitzinger, 'Qualitative research: introducing focus groups', British Medical Journal, 311(7000) (1995), 299–302; E. F. Fern, 'The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality', Journal of Marketing Research, Vol. 19, No. 1 (1982), 1–13.

31. J. Kitzinger, 'Qualitative research: introducing focus groups', British Medical Journal, 311(7000) (1995), 299–302.

32. K. Krippendorff, Content analysis: An introduction to its methodology (Sage Publications Inc., 2004). H. F. Hsieh and S. E. Shannon, "Three approaches to qualitative content analysis", Qualitative Health Research, 15(9) (2005), 1277–1288; K. A. Neuendorf, The ContentAanalysis Guidebook (Sage Publications Inc., 2002).

33. E. F. Fern, "The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality", Journal of Marketing Research, Vol. 19, No. 1 (1982), 1–13, 1982.

34. S. Elo and H. Kyngas, "The qualitative content analysis process", Journal of Advanced Nursing, 62(1) (2008), 107–115; H. F. Hsieh and S. E. Shannon, "Three approaches to qualitative content analysis," Qualitative Health Research, 15(9) (2005), 1277–1288.

35. P. D. Barbara Downe-Wamboldt RN, "Content analysis: Method, applications, and issues", Health Care for Women International, 13(3) (1992, 313–321).

36. I. Dey, Qualitative data analysis: A user-friendly guide for social scientists (London: Routledge, 1993).

37. https://cetic.br/noticia/acesso-a-internet-por-banda-larga-volta-a-crescer-nos-domicilios-brasileiros/ (acessado em 7 de maio de 2019).

38. https://www.itu.int/net4/ITU-D/idi/2017/index.html (acessado em 7 de maio de 2019).

39. http://reports.weforum.org/global-competitiveness-index-2017-2018/countryeconomy-profiles/#economy=BRA (visitado em 7 de maio de 2019).

40. https://ww2.frost.com/files/5515/2878/9339/Digital_Market_Overview_FCO_Brazil_25May18.pdf (acessado em 7 de maio de 2019).

41. Ibid.

42. G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil: Threats and Responses", Strategic Paper, Igarape Institute, 2014, https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf (visitado em 7 de maio de 2019).

43. Brasil 2022, Presidência da República, Secretaria de Assuntos Estratégicos, 2010.

44. Livro Verde: Segurança Cibernética no Brasil, Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações, Brasília, 2010, http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf/view (visitado em 29 de julho de 2018).

45. Estratégia Nacional de Defesa, Ministério da Defesa, 2012, http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm (visitado em 29 de julho de 2018).

46. Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015–2018, Presidência da República, Gabinete de Segurança Institucional, Secretaria Executiva Departamento de Segurança da Informação e Comunicações, 2015, http://dsic.planalto.gov.br/legislacao/4_Estrategia_de_SIC.pdf (visitado em 29 de julho de 2018).

47. O documento Estratégia ainda não foi traduzido oficialmente para o inglês, razão pela qual os serviços de tradução do Google foram usados.

48. http://www2.planalto.gov.br/conheca-a-presidencia/ministros (visitado em 7 de maio de 2019).

49. Article 19, "Brazil: Cyber-security strategy", 2016; G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil", 2014, Strategic Paper.

50. http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23 (visitado em 7 de maio de 2019).

51. Ibid., Art. 5.

52. Ibid., Art. 6.

53. http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23 art. 6 (visitado em 7 de maio de 2019).

54. Estratégia Nacional de Segurança Cibernética 2020, Decreto Federal No. 10.222, http://www.in.gov.br/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419 (visitado em 16 de abril de 2020).

55. OneTrust Data Guidance, "Brazil: President approves national cybersecurity strategy", 2020, https://platform.dataguidance.com/news/brazil-president-approves-national-cybersecurity-strategy (visitado em 16 de abril de 2020).

56. Ibid..

57. Lei No. 13,844, Junho 2019, que estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios, http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm (visitado em 15 de abril de 2020).

58. Imagem extraída de https://www.cert.br/csirts/brazil/ (visitado em 7 de maio de 2019).

59. Núcleo de Informação e Coordenação do Ponto BR, https://bcp.nic.br/ (visitado em 7 de maio de 2019).

60. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, https://cartilha.cert.br/ (visitado em 7 de maio de 2019).

61. Equipe de Resposta a Incidentes de Segurança Cibernética, https://www.cert.br/csirts/brazil/ (visitado em 7 de maio de 2019).

62. Cristine Hoepers, "Incident Handling in Brazil," 2010, https://www.cert.br/docs/palestras/certbr-certpt2010.pdf 12 (visitado em 7 de maio de 2019).

63. Lucimara Desiderá, "Incident Handling in High Profile International Events: Lessons Learned and the Road Ahead", 2016, https://www.cert.br/docs/palestras/certbr-tcfirst-praga2016.pdf (visitado em 7 de maio de 2019).

64. Cristine Hoepers, "Evolution of the Scenario of Incidents in Brazil", 2018, https://www.cert.br/docs/palestras/certbr-oas2018.pdf 21 (visitado em 7 de maio de 2019).

65. Ibid.

66. Equipe de Resposta a Incidentes de Segurança Cibernética, Projeto Spampots, https://honeytarg.cert.br/spampots/ (visitado em 7 de maio de 2019)

67. Departamento de Segurança da Informação, http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf/view (visitado em 7 de maio de 2019)

68. http://www.planejamento.gov.br/assuntos/orcamento-1/orcamentos-anuais/2018/legislacao/alteracoes/lei-no-13-749-de-22-de-novembro-de-2018.pdf (visitado em 7 de maio de 2019).

69. G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil", Strategic Paper, 2014.

70. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8491.htm#art2 (visitado em 7 de maio de 2019).

71. http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23 art. 6 (visitado em 7 de maio de 2019).

72. https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf 93-95 (visitado em 7 de maio de 2019).

73. http://www.serpro.gov.br/ (visitado em 7 de maio de 2019).

74. CICG-IPSOS "Global Survey on Internet Security and Trust" (2018 Poll, "Part 1: Privacy, Security, Access and Trust").

75. https://gvpesquisa.fgv.br/sites/gvpesquisa.fgv.br/files/arquivos/meirelles_-_information_technology_and_egovernment_in_brazil_.pdf (visitado em 7 de maio de 2019).

76. https://www.bb.com.br/pbb/pagina-inicial/bb-seguranca/dicas-de-seguranca#/ (visitado em 7 de maio de 2019).

77. https://www.itau.com.br/seguranca/ (visitado em 7 de maio de 2019).

78. http://www.planejamento.gov.br/EGD/arquivos/revisao-da-estrategia-de-governanca-digital-2015-2019.pdf (visitado em 7 de maio de 2019).

79. https://principios.cgi.br/ (visitado em 7 de maio de 2019).

80. "Digital Government Review of Brazil: Towards the Digital Transformation of the Public Sector", OECD, 2018.

81. Ver e.g. http://www.ejeg.com/issue/download.html?idArticle=417 147; https://www.cetic.br/media/docs/publicacoes/2/TIC_eGOV_2017_livro_eletronico.pdf 219 (visitado em 7 de maio de 2019).

82. https://www.ctir.gov.br/arquivos/alertas/2018/ALERTA_CTIRGOV_2018_03_SQL_Injection.pdf (visitado em 7 de maio de 2019).

83. https://www.cetic.br/media/docs/publicacoes/2/tic_dom_2017_livro_eletronico.pdf 253 & 333 (visitado em 7 de maio de 2019).

84. Ver e.g. https://www.kabum.com.br/cgi-local/site/institucional/politicas.cgi (visitado em 7 de maio de 2019).

85. Ver e.g. https://www.magazineluiza.com.br/estaticas/seguranca-maxima/ (visitado em 7 de maio de 2019).

86. https://nic.br/media/docs/publicacoes/13/fasciculo-comercio-eletronico.pdf (visitado em 7 de maio de 2019).

87. CIGI-IPSOS "Global Survey on Internet Security and Trust" (2018 Poll, "Part 2: E-commerce") https://www.cigionline.org/internet-survey-2018 (visitado em 7 de maio de 2019).

88. https://www1.folha.uol.com.br/mercado/2018/07/senado-aprova-projeto-sobre-protecao-de-dados-pessoais.shtml; g1.globo.com/jornal-nacional/noticia/2018/07/comissao-do-senado-aprova-projeto-de-lei-de-protecao-de-dados-pessoais.html (visitado em 7 de maio de 2019); https://www.cartacapital.com.br/sociedade/entenda-o-que-muda-com-a-nova-lei-de-protecao-de-dados (visitado em 7 de maio de 2019).

89. http://www.inhope.org/gns/our-members/Brazil.aspx , http://new.safernet.org.br/ (visitado em 7 de maio de 2019).

90. http://www.pf.gov.br/ (visitado em 7 de maio de 2019).

91. www.disque100.gov.br (visitado em 7 de maio de 2019).

92. http://www.caixa.gov.br/site/english/About-Caixa/Paginas/default.aspx (visitado em 7 de maio de 2019).

93. http://www.bcb.gov.br/en#!/home (visitado em 7 de maio de 2019).

94. http://g1.globo.com/tecnologia/noticia/2016/02/facebook-cria-central-de-prevencao-ao-bullying-no-brasil.html (visitado em 7 de maio de 2019).

95. SaferNet Brazil, http://new.safernet.org.br/content/o-que-fazemos (visitado em 14 de julho de 2018).

96. INHOPE Association, SaferNet Brazil, http://www.inhope.org/gns/our-members/Brazil.aspx (visitado em 14 de julho de 2018).

97. Hotline, http://new.safernet.org.br/denuncie (visitado em 14 de julho de 2018).

98. SaferNet Brasil, http://new.safernet.org.br/content/o-que-fazemos (visitado em 14 de julho de 2018).

99. SaferNet Brasil em parceria com Google Brasil, http://www.safernet.org.br/site/institucional/parcerias/google (visitado em 14 de julho de 2018).

100. CGI.br, https://www.cgi.br/about/ (visitado em 14 de julho de 2018).

101. Núcleo de Informação e Coordenação do Ponto BR (NIC.br), https://www.nic.br/who-we-are/ (visitado em 14 de julho de 2018

102. Antispam.br, http://www.antispam.br/ (visitado em 14 de julho de 2018).

103. InternetSegura.br, https://www.internetsegura.br/ (visitado em 14 de julho de 2018).

104. CERT.br "Team Update: New Awareness Materials", 2017, https://www.cert.br/docs/palestras/certbr-natcsirts2017-2.pdf (visitado em 12 de julho de 2018).

105. Ministério Público Federal, em parceria com Safernet, MPF debate segurança e bom uso da internet com educadores pessoenses, 2015, http://pfdc.pgr.mpf.mp.br/informativos/edicoes-2015/dezembro/em-parceria-com-safernet-mpf-debate-seguranca-e-bom-uso-da-internet-com-educadores-pessoenses (visitado em 10 de setembro de 2018).

106. Federação das Indústrias do Estado de São Paulo (FIESP) http://www.fiesp.com.br/?temas=seguranca (visitado em 10 de setembro de 2018).

107. Brasscom, https://brasscom.org.br/events/forum-nacional-seguranca-cibernetica-nas-instituicoes-financeiras-impactos-da-resolucao-no-4-658/ (visitado em 10 de setembro de 2018).

108. http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23 (visitado em 7 de maio de 2019).

109. Ver nota ao pé 94.

110. Ministério da Educação, Catálogo Nacional dos Cursos Superiores de Tecnologia, http://portal.mec.gov.br/catalogo-nacional-dos-cursos-superiores-de-tecnologia- (visitado em 10 de setembro de 2018).

111. Ibid.

112. Cursos da Universidade de São Paulo, http://www5.usp.br/english/education/undergraduate/courses-offered/?lang=en (visitado em 25 de julho de 2018).

113. Universidade Federal do ABC, Ciência da Computação, http://ufabc.edu.br/en/graduate-program/?id=6 (visitado em 25 de julho de 2018).

114. Ibid..

115. RNP, Treinamento em Cibersegurança, https://esr.rnp.br/seg12 (visitado em 25 de julho de 2018).

116. RNP, Dia Internacional de Segurança Informática, https://disi.rnp.br/en (visitado em 10 de setembro de 2018).

117. Centro Universitário Senac, curso de pós-graduação em defesa cibernética, https://www.df.senac.br/faculdade/wp-content/uploads/2018/01/desefa-ciberntica.pdf (visitado em 25 de julho de 2018).

118. Trend Micro, "The rise of the Brazilian underground", 2016, https://blog.trendmicro.com/the-rise-of-the-brazilian-underground/ (visitado em 11 de julho de 2018).

119. Base Nacional Comum, http://basenacionalcomum.mec.gov.br/wp-content/uploads/2018/04/BNCC_EnsinoMedio_embaixa_site.pdf%20 https:/www.youtube.com/watch/?v=NT9Whez23gE (visitado em 25 de julho de 2018).

120. Cursos de divisão ministrados pelo CERT.br, https://www.cert.br/cursos/ (visitado em 14 de julho de 2018).

121. Portal de boas práticas (BCP.nic.br) https://bcp.nic.br/sobre/ (visitado em 14 de julho de 2018).

122. Ibid..

123. ITU, Perfil de Cyberwellness, Brasil, 2012, https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf (visitado em 11 de maio de 2018).

124. Cursos do CERT.br, https://www.cert.br/cursos/ (visitado em 10 de setembro de 2018).

125. Comando de defesa cibernética, https://ava-enadciber.eb.mil.br/ (visitado em 25 de julho de 2018).

126. Fundação Bradesco, curso sobre a segurança da informação, https://www.ev.org.br/curso/informatica/infraestrutura-de- ti/seguranca-da-informacao?return=/cursos/informatica (visitado em 25 de julho de 2018).

127. J. L. Marciano, "Applying COBIT in a Government Organization", 2015, http://www.isaca.org/Knowledge- Center/Research/Documents/COBIT-Focus-Applying-COBIT-in-a-Government-Organization_nlt_Eng_0415.pdf (visitado em 13 de julho de 2018).

128. Ibid..

129. Federação Brasileira de Bancos, https://portal.febraban.org.br/ (visitado em 18 de maio de 2019).

130. Lei de Crimes Cibernéticos (Lei No. 12,737/2012) também conhecida como "Lei Carolina Dieckmann", http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm (visitado em 14 de maio de 2018).

131. Marco Civil da Internet no Brasil, Lei 12.965, 23 de abril 2014, que estabelece os princípios, garantias, direitos e deveres para o uso da Internet no Brasil – Brasília: Câmara dos Deputados, Edições Câmara, 2016 (Série legislação; No. 204), bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1 O Marco Civil da Internet no Brasil em inglês (visitado em 14 de abril de 2018).

132. Diego R. Canabarro and Thiago Borne, "Reflections on the Fog of (Cyber) War", NCDG Policy Working Paper No. 13-002 (2013), https://www.umass.edu/digitalcenter/sites/default/files/Brazil%20and%20The%20Fog%20of%20%28Cyber%29War.pdf (visitado em 11 de maio de 2018).

133. Ministério da Defesa, Política de Defesa Cibernética, Portaria No. 3.389, 2012, http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2012&jornal=1&pagina=11&totalArquivos=304 (visitado em 11 de maio de 2018).

134. Documento técnico sobre defesa nacional 2012, https://www.defesa.gov.br/arquivos/estado_e_defesa/livro_branco/lbdn_2013_ing_net.pdf (visitado em 11 de maio de 2018).

135. Decreto 6703 da Estratégia Nacional de Defesa, 2008, http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm (visitado em 11 de maio de 2018).

136. Presidência da República, Proteção da Infraestrutura Crítica de Informação e Comunicação, 2010, http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf/view (visitado em 11 de maio de 2018).

137. Anatel – Consulta Pública n° 21, "Regulation on the risk management of telecommunications networks and use of telecommunications services in emergency and disaster situations", https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C1674&Tipo=1&Opcao=finalizadas (visitado em 11 de maio de 2018).

138. ITU, Perfil de Cyberwellness, Brasil, 2012, https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf (visitado em 11 de maio de 2018).

139. A. Ch. Raul, The Privacy, Data Protection and Cybersecurity Law Review (Fourth Edition, Law Business Research Ltd., 2017).

140. Carolina Dieckmann é uma famosa atriz brasileira que teve a conta de e-mail invadida e fotos íntimas publicadas na Internet.

141. Código Penal (1940) Decreto-Lei No. 2.848, 7 de dezembro de 1940, http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm (visitado em 11 de maio de 2018).

142. S. S. M. Ribeiro, Democracy after the internet: Brazil between facts, norms, and code (Vol. 27, Springer 2016).

143. Ibid.

144. Marco Civil da Internet no Brasil, Lei 12.965, 23 de abril de 2014, que estabelece os princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Câmara dos deputados, Edições Câmara, 2016 (Série legislação; No. 204), bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1 Marco Civil da Internet no Brasil em inglês (visitado em 14 de abril de 2018).

145. A. Ch. Raul, The Privacy, Data Protection and Cybersecurity Law Review, (Fourth Edition, Law Business Research Ltd. 2017).

146. Ministério Público Federal, nota técnica sobre a Convenção ETS 185 do Conselho da Europa - Convenção sobre Crime Cibernético - Convenção de Budapeste, segunda nota técnica CCR/SCI No. 1/2018, 2018, http://www.transparencia.mpf.mp.br/conteudo/servico-de-informacao-ao-cidadao/validacao-de-documentos (visitado em 14 de junho de 2018).

147. "How to be compliant with Brazil's Data Protection Act", IAPP, 2018, https://iapp.org/news/a/how-tobecompliantwithbrazilsdataprotectionact/?mkt_ (consultdo el 10 de septiembre de 2018).

148. Constituição da República Federativa do Brasil, 1998, http://english.tse.jus.br/arquivos/federal-constitution (visitado em 14 de maio de 2018).

149. Código Penal (Decreto-Lei n° 2.848, 7 de dezembro de 1940) (1940)
http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm (visitado em 11 de maio de 2018).

150. Código de Defesa do Consumidor (Lei 8,078/1990) (1990)
https://www.emergogroup.com/sites/default/files/file/lei_8.078_1990_consumer_protection_code.pdf (visitado em 14 de maio de 2018).

151. Marco Civil da Internet no Brasil, Lei 12.965, 23 de abril de 2014, estabelece os princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Câmara dos Deputados, Edições Câmara, 2016, (Série legislação; No. 204), bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1 Marco Civil da Internet no Brasil em inglês (visitado em 14 de abril de 2018).

152. "Brazil president approves data protection bill – but vetoes key accountability measures", Visitado neste momento, 2018, https://www.accessnow.org/brazil-president-approves-data-protection-bill-but-vetoes-key-accountability- measures/ (visitado em 10 de setembro de 2018).

153. A. Ch. Raul, The Privacy, Data Protection and Cybersecurity Law Review, (Fourth Edition, Law Business Research Ltd., 2017).

154. C. Barbosa, P. Vilhena, K. L. Advogados, "Data protection in Brazil: overview", Practical Law, Global Guide 2016-17, 2016, https://uk.practicallaw.thomsonreuters.com/4-520 1732?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk (visitado em 14 de junho de 2018).

155. Código Civil Brasileiro, 2002, http://www.wipo.int/wipolex/en/text.jsp?file_id=226198 (visitado em 14 de junho de 2018).

156. Rafael Mendes Loureiro and Leonardo A. F. Palhares, Cybersecurity - Brazil. Getting the Deal Through (Law Business Research Ltd.) https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/ (visitado em 14 de junho de 2018).

157. Lei sobre Direitos Autorais e Direitos Conexos, Lei No. 9.610, 1998, http://www.wipo.int/wipolex/en/text.jsp?file_id=125393 (visitado em 14 de junho de 2018).

158. Hunton Andrews Kurth, "Brazil's Senate Passes General Data Protection Law", 2018, https://www.huntonprivacyblog.com/2018/07/11/brazils-senate-passes-general-data-protection-law/ (visitado em 10 de setembro de 2018).

159. Rafael Mendes Loureiro and Leonardo A. F. Palhares, Cybersecurity - Brazil. Getting the Deal Through (Law Business Research Ltd.) https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/ (visitado em 14 de junho de 2018).

160. Human Rights Watch, Relatório Mundial 2017, https://www.hrw.org/world-report/2017/country-chapters/brazil (visitado em 14 de junho de 2018).

161. Ibid..

162. "Brazil court orders WhatsApp messaging to be suspended", BBC News, 2015, https://www.bbc.co.uk/news/world-latin-america-35119235 (visitado em 14 de junho de 2018).

163. W. Connors, "Facebook Executive Arrested in Brazil", Wall Street Journal, 2016,

164. https://www.wsj.com/articles/facebook-executive-arrested-in-brazil-1456851506 (visitado em 16 de junho de 2018).
Law to combat child pornography online, "Statute of Children and Adolescents, to improve combat the production, sale and distribution of child pornography and criminalize the acquisition and possession of such material and other related behaviors to pedophilia on the internet", 2008, https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm (visitado em 16 de junho de 2018).

165. ITU, Perfil de Cyberwellness, Brasil, 2012, https://www.itu.int/en/ITUD/Cybersecurity/Documents/Country_Profiles/Brazil.pdf (visitado em 11 de maio de 2018).

166. Ibid..

167. A. Ch. Raul, The Privacy, Data Protection and Cybersecurity Law Review, (Fourth Edition, Law Business Research Ltd. 2017).

168. Janice K. Song, "Protecting Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying", World Bank, License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), 2015, https://www.icmec.org/wpcontent/uploads/2015/10/Protecting_Children_from_Cybercrime__Legislative_Responses_in_Asia_to_Fight_Child_Pornography__Online_Grooming__and_Cyberbullying_2015.pdf (visitado em 16 de junho de 2018).

169. Ibid..

170. ITU, Perfil Cyberwellness, Brasil, 2012,

171. Ibid..

172. Lei sobre Direitos Autorais e Direitos Conexos, Lei No. 9.610 (1998), http://www.wipo.int/wipolex/en/text.jsp?file_id=125393 (visitado em 14 de junho de 2018).

173. Rafael Mendes Loureiro and Leonardo A. F. Palhares, Cybersecurity - Brazil Getting the Deal Through (Law Business Research Ltd.) https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/ (visitado em 14 de junho de 2018).

174. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências, Lei No. 9.609 (1998), http://www.wipo.int/wipolex/en/details.jsp?id=513 (visitado em 14 de junho de 2018).

175. Decreto-Lei da Internet No. 8,771/2016 (2016), http://www.internetlab.org.br/wp- content/uploads/2016/05/Decree-MarcoCivil-English.pdf (visitado em 14 de junho de 2018).

176. Ibid..

177. Código de Defesa do Consumidor (Law 8,078/1990) (1990) https://www.emergogroup.com/sites/default/files/file/lei_8.078_1990_consumer_protection_code.pdf (visitado em 14 de maio de 2018).

178. C. Barbosa, P. Vilhena, and K. L. Advogados, "Data protection in Brazil: overview", Practical Law, Global Guide 2016-17, 2016, https://uk.practicallaw.thomsonreuters.com/4-5201732?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk (visitado em 14 de junho de 2018).

179. Data protection and Privacy - Brazil, 2017, Ricardo Barretto Ferreira da Silva and Paulo Branch, "Getting the Deal Through", Law Business Research Ltd., https://gettingthedealthrough.com/area/52/jurisdiction/6/data- protection-privacy-brazil/ (visitado em 14 de junho de 2018.

180. Ibid..

181. E-commerce - Brasil, 2017, Raphael de Cunto, Pedro Paulo Barradas Barata and Beatriz Landi Laterza Figueiredo, "Getting the Deal Through", https://gettingthedealthrough.com/area/11/jurisdiction/6/e-commerce- brazil/ (visitado em 14 de junho de 2018).

182. Marco Civil da Internet no Brasil, Lei 12.965, 23 de abril 2014, que estabelece os princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Câmara dos Deputados, Edições Câmara, 2016 (Série legislação; No. 204), bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1 Marco Civil da Internet no Brasil em inglês (visitado em 14 de abril de 2018).

183. Lei de Importunação Sexual (No. 13,718) http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm (visitado em 16 de abril de 2020).

184. Comissão Econômica para a América Latina, Relatório de Revisão Global em Âmbito Nacional sobre a Implementação da Declaração de Beijing e Plataforma de Ação - Brasil, 2019, https://www.cepal.org/sites/default/files/informe_beijing25_brasil.pdf (visitado em 16 de abril de 2020).

185. "Governo brasileiro aprova lei que garante mais proteção às mulheres", Governo do Brasil, 2018, http://www.brazil.gov.br/about-brazil/news/2018/09/brazilian-government-approves-law-that-guarantees-more-protection-to-women-1 (visitado em 16 de abril de 2020).

186. G. Diniz, R. Muggah and M. Glenny, "Deconstructing cyber security in Brazil: Threats and Responses", Strategic Paper, Igarape Institute, 2014, https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf (visitado em 14 de abril de 2018).

187. Ibid..

188. Ibid..

189. ""Skills of the Federal Police gain international recognition", Polícia Federal, 2014, http://www.pf.gov.br/agencia/noticias/2014/10/pericias-da-policia-federal-ganham-reconhecimento-internacional (visitado em 10 de setembro de 2018).

190. Janice K. Song, "Protecting Children from Cybercrime: Legislative Responses in Asia to Fight Child Pornography, Online Grooming, and Cyberbullying", World Bank, 2015, license: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), https://www.icmec.org/wpcontent/uploads/2015/10/Protecting_Children_from_Cybercrime__Legislative_Responses_in_Asia_to_Fight_Child_Pornography__Online_Grooming__and_Cyberbullying_2015.pdf (visitado em 16 de junho de 2018).

191. Rafael Mendes Loureiro and Leonardo A. F. Palhares, Cybersecurity - Brazil. Getting the Deal Through (Law Business Research Ltd.) https://gettingthedealthrough.com/area/72/jurisdiction/6/cybersecurity-brazil/ (visitado em 14 de junho de 2018).

192. Marco Civil da Internet no Brasil, Lei 12.965, 23 de abril de 2014, que estabelece os princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Câmara dos Deputados, Edições Câmara, 2016 (Série legislação; No. 204), bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1 O Marco Civil da Internet no Brasil em inglês (visitado em 14 de abril de 2018).

193. Electronic Frontier Communication, "State Surveillance of Communications in Brazil", https://necessaryandproportionate.org/files/2016/07/08/brazil_faq_en.pdf (visitado em 14 de junho de 2018).

194. Ministério Público Federal, 2014, http://www.mpf.mp.br/atuacaotematica/ccr2/coordenacao/comissoesegruposdetrabalho/combatecrimescirberneticos/relatorios/Oficio%20PRSP%20GABPRR28MGBAS%2066526%20-%2014.11.12.pdf (visitado em 10 de setembro de 2018).

195. Cybercrime@coe atualização, Conselho da Europa, 2018, https://rm.coe.int/cybercrime-coe-update-2018- q1/16807baf95 (visitado em 14 de junho de 2018).

196. Octopus 2018: Co-operation against Cybercrime, 11-13 de julho de 2018, Conselho da Europa, Estrasburgo, França, https://www.coe.int/en/web/cybercrime/octopus-interface-2018 (visitado em 14 de julho de 2018).

197. OAS, Cybercrime, https://www.oas.org/juridico/english/cyber.htm (visitado em 10 de setembro de 2018).

198. A. Mari, "Microsoft Brazil to deliver digital crime training program to Public Prosecutor's Office", ZDnet, 2018, https://www.zdnet.com/article/microsoft-brazil-to-deliver-digital-crime-training-program-to-public-prosecutors- office/ (visitado em 14 de junho de 2018)

199. Ministério da Justiça e Segurança Pública, "O Ministério da Justiça e Segurança Pública coordena operação integrada contra abuso e exploração sexual cometidos pela Internet", 2019, https://www.justica.gov.br/news/collective-nitf-content-1553775485.52 (visitado em 15 de abril de 2020)

200. Lei No. 13,844, junho de 2019, que estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios, http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13844.htm (visitado em 15 de abril de 2020).

201. ITU, Perfil de Cyberwellness, Brasil, 2012,

202. Ibid..

203. Ibid..

204. FIRST, Cert.br, https://www.first.org/members/teams/cert-br (visitado em 11 de maio de 2018)

205. "INTERPOL and Banco do Brasil S/A sign co-operation agreement against cybercrime", INTERPOL, 2018, https://www.interpol.int/News-and-media/News/2018/N2018-046 (visitado em 14 de julho de 2018)

206. G. Diniz, R. Muggah, and M. Glenny, "Deconstructing cyber security in Brazil: Threats and Responses", Strategic Paper, Igarape Institute, 2014, https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf (visitado em 14 de abril de 2018).

207. INTERPOL, Brasil, https://www.interpol.int/Member-countries/Americas/Brazil (visitado em 14 de julho de 2018).

208. "Today, Brazil and Europol signed an agreement to expand co-operation to combat cross-border criminal activities", Europol, 2017, https://www.europol.europa.eu/newsroom/news/today-brazil-and-europol-signed-agreement-to-expand-co-operation-to-combat-cross-border-criminal-activities (visitado em 14 de julho de 2018).

209. http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf/view (visitado em 11 de maio de 2019).

210. https://www.pcisecuritystandards.org (visitado em 11 de maio de 2019).

211. http://www.mastercard.com/sea/consumer/standard-mastercard.html (visitado em 11 de maio de 2019).

212. https://usa.visa.com/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf (visitado em 11 de maio de 2019).

213. https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf (visitado em 10 de maio de 2019).

214. https://cetic.br/noticia/acesso-a-internet-por-banda-larga-volta-a-crescer-nos-domicilios-brasileiros/ (visitado em 11 de maio de 2019).

215. http://www.allisps.com/en/offers/BRAZIL (visitado em 11 de maio de 2019).

216. http://www.abranet.org.br/?UserActiveTemplate=site (visitado em 11 de maio de 2019).

217. S. H. Bucke Brito, M. A. Silva Santos, R. dos Reis Fontes, D. A. Lachos Perez, H. Lourenço da Silva, and C. R. Esteve Rothenberg, "An Analysis of the Largest National Ecosystem of Public Internet eXchange Points: The Case of Brazil", Journal of Communication and Information Systems, 31(1), 2016.

218. http://ix.br (visitado em 11 de maio de 2019).

219. Ver p.ex., Banco Central do Brasil, Resolução CMN 4,658, 26 de abril, 2018, https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf (visitado em 13 de maio de 2019).

220. CGI.br-NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro – TIC Governo Eletrônico, 2017, https://www.cetic.br/tics/governo/2017/orgaos/B6/ (visitado em 17 de maio de 2019).

221. http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm (visitado em 13 de maio de 2019).

222. http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/12/2018&jornal=515&pagina=23 (visitado em 7 de maio de 2019).

Revisão Da Capacidade De Cibersegurança

República Federativa do Brasil

Revisão Da Capacidade De Cibersegurança

República Federativa do Brasil

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

GSI-PR

GREAT for PARTNERSHIP

OEA Mais direitos para mais pessoas

Revisão Da Capacidade De Cibersegurança

República Federativa do Brasil