REVISÃO DA CAPACIDADE DE SEGURANÇA CIBERNÉTICA

Brasil

Agosto de 2023

Global Cyber Security Capacity Centre
OXFORD UNIVERSITY INNOVATION
UNIVERSITY OF OXFORD

ÍNDICE

ADMINISTRAÇÃO DE DOCUMENTOS

Principais pesquisadores: Dr. Marcel Stolz, Dra. Louise Axon

Revisados por: Professora Sadie Creese, Professor William Dutton, Professor Michael Goldsmith, Dr. Jamie Saunders, Professor David Wall, Professor Basie Von Solms, Carolin Weisser Harris

Aprovado por: Professor Michael Goldsmith

Versão	*Data*	*Notas*
1	*23/10/2023*	*Primeiro rascunho dos investigadores principais apresentado ao Conselho Técnico do GCSCC*
2	*03/11/2023*	*Segundo rascunho enviado aos anfitriões.*
3	*20/11/2023*	*Feedback recebido dos anfitriões*
4	*28/11/2023*	*Relatório final enviado aos anfitriões.*

LISTA DE ABREVIAÇÕES

ABES	Associação Brasileira das Empresas de Software
ABIN	Agência Brasileira de Inteligência
Anatel	Regulador do setor das telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
BACEN	Banco Central do Brasil
C2	Comando e controle
AC	Autoridade de Certificação
CAIS	CSIRT da Rede Brasileira Acadêmica e de Pesquisa
CAMP	Aliança de Cibersegurança para o Progresso Mútuo
CCDCOE	Centro Cooperativo de Excelência em Defesa Cibernética
CDCiber	Escola Nacional de Defesa Cibernética
CERT	Equipe de resposta a emergências informáticas
CERT.br	Equipe Nacional Brasileira de Resposta a Emergências Informáticas
CGI.br	Comitê Gestor da Internet Brasileira
CI	Infraestrutura crítica
CEI CSC	Centro para controles críticos de segurança para segurança na Internet
CISO	Diretor de Segurança da Informação
CMM	Modelo de maturidade da capacidade de segurança cibernética para nações (Cybersecurity Capacity Maturity Model for Nations)
ComDCiber	Comando de Defesa Cibernética
CSIRT	Equipe de resposta a incidentes de segurança cibernética
CTF	Captura a bandeira
CTI	Inteligência sobre ameaças cibernéticas
CTIR.gov	Centro Brasileiro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos Governamentais
CVE	Vulnerabilidades e exposições comuns
DDoS	Negação de serviço distribuída (ataque)
DSIC	Departamento de Informação e Segurança Cibernética
UE	União Europeia
FCDO	Escritório de Relações Exteriores, Commonwealth e Desenvolvimento
Febraban	Federação Brasileira de Bancos
FIRST	Fórum de equipes de segurança e resposta a incidentes
PFA	Administração Pública Federal
GCSCC	Centro Global de Capacidade de Cibersegurança

GDPR	Regulamento Geral de Proteção de Dados
GEG	Grupo de especialistas governamentais
GSI	Gabinete de Segurança Institucional da Presidência da República
TIC	Tecnologia da informação e comunicações
BID	Banco Interamericano de Desenvolvimento
IGF	Fórum de Governança da Internet
ISAC	Centro de análise e intercâmbio de informações
ISO	Organização Internacional de Padrões
ISP	Provedor de internet
IXP	Ponto de troca de tráfego na internet
KPI	Indicador-Chave de Desempenho
LAC4	Centro de Competência Cibernética da América Latina e Caribe
LAC-AAWG	Grupo de Trabalho Antiabuso da América Latina e do Caribe
LGPD	Lei Geral de Proteção de Dados Pessoais
Mercosul	Mercado Comum do Sul
MFA	Ministério de Relações Exteriores
MISP	Plataforma de compartilhamento e inteligência de ameaças de código aberto
MoD	Ministro da Defesa
MoU	Memorando de entendimento
OTAN	Organização do Tratado do Atlântico Norte
NCRA	Avaliação Nacional de Risco Cibernético
NCS	Estratégia Nacional de Cibersegurança
NCSC	Centro Nacional de Segurança Cibernética
NIC.br	Centro de Informações da Rede Brasileira
NIST LCR	Marco de segurança cibernética do Instituto Nacional de Padronização e Tecnologia
OEA	Organização dos Estados Americanos
GTCA	Grupo de trabalho de composição aberta
KPI	Infraestrutura de chave pública
PlanGIC	Plano de Gestão de Incidentes Cibernéticos (para a PFA)
PlanSIC	Plano Nacional de Segurança de Infraestruturas Críticas
PNCiber	Política Nacional de Cibersegurança
PNSI	Política Nacional de Segurança da Informação
ReGIC	Rede Federal de Gerenciamento de Incidentes Cibernéticos
SDN	Rede definida por software

SIM3	Modelo de maturidade de gerenciamento de incidentes de segurança
SMDC	Sistema militar de defesa cibernética
PME	Pequena ou média empresa
SOC	Centro de operações de segurança
TCU	Tribunal de Contas da União
TLS	Segurança da camada de transporte
ONU	Nações Unidas

SUMÁRIO EXECUTIVO

Em colaboração com o Escritório de Assuntos Exteriores, Commonwealth e Desenvolvimento (FCDO) do Reino Unido e a Organização dos Estados Americanos (OEA), o Centro Global de Capacidade de Segurança Cibernética (GCSCC, ou "o Centro") conduziu uma revisão da maturidade das capacidades de segurança cibernética no Brasil a convite do Gabinete de Segurança Institucional da Presidência da República (GSI). O objetivo desta revisão foi determinar áreas de capacidade nas quais o Governo poderia investir estrategicamente, para que pudesse melhorar seu estado de segurança cibernética nacional.

Durante o período de 28 a 30 de agosto de 2023, as seguintes partes interessadas participaram em mesas redondas: academia, justiça criminal, segurança pública, funcionários de tecnologia da informação e representantes de entidades do setor público, proprietários de infraestrutura crítica, formuladores de políticas, funcionários de tecnologia da informação do governo e o setor privado (incluindo instituições financeiras), empresas de telecomunicações e setor bancário, bem como parceiros internacionais. Essas sessões foram realizadas presencialmente no Brasil.

As consultas foram conduzidas utilizando o Modelo de Maturidade da Capacidade de Segurança Cibernética para Nações (CMM) do Centro, que define cinco dimensões da capacidade de segurança cibernética:

- *Política e estratégia de segurança cibernética*
- *Cultura e sociedade de segurança cibernética*
- *Criação de conhecimento e capacidades em segurança cibernética*
- *Marcos legais e regulatórios*
- *Padrões e tecnologias*

Cada Dimensão contém uma série de Fatores que descrevem o que significa ter capacidade de segurança cibernética. Cada Fator apresenta uma série de *Aspectos* que agrupam *Indicadores* relacionados, que descrevem etapas e ações que, uma vez observadas, definem o estado de maturidade daquele Aspecto. Existem cinco estágios de maturidade, que vão desde o estágio inicial até o estágio dinâmico. A etapa inicial implica uma abordagem *ad hoc* da capacidade, enquanto a etapa dinâmica representa uma abordagem estratégica e a capacidade de se adaptar dinamicamente ou de se modificar em resposta a considerações ambientais. Para obter mais detalhes sobre as definições, consulte o documento CMM.[1]

A Figura 1 abaixo fornece uma representação geral da capacidade de segurança cibernética no Brasil e ilustra as estimativas de maturidade em cada Dimensão. Cada Dimensão representa um quinto do gráfico, portanto os cinco estágios de maturidade de cada Fator se estendem para fora do centro do gráfico; "início" está mais próximo do centro do gráfico e "dinâmico" é colocado no perímetro.

[1] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition,", fevereiro de 2017, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

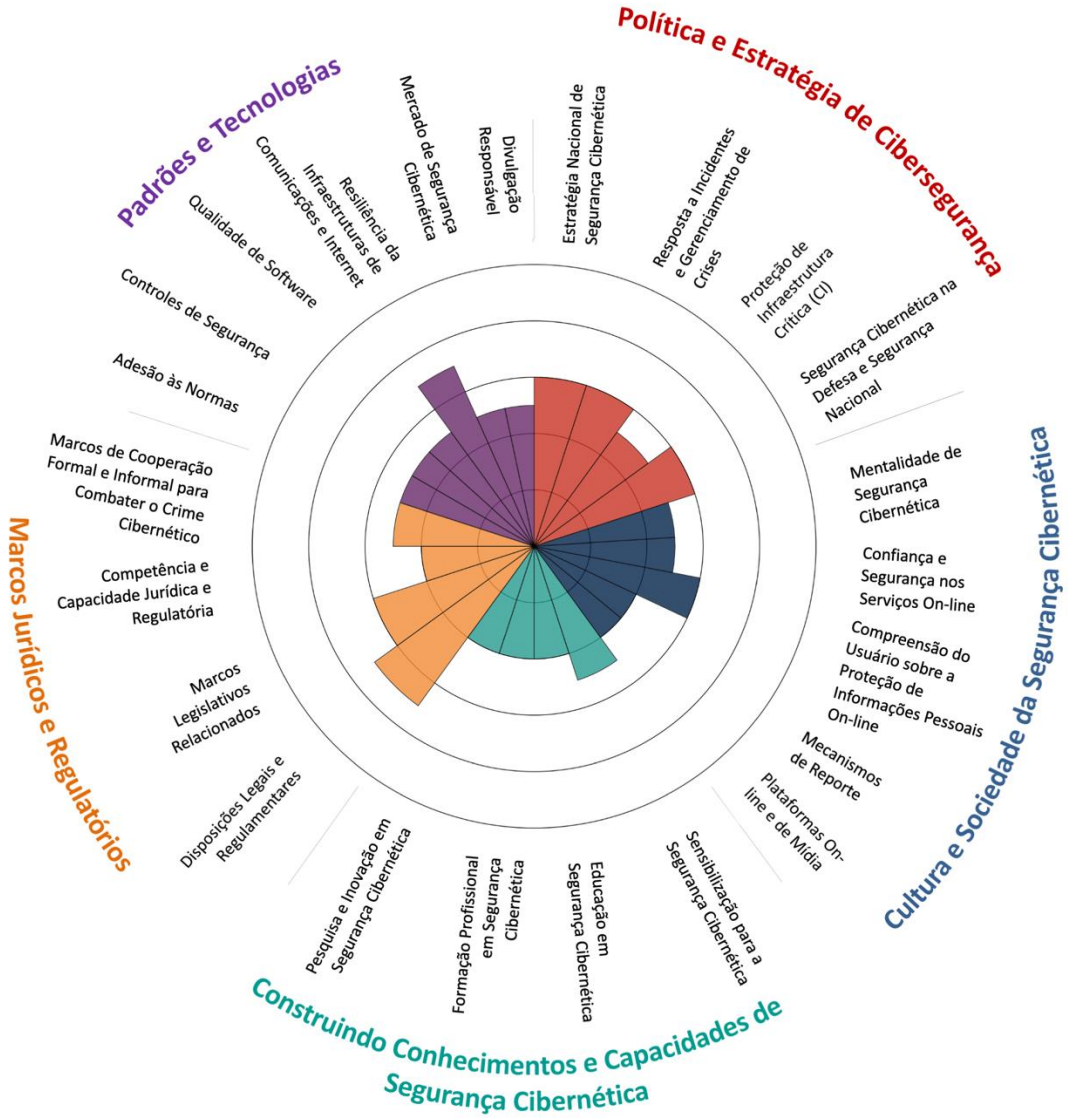


Figura1. Representação geral da capacidade de segurança cibernética no Brasil – revisão CMM 2023

Esta foi a segunda avaliação do CMM do Brasil, após a primeira em 2020. Além disso, o Brasil participou dos Estudos Regionais de Capacidade de Segurança Cibernética (baseados no CMM) realizados pela Organização dos Estados Americanos (OEA) e pelo Banco Interamericano de Desenvolvimento (BID) em 2016 e novamente em 2020 (resultados dos Estudos Regionais de 2020). O estudo foi baseado na revisão do CMM de 2020).

A Figura 2 abaixo mostra a representação geral da capacidade de segurança cibernética no Brasil conforme apresentada no relatório CMM 2020.[2]

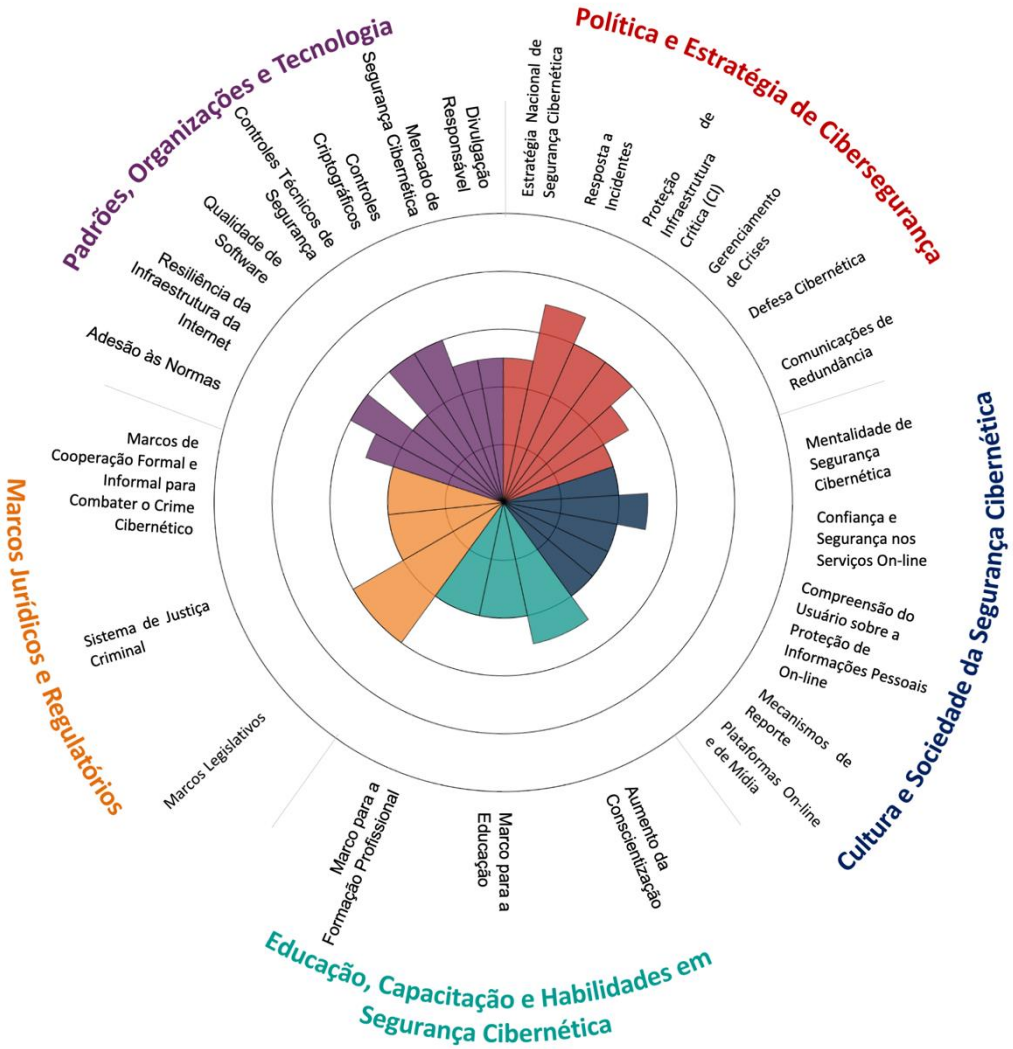


Figura2. Representação geral da capacidade de segurança cibernética no Brasil – revisão CMM 2020

[2] O CMM foi revisto em 2021 para refletir o cenário em constante mudança de risco e controle da cibersegurança, e o ambiente operacional em mudança no qual as nações devem fornecer segurança cibernética. Portanto, existem algumas diferenças entre o CMM utilizado na revisão de 2020 e na revisão de 2023; diferenças na estrutura das dimensões e na formulação dos nomes dos *Fatore*s podem ser vistas nos gráficos.

‡ Para fins de compatibilidade com versões anteriores, este resumo apresenta os níveis de maturidade observados na avaliação do CMM de 2023 no âmbito de uma versão anterior do CMM que serviu de base para a revisão do CMM do Brasil realizada em 2020.

*Os fatores que avançaram para o próximo estágio de maturidade receberam a classificação "+ +". Os fatores que registaram melhorias em alguns dos seus indicadores, mas não progrediram o suficiente para justificar uma melhoria na próxima fase de maturidade, foram marcados com "+". Fatores sem

A Tabela 1 apresenta um resumo do desenvolvimento de capacidades para todos os fatores avaliados em 2020 e em 2023.

	Estagio de maturidade‡		Mudanças de capacidade*
Fatores baseados no CMM 2017	**2020**	**2023**	
D1 Política e Estratégia de Segurança Cibernética			
D1.1 Estratégia Nacional de Segurança Cibernética	Formativo para Estabelecido	Estabelecido	++
D1.2 Resposta a Incidentes	Estabelecido como estratégico	Estabelecido	-
D1.3 Proteção de Infraestrutura Crítica	Estabelecido	Formativo para Estabelecido	-
D1.4 Gestão de Crises	Estabelecido	Estabelecido	
D1.5 Defesa Cibernética	Formativo para Estabelecido	Estabelecido	++
D1.6 Redundância de Comunicações	Formativo	Estabelecido	++
D2 Cultura e Sociedade de Segurança Cibernética			
D2.1 Mentalidade de Segurança Cibernética	Formativo	Formativo para Estabelecido	++
D2.2 Confiança e Segurança na Internet	Formativo para Estabelecido	Formativo para Estabelecido	o
D2.3 Compreensão do Usuário sobre Informações Pessoais	Formativo	Estabelecido	++
D2.4 Mecanismos de Reporte	Formativo	Formativo	o
D2.5 Mídia e Redes Sociais	Formativo para Estabelecido	Formativo	-
D3 Educação, Capacitação e Habilidades em Segurança Cibernética			
D3.1 Aumento da Conscientização	Formativo para Estabelecido	Formativo para Estabelecido	o
D3.2 Marco para a Educação	Formativo	Formativo para Estabelecido	++
D3.3 Marco para a Formação Profissional	Formativo	Formativo para Estabelecido	++
D4 Marcos Legais e Regulatórios			
D4.1 Marcos Jurídicos	Estabelecido	Estabelecido como estratégico	++
D4.2 Sistema de Justiça Criminal	Formativo	Formativo para Estabelecido	++
D4.3 Marcos de Cooperação Formais e Informais	Formativo	Formativo para Estabelecido	++

progresso notável foram registrados com nota neutra “o”. Qualquer regressão foi marcada como “--”/“-” de forma correspondente. É importante observar que a revisão do CMM 2021 criou alguns novos requisitos que devem ser atendidos para atingir os estágios de maturidade. A regressão ocorre como resultado destes novos requisitos, e não como uma regressão real na prática.

D5 Padrões, Organizações e Tecnologias			
D5.1 Adesão às Normas	Formativo para Estabelecido	Formativo para Estabelecido	o
D5.2 Resiliência da Infraestrutura da Internet	Estabelecido	Estabelecido como estratégico	++
D5.3 Qualidade de Software	Formativo	Formativo para Estabelecido	++
D5.4 Controles Técnicos de Segurança	Estabelecido	Formativo para Estabelecido	-
D5.5 Controles Criptográficos	Estabelecido	Formativo para Estabelecido	-
D5.6 Mercado de Segurança Cibernética	Formativo para Estabelecido	Formativo para Estabelecido	o
D5.7 Divulgação Responsável	Formativo para Estabelecido	Formativo para Estabelecido	o

Tabela 1: Desenvolvimento de capacidade comparando avaliações do CMM no Brasil em 2020 e 2023

Política e estratégia de segurança cibernética

A primeira estratégia nacional de segurança cibernética (NCS) brasileira, E-Ciber[3], foi adotado em fevereiro de 2020. Foi desenvolvido através de um processo de consulta com uma série de partes interessadas relevantes e apoiado por uma avaliação nacional do risco de cibersegurança, que está documentada na NCS. A NCS foi originalmente desenvolvida para ser válida por um ciclo de quatro anos: 2020-2023, após o qual foi planejada sua renovação. Uma mudança na administração brasileira provocou um atraso nesta renovação, o que levou a um acordo para prorrogar a validade da NCS existente por mais um ano. O processo de revisão está programado para começar no final de 2023.

Existe um programa de atividades destinadas a implementar a NCS, de acordo com um Plano de Ação da NCS. O programa de implementação da NCS inclui uma série de "Planos Nacionais" que se centram na criação da legislação e dos orçamentos necessários para implementar os objetivos estratégicos da NCS. Os vários componentes dos Planos Nacionais ainda não foram formalmente adotados, mas estão em várias fases do processo de aprovação pelo Congresso; alguns, como o Plano Nacional de Segurança de Infraestruturas Críticas (PlanSIC), já foram aprovados.

Embora várias atividades estejam em andamento para implementar vários aspectos da NCS, atualmente não está claro como os investimentos em todas as diferentes intervenções que formam o programa nacional de segurança cibernética estão sendo coordenados. Existe também atualmente uma monitorização limitada do impacto coletivo das intervenções realizadas: ainda não foram definidas métricas para monitorizar o impacto do programa nacional de cibersegurança. Prosseguem as discussões sobre quais organizações devem fazer parte do órgão de coordenação do programa nacional de cibersegurança implementado pela

[3] https://ciberseguranca.igarape.org.br/en/national-cybersecurity-strategy-e-ciber-2020

NCS. Há discussões em curso sobre a possível função que uma nova agência de segurança cibernética poderia assumir nesse sentido.

O Brasil participa ativamente de diversos fóruns e órgãos operacionais internacionais e regionais sobre segurança cibernética, e também está começando a participar no apoio a iniciativas regionais de criação de capacidades. Também foram tomadas medidas para melhorar a capacidade e coordenação da diplomacia cibernética: o Brasil nomeou seu primeiro diplomata cibernético em 2019, que participou de duas edições do GEG da ONU. Será importante continuar a aperfeiçoar os objetivos do envolvimento internacional e validar que eles são claramente compreendidos por todas as partes relevantes.

O Brasil é um país grande, com uma variedade de estruturas distribuídas que evoluíram para abordar vários aspectos da segurança cibernética, incluindo múltiplas Equipes de Resposta a Emergências Informáticas (CERTs) para fornecer resposta a incidentes: dois CERTs de nível nacional, CTIR.gov e CERT.br. e um grande número de CERTs subnacionais. Este arranjo distribuído funciona de forma eficaz. É importante estar ciente de que os incidentes cibernéticos são muitas vezes inerentemente transversais e, como tal, a sua resposta deve muitas vezes funcionar em todos os setores e instituições. É, portanto, especialmente importante, em particular para a resposta a incidentes cibernéticos, que a capacidade de resposta das várias partes envolvidas como um todo seja eficaz e testada regularmente. Recomendamos que seria benéfico testar (por exemplo, através de exercícios práticos ou teóricos) as capacidades de colaboração e intercâmbio rápido de informações entre as diversas entidades nacionais, regionais e setoriais.

Da mesma forma, a gestão de crises no Brasil não é centralizada, mas organizada por setores, com cada setor tendo sua própria equipe de gestão de crises que responde às crises que afetam o seu setor. De modo geral, os participantes na revisão do CMM consideraram que a integração da segurança cibernética na gestão de crises era eficaz, tendo sido fortalecida através da prática em eventos reais e periodicamente através de um programa robusto de exercícios de crise. Em particular, o Exercício Cyber Guardian é realizado anualmente desde 2018 e centra-se na proteção do CI contra cenários de crise cibernética e na coordenação de testes e treinamentos entre os setores público e privado nesses cenários. Embora a abordagem descentralizada e aplicada regularmente seja considerada sólida, é fundamental continuar a testar periodicamente as capacidades das várias entidades relevantes para se coordenarem contra uma vasta gama de potenciais cenários de cibersegurança. Os resultados destes exercícios devem ser avaliados para estabelecer lições aprendidas periodicamente atualizadas. Ao estabelecer as lições aprendidas, deve considerar-se se seria benéfico designar um órgão responsável pela coordenação da gestão de crises cibernéticas (e apoiar processos mais amplos de gestão de crises em que exista um elemento de segurança cibernética) e/ou integrar formalmente a segurança cibernética, num quadro mais amplo de gestão de crises.

O Plano Nacional de Segurança de Infraestruturas Críticas (PlanSIC) foi aprovado pelo Decreto 11.200 em setembro de 2022.[4] Através do PlanSIC, são feitos progressos na identificação de infraestruturas críticas (IC), na coordenação e atribuição de responsabilidades pela sua proteção e no desenvolvimento de padrões de segurança cibernética recomendados para todos os setores de CI. Muitos elementos do PlanSIC ainda não estão totalmente implementados e, como tal, a segurança cibernética ainda não está regulamentada em todos os setores de CI.

[4] https://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2022/Decreto/D11200.htm

Os participantes afirmaram que a estrutura regulatória ainda não foi decidida; e está atualmente em fase de estudo incluído nos trabalhos dos grupos técnicos constituídos e será levado ao congresso para discussão. Durante as sessões de revisão do CMM, houve algum debate entre os participantes sobre os benefícios relativos de atribuir a competência para regular a segurança cibernética em todos os setores de CI a um único órgão, como a agência nacional de segurança cibernética planejada ou a GSI, ou desenvolver a estrutura regulamentar por setor. Neste último caso, os participantes expressaram a opinião de que a agência ou o GSI ainda poderia desempenhar um papel valioso na coordenação e no apoio aos reguladores individuais do setor de CI, por exemplo, recomendando padrões mínimos de segurança cibernética intersetoriais.

Na prática, o nível de regulamentação da cibersegurança varia atualmente entre os diferentes setores de IC. Os requisitos de cibersegurança são definidos por alguns reguladores do setor, cada um dos quais tem autonomia na gestão do seu setor em relação à cibersegurança, e com diferentes níveis de requisitos e monitorização de conformidade como resultado. Os setores mais avançados nesse sentido foram a Administração Pública Federal (PFA), o setor financeiro e o setor de telecomunicações. Nos setores regulamentados de CI, as operadoras implementam boas práticas de segurança cibernética. Fora destes setores, os participantes relataram que muitas organizações implementam boas práticas de segurança cibernética e autoavaliações em relação aos padrões reconhecidos da indústria, embora o nível do curso varie entre as organizações.

Existem várias políticas e doutrinas para a segurança cibernética na defesa nacional. A Política de Defesa Cibernética foi publicada em 2012 e a primeira Doutrina de Defesa Cibernética foi aprovada em 2014. A cibersegurança também foi identificada na Estratégia Nacional de Defesa como uma das três prioridades estratégicas, juntamente com nuclear e espacial, desde 2008. No final de 2020, foram estabelecidas novas leis diretrizes e organizacionais para a defesa cibernética. Os participantes relataram que importantes decretos e instrumentos jurídicos desde 2020 levaram a uma implementação mais consistente da doutrina e a uma melhor capacidade de participação internacional.

No Brasil existem capacidades de defesa cibernética e estruturas organizacionais. Existem unidades cibernéticas dentro de cada uma das três forças (Marinha, Exército e Aeronáutica), bem como um comando conjunto (ComDCiber). A Escola Nacional de Ciberdefesa oferece formação aos oficiais do comando conjunto e das unidades cibernéticas das três forças, sendo também ministrada formação às unidades cibernéticas das forças individualmente, sendo o exercício descrito como uma parte crítica da formação. Foram descritos alguns desafios relacionados com orçamentos insuficientes para a defesa cibernética, com o objetivo relatado de desenvolver um planejamento baseado em capacidades para avaliar e colocar em prática os recursos necessários.

Foi relatado que desde o CMM 2020, a coordenação entre as entidades civis e de defesa foi melhorada, através de uma maior integração entre o IC e as entidades de defesa. A responsabilidade do Ministério da Defesa (MoD) no que diz respeito à proteção das CI foi formalizada através do PlanSIC, embora ainda não tenham sido definidas funções e orçamentos específicos para tal. Estão também em curso esforços para melhorar a compreensão da dependência das entidades militares e de segurança nacional relativamente à segurança cibernética de outras partes da IC através de grupos técnicos que estão analisando a interdependência entre setores da IC (incluindo os militares).

Cultura e sociedade de segurança cibernética

As discussões entre as partes interessadas indicaram a presença de iniciativas que abordam a conscientização para os riscos de segurança cibernética em todas as agências governamentais, incluindo algumas agências que antecipam proativamente novos riscos de segurança cibernética. No entanto, os relatórios externos discutidos nos meios de comunicação social também documentam algumas deficiências: criticam a falta de atividade dos gestores empresariais no setor público, apontando uma incompatibilidade entre as iniciativas de conscientização dentro das agências governamentais e o nível real de sensibilização relativamente aos riscos de segurança cibernética. A real priorização da segurança cibernética entre agências governamentais parece variar amplamente, incluindo lacunas significativas dentro de algumas agências. Da mesma forma, as práticas seguras de cibersegurança não parecem ser implementadas de forma adequada, embora existam diretrizes e procedimentos. Pelas razões expostas, o setor público seria atualmente considerado no nível estabelecido.

Relativamente ao setor privado, o nível de conscientização varia consoante a dimensão das empresas. As principais empresas públicas e privadas têm um nível muito elevado de conscientização para a cibersegurança, fazem da cibersegurança uma prioridade e também implementam práticas seguras de cibersegurança. No entanto, as pequenas e médias empresas carecem de recursos e conhecimentos relativamente às práticas de segurança cibernética e, por razões financeiras, a segurança cibernética raramente é uma prioridade. As partes interessadas não apontaram quaisquer pesquisas sistemáticas, métricas ou outros indicadores/fontes de informação sobre a conscientização dos usuários da Internet, seu conhecimento sobre práticas seguras e sua priorização de segurança cibernética. É essencial que o Brasil conduza estudos sistemáticos e colete métricas. Pela ausência de métricas ou estudos, o nível de maturidade em relação aos internautas não pode ser avaliado como superior ao Formativo. Uma proporção limitada, mas crescente, de utilizadores da Internet tem um nível mínimo de conscientização em relação aos riscos de segurança cibernética e segue práticas seguras.

Conforme indicado, há uma falta geral de estudos sistemáticos e métricas no Brasil sobre os usuários da Internet e seu comportamento. Portanto, o nível de confiança dos usuários da Internet não pode ser avaliado com certeza e os respetivos estudos, incluindo métricas relevantes, devem ser realizados. Devido a diversas iniciativas, pode-se presumir que o nível de confiança dos usuários nos serviços online se encontra numa fase de formação. Métricas e estudos sistemáticos, bem como uma extensa campanha dirigida ao público, levariam presumivelmente rapidamente a atingir a fase “Estabelecida”. As iniciativas também abordam a desinformação, o que significa que pelo menos uma fase Formativa também é alcançada neste aspecto. Em relação ao governo eletrônico, governo digital e comércio eletrônico, o Brasil já havia alcançado um patamar elevado no CMM anterior (2020). A etapa Brasil permanece no nível Estabelecido. Em 2019, 48% de todas as transações bancárias foram realizadas online e o número duplicou desde então. Os bancos introduziram um novo sistema seguro para transações online instantâneas, que foi bem recebido pelos usuários.

A compreensão dos usuários sobre a proteção de informações pessoais online precisa de ser revista no contexto de uma nova Lei Geral sobre a Proteção de Dados Pessoais (LGPD), que

está amplamente alinhada com o RGPD da UE.[5] A ANPD é o órgão fiscalizador nacional da proteção de dados pessoais e também realiza iniciativas de conscientização; Suas atividades e a implementação e fiscalização da LGPD indicam que uma proporção cada vez maior de usuários possui habilidades para gerenciar sua privacidade online.[6,7]. Isto é apoiado por relatos da mídia.[8]

O CTIR e os CERTs sectoriais fornecem mecanismos de elaboração de relatórios para o setor público e privado. O CERT.br atua como um CSIRT de última instância em nível nacional, onde também, em geral, os usuários podem reportar incidentes. Contudo, os mecanismos de denúncia não são promovidos entre o público em geral. Por conseguinte, deveria ser criada uma plataforma e uma entidade especificamente destinadas aos usuários da Internet em geral e, potencialmente, também às PME.

Além dos grandes incidentes de cibersegurança, a cobertura mediática é principalmente dedicada à fraude financeira. As reportagens dos meios de comunicação social poderiam ser mais amplas e, também ter como objetivo aumentar a conscientização dos cidadãos e a promover melhores práticas. As discussões nas mídias sociais ocorrem de maneira ad hoc. O Brasil não tem uma cultura positiva de denúncias de irregularidades. A maioria das reportagens sobre denúncias não é encontrada na mídia.

Criação de Conhecimento e Capacidades em Segurança Cibernética

No Brasil existem diversas campanhas de conscientização sobre segurança cibernética. Mais importante ainda, o internetsegura.br, uma iniciativa do NIC.br e do CERT.br, presta assessoria ao público em geral.[9]As campanhas e atividades do NIC.br e suas suborganizações poderiam se beneficiar de um maior apoio governamental, por exemplo, por meio de maior financiamento e promoção apoiados pelo governo. O impacto destes programas não é monitorizado através de inquéritos ou métricas orientadas para resultados. Seria benéfico uma coordenação sistemática e um portal específico para o público em geral. As partes interessadas indicaram que muitas campanhas de conscientização são realizadas pelo setor privado, particularmente no setor bancário, uma vez que isto também é impulsionado por requisitos do regulador. Novamente, não há análises sistemáticas utilizando métricas e estudos, e as diversas iniciativas do setor privado não são coordenadas centralmente. Empresas internacionais de capacitação em segurança cibernética também oferecem cursos para executivos no Brasil.[10] O setor privado poderia se beneficiar de cursos obrigatórios de cibersegurança em todos os setores para executivos das empresas.

---

[5] "General Personal Data Protection Act (LGPD)", lgpd-brazil.info, consultado em 22 de outubro de 2023, https://lgpd-brasil.info/.

[6] "Autoridade Nacional de Proteção de Dados", ANPD, consultada em 22 de outubro de 2023, https://www.gov.br/anpd/pt-br.

[7] "How to protect your personal data", ANPD, consultada em 22 de outubro de 2023, https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_senacon_ingles.pdf.

[8] Angélica Mari, "Data privacy awareness grows in Brazil", ZDNET, 15 de maio de 2020, https://www.zdnet.com/article/data-privacy-awareness-grows-in-brazil/.

[9] "Secure Internet", internetsegura.br, consultado em 22 de outubro de 2023, traduzido por *Firefox Full page Translation*, https://internetsegura.br/.

[10] "Cyber Security Training – Brazil", The Knowledge Academy, acessado em 22 de outubro de 2023, https://www.theknowledgeacademy.com/br/courses/cyber-security-training/.

As partes interessadas indicaram que os cursos de Ciência da Computação oferecidos nas universidades são harmonizados por meio de um currículo coordenado pela Sociedade Brasileira de Computação (SBC).[11] Os interessados também indicaram que a SBC concluiu a preparação da definição de um curso de graduação em segurança cibernética em 2022, o que permitirá às universidades oferecer um programa inteiramente dedicado à segurança cibernética. No entanto, ainda não há evidências disponíveis online para o programa deste curso. Em particular, a segurança cibernética ainda não é um tema amplamente adotado em disciplinas não técnicas e não está claro se as universidades também oferecem palestras e seminários sobre segurança cibernética destinados a um público não especializado, por exemplo, em cursos de direito ou de ética. Embora a SBC também aborde a educação em ciências da computação no currículo do ensino fundamental e médio, não está claro se a segurança cibernética faz realmente parte destes níveis, além disso, dado que o ensino fundamental e médio é parcialmente da responsabilidade do nível de governo municipal e estadual. Os participantes indicaram que, embora existam muitas iniciativas e atividades, o sistema educativo se beneficiaria de uma coordenação mais coerente da educação em matéria de cibersegurança.

No que diz respeito à formação vocacional e profissional, as partes interessadas indicaram que não existe atualmente uma coordenação nacional dessa formação. Existem muitas iniciativas ad hoc e da indústria. No entanto, existe uma lacuna significativa na força de trabalho e um problema com a mudança de profissionais qualificados para o estrangeiro devido aos salários mais elevados. As partes interessadas indicaram que uma das principais desvantagens do cenário da formação profissional é uma abordagem transversal que integra os requisitos da indústria com a oferta de educação com foco no profissional.

De acordo com as partes interessadas, as atividades de P&D em cibersegurança são realizadas principalmente como parte de atividades convencionais de investigação em ciências informáticas, por exemplo, como parte de investigação e desenvolvimento em segurança de redes ou sistemas. O principal obstáculo para atingir o nível Estabelecido é a falta de financiamento nacional sistemático especificamente para questões de segurança cibernética e que também vai além do domínio da tecnologia e da informática. Uma próxima versão de uma estratégia nacional de cibersegurança deverá considerar a disponibilização de financiamento específico deste tipo, que também aborde disciplinas para além da tecnologia e da informática. Além disso, as métricas devem ser implementadas sistematicamente para medir o desempenho das atividades de P&D em segurança cibernética.

Marcos Jurídicos e Regulatórios

A legislação substantiva sobre crimes cibernéticos foi revisada de forma abrangente na Revisão do CMM de 2020 do Brasil; o leitor deve consultar o relatório de 2020 para obter uma lista detalhada de crimes cibernéticos e leis criminais específicas. As partes interessadas indicaram que as leis relativas à cadeia de custódia digital foram melhoradas:[12] Graças à legislação secundária, a cadeia de custódia digital pode agora ser plenamente estabelecida, auxiliando nas investigações criminais e no direito processual penal (por exemplo, LEI Nº

[11] "Sociedad Brasileira de Computação", SBC, consultada em 22 de outubro de 2023, https://www.sbc.org.br/.

[12] O termo "cadeia de custódia digital", nesse contexto, refere-se à documentação da propriedade de um ativo digital (por exemplo, dados) e sua transferência de uma pessoa ou organização para outra, incluindo a data exata, a hora e a finalidade da transferência, entre outros.

14.155, DE 27 DE MAIO DE 2021[13] foi adaptado para incluir aspectos digitais). Segue a norma ISO 17005. O Brasil assinou a Convenção de Budapeste e a implementação de seus requisitos na legislação nacional está em andamento, embora muitos requisitos já tenham sido implementados antes da assinatura da convenção. O segundo protocolo da Convenção de Budapeste é de particular importância para o Brasil, pois melhora as possibilidades de cooperação internacional e intercâmbio de informações para as autoridades brasileiras. No entanto, o Brasil já foi integrado em redes de cooperação policial, por exemplo, através da Interpol e do G7. A abordagem geral do Brasil ao crime cibernético baseia-se na abordagem do crime cibernético através da lei convencional. Uma lei específica para o cibercrime só é introduzida quando a lei convencional não consegue cobrir adequadamente os casos de cibercrime. Por exemplo, os casos de ransomware são tratados como extorsão convencional. Atualmente, a legislação brasileira não exige que violações de dados sejam comunicadas, desde que não incluam dados pessoais. No que diz respeito aos dados pessoais, estes são abrangidos pela recentemente introduzida Lei Geral de Proteção de Dados Pessoais (LGPD), que é semelhante ao RGPD da UE.[14] Alguns setores, por exemplo o bancário, exigem relatórios obrigatórios. No entanto, seria útil um requisito geral de apresentação de relatórios obrigatórios, provavelmente em todos os setores. Devido às atividades em andamento para melhorar as disposições legais e regulatórias, o Brasil já pode ser considerado parcialmente no nível Estratégico. Contudo, as partes interessadas indicaram que nenhuma avaliação sistemática do impacto nos direitos humanos foi realizada no que diz respeito à lei do crime cibernético, embora alguns aspectos sejam cobertos pela LGPD.

Conforme observado, o Brasil implementou uma estrutura abrangente para a proteção de dados pessoais (LGPD). A supervisão é assegurada através de uma agência líder designada, a ANPD. O Brasil também possui uma lei de proteção à criança em vigor para o domínio digital, que é revisada e adaptada periodicamente. A proteção do consumidor on-line é coberta principalmente pela legislação convencional. Entretando, o phishing não é atualmente considerado um ato criminoso em si. Os participantes afirmaram que a criminalização do phishing levaria a um aumento considerável nas investigações criminais; no entanto, deveria ser considerada uma lei que pudesse abranger o estabelecimento sistemático de infraestruturas para fins de phishing. Além disso, a criminalização do phishing por si só levaria presumivelmente a uma diminuição das campanhas de phishing devido ao efeito dissuasor da criminalização. A Propriedade Intelectual é protegida pela lei convencional. No entanto, a lei não foi concebida especificamente no que diz respeito aos riscos on-line.

A capacidade institucional no Brasil varia muito, dependendo do pessoal específico e do nível de administração. O Brasil não possui atualmente um centro de jurisdição centralizado para casos de crimes cibernéticos, que também poderia ser acessado pela polícia estadual; em vez disso, essa capacidade está integrada à Polícia Federal. A polícia a nível estatal também tem de investigar casos de crimes cibernéticos, mas não existe nenhum mecanismo entre os estados ou entre os níveis estadual e federal para garantir capacidades suficientes e partilha de conhecimentos. De acordo com as partes interessadas, o número de peritos na aplicação da lei permaneceu quase inalterado ao longo dos últimos 20 anos, o que é insuficiente para resolver todos os casos de cibercriminalidade. No que diz respeito aos procuradores, as partes interessadas relataram que os recursos, competências e capacidades satisfazem as necessidades atuais. No entanto, a situação parece ser diferente com os tribunais. As partes interessadas afirmaram que os tribunais parecem não ter juízes com formação suficiente para

[13] "LEI Nº 14.155, DE 27 DE MAIO DE 2021", GSI, consultado em 2 de novembro de 2023, https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm.

[14] "General Personal Data Protection Act (LGPD)", lgpd-brazil.info, consultado em 22 de outubro de 2023, https://lgpd-brasil.info/.

alguns casos de cibercriminalidade. De acordo com as partes interessadas, os organismos reguladores dispõem de pessoal adequado e possuem as competências e capacidades necessárias.

Conforme observado acima, o Brasil assinou e ratificou a Convenção de Budapeste. Os esforços atuais incluem a integração de uma capacidade 24 horas por dia, 7 dias por semana, que permite à polícia brasileira buscar e responder a solicitações de assistência. As partes interessadas também indicaram que as colaborações público-privadas funcionam sem problemas e que o intercâmbio entre o setor privado, os serviços de informações e as forças armadas está estabelecida e funciona bem. Entretando, esta afirmação não pôde ser confirmada através de fontes externas. A vontade de colaborar e trocar abertamente informações, especialmente por parte da indústria privada e de ONG, poderia ser ainda maior se o intercâmbio de informações fosse confiado a uma agência de segurança cibernética separada da comunidade de inteligência, militar e policial.

Padrões e tecnologias

Ainda não foi identificada uma base de referência acordada a nível nacional de padrões e boas práticas relacionadas com a segurança cibernética para orientar as organizações dos setores público e privado. A NCS estabelece como ação estratégica (dentro da Ação Estratégica 2.3.1) melhorar a adoção de padrões internacionalmente reconhecidos pelos setores público e privado. Vários padrões são seguidos em setores mais avançados e organizações maiores. Na Administração Pública Federal (PFA) e nos setores financeiro e de telecomunicações, o cumprimento dos padrões de segurança cibernética é orientado pela regulamentação. Em outros setores, a implementação de normas de cibersegurança é mais ad hoc e não é supervisionada por uma autoridade, embora estejam disponíveis fontes de orientação.

Para promover a adoção consistente de padrões de segurança cibernética em organizações de todos os setores e níveis de maturidade, pode ser benéfico desenvolver uma linha de base acordada nacionalmente de padrões e boas práticas relacionadas à segurança cibernética, contra a qual organizações de setores públicos e privados possam, em alguns casos, serem auditadas e, em outros, autoavaliadas. Isto deve incluir padrões para aquisição de tecnologia e padrões para segurança tecnológica e prestação de serviços.

Os controles de segurança tecnológica são implementados por organizações dos setores público e privado. Dada a variabilidade nos níveis de adoção de padrões entre organizações, o nível de implementação destes controles varia significativamente entre diferentes setores e tamanhos de organização. Nos setores regulamentados acima descritos, há um alto nível de implantação de controle técnico e criptográfico de acordo com os padrões internacionais. Nos setores que não estão regulamentados para a implementação de padrões de cibersegurança, existem, como seria de esperar, diferentes níveis de implementação de controles de segurança técnicos e criptográficos.

Alguns participantes expressaram a opinião de que muitas organizações do setor privado não estão implementando controles técnicos de segurança a um nível adequado para gerenciar riscos, com controles irregulares e manuais e processos ausentes ou raramente são atualizados. Os participantes também expressaram algumas preocupações sobre os níveis mais baixos de adoção de controles técnicos e criptográficos apropriados pelas PME, que normalmente têm recursos financeiros limitados para investir em segurança cibernética. Muitas PME dependem de serviços em nuvem e foram levantadas preocupações sobre a falta de conhecimento sobre como configurar e manter instâncias em nuvem com segurança, o que poderia levar à vulnerabilidade.

Os fornecedores de serviços de Internet, especialmente os de maior dimensão, oferecem uma gama de controles técnicos de segurança aos seus clientes intermediários. Atualmente estão em andamento campanhas para aumentar a adoção de controles anti-DDoS e anti-spoofing por parte dos ISPs para proteger seus clientes finais. Alguns prestadores de serviços estão implementando ferramentas como o TLS para proteger as comunicações entre servidores e usuários, e o governo procura aumentar a adoção de certificados digitais e protocolos de segurança que eles permitem.

Atualmente não existe um catálogo de plataformas e aplicações de software seguras disponíveis para organizações dos setores público e privado, nem há orientações consistentes fornecidas a todas as organizações sobre o desenvolvimento e manutenção de software seguro. Em alguns setores, existem diretrizes e requisitos regulatórios em torno da segurança de software. Por exemplo, para a PFA, existe um inventário de software seguro e existem processos para desenvolver e manter software seguro de acordo com os regulamentos. Os setores financeiro e de telecomunicações também têm alguns requisitos regulamentares para a segurança de software. Em outros setores como o elétrico, existem disposições que estabelecem que as empresas devem ter políticas de desenvolvimento e manutenção de software seguro; no entanto, esses critérios não são regulamentados.

Fora dos setores mais maduros descritos acima, a qualidade e a segurança do software são variáveis. Os participantes não tinham conhecimento das recomendações dadas pelo governo sobre o desenvolvimento de software seguro, a seleção de aplicações de software seguras ou a manutenção de software seguro, que se estenderiam às organizações do setor privado. Os participantes expressaram a opinião de que seria conveniente orientar todas as organizações sobre plataformas e aplicativos de software seguros, o que orientaria todas as organizações no Brasil na seleção do software a ser usado. Além disso, pode ser vantajoso estender a orientação a todas as organizações sobre os processos de desenvolvimento e manutenção de software seguro.

No Brasil, serviços confiáveis de Internet estão amplamente disponíveis e são usados regularmente, inclusive para transações comerciais e de comércio eletrônico, e processos de autenticação adequados foram estabelecidos para a maioria das transações. Em geral, os participantes concordaram que existe um alto nível de resiliência da infraestrutura brasileira de internet e parece que nenhum evento no Brasil causou interrupções significativas neste tipo de serviço. Isso se deve em grande parte à estrutura descentralizada, já que há muitos Provedores de Serviços de Internet (ISPs) operando no Brasil, bem como a presença de muitos Pontos de Troca Tráfego de Internet (IXPs).

O setor de telecomunicações é regulamentado em geral e em termos de segurança cibernética pela Agência Nacional de Telecomunicações, Anatel, que estabelece diversos requisitos de segurança cibernética. Os participantes relataram que os requisitos de segurança cibernética da Anatel ainda não são obrigatórios, mas pretendem ser. Estas regras aplicam-se, em teoria, a todos os operadores de telecomunicações. A Anatel destacou que, na prática, com cerca de 1.500 PSI no país, não é possível realizar auditorias para todas as operadoras. Como tal, não está claro se estas práticas (gestão de tecnologias implementadas, avaliações de risco, monitorização de redes e testes de resiliência, e planos de resposta a incidentes) são consistentemente alcançadas entre fornecedores de infraestruturas de Internet. No geral, os participantes concordaram que a cibersegurança operacional é forte entre os ISPs de maior dimensão, mas que pode haver lacunas no que diz respeito aos ISPs de pequena e média dimensão.

Em geral, os participantes concordaram que a maioria das tecnologias de segurança cibernética no Brasil são importadas do exterior, muitas vezes através de integradores nacionais. Embora exista alguma produção nacional de tecnologias de cibersegurança e o mercado interno pareça estar crescendo, os produtos de cibersegurança criados internamente não são atualmente os líderes de mercado. Existe uma variabilidade no grau em que as organizações são atualmente capazes de identificar e gerir as implicações de segurança da dependência de tecnologias estrangeiras. Isto poderia criar riscos no contexto de uma cadeia de abastecimento internacional.

Existem amplos serviços de consultoria em segurança cibernética disponíveis para organizações públicas e privadas no Brasil. Os participantes descreveram um mercado ativo, com muitas empresas nacionais e grandes empresas internacionais oferecendo serviços de consultoria. A compreensão das organizações sobre como avaliar o risco e a confiabilidade ao contratar um provedor de serviços de segurança cibernética varia dependendo da sua maturidade e apetite por risco. Atualmente não há nenhum credenciamento de prestadores de serviços de cibersegurança por um órgão nacional. Isto pode ser útil para orientar as organizações na seleção de prestadores de serviços confiáveis e seguros, especialmente para organizações com conhecimento limitado de segurança cibernética, para embasar suas decisões.

Há um uso generalizado de serviços em nuvem pelas organizações brasileiras. Algumas organizações realizam avaliações de risco para determinar como mitigar os riscos de terceirização de TI para terceiros ou serviços em nuvem; Em particular, as organizações de maior dimensão tendem a ter requisitos de segurança em vigor quando adquirem serviços. Para alguns setores, incluindo a PFA e o setor financeiro, isto é impulsionado pela regulamentação. Foram destacadas questões potenciais para as PME, uma vez que muitas delas dependem de serviços em nuvem para serviços de TI e de segurança cibernética. Os participantes descreveram a falta de compreensão de como usar a nuvem com segurança em organizações que não possuem uma equipe dedicada de TI ou de segurança cibernética. Isso produz erros de configuração ou falhas de atualização, gerando uma vulnerabilidade. Poderia ser conveniente ampliar a conscientização ou formação mais substancial às PME para a utilização segura da nuvem e avaliação de riscos, ou emitir orientações específicas sobre segurança na nuvem adequadas para organizações que têm menos recursos e capacidades e de segurança cibernética.

O mercado de seguros cibernéticos no Brasil está em seus estágios iniciais. Foi relatado que a maioria das ofertas de produtos de seguros cibernéticos vem de companhias de seguros multinacionais, e os participantes estão cientes de que existem poucas empresas locais que oferecem produtos de seguros cibernéticos. Até recentemente, a adesão às ofertas de seguros cibernéticos tem sido feita principalmente por grandes empresas multinacionais, mas a demanda por parte das organizações brasileiras está supostamente começando a crescer. A necessidade de produtos específicos de seguro cibernético foi reconhecida e os participantes relataram que o seguro de continuidade de negócios no Brasil não tende a cobrir incidentes cibernéticos. Foi levantada a questão da acessibilidade dos produtos de seguro cibernético oferecidos atualmente, o que impede que algumas organizações de contratarem apólices de seguro cibernético. Embora tenham sido relatadas algumas discussões do grupo de trabalho sobre a acessibilidade das ofertas de seguros cibernéticos, também não está claro se houve alguma identificação estratégica das necessidades do mercado de seguros cibernéticos. Identificar as necessidades das organizações no Brasil nessa área por meio da avaliação dos

riscos financeiros para os setores público e privado, bem como dos desafios relacionados aos custos, seria útil para informar o desenvolvimento do mercado de seguros cibernéticos.

INTRODUÇÃO

Em colaboração com o Escritório de Assuntos Exteriores, Commonwealth e desenvolvimento (FCDO) do Reino Unido e a Organização dos Estados Americanos (OEA), o Centro Global de Capacidade de Segurança Cibernética (GCSCC, ou "o Centro") conduziu uma revisão da maturidade das capacidades de segurança cibernética no Brasil a convite do Gabinete de Segurança Institucional da Presidência da República (GSI). O objetivo desta revisão foi determinar áreas de capacidade nas quais o Governo poderia investir estrategicamente, para que pudesse melhorar seu estado de segurança cibernética nacional.

Durante o período de 28 a 30 de agosto de 2023, foi realizado um processo de consulta de três dias no Brasil. Isto foi precedido por uma fase de pesquisa documental em que os investigadores do GCSCC recolheram informações de documentos disponíveis on-line e fornecidos pelo GSI. As partes interessadas das seguintes organizações participaram pessoalmente nas consultas:

- Entidades do setor público:
  - Gabinete Institucional da Presidência da República (GSI)
  - Ministro da Defesa
  - Ministério da Educação
  - Departamento da Agricultura
  - Ministério da Gestão e Inovação nos Serviços Públicos
  - Ministério da Justiça e Segurança Pública
  - Ministério das Comunicações
  - Ministério de Relações Exteriores
  - Ministério de Minas e Energia
  - Ministério do Desenvolvimento, Indústria, Comércio e Serviços
  - Ministério do Planejamento e Orçamento
  - Ministério do Trabalho e Emprego
  - Agência Brasileira de Inteligência (ABIN)
  - Agência Nacional de Energia Elétrica
  - Agência Nacional de Telecomunicações (ANATEL)
- Polícia Federal
- Representantes militares e de defesa
- Universidades
- Sociedades profissionais
- Provedores de serviços de telecomunicações e provedores de serviços de Internet (ISPs)
- Operadores de infraestrutura crítica (CI)
- Equipes nacionais e subnacionais de resposta a emergências informáticas (CERTs)
- Provedores de serviços e tecnologia de segurança cibernética

DIMENSÕES DA CAPACIDADE DE SEGURANÇA CIBERNÉTICA

As consultas basearam-se no Modelo de Maturidade de Capacidade de Segurança Cibernética (CMM) do GCSCC,[15]que é composto por cinco dimensões diferentes de capacidade de segurança cibernética (ver Figura 3).

Figura 3. Dimensões do CMM.

[15] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations, Edição de 2021", março de 2021, https://gcscc.ox.ac.uk/the-cmm#/.

Cada Dimensão consiste num conjunto de *Fatores,* que descrevem e definem o que significa ter capacidade de segurança cibernética. A Tabela 2: Dimensões e Fatores considerados no CMM. mostra as cinco Dimensões juntamente com os *Fatores* que cada uma apresenta:

DIMENSÕES	***FATORES***
Dimensão 1 **Política e estratégia de segurança cibernética**	D1.1 Estratégia Nacional de Segurança Cibernética D1.2 Resposta a incidentes e gestão de crises D1.3 Proteção de infraestrutura crítica (CI) D1.4 Cibersegurança em Defesa e Segurança Nacional
Dimensão 2 **Cultura e sociedade de segurança cibernética**	D2.1 Mentalidade de segurança cibernética D2.2 Confiança e segurança nos Serviços On-line D2.3 Compreensão do usuário sobre proteção de informações pessoais on-line D2.4 Mecanismos de reporte D2.5 Mídia e plataformas on-line
Dimensão 3 **Criação de conhecimento e capacidades em segurança cibernética**	D3.1 Aumentar a conscientização sobre segurança cibernética D3.2 Educação em segurança cibernética D3.3 Formação Profissional em Cibersegurança D3.4 Pesquisa e Inovação em Segurança Cibernética
Dimensão 4 **Marcos Jurídicos e regulatórios**	D4.1 Disposições Jurídicas e regulamentares D4.2 Marcos legislativos relacionados D4.3 Competências e capacidades jurídicas e regulamentares D4.4 Marcos de cooperação formais e informais para combater o crime cibernético

DIMENSÕES	*FATORES*
Dimensão 5	D5.1 Aderência aos padrões
Padrões e tecnologias	D5.2 Controles de segurança
	D5.3 Qualidade de software
	D5.2 Resiliência de comunicação e infraestrutura de Internet
	D5.5 Mercado de segurança cibernética
	D5.6 Divulgação responsável

Estágios de maturidade da capacidade de segurança cibernética

Cada *Dimensão* contém uma série de *Fatores* que descrevem o que significa ter capacidade de segurança cibernética. Cada *Fator* apresenta uma série de *Aspectos* que agrupam Indicadores relacionados, que descrevem etapas e ações que, uma vez observadas, definem o estado de maturidade daquele Aspecto. Existem cinco estágios de maturidade, que vão desde o estágio inicial até o estágio dinâmico. A etapa inicial implica uma abordagem *ad hoc* da capacidade, enquanto a etapa dinâmica representa uma abordagem estratégica e a capacidade de se adaptar dinamicamente ou de se modificar em resposta a considerações ambientais. As cinco *Etapas* são definidas da seguinte forma:

- **Início:** neste *Cenário*, ou não existe maturidade em termos de cibersegurança ou a sua natureza é muito embrionária. Poderão existir discussões iniciais sobre o desenvolvimento de capacidades de cibersegurança, mas não foram tomadas medidas concretas. Pode haver uma ausência de evidência observável no *Cenário*;

- **Formativo:** algumas características do *Aspecto* começaram a crescer e a se formular, mas podem ser *Ad hoc*, desorganizado, mal definido ou simplesmente nova. Contudo, a evidência desta atividade pode ser claramente demonstrada;

- **Estabelecido:** existem indicadores do *Aspecto* e as evidências mostram que eles estão funcionando. Contudo, não há uma consideração bem pensada da alocação relativa de recursos. Poucas decisões de compromisso foram tomadas relativamente ao investimento relativo nos vários elementos do *Aspecto*. Ainda assim, o *Aspecto* é funcional e definido;

Tabela 2: Dimensões e Fatores considerados no CMM.

- **Estratégico:** foram tomadas decisões sobre quais partes do *Aspecto* são importantes e quais são menos importantes para uma organização ou nação específica. A fase

Estratégica reflete o fato de estas escolhas terem sido feitas, condicionadas às circunstâncias particulares da nação ou organização; e

- **Dinâmico:** neste *Estágio*, existem mecanismos claros para alterar a estratégia nacional dependendo das circunstâncias prevalecentes, tais como tecnologia ambiental de ameaça, conflito global ou uma mudança significativa numa área de preocupação (por exemplo, crime cibernético ou privacidade). Há também provas de liderança global em questões de segurança cibernética. Pelo menos setores-chave criaram métodos para mudar estratégias em qualquer fase do seu desenvolvimento. A rápida tomada de decisões, a realocação de recursos e a atenção constante ao ambiente em mudança são características deste *Estágio*.

A atribuição dos estádios de maturidade baseia-se na evidência recolhida, incluindo a visão geral ou consensual das contas apresentadas pelas partes interessadas, a investigação documental e o julgamento profissional dos investigadores do GCSCC. Utilizando a metodologia GCSCC estabelecida acima, este relatório apresenta os resultados da revisão da capacidade de segurança cibernética do Brasil e conclui com recomendações sobre os próximos passos que poderiam ser considerados para melhorar a capacidade de segurança cibernética no país.

CONTEXTO DE SEGURANÇA CIBERNÉTICA NO BRASIL

O Brasil é um país grande que cobre aproximadamente 8,5 milhões de quilômetros quadrados (cerca de metade da área total da América do Sul). Sua população é de aproximadamente 216 milhões de pessoas. No início de 2023, havia cerca de 181,8 milhões de usuários de Internet no Brasil: uma taxa de penetração da Internet de 84,3%, com cerca de 70,6% da população também usando mídias sociais.[16]Há também um uso generalizado de conexões de telefonia móvel celular, cujo número no início de 2023 equivale a 102,4 por cento da população.

O Brasil está dividido em 26 estados e um distrito federal. Cada uma dessas unidades federativas possui governo e constituição próprios, com substancial grau de autonomia.[17]Os estados são ainda divididos em municípios. Os governos locais partilham com o governo federal a responsabilidade pela prestação de serviços públicos, assumindo a responsabilidade primária por serviços como educação, saúde e aplicação da lei, com assistência financeira e técnica do governo federal. Há aspectos, como o ensino superior e a aplicação da lei relacionados com o crime organizado, pelos quais se assume maior responsabilidade a nível federal.

É importante levar em consideração o sistema federal, bem como o grande tamanho do país (em termos de território e população), ao avaliar a segurança cibernética do Brasil, pois levam a variações significativas em todo o país nas medidas de implementação tomadas e nos níveis de segurança cibernética, capacidade e recurso.

Em termos de prontidão do Brasil de aproveitar as oportunidades oferecidas pelas tecnologias digitais, o Network Readiness Index 2022 Camboja* classificou o Brasil em 44º lugar entre 131 economias que incluídas, com desempenho acima da média do grupo de renda média alta nos quatro pilares: Tecnologia, Pessoas, Governança e Impacto. Seu principal ponto forte está relacionado às Pessoas, enquanto o maior espaço para melhorias está relacionado ao Impacto.[18]

O Brasil participa do Índice Global de Cibersegurança (IGC) da União Internacional de Telecomunicações (UIT), tendo enviado recentemente respostas ao questionário da quinta edição. Na quarta edição de 2020, o Brasil ficou em 18º lugar mundial e em 3º lugar entre 35 países da região das Américas.[19]As medidas legais foram apontadas como uma área de relativa força, enquanto as medidas técnicas e organizacionais foram uma área de crescimento potencial.

[16]https://datareportal.com/reports/digital-2023-brazil
[17]https://forumfed.org/document/republica-federal-de-brasil/
[18]https://networkreadinessindex.org/country/brazil/
[19]https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Como Estado membro da Associação da Organização dos Estados Americanos (OEA), o Brasil participa do programa de segurança cibernética da OEA[20]e sua Rede CSIRTAmericas, bem como diversas iniciativas, debates e instâncias de formação em segurança cibernética com outros países da região. O Brasil também participa ativamente de organizações e fóruns internacionais relevantes, com a participação de representantes do Ministério das Relações Exteriores, do GSI e do Comando de Defesa Cibernética (ComDCiber) e de outras agências. Isto inclui a participação nas discussões sobre segurança cibernética da UIT e do G20 e a participação ativa no Grupo de Trabalho Aberto das Nações Unidas (OEWG) sobre Tecnologias de Informação e Comunicação (TIC), nos Especialistas Governamentais das Nações Unidas sobre a Promoção do Comportamento Responsável do Estado no Ciberespaço no Contexto do Segurança Internacional (GGE) e grupos de trabalho ad hoc da ONU, inclusive sobre crime cibernético[21]. O Brasil presidiu o GGE da ONU duas vezes (2014-15 e 2019-21)[22]. As partes interessadas relevantes relataram que os representantes brasileiros fizeram contribuições ativas em torno da aplicação do direito internacional no ciberespaço, da evolução das ameaças cibernéticas e da proteção da CI, bem como da necessidade de garantir que os processos da ONU se concentrem na necessidade de desenvolver capacidade global de segurança cibernética.

Uma série de intervenções foram feitas desde a última revisão do CMM pelo GCSCC, que foi publicada em 2020. As principais intervenções incluem o desenvolvimento de planos legais para a proteção de infraestruturas críticas (CI), a formalização da coordenação da resposta a incidentes dentro do governo federal e a assinatura da Convenção de Budapeste sobre Crime Cibernético.

Estas intervenções estão em diferentes fases de implementação e nem todas tiveram ainda tempo suficiente para gerar progressos suficientemente significativos para levar a um aumento na fase de maturidade avaliada de acordo com o CMM. Além disso, os desafios políticos, incluindo uma mudança de governo, causaram alguns atrasos, especialmente na renovação da estratégia nacional de cibersegurança (NCS), que deveria ser lançada em 2023, mas foi adiada por um ano. No entanto, estas intervenções representam um forte progresso no sentido de alcançar níveis mais elevados de maturidade em segurança cibernética no país, conforme descrito ao longo deste relatório.

As recomendações que fazemos neste relatório fornecem nossa opinião sobre as melhorias na capacidade de segurança cibernética e a maturidade das capacidades que o Brasil deve considerar para priorização. Em alguns casos, o trabalho já está em curso como parte de projetos em curso, mas incluímos novamente a recomendação, uma vez que a capacidade ainda não foi totalmente alcançada. O momento desta revisão do CMM também oferece oportunidades para fazer recomendações que podem apoiar a próxima renovação da NCS.

[20] https://www.oas.org/es/topics/ciber_security.asp

[21] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[22] https://disarmament.unoda.org/group-of-gubernamental-experts/

RELATÓRIO DE REVISÃO

DESCRIÇÃO GERAL

Esta seção fornece uma representação geral da capacidade de segurança cibernética no Brasil. A Figura 4 abaixo apresenta as estimativas de maturidade em cada *Dimensão*. Cada Dimensão representa um quinto do gráfico, portanto os cinco estágios de maturidade de cada Fator se estendem para fora do centro do gráfico; "início" está mais próximo do centro do gráfico e "dinâmico" é colocado no perímetro.

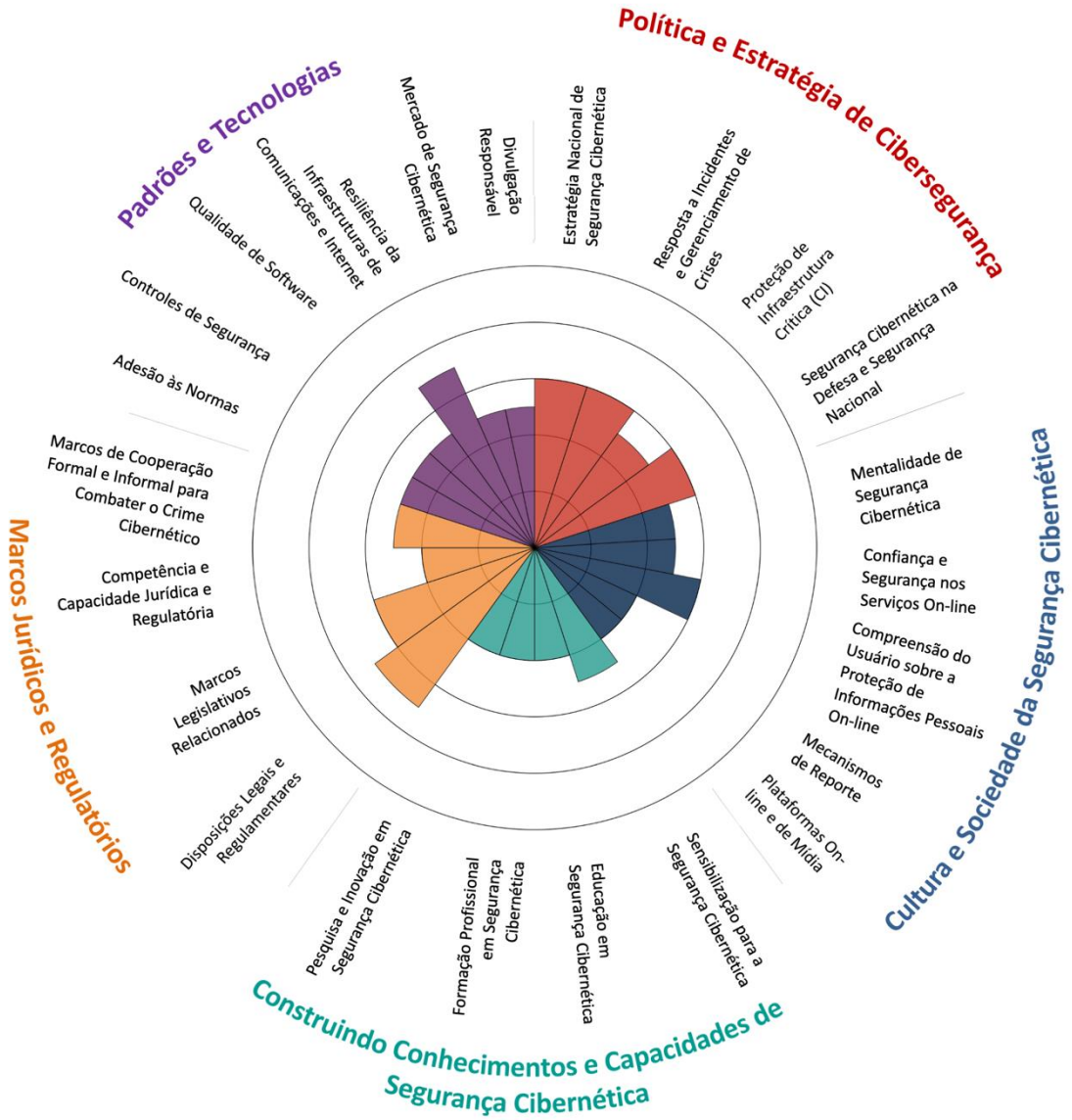


Figura 4: Representação geral da capacidade de segurança cibernética no Brasil – revisão CMM 2023

Esta foi a segunda avaliação do CMM do Brasil, após a primeira em 2020. A capacidade de segurança cibernética do Brasil também foi avaliada por meio de um questionário baseado no CMM do Estudo Regional conduzido pela Organização dos Estados Americanos (OEA) e pelo Banco Interamericano de Desenvolvimento (BID) em 2016 e novamente em 2020 (os resultados de 2020). O estudo regional baseou-se na revisão do CMM de 2020.

A Figura 5 abaixo mostra a representação geral da capacidade de segurança cibernética no Brasil, conforme apresentada no relatório CMM 2020. O CMM foi revisado em 2021 para refletir o cenário em constante mudança de risco e controle de segurança cibernética e o ambiente operacional. Portanto, existem algumas diferenças entre o CMM utilizado na revisão de 2020 e na revisão de 2023; as diferenças na estrutura das dimensões e na formulação dos nomes dos Fatores podem ser vistas nos gráficos.

Uma comparação entre a Figura 4 e a Figura 5 indica até que ponto a capacidade de segurança cibernética no Brasil, medida pelo CMM, mudou nos últimos quatro anos.

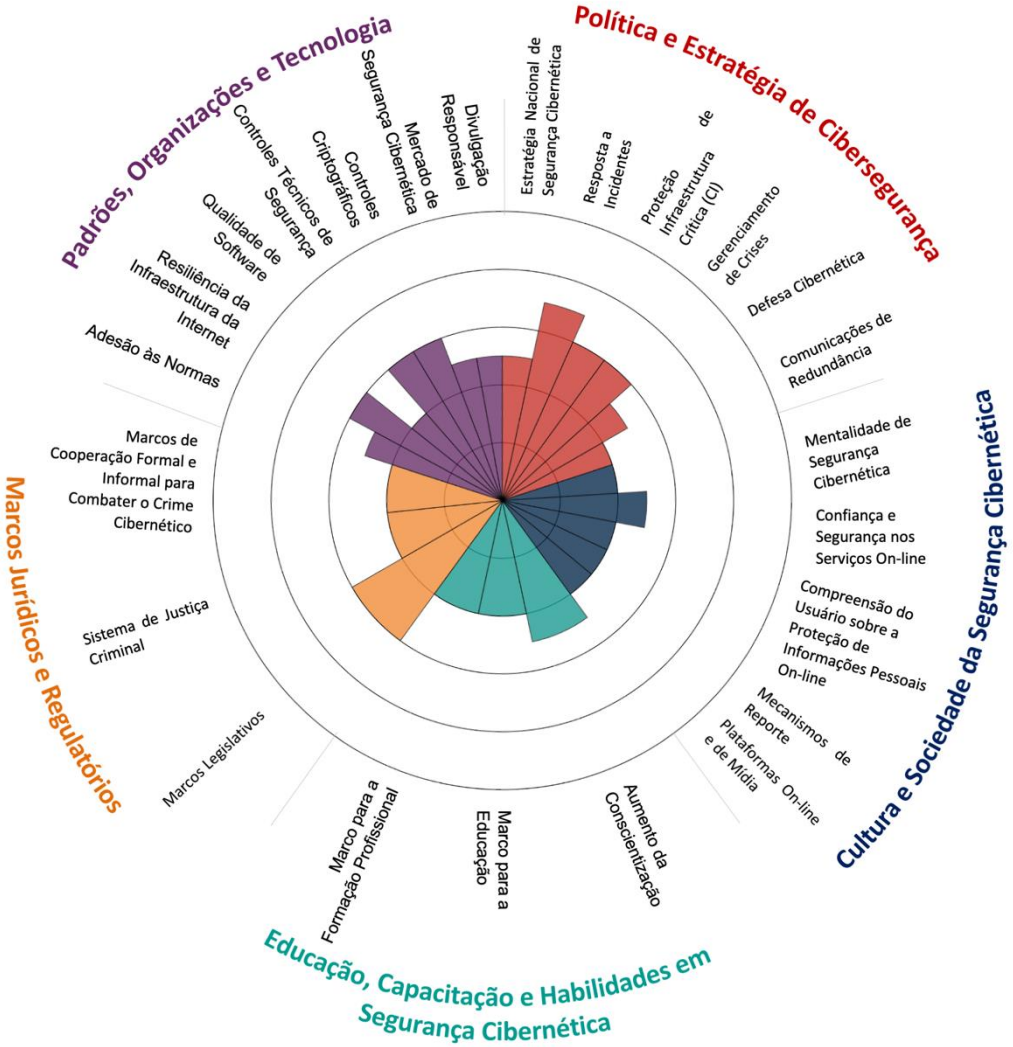


Figura 5: Representação geral da capacidade de segurança cibernética no Brasil – revisão CMM 2020

A Tabela 2 apresenta um resumo do desenvolvimento de capacidades para todos os fatores avaliados em 2020 e em 2023.

	Estagio de maturidade‡		Mudanças de capacidade*
Fatores baseados no CMM 2017	**2020**	**2023**	
D1 Política e estratégia de segurança cibernética			
D1.1 Estratégia Nacional de Segurança Cibernética	Formativo para Estabelecido	Estabelecido	++
D1.2 Resposta a incidentes	Estabelecido como Estratégico	Estabelecido	-
D1.3 Proteção de infraestrutura crítica	Estabelecido	Formativo para Estabelecido	-
D1.4 Gestão de crises	Estabelecido	Estabelecido	o
D1.5 Defesa cibernética	Formativo para Estabelecido	Estabelecido	++
D1.6 Redundância de Comunicações	Formativo	Estabelecido	++
Cultura e sociedade de segurança cibernética			
D2.1 Mentalidade de segurança cibernética	Formativo	De formativo a Estabelecido	++
D2.2 Confiança e segurança na Internet	Formativo para Estabelecido	Formativo para Estabelecido	o
D2.3 Compreensão do usuário sobre informações pessoais	Formativo	Estabelecido	++
D2.4 Mecanismos de reporte	Formativo	Formativo	o
D2.5 Mídia e redes sociais	Formativo para Estabelecido	Formativo	-
D3 Educação, capacitação e habilidades em segurança cibernética			
D3.1 Conscientização	Formativo para Estabelecido	Formativo para Estabelecido	o
D3.2 Marco para a educação	Formativo	Formativo para Estabelecido	++
D3.3 Marco para a formação profissional	Formativo	Formativo para Estabelecido	++

‡ Para fins de compatibilidade com versões anteriores, este resumo apresenta os níveis de maturidade observados na avaliação do CMM 2023 no âmbito de uma versão anterior do CMM que serviu de base para a revisão do CMM Brasil 2020.

*Os fatores que avançaram para o próximo estágio de maturidade receberam a classificação "+ +". Os fatores que registaram melhorias em alguns dos seus indicadores, mas não progrediram o suficiente para justificar uma melhoria na próxima fase de maturidade, foram marcados com "+". Fatores sem progresso notável foram registrados com nota neutra "o". Qualquer regressão foi marcada como "- -"/"-" correspondentemente. É importante observar que a revisão do CMM 2021 criou alguns novos requisitos que devem ser atendidos para atingir os estágios de maturidade. A regressão ocorre como resultado destes novos requisitos, e não como uma regressão real na prática.

D4 Marcos legais e regulatórios			
D4.1 Marcos jurídicos	Estabelecido	Estabelecido como estratégico	++
D4.2 Sistema de justiça criminal	Formativo	Formativo para Estabelecido	++
D4.3 Marcos de cooperação formais e informais	Formativo	Formativo para Estabelecido	++
D5 Padrões, organizações e tecnologias			
D5.1 Aderência aos padrões	Formativo para Estabelecido	Formativo para Estabelecido	o
D5.2 Resiliência da infraestrutura da Internet	Estabelecido	Estabelecido como estratégico	++
D5.3 Qualidade de software	Formativo	Formativo para Estabelecido	++
D5.4 Controles técnicos de segurança	Estabelecido	Formativo para Estabelecido	-
D5.5 Controles criptográficos	Estabelecido	Formativo para Estabelecido	-
D5.6 Mercado de segurança cibernética	Formativo para Estabelecido	Formativo para Estabelecido	o
D5.7 Divulgação responsável	Formativo para Estabelecido	Formativo para Estabelecido	o

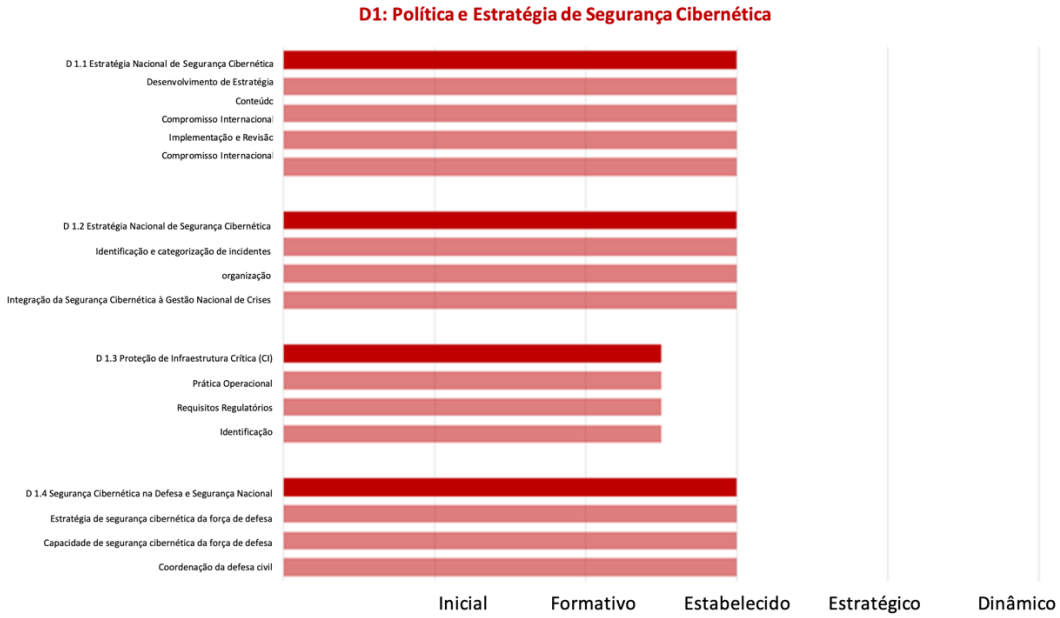
Tabela 2: Desenvolvimento de capacidade comparando avaliações CMM do Brasil em 2020 e 2023

DIMENSÃO 1
POLÍTICA E ESTRATÉGIA DE SEGURANÇA CIBERNÉTICA

Esta *Dimensão* explora a capacidade do Brasil de desenvolver e implementar uma estratégia de segurança cibernética e aumentar sua resiliência por meio do aperfeiçoamento de sua resposta a incidentes, defesa cibernética e capacidades de proteção de infraestrutura crítica. Considera estratégias e políticas eficazes para fornecer capacidade nacional de segurança cibernética, mantendo, ao mesmo tempo os benefícios de um ciberespaço vital para o governo, as empresas internacionais e a sociedade em geral.

Figura 6: Fatores e aspectos examinados na Dimensão 1

RESUMO DOS RESULTADOS



D1.1 ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA

A estratégia de cibersegurança é essencial para a integração de uma agenda de segurança cibernética a nível governamental, pois ajuda a priorizar à segurança cibernética como uma área política importante, determina as responsabilidades e os mandatos dos principais atores governamentais e não governamentais nesta área e orienta a alocação de recursos para as questões e prioridades existentes de segurança cibernética.

***Estágio*:** Estabelecido

A estratégia nacional de segurança cibernética (NCS) brasileira, E-Ciber, foi publicada[23]. A NCS foi aprovada pelo Decreto Presidencial nº. 10.222[24]e adotado em fevereiro de 2020. O desenvolvimento do NCS foi liderado pelo Gabinete de Segurança Institucional da Presidência da República (GSI), que propõe diretrizes e estratégias para a segurança cibernética através do Departamento de Segurança da Informação e Comunicações (DSIC). O exposto acima estava em conformidade com o disposto na Política Nacional de Segurança da Informação. (PNSI, Decreto nº 9.637, de 26 de dezembro de 2018), que previu a elaboração de um NCS integrado em módulos que abrangem cibersegurança, ciberdefesa, segurança de

[23] https:// cibersegurança.igarape.org.br/en/national-cybersecurity-strategy-e-ciber-2020/

[24] http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm

infraestruturas críticas (CI), segurança de informação confidencial e proteção contra vazamento de dados.

A NCS foi desenvolvida através de um processo de consulta com uma série de partes interessadas do governo, organizações dos setores público e privado, academia e sociedade civil. O processo de consulta e os grupos de partes interessadas consultados estão detalhados na introdução da NCS e, durante as sessões de revisão do CMM, as partes interessadas confirmaram a sua participação no processo e a consequente representação das suas necessidades e interesses na NCS. As consultas foram divididas em três subgrupos e foram realizadas 31 reuniões de subgrupos no total: 1) governança cibernética; dimensão normativa; Investigação, desenvolvimento e inovação; Educação; dimensão internacional e parcerias estratégicas; 2) confiança digital, prevenção e mitigação de ameaças; 3) proteção estratégica: governo e infraestrutura. Um rascunho foi então disponibilizado online para comentários públicos; Nesta etapa foi recebida a participação de 31 pessoas e 10 organizações públicas e privadas.

A NCS foi originalmente desenvolvida para ser válida por um ciclo de quatro anos: 2020-2023, após o qual foi planejada sua renovação. Uma mudança na administração brasileira provocou um atraso nesta renovação, o que levou a um acordo para prorrogar a validade da NCS existente por mais um ano. O processo de revisão está previsto para começar no final de 2023, sendo o GSI o órgão responsável pela revisão da atual NCS e pela elaboração da renovação. A GSI descreveu planos para envolver uma vasta gama de partes interessadas em consultas para o processo de renovação do NCS, incluindo organizações dos setores público e privado, universidades e sociedade civil, além de envolver instituições de investigação e desenvolvimento em segurança cibernética para considerar como avaliar o impacto das tecnologias emergentes. A GSI também descreveu planos para uma revisão de apoio da legislação atual relacionada com a segurança cibernética.

Os objetivos estratégicos são definidos na NCS: tornar o Brasil mais próspero e confiável no ambiente digital; aumentar a resiliência brasileira às ameaças cibernéticas; e fortalecer o papel brasileiro na segurança cibernética no cenário internacional. O conteúdo do N 2020-2023 está dividido em 10 ações estratégicas: 1) Fortalecer as ações de cibergovernança; 2) Estabelecer um modelo de governança centralizada a nível nacional; 3) Promover um ambiente participativo, colaborativo, confiável e seguro entre o setor público, o setor privado e a sociedade; 4) Elevar o nível de proteção governamental; 5) Elevar o nível de proteção das Infraestruturas Nacionais Críticas; 6) Melhorar o marco jurídico relativo à segurança cibernética; 7) Incentivar a concepção de soluções inovadoras de cibersegurança; 8) Ampliar a cooperação internacional do Brasil em segurança cibernética; 9) Expandir a aliança de cibersegurança entre o setor público, o setor privado, a academia e a sociedade; 10) Elevar o nível de maturidade da sociedade em segurança cibernética. Os participantes relataram que todas as cinco dimensões do CMM foram consideradas no processo de desenvolvimento do conteúdo da NCS.

A NCS foi desenvolvida com base numa avaliação dos riscos nacionais de cibersegurança específicos de cada país. Os resultados estão resumidos na seção “diagnóstico” da NCS. Isso considera riscos específicos de segurança cibernética para o Brasil e foi formulado com base em consultas às partes interessadas e estatísticas existentes (por exemplo, de uma pesquisa de terceiros com 200 empresas brasileiras em 2019 sobre as principais preocupações e ataques de segurança cibernética sofridos). Para a próxima renovação da NCS, será importante garantir que esta avaliação nacional dos riscos de segurança cibernética para apoiar o desenvolvimento de conteúdos da NCS. Isso deve incluir a consideração dos riscos de cibersegurança decorrentes do uso de tecnologias emergentes em infraestruturas críticas e

na sociedade em geral, e pode se basear em percepções sobre incidentes e ameaças cibernéticas divulgados nas redes de intercâmbio de informações.

Foi considerada a forma como o NCS pode apoiar objetivos mais amplos de política on-line, pois descreve a necessidade de alinhamento com a Estrutura dos Direitos Civis para a Internet (Lei nº 12.965 de 2014), que *"regula o uso da Internet no Brasil por meio do fornecimento de princípios, garantias, direitos e deveres para aqueles que utilizam a rede mundial, e diretrizes para a ação do Estado, protegendo os dados pessoais e a privacidade dos usuários no ambiente on-line"*, e considera explicitamente como isso deve informar o desenvolvimento de quadros jurídicos, bem como os termos do compromisso a nível internacional. As partes interessadas envolvidas no planeamento do processo de renovação do NCS também descreveram a necessidade de futuras consultas para considerar questões observadas em debates internacionais. Entre eles, destacam-se a inclusão de género e a inclusão social em termos de como promover a cultura da segurança cibernética numa sociedade social e economicamente diversa. Também foram descritos planos para se concentrar na revisão das disposições legais existentes para a proteção de crianças on-line e a proteção de informações pessoais como parte do processo de renovação do NCS.

Existe um programa de atividades concebido para implementar a NCS, de acordo com o seu Plano de Ação, que não foi fornecido à equipe de revisão da CMM, mas supostamente delineou as ações necessárias para implementar a NCS. O programa de implementação da NCS inclui uma série de "Planos Nacionais" que se centram na criação da legislação e dos orçamentos necessários para implementar os objetivos estratégicos do NCS. Juntamente com a NCS, estes Planos Nacionais foram idealizados pelo PNSI de 2018. Os vários componentes dos Planos Nacionais ainda não foram formalmente adotados, mas estão em vários estágios do processo de aprovação pelo Congresso; alguns, como o Plano Nacional de Segurança de Infraestruturas Críticas (PlanSIC), já foram aprovados (ver Secção D1.3).

Atualmente não está claro como os investimentos nas diferentes intervenções que compõem o programa nacional de segurança cibernética são coordenados. No momento, esse plano não tem um processo para alocar orçamento, nem para identificar e aumentar défices orçamentais que poderiam prejudicar a implementação da NCS. Os participantes salientaram a importância de alocar o orçamento necessário para várias componentes do programa nacional de segurança cibernética, para garantir que sejam feitos investimentos adequados nesta área para apoiar a transformação digital em curso. A intenção é que os Planos Nacionais acabem por criar um orçamento nacional dedicado à segurança cibernética, atribuído a um órgão de coordenação. Atualmente, para executar as ações do programa, as organizações investem em diversas campanhas de forma descentralizada. Os departamentos governamentais têm autonomia para decidir os seus investimentos em segurança cibernética e são feitas campanhas de conscientização para incentivar cada departamento governamental a alocar recursos para investir em segurança cibernética. Segundo informações, há planos para criar um novo tipo de despesa dentro do governo que permitiria que os departamentos governamentais alocassem formalmente recursos para a segurança cibernética.

Também não é claro como é monitorizado o impacto coletivo das intervenções realizadas. O Plano de Ação NCS não define métricas ou indicadores-chave de desempenho (KPI) para monitorizar a consecução dos resultados do programa nacional de cibersegurança. Como tal, existe apenas uma monitorização limitada do sucesso ou revisão de processos. O GSI descreveu as dificuldades atuais na medição das ações estratégicas para a NCS e relatou os esforços atuais para validar o progresso no programa de implementação da NCS através de

uma consultoria terceirizada, que validará o progresso atual e identificará métricas e indicadores para avaliar a concretização dos objetivos.

Como parte da próxima revisão da NCS, será importante garantir que exista um processo para alocar orçamento à implementação das diversas ações da NCS e identificar quaisquer défices orçamentais para que possam ser apresentados ao órgão de coordenação. O desenvolvimento de processos e métricas de revisão de programas com recursos adequados também será importante para permitir que um órgão de coordenação garanta de forma abrangente que os responsáveis pela implementação de vários aspectos da NCS sejam responsabilizados. Fornecerão também uma abordagem para identificar riscos, questões de implementação e dependências, que podem ser encaminhadas para o órgão de coordenação, conforme necessário. Portanto, será importante incluir a definição de processos e métricas de revisão da NCS na sua próxima revisão, apoiada pelas conclusões dos atuais esforços de validação.

Em termos de governança nacional da cibersegurança, o nível político e estratégico da governança da cibersegurança é atribuído ao GSI, enquanto a defesa cibernética é atribuída ao Ministério da Defesa (MoD). Prosseguem as discussões sobre quais organizações devem fazer parte do órgão de coordenação do programa nacional de cibersegurança implementado pela NCS. A NCS estabelece ações para o estabelecimento de um modelo centralizado de governança da cibersegurança, destacando os modelos centralizados adotados nos EUA, Reino Unido, Portugal, França, Índia, Malásia, Singapura, Coreia do Sul e Japão: "*é importante conceder a uma agência governamental a responsabilidade de orientar o tema em nível nacional, organizá-lo e propor medidas e regulamentações, com a participação de representantes de todos os setores da sociedade. Exceções são feitas apenas em aspectos relacionados à defesa cibernética e à guerra, que são de responsabilidade do Ministério da Defesa, o que em nenhum caso impede a necessária interação, neste sentido, entre as áreas de segurança e defesa"*.

A este respeito, há um debate em curso sobre a criação de uma nova agência nacional de cibersegurança para coordenar atividades entre setores, e a consideração de quais organizações farão parte desta agência. Esta nova agência é proposta no Novo Projeto de Lei da Política Nacional de Cibersegurança (PNCiber), que também propõe a criação de um novo Comitê Nacional de Segurança Cibernética e de um Escritório Nacional de Gestão de Crises Cibernéticas. O Projeto de Lei do PNCiber está atualmente em fase de discussão (e os resultados documentados da consulta foram fornecidos à equipe de revisão do CMM) para aprimorar o texto e realizar uma análise jurídica. Posteriormente, será submetido ao Congresso para aprovação.

A função e o modelo operacional da agência ainda não foram totalmente determinados; há uma discussão em curso entre as partes interessadas no país sobre os aspectos dos modelos internacionais nos quais poderiam se basear. Espera-se que no futuro esta agência consiga ter um orçamento nacional para a cibersegurança e coordenar as ações dos vários "proprietários" das ações da NCS. Há um debate sobre se esta agência poderia assumir um papel regulador intersetorial ou se o seu papel deveria centrar-se na promoção da colaboração, confiança e compromisso entre as partes interessadas. Alguns participantes levantaram preocupações sobre o potencial conflito entre esta agência impor requisitos obrigatórios e impor sanções, e a necessidade de promover um ambiente em que as partes interessadas estejam dispostas a envolver-se e colaborar. É importante que a função da agência esteja claramente definida: até que ponto tem uma função de supervisão estratégica, uma função de execução operacional, ou ambas. Também é importante definir claramente como as suas responsabilidades interagem com outras funções regulatórias e de segurança no governo: por exemplo, se a

agência tiver um papel regulatória, é preciso deixar claro como essa função interage com as estruturas regulatórias existentes no país.

O Brasil também participa ativamente de organizações e fóruns internacionais relevantes, com a participação de representantes do Ministério das Relações Exteriores, do GSI e do Comando de Defesa Cibernética (ComDCiber) e de outras agências. Isto inclui a participação nas discussões sobre segurança cibernética da UIT e do G20 e a participação ativa no Grupo de Trabalho Aberto das Nações Unidas (OEWG) sobre Tecnologias de Informação e Comunicação (TIC), nos Especialistas Governamentais das Nações Unidas sobre a Promoção do Comportamento Responsável do Estado no Ciberespaço no Contexto de Segurança Internacional (GGE) e grupos de trabalho ad hoc da ONU, inclusive sobre crime cibernético[25]. O Brasil presidiu o GGE da ONU duas vezes (2014-15 e 2019-21)[26]. As partes interessadas relevantes relataram que os representantes brasileiros fizeram contribuições ativas em torno da aplicação do direito internacional no ciberespaço, da evolução das ameaças cibernéticas e da proteção da CI, bem como da necessidade de garantir que os processos da ONU se concentrem na necessidade de desenvolver capacidade global de segurança cibernética.

As Equipes Brasileiras de Resposta a Incidentes de Segurança Cibernética (CSIRT) em nível nacional são membros do Fórum de Equipes de Resposta a Incidentes e Segurança (FIRST) em nível global, e especialistas brasileiros dão contribuição de destaque para as atividades e desenvolvimento do FIRST e outros fóruns internacionais do CERT, como o Fórum de Melhores Práticas do CERT do Fórum de Governança da Internet das Nações Unidas (IGF).

No nível regional, o Brasil é membro da Organização dos Estados Americanos (OEA) e participa de seu programa de segurança cibernética[27]e sua Rede CSIRTAmericas[28]. Os participantes relataram que o Brasil e a OEA estão considerando organizar conjuntamente eventos de segurança cibernética para a região. O Brasil também participa do Comitê Cibernético do projeto Agenda Digital do Mercado Comum do Sul (Mercosul), do qual o Brasil ocupa a presidência este ano, que estaria negociando um acordo sobre segurança cibernética e discutindo a possibilidade de desenvolver uma taxonomia comum de segurança cibernética para a região. Os participantes viram o Brasil como uma referência para a região e compartilharam sua experiência no desenvolvimento da capacidade nacional de segurança cibernética em eventos regionais para ajudar outros países da região.

O Brasil também está começando a participar ativamente no apoio a iniciativas regionais de capacitação. Por exemplo, em setembro de 2022, o Brasil assinou um memorando de entendimento (MoU) para colaborar no projeto CyberNet da UE. Este projeto visa estabelecer e operar o Centro de Competências Cibernéticas da América Latina e do Caribe (LAC4). O Brasil contribuirá para "*a identificação das necessidades de desenvolvimento de capacidade cibernética e o desenvolvimento de planos de capacitação da LAC4 para apoiar os esforços de segurança cibernética do Brasil e da região da LAC4*".[29]

Em termos de compromisso em nível internacional, o conteúdo da NCS detalha explicitamente a necessidade de ser guiado pelos princípios constitucionais brasileiros e pelos valores fundamentais que devem nortear o programa nacional de segurança cibernética, incluindo o respeito à democracia e aos direitos humanos, identificando como relevante o Marco Civil da

[25] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[26] https://disarmament.unoda.org/group-of-gubernamental-experts/

[27] https://www.oas.org/es/topics/ciber_security.asp

[28] https://csirtamericas.org/es

[29]https://www.eucybernet.eu/celebrating-the-signature-of-the-memorandum-of-understanding-with-brazil-to-establish-cooperation-in-lac4-activities /

Internet (Lei nº 12.965 de 2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709 de 2018), combinado com as políticas para o desenvolvimento da Internet brasileira. Na prática, os participantes relataram que o Brasil opta por participar amplamente nos debates internacionais e que os departamentos ou ministérios que representam o Brasil em fóruns internacionais consultariam e seriam coordenados pelo Ministério das Relações Exteriores. Também foram tomadas medidas para melhorar a capacidade e coordenação da diplomacia cibernética: o Brasil nomeou seu primeiro diplomata cibernético em 2019, que participou de duas edições do GEG da ONU.[30]

É importante garantir que haja validação periódica de que os objetivos nesta área sejam claros e compreendidos por todos os participantes envolvidos, e que exista um processo para monitorizá-los. O refinamento contínuo dos objetivos também é importante: por exemplo, o Brasil poderia eventualmente pretender expandir seus objetivos em relação à criação de comunidades internacionais de interesse em torno de metas específicas de política de segurança cibernética e de uma participação mais ativa promoção da capacidade de segurança cibernética em outros países.

D1.2 RESPOSTA A INCIDENTES E GERENCIAMENTO DE CRISES.

Esse Factor aborda a capacidade do Governo de identificar e determinar as características dos incidentes em todo o país. Analisa também a capacidade do Governo para organizar, coordenar e implementar a resposta a incidentes e se a segurança cibernética foi integrada ao marco quadro nacional de gestão de crises.

***Estágio*:** Estabelecido

O Brasil é um país grande, com uma série de estruturas distribuídas que evoluíram para lidar com vários aspectos da segurança cibernética, incluindo vários CERTs para fornecer resposta a incidentes. Este arranjo distribuído funciona de forma eficaz. É importante lembrar que os incidentes cibernéticos são muitas vezes frequentemente transversais e, como tal, a resposta a incidentes cibernéticos deve muitas vezes funcionar em todos os setores e instituições. Portanto, é especialmente importante que a capacidade das várias partes envolvidas para responder como um todo seja eficaz e testada regularmente. Nesta seção, descrevemos a configuração distribuída de equipes de resposta a incidentes altamente capacitadas no Brasil e fazemos algumas observações sobre os benefícios potenciais de testar a colaboração e as capacidades de intercâmbio rápido de informações entre as diversas entidades nacionais, regionais e setoriais.

Dois CERTs principais fornecem serviços de resposta a incidentes em escala nacional no Brasil: CTIR.gov e CERT.br. O Centro Brasileiro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR.gov) é responsável por coordenar a resposta a incidentes de segurança cibernética relacionados às redes Administração Pública Federal do Brasil (PFA).[31]Cada órgão da PFA é obrigado a ter a sua própria equipe de resposta a incidentes cibernéticos ou CSIRT e órgão de TI responsável. CTIR.gov fornece um ponto único de contato

[30] https://directionsblog.eu/unpacking-brazils-cyber-diplomacy/
[31] https://www.gov.br/ctir/pt-br/assuntos/rfc-2350-1/rfc-2350

para notificação de incidentes das instituições PFA, que é obrigatório para todas as instituições PFA. CTIR.gov foi criado em 2006 e faz parte do Departamento de Segurança da Informação e Cibersegurança (DSIC) do GSI. Além de receber notificações e fornecer suporte de resposta a incidentes, o CTIR.gov monitora ativamente as redes do governo em busca de ameaças e vulnerabilidades usando sensores e honeypots.

CERT.br é a Equipe Nacional de Resposta a Emergências Informáticas, que fornece serviços de gerenciamento de incidentes para qualquer rede conectada à Internet brasileira. É descrito como um "CSIRT Nacional de último recurso",[32]fornecendo um ponto central para notificação de incidentes, suporte técnico de gestão de incidentes para analisar e recuperar sistemas comprometidos e facilitar qualquer coordenação necessária entre profissionais de segurança para resposta a um incidente, especialmente para *"casos em que nenhum contato de tratamento de incidentes é conhecido para uma determinada rede*". É um serviço gratuito para a comunidade brasileira da Internet, financiado pelo registro de domínio e mantido pelo Centro de Informação da Rede Brasileira (NIC.br), órgão executivo do Comitê Gestor da Internet Brasileira (CGI.br). O reporte ao CERT.br é voluntário para todas as organizações. São mantidas estatísticas públicas de incidentes tratados e relatórios recebidos de CSIRTs, administradores de rede e usuários.[33]

As atividades do CERT.br têm como objetivo estratégico aumentar o nível de segurança e a capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil. Juntamente com os serviços de tratamento de incidentes, o CERT.br oferece capacitação e orientação em resposta a incidentes para funcionários do CSIRT e conduz iniciativas para incentivar a adoção de melhores práticas de segurança. Participam da formação de comunidades baseadas na confiança para compartilhar inteligência sobre ameaças, incluindo grupos no setor de energia administrados pela Petrobras e no setor financeiro, e incentivam o uso de Plataformas de Compartilhamento e Inteligência de Ameaças de Código Aberto (MISP) para compartilhamento de informações (incluindo a realização de workshops MISP). O CERT.br também monitora ativamente a Internet brasileira para detecção de incidentes e análise de tendências de ameaças atuais e emergentes, utilizando uma rede de honeypots e sensores, bem como executando um conjunto de honeypots em outros países para analisar tendências de ameaças.

Existem vários CERTs subnacionais no Brasil, muitos dos quais estão listados no site CERT.br[34]). Isto inclui os CERT dos organismos da PFA (conforme descrito acima) e os CERT dos vários setores. Por exemplo, para instituições acadêmicas, o CSIRT da Rede Acadêmica e de Pesquisa Brasileira, CAIS/RNP, é um CSIRT maduro e certificado pelo Modelo de Maturidade de Gerenciamento de Incidentes de Segurança (SIM3) que mantém e analisa um registro de incidentes, publica informações de capacitação e alertas para instituições acadêmicas no Brasil, atua na resposta a incidentes e promove práticas de segurança, além de ser membro do Fórum de Equipes de Segurança e Resposta a Incidentes, FIRST[35]. Os CERTs também existem nos setores financeiro, energético, de telecomunicações e de saúde, entre outros. Os CERTs subnacionais variam na sua capacidade, sendo que alguns obtiveram a acreditação SIM3, enquanto outros têm recursos mais limitados.

Tanto CTIR.gov quanto CERT.br coordenam-se com parceiros internacionais para compartilhar informações sobre ameaças e cooperar na resposta a incidentes cibernéticos. Tanto CTIR.gov

[32] https://www.cert.br/

[33] https://stats.cert.br/

[34] https://www.cert.br/csirts/brasil/

[35] https://www.first.org/members/teams/cais-rnp

quanto CERT.br são membros da FIRST[36]e representantes do CERT.br fazem contribuições importantes para o desenvolvimento das políticas e iniciativas da FIRST. CTIR.gov também é afiliado à Rede regional CSIRT Américas administrada pela Organização dos Estados Americanos (OEA),[37]e com o Grupo de Trabalho Antiabuso da América Latina e Caribe (LAC-AAWG), além de tratar de assuntos internacionais. A nível setorial, existe também alguma colaboração internacional na resposta a incidentes; Por exemplo, a Anatel é membro da Aliança de Segurança Cibernética para o Progresso Mútuo (CAMP), que fornece uma rede global para compartilhamento de informações e resposta coletiva.[38]

Os registros de incidentes são mantidos pelo CTIR.gov e CERT.br, bem como por vários CERTs subnacionais, que classificam e analisam seus registros de incidentes para obter insights que informam suas ações e para permitir a disseminação de alertas e recomendações aos seus constituintes, e publicam informações de tendências. on-line. CTIR.gov também relatou utilizar a análise de seu cadastro para estabelecer políticas públicas para melhorar o nível de segurança nas redes da PFA.

O nível de notificação de incidentes por parte das organizações varia de acordo com os seus requisitos regulamentares e capacidade de identificação de incidentes. Embora todos os organismos da PFA sejam obrigados a ter um CSIRT e a comunicar incidentes ao CTIR.gov, os participantes relataram que a sua capacidade e experiência para identificar e responder a incidentes variam. No setor financeiro, as organizações são obrigadas a reportar incidentes ao Banco Central do Brasil (BACEN), de acordo com a sua regulamentação setorial (conforme descrito mais detalhadamente em D1.3), embora os participantes novamente tenham notado variação na capacidade das organizações do setor financeiro para identificar e relatar incidentes. Da mesma forma, os provedores de telecomunicações são obrigados a notificar incidentes de segurança cibernética ao seu regulador, a Anatel, por meio de Resolução nº 740 de 2020, e as organizações do setor têm capacidades diversas para fazê-lo. O CERT.br descreveu a variação nos níveis de relatórios e informações compartilhadas pelas organizações dentro de sua abrangência, com organizações mais maduras tendendo a relatar e participar sistematicamente no compartilhamento de informações, enquanto organizações menores podem relatar apenas nos casos em que necessitam de assistência.

Existem algumas iniciativas para apoiar as organizações no desenvolvimento da sua capacidade de resposta a incidentes. Os participantes relataram que existe uma iniciativa para criar um centro de especialização para prestar apoio às organizações governamentais na identificação e resolução de incidentes, especialmente para organizações com níveis mais baixos de maturidade e pessoal especializado limitado. Além disso, os CERTs subnacionais são apoiados no desenvolvimento de sua capacidade por meio de eventos como o Fórum Brasileiro de CSIRTs, organizado pelo CERT.br, que inclui workshops e tutoriais sobre temas como acreditação SIM3.[39]O CERT.br possui auditores SIM3 qualificados e está trabalhando com a OpenCSIRT Foundation para criar perfis para SIM3, contra os quais o CERT.br planeja credenciar CSIRTs brasileiros a partir do próximo ano. O CERT.br também auxilia novos CSIRTs no estabelecimento de suas atividades no Brasil.

Desde a revisão do CMM de 2020, houve iniciativas para formalizar a coordenação da gestão federal de incidentes cibernéticos e estendê-la voluntariamente a empresas públicas, empresas de capital misto empresas e suas subsidiárias. A Rede Federal de Gerenciamento de

[36] https://www.first.org/members/teams/

[37] https://csirtamericas.org/en/member_teams),

[38] https://www.cybersec-alliance.org/camp/index.do

[39] https://forum.cert.br/

Incidentes Cibernéticos (ReGIC) foi formalmente criada em 2021 pelo Decreto 10.748, de 16 de julho de 2021,[40]de acordo com o disposto na Política Nacional de Segurança da Informação de 2018 (embora os participantes tenham relatado que na prática esta rede está em desenvolvimento desde 2006). Trata-se de uma rede intergovernamental de equipes de resposta a incidentes cibernéticos, coordenada por CTIR.gov, cujo objetivo é melhorar a coordenação da resposta a incidentes entre entidades da PFA.

De acordo com o Decreto que institui o ReGIC, é obrigatória a participação de "*órgãos e entidades da administração pública federal direta, autônoma e fundacional" no ReGIC; A participação das "empresas públicas e sociedades de economia mista federais e suas subsidiárias"* é voluntária e ocorre mediante adesão. O ReGIC tem como objetivo "*melhorar e manter a coordenação entre órgãos e entidades da administração pública para a prevenção, tratamento e resposta a incidentes cibernéticos para elevar o nível de resiliência da cibersegurança dos seus ativos de informação. Tem como objetivo divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos; compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas; divulgar informações sobre ataques cibernéticos; promover a cooperação entre os participantes da Rede e incentivar a rapidez na resposta a incidentes cibernéticos"*.

Além disso, em 2022 foi aprovado o Plano de Gestão de Incidentes Cibernéticos da administração pública federal (PlanGIC) pela Portaria GSI/PR 120[41]e entrou em vigor. Este plano estabelece os procedimentos de gestão de incidentes cibernéticos a serem observados pelos participantes da rede ReGIC. De acordo com o PlanGIC, todos os participantes no ReGIC devem notificar os incidentes cibernéticos ao CTIR.gov (ou no caso de entidades externas à PFA que sejam membros voluntários, reportar à equipe de coordenação setorial a que estão vinculados). CTIR.gov compartilha alertas, informações sobre ameaças e vulnerabilidades, recomendações e estatísticas relacionadas a incidentes cibernéticos com membros da rede ReGIC.

Fora do ReGIC, existe intercâmbio regular de informações sobre ameaças e vulnerabilidades em alguns setores; No entanto, isto varia de acordo com o nível de regulamentação e capacidade de segurança cibernética do setor. Para o setor de telecomunicações, o regulador Anatel informou manter um fórum constante para a troca de informações sobre ameaças cibernéticas (CTI) e informações sobre vulnerabilidades entre as operadoras, com o envolvimento de outros órgãos, como o serviço de inteligência, ABIN, por meio de canais anonimizados e eficientes. O setor financeiro também reportou um elevado nível de intercâmbio de CTI entre os operadores.

O setor de Defesa possui seu próprio Plano Setorial de Gestão de Incidentes Cibernéticos (PSGIC-Def), estabelecido através da Portaria nº 4.174 do Ministério da Defesa, de 16 de agosto de 2023, destinado a orientar a coordenação da resposta a incidentes entre as equipes de resposta a incidentes do MoD e das três forças armadas. O plano supostamente busca alinhamento com as melhores práticas previstas no Modelo SIM3. Uma outra Portaria do MoD (#4138 de 14 de agosto de 2023) estabelece funções de coordenação entre o setor de Defesa e o ReGIC.

Ainda não existe um requisito de relatório de incidentes consistente em todas as organizações de CI no Brasil. Conforme descrito mais detalhadamente em D1.3, o progresso no sentido da regulamentação da segurança cibernética da CI está sendo feito no âmbito do Plano Nacional de Segurança de Infraestruturas Críticas (PlanSIC), que descreve responsabilidades e afirma

[40] http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm

[41] https://www.in.gov.br/pt/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918

que o GSI é o órgão coordenador da atividade de segurança cibernética da CI. Os requisitos do PlanSIC ainda não estão totalmente implementados, mas, foi relatado, eventualmente resultarão em um requisito regulamentado para que o CI informe incidentes cibernéticos. O Decreto ReGIC também estabeleceu em 2021 que as agências reguladoras do Brasil, Banco Central do Brasil e Comissão Nacional de Energia Nuclear são responsáveis por estabelecer ou designar uma equipe de coordenação setorial para "*equipe de prevenção, tratamento e resposta a incidentes cibernéticos"* e que esses órgãos são responsáveis por *"coordenar as atividades de segurança cibernética e centralizar as notificações de incidentes de outras equipes do setor regulado"*. A implementação deste requisito está em andamento.

Como a notificação ainda não é obrigatória em todo o CI, CTIR.gov ainda não recebe relatórios de incidentes cibernéticos de forma confiável em todo o CI. Os relatórios são recebidos numa base ad-hoc através da participação voluntária de entidades fora da PFA no ReGIC, através de relações informais com CERTs e reguladores setoriais (por exemplo, foram descritos relatórios regulares de incidentes da Anatel, a autoridade para o setor das telecomunicações, para o GSI). , e por meio de notificação de incidentes relevantes pelo CERT.br. Os representantes das autoridades setoriais na revisão afirmaram que atualmente, se uma autoridade setorial ou CSIRT considerasse que um incidente poderia ter um impacto intersetorial, eles se coordenariam de forma informal com os setores relevantes, apoiados pelo CERT.br ou CTIR. governo

Este conjunto informal de relações parece estar funcionando bem, mas é preciso considerar se essas relações informais funcionariam em um incidente cibernético complexo e transversal, como as funções do CTIR.gov e do CERT.br poderiam evoluir para proporcionar uma melhor colaboração entre setores e se haveria benefícios em formalizar a missão intersetorial do CERT.br (ou seja, os tipos de organizações que são responsáveis de apoiar). Os exercícios práticos poderiam ajudar a esclarecer estes processos.

Além disso, embora vários CERTs maduros tenham registros de incidentes, estes não estão atualmente consolidados em uma única lista. Isto pode dificultar a avaliação de tendências em toda a economia ou a obtenção de um aviso antecipado de forma fiável sobre um incidente que possa afetar várias organizações. Na prática, os participantes relataram uma forte coordenação e relações baseadas em confiança entre os CSIRTs, particularmente CERT.br e CTIR.gov, interagindo conforme necessário (por exemplo, com o CERT.br notificando o CTIR.gov sobre quaisquer incidentes ou ameaças identificadas que possam impactar as redes governamentais), significam que informações relevantes são intercambiadas e que uma visão geral suficiente é mantida por essas duas entidades. Há também relatos de fortes relações entre CTIR.gov e CERT.br, e os CERTs subnacionais, em termos de troca de informações.

No entanto, é importante verificar se os atuais registos distribuídos são suficientemente coordenados para permitir a identificação, categorização e resposta a um incidente cibernético a nível nacional (ou seja, um incidente que conduz ou contribui para um cenário de crise) em toda a gama de possíveis cenários e condições. Além disso, é importante garantir que a visibilidade dos incidentes de segurança cibernética no Brasil seja suficientemente coordenada para permitir a análise de tendências que possam informar a estratégia nacional e a alocação de recursos para atividades de segurança cibernética.

Com base nos resultados dos testes desses aspectos do acordo atual, pode ser conveniente considerar se o CTIR.gov ou o CERT.br deveriam ser responsáveis pela manutenção de um registro central. É importante notar que as disposições do PlanSIC descrevem os requisitos de notificação para o CI que deverão eventualmente levar a uma capacidade mais forte do CTIR.gov para manter um registo abrangente de relatórios de incidentes dentro do CI; No

entanto, estas disposições ainda não foram totalmente implementadas. Também pode ser benéfico formalizar as condições e os limites para o intercâmbio e escalonamento de informações, e os processos e pontos de contacto existentes para o intercâmbio de informações entre CSIRT, incluindo pontos de contacto e responsabilidades, a fim de garantir que todas as funcionalidades necessárias são institucionalizadas e pode continuar a funcionar em caso de mudança de pessoal, por exemplo. Os participantes na revisão do CMM sugeriram a possibilidade de uma agência nacional de cibersegurança planejada para assumir uma função facilitadora em relação ao rápido compartilhamento de informações e à colaboração eficaz entre as diversas entidades nacionais, regionais e setoriais.

Os participantes da revisão relataram que a gestão de crises no Brasil não é centralizada, mas organizada por setor, com cada setor tendo sua própria equipe de gestão de crises que responde às crises que afetam seu setor. Além disso, no caso de uma crise relacionada à segurança cibernética, o GSI observou que seria criado um comitê interagências, sendo CTIR.gov também responsável por orientar o GSI e o Gabinete do Presidente, e que eles podem fornecer apoio para ativar uma sala de crise que reúna as principais partes interessadas de todos os setores. Não existe, no entanto, nenhuma integração formal do quadro nacional de gestão de crises de cibersegurança, nem foi atribuída uma autoridade de gestão de incidentes cibernéticos.

De modo geral, os participantes na revisão do CMM consideraram que a integração da segurança cibernética no gerenciamento de crises como sendo eficaz, tendo sido fortalecida por meio da prática tanto em eventos do mundo real como em exercícios. Na última década, o Brasil sediou vários grandes eventos mundiais, incluindo a visita do Papa (2013), a Copa do Mundo de futebol (2014) e os Jogos Olímpicos (2016). O alto nível de coordenação necessário para proteger o CI contra possíveis ataques criou uma sólida experiência e relacionamentos, que, segundo os participantes, sustentam um sistema eficaz. Também foi relatado que o Brasil tem ajudado outros países com capacidade nesta área: foi dado o exemplo de o Brasil ajudar o Peru a preparar seu centro de operações cibernéticas antes de sediar os Jogos Pan-Americanos de 2019.

A abordagem à coordenação intersetorial também é testada regularmente através de um forte programa de exercícios de crise. Em particular, o Exercício Cyber Guardian, organizado pelo Comando de Defesa Cibernética (ComDCiber) em parceria com o GSI, é realizado anualmente desde 2018. O exercício se concentra na proteção do CI contra cenários de crise cibernética, e na coordenação de testes e de formação entre os setores público e privado nestes cenários. Os cenários são desenvolvidos por meio de discussões com as partes interessadas para chegar a acordo sobre os incidentes e condições mais importantes a serem testadas. Os sistemas de comunicações de emergência estão em funcionamento e sua eficácia e resiliência são testadas durante o exercício. Os participantes relataram que este é o maior exercício deste tipo na região, e que outros países da região são observadores frequentes do exercício brasileiro.

O primeiro exercício Cyber Guardian em 2018 reuniu os setores energético, nuclear e de defesa; isto agora se expandiu para envolver uma ampla gama de partes interessadas (com relatos de envolvimento de muitas das partes interessadas presentes em nossa revisão do CMM) das forças de defesa, CI (um objetivo do PlanSIC é garantir que todos os setores da CI estejam envolvidos nestes exercícios), governo, setor privado e serviços de inteligência. Os participantes relataram que na edição do exercício que ocorrerá em outubro de 2023, a intenção é envolver as agências reguladoras, CSIRTs e organizações representativas de todos os 14 setores de IC identificados no PlanSIC (ver D1.3).

Os incidentes cibernéticos podem ser transversais e evoluir muito rapidamente e, como tal, o nível de coordenação necessário pode exigir um grau de coordenação mais elevado do que noutros tipos de crises. Embora a abordagem descentralizada e regularmente exercitada seja considerada forte, é fundamental continuar testando regularmente as capacidades de coordenação das várias entidades relevantes diante uma vasta gama de possíveis cenários de segurança cibernética. Os resultados destes exercícios devem ser avaliados para estabelecer lições aprendidas atualizadas periodicamente. Ao estabelecer as lições aprendidas, deve considerar-se se seria conveniente designar um órgão responsável pela coordenação do gerenciamento de crises cibernéticas (e apoiar processos mais amplos de gestão de crises em que haja um elemento de segurança cibernética) e/ou integrar formalmente a segurança cibernética em um marco mais amplo de gerenciamento de crises.

D1.3 PROTEÇÃO DE INFRAESTRUTURA CRÍTICA (CI)

Este Fator *estuda a capacidade do Governo para identificar ativos de CI, os requisitos regulatórios específicos para a segurança cibernética de CI e a implementação de boas práticas de segurança cibernética pelos operadores de CI.*

***Estágio*: Formativo para Estabelecido**

O Plano Nacional de Segurança de Infraestruturas Críticas (PlanSIC) foi aprovado pelo Decreto 11.200 em setembro de 2022.[42]Descreve detalhes de implementação e responsabilidades para atingir os objetivos da Política Nacional de Segurança de Infraestrutura Crítica (Decreto 9.573 aprovado em novembro de 2018) e da Estratégia Nacional de Segurança de Infraestrutura Crítica (Decreto 10.569 de dezembro de 2020), que detalha os objetivos estratégicos alinhados com o Político. O GSI é considerado o órgão coordenador das atividades de segurança de CI.

Através do PlanSIC, estão sendo feitos progressos na identificação da CI, na coordenação e atribuição de responsabilidades pela sua proteção e no desenvolvimento de padrões de segurança cibernética recomendados para todos os setores da CI. Muitos elementos do PlanSIC ainda não estão totalmente implementados e, como tal, a segurança cibernética ainda não está regulamentada em todos os setores de CI. Foram criados grupos técnicos compostos pelos ministérios e organizações relevantes para cada um dos setores da IC para trabalhar em prol destes objetivos. Começamos esta seção descrevendo o progresso alcançado através do PlanSIC, antes de descrever o estado atual da regulamentação de IC no Brasil.

O PlanSIC identifica sete áreas prioritárias, dentro das quais são identificados 14 setores de CI: Águas (setores de CI: Represas, Abastecimento Urbano de Água. Responsável: Ministério do Desenvolvimento Regional); Energia (Eletricidade; Peganbio – Petróleo, Gás Natural e Biocombustíveis. Responsável: Ministério de Minas e Energia); Transportes (Terrestre, Aéreo, Aquaviário. Responsável: Ministério da Infraestrutura); Comunicações (Telecomunicações, Radiodifusão, Correios. Responsável: Ministério das Comunicações); Finanças (Responsável: Ministério da Economia); Biossegurança e Bioproteção (Responsável: Ministério da Saúde),

[42] https://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2022/Decreto/D11200.htm

Defesa (Responsável: Ministério da Defesa). Segundo informações, há planos para que o setor do Governo Digital também seja incluído como área prioritária. Pretende-se que, no âmbito do PlanSIC, todos estes setores de IC identificados eventualmente sejam regulamentados quanto à segurança cibernética.

Em termos de padrões de segurança cibernética para o CI, várias responsabilidades são descritas no PlanSIC. O GSI é responsável por preparar orientações e regulamentações para incentivar a adoção de padrões e boas práticas no IC. Em particular, a GSI relatou o trabalho no sentido de um projeto de lei para criar uma política nacional sobre requisitos de segurança cibernética. A política que existe atualmente aplica-se apenas a organizações do governo federal; pretende-se que a nova política expanda esta política para criar um marco abrangente de requisitos mínimos de segurança cibernética para todos os setores de IC. A GSI também é responsável por fornecer uma orientação consolidada sobre regulamentos identificados como relacionados à segurança de CI em seu site institucional.

Pretende-se que os reguladores do setor adaptem o guia e a regulamentação cross-CI preparadas pela GSI de acordo com as necessidades do seu setor. De acordo com o PlanSIC, os ministérios a cargo são responsáveis pela elaboração de guias complementares para as respectivas áreas prioritárias, bem como planos setoriais de Segurança de Infraestruturas Críticas, que serão encaminhados para um novo Comité Diretor de Segurança de Infraestruturas Críticas para aprovação. Estes planos setoriais pretendem ser documentos complementares ao PlanSIC, que abordam as ações de segurança de IC de acordo com as especificidades de cada setor, orientando sobre *"os níveis desejáveis de proteção, sobre as atividades de segurança a realizar e sobre a priorização na alocação de recursos"*.

Os participantes afirmaram que a estrutura regulatória ainda não foi decidida; Este está atualmente em fase de estudo incluído nos trabalhos dos grupos técnicos constituídos e será levado ao congresso para discussão. Algumas responsabilidades de supervisão pretendidas estão descritas no PlanSIC, que afirma que o GSI será responsável pela realização de visitas técnicas para monitorar as atividades de segurança de CI, que podem incluir o preenchimento de listas de verificação ou questionários para orientar ações de acompanhamento. A Estratégia Nacional de Segurança de Infraestruturas Críticas também inclui como objetivo estratégico estabelecer uma estrutura de governança para a segurança de CI. O PlanSIC afirma que este objetivo será alcançado através da criação do Comité Diretor de Segurança de Infraestruturas Críticas, que "*será composto por um conjunto de órgãos responsáveis por articular, orientar, propor e gerir a implementação de ações relacionadas com a Segurança das Infraestruturas Críticas, que procurará também garantir o cumprimento das metas estabelecidas neste Plano [PlanSIC]*". Prevê-se que este ano (2023) seja aprovado um novo decreto, que estabelece formalmente esta estrutura de gestão para segurança de CI.

Durante as sessões de revisão do CMM, houve algum debate entre os participantes sobre os benefícios relativos de atribuir a competência para regular a segurança cibernética em todos os setores de CI a um único organismo, como a planeada agência nacional de segurança cibernética ou GSI, ou desenvolver a estrutura regulamentar por setor. Neste último caso, os participantes expressaram a opinião de que a agência ou o GSI ainda poderia desempenhar um papel valioso na coordenação e no apoio aos reguladores individuais do setor de CI, por exemplo, recomendando padrões mínimos de segurança cibernética intersetoriais. Se a nova agência nacional de cibersegurança tiver uma função regulatória, será importante que o seu mandato seja claro, especialmente no que diz respeito à forma como quaisquer

responsabilidades regulatórias de segurança cibernética que assuma se alinhem com as atividades regulatórias dos reguladores do setor.

O PlanSIC afirma ainda o objetivo de estabelecer o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas (e outros protocolos de integração entre este sistema e CTIR.gov), uma estrutura operacional para a segurança de CI do país, incluindo mecanismos seguros de intercâmbio de informações para apoiar a cooperação entre o público e setor privado, ferramentas para análise de riscos e interdependências dos ICs e metodologias para identificação contínua dos ICs. Esta estrutura pode, portanto, eventualmente ser importante para garantir que a lista de Activos de IC seja mantida atualizada e possa ser adaptada conforme necessário, e que as interdependências entre setores, nas quais as infraestruturas digitais de um setor como o Financeiro podem depender da prestação de serviços de outro setor como Telecomunicações ou Energia, por exemplo, possam ser gerenciadas. Os participantes na revisão relataram um trabalho constante para a identificação e gestão de interdependências entre setores, dentro dos grupos técnicos criados sobre segurança de CI. Não ficou claro nas sessões de revisão ou nos planos documentados até que ponto as dependências transfronteiriças (em que ativos brasileiros de IC podem depender da infraestrutura de outras nações) estão sendo consideradas.

Na prática, atualmente o nível de regulamentação da segurança cibernética varia entre os diferentes setores de IC. Os requisitos de segurança cibernética são definidos por alguns reguladores do setor, cada um dos quais tem autonomia em termos de gestão do seu setor em relação a segurança cibernética, com diferentes níveis de requisitos e monitorização de conformidade como resultado. A PFA e os setores financeiro e de telecomunicações foram considerados pelos participantes como os setores mais avançados neste aspecto.

O DSIC do GSI propõe requisitos obrigatórios para a segurança cibernética do PFA. A segurança cibernética na PFA é fiscalizada pelo Tribunal de Contas da União (TCU), que realiza auditorias alinhadas à regulamentação. Todas as instituições federais são obrigadas a realizar avaliações de risco cibernético, atualizadas anualmente com base nas lições aprendidas em incidentes maiores. A Instrução Normativa GSI/PR 3 (maio de 2021) dispõe sobre processos relacionados à gestão de riscos de segurança da informação em órgãos e entidades da PFA. De acordo com o PlanGIC, todos os participantes da Rede Federal de Gerenciamento de Incidentes Cibernéticos (ReGIC, que, conforme descrito em D1.2, inclui obrigatoriamente todas as entidades da PFA) devem notificar os incidentes cibernéticos ao CTIR.gov. Exercícios regulares de referência também são realizados pela Secretaria de Auditoria de Tecnologia da Informação (Sefti/TCI) para medir o desenvolvimento da segurança cibernética na PFA.

Para o setor financeiro, as Resoluções nº 4.658 do Banco Central (BACEN)[43](2018), nº 4.893 e nº 85 (ambos promulgados em 2021) regulamentam a adoção de medidas de segurança cibernética. Os regulamentos exigem que as instituições financeiras adotem controles e procedimentos para prevenir e responder a incidentes de segurança cibernética e nomeiem um responsável pela supervisão das suas políticas de segurança cibernética. A conformidade das instituições financeiras com a regulamentação é auditada pelo BACEN. As instituições financeiras também são obrigadas a notificar o BACEN em caso de violação de dados (embora os prazos não sejam especificados) e a reportar anualmente ao BACEN divulgando quaisquer incidentes de segurança cibernética.[44]A Resolução nº 4.658 também estabelece requisitos

[43] https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf
[44] http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm

para contratação de serviços de processamento de dados, armazenamento de dados e computação em nuvem.

Para o setor de telecomunicações, que é regulamentado pela Anatel, a Resolução nº 740 de 2020 estabeleceu uma regulamentação de segurança cibernética que, relataram os participantes, foi uma evolução das regulamentações anteriores para o setor.[45]Cada empresa de telecomunicações no Brasil é obrigada a identificar seus ativos, realizar testes regulares de vulnerabilidade, adotar padrões e boas práticas em segurança cibernética e desenvolver um plano de gerenciamento de riscos cibernéticos, uma política de capacitação em segurança cibernética e processos claros de resposta a incidentes. A Resolução também estabelece que os incidentes de segurança cibernética devem ser notificados à Anatel e inclui disposições sobre auditoria da cadeia de fornecimento das principais prestadoras de serviços de telecomunicações. A Anatel mantém um grupo de trabalho com as principais operadoras de telecomunicações para se manter atualizado sobre a gestão de riscos de segurança cibernética, incluindo a análise de riscos relativos a desenvolvimentos tecnológicos mais recentes, como o 5G. A Anatel observou que, com aproximadamente 1.500 prestadoras de serviços de telecomunicações no país, não é possível realizar auditorias para todas as operadoras, e a auditoria é priorizada do ponto de vista da gestão de riscos.

Tanto no setor financeiro como no das telecomunicações, as diretrizes não contêm requisitos técnicos prescritivos, mas estabelecem que cada instituição deve estabelecer a sua própria política de segurança cibernética e manter um plano de resposta a incidentes. Alguns participantes do setor financeiro observaram que poderia ser útil ter uma base mais prescritiva que pudesse ser utilizada por diferentes setores e infraestruturas em termos de normas e controles técnicos e criptográficos.

Fora dos setores financeiro e de telecomunicações, os requisitos obrigatórios em matéria de cibersegurança ainda não foram implementados. Em alguns setores, foram estabelecidos requisitos, mas o cumprimento ainda não é monitorizado. Por exemplo, para o setor da Energia, a Resolução 964 de Dezembro de 2021 entrou em vigor em Julho de 2022 e estabelece requisitos para a adoção de normas e boas práticas, notificação de incidentes cibernéticos e intercâmbio de informações sobre ameaças.[46]A conformidade ainda não foi avaliada; a Resolução afirma que estará sujeita à avaliação regulatória após sete anos de vigência. Todos os setores têm requisitos obrigatórios para caso de violação de dados pessoais: de acordo com a Lei Geral de Proteção de Dados Pessoais que entrou em vigor em agosto de 2020 (ver D4.2), as violações de dados pessoais devem ser comunicadas por qualquer instituição brasileira à Autoridade Nacional de Proteção de Dados. (ANPD) e ao titular dos dados.

Em termos de compartilhamento de informações sobre ameaças e vulnerabilidades, as instituições da administração pública federal direta, autônoma e fundacional são obrigadas a participar da Rede Federal de Gestão de Incidentes Cibernéticos, ReGIC, por meio da qual são compartilhadas informações sobre ameaças, incidentes e vulnerabilidades, com algumas outras organizações, como empresas públicas federais e sociedades de economia mista, participando voluntariamente. Também existem mecanismos de intercâmbio de informações sobre ameaças em alguns setores fora do PFA. Por exemplo, para o setor de telecomunicações, existe um grupo de trabalho criado pela Anatel e administrado por meio

[45] https://www.in.gov.br/web/dou/-/resolucao-n-740-de-21-de-dezembro-de-2020-296152776
[46]https://www.in.gov.br/pt/web/dou/-/resolucao-normativa-aneel-n-964-de-14-de-dezembro-%20de-2021-369359262

de uma plataforma MISP na qual grandes e médias operadoras compartilham informações sobre ameaças e vulnerabilidades. Este grupo de trabalho foi criado por regulamento e promove a cooperação entre diferentes operadores. Para o setor financeiro, a Federação Brasileira de Bancos (Febraban) cria grupos de trabalho para compartilhamento de inteligência sobre ameaças cibernéticas (CTI) usando plataformas como o MISP, e informou também o intercâmbio de informações com outros setores. Da mesma forma, as empresas do setor do petróleo e do gás relataram ter participado em redes de intercâmbio de CTI através de plataformas MISP, partilhando com uma série de outras instituições do setor, bem como com organizações dos setores financeiro, educacional e retalhista. Os participantes do setor financeiro também relataram participar de redes internacionais de intercâmbio de CTI: o Centro de Análise e Intercâmbio de Informações de Serviços Financeiros (FS-ISAC). Conforme descrito, pretende-se que o Sistema Integrado de Dados de Segurança de Infraestrutura Crítica também apoie e formalize os canais para compartilhamento de CTI entre organizações de CI.

Nos setores regulamentados de CI, as operadoras implementam boas práticas de segurança cibernética. Fora destes setores, os participantes relataram que muitas organizações implementam boas práticas de segurança cibernética e autoavaliações em relação aos padrões reconhecidos da indústria, embora o nível varie entre as organizações. Conforme descrito em D1.2.3, os operadores de CI participam plenamente na resposta a incidentes nacionais e nos exercícios de gestão de crises; em particular, o exercício Cyber Guardian.

D1.4 CIBERSEGURANÇA NA DEFESA E SEGURANÇA NACIONAL

Este Fator explora se o governo tem capacidade para conceber e implementar uma estratégia de segurança cibernética no âmbito da segurança e defesa nacional. Analisa também o nível de capacidade de cibersegurança no âmbito do estabelecimento de segurança e defesa nacional, e os acordos de colaboração em matéria de cibersegurança entre entidades civis e de defesa.

Estágio: Estabelecido

Existem várias políticas e doutrinas para a segurança cibernética na defesa nacional. A Política de Defesa Cibernética foi lançada em 2012 e a primeira Doutrina de Defesa Cibernética foi aprovada em 2014. O ciberespaço também foi identificado na Estratégia de Defesa Nacional como uma das três prioridades estratégicas, ao lado da nuclear e do espaço, desde 2008. De acordo com a Estratégia de Defesa Nacional, as principais capacidades de defesa nacional são a proteção, a resposta imediata e a dissuasão, e esta é a base para definir as prioridades da defesa cibernética. Estes documentos estratégicos fundamentais são apoiados por doutrinas operacionais e manuais de campo.

No final de 2020, foram estabelecidos novos atos doutrinários e organizacionais para a defesa cibernética: em particular, o novo manual de operações conjuntas (Portaria Normativa nº 84/GM-MD, de 15 de setembro de 2020), que inclui capítulos sobre defesa cibernética: Capítulo VII – Comando de Defesa Cibernética e Capítulo XII – Guerra Cibernética em

Operações Conjuntas. Esses capítulos definem a prioridade do uso do ciberespaço como ferramenta operacional, além de seu alinhamento aos conceitos de Inteligência, Comando e Controle (C2) e Operações de Informação. Os participantes afirmaram ainda que a Política de Defesa Cibernética de 2014 está em fase de atualização. Os participantes relataram que decretos e instrumentos jurídicos importantes desde 2020, em particular a Portaria Normativa nº 3781/GM-MD, de 17 de novembro de 2020, levaram a uma implementação mais consistente da doutrina e a uma melhor capacidade de envolvimento internacional.

Capacidades de defesa cibernética e estruturas organizacionais estão em vigentes no Brasil. Existem unidades cibernéticas dentro de cada uma das três forças (Marinha, Exército e Força Aérea). O Exército criou seu Programa Estratégico de Defesa Cibernética em 2010, instituindo seu Centro de Defesa Cibernética (CDCiber). O Ministério da Defesa criou o Programa de Defesa Cibernética em 2014, que buscava melhorar a interoperabilidade da defesa cibernética entre as forças. Com base nas diretivas emitidas pelo Ministério da Defesa no âmbito deste programa, foram criados o Comando de Defesa Cibernética (ComDCiber, o comando operacional cibernético conjunto desde 2016) e a Escola Nacional de Defesa Cibernética. Os participantes observaram que a expansão das capacidades de defesa cibernética nessa época foi motivada, em parte, pelos grandes eventos esportivos organizados pelo Brasil (a Copa do Mundo de Futebol de 2014 e as Olimpíadas de 2016).

O papel do ComDCiber como comando conjunto na defesa cibernética foi reforçado pelos desenvolvimentos nos últimos anos; em particular, a definição da organização da ComDCiber no manual de operações conjuntas de 2020 e as disposições feitas na Portaria Normativa nº 3.781/GM-MD, de 17 de novembro de 2020, que afirma o ComDCiber como comando conjunto, de atuação permanente, e órgão central do SMDC. O orçamento fornecido à ComDCiber através do Ministério da Defesa também melhorou.

O Sistema Militar de Defesa Cibernética (SMDC) foi criado pelo Ministério da Defesa para estabelecer a estrutura institucional abrangente para coordenar os esforços de defesa cibernética do Brasil. É composto pela ComDCiber, Escola Nacional de Defesa Cibernética e CDCiber. O SMDC organiza a capacitação das forças de defesa cibernética e desenvolve e atualiza as doutrinas e políticas de defesa cibernética.

A Escola Nacional de Defesa Cibernética, por meio da SMDS, oferece capacitação ao comando conjunto e aos oficiais das unidades cibernéticas das três forças, por meio da contratação de instrutores e programas especializados do Brasil e do exterior. Há também formação fornecida separadamente às unidades cibernéticas das três forças: a Força Aérea, por exemplo, realizou e catalogou uma avaliação das necessidades de formação e informou ter fornecido formação adicional aos seus oficiais nesta base. A Agência Brasileira de Inteligência (ABIN) também relatou a aplicação de recursos especializados de inteligência para dar suporte à capacitação cibernética e às operações das forças de defesa. Os participantes descreveram a capacitação cibernético ministrado por instituições de ensino brasileiras, principalmente da escola de formação do Exército, para oficiais militares estrangeiros, sendo que aproximadamente 75 oficiais estrangeiros foram treinados no Brasil até o ano passado.

Atualmente, não existem elementos de cibersegurança incluídos na formação das forças militares mais amplas, fora destas unidades cibernéticas, mas isto está planejado para o futuro, a fim de aumentar a conscientização sobre segurança cibernética das forças de defesa. A capacitação das forças mais amplas será cada vez mais importante à medida que a segurança cibernética se torna cada vez mais relevante para uma ampla gama de diferentes cenários militares.

Os exercícios foram destacados como uma parte crítica da capacitação em defesa cibernética. O exercício AZUVER é um exercício anual de formação conjunta dos três serviços e envolve cenários cibernéticos. Os participantes relataram que são realizados exercícios conjuntos de Capture-the-Flag (CTF) para as unidades cibernéticas das três forças. O exercício Cyber Guardian, organizado pela ComDCiber em parceria com o GSI, é outro exercício crítico de capacitação para as forças de defesa junto com vários outros atores brasileiros da CI, governo, setor privado e ABIN, que é descrito em mais detalhes em D1.2, no contexto da gestão de crises. Os participantes descreveram este como o exercício de formação mais importante para as forças de defesa cibernética no que diz respeito ao envolvimento e assistência na proteção da CI.

Os mecanismos para facilitar a colaboração com aliados na defesa cibernética são capacitados e testados através de exercícios internacionais. Desde 2018, o Brasil participa do exercício anual de defesa cibernética Locked Shields, organizado pelo Centro Cooperativo de Excelência em Defesa Cibernética (CCDCOE) da Organização do Tratado do Atlântico Norte (OTAN), em Tallinn. A ComDCiber também participa de reuniões internacionais, incluindo as reuniões anuais do Fórum Iberoamericano de Ciberdefesa, do qual o Brasil atualmente mantém a secretaria, e outras reuniões entre Comandantes de Defesa Cibernética que são organizadas em diferentes países. Conforme descrito em D1.1, os representantes brasileiros, incluindo o comando operacional cibernético conjunto das forças de defesa, ComDCiber, estão ativamente engajados no debate global sobre o direito internacional humanitário e as normas de comportamento por meio do OEWG da ONU e do GGE. No futuro, para atingir os estágios mais elevados de maturidade do CMM, é importante que consideremos como a estratégia brasileira de defesa cibernética pode ser projetada para contribuir para promover a estabilidade no ciberespaço, incluindo medidas para prever e influenciar as estratégias, ações e reações de potenciais aliados e adversários.

Os recursos para a defesa cibernética são organizados anualmente entre as diversas forças e instituições e o Ministério da Defesa. Os participantes descreveram os desafios decorrentes da falta de ainda um orçamento plurianual para a defesa cibernética. Também foram descritos desafios decorrentes do orçamento mais limitado atribuído à defesa cibernética em comparação com outros programas (foi feita uma comparação com os programas estratégicos para o Exército e a Força Aérea, que supostamente têm orçamentos muito maiores e mais estáveis), levando a recursos limitados disponíveis para a compra de programas e equipamentos de capacitação.

Os participantes relataram o objetivo de desenvolver um planejamento baseado em capacidades para alocar recursos dedicados à defesa cibernética. Será importante estabelecer estes processos, permitindo a revisão dos recursos atuais diante de uma série de cenários plausíveis (que podem ser apoiados pela avaliação nacional mais ampla dos riscos de segurança cibernética e pela consideração de outras exigências que possam ser colocadas às forças cibernéticas), a fim de para garantir que os orçamentos adequados estejam em vigor. Para aumentar a disponibilidade de pessoal qualificado, pode ser conveniente considerar a criação de uma força de reserva cibernética ou outro mecanismo que permita à comunidade de defesa aproveitar as competências e capacidades de segurança cibernética da sociedade em geral.

Foi relatado que desde o CMM 2020, a coordenação entre as entidades civis e de defesa foi melhorada, através de uma maior integração entre a IC e as entidades de defesa. A responsabilidade do MoD em relação à proteção da IC foi formalizada através do Plano de Segurança da CI (PlanSIC), que, embora ainda não totalmente implementado, afirma que a implementação do PlanSIC e os planos de segurança setoriais em desenvolvimento (descritos

em D1.3) terão o apoio do Ministério da Defesa. O PlanSIC também atribui ao MoD a responsabilidade de envolver os setores de CI nos exercícios Cyber Guardian, que o MoD realiza através do ComDCiber.

Dado que os planos setoriais de segurança de IC estão atualmente em desenvolvimento, as responsabilidades específicas das entidades de defesa no que diz respeito à assistência na proteção dos vários setores de IC ainda não foram formalizadas. Da mesma forma, os respetivos papéis das entidades de defesa na gestão de crises cibernéticas ainda não estão formalizados. Como tal (devido à falta de planejamento de recursos baseado na capacidade para o programa de defesa cibernética atualmente, conforme descrito acima), os recursos exigidos pelas entidades de defesa cibernética para apoiar as autoridades civis e de CI ainda não foram formalmente atribuídos.

Apesar de as responsabilidades específicas e o orçamento ainda não terem sido formalizados, foram dados vários exemplos de coordenação entre entidades civis e de defesa; por exemplo, entidades de defesa que ajudaram os setores da CI e o governo no caso de incidentes cibernéticos significativos. O serviço de inteligência, ABIN, troca informações sobre ameaças, inclusive relacionadas à ciberespionagem e ameaças persistentes avançadas (APTs) com contrapartes internacionais, e apoia as forças de defesa, bem como CTIR.gov, a CI e outras organizações com informações relevantes. Isto supostamente inclui parcerias bidirecionais de intercâmbio de informações com empresas públicas e privadas, bem como a participação em vários grupos de intercâmbio de CTI, inclusive para os setores governamental, financeiro e acadêmico. Os participantes descreveram os benefícios do exercício anual Cyber Guardian para capacitar e testar as diversas funções da CI e das partes interessadas na defesa no caso de uma crise cibernética.

Estão em curso iniciativas para melhorar a compreensão da dependência das entidades de segurança nacional e militares da segurança cibernética de outras partes do CI. Conforme descrito em D1.3, vários grupos técnicos estão atualmente estudando a segurança para os setores de CI identificados no PlanSIC; a defesa é um setor de CI identificado sob a responsabilidade do Ministério da Defesa. Os grupos técnicos que estão atualmente envolvidos no estudo da interdependência entre os setores da CI, incluindo a dependência dos militares de outros setores, incluem representantes do Ministério da Defesa e de três forças armadas. Foi relatado que esses estudos produzirão resultados nos próximos anos. Os estudos deverão eventualmente informar a Política ou Doutrina de Defesa Cibernética, bem como o desenvolvimento de mecanismos formais para identificar e gerenciar regularmente essas interdependências.

RECOMENDAÇÕES

Seguindo as informações apres*entadas durante a revisão da maturidade da* Política e Estratégia de Segurança Cibernética, o Centro Global de Capacidade de Segurança Cibernética desenvolveu o seguinte conjunto de recomendações para consideração do Governo do Brasil. Estas recomendações fornecem conselhos e medidas destinadas a aumentar a capacidade de segurança cibernética existente, em linha com as considerações do Modelo de Maturidade da Capacidade de Segurança Cibernética do GCSCC. As recomendações são fornecidas especificamente para cada *Fator*.

Dado que os processos de renovação do NCS irão iniciar-se em breve, são feitas as seguintes recomendações para a renovação do NCS:

R1.1.1 Desenvolver e publicar uma NCS revista através de um processo que envolve consultas com os principais grupos de partes interessadas, incluindo representantes do governo, do setor privado, da sociedade civil e de parceiros internacionais. O desenvolvimento da nova NCS deve também ser orientado por uma avaliação dos progressos realizados em relação à atual NCS e por uma avaliação atualizada do risco de cibersegurança nacional (que atualiza o "diagnóstico" de risco incluído na atual NCS). O desenvolvimento da NCS também pode ser orientado pelas recomendações desta revisão do CMM.

R1.1.2 Atualizar a avaliação do risco de segurança cibernética nacional, consulte as partes interessadas relevantes de grupos, incluindo a CI, a comunidade de segurança nacional e o setor privado, e garanta que o processo leva em conta os riscos de segurança cibernética decorrentes do uso de tecnologias emergentes em infraestruturas críticas e na sociedade em geral. O processo também pode basear-se em conhecimentos sobre incidentes cibernéticos e ameaças compartilhados em redes de intercâmbio de informações. Considere implementar um processo para atualizar regularmente a avaliação de riscos à luz de uma ameaça e de um cenário tecnológico em mudança.

R1.1.3 Ao elaborar a NCS e como parte dos processos de consulta, considere a forma como a NCS pode incorporar ou apoiar objetivos políticos on-line mais amplos, tais como: proteção da criança; a promoção dos direitos humanos; a promoção da igualdade, diversidade e inclusão; e gestão da desinformação. Certifique-se de que isso esteja claramente indicado na NCS.

R1.1.4 Desenvolver e publicar um Plano de Ação detalhado da NCS para a nova NCS, descrevendo um programa de implementação que cubra o âmbito da estratégia. Este plano deve atribuir ações dentro do programa a "proprietários" específicos (intervenientes relevantes do governo e de outros setores). Garantir que existe um processo para alocar o orçamento para a execução dos vários componentes da estratégia e para identificar, escalar e mitigar o impacto de quaisquer défices orçamentais.

R1.1.5 Designar um órgão de coordenação para o programa de implementação da estratégia nacional e garantir que este órgão tenha autoridade suficiente para garantir que os "donos" da ação sejam responsabilizados. Observando o potencial da nova agência nacional de segurança cibernética para assumir este papel de coordenação, é importante que o papel da agência seja claramente definido: até que ponto tem uma função de supervisão estratégica, uma função de execução operacional, ou ambos. É também importante definir claramente como as suas responsabilidades interagem com outras funções de segurança e regulação do governo.

R1.1.6 Definir dentro da NCS os principais resultados contra os quais o sucesso pode ser medido, implementar processos e mecanismos de revisão para permitir que os

"proprietários" da estratégia monitorizem a consecução destes resultados da NCS, abordem questões de implementação e escalem riscos, problemas e dependências para as autoridades relevantes. Os esforços de validação da NCS que estão atualmente a decorrer poderão fornecer suporte para a definição de métricas de progresso e processos de revisão. Garantir que estes processos sejam adequadamente financiados.

R1.1.7 Definir métricas orientadas para resultados que podem ser usadas para monitorar o impacto que o programa está tendo na redução de riscos e danos. Utilizar estas métricas para aperfeiçoar continuamente o Plano de Ação e para informar decisões de financiamento e prioridades.

R1.1.8 Garantir que os processos de revisão e renovação para a próxima NCS estejam formalmente implementados. Estes processos devem descrever como identificar as lições aprendidas com a implementação atual da estratégia.

R1.1.9 Garantir que o conteúdo da NCS tenha em conta os riscos de cibersegurança decorrentes da utilização de tecnologias emergentes em infraestruturas críticas e da economia e da sociedade em geral. Estabelecer processos para avaliar regularmente os riscos emergentes de cibersegurança e utilizar os resultados para atualizar a NCS e o Plano de Ação.

R1.1.10 Consultar regularmente todas as partes interessadas relevantes para refinar e atualizar os objetivos de envolvimento internacional: por exemplo, o Brasil pode pretender eventualmente expandir os seus objetivos em torno da construção de comunidades internacionais de interesse em torno de objetivos específicos da política de segurança cibernética e de uma participação mais ativa na construção de capacidade de segurança cibernética em outros países. Garantir que exista uma validação regular de que os objetivos nesta área sejam claros e compreendidos por todos os participantes envolvidos, e que haja um processo implementado para monitorizar a concretização dos objetivos.

RESPOSTA A INCIDENTES E GERENCIAMENTO DE CRISES

R1.2.1 Testar a capacidade do sistema distribuído de CERTs funcionar no caso de um grande incidente ou crise cibernética entre setores. Exercícios teóricos e práticos podem ajudar a esclarecer estes processos. É importante que esta capacidade seja testada diante da variedade de potenciais cenários de cibersegurança que o país pode enfrentar e que os exercícios tenham em conta as mudanças no cenário tecnológico e de ameaças. Com base na avaliação contínua das lições aprendidas com estes testes, pode ser valioso:

- Considerar como as funções do CTIR.gov e do CERT.br poderiam evoluir para proporcionar uma melhor colaboração entre os setores, incluindo se haveria

benefício na formalização da missão intersetorial do CERT.br (ou seja, os tipos de organizações que são responsáveis por apoiar);
- Considerar a formalização das condições, limites e processos para o intercâmbio de informações e escalonamento entre CERTs, incluindo a definição dos pontos de contato e responsabilidades, a fim de garantir que todas as funcionalidades necessárias sejam institucionalizadas e possam continuar funcionando no caso de uma mudança de pessoal, por exemplo.

R1.2.2 Verificar se os atuais registos distribuídos de incidentes cibernéticos estão suficientemente coordenados para permitir a identificação, categorização e resposta a um incidente cibernético a nível nacional sob toda a gama de cenários e condições possíveis. Esta avaliação poderá ser incluída nos testes descritos em D1.2.1. Além disso, é importante garantir que a visibilidade dos incidentes de segurança cibernética no Brasil seja suficientemente coordenada para permitir a análise de tendências de ameaças, riscos, danos e perdas que possam informar a estratégia nacional e a alocação de recursos para atividades de segurança cibernética.

R1.2.3 Com base nas conclusões da avaliação descrita em D1.2.3, pode ser valioso considerar se o CTIR.gov ou o CERT.br deveriam ser responsáveis pela manutenção de um registro central de incidentes cibernéticos.

R1.2.4 Considerar que papel facilitador a agência nacional de segurança cibernética planejada poderia desempenhar em relação às Recomendações R1.2.1 a R1.2.3.

R1.2.5 Continuar exercendo regularmente as capacidades das diversas entidades relevantes para se coordenarem diante de uma vasta gama de potenciais cenários de crise de cibersegurança e para coordenarem com outros setores no caso de uma crise mais ampla com componentes de cibersegurança. Os resultados destes exercícios devem ser avaliados para estabelecer lições aprendidas periodicamente atualizadas. Ao estabelecer as lições aprendidas, deve-se considerar se seria benéfico designar um órgão responsável pela coordenação da gestão de crises cibernéticas (e por apoiar processos mais amplos de gestão de crises em que exista um elemento de segurança cibernética) e/ou integrar formalmente a segurança cibernética em um marco mais amplo de gestão de crises.

PROTEÇÃO DE INFRAESTRUTURA CRÍTICA (CI)

R1.3.1 Finalizar e emitir requisitos regulatórios de segurança cibernética para todos os setores de CI identificados no PlanSIC. Estes requisitos devem incluir normas adequadas de segurança cibernética que devem ser cumpridas e requisitos obrigatórios de comunicação de violações e divulgação de vulnerabilidades.

R1.3.2 Implementar processos formais para avaliar a conformidade do operador de CI com os padrões regulatórios e a divulgação de incidentes e vulnerabilidades. Conforme observado, estão em andamento discussões sobre a estrutura regulatória que será adotada. Será importante considerar o seguinte ao estabelecer a estrutura regulatória:

- Garantir que sejam realizados processos de consulta suficientes para satisfazer as necessidades dos reguladores e das organizações dentro dos setores de IC, particularmente no que diz respeito aos benefícios potenciais de uma regulamentação entre IC monitorizada por um único organismo versus regulamentação baseada no setor.
- Se algum organismo assumir um papel regulador intersetorial, como foi sugerido, pode ser o caso, assegurando que seu mandato seja claro, particularmente no que diz respeito às suas responsabilidades, assume o alinhamento com as atividades regulatórias existentes dos reguladores do setor.

R1.3.3 Continuar o trabalho na identificação de interdependências entre os setores de IC, para compreender os potenciais riscos sistémicos e da cadeia de abastecimento e melhorar a capacidade de identificar rapidamente a agregação de riscos. Documentar formalmente essas dependências e a abordagem para gerenciá-las.

R1.3.4 Identificar dependências transfronteiriças, nas quais os ativos brasileiros de IC podem depender da infraestrutura de outras nações. Documentar formalmente essas dependências e a abordagem para gerenciá-las.

R1.3.5 Considerar como aumentar o intercâmbio de informações sobre ameaças e vulnerabilidades entre todos os setores de IC, a fim de garantir que todas as organizações de IC necessárias recebam informações relevantes. Isto pode envolver consultas para compreender os pontos fortes e os desafios atuais. As abordagens podem incluir a criação de estruturas formais adicionais para o intercâmbio automático de informações entre todos os setores de IC (por exemplo, usando plataformas MISP); abordagens para construir relacionamentos e confiança para apoiar o intercâmbio de informações; e requisitos regulatórios.

R1.3.6 Implementar processos de revisão regulares para garantir que a lista de ativos de IC identificados no PlanSIC possa adaptar-se às mudanças no ambiente técnico e socioeconómico.

SEGURANÇA CIBERNÉTICA NA DEFESA E SEGURANÇA NACIONAL

R1.4.1 Implementar processos regulares de consulta e revisão para garantir que a estratégia e a doutrina de defesa cibernética sejam adaptáveis às capacidades em mudança e ao ambiente geopolítico e de ameaças em evolução.

R1.4.2 Considerar como a estratégia brasileira de defesa cibernética pode ser projetada para contribuir para promover a estabilidade no ciberespaço, incluindo medidas para prever e influenciar as estratégias, ações e reações de potenciais aliados e adversários.

R1.4.3 Desenvolver elementos de cibersegurança no âmbito da formação operacional e de comando mais ampla das forças militares, a fim de aumentar a sensibilização para a cibersegurança em todas as forças de defesa.

R1.4.4 Estabelecer processos de planejamento baseados em capacidades para apoiar a alocação de recursos para a defesa cibernética. Estes podem incluir uma revisão

dos recursos atuais em relação a uma série de cenários plausíveis (que podem ser apoiados por uma avaliação nacional mais ampla dos riscos de segurança cibernética e pela consideração de outras exigências que possam ser impostas às forças cibernéticas), a fim de garantir a existência dos orçamentos adequados.

R1.4.5 Considerar a criação de mecanismos que permitam à comunidade de defesa e de segurança nacional aproveitar as competências e capacidades de segurança cibernética da economia e da sociedade em geral (por exemplo, através de uma força de reserva cibernética formal).

R1.4.6 Formalizar as funções e responsabilidades específicas das entidades de defesa cibernética no que diz respeito à assistência na proteção dos vários setores de IC e no âmbito dos procedimentos de gestão de crises do país. Garantir que o orçamento alocado em R1.4.5 inclua os recursos necessários para apoiar as autoridades civis e de CI.

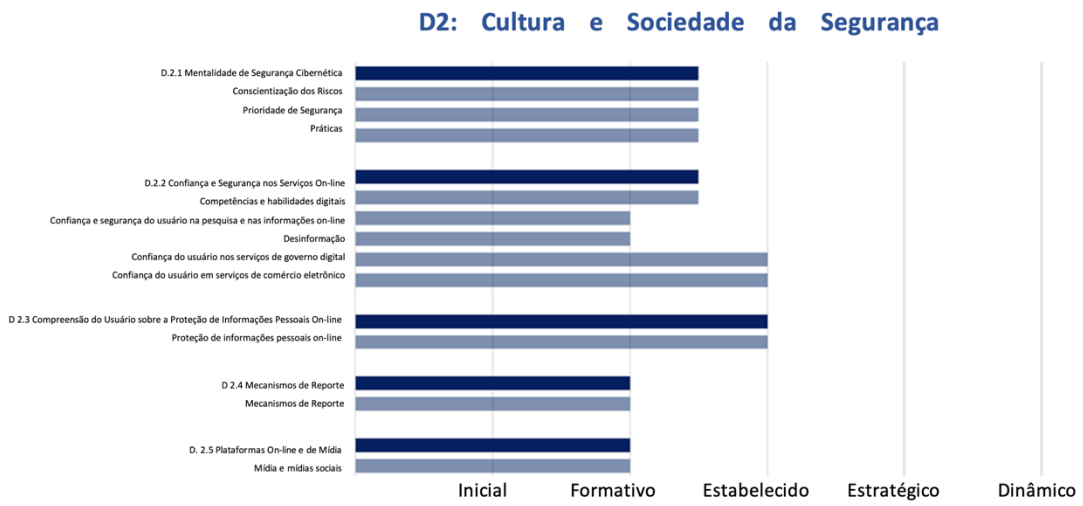
R1.4.7 Concluir a identificação em curso da dependência das entidades militares e de segurança nacional da segurança cibernética de outras partes da IC. Desenvolver mecanismos formais para rever regularmente a identificação e gestão destas dependências. Usar os resultados para informar a política e a doutrina de defesa cibernética.

DIMENSÃO 2
CULTURA E SOCIEDADE DE SEGURANÇA CIBERNÉTICA

Esta dimensão analisa elementos importantes de uma cultura de segurança cibernética responsável, como a compreensão de seus riscos relacionados na sociedade, o nível de confiança nos serviços de Internet, nos serviços de governo eletrônico e de comércio eletrônico, e a compreensão dos usuários sobre a proteção de informações pessoais on-line. Além disso, esta *Dimensão* explora a existência de mecanismos de denúncia que funcionam como canais para os usuários denunciarem crimes cibernéticos. Além disso, esta *Dimensão* analisa o papel dos meios de comunicação social e das redes sociais na formação de valores, atitudes e comportamentos de segurança cibernética.

Figura 7: Fatores e aspectos examinados na Dimensão 2.

RESUMO DOS RESULTADOS



D2.1 MENTALIDADE DE SEGURANÇA CIBERNÉTICA

Este Fator avalia até que ponto a segurança cibernética é priorizada e incorporada nos valores, atitudes e práticas do governo, do setor privado e dos usuários de toda a sociedade em geral. Uma mentalidade de cibersegurança consiste em valores, atitudes e práticas – incluindo hábitos de usuários individuais, especialistas e outros atores – no ecossistema de segurança cibernética que aumentam a capacidade dos usuários de se protegerem on-line.

***Estágio*: Formativo para Estabelecido**

As discussões entre as partes interessadas indicaram a presença de iniciativas que abordam a conscientização para os riscos de segurança cibernética em todas as agências governamentais. Além disso, diversas discussões com as partes interessadas também indicaram que algumas agências tentam antecipar proativamente novos riscos de segurança cibernética. Uma materialização disto pode ser vista, por exemplo, nos planos para estabelecer uma agência governamental central para a segurança cibernética, a fim de coordenar melhor as atividades de segurança cibernética das agências governamentais, incluindo a antecipação de riscos.

Embora as disposições legais e os procedimentos governamentais apoiem esta visão, também podem ser encontradas percepções mais críticas sobre a conscientização para os riscos de segurança cibernética nas agências governamentais. Por exemplo, um relatório divulgado pelo Tribunal de Contas da União lista deficiências em muitos órgãos públicos no que diz

respeito aos mecanismos básicos de segurança cibernética.[47]O relatório "aponta para ações de segurança cibernética que precisam ser implementadas com urgência pelos órgãos federais. Estas incluem a necessidade de os gestores públicos fazerem inventário e controlarem o equipamento e software de TI corporativo; o fornecimento de vulnerabilidade contínua e gerenciamento de resposta a incidentes; e o estabelecimento de programas de conscientização e capacitação em segurança."[48]A criticada falta de atividade por parte dos gestores empresariais no setor público aponta para uma incompatibilidade de consciência entre o aumento de iniciativas dentro das agências governamentais e o atual nível de consciência no que diz respeito aos riscos de segurança cibernética. Além disso, indica que embora, em geral, o governo pretenda tornar a segurança cibernética uma prioridade no setor público, a situação atual em algumas agências governamentais varia fortemente, incluindo lacunas significativas dentro de algumas agências.

Da mesma forma, as práticas seguras de cibersegurança não parecem ser implementadas de forma adequada, embora existam diretrizes e procedimentos. Por conseguinte, seria útil implementar um marco de monitorização em todas as entidades do setor público, que poderia, por exemplo, ser coordenado por uma agência central de segurança cibernética.

Pelas razões expostas, o setor público seria atualmente avaliado como estando no nível Estabelecido, com alguns valores atípicos em direção ao Formativo, por um lado, mas também fortes indicadores de que algumas agências atingiram o nível Estratégico. No que diz respeito ao nível dos Estados Federais em matéria de segurança cibernética, não foi possível apresentar um marco consistente. Alguns estados estão mais avançados do que outros e, portanto, a conscientização sobre segurança cibernética, a prioridade da segurança e as práticas não devem ser consideradas apenas em nível federal, mas também é necessário um nível mais alto de atividades sistemáticas e coordenadas em nível estadual e até mesmo comunitário - em especial. As iniciativas a nível estadual e municipal também devem ser registadas e monitorizadas por uma entidade a nível federal, como uma agência de segurança cibernética designada.

No que diz respeito ao setor privado, o nível de sensibilização varia dependendo da dimensão das empresas, como é frequentemente o caso na maioria dos países. As partes interessadas indicaram que as principais empresas públicas e privadas têm um nível muito elevado de sensibilização para a cibersegurança, fazem da cibersegurança uma prioridade e também implementam práticas seguras de cibersegurança. Em particular, as empresas privadas de propriedade pública têm um nível muito elevado de conformidade no que diz respeito às práticas de segurança cibernética e indicaram implementar a segurança cibernética com prioridade e trabalhar num nível geral de conscientização em todas as suas empresas.

No entanto, as pequenas e médias empresas carecem de recursos e conhecimentos relativamente às práticas de segurança cibernética e, por razões financeiras, a segurança cibernética raramente é uma prioridade. Além disso, não foram mencionadas campanhas específicas de conscientização dirigidas às pequenas e médias empresas. Com relação às

[47] "5 Controles de Segurança Cibernética", Tribunal de Contas de União, 16 de agosto de 2022, https://portal.tcu.gov.br/5-controles-de-seguranca-cibernetica.htm.

[48] Ana Ferraz: "Accounts Court warns of serious cybersecurity risks in the public sector", The Brazilian Report, 24 de agosto de 2022, https://brazilian.report/liveblog/2022/08/24/serious-cybersecurity-risks-public-sector/.

empresas maiores, o nível do Brasil para esse fator pode ser Estabelecido como Estratégico. No entanto, no que diz respeito às empresas menores, o nível não pode ser avaliado como superior ao Formativo. Não está claro se a responsabilidade pelas pequenas e médias empresas deve recair sobre o nível federal ou estadual – em qualquer caso, o monitoramento sistemático, incluindo pesquisas e métricas, deve ser coletado e compilado através de uma entidade designada no nível federal.

O nível variável de conscientização e prática de segurança cibernética, dependendo do estado federal, também foi destacado por profissionais de segurança cibernética citados em um artigo no Intelligent CIO:[49] *"A causa da irregularidade nos investimentos em cibersegurança nos diferentes territórios nacionais é consenso entre especialistas"*, destacando uma "falta de comunicação entre os setores público e privado". O artigo afirma ainda que há uma falta de consciência coletiva no que diz respeito à conscientização para a segurança cibernética e medidas adequadas entre as forças militares, inteligência, agências governamentais e empresas.

Outros países encontraram uma atitude reservada por parte de empresas privadas em colaborar diretamente com os setores militar ou de inteligência, o que também pode ser o caso do Brasil. Portanto, pode ser útil tentar estabelecer uma abordagem coletiva para a conscientização e boas práticas em matéria de segurança cibernética através de uma entidade (semi)governamental separada destas instituições, dentro da qual tal colaboração possa ocorrer. Além disso, as partes interessadas levantaram a questão de reunir a todas as entidades de diferentes setores, apesar da legislação apoiar tal abordagem. Isso pode ser resolvido por meio da abordagem descrita anteriormente. Além disso, devido à estrutura federal do Brasil, pode ser conveniente considerar a criação de órgãos semelhantes com responsabilidades específicas em nível estadual, que colaborem com uma entidade de nível federal.

No que diz respeito à sensibilização dos utilizadores da Internet, ao seu conhecimento relativamente a práticas seguras e à sua priorização da cibersegurança, as partes interessadas não apontaram quaisquer inquéritos sistemáticos, métricas ou outros indicadores/fontes de informação que pudessem fornecer uma imagem parcial ou completa. Portanto, é essencial que o Brasil conduza pesquisas sistemáticas e colete métricas sobre isso – embora a responsabilidade por esse problema possa recair sobre uma entidade dedicada à segurança cibernética no nível federal, tais pesquisas poderiam ser terceirizada para universidades e os estados federais também poderiam realizar pesquisas em nível estadual para obter uma imagem mais clara da situação em seu respectivo estado. Tal configuração também permitiria aos estados acrescentar aspectos às pesquisas e métricas relevantes para o seu ambiente específico.

Pela ausência de métricas ou estudos, o nível de maturidade em relação aos usuários não pode ser avaliado como superior ao Formativo. Segundo os participantes nas reuniões de partes interessadas, muitas pessoas não atribuem importância suficiente ao problema da segurança cibernética. Devido a várias iniciativas destinadas também aos usuários finais enumerados na Dimensão 3, pode avaliar-se que uma proporção limitada, mas crescente, de

[49] Natalio Moraes, "Brazil advances in world cybersecurity ranking", Intelligent CIO, 1º de setembro de 2022, https://www.intelligentcio.com/latam/2022/09/01/brazil-advances-in-world-cybersecurity-ranking/.

usuários da Internet tem um nível mínimo de conscientização no que diz respeito aos riscos de segurança cibernérica e também segue práticas seguras. Os inquéritos podem estar disponíveis de forma ad hoc, por exemplo, no que diz respeito a casos de crimes cibernéticos na população em geral (ver Dimensão 4), mas carecem da profundidade e amplitude previstas no Fator D 2.1 Mentalidade de Segurança Cibernética. Portanto, o nível de maturidade dos usuários da Internet para este Fator não pode ser avaliado superior ao Formativo.

D2.2 CONFIANÇA E SEGURANÇA NOS SERVIÇOS ON-LINE

Este Factor analisa as competências críticas, a gestão da desinformação, o nível de confiança dos usuários na utilização de serviços on-line em geral, e de serviços de governo eletrônico e de comércio eletrônico em particular.

***Estágio*: Formativo para Estabelecido**

Conforme descrito no Fator anterior, não estão disponíveis pesquisas ou métricas em grande escala que forneçam informações sobre a conscientização e o comportamento on-line dos usuários, e como eles podem variar entre os diferentes segmentos do público. Por isso, também, o nível de confiança dos usuários da Internet não pode ser avaliado com certeza e as respectivas pesquisas devem ser realizadas, incluindo métricas relevantes.

Devido a diversas iniciativas, pode-se presumir que o nível de confiança dos usuários nos serviços on-line se encontra numa fase formativa. Estas iniciativas dirigem-se muitas vezes aos mais jovens, por exemplo, estudantes universitários ou escolares e adolescentes em geral, mas também a pais. No entanto, alguns programas também incluem a conscientização dos usuários em geral, bem como das pessoas com mais de 60 anos, que muitas vezes apresentam níveis mais elevados de incerteza sobre o uso da Internet e das redes sociais. Alguns dos principais intervenientes no que diz respeito a estas iniciativas são brevemente descritos a seguir:

- *CGI.br* é o Comitê Gestor da Internet no Brasil e *"tem a atribuição de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil e diretrizes para a execução do registro de Nomes de Domínio, alocação de Endereço IP (Protocolo de Internet) e administração correspondente ao Primeiro Nível Domínio ".br". Também promove estudos e recomenda procedimentos para segurança na Internet e propõe programas de pesquisa e desenvolvimento";*[50]

[50] "About the CGI.br", CGI.br, acessado em 22 de outubro de 2023, traduzido por Firefox Fullpage Translation, https://cgi.br/sobre/.

- *CERT.br é* um CSIRT nacional *"de Último Recurso, mantido pelo NIC.br, e presta serviços na área de tratamento de incidentes de segurança da informação para qualquer rede que utilize recursos gerenciados pelo NIC.br"*;[51]
- *RNP.br é "a rede brasileira de ensino e pesquisa* "e conecta *"mais de 4 milhões de estudantes, professores e pesquisadores brasileiros em universidades, institutos educacionais e culturais, agências de pesquisa, hospitais universitários, parques e polos tecnológicos"*.[52]

O NIC.br mantém um portal que promove o uso seguro da Internet chamado internetsegura.br.[53]Destina-se a crianças, adolescentes, pais e educadores, maiores de 60 anos, técnicos e internautas em geral interessados. Uma apresentação do CERT.br lista ainda uma série de iniciativas de conscientização dirigidas a um público semitécnico e referindo-se às já mencionadas iniciativas de conscientização para o público em geral.[54]Devido a esta evidência, o nível de maturidade do Fator D 2.2 Confiança e Segurança nos Serviços On-line no que diz respeito ao comportamento geral dos usuários quando interagem com serviços on-line pode ser avaliado como minimamente Formativo.

Métricas e estudos sistemáticos, bem como uma extensa campanha dirigida ao público, levariam presumivelmente rapidamente a atingir a fase "Estabelecido". As iniciativas também abordam a desinformação, o que significa que pelo menos uma fase Formativa também é alcançada neste aspecto. Seria útil uma maior participação do governo em programas para reforçar a preparação do público contra a desinformação on-line. Tal envolvimento poderia, por exemplo, se materializar por meio de um apoio financeiro mais forte e ampla promoção também através de canais governamentais das iniciativas acima mencionadas do NIC.br e CERT.br.

No que diz respeito ao governo eletrônico, ao governo digital e o comércio eletrônico, o Brasil já atingiu um nível elevado no Relatório CMM anterior, que remonta a 2020. Nenhuma adição específica foi mencionada pelas partes interessadas e uma base de avaliação importante, um relatório da OCDE sobre o governo digital do Brasil desde 2018, ainda não foi atualizado.[55]No que diz respeito à confiança dos usuários nos serviços de governo eletrônico, o estágio do Brasil permanece no nível Estabelecido.

Também no que diz respeito aos serviços de comércio eletrônico, a situação permanece num nível elevado, conforme já indicado pelo Relatório CMM em 2020. As partes interessadas indicaram que, em particular, o elevado nível de transações bancárias eletrônicas fala de um elevado nível de confiança dos usuários em serviços de comércio eletrônico. Segundo as partes interessadas, em 2019, 48% de todas as transações bancárias ocorreram on-line e o número duplicou desde então. Além disso, os bancos introduziram um sistema novo e seguro

[51]"About CERT.br", CERT.be, acessado em 22 de outubro de 2023, traduzido por Firefox Fullpage Translation, https://cert.br/.

[52] "Who we are", RNP.br, acesso em 22 de outubro de 2023, https://www.rnp.br/en/about/who-we-are.

[53] "Safe Internet", internetsegura.br, consultado em 22 de outubro de 2023, traduzido por Firefox Full Page Translation,https://internetsegura.br/.

[54] "Security Awareness Initiatives in Brazil", CERT.br, acessado em 22 de outubro de 2023, https://cert.br/docs/palestras/certbr-natcsirt2023.pdf.

[55] "Digital Government Review of Brazil: Towards the Digital Transformation of the Public Sector", OCDE, 2018.

para transações on-line instantâneas. Foi bem recebido pelos usuários. Seria útil se o setor privado conduzisse pesquisas e definisse métricas para sustentar e refinar essas afirmações e para que o Brasil atingisse o estágio estratégico no que diz respeito ao comércio eletrônico.

D2.3 COMPREENSÃO DO USUÁRIO SOBRE PROTEÇÃO DE INFORMAÇÕES PESSOAIS ON-LINE

Este Factor analisa se os usuários da Internet e as partes interessadas dos setores público e privado reconhecem e compreendem a importância de proteger as informações pessoais on-line e se são sensíveis aos seus direitos de privacidade.

***Estágio*: Estabelecido**

A compreensão dos usuários sobre a proteção de informações pessoais online deve ser revista no contexto de uma nova Lei Geral de Proteção de Dados Pessoais (LGPD).[56]É uma lei abrangente de proteção de dados pessoais e está amplamente alinhada com o GDPR da UE. A lei exige o desenvolvimento de políticas de privacidade, tanto para o setor privado como para o setor público. O desenvolvimento e a implementação da lei levaram à realização de um debate público sobre a proteção de dados.

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão nacional de fiscalização da proteção de dados pessoais e também realiza iniciativas de conscientização.[57,58]As atividades da ANPD juntamente com a implementação e fiscalização da LGPD indicam que uma proporção crescente de usuários possui habilidades para gerenciar sua privacidade on-line. Isto também é apoiado por reportagens da mídia sobre o assunto.[59]Portanto, o Brasil atingiu claramente um estágio Estabelecido em relação a esse Fator.

[56] "General Personal Data Protection Act (LGPD)", lgpd-brazil.info, consultado em 22 de outubro de 2023, https://lgpd-brasil.info/.

[57] "Autoridade Nacional de Proteção de Dados", ANPD, consultada em 22 de outubro de 2023, https://www.gov.br/anpd/pt-br.

[58] "How to protect your personal data", ANPD, consultada em 22 de outubro de 2023, https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_senacon_ingles.pdf.

[59] Angélica Mari, "Data privacy awareness grows in Brazil", ZDNET, 15 de maio de 2020, https://www.zdnet.com/article/data-privacy-awareness-grows-in-brazil/.

D2.4 MECANISMOS DE REPORTE

Este Factor explora a existência de mecanismos de denúncia que funcionam como canais para os usuários denunciarem crimes relacionados à Internet, como fraude on-line, cyber-bullying, abuso infantil on-line, roubo de identidade, violações de privacidade e segurança e outros incidentes.

***Estágio*: Formativo**

O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR) fornece mecanismos de notificação para instituições governamentais.[60] Além disso, os CERT setoriais fornecem mecanismos de elaboração de relatórios para o setor privado. O CERT.br atua como um CSIRT de última instância em nível nacional, onde também, em geral, os usuários podem reportar incidentes. No entanto, estes mecanismos de denúncia para o público em geral não são amplamente divulgados e o seu público-alvo não é o público em geral, mas sim o último recurso que "pega todos" que não têm outro lugar para recorrer. Por conseguinte, deve ser criada uma plataforma e uma entidade que vise especificamente os usuários da Internet em geral, e potencialmente também as PME. Uma agência dedicada à segurança cibernética poderia, por exemplo, assumir esta função e, também promover este serviço entre os usuários da Internet. Também não existem métricas centralizadas disponíveis que concatenem todos os incidentes relatados sistematicamente pelo setor privado, pelo setor público e pelos usuários da Internet em geral. Portanto, o Brasil atualmente se encontra em um estágio Formativo.

D2.5 MÍDIA E PLATAFORMAS ON-LINE

Este Fator *explora se a segurança cibernética é um assunto comum de discussão na grande mídia e uma questão para ampla discussão nas redes sociais. Além disso, este* Fator *analisa o papel dos meios de comunicação social na transmissão de informações sobre a segurança cibernética ao público, moldando assim os valores, as atitudes e o comportamento on-line dos cidadãos em matéria de segurança cibernética.*

***Estágio*: Formativo**

As partes interessadas indicaram que a cobertura mediática é sobretudo dedicada à fraude financeira. Além disso, os incidentes de segurança cibernética de maior dimensão nos setores público e privado são cobertos pelos mídia de comunicação social. No entanto, as reportagens

[60] "Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo", CTIR, acessado em 22 de outubro de 2023, https://www.gov.br/ctir/pt-br.

das mídias de comunicação social poderiam ser mais amplas e informar os cidadãos, a fim de aumentar a sua conscientização e promover as melhores práticas. Além disso, as discussões nas redes sociais acontecem de forma ad hoc. O Brasil não tem uma cultura positiva de denúncia e, portanto, os relatórios sobre denúncias geralmente não são encontradas na mídia.

RECOMENDAÇÕES

Com base nas consultas, são fornecidas as seguintes recomendações para consideração em relação à maturidade da Cultura e Sociedade de Segurança Cibernética. Estes visam fornecer possíveis próximos passos a serem seguidos para melhorar a capacidade de segurança cibernética existente, em linha com as considerações do Modelo de Maturidade da Capacidade de Segurança Cibernética do GCSCC.

MENTALIDADE DE SEGURANÇA CIBERNÉTICA

R2.1.1 Considerar a implementação de um marco de monitorização, a fim de garantir a sensibilização, a implementação de práticas seguras e a segurança cibernética como uma prioridade em todas as entidades do setor público. A supervisão para garantir a implementação deve ser atribuída a uma agência centralizada e dedicada, como uma agência nacional de segurança cibernética ou CIRT.

R2.1.2 Considerar a possibilidade de obrigar os estados para garantir atividades semelhantes às do nível federal dentro da sua soberania e em nível comunitário.

R2.1.3 Garantir campanhas de sensibilização dirigidas às PME, a fim de abordar a segurança cibernética como uma prioridade e promover práticas seguras de segurança cibernética. Considere delegar essa responsabilidade ao nível estadual e coordene as atividades entre os estados por meio de uma entidade dedicada à segurança cibernética em nível federal.

R2.1.4 Considerar a criação de um órgão que possa coordenar uma abordagem coletiva relativamente à sensibilização para a cibersegurança e às práticas seguras em todo o setor privado, no setor público e na comunidade de defesa e inteligência. O órgão deve ser liderado por uma autoridade civil, a fim de garantir a vontade do setor privado de colaborar plena e abertamente.

R2.1.5 Garantir que as métricas sejam definidas e que sejam realizadas pesquisas, a fim de obter uma imagem completa no que diz respeito à mentalidade dos usuários em geral e de todo o setor privado, incluindo as PME.

CONFIANÇA E SEGURANÇA NA INTERNET

R2.2.1 Garantir que as métricas sejam definidas e que as pesquisas sejam realizadas, a fim de obter uma visão completa da confiança dos usuários na Internet.

R2.2.2 Garantir a promoção das campanhas atualmente lideradas pelo CERT.br e NIC.br, com o objetivo de informar a sociedade em geral.

COMPREENSÃO DO USUÁRIO SOBRE PROTEÇÃO DE INFORMAÇÕES PESSOAIS ON-LINE

R2.3.1 Garantir uma maior promoção da proteção de dados online entre os usuários em geral, independentemente do seu contexto demográfico.

R2.3.2 Implementar mecanismos que garantam que a privacidade e a segurança não concorram.

MECANISMOS DE RELATÓRIOS

R2.4.1 Criar uma entidade e plataforma dedicada que forneça mecanismos de denúncia aos usuários da Internet em geral e às PME; tal entidade também poderia ser federalizada, sendo implementada em nível estadual e coordenada por meio de uma agência de segurança cibernética em nível federal.

R2.4.2 Garantir que as métricas para todos os relatórios (PME, grandes empresas, setor público, usuários da Internet em geral) sejam recolhidas em métricas e pesquisas, a fim de obter uma imagem completa de quaisquer atividades de relatório.

MÍDIA E PLATAFORMAS ON-LINE

R2.5.1 Incentivar os meios de comunicação social a informar não só sobre os principais incidentes de cibersegurança, mas também sobre as melhores práticas e aumentar a sua sensibilização pessoal para a segurança cibernética. Os meios de comunicação social também poderiam ser incentivados a promover uma cultura de denúncia positiva através da divulgação de exemplos de denúncias que tiveram um impacto positivo na cultura de segurança cibernética.

R2.5.2 Incentivar as ONG a criarem um espaço nas redes sociais para discussões sobre segurança cibernética.

DIMENSÃO 3

CONSTRUINDO CONHECIMENTOS E CAPACIDADES DE SEGURANÇA CIBERNÉTICA

Esta Dimensão analisa a disponibilidade, qualidade e aceitação de programas para vários grupos de partes interessadas, incluindo o Governo, o setor privado e a população como um todo, e relaciona-se com programas de conscientização para a segurança cibernética, programas formais de educação em segurança cibernética e programas de formação profissional.

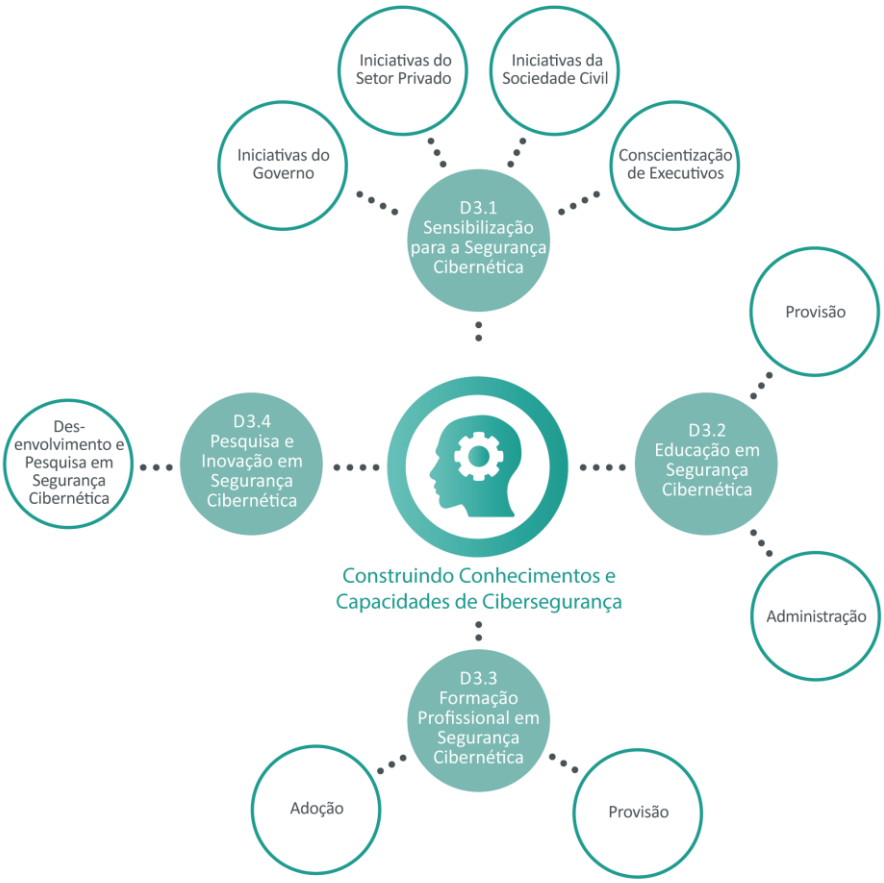
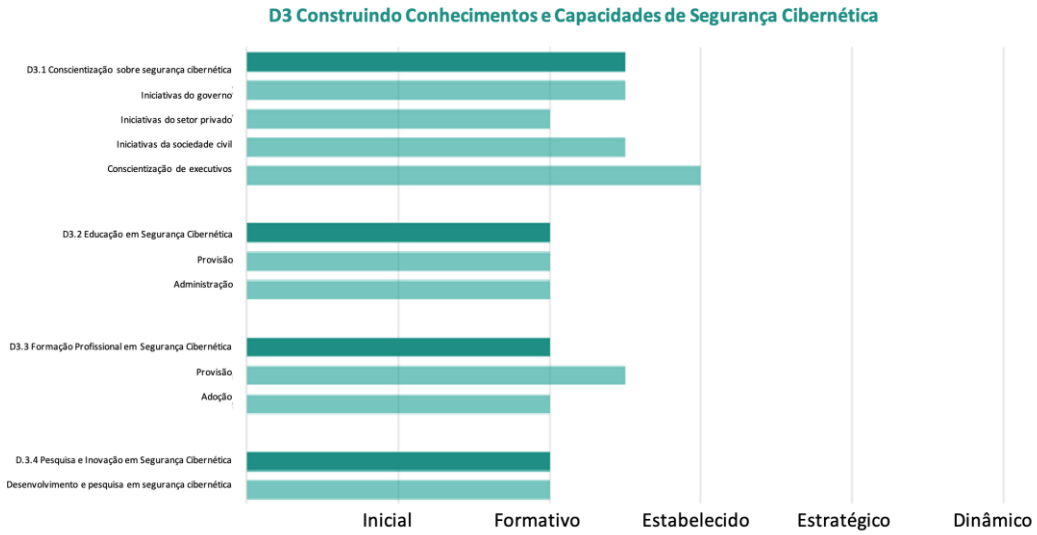


Figura 8: Fatores e aspectos examinados na Dimensão 3.

RESUMO DOS RESULTADOS



D3.1 DESENVOLVER A CONSCIENTIZAÇÃO SOBRE SEGURANÇA CIBERNÉTICA

Este Fator *concentra-se na disponibilidade de programas que aumentem a conscientização sobre segurança cibernética em todo o país, concentrando-se nos riscos e ameaças à segurança cibernética e nas formas de enfrentá-los.*

***Estágio*:** Formativo para Estabelecido

O NCS *E-Ciber* do Brasil identifica a conscientização sobre segurança cibernética como uma das três áreas de atividade na seção 2.4 Educação. Recomenda a criação de planos de sensibilização em escolas e instituições, portais de boas práticas e campanhas educativas. No entanto, a E-Ciber não fornece uma visão geral das ações específicas que devem ser implementadas – geralmente recomenda aumentar a conscientização por meio de várias possibilidades para fazê-lo, incluindo exemplos de outros países. Portanto, esta revisão baseia-se principalmente nas declarações das partes interessadas e nas evidências de atividades de conscientização disponíveis on-line.

Diversas campanhas de conscientização sobre segurança cibernética já foram listadas na Dimensão 2. Mais importante ainda, o *internetsegura.br*, uma iniciativa do NIC.br e do

CERT.br, presta consultoria ao público em geral.[61]CERT.br e NIC.br são organizações que funcionam sob a chancela de mandatos governamentais e podem ser caracterizadas como organizações multissetoriais. A estrutura de governança dessas organizações é brevemente descrita a seguir, com base nas informações disponibilizadas no site do NIC.br.[62]

O CGI.br é o Comitê Gestor da Internet no Brasil, que *"foi criado pela Portaria Interministerial nº 147, de 31 de maio de 1995, alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003, com o objetivo de coordenar e integrar todas as iniciativas de serviços de Internet no Brasil, bem como promover a qualidade técnica, a inovação e a difusão dos serviços disponíveis."*[63]Embora estabelecido por meio de portaria nacional e decreto presidencial, o comitê não é uma instituição governamental per se. Inclui nove representantes do governo federal, quatro representantes do setor empresarial, quatro representantes do terceiro setor (ou seja, ONGs), três representantes da comunidade científica e tecnológica e um especialista em Internet. Portanto, pode ser caracterizado como um órgão multissetorial, incluindo representantes do governo, do setor privado, da sociedade civil/ONGs, da ciência e da tecnologia, bem como um especialista no assunto. Conforme mostra a Figura 9, o CGI.br funciona como órgão de governo do NIC.br por meio da constituição dos membros com direito a voto na Assembleia Geral do NIC.br. O NIC.br é subdividido em diferentes entidades organizacionais, incluindo o CERT.br.

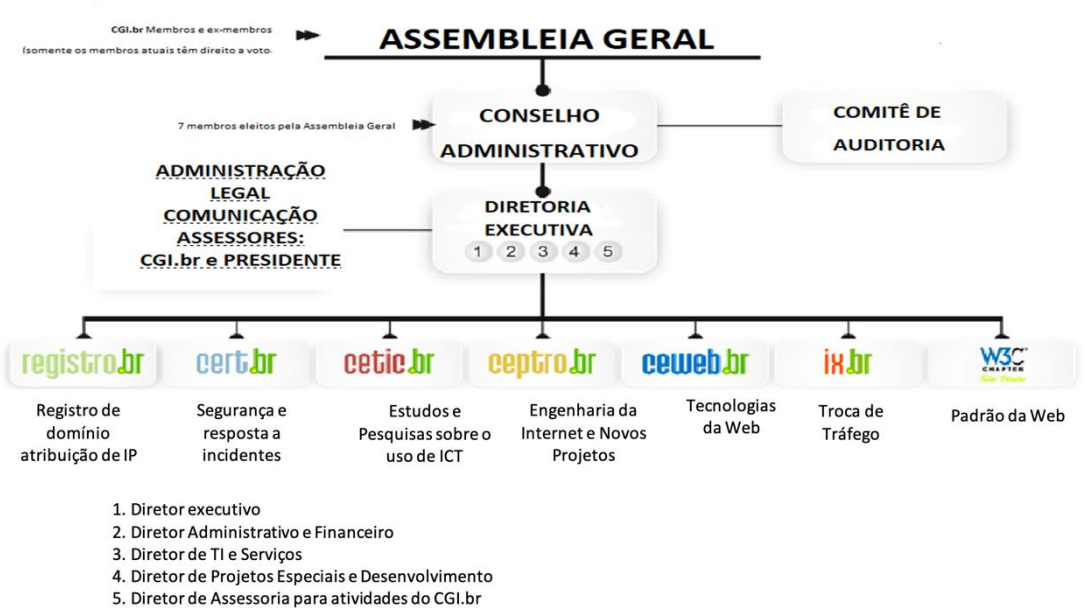


Figura 9: Estrutura de governança do NIC.br e suas suborganizações, conforme listadas no site do NIC.br.[64]

As campanhas e atividades do NIC.br e suas suborganizações poderiam se beneficiar de um maior apoio governamental, por exemplo, por meio de maior financiamento e promoção apoiados pelo governo. O impacto destes programas não é monitorado por meio de pesquisas ou métricas orientadas para os resultados. Além disso, uma coordenação sistemática e um portal dedicado ao público em geral, por exemplo, fornecido por uma agência dedicada à

[61] "Safe Internet", internetsegura.br, consultado em 22 de outubro de 2023, traduzido por Firefox Full Page Translation, https://internetsegura.br/.
[62] "Who we are", NIC.br, acesso em 2 de novembro de 2023, https://nic.br/who-we-are/.
[63] "About the CGI.br", CGI.br, acesso em 2 de novembro de 2023,https://cgi.br/about/.
[64] " Who we are", NIC.br, acesso em 2 de novembro de 2023, https://nic.br/who-we-are/.

segurança cibernética, seriam benéficos, como também foi formulado na secção 2.4 da E-Ciber. As atividades de conscientização do CERT.br e do NIC.br também abordam o pessoal técnico do setor privado, conforme descrito em uma apresentação geral fornecida anteriormente na Dimensão 2.[65]Por exemplo, o Programa Internet+Segura fornece melhores práticas com relação a configurações úteis contra ataques comuns à rede.[66]Embora as atividades cumpram claramente os requisitos da fase Formativa, também indicam avanços em direção à fase Estabelecida. Os requisitos mais importantes para alcançar plenamente a fase estabelecida que ainda precisam de ser cumpridos são o fornecimento de métricas e pesquisas, bem como uma coordenação sistemática das iniciativas do governo e da sociedade civil.

As partes interessadas indicaram que muitas campanhas de sensibilização são realizadas pelo setor privado, particularmente no setor bancário, uma vez que isto também é impulsionado por requisitos do regulador. No entanto, não existem revisões sistemáticas por meio de métricas e pesquisas e as diversas iniciativas do setor privado não são coordenadas centralmente. Embora os indicadores para atingir a fase Formativa sejam claramente fornecidos, seria necessária uma coordenação e revisão sistemáticas das atividades do setor privado, a fim de atingir a fase Estabelecida.

Empresas internacionais de capacitação em segurança cibernética também oferecem cursos para executivos no Brasil.[67]As partes interessadas indicaram que existe intercâmbio de conhecimentos entre executivos de grandes empresas no que diz respeito à segurança cibernética. Além disso, as empresas negociadas na bolsa de valores adotaram protocolos para vice-presidentes, conselhos de administração e CEOs, incluindo decisões de investimento no que diz respeito à abordagem dos riscos de segurança cibernética. No setor bancário, existe uma comissão executiva para a cibersegurança, onde os executivos se reúnem regularmente para discutir aspectos da cibersegurança. As empresas maiores também realizam exercícios de simulação de segurança cibernética em todos os níveis. Portanto, o estágio Estabelecido é alcançado. No entanto, as partes interessadas também indicaram que as pequenas empresas não estão conscientes dos riscos e carecem de formação. O setor privado poderia beneficiar de cursos obrigatórios de segurança cibernética em todos os setores para executivos de grandes empresas e de uma maior promoção e oferta de cursos de nível executivo para PME. Atualmente, a estratégia cibernética do Brasil não atribui um orçamento dedicado ao estabelecimento de um programa de formação de gestores. Isto deve ser considerado numa próxima revisão da estratégia e, entretanto, deve ser atribuído um orçamento para a criação de programas de formação coordenados.

[65] "Security Awareness Initiatives in Brazil", CERT.br, acessado em 22 de outubro de 2023, https://cert.br/docs/palestras/certbr-natcsirt2023.pdf.

[66] "Para fazermos uma Internet mais Segura", Programa Internet+Segura, acessado em 22 de outubro de 2023, https://bcp.nic.br/i+seg/.

[67] "Cyber Security Training – Brazil", The Knowledge Academy, acessado em 22 de outubro de 2023, https://www.theknowledgeacademy.com/br/courses/cyber-security-training/.

D3.2 EDUCAÇÃO EM SEGURANÇA CIBERNÉTICA

Este Fator *aborda a disponibilidade e o fornecimento de programas de educação em segurança cibernética de alta qualidade e a disponibilidade de professores e palestrantes qualificados em número suficiente. Além disso, este* Fator *examina a necessidade de melhorar a educação em segurança cibernética a nível nacional e institucional, e a colaboração entre o governo e a indústria para garantir que os investimentos educacionais atendam às necessidades do ambiente de educação em segurança cibernética em todos os setores.*

***Estágio*:** Formativo

À semelhança do Fator anterior, a educação em segurança cibernética é elencada como área de atuação sob o termo "Formação" na seção 2.4 do E-Ciber. A NCS menciona a necessidade da criação de cursos e da inserção da segurança cibernética como disciplina nos currículos escolares de todos os níveis, inclusive das universidades. Contudo, nenhuma ação específica está listada no E-Ciber sobre como isso deve ser alcançado. Embora exista um plano de ação, nenhum acesso a este plano de ação foi fornecido aos autores deste relatório. Por conseguinte, a avaliação baseia-se principalmente em declarações das partes interessadas e em provas recolhidas on-line. O E-Ciber menciona que a segurança cibernética "nas escolas brasileiras ainda é muito incipiente, senão inexistente".[68]

As partes interessadas indicaram que os cursos de Ciência da Computação oferecidos nas universidades são harmonizados por meio de um currículo coordenado pela Sociedade Brasileira de Computação (SBC).[69]A segurança de sistemas é um componente padrão do currículo não apenas de ciência da computação, mas também de outros cursos de graduação relacionados a informática e software definidos pela SBC em 2017.[70]Os interessados também indicaram que a SBC concluiu a preparação da definição de um curso de graduação em segurança cibernética em 2022, o que permitirá às universidades oferecer um programa inteiramente dedicado à segurança cibernética. No entanto, ainda não há evidências disponíveis online para o programa deste curso. Embora estes sejam indicadores necessários para atingir a fase estabelecida, alguns outros indicadores desta fase ainda precisam de ser alcançados. Em particular, a segurança cibernética ainda não é um tema amplamente adotado em disciplinas não técnicas e não está claro se as universidades também oferecem palestras e seminários sobre segurança cibernética destinados a um público não especializado, por exemplo, em cursos de direito ou de ética. Alguns participantes indicaram que diversas universidades em determinadas regiões oferecem tais cursos, palestras e seminários. No entanto, este ainda não parece ser o caso em todo o país.

Embora a SBC também aborde a educação em ciências da computação no currículo do ensino fundamental e médio, não está claro se a segurança cibernética faz realmente parte destes níveis, além disso, dado que o ensino fundamental e médio é parcialmente da

[68] Ver seção 2.4 do E-Ciber.

[69] "Sociedad Brasileira de Computação", SBC, consultada em 22 de outubro de 2023, https://www.sbc.org.br/.

[70] "Referências de Formação para Cursos de Graduação em Computação" 2017, SBC, acessado em 22 de outubro de 2023, https://www.sbc.org.br/documentos-da-sbc/send/127-educacao/1155-rereferenceis-de-formacao-para-cursos-de-graduacao-em-computacao-outubro-2017.

responsabilidade do nível de governo comunitário e estadual. Os participantes indicaram que, embora existam muitas iniciativas e atividades, o sistema educativo se beneficiaria de uma coordenação mais coerente da educação em segurança cibernética. Além disso, deverá ser reservado um orçamento específico para a educação em matéria de segurança cibernética. Atualmente, não existe financiamento nacional dedicado à pesquisa em segurança cibernética e também o financiamento para concursos e bolsas de estudo neste domínio é limitado e não é coordenado a nível nacional. Como o currículo de segurança cibernética para cursos universitários de graduação acabou de ser estabelecido, também não há métricas disponíveis – da mesma forma, não existem métricas para o ensino fundamental ou médio em segurança cibernética. Não foram fornecidos dados sobre a disponibilidade de professores qualificados para a segurança cibernética. As discussões com as partes interessadas sugerem que os conhecimentos especializados de ensino estão provavelmente disponíveis no ensino superior, mas faltam principalmente nos níveis fundamental e médio. Portanto, pode-se afirmar que existe um pequeno grupo de professores qualificados, mas que são necessárias mais iniciativas para estabelecer uma ampla disponibilidade de professores.

D3.3 FORMAÇÃO PROFISSIONAL EM SEGURANÇA CIBERNÉTICA

Este Fator *aborda e analisa a disponibilidade e o fornecimento de programas de formação profissional em segurança cibernética acessíveis para construir um quadro de profissionais de segurança cibernética. Além disso, este* Fator *analisa a adoção de formação em segurança cibernética e a transferência horizontal e vertical de conhecimentos e competências em segurança cibernética dentro das organizações, e como esta transferência de competências se traduz num aumento contínuo de quadros de profissionais de segurança cibernética.*

***Estágio*:** Formativo

Tal como acontece com os Fatores anteriores desta Dimensão, a formação profissional em cibersegurança é mencionada nas NCS na secção 2.4. A NCS descreve a dificuldade de adquirir pessoal qualificado: 34% dos empregadores brasileiros teriam dificuldade em recrutar talentos. As maiores dificuldades das empresas brasileiras no processo de contratação são a falta de competências técnicas (33%), a falta de experiência (23%) e a falta de habilidades interpessoais (19%). A E-Ciber afirma ainda que "*o setor privado foca intensamente no desenvolvimento da força de trabalho.*"[71] Além disso, a estratégia formula a "fuga de cérebros" como um problema para a economia brasileira no que diz respeito ao pessoal capacitado. Mais uma vez, não foram listadas ações específicas para resolver a situação descrita e nenhum acesso ao plano de implementação/ação da NCS foi fornecido aos autores, razão pela qual a avaliação a seguir se baseia principalmente nas discussões das partes interessadas e nas evidências encontradas on-line.

No que diz respeito à formação vocacional e profissional, as partes interessadas indicaram que não existe atualmente uma coordenação nacional dessa formação. Existem muitas iniciativas ad hoc e da indústria. No entanto, existe uma lacuna significativa na força de trabalho e um problema com a mudança de profissionais qualificados para o estrangeiro

[71] Ver seção 2.4 do E-Ciber.

devido aos salários mais elevados. Existem certificações internacionais comuns para profissionais de segurança cibernética. Contudo, existem apenas disposições limitadas de formação ministradas a nível nacional que proporcionariam profundidade suficiente no que diz respeito às competências tecnológicas e práticas. As partes interessadas indicaram que muitos cursos profissionais não vão além dos conceitos e não oferecem formação prática. Certos setores oferecem os seus próprios programas de formação, que não são coordenados com outros setores ou a nível nacional. Para preencher essa lacuna, instituições como o NIC.br oferecem treinamentos e iniciativas para integrar os jovens e levá-los a conhecer o domínio da segurança cibernética como uma possível área de emprego. Exemplos são programas como *Hackers do Bem* ("Hackers for Good")[72], dirigido aos jovens, ou seminários gratuitos sobre segurança cibernética oferecidos pela *Escola Superior de Redes*[73].

As partes interessadas relataram a disponibilidade de um curso universitário de segurança cibernética com foco prático. No entanto, as pessoas lutam com a integração no mercado de trabalho, uma vez que não têm experiência prática. Portanto, seria útil aumentar a interligação entre as faculdades de segurança cibernética e a indústria como parte dos cursos, a fim de proporcionar aos formandos experiência prática de trabalho antes de se formarem. As partes interessadas indicaram que uma das principais desvantagens do panorama da formação profissional é uma abordagem transversal que integra os requisitos da indústria com a oferta de educação centrada no profissionalismo. Embora exista coordenação informal, um órgão dedicado deve assumir a coordenação dos requisitos da indústria e dos currículos dos prestadores de formação locais.

Embora as discussões tenham mostrado que os indicadores exigidos para o Estágio Formativo são atendidos, o Brasil ainda precisa coordenar suas atividades para a formação profissional de forma mais ampla. Em particular, as necessidades da sociedade têm de ser sistematicamente analisadas e integradas em programas de formação vocacional e profissional que têm de ser coordenados a nível nacional e setorial. Além disso, o governo deve financiar e incentivar iniciativas para que profissionais qualificados permaneçam no país após a conclusão bem-sucedida dos cursos e após adquirirem experiência na indústria. Além disso, muitos programas parecem centrar-se nos jovens. O Brasil poderia explorar a possibilidade de programas de transição de carreira para profissionais não relacionados à segurança cibernética. Finalmente, os programas de formação profissional devem ser revistos regular e sistematicamente por meio de métricas, a fim de avaliar se a formação ministrada atende às demandas do setor público e privado e se o financiamento é suficiente.

[72] "Hackers do Bem", Hackers do Bem, acessado em 22 de outubro de 2023, https://conteudo.hackersdobem.org.br/oprograma.

[73] "Escola Superior de Redes, Instituto SANS", Escola Superior de Redes, acessado em 22 de outubro de 2023, https://esr.rnp.br/.

D3.4 PESQUISA E INOVAÇÃO EM SEGURANÇA CIBERNÉTICA

Este Fator *aborda a ênfase colocada na pesquisa e inovação em segurança cibernética para enfrentar os desafios tecnológicos, sociais e empresariais e para promover a construção de conhecimentos e capacidades de segurança cibernética no país.*

***Estágio*:** Formativo

A NCS do Brasil lista sua abordagem em relação à pesquisa, desenvolvimento e inovação na Seção 2.2. Descreve que as iniciativas de investigação, desenvolvimento e inovação na área da segurança cibernética requerem maior prioridade. A NCS identifica lacunas nas atividades de investigação em cibersegurança e define o requisito de promover uma coordenação nacional de atividades e financiamento. A E-Ciber estabelece a exigência de implementação de programas de mestrado e doutorado, a fim de melhorar a pesquisa, o desenvolvimento e a inovação em segurança cibernética. No entanto, não está claro como isto deve ser implementado especificamente, embora isto possa ser definido num plano de ação ao qual os autores não tiveram acesso. A avaliação a seguir, portanto, baseia-se principalmente em evidências encontradas on-line e em discussões das partes interessadas.

De acordo com as partes interessadas, as atividades de I&D em segurança cibernética são realizadas principalmente como parte de atividades convencionais de pesquisa em ciências informáticas, por exemplo, como parte de pesquisa e desenvolvimento em segurança de redes ou sistemas. Exemplos de tais atividades estão listados a seguir:

- *SBSeg* um simpósio brasileiro anual de pesquisa em segurança da informação e sistemas computacionais.[74]Centra-se nos aspectos tecnológicos da cibersegurança, como fica evidente, por exemplo, no seu programa em 2023;[75]
- *RNP.br*, o provedor da rede nacional de pesquisa, oferece uma subvenção de inovação e pesquisa para projetos tecnologicamente inovadores que abrange também a segurança cibernética;[76]
- As partes interessadas mencionaram vários projetos de pesquisa em universidades sobre temas de segurança cibernética, que foram realizados nos últimos 3 a 5 anos. Esses projetos têm foco tecnológico.

As partes interessadas também destacaram que a pesquisa está integrada na colaboração internacional e, em particular, regional na América Latina. Não existem métricas sistemáticas para avaliar o desempenho da I&D no que diz respeito à segurança cibernética, mas existem métricas ad hoc.

Portanto, o Brasil cumpre claramente todos os indicadores exigidos para o Estágio Formativo. Alguns indicadores para o nível estabelecido também podem estar presentes. O principal

[74] "SBSeg Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais", SBSeg, acessado em 22 de outubro de 2023, https://sbseg2023.ufjf.br/.

[75] "Programação SBSeg 2023", SBSeg, acessado em 22 de outubro de 2023, https://sbseg2023.ufjf.br/programacao/.

[76] "Programa de Bolsas de Incentivo à Pesquisa, Desenvolvimento e Inovação", RNP.br, acessado em 22 de outubro de 2023, https://www.rnp.br/en/node/7766.

obstáculo para atingir o nível Estabelecido é a falta de financiamento nacional sistemático especificamente para questões de segurança cibernética e que também vai além do domínio da tecnologia e da computação. Uma próxima versão de uma estratégia nacional de cibersegurança deverá considerar a disponibilização de financiamento específico deste tipo, que também aborde disciplinas para além da tecnologia e da computação. Além disso, as métricas devem ser implementadas sistematicamente para medir o desempenho das atividades de I&D em segurança cibernética.

RECOMENDAÇÕES

Seguindo as informações apresentadas durante a revisão da maturidade do Desenvolvimento de Conhecimentos e Capacidades em Segurança Cibernética, o seguinte conjunto de recomendações é fornecido ao Brasil. Estas recomendações visam fornecer orientações e passos a seguir para fortalecer a capacidade de segurança cibernética existente, seguindo as considerações do Modelo de Maturidade da Capacidade de Cibersegurança do GCSCC.

CONSTRUINDO CONSCIÊNCIA DE SEGURANÇA CIBERNÉTICA

R3.1.1 Os processos de revisão do programa e as métricas orientadas para os resultados devem ser implementados para iniciativas de conscientização para a cibersegurança no governo, na sociedade civil e no setor privado, obrigatórias e monitorizadas por uma agência dedicada à cibersegurança.

R3.1.2 Deve ser implementada uma coordenação sistemática das iniciativas de sensibilização do setor privado. Isto poderia, por exemplo, ser apoiado por uma agência nacional dedicada à cibersegurança e integrado no portal existente *internetsegura.br*.

R3.1.3 Cursos obrigatórios de segurança cibernética para executivos de empresas maiores devem ser considerados e coordenados por um parceiro autorizado, como uma agência nacional de segurança cibernética ou o NIC.br. Para as PME, esses cursos devem ser oferecidos gratuitamente ou a baixo custo, a fim de refletir as pressões económicas que as PME enfrentam frequentemente.

R3.1.4 Uma futura versão da estratégia nacional de segurança cibernética deverá atribuir um orçamento específico para programas de formação para gestores, em particular para PME que enfrentam limitações económicas. Antes da próxima versão de uma estratégia de segurança cibernética, a lacuna financeira poderia ser preenchida através da atribuição de parte do orçamento do governo para este fim.

EDUCAÇÃO EM SEGURANÇA CIBERNÉTICA

R3.2.1 Considerar a introdução da segurança cibernética como parte de cursos não especializados em universidades de todo o país, por exemplo, em ética ou direito. Considere oferecer seminários e palestras sobre segurança cibernética para um público não especializado, por meio da adição de segurança cibernética aos

currículos de outros cursos com sobreposição de tópicos. Introduz, com alta prioridade, programas de graduação dedicados à segurança cibernética (bacharelado, mestrado e doutorado) em todas as universidades. Estas tarefas devem ser confiadas a um órgão específico, como a Sociedade Brasileira de Computação ou uma agência nacional de segurança cibernética.

R3.2.2 Considerar a coordenação da educação em segurança cibernética abaixo do nível universitário (por exemplo, ensino fundamental e médio e superior) através do Ministério da Educação, em colaboração com outras partes interessadas, como o NIC.br e uma agência nacional de segurança cibernética.

R3.2.3 Considerar a introdução de um orçamento nacional e estadual dedicado a todos os níveis de educação em segurança cibernética (ensino fundamental e médio e superior etc.). Esta tarefa deve ser assumida por um órgão específico, por exemplo, uma entidade do Ministério da Educação.

R3.2.4 Alocar um orçamento nacional para bolsas de estudo para estudantes de segurança cibernética e concursos de segurança cibernética. Isto deve ser confiado a um órgão específico, como um conselho nacional de investigação ou o Ministério da Educação.

R3.2.5 Implementar métricas e pesquisas para monitorar a eficácia e a procura de educação em segurança cibernética, exigidas por uma agência nacional de cibersegurança em colaboração com o Ministério da Educação.

FORMAÇÃO PROFISSIONAL EM SEGURANÇA CIBERNÉTICA

R3.3.1 Considerar a coordenação nacional da formação profissional através de um órgão específico, como o Ministério da Educação ou uma agência nacional de segurança cibernética. A coordenação deve abranger uma abordagem transversal, integrando as necessidades da indústria nos currículos de formação.

R3.3.2 Estabelecer uma forte interconexão entre os programas universitários de segurança cibernética e a indústria; por exemplo, permitindo que os alunos adquiram experiência prática de trabalho na indústria como parte de cursos universitários de segurança cibernética. Isto deve ser incluído como uma visão estratégica numa futura versão de uma Estratégia Nacional de Cibersegurança e atribuído a um órgão dedicado, por exemplo, dentro do Ministério da Educação ou de uma agência nacional de segurança cibernética.

R3.3.3 Estabelecer, através de um mandato do Ministério da Educação a uma entidade dedicada, mecanismos e fundos dedicados para incentivar profissionais formados e profissionais com experiência profissional a permanecerem no mercado de trabalho do país.

R3.3.4 Considere estabelecer e financiar programas de transição de carreira para profissionais que não sejam de segurança cibernética. Isso deveria ser atribuído pelo governo para uma instituição dedicada do setor privado ou ONG, ou NIC.br.

R3.3.5 Realizar revisões e estudos e estabelecer métricas para monitorar se os programas de formação ministrados atendem às demandas do setor público e privado. Esta tarefa deve ser encomendada a uma agência dedicada à segurança cibernética.

PESQUISA E INOVAÇÃO EM SEGURANÇA CIBERNÉTICA

R3.4.1 Incluir financiamento nacional dedicado para atividades de P&D em segurança cibernética, incluindo tópicos além da tecnologia e da ciência da computação, como parte da próxima versão de uma estratégia nacional de segurança cibernética e atribuir a responsabilidade a um órgão específico, como um conselho nacional de pesquisa.

R3.4.2 Recolher sistematicamente métricas sobre todas as atividades de I&D em segurança cibernética e exigências de pesquisas a nível nacional, a fim de apresentar relatórios sobre o desempenho das atividades de I&D e o financiamento concedido. Isto deve ser atribuído pelo Ministério da Educação a uma entidade específica, como um gabinete nacional de estatística ou similar.

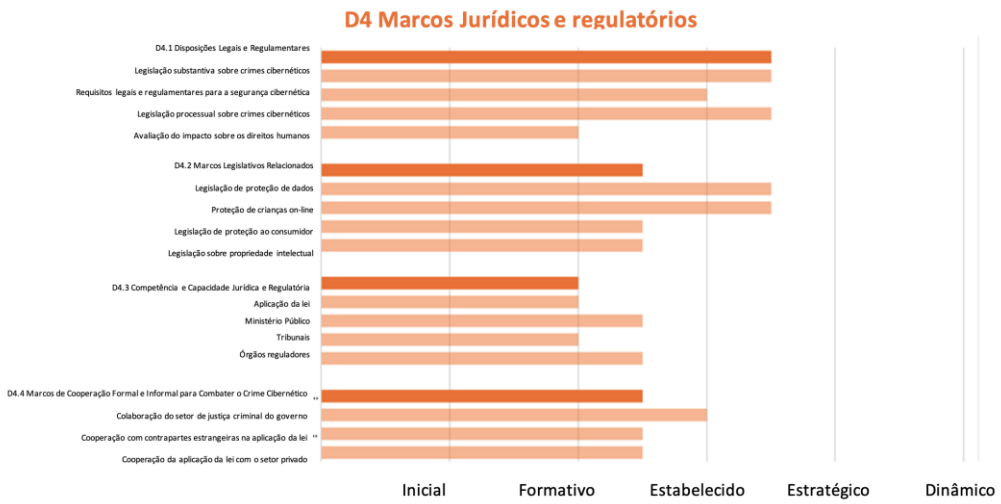
R3.4.3 Considerar a possibilidade de iniciar um fórum ou simpósio nacional sobre segurança cibernética, que aborde tópicos tecnológicos e não tecnológicos, como direito cibernético, segurança cibernética e política internacional, ou ética cibernética. Esta tarefa deve ser confiada a um órgão especializado, por exemplo, um conselho nacional de pesquisa ou uma agência nacional de segurança cibernética, em colaboração com o meio académico e o setor privado.

DIMENSÃO 4
MARCOS JURÍDICOS E REGULATÓRIOS

Esta *Dimensão* examina a capacidade do Governo para conceber e promulgar legislação nacional que se relacione direta e indiretamente com a segurança cibernética, com especial ênfase nos tópicos de requisitos regulamentares para a segurança cibernética, legislação relacionada com o crime cibernético e legislação relacionada. A capacidade de fazer cumprir essas leis é examinada através da aplicação da lei, da promotoria, dos organismos reguladores e tribunais. Além disso, esta Dimensão observa questões como os marcos de cooperação formais e informais para combater o crime cibernético.

Figura 9: Fatores e aspectos examinados na Dimensão 4.

RESUMO DOS RESULTADOS



D4.1 DISPOSIÇÕES JURÍDICAS E REGULATÓRIAS

Este Fator *aborda diversas disposições legislativas e regulamentares relacionadas com a segurança cibernética, incluindo requisitos jurídicos e regulatórios, legislação substantiva e processual sobre crimes cibernéticos e avaliação de impacto nos direitos humanos.*

***Estágio*:** Estabelecido para Estratégico

A legislação substantiva sobre crimes cibernéticos foi revisada de forma abrangente na Revisão do CMM de 2020 do Brasil. O leitor deve consultar o relatório de 2020 para obter uma lista detalhada de crimes cibernéticos e leis criminais específicas. As alterações na lei desde a revisão anterior do CMM são fornecidas a seguir, quando aplicável.

As partes interessadas indicaram que as leis relativas à cadeia de custódia digital foram melhoradas:[77]Graças à legislação secundária, a cadeia de custódia digital pode agora ser plenamente estabelecida, auxiliando nas investigações criminais e no direito processual penal (por exemplo, LEI Nº 14.155, DE 27 DE MAIO DE 2021[78]foi adaptado para incluir aspectos digitais). Segue a norma ISO 17005. Os participantes afirmaram que a legislação penal reflete adequadamente o crime cibernético; Questões como acesso não autorizado são bem regulamentadas. A Convenção de Budapeste foi assinada em 2023. De acordo com as partes interessadas, a legislação nacional já cobria amplamente a sua implementação. O referido estabelecimento de uma cadeia de custódia digital uma das principais mudanças implementadas para garantir ainda mais a conformidade. Contudo, é necessário iniciar um

[77] O termo "cadeia de custódia digital", neste contexto, refere-se à documentação da propriedade de um ativo digital (por exemplo, dados) e sua transferência de uma pessoa ou organização para outra, incluindo a data exata, a hora e a finalidade da transferência etc.

[78] "LEI Nº 14.155, DE 27 DE MAIO DE 2021", GSI, consultado em 2 de novembro de 2023,https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm.

processo para garantir que os requisitos da Convenção de Budapeste sejam totalmente consistentes com a legislação nacional brasileira. Este processo está em curso. O segundo protocolo da Convenção de Budapeste é de particular importância para o Brasil, pois melhora as possibilidades de cooperação internacional e o intercâmbio de informações para as autoridades brasileiras. No entanto, o Brasil já foi integrado em redes de cooperação policial, por exemplo, através da Interpol e do G7. A Convenção de Budapeste deverá permitir que o Brasil troque informações com muita rapidez e obtenha os dados necessários para investigações muito rapidamente. A Polícia Federal também está envolvida no projeto No More Ransom como "Parceiro de Apoio", oferecendo tempo e recursos para ajudar a promover o projeto nacional e internacionalmente.[79]O objetivo do projeto é *"ajudar as vítimas de ransomware a recuperar seus dados criptografados sem ter que pagar aos criminosos"*.[80]O projeto também visa a prevenção do crime por meio da educação de usuários e empresas. Isto é apoiado pela Polícia Federal, promovendo o projeto e compartilhando conhecimento dentro do Brasil.

Geralmente, a abordagem do Brasil baseia-se no tratamento do crime cibernético através da lei convencional; a lei específica para o crime cibernético só é introduzida quando a lei convencional não consegue abranger adequadamente os casos de crime cibernético. Por exemplo, os casos de ransomware são tratados como extorsão convencional.

Atualmente, a legislação brasileira não exige que violações de dados sejam comunicadas, desde que não incluam dados pessoais. No que diz respeito aos dados pessoais, estes são abrangidos pela recentemente introduzida Lei Geral de Proteção de Dados Pessoais (LGPD), que é semelhante ao RGPD da UE.[81]Um guia detalhado sobre as semelhanças e diferenças entre LGPD e GDPR pode ser encontrado no site da Comissão Europeia.[82]O guia descreve como a maioria dos aspectos do LGDP são consistentes com o GDPR, com algumas exceções no domínio da investigação e proteção contra discriminação. No que diz respeito à proteção de dados pessoais de crianças, a LGPD é mais rigorosa que o GDPR, mas o limite de idade fornecido é inferior ao do GDPR. Outras diferenças descritas pelo guia muitas vezes afirmam que a LGPD é, na verdade, muitas vezes mais restritiva, ou seja, fornece um nível mais rigoroso de proteção de dados pessoais.

Alguns setores, por exemplo o bancário, exigem relatórios obrigatórios. No entanto, um requisito geral para a notificação obrigatória seria provavelmente útil em todos os setores – como um requisito mínimo de notificação para incidentes em setores onde não existe uma entidade reguladora ou não exige a notificação.

Devido às atividades em andamento para melhorar as disposições legais e regulatórias, o Brasil já pode ser considerado parcialmente no nível Estratégico. Contudo, deve-se dar especial atenção à consideração de outros mecanismos de notificação obrigatória. Deve ser descrito um requisito legal de notificação para todos os setores sob a forma de um requisito mínimo de notificação de incidentes. Em setores não críticos, e no caso de não haja dados pessoais em questão, essas denúncias podem até ser anonimizadas, com a vantagem de

---

[79] "No More Ransom", nomoreransom.org, acessado em 22 de outubro de 2023, https://www.nomoreransom.org/cs/index.html.

[80] "About the Project", nomoreransom.org, acessado em 02 de novembro de 2023, https://www.nomoreransom.org/en/about-the-project.html.

[81] " General Personal Data Protection Act (LGPD)", lgpd-brazil.info, consultado em 22 de outubro de 2023, https://lgpd-brasil.info/.

[82] " Comparing privacy laws: GDPR v. LGPD", DataGuidance by OneTrust, acessado em 02 de novembro de 2023, https://ec.europa.eu/futurium/en/system/files/ged/dataguidance-gpdr-lgpd-for-print.pdf.

fornecer às autoridades um quadro mais claro das atividades maliciosas realizadas no setor privado.

As partes interessadas também indicaram que não foi realizada uma avaliação sistemática do impacto nos direitos humanos. Os participantes também afirmaram que devido à introdução da LGDP muitos aspectos relativos aos direitos humanos já estão refletidos nas disposições legais e regulatórias. No entanto, deve ser feita uma revisão sistemática da legislação sobre o cibercrime sobre o seu impacto nos direitos humanos, a fim de garantir que o objetivo benevolente de combater o cibercrime não tenha impacto nos direitos dos cidadãos on-line.

D4.2 MARCOS LEGISLATIVOS RELACIONADOS

Este Factor aborda os marcos legislativos relativos à segurança cibernética, incluindo proteção de dados, proteção infantil, proteção do consumidor e propriedade intelectual.

***Estágio*:** Formativo para Estabelecido (com elementos de Estratégico)

Conforme afirmado anteriormente, o Brasil introduziu uma Lei Geral de Proteção de Dados Pessoais (LGPD) abrangente, concebida de forma semelhante ao GDPR da UE. [83]A agência líder designada é a Autoridade Nacional de Proteção de Dados (ANPD).[84] Portanto, o estágio Estabelecido é claramente alcançado com relação a este aspecto. Dado que a lei é nova, provavelmente ainda não foi revista desde a sua introdução. Para atingir o nível Estratégico, o Brasil se beneficiaria de uma revisão regular de sua legislação de proteção de dados pessoais e, também deveria procurar promulgar mecanismos em sua estrutura, de modo que a lei possa se adaptar rapidamente às tecnologias emergentes. Isso poderia ser definido como responsabilidade da ANPD.

O Brasil também possui uma lei de proteção infantil implementada para a esfera digital, que é revisada e adaptada periodicamente. Por exemplo, adaptações recentes reforçam a luta contra a pornografia infantil on-line. Da mesma forma que a proteção de dados, o Brasil poderia se beneficiar de um mecanismo que levasse em conta as tecnologias emergentes em sua legislação de proteção infantil on-line.

A proteção do consumidor on-line é coberta principalmente pelo direito convencional, conforme descrito no Relatório CMM de 2020. No entanto, o phishing não é atualmente considerado um ato criminoso em si. Isto cria uma lacuna no quadro jurídico e o Brasil pode querer considerar preencher essa lacuna. Em particular, porque o Brasil é caracterizado como líder em ataques de phishing em todo o mundo em artigo da zdnet.com.[85]Os participantes afirmaram que a criminalização do phishing levaria a um aumento significativo nas investigações criminais; no entanto, deveria ser considerada uma lei que pudesse abranger o estabelecimento sistemático de infraestruturas para fins de phishing. Além disso, a

[83] "General Personal Data Protection Act (LGPD)", lgpd-brazil.info, consultado em 22 de outubro de 2023, https://lgpd-brasil.info/.

[84] "Autoridade Nacional de Proteção de Dados", ANPD, consultada em 22 de outubro de 2023, https://www.gov.br/anpd/pt-br.

[85] Angélica Mari, "Brazil leads in phishing attacks", ZDNET, 24 de março de 2021,

criminalização do Phishing em si provavelmente levaria a uma diminuição das campanhas de Phishing devido ao efeito dissuasivo da criminalização, mesmo que nem todas as campanhas de Phishing fossem investigadas. A justificativa atual para não abranger o Phishing no direito penal é que o envio de e-mails de Phishing ainda não é a materialização de um efeito nocivo – apenas a exploração da ação de um usuário em resposta a um e-mail de Phishing é considerada como tal. Esta materialização já está abrangida pelo direito penal convencional relativo à fraude. Uma rede criminosa que opere sistematicamente uma infraestrutura para phishing, no entanto, poderia ser processada no caso de uma legislação sobre phishing e poderia ter um efeito preventivo no que diz respeito à fraude on-line.

A Propriedade Intelectual é protegida pela lei convencional. No entanto, a lei não foi concebida especificamente no que diz respeito aos riscos on-line. Embora possa fornecer a base para a proteção e a ação penal para a maioria dos casos on-line, pode ser útil realizar uma análise específica, a fim de identificar potenciais casos on-line, que não são abrangidos pela legislação atual. Em particular, porque as partes interessadas não têm certeza se a legislação atual é suficiente para o ciberespaço.

Devido ao nível avançado da lei, o *Fator D4.2 Marcos Legislativos Relacionados*, este Fator pode ser avaliado como atendendo a todos os requisitos do Estágio Estabelecido e até mesmo alguns do Estágio Estratégico, com exceção dos pontos referentes à propriedade intelectual e à proteção do consumidor no ciberespaço. Além disso, as mudanças em curso na legislação com relação ao ambiente on-line refletem uma visão estratégica da legislação sobre crimes cibernéticos e da proteção legal contra riscos de segurança cibernética on-line no Brasil.

D4.3 COMPETÊNCIA E CAPACIDADE JURÍDICA E REGULATÓRIA

Este Factor estuda a capacidade da aplicação da lei para investigar crimes cibernéticos, a capacidade do Ministério Público para apresentar casos de crimes cibernéticos e provas electrónicas, e a capacidade do tribunal para presidir casos de crimes cibernéticos e aqueles que envolvem provas electrónicas. Finalmente, este Fator analisa a existência de órgãos reguladores intersetoriais para supervisionar o cumprimento de regulamentações específicas de segurança cibernética.

***Estágio*:** Formativo

A capacidade institucional no Brasil varia muito, dependendo do pessoal específico e do nível de administração. Embora o nível da Polícia Federal tenha capacidades adequadas de aplicação da lei, tal capacidade pode não estar presente nos níveis estadual e local. A distribuição de responsabilidade entre os níveis de polícia federal e estadual depende da gravidade e do impacto de um caso: Casos de grande porte e casos com conexão internacional (por exemplo, redes internacionais de crimes cibernéticos) são investigados pela Polícia Federal. Os casos menores são de responsabilidade da Polícia Civil em nível estadual. O Brasil não possui atualmente um centro de competência centralizado para casos de crimes cibernéticos, que também seria acessível à polícia em nível estadual; em vez disso, essa capacidade está integrada à Polícia Federal. A polícia em nível estatal também tem de investigar casos de crimes cibernéticos, mas não existe nenhum mecanismo entre os estados ou entre os níveis estadual e federal para garantir capacidades suficientes e intercâmbio de

conhecimentos. As partes interessadas indicaram que, na prática, presumivelmente, a colaboração acontece entre as unidades policiais estaduais e com a Polícia Federal. No entanto, essa colaboração deveria ser formalizada e um centro de competência para o intercâmbio de conhecimentos e experiências deveria ser estabelecido, o que também poderia fornecer capacidade investigativa, para estados que carecem de recursos suficientes em termos de pessoal ou infraestruturas. Embora as forças policiais possam ter capacidade suficiente em termos de conhecimento, muitas vezes carecem de pessoal suficiente para casos menores, incluindo o crime digital. Isto se aplica particularmente às unidades policiais estaduais. Embora a Polícia Federal ofereça capacitação aos seus policiais, a situação em nível estadual não é clara, uma vez que está sob a soberania dos respectivos estados. De acordo com as partes interessadas, o número de peritos na aplicação da lei permaneceu quase inalterado ao longo dos últimos 20 anos, o que é insuficiente para resolver todos os casos de cibercriminalidade. Além disso, devido à estrutura de carreira da polícia, o pessoal formado pode ser transferido para um domínio diferente e, assim, o conhecimento e a experiência podem ser perdidos. Conforme descrito, as disposições para o estabelecimento de uma cadeia de custódia digital estão bem estabelecidas.

No que diz respeito aos procuradores, as partes interessadas relataram que os recursos, competências e capacidades satisfazem as necessidades atuais; ou seja, os procuradores geralmente dispõem de recursos e conhecimentos suficientes para conduzir casos de crimes cibernéticos. No entanto, a situação parece ser diferente com os tribunais. As partes interessadas afirmaram que os tribunais parecem não ter juízes com formação suficiente para alguns casos de cibercriminalidade. Essa capacitação é realizada, se for o caso, ad hoc. Embora seja difícil melhorar esta situação, uma vez que os tribunais são independentes dos poderes legislativo e executivo do estado, o legislativo e o governo devem tentar encorajar os tribunais a aumentarem a sua experiência no que diz respeito ao cibercrime, por exemplo, assegurando o financiamento de cursos ou seminários para juízes.

De acordo com as partes interessadas, os organismos reguladores dispõem de um nível adequado de pessoal e possuem as competências e capacidades necessárias para abordar a segurança cibernética sob a sua responsabilidade.

No geral, especialmente as competências e capacidades de aplicação da lei devem ser mais fortemente coordenadas a nível federal e entre estados, a fim de atingir o nível estabelecido. Especialmente, devem ser abordadas questões de pessoal e formação, bem como mecanismos de colaboração em caso de carências entre estados e entre os níveis estadual e federal.

D4.4 MARCOS DE COOPERAÇÃO FORMAL E INFORMAL PARA COMBATER O CRIME CIBERNÉTICO

Este Fator *aborda a existência e a função de mecanismos formais e informais que permitem a cooperação entre intervenientes nacionais e transfronteiriços para dissuadir e combater o crime cibernético.*

***Estágio*:** Formativo para Estabelecido

Conforme indicado anteriormente, o Brasil assinou e ratificou a Convenção de Budapeste e já colaborou anteriormente internacional e regionalmente (com países latino-americanos e os EUA) em questões de crime cibernético. Recentemente, foi introduzida legislação para garantir a plena conformidade com os requisitos da Convenção de Budapeste.[86]Os esforços incluem a integração de uma capacidade 24 horas por dia, 7 dias por semana, permitindo que a polícia brasileira busque e responda a solicitações de assistência. Quando este processo é concluído, atinge-se o estágio Estabelecido em relação a estes indicadores. No entanto, como o processo está em curso, a fase estabelecida ainda não pode ser totalmente concedida.

As partes interessadas também indicaram que as colaborações público-privadas funcionam sem problemas e que o intercâmbio de informações entre o setor privado, os serviços de informações e as forças armadas está estabelecida e funciona bem. Contudo, esta afirmação não pôde ser confirmada através de fontes externas (por exemplo, do setor privado). O GSI atualmente atua como ponto de intercâmbio de informações entre as autoridades policiais, militares, de inteligência e o governo central/gabinete do presidente. Pode ser útil rever este acordo no que diz respeito a um potencial estabelecimento de uma agência dedicada à segurança cibernética a nível federal. A vontade de colaborar e trocar abertamente informações, especialmente por parte da indústria privada e de ONG, poderia ser ainda maior se o intercâmbio de informações fosse confiado a uma agência de segurança cibernética separada da comunidade de inteligência, militar e policial.

RECOMENDAÇÕES

Seguindo as informações apresentadas sobre a revisão da maturidade dos marcos jurídicos e regulatórios de segurança cibernética, o seguinte conjunto de recomendações é fornecido ao Brasil. Estas recomendações visam fornecer orientações e passos a seguir para fortalecer a capacidade de cibersegurança existente, seguindo as considerações do Modelo de Maturidade da Capacidade de Cibersegurança do GCSCC.

DISPOSIÇÕES JURÍDICAS E REGULATÓRIAS

R4.1.1 Considerar a possibilidade de implementar um requisito mais amplo de notificação obrigatória de incidentes de segurança cibernética, em particular para grandes empresas e CNI.

R4.1.2 Considerar a possiblidade de realizar uma avaliação sistemática do impacto nos direitos humanos da legislação sobre crimes cibernéticos, que vá além dos aspectos da privacidade e da proteção de dados.

[86] Isto já foi descrito no Fator D4.1 Disposições Legais e Regulamentares. Em particular, a introdução do LEI Nº 14.155 em maio de 2021 foi um passo importante para a conformidade.

MARCOS LEGISLATIVOS RELACIONADOS

R4.2.1 Considerar a adoção de mecanismos de adaptação às proteções legais com relação às tecnologias emergentes no que diz respeito à proteção de dados, proteção do consumidor, proteção da propriedade intelectual e proteção das crianças on-line.

R4.2.2 Considerar a inclusão de campanhas de phishing em grande escala no âmbito da lei penal e o estabelecimento de infraestruturas preparadas para campanhas de phishing em grande escala.

R4.2.3 Rever se a legislação (convencional) sobre propriedade intelectual que abrange aspectos específicos do ambiente on-line, como plataformas de streaming e intercâmbio de arquivos ou cópias digitais de propriedade intelectual.

COMPETÊNCIA E CAPACIDADE JURÍDICA E REGULATÓRIA

R4.3.1 Considerar a criação de um centro nacional para investigações policiais de casos de crimes digitais ou cibernéticos, que poderia funcionar como um centro de competência, intercâmbio de conhecimentos e último recurso em caso de limitações de recursos para a polícia a nível federal e a nível estadual. Em particular, a atual configuração de um centro de competências em segurança cibernética para investigações policiais a nível federal deverá ser acessível às unidades policiais em nível estadual. Os mecanismos de colaboração devem ser formalizados.

R4.3.2 Fornecer financiamento suficiente para o pessoal adequado de especialistas em aplicação da lei relacionada com o ciberespaço a nível federal e garantir que os estados forneçam financiamento e recursos humanos suficientes para construir uma capacidade adequada de aplicação da lei e competência no que diz respeito à aplicação da lei. Além disso, as disposições burocráticas da polícia estadual e federal deveriam ser revistas, a fim de reter especialistas com competências nos departamentos onde essas competências estão mais bem colocadas.

R4.3.3 Considerar a criação de formação para juízes e outros profissionais judiciais no que diz respeito ao cibercrime. Capacitações semelhantes também deveriam ser oferecidos para a profissão jurídica no Brasil em geral, seja por meio de uma entidade pública ou de uma entidade privada autorizada.

MARCOS DE COOPERAÇÃO FORMAL E INFORMAL PARA COMBATE AO CRIME CIBERNÉTICO

R4.4.1 Garantir que a revisão do cumprimento da Convenção de Budapeste seja concluída e que a legislação seja adaptada em conformidade, incluindo o estabelecimento de uma capacidade sólida, 24 horas por dia, 7 dias por semana, para intercâmbio com redes internacionais.

R4.4.2 Considerar atribuir a responsabilidade pelas relações formais entre o governo e os sistemas de justiça criminal, bem como pela troca de informações com o setor privado e público em geral, a uma (futura) agência nacional dedicada à segurança cibernética.

DIMENSÃO 5
PADRÕES E TECNOLOGIAS

Esta *Dimensão* aborda a utilização eficaz e generalizada da tecnologia de cibersegurança para proteger indivíduos, organizações e infraestruturas nacionais. A *Dimensão* examina especificamente a implementação de normas e boas práticas de segurança cibernética, a implementação de processos e controlos e o desenvolvimento de tecnologias e produtos, a fim de reduzir os riscos de segurança cibernética.

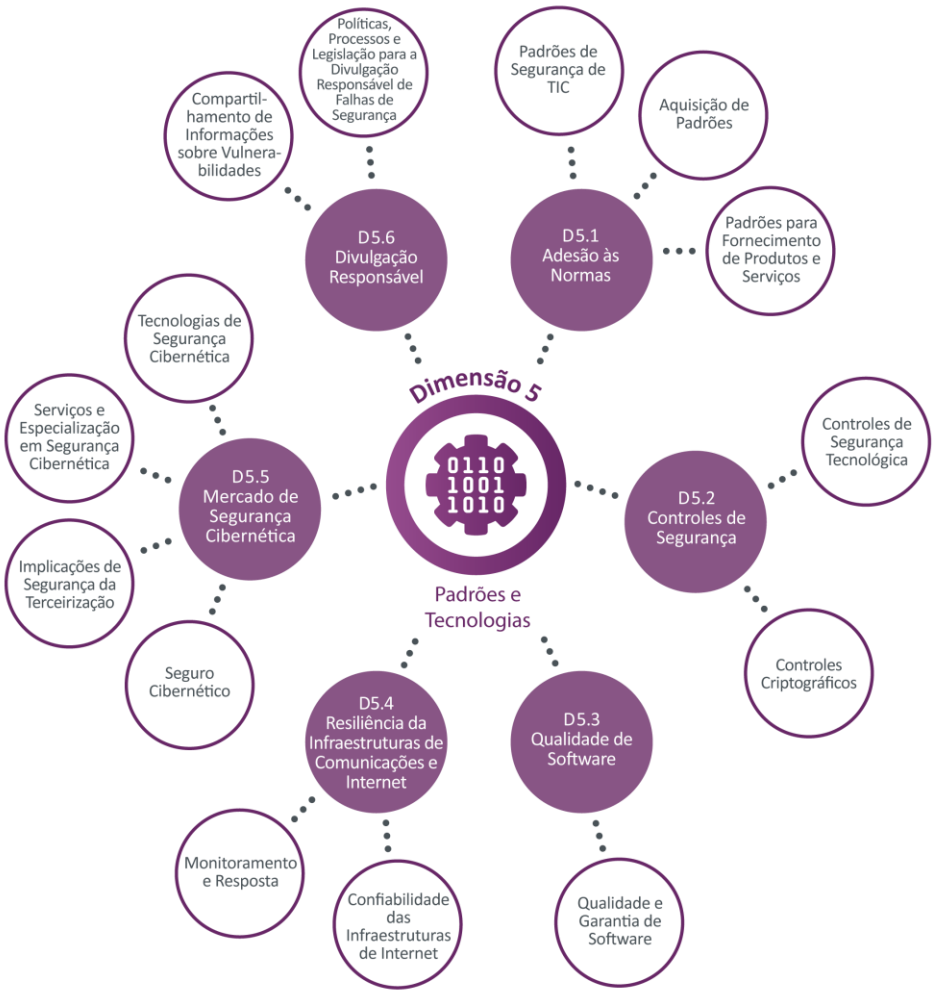
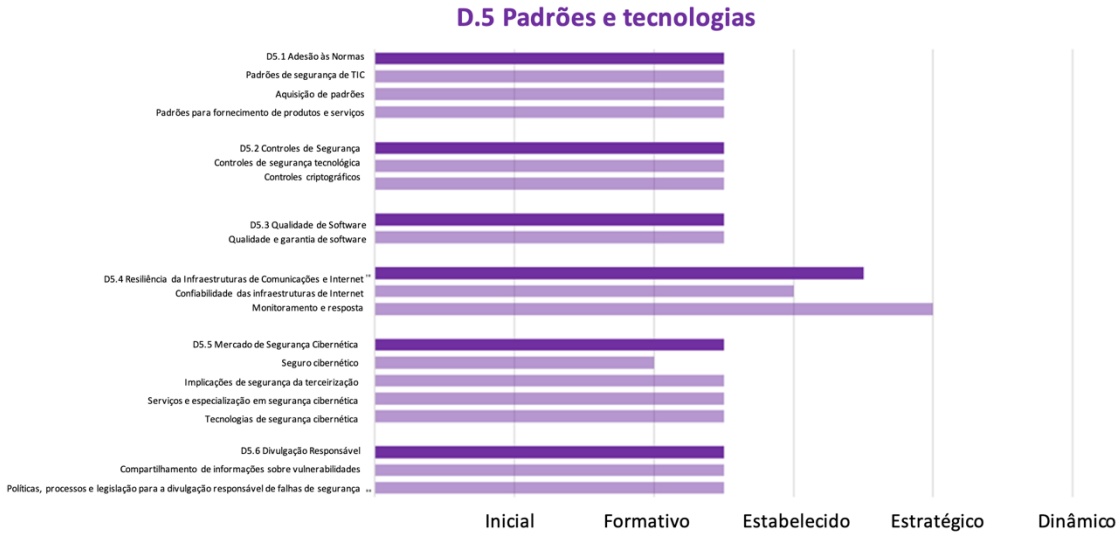


Figura 10: Fatores e aspectos examinados na Dimensão 5.

RESUMO DOS RESULTADOS



D5.1 ADESÃO AOS PADRÕES

Este Fator *analisa a capacidade do Governo para promover, avaliar a implementação e monitorar o cumprimento dos padrões e boas práticas internacionais de segurança cibernética.*

***Estágio*:** Formativo para Estabelecido

Ainda não foi identificada uma linha de base acordada a nível nacional de padrões e boas práticas relacionadas com a segurança cibernética para orientar as organizações nos setores público e privado. A NCS estabelece como ação estratégica (dentro da Ação Estratégica 2.3.1) melhorar a adoção de padrões internacionalmente reconhecidos pelos setores público e privado.

Vários padrões são seguidos em setores mais avançados e organizações maiores. Em vários setores, a adesão às normas de cibersegurança é impulsionada pela regulamentação. Para o PFA, são estabelecidos requisitos de normas de segurança cibernética e a implementação das normas é auditada; estes são amplamente baseados no conjunto de padrões de segurança cibernéticas da Organização Internacional para Padronização (ISO) 27000. Para os setores financeiro e de telecomunicações, as instituições são obrigadas a estabelecer a sua própria política de segurança cibernética baseada em padrões internacionais; Os regulamentos não são prescritivos sobre quais padrões devem ser usados. OS participantes afirmaram que os padrões internacionais mais comumente seguidos incluem o Marco de Segurança Cibernética (CSF) do Instituto Nacional de Padrões e Tecnologia (NIST); ISO 27001 e os controles críticos

de segurança do Centro de Segurança da Internet (CIS). Para o setor financeiro, isto também é impulsionado pelos requisitos das normas para operar no sistema financeiro internacional. Alguns participantes do setor financeiro observaram que poderia ser benéfico dispor de uma base mais específica que pudesse ser utilizada por diferentes setores e infraestruturas em termos de normas e controles técnicos e criptográficos.

Em outros setores, a implementação de normas de cibersegurança é mais ad hoc e não é supervisionada por uma autoridade, embora estejam disponíveis fontes de orientação. O departamento de Governo Digital publicou uma estrutura de 33 controles de segurança cibernética, adaptando os Controles Críticos de Segurança do CIS, para orientar as instituições governamentais digitais (das quais existem mais de 250). A rede acadêmica CERT (CAIS) trabalha com o setor acadêmico para orientar sobre padrões de segurança cibernética, baseados em padrões internacionais como a ISO 27001, que são adaptados para atender às realidades do setor. O CERT.br disponibiliza em seu site links para uma ampla gama de materiais de orientação sobre a implementação de controles técnicos e criptográficos de segurança, que podem ser acessados por qualquer organização.[87]O CERT.br também descreveu a colaboração com PSI para promover a adoção de padrões e melhores práticas de segurança cibernética.

Foram implementadas algumas medidas para apoiar as PME; em particular, recomendações ("Segurança da Informação para Pequenos Agentes de Processamento"[88]) são emitidas pela Autoridade Nacional de Proteção de Dados (ANPD) para ajudar PMEs que estão processando dados pessoais a atingir um nível mínimo de segurança para cumprir a Lei Geral de Proteção de Dados Pessoais (LGPD), incluindo orientações sobre senhas fortes e autenticação de dois fatores quando utilizem serviços em nuvem. As associações industriais relataram discussões em curso sobre como aumentar a maturidade da segurança cibernética das PME e produziram orientações para este público. Os participantes expressaram a opinião de que seria útil continuar trabalhando neste sentido, estabelecendo diretrizes mais amplas de segurança cibernética para que as pequenas empresas utilizem ao adotar controles técnicos e criptográficos.

Para promover a adoção consistente de padrões de segurança cibernética em organizações de todos os setores e níveis de maturidade, pode ser benéfico desenvolver uma linha de base acordada nacionalmente de padrões e boas práticas relacionadas à segurança cibernética, contra a qual organizações de setores públicos e privados possam, em alguns casos, serem auditadas e, em outros se autoavaliar. Como observaram os participantes, o conjunto de padrões de base teria de ter em conta os diversos contextos e os diferentes níveis de maturidade e recursos das organizações, e teria de complementar e interagir adequadamente com as diretrizes e regulamentos setoriais existentes. Foi expressa a opinião de que o desenvolvimento e a promoção de uma base de padrões nacionais de segurança cibernética poderia ser uma função da nova Agência Nacional de Segurança Cibernética (que, conforme descrito em D1, está em desenvolvimento).

Em termos de padrões de segurança cibernética e melhores práticas na orientação dos processos de aquisição, há novamente variações de acordo com a regulamentação e o nível das organizações. Como parte da regulamentação de segurança cibernética da PFA, os requisitos de segurança cibernética são impostos às instituições da PFA no que diz respeito à aquisição de hardware e software, gestão do ciclo de vida e utilização de serviços em nuvem.

[87]https://www.cert.br/links/

[88]https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf

A GSI estabeleceu em agosto de 2021 instruções normativas para agências da PFA sobre a aquisição de serviços em nuvem, incluindo requisitos de segurança.[89]O Banco Central (BACEN) também estabelece requisitos para o setor financeiro na contratação de serviços de processamento, armazenamento de dados e computação em nuvem, por meio da Resolução nº 4.658 de 2018.[90]

Em alguns outros setores e organizações menores, os requisitos para práticas de segurança cibernética nas aquisições não são definidos e a adesão aos padrões que orientam os aspectos relacionados à segurança cibernética dos processos de compra (incluindo gestão de riscos, gestão do ciclo de vida, garantia de software e hardware, terceirização e uso de serviços em nuvem) é ad hoc. Os setores, incluindo o da Eletricidade, notaram a necessidade de uma melhor gestão dos riscos da cadeia de abastecimento decorrentes da falta de práticas de segurança cibernética que orientem os processos de aquisição. Pode ser conveniente estabelecer e promover orientações nesta área que se estendam a um conjunto mais amplo de setores e tamanhos de organizações.

As principais atividades e metodologias para o desenvolvimento seguro e a gestão do ciclo de vida de software, hardware e prestação de serviços geridos e serviços em nuvem estão sendo identificadas e discutidas nas comunidades profissionais. Por exemplo, há alguma consideração estratégica dos requisitos de segurança cibernética dos softwares produzidos pelas empresas brasileiras. A Associação Brasileira das Empresas de Software (ABES) mantém diversos grupos de trabalho para discutir questões específicas relacionadas às empresas de software, incluindo grupos de trabalho sobre Segurança Cibernética e Proteção de Dados.[91]O grupo de trabalho de Segurança Cibernética tem como objetivo estabelecer um "*espaço de discussões internas e acompanhamento de regulamentações específicas, engajamento com os interessados, além de promover o intercâmbio e disseminação de informações entre os associados e os mais diversos segmentos da sociedade".*

Os participantes também relataram que empresas locais de nuvem trabalham com grandes empresas multinacionais de segurança cibernética para criar plataformas de nuvem seguras e robustas para oferecer aos clientes[92]; foi destacado um exemplo particular de um projeto desse tipo que visa melhorar a segurança cibernética, a disponibilidade e a qualidade dos serviços públicos municipais.[93]A Anatel estabelece requisitos para fornecedores de equipamentos para o setor de telecomunicações, que ainda não foram totalmente auditados, mas visam gerenciar o risco da cadeia de abastecimento.[94]

As normas para o desenvolvimento de software, garantia de qualidade de hardware, prestação de serviços geridos e segurança na nuvem ainda não estão a ser promovidas de forma consistente pelo governo aos fornecedores. A identificação e a promoção dos padrões relevantes ajudariam a promover uma adoção mais consistente de práticas de segurança pelos fornecedores.

[89] https://digitalpolicyalert.org/event/4032-normative-instructions-on-cloud-computing-services
[90] https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf
[91] https://abes.com.br/pt/servicos/comites-e-%20grupos-de-trabalho/
[92] https://www.loja.serpro.gov.br/pt/govshield
[93] https://portal.campinas.sp.gov.br/noticia/47964
[94] https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2021/1505-ato-77

D5.2 CONTROLES DE SEGURANÇA

Este Fator *analisa as evidências relativas à implementação de controles de segurança pelos usuários e pelos setores público e privado, e se o conjunto de controles tecnológicos de segurança cibernética se baseia em estruturas de segurança cibernética estabelecidas.*

***Estágio*:** Formativo para Estabelecido

Os controles de segurança tecnológica são implementados por organizações dos setores público e privado. Dada a variabilidade nos níveis de adoção de normas entre organizações (conforme descrito em D5.1), o nível de implementação destes controles varia significativamente entre diferentes setores e tamanhos de organização.

Dentro do PFA, para o qual existem requisitos obrigatórios e auditados de conformidade de segurança cibernética, a adoção e implementação de controles técnicos e criptográficos estão supostamente avançadas. Os avanços nos controles técnicos implementados também foram impulsionados pela criação da Lei Geral de Proteção de Dados Pessoais (LGPD), com mais instituições federais estabelecendo centros de operações de segurança (SOC) e fazendo uso de inteligência contra ameaças cibernéticas (CTI). Os participantes observaram que nos governos estaduais e municipais, onde a regulamentação da PFA não se aplica, a aplicação de controles técnicos é muito mais variável, dependendo das capacidades e recursos de segurança cibernética das instituições.

Outro exemplo avançado é o setor financeiro, onde a regulamentação do BACEN tem levado as instituições a criarem suas próprias políticas de segurança cibernética e a adotarem controles de segurança técnicos e criptográficos alinhados a elas. Embora a regulamentação do BACEN não prescreva os controles técnicos precisos que devem ser implementados, existem requisitos específicos para protocolos de segurança e criptografia usados pelas instituições participantes do sistema brasileiro de pagamentos e de intercâmbios financeiras.

Nos setores que não estão regulamentados para a implementação de normas de cibersegurança, existem, como seria de esperar, diferentes níveis de implementação de controles de segurança técnicos e criptográficos. Algumas das organizações mais avançadas adotam controles técnicos atualizados em conformidade com as normas internacionais, estabeleceram CERTs e SOCs, participam em redes de partilha de CTI e implementam protocolos de encriptação atualizados para dados em trânsito e em repouso. Alguns participantes expressaram a opinião de que muitas organizações do setor privado não estão implementando controles técnicos de segurança a um nível adequado para gerenciar riscos, com controles irregulares e manuais e processos ausentes ou raramente atualizados.

Os participantes relataram algumas preocupações sobre níveis mais baixos de adoção de controles técnicos e criptográficos apropriados pelas PME, que normalmente têm apenas recursos financeiros limitados para investir em segurança cibernética. Muitas PME dependem de serviços em nuvem e foram levantadas preocupações sobre a falta de conhecimento sobre como configurar e manter instâncias em nuvem com segurança, o que poderia levar à vulnerabilidade. Conforme descrito em D5.1.1, existem algumas iniciativas, incluindo as da Autoridade Nacional de Proteção de Dados, que podem servir de orientação para as PME, mas existe uma visão geral de que é necessário mais apoio às PME na área da implementação do

controle da segurança cibernética. As associações industriais também relataram discussões em curso sobre como aumentar a maturidade da segurança cibernética das PME (especialmente considerando que algumas PME prestam serviços a organizações maiores e podem apresentar vulnerabilidades a elas), além de terem realizado orientações e capacitação sobre requisitos mínimos de segurança voltados para esse público.

Os fornecedores de serviços de Internet, especialmente os de maior dimensão, oferecem uma gama de controlos técnicos de segurança aos seus clientes intermédios. Atualmente, estão sendo realizadas campanhas conjuntas entre o NIC.br, os principais fornecedores de telecomunicações e outras partes interessadas, para aumentar a adoção de controles anti-DDoS e anti-spoofing pelos PSI para proteger seus clientes finais. Alguns prestadores de serviços estão implementando ferramentas como o TLS para proteger as comunicações entre servidores e usuários, e o governo procura aumentar a adoção de certificados digitais e os protocolos de segurança permitidos.

O Brasil estabeleceu uma infraestrutura nacional de chave pública (KPI), ICP-Brasil, em 2001. O Instituto Nacional de Tecnologia da Informação (ITI) é a Autoridade Certificadora Raiz (CA), que certifica outras CAs e Autoridades de Registro (RAs) na cadeia. Há requisitos rigorosos para que as CAs Raiz e CAs que lidam com KPI no Brasil sejam certificadas. A NCS refere que os certificados digitais ainda não são amplamente utilizados nas empresas, "*devido a algumas dificuldades, como o elevado número de processos de emissão de certificados, o elevado custo para os cidadãos e o baixo número de unidades certificadoras por habitante*", e que o governo está buscando otimizar processos e expandir a oferta para permitir uma maior adoção.

O CERT.br estabeleceu recentemente uma ferramenta disponível ao público que permite às organizações testar a implementação de protocolos criptográficos como o TLS em seus serviços de Internet e sites. A ferramenta está sendo usada para avaliar a segurança de sites do governo.

D5.3 QUALIDADE DE SOFTWARE

Este Fator examina a qualidade da implantação de software e os requisitos funcionais nos setores público e privado. Além disso, este Fator analisa a existência e o aprimoramento de políticas e processos de atualização e manutenção de software com base em avaliações de risco e na natureza crítica dos serviços.

***Estágio*:** Formativo para Estabelecido

Atualmente não existe um catálogo de plataformas e aplicações de software seguras disponíveis para organizações dos setores público e privado, nem há orientações consistentes fornecidas a todas as organizações sobre o desenvolvimento e manutenção de software seguro.

Para a PFA, existe um inventário de software seguro, existem recomendações para o desenvolvimento seguro de software para uso do governo, e procedimentos de manutenção

de software, incluindo patches e KPIs para avaliar a eficácia da aplicação dos patches, de acordo com os regulamentos de segurança cibernética da PFA. O setor financeiro é obrigado a cumprir a regulamentação do BACEN sobre a segurança do software utilizado e sobre o gerenciamento seguro do ciclo de vida. No setor das telecomunicações, as disposições de auditoria da cadeia de abastecimento (que são descritas mais detalhadamente em D5.1) significam que os fornecedores de software para o setor devem ter políticas de segurança cibernética implementadas. Isso ainda não está totalmente regulamentado, mas pretende-se que a Anatel tenha competência para auditar fornecedores de software para serviços de telecomunicações. Observou-se que isto é de particular importância dada a tendência de incorporação de redes definidas por software (SDN) na infraestrutura de telecomunicações. Em outros setores como o elétrico, existem disposições que estabelecem que as empresas devem ter políticas de desenvolvimento e manutenção de software seguro. No entanto, esses critérios não são regulamentados.

Fora dos setores mais maduros descritos acima, a qualidade e a segurança do software são variáveis. Os participantes não tinham conhecimento das recomendações dadas pelo governo sobre o desenvolvimento de software seguro, a seleção de aplicações de software seguras ou a manutenção de software seguro, que se estenderiam às organizações do setor privado. Os participantes expressaram a opinião de que seria benéfica orientar todas as organizações sobre plataformas e aplicativos de software seguros, orientando todas as organizações no Brasil na seleção do software para uso. Além disso, orientações que se estendem a todas as organizações sobre processos seguros de desenvolvimento e manutenção de software podem ser benéficas.

D5.4 RESILIÊNCIA DA INFRAESTRUTURA DE COMUNICAÇÕES E INTERNET

Este Fator aborda a existência de serviços e infraestruturas de Internet confiáveis no país, bem como processos de segurança rigorosos nos setores público e privado. Além disso, isso Fator analisa o controle que o Governo pode ter sobre a sua infraestrutura de Internet e até que ponto as redes e sistemas são externalizados.

***Estágio*: Estabelecido para Estratégico**

No Brasil, serviços confiáveis de Internet estão amplamente disponíveis e são usados regularmente, inclusive para transações comerciais e de comércio eletrônico, e processos de autenticação adequados foram estabelecidos para a maioria das transações. Em geral, os participantes concordaram que existe um alto nível de resiliência da infraestrutura brasileira de internet e parece que nenhum evento no Brasil causou interrupções significativas neste tipo de serviço. Isso se deve em grande parte à estrutura descentralizada, já que há muitos Fornecedores de Serviços de Internet (ISPs) operando no Brasil, bem como a presença de muitos Pontos de Troca de Tráfego de Internet (IXPs).

Os serviços de Internet no Brasil são coordenados pelo Comitê Gestor da Internet no Brasil (CGI.br).), que "*é composto por membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica e, como tal, constitui um modelo único de governança da Internet para a participação efetiva da sociedade nas decisões que envolvem implementação, gestão*

e uso de redes".[95]As decisões do CGI.br são implementadas pelo Centro de Informação da Rede Brasileira, NIC.br.[96]Através destes órgãos, a infraestrutura nacional da Internet é gerenciada formalmente e a abordagem redundante e descentralizada é promovida.

Existem mais de 15.000 ISPs registrados no Brasil; um dos maiores mercados desse tipo no mundo.[97]Grandes operadoras, incluindo Claro, Telefônica e Oi, operam ao lado de uma ampla gama de provedores de menor porte. O sistema IX.br é o sistema IXP do Brasil, com 31 IXPs no Brasil em regiões metropolitanas, sob a gestão centralizada do CGI.br. A gestão inclui decisões estratégicas que foram tomadas sobre a necessidade de desenvolver mais IXPs para ajudar a criar resiliência. O NIC.br desempenha um papel ativo na manutenção do cenário dos IXP, financiando IXPs em áreas que ainda não têm condições de financiá-los.

O setor de telecomunicações é regulamentado em geral e para segurança cibernética pela Agência Nacional de Telecomunicações do Brasil, Anatel. A Anatel estabeleceu requisitos regulatórias por meio Resolução nº 740 de 2020 para as empresas de telecomunicações identificar os seus ativos, realizar testes regulares de vulnerabilidade, adotar normas e padrões nacionais ou internacionais de boas práticas em segurança cibernética e desenvolver um plano de gestão de riscos cibernéticos, uma política de formação em segurança cibernética e processos claros de resposta a incidentes. A Resolução estabelece requisitos para as tecnologias implantadas pelos prestadores de serviços de telecomunicações, afirmando que os prestadores devem utilizar, "*no âmbito das suas redes e serviços, produtos e equipamentos de telecomunicações de fornecedores que tenham uma política de cibersegurança compatível com os princípios e orientações estabelecidos no presente Regulamento e realizem processos periódicos de auditoria independente*". A Lei de Requisitos de Segurança Cibernética para Equipamentos de Telecomunicações (nº 77 de 2021) estabelece requisitos de segurança cibernética mais detalhados para equipamentos de telecomunicações, por meio dos quais os provedores podem submeter à Anatel a aprovação de seus equipamentos, a fim de serem autorizados a vender para provedores de telecomunicações brasileiros.[98]

A Anatel também publicou a Lei 2.346 (2023), que estabelece requisitos mínimos de segurança cibernética para fornecedores de equipamentos instalados no cliente (CPE, incluindo modems, roteadores, pontos de acesso), incluindo requisitos para senhas de fábrica e definidas pelo usuário, e outros controles, como criptografia controles para proteção de senhas e chaves de acesso.[99]O regulamento CPE entrará em vigor em março de 2024.

Os participantes relataram que os requisitos de segurança cibernética da Anatel ainda não são obrigatórios, mas pretendem ser. Estas regras aplicam-se, em teoria, a todos os operadores de telecomunicações. A Anatel observou que, na prática, com cerca de 1.500 ISPs no país, não é possível realizar auditorias para todas as operadoras. Como tal, não está claro que estas práticas – a gestão de tecnologias implementadas, avaliações de risco, monitorização de redes e testes de resiliência, e planos de resposta a incidentes – serão alcançadas de forma consistente em todos os fornecedores de infraestruturas de Internet.

---

[95] https://www.cgi.br/about/

[96] https://nic.br/about-nic-br/

[97]https://www.bnamericas.com/en/features/snapshot-brazils-3-largest-isps-and-their-capex-plans#:~:text=With%20over%2015%2C000%20registered%20internet,tal %20mercados%20em%20no%20mundo.

[98] https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2021/1505-ato-77

[99]https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqbjrZLCNfqeRg-L-C3Gb-1Azwysygy9rWoUM4rT_yI3XCuM z8 fweImNoyttQO8pA5ey8n7x_4PlmD_H2Fc85VrG

Entre os ISPs maiores há geralmente uma prática forte, orientada pela regulamentação da Anatel, com CERTs estabelecidos. Os participantes sentiram que pode haver atualmente lacunas em algumas destas capacidades, particularmente no que diz respeito aos ISPs de pequena e média dimensão. Ainda não existe uma supervisão completa das tecnologias utilizadas e adquiridas pelos fornecedores de infraestruturas de Internet, o que conduz a alguma penetração de fornecedores estrangeiros com potenciais problemas de segurança, ou de fornecedores com falta de maturidade em segurança, embora, como descrito, estejam sendo feitos progressos na gestão e aquisição controlada dessas tecnologias críticas.

Um panorama semelhante foi descrito para a presença de tecnologias de monitorização de segurança e planos de resposta a incidentes, com níveis variáveis de maturidade na vasta gama de fornecedores de infraestruturas de Internet. Dada a importância significativa dos fornecedores de pequena e médio porte para a manutenção de uma infraestrutura nacional de Internet resiliente, pode ser valioso considerar novas medidas para desenvolver práticas consistentes de segurança cibernética, tais como o desenvolvimento de diretrizes de segurança cibernética especializadas e mais básicas para PSI menores. Os participantes destacaram o apoio e orientação do grupo de operadoras de rede NIC.br, e a capacitação fornecida aos ISPs pelo NIC.br e CERT.br (que é mantido pelo NIC.br), e as parcerias de capacitação do NIC.br com os consultores que são frequentemente contratados para implementar tecnologias e processos de resposta para ISP menores.

Existem processos implementados para manter uma compreensão atualizada das ameaças à infraestrutura brasileira da Internet e para avaliar os riscos relacionados às tecnologias emergentes. Os participantes relataram que uma das principais missões do NIC.br é melhorar a segurança da Internet brasileira e aumentar a capacidade de tratamento de incidentes. O CERT.br conduz programas abrangentes para detectar e analisar ameaças e incidentes que ocorrem na Internet brasileira, usando honeypots e feeds rastreados relacionados a endereços IP brasileiros de parceiros internacionais. Os operadores de infraestrutura são notificados pelo CERT.br sobre ameaças e vulnerabilidades, juntamente com informações sobre como mitigá-las. Além disso, a Anatel mantém um grupo de trabalho com as principais operadoras de telecomunicações para se manter atualizado sobre a gestão de riscos de segurança cibernética, incluindo a análise de riscos relativos a desenvolvimentos tecnológicos mais recentes, como o 5G. Também foram estabelecidos requisitos mínimos de segurança cibernética para o estabelecimento de redes 5G, pela Instrução Normativa GSI nº 4 (2020).[100]

D5.5 MERCADO DE SEGURANÇA CIBERNÉTICA

Este Fator aborda a disponibilidade e o desenvolvimento de tecnologias competitivas de segurança cibernética, produtos de seguro cibernético, serviços e conhecimentos especializados em segurança cibernética e as implicações de segurança da terceirização.

***Estágio*:** Formativo para Estabelecido

[100]https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=27/03/2020&jornal=515&pagina=2

Em geral, os participantes concordaram que a maioria das tecnologias de segurança cibernética no Brasil são importadas do exterior, muitas vezes através de integradores nacionais. Embora exista alguma produção nacional de tecnologias de cibersegurança e o mercado interno pareça estar crescendo, os produtos de cibersegurança criados internamente não são atualmente os líderes de mercado. Observou-se a exceção das forças armadas, dos serviços de defesa e de inteligência, onde dão prioridade às tecnologias desenvolvidas internamente. A NCS estabelece como objetivo estratégico incentivar o desenvolvimento de soluções de segurança cibernética e de empresas emergentes brasileiras de segurança cibernética, e uma série de iniciativas para promover e financiar empresas emergentes de tecnologia existentes no Brasil.

Existe uma variabilidade no grau em que as organizações são atualmente capazes de identificar e gerenciar as implicações de segurança da dependência de tecnologias estrangeiras. Isto poderia criar riscos no contexto de uma cadeia de abastecimento internacional. Conforme observado nos Fatores anteriores do D5, os requisitos e práticas de segurança cibernética entre setores e organizações ou portes diferentes; alguns reguladores, por exemplo no setor das telecomunicações, impõem requisitos aos fornecedores de tecnologias para o seu setor. Estas ainda não foram totalmente implementadas e, neste setor de exemplo, alguns participantes expressaram preocupações sobre os perigos potenciais da dependência de tecnologias estrangeiras por parte dos provedores de telecomunicações brasileiros.

Existem amplos serviços de consultoria em segurança cibernética disponíveis para organizações públicas e privadas no Brasil. Os participantes descreveram um mercado ativo, com muitas empresas nacionais e grandes empresas internacionais oferecendo serviços de consultoria. O mercado é percebido como muito ativo no fornecimento de serviços de Centro de Operações de Segurança (SOC), CSIRT como serviço e serviços locais de Inteligência de Ameaças Cibernéticas (CTI) de alta qualidade. Os participantes também relataram que as competências brasileiras em segurança cibernética são exportadas internacionalmente à medida que os serviços de consultoria brasileiros são contratados no exterior. As partes interessadas de organizações que contratam consultores de segurança cibernética descreveram que recebem um elevado nível de concorrência de alta qualidade em resposta às suas propostas. Os fornecedores geralmente fornecem detalhes das certificações profissionais que possuem.

Os participantes também relataram que, para uma série de setores, um conceito de segurança como serviço é oferecido pela autoridade do setor (por vezes através dos seus parceiros comerciais). Por exemplo, o CAIS (para a rede académica), o departamento de Governo Digital (para instituições governamentais digitais) e o Departamento de Defesa oferecem serviços como CSIRT, intercâmbio CTI, análise de vulnerabilidades e testes de penetração.

Organizações maiores descreveram os processos de licitação que realizam para selecionar prestadores de serviços de segurança cibernética, que incluem a verificação de credenciamentos, experiência, habilidades técnicas e padrões de segurança cibernética seguidos (por exemplo, ISO 27001). Os participantes observaram que a consideração de tais fatores pelas organizações na contratação de um fornecedor de serviços de segurança cibernética varia dependendo da sua maturidade e apetite ao risco. Atualmente não existe acreditação de fornecedores de serviços de segurança cibernética por um organismo nacional. Isto pode ser valioso para orientar as organizações na seleção de fornecedores de serviços confiáveis e seguros, especialmente para organizações com experiência limitada em

segurança cibernética, informando as suas decisões. Os participantes também expressaram a opinião de que a oportunidade de obter tal acreditação poderia beneficiar os fornecedores de serviços.

Foi expressa a opinião de que a acreditação de empresas que fornecem produtos e serviços em segurança cibernética poderia ser um papel que a Agência Nacional de Segurança Cibernética (que, conforme descrito em D1, está em desenvolvimento) poderia assumir. Outra abordagem potencial recomendada pelos participantes foi um modelo de autorregulação, no qual as grandes empresas podem avaliar as pequenas empresas que lhes prestam serviços de cibersegurança e emitir sinais de aprovação, que os fornecedores utilizam como reconhecimento.

Os participantes observaram o défice de mão-de-obra em cibersegurança (que é discutido mais detalhadamente em D3, observando que este é um problema mundial), o que aumenta o custo de contratação de consultores de cibersegurança. Foram expressas opiniões de que a capacidade nesta área precisa de continuar a aumentar, a fim de satisfazer a demanda crescente por serviços de segurança cibernética.

Há um uso generalizado de serviços em nuvem pelas organizações brasileiras. Algumas organizações realizam avaliações de risco para determinar como mitigar os riscos de terceirização de TI para terceiros ou serviços em nuvem; em particular, as organizações maiores tendem a ter requisitos de segurança implementado quando adquirem serviços, incluindo nuvem. Conforme descrito nas Secções 5.1 e 5.2, o nível de maturidade da segurança cibernética varia entre setores e organizações de diferentes tamanhos, e isto também tem impacto na capacidade das organizações de gerir riscos de segurança cibernética quando subcontratam.

Para alguns setores, a gestão das implicações de segurança da terceirização é impulsionada pela regulamentação. A GSI estabeleceu em agosto de 2021 instruções normativas para agências da PFA sobre a aquisição de serviços em nuvem, incluindo requisitos de segurança cibernética e privacidade de dados.[101]O Banco Central (BACEN) também estabelece exigências para o setor financeiro na contratação de serviços de processamento, armazenamento de dados e computação em nuvem, por meio da Resolução nº 4.658 de 2018.[102]O departamento de Governo Digital, um ponto central de contacto para mais de 250 instituições de governo digital, criou modelos para a aquisição de serviços em nuvem. Supostamente, nos próximos meses, as instituições terão acesso a este modelo adicional para validar requisitos e apoiar processos de licitação.

Foram destacadas questões potenciais para as PME, uma vez que muitas delas dependem de serviços em nuvem para serviços de TI e de segurança cibernética. Os participantes descreveram a falta de compreensão de como usar a nuvem com segurança em organizações que não possuem uma equipe dedicada de TI ou de segurança cibernética. Isso produz erros de configuração ou falhas de atualização, gerando uma vulnerabilidade. Poderia ser benéfico estender a sensibilização ou formação mais substancial às PME para a utilização segura da nuvem e avaliação de riscos, ou emitir orientações específicas sobre segurança na nuvem

[101] https://digitalpolicyalert.org/event/4032-normative-instructions-on-cloud-computing-services
[102] https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf

adequadas para organizações que tenham capacidades e recursos de segurança cibernética mais baixos.

As empresas locais que fornecem serviços em nuvem relataram oferecer diretrizes e salvaguardas para ajudar a orientar os clientes na adoção segura de serviços em nuvem. Por exemplo, em alguns casos, empresas locais que atuam como intermediárias para vários outros serviços em nuvem realizam a gestão de riscos para esses provedores, salvaguardando os seus clientes.

O mercado de seguros cibernéticos no Brasil está em seus estágios iniciais. A maioria das ofertas de produtos de ciberseguro, foi relatado, é feita por companhias de seguros multinacionais, com os participantes cientes de que poucas empresas locais oferecem produtos de ciberseguro. Alguns dos produtos internacionais oferecidos especificam condições (por exemplo, requisitos de controle de segurança cibernética) que as organizações devem cumprir para serem seguráveis.

Muitos participantes na análise conheciam os produtos de seguro cibernético, mas estes ainda não tinham sido adoptados pelas suas organizações. Até recentemente, a adesão às ofertas de seguros cibernéticos tem sido feita principalmente por grandes empresas multinacionais, mas a procura por parte das organizações brasileiras está supostamente começando a crescer. A necessidade de produtos específicos de seguro cibernético foi reconhecida e os participantes relataram que o seguro de continuidade de negócios no Brasil não tenderia a cobrir incidentes cibernéticos.

Foi levantada a questão da acessibilidade dos produtos de seguro cibernético oferecidos atualmente, impedindo que algumas organizações adotassem apólices de seguro cibernético. Não houve evidências de que fossem oferecidos produtos de ciberseguro adequados para pequenas e médias empresas. Embora tenham sido relatadas algumas discussões em grupos de trabalho sobre a acessibilidade das ofertas de seguros cibernéticos, também não está claro se as necessidades do mercado de seguros cibernéticos ainda foram estrategicamente identificadas. Identificar as necessidades das organizações no Brasil nesta área por meio da avaliação dos riscos financeiros para os setores público e privado, bem como dos desafios relacionados aos custos, seria benéfico para informar o desenvolvimento do mercado de seguros cibernéticos.

D5.6 DIVULGAÇÃO RESPONSÁVEL

***Estágio*:** Formativo para Estabelecido

Este Fator explora o estabelecimento de um marco de divulgação responsável para a recepção e divulgação de informações sobre vulnerabilidade entre setores, e se existe capacidade suficiente para rever e atualizar continuamente este marco.

A presença de uma política ou marco de divulgação responsável varia entre as organizações. Existe um marco de divulgação de vulnerabilidades para o governo federal, que permite aos pesquisadores que encontram vulnerabilidades em sites do governo reportá-las. A Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) apoia o intercâmbio de informações sobre ameaças e vulnerabilidades entre instituições da PFA (e a participação de todas as instituições da PFA é obrigatória), com outras organizações capazes de aderir de forma voluntária. O CTIR.gov publica alertas sobre vulnerabilidades e ameaças à PFA em seu site, apoiado na consulta de fontes como o CERT.br e nas bases de dados de vulnerabilidades relativas aos principais fornecedores de soluções de TI.[103]

Fora do governo, os participantes relataram que as empresas maiores e mais avançadas tendem a ter os seus próprios canais e marcos para uma divulgação responsável. Esses marcos incluem políticas de divulgação e diretrizes claras sobre o processo e o cronograma para resolução. Algumas dessas empresas mais avançadas executam programas de recompensa por erros; foram citados exemplos específicos no setor financeiro. Algumas outras empresas utilizam um proxy CERT para receber notificações de vulnerabilidades em sua infraestrutura e fornecer feedback para pesquisadores brasileiros e estrangeiros. Os participantes observaram que, como geralmente acontece em todo o mundo, às vezes a resposta e a resolução por parte de uma empresa que foi notificada sobre uma vulnerabilidade podem não ser imediatas; isso depende da natureza da vulnerabilidade e da maturidade da empresa.

O CERT.br desempenha um papel significativo na disseminação de informações sobre vulnerabilidades e inteligência de ameaças para suas organizações clientes (que, conforme descrito em D1.2, podem incluir voluntariamente qualquer organização no Brasil) por meio de canais formais. As informações de vulnerabilidade são coletadas por meio de sensores, informações de vulnerabilidade e ameaças compartilhadas pelas organizações e CERTs com as quais trabalham e parcerias internacionais, publicadas no portal CERT.br,[104]e disseminado para vários grupos de intercâmbio de informações por meio de plataformas MISP.

Outros CERTs descreveram desempenhar um papel semelhante; Por exemplo, o CAIS, o CERT da rede académica, recebe e divulga informações sobre vulnerabilidades das suas partes interessadas e também cria alertas sobre novas vulnerabilidades listadas na plataforma

[103] https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2023
[104] https://stats.cert.br/

internacional Vulnerabilidades e Exposições Comuns (CVEs) que são distribuídas às suas partes interessadas. Em vários outros setores, existem mecanismos para intercâmbio de informações sobre vulnerabilidades: para o setor de telecomunicações, grupos de trabalho estabelecidos pela Anatel permitem que as operadoras compartilhem informações sobre ameaças e vulnerabilidades usando plataformas MISP; também existem grupos de confiança que partilham informações sobre ameaças e vulnerabilidades através de plataformas MISP nos setores financeiro e de petróleo e gás, por exemplo.

Não existem proteções legais específicas para as partes que divulgam falhas de segurança de forma responsável. Os participantes descreveram uma cultura geral das empresas mais maduras, que administram seus próprios canais de divulgação ou recebem divulgações por meio de um CERT, compreendendo os benefícios da divulgação responsável e acolhendo a divulgação responsável de vulnerabilidades, e abstendo-se de tentar ações legais contra uma parte que divulga informações de forma responsável. Embora há quinze anos, as empresas poderiam ter-se sentido ameaçadas e desafiada por investigadores que lhes revelavam tais informações, hoje as empresas maiores tendem a ver estes investigadores como aliados.

Algumas empresas menos maduras, no entanto, podem ainda não compreender os benefícios da divulgação responsável. A fim de encorajar uma gama mais ampla de organizações a introduzir políticas, canais e abordagens de resolução de divulgação responsável, e programas de recompensa por erros, percebeu-se que a conscientização sobre a divulgação responsável (e como ela é diferente de ataques genuínos e extorsão) seria ser benéfico.

RECOMENDAÇÕES

Seguindo as informações apresentadas sobre a revisão da maturidade dos Padrões e Tecnologias de segurança cibernética, o seguinte conjunto de recomendações é fornecido ao Brasil. Estas recomendações visam fornecer orientações e passos a seguir para fortalecer a capacidade de segurança cibernética existente, seguindo as considerações do Modelo de Maturidade da Capacidade de Cibersegurança do GCSCC.

ADESÃO AOS PADRÕES

R5.1.1 Desenvolver uma base de padrões e boas práticas de segurança cibernética acordada a nível nacional, contra a qual as organizações dos setores público e privado possam autoavaliar-se. Os padrões de base precisarão levar em conta diversos contextos e diferentes capacidades e níveis de recursos de segurança cibernética das organizações, e precisarão complementar e interagir adequadamente com os regulamentos de CI existentes e futuros (que são descritos mais detalhadamente em D1.3). Além dos padrões de segurança das TIC, a linha de base deve incluir:

- padrões e melhores práticas de segurança cibernética que orientam os processos de aquisição (incluindo gestão de riscos, gestão do ciclo de vida, garantia de software e hardware, terceirização e uso de serviços em nuvem).

- padrões de segurança cibernética para o fornecimento de produtos e serviços (incluindo desenvolvimento de software, garantia de qualidade de hardware, fornecimento de serviços gerenciados e segurança em nuvem).

R5.1.2 Considerar emitir orientações para organizações de pequena e média porte sobre como implementar um nível mais básico de controles de segurança cibernética que seja alcançável com recursos financeiros e de pessoal mais limitados. O esquema Cyber Essentials do Reino Unido pode ser um exemplo útil.

R5.1.3 Atribuir a uma entidade a responsabilidade de medir (por exemplo, coletar e analisar estatísticas sobre) a utilização de padrões de segurança cibernética nos setores público e privado.

R5.1.4 Estabelecer programas governamentais para promover a adesão aos padrões identificados em todas as organizações no Brasil. Use informações sobre adoção (gerados por meio do R5.1.3) para identificar e promover a conscientização em grupos de organizações com níveis mais baixos de adoção.

CONTROLES DE SEGURANÇA

R5.2.1 Promover o uso de padrões de segurança cibernética em organizações públicas e privadas no Brasil, para que os conjuntos de controle tecnológico de segurança cibernética usados pelas organizações reflitam consistentemente marcos, padrões e boas práticas de segurança cibernética estabelecidos.

R5.2.2 Emitir orientação ou apoio às PME para aumentar a sua conscientização sobre como adotar serviços em nuvem com segurança.

R5.2.3 Considerar como aumentar o uso de certificados digitais pelas organizações no Brasil. Isto pode incluir a realização de campanhas de concientização ou a implementação de medidas de fatores práticos proibitivos.

R5.2.4 Promover o uso de ferramentas para testar a implementação de protocolos criptográficos, como a ferramenta disponibilizada ao público pelo CERT.br.

QUALIDADE DE SOFTWARE

R5.3.1 Emitir orientações para todas as organizações sobre como identificar plataformas e aplicativos de software seguros e confiáveis. Isto pode assumir a forma de um catálogo de software garantido ou de orientação sobre como avaliar a qualidade do software, requisitos funcionais e de segurança.

R5.3.2 Emitir orientações para todas as organizações sobre atualizações e manutenção de software (incluindo gerenciamento de patches).

R5.3.3 Desenvolver uma estrutura para medir a segurança do software e a aplicação de políticas de manutenção de software em todos as organizações (por exemplo, coleta e análise de estatísticas).

R5.3.4 Designar um órgão responsável por coletar evidências de segurança e deficiências de software e caracterizar aplicativos de software quanto à sua confiabilidade, usabilidade, desempenho e segurança em conformidade com padrões e boas práticas internacionais. As informações coletadas podem ser utilizadas para orientar organizações no Brasil.

RESILIÊNCIA DA INFRAESTRUTURA DE COMUNICAÇÕES E INTERNET

R5.4.1 Identificar (por exemplo, por meio de consultas com partes interessadas do setor de telecomunicações) como manter a supervisão das práticas de segurança cibernética e da aquisição de tecnologias no grande número de ISPs no Brasil. Considere se a implementação de abordagens automatizadas para relatórios e análise de práticas pode ser benéfica.

R5.4.2 Dada a importância dos ISP de pequena e médio porte para a manutenção de uma infraestrutura nacional de Internet resiliente, considerar novas medidas para desenvolver práticas consistentes de cibersegurança, tais como o desenvolvimento de diretrizes de cibersegurança especializadas e mais básicas para ISP de menor dimensão

R5.4.3 Garantir que a regulamentação da Anatel seja mantida atualizada por meio de avaliações regulares dos impactos das tecnologias emergentes, dos riscos para o setor de telecomunicações e de processos para conformidade com padrões internacionais.

MERCADO DE SEGURANÇA CIBERNÉTICA

R5.5.1 É aconselhável que as partes interessadas relevantes considerem as implicações de segurança da utilização de tecnologias estrangeiras de cibersegurança e considerem se são necessárias quaisquer ações para mitigar riscos potenciais.

R5.5.2 Emitir e promover orientações para organizações no Brasil sobre como identificar e gerenciar as implicações de segurança da dependência de tecnologias estrangeiras.

R5.5.3 Ao promover o crescimento do mercado nacional de tecnologia de segurança cibernética, garantir que os processos de desenvolvimento seguros sejam promovidos, de acordo com padrões internacionalmente aceitos.

R5.5.4 Analisar a oferta e a demanda por fornecedores de serviços de segurança cibernética para empresas brasileiras, para garantir que a oferta atenda à demanda continuamente crescente.

R5.5.5 Criar uma abordagem para credenciar prestadores de serviços de segurança cibernética. A acreditação pode vir de um órgão central (como a nova agência nacional de segurança cibernética), ou pode seguir um modelo de autorregulação, conforme sugerido pelos participantes, em que as empresas maiores podem avaliar as empresas menores que lhes prestam serviços de segurança cibernética e emitir selos de aprovação, que os provedores usam como reconhecimento.

R5.5.6 Ampliar ofertas de conscientização ou capacitação para PMEs sobre o uso seguro da nuvem e avaliação dos riscos associados ou emitir diretrizes de segurança na nuvem adequadas para organizações que tenham menor capacidade e recursos de segurança cibernética.

R5.5.7 Identificar as necessidades das organizações no Brasil por meio de consultas para avaliar os riscos financeiros para os setores público e privado, bem como os desafios relacionados aos custos, para informar o desenvolvimento do mercado de seguros cibernéticos.

DIVULGAÇÃO RESPONSÁVEL

R5.6.1 Realizar ações de sensibilização para as organizações sobre a divulgação responsável de vulnerabilidades (e como esta é diferente de ataques genuínos e extorsão), a fim de aumentar a sensibilização e garantir a compreensão dos benefícios da divulgação responsável.

R5.6.2 Promover o desenvolvimento de políticas, canais e abordagens de resolução de divulgação responsável, além de programas de recompensa por erros entre uma gama mais ampla de organizações brasileiras. Isto pode ser apoiado por uma maior conscientização, conforme recomendado em R5.6.1.

R5.6.2 Considerar implementar proteções legais específicas para as partes que divulgam falhas de segurança de forma responsável.

REFLEXÕES ADICIONAIS

O nível de envolvimento das partes interessadas na revisão foi bom e a representação e composição dos grupos de partes interessadas foi, em geral, equilibrada e ampla. Isto permitiu à equipe de revisão recolher evidências abrangentes para apoiar esta revisão do CMM.

APÊNDICES

METODOLOGIA - MEDINDO MATURIDADE

A implementação do CMM envolve a coleta de dados através de consultas às partes interessadas no país (normalmente ao longo de três dias) e remotamente através de pesquisa documental. Foi concebido para produzir um relatório baseado em evidências que será submetido aos representantes governamentais do país em estudo e incluirá recomendações para:

- comparar a maturidade da capacidade de segurança cibernética de um país;
- fornecer um conjunto detalhado de ações pragmáticas para contribuir para o avanço da capacidade de segurança cibernética;
- identificar lacunas de maturidade; e
- identificar prioridades para investimento e capacitação futura.

Durante a revisão de um país, dimensões específicas são discutidas com grupos relevantes de partes interessadas. A cada grupo de partes interessadas é solicitado responder a uma ou duas dimensões do CMM, dependendo da sua experiência. Por exemplo, os grupos acadêmicos, da sociedade civil e de governança da Internet seriam todos convidados a discutir a Dimensão 2 "Cultura e Sociedade de Segurança Cibernética" e a Dimensão 3 "Construindo Conhecimentos e Capacidades de Segurança Cibernética" do CMM.

Coleta de dados

A Equipe de Revisão reúne as evidências necessárias para identificar os estágios de maturidade em todo o CMM por meio de pesquisa documental, entrevistas aprofundadas e discussões de grupos focais modificados, utilizando a ferramenta de codificação de campo estruturado (SFC) da CMM para capturar os resultados. As funções da Equipe de Revisão incluem a de facilitador para liderar as sessões de grupo e um responsável por anotações.

O CMM utiliza uma **metodologia modificada de discussão de grupos focais** que extrai dados que complementam e ajudam a validar entrevistas aprofundadas e pesquisas documentais.[105]Tal como acontece com as entrevistas, as discussões em grupos focais são uma metodologia interativa com a vantagem de que, durante o processo de coleta de dados, podem surgir diversos pontos de vista e concepções à medida que os participantes acompanham a discussão. Em vez de colocar questões a participantes específicos, os investigadores facilitam uma discussão entre os participantes, encorajando-os a adotar,

[105] Willians, M. (2003). Questionnaire design. In *Making sense of social research* (págs. 104-123). Publicações SAGE, Ltd, https://www.doi.org/10.4135/9781849209434; Knodel, J. (1993). The design and analysis of focus group studies: a practical approach. In Morgan, D. L. (Ed.), *Successful focus groups: Advancing the state of the art*. Em Morgan, DL (Ed.), *Grupos focais de sucesso: Avançando o estado da arte*(págs. 35-50). Publicações SAGE, Inc., https://www.doi.org/10.4135/9781483349008; Richard A. Krueger, RA, e Mary Anne Casey, MA, (2009) Focus-groups: A Practical Guide for Applied Research. Publicações SAGE, Londres.

defender ou explicar diferentes perspectivas.[106]É esta interação que oferece vantagens em relação a outras metodologias, permitindo aos participantes o entendimento mútuo e a sensibilização de todos para as práticas e capacidades de cibersegurança.[107]Durante as revisões do CMM, a Equipe de Revisão conduz a discussão para abordar todos os aspectos dentro das dimensões relevantes.

Para determinar o nível de maturidade da capacidade de segurança cibernética, cada *Aspecto* possui um conjunto de indicadores correspondentes a todos os cinco estágios de maturidade. O método de consenso é usado para conduzir as discussões dentro das sessões, por exemplo, para que as partes interessadas forneçam evidências sobre quantos indicadores foram implementados pelo país e determinem o nível de maturidade de cada aspecto do modelo. Durante as discussões em grupos focais, os pesquisadores usam perguntas semiestruturadas para manter as discussões em torno de indicadores relevantes. A discussão entre as partes interessadas fornece evidências sobre a implementação de indicadores. Ao avaliar o nível de maturidade, se não houver provas de que todos os indicadores foram cumpridos numa determinada fase, então esse país ainda não atingiu essa fase de maturidade.

Inconsistências entre as partes interessadas ocorrerão inevitavelmente. Da mesma forma, a informação conhecida por uma parte interessada num setor pode não ser familiar noutros setores. Consequentemente, a Equipe de Revisão não conseguirá perceber estas lacunas de informação e depois investigá-las.

A pesquisa documental e os grupos focais modificados levantam inevitavelmente algumas questões adicionais e possíveis inconsistências. Por esta razão, e para obter uma compreensão mais aprofundada das principais e por vezes únicas políticas e práticas, é também realizado um conjunto de entrevistas aprofundadas durante e em algumas ocasiões após a pesquisa de campo.

Análise de dados

Com o consentimento prévio dos participantes, todas as sessões são gravadas. As respostas individuais são tratadas como confidenciais de acordo com a Regra da Chatham House aplicada na comunicação dos nossos resultados.[108] Após a realização de uma revisão do país, **os dados coletados durante as consultas** com as partes interessadas e as notas tomadas durante as sessões são usados para encontrar evidências e **definir os estágios de maturidade** para cada *Aspecto* do CMM. O relatório do CMM agrega essas informações e determina o a maturidade de cada Fator do CMM.

Durante a revisão, é realizada uma investigação documental adicional para preencher quaisquer lacunas que surjam durante o processo de coleta de dados no país e para validar as provas fornecidas. Na elaboração do **relatório CMM**, muitas vezes são necessárias mais pesquisas documentais e entrevistas para abordar qualquer informação ausente para validar e verificar os resultados. Por exemplo, as partes interessadas podem nem sempre estar cientes dos desenvolvimentos recentes no seu país, ou se o país assinou uma convenção

[106] Kitzinger, J. (1994). The methodology of focus groups: the importance of interaction between research participants. Sociology of health & illness, 16(1), 103-121. https://doi.org/10.1111/1467-9566.ep11347023; Kitzinger, J. (1995). Qualitative research: introducing focus groups. Bmj, 311(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299; Fern, EF (1982). 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, 19(1), 1–13. https://doi.org/10.1177/002224378201900101

[107] Kitzinger, J. (1995). Qualitative research: introducing focus groups. B*mj*, 311(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299

[108] https://www.chathamhouse.org/about/chatham-house-rule

específica sobre política de proteção de dados pessoais. Portanto, sites oficiais de governos ou ministérios, relatórios anuais de organizações internacionais, sites de universidades, entrevistas em profundidade etc. podem ser usados como fontes complementares de informação. Este tipo de investigação adicional ajuda a garantir que o relatório reflete com precisão a capacidade de segurança cibernética do país anfitrião. Em cada caso, a equipe não privilegia nenhuma fonte específica de informação, mas procura chegar a um consenso sobre o estatuto mais válido de cada indicador do modelo.

Desenvolvendo recomendações

Para cada *Dimensão*, são fornecidas **recomendações** sobre os próximos passos a tomar para que o país melhore a sua capacidade de segurança cibernética. Se a capacidade de um país para um determinado *Aspecto* estiver, por exemplo, numa fase formativa de maturidade, então, olhando para o CMM, os indicadores que ajudarão o país a passar para a fase seguinte podem ser facilmente identificados. As recomendações também podem surgir de discussões com e entre as partes interessadas. As recomendações fornecem conselhos e medidas destinadas a aumentar a capacidade existente de segurança cibernética de acordo com as considerações do CMM. As recomendações são fornecidas especificamente para cada *Fator*.

Após uma revisão pelo Conselho Técnico do GCSCC, o relatório preliminar é submetido ao Anfitrião Local para feedback seguro. Se surgirem novas evidências, o relatório preliminar será revisado e os estágios de maturidade de cada *Aspecto e Fator* no CMM serão atualizados correspondentemente. Assim que todas as partes aprovarem o relatório preliminar, o anfitrião local assumirá a liderança no processo de publicação. A aprovação da publicação é reponsabilidade do país anfitrião e, se isso for acordado, o anfitrião local é incentivado a publicá-la através de um portal oficial do governo ou outro meio de comunicação.

Gerenciamento de dados e considerações éticas

As discussões em grupos focais são conduzidas online nas plataformas Microsoft Teams™ e Zoom™. (*dependendo das plataformas preferidas por cada nação*) As discussões são gravadas em gravadores externos para garantir a confidencialidade dos dados e informações coletadas, e para transcrição futura para fins de redação do relatório do CMM. As gravações permanecem anônimas. As conclusões do estudo documental, entrevistas aprofundadas e discussões em grupos focais são consolidadas durante a análise.

Centro Global de Capacidade de Segurança Cibernética

Departamento de Ciência da Computação, Universidade de Oxford

Edifício Wolfson, Oxford OX1 3QD,

Reino Unido

Tel: +44 (0)1865 287434

E-mail: cibercapacidade@cs.ox.ac.uk

Sites: https://gcscc.ox.ac.uk/home-page#/ www.oxfordmartin.ox.ac.uk/cyber-security

Patrocinado por

UK Government