CYBERSECURITY CAPACITY REVIEW

Brazil

August 2023

Global Cyber Security Capacity Centre

TABLE OF CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: Dr Marcel Stolz, Dr Louise Axon

Reviewed by: Professor Sadie Creese, Professor William Dutton, Professor Michael Goldsmith, Dr Jamie Saunders, Professor David Wall, Professor Basie Von Solms, Carolin Weisser Harris

Approved by: Professor Michael Goldsmith

Version	*Date*	*Notes*
1	*23/10/2023*	*First draft by lead researchers submitted to the GCSCC Technical Board*
2	*3/11/2023*	*Second draft submitted to hosts*
3	*20/11/2023*	*Feedback received from hosts*
4	*28/11/2023*	*Final report submitted to hosts*

LIST OF ABBREVIATIONS

ABES	Brazilian Association of Software Companies
ABIN	Brazilian Intelligence Agency
Anatel	Telecommunications sector regulator
ANPD	National Data Protection Authority
BACEN	Central Bank of Brazil
C2	Command and control
CA	Certificate Authority
CAIS	Brazilian Academic and Research Network CSIRT
CAMP	Cybersecurity Alliance for Mutual Progress
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CDCiber	National School of Cyber Defence
CERT	Computer Emergency Response Team
CERT.br	Brazilian National Computer Emergency Response Team
CGI.br	Brazilian Internet Steering Committee
CI	Critical Infrastructure
CIS CSC	Center for Internet Security Critical Security Controls
CISO	Chief Information Security Officer
CMM	Cybersecurity Capacity Maturity Model for Nations
ComDCiber	Cyber Defence Command
CSIRT	Computer Security Incident Response Team
CTF	Capture The Flag
CTI	Cyber threat intelligence
CTIR.gov	Brazilian Center for the Prevention, Handling and Response of Government Cyber Incidents
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed denial of service (attack)
DSIC	Department of Information and Cybersecurity
EU	European Union
FCDO	Foreign, Commonwealth and Development Office
Febraban	Brazilian Federation of Banks
FIRST	Forum of Incident Response and Security Teams
FPA	Federal Public Administration
GCSCC	Global Cyber Security Capacity Centre
GDPR	General Data Protection Regulation

GGE	Group of Governmental Experts
GSI	Gabinete de Segurança Institucional da Presidência da República (Institutional Security Cabinet of the Presidency of the Republic)
ICT	Information and Communication Technologies
IDB	Inter-American Development Bank
IGF	Internet Governance Forum
ISAC	Information Sharing and Analysis Centre
ISO	International Standards Organisation
ISP	Internet Service Provider
IXP	Internet exchange point
KPI	Key performance indicator
LAC4	Latin America and Caribbean Cyber Competence Centre
LAC-AAWG	Latin America and Caribbean Anti-Abuse Working Group
LGPD	**General** Personal Data Protection Law
Mercosul	Southern Common Market
MFA	Ministry of Foreign Affairs
MISP	Open Source Threat Intelligence and Sharing Platform
MoD	Ministry of Defence
MoU	Memorandum of understanding
NATO	North Atlantic Treaty Organisation
NCRA	National Cyber Risk Assessment
NCS	National Cybersecurity Strategy
NCSC	National Cyber Security Centre
NIC.br	Brazilian Network Information Centre
NIST CSF	National Institute of Standards and Technology Cyber Security Framework
OAS	Organization of American States
OEWG	Open Ended Working Group
PKI	Public key infrastructure
PlanGIC	Cyber Incident Management Plan (for the FPA)
PlanSIC	National Critical Infrastructure Security Plan
PNCiber	National Cybersecurity Policy
PNSI	National Information Security Policy
ReGIC	Federal Cyber Incident Management Network
SDN	Software-defined network
SIM3	Security Incident Management Maturity Model

SMDC	Cyber Defence Military System
SME	Small or medium-sized enterprise
SOC	Security Operations Centre
TCU	Federal Court of Accounts
TLS	Transport-layer security
UN	United Nations

EXECUTIVE SUMMARY

In collaboration with the UK's Foreign, Commonwealth and Development Office (FCDO) and the Organization of American States (OAS), the Global Cyber Security Capacity Centre (GCSCC, or "the Centre") undertook a review of the maturity of cybersecurity capacity in Brazil at the invitation of the Institutional Security Cabinet of the Presidency of the Republic (GSI). The objective of this review was to determine areas of capacity in which the Government might strategically invest, so that it may improve its national cybersecurity status.

Over the period 28th-30th August 2023, the following stakeholders participated in round-table consultations: academia, criminal justice, law enforcement, information technology officers and representatives from public sector entities, critical infrastructure owners, policy makers, information technology officers from the government and the private sector (including financial institutions), telecommunications companies, and the banking sector as well as international partners. These sessions took place in person, in Brazil.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model for Nations (CMM), which defines five *Dimensions* of cybersecurity capacity:

- *Cybersecurity Policy and Strategy*
- *Cybersecurity Culture and Society*
- *Building Cybersecurity Knowledge and Capabilities*
- *Legal and Regulatory Frameworks*
- *Standards and Technologies*

Each Dimension contains a number of *Factors* which describe what it means to possess cybersecurity capacity. Each Factor presents a number of *Aspects* grouping together related *Indicators*, which describe steps and actions that, once observed, define the stage of maturity of that Aspect. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an *ad-hoc* approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM document.[1]

Figure 1 below provides an overall representation of the cybersecurity capacity in Brazil, and illustrates the maturity estimates in each Dimension. Each Dimension represents one fifth of the graphic, with the five stages of maturity for each Factor extending outwards from the centre of the graphic; "start-up" is closest to the centre of the graphic and "dynamic" is placed at the perimeter.

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

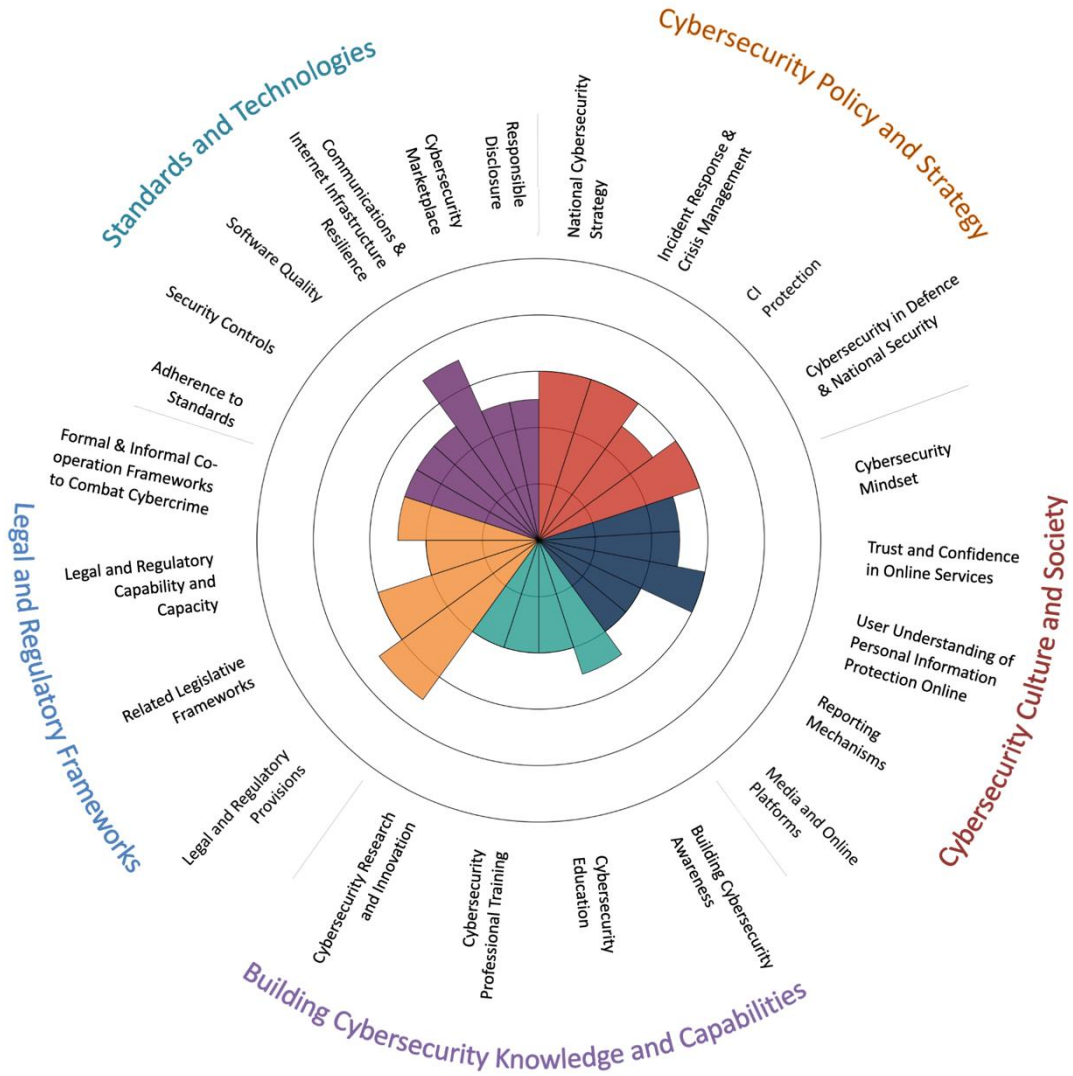


Figure 1: Overall representation of the cybersecurity capacity in Brazil – CMM review 2023

This was the second CMM review of Brazil, following the first in 2020. Additionally, Brazil has participated in the cybersecurity capacity Regional Studies (based on the CMM) conducted by the Organization of American States (OAS) and Inter-American Development Bank (IDB) in 2016, and again in 2020 (the results of the 2020 Regional Study were informed by the 2020 CMM review).

Figure 2 below shows the overall representation of the cybersecurity capacity in Brazil as presented in the 2020 CMM report.[2]

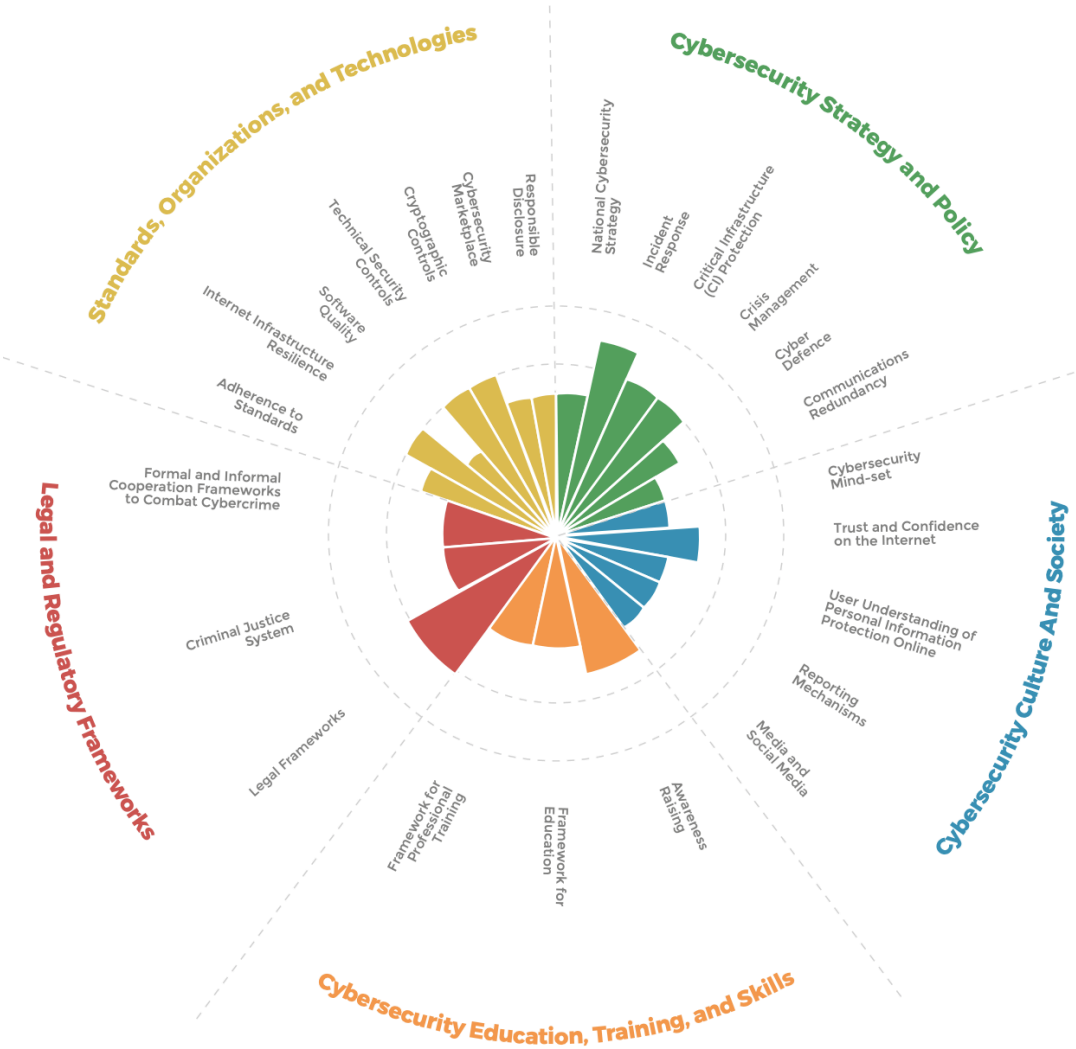


Figure 2: Overall representation of the cybersecurity capacity in Brazil – CMM review 2020

[2] The CMM was revised in 2021 to reflect the continuously changing cybersecurity risk and control landscape, and the changing operational environment in which nations have to deliver cybersecurity. There are, therefore, some differences between the CMM used in the 2020 review and in the 2023 review; differences in the structure of dimensions and phrasing of *Factor* names can be seen from the graphs.

Table 1 provides a summary overview of capacity developments for all factors assessed both in 2020 and 2023.

	Maturity Stage‡		Capacity Changes*
Factors based on CMM 2017	2020	2023	
D1 Cybersecurity Policy and Strategy			
D1.1 National Cybersecurity Strategy	Formative to Established	Established	++
D1.2 Incident Response	Established to Strategic	Established	-
D1.3 Critical Infrastructure Protection	Established	Formative to Established	-
D1.4 Crisis Management	Established	Established	o
D1.5 Cyber Defence	Formative to Established	Established	++
D1.6 Communications Redundancy	Formative	Established	++
D2 Cybersecurity Culture and Society			
D2.1 Cybersecurity Mind-Set	Formative	Formative to Established	++
D2.2 Trust and Confidence on the Internet	Formative to Established	Formative to Established	o
D2.3 User Understanding of Personal Information	Formative	Established	++
D2.4 Reporting Mechanisms	Formative	Formative	o
D2.5 Media and Social Media	Formative to Established	Formative	-
D3 Cybersecurity Education, Training, and Skills			
D3.1 Awareness Raising	Formative to Established	Formative to Established	o
D3.2 Framework for Education	Formative	Formative to Established	++
D3.3 Framework for Professional Training	Formative	Formative to Established	++
D4 Legal and Regulatory Frameworks			
D4.1 Legal Frameworks	Established	Established to Strategic	++
D4.2 Criminal Justice System	Formative	Formative to Established	++

‡ For reasons of backward compatibility, this overview presents maturity levels observed in the 2023 CMM assessment in the framework of a previous version of the CMM that had served as the basis for the CMM review of Brazil conducted in 2020.

* Factors that have advanced to the next maturity stage have received the mark «+ +». Factors that have seen improvements in some of its indicators but not sufficient progress to warrant an upgrade in the next maturity stage have been marked «+». Factors without notable progress have been registered with the neutral mark «o». Any regression has been marked «- -»/«-», correspondingly. It is important to note that the CMM 2021 revision has created some new requirements that must be met in order to reach maturity stages. Regression occurs as a result of these new requirements, rather than an actual regression in practice.

D4.3 Formal and Informal Cooperation Frameworks	Formative	Formative to Established	++
D5 Standards, Organisations, and Technologies			
D5.1 Adherence to Standards	Formative to Established	Formative to Established	o
D5.2 Internet Infrastructure Resilience	Established	Established to Strategic	++
D5.3 Software Quality	Formative	Formative to Established	++
D5.4 Technical Security Controls	Established	Formative to Established	-
D5.5 Cryptographic Controls	Established	Formative to Established	-
D5.6 Cybersecurity Marketplace	Formative to Established	Formative to Established	o
D5.7 Responsible Disclosure	Formative to Established	Formative to Established	o

Table 1: Capacity developments comparing CMM assessments of Brazil in 2020 and 2023

Cybersecurity Policy and Strategy

The first Brazilian national cybersecurity strategy (NCS), E-Ciber[3], was adopted in February 2020. It was developed through a process of consultations with a range of relevant stakeholders, and supported by an assessment of national cybersecurity risks, which is documented in the NCS. The NCS was originally developed to be valid for a four-year cycle: 2020-2023, after which renewal was planned. A change in the Brazilian administration has led to delay in this renewal, leading to an agreement to expand the term of the existing NCS for another year. The process of revision is planned to begin at the end of 2023.

There is a programme of activity designed to deliver the NCS, according to an NCS Action Plan. The NCS delivery programme includes a series of "National Plans" that are focused on creating the legislations and budgets needed to execute the strategic objectives of the NCS. The various components of the National Plans are not yet formally adopted but are at various stages in the congress approval process; some, such as the National Critical Infrastructure Security Plan (PlanSIC) have already been passed.

While various activities are underway to implement various aspects of the NCS, it is not currently clear how investments in all of the different interventions that form the national cybersecurity programme are being coordinated. There is also currently limited monitoring of the collective impact of the interventions being made is being monitored: metrics for monitoring the impact of the national cybersecurity programme have not yet been defined. Discussions are ongoing on which organisations should be part of the coordinating body for the national cybersecurity programme that implements the NCS. There is ongoing discussion of the potential role that a new cybersecurity agency might take in this regard.

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

Brazil actively participates in various international and regional cybersecurity forums and operational bodies, and is also starting to engage in supporting regional capacity-building initiatives. There have also been steps taken to advance the capacity and coordination of cyber diplomacy: Brazil designated its first cyber diplomat in 2019, who has participated in two editions of the UN GGE. Continuing to refine international engagement objectives, and validate that they are clearly understood by all relevant parties, will be important.

Brazil is a large country with a range of distributed structures that have evolved to deal with various aspects of cybersecurity, including multiple Computer Emergency Response Teams (CERTs) to provide incident response: two national-level CERTs, CTIR.gov and CERT.br, and a large number of subnational CERTs. This distributed arrangement is reported to function effectively. It is important to remain cognisant that cyber incidents are inherently often cross-cutting, and as such cyber incident response often needs to function across sectors and institutions. It is therefore especially important, for incident response related to cyber in particular, that the ability of the various parts involved to respond as a whole is effective and regularly tested. We recommend that is would be beneficial to test (e.g., through practical or table-top exercises) the collaboration and rapid information-sharing capabilities between the various national, regional and sectoral entities.

Similarly, crisis management in Brazil is not centralised, but organised by sector, with each sector having its own crisis-management team that responds to crises affecting its sector. Participants in the CMM review generally viewed the integration of cybersecurity into crisis management as being effective, having being strengthened through practice in real-world events and regularly via a strong programme of crisis exercising. In particular, the Cyber Guardian Exercise has been conducted annually since 2018, and focuses on protection of the CI against cyber crisis scenarios, and on testing and training coordination between the public and private sectors in these scenarios. While the decentralised, regularly exercised approach is reported to be strong, it is critical to continue to regularly test the capabilities of the various relevant entities to coordinate in the face of a wide range of potential cybersecurity scenarios. The findings from these exercises should be evaluated to establish regularly updated lessons learned. In establishing lessons learned, consideration should be given to whether it would be beneficial to assign a body responsible for coordinating cyber crisis management (and for supporting wider crisis-management processes in which there is a cybersecurity element), and/or to formally integrate cybersecurity into a broader crisis-management framework.

The National Critical Infrastructure Security Plan (PlanSIC) was approved by Decree 11,200 in September 2022.[4] Through PlanSIC, progress is being made towards identifying the critical infrastructure (CI), coordinating and assigning responsibilities for its protection, and developing recommended cybersecurity standards for all CI sectors. Many elements of PlanSIC are not yet fully implemented, and as such cybersecurity is not yet regulated across all CI sectors.

Participants stated that the regulatory structure has not yet been decided; this is currently in the study phase included in the work of the established technical groups, and will be taken to congress for discussion. During the CMM review sessions, there was some debate amongst participants as to the relative benefits of assigning the competence to regulate cybersecurity across the CI sectors to a single body such as the planned national cybersecurity agency or GSI, or to developing the regulatory structure per sector. In the latter case, participants

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

expressed the view that the agency or GSI might still play a valuable role in coordinating and supporting the individual CI-sector regulators, for example in the form of recommending minimal cross-sector cybersecurity standards.

In practice, currently the level of cybersecurity regulation varies across different CI sectors. Cybersecurity requirements are provided by some sector regulators, each of which has autonomy in terms of the management of their sector in relation to cybersecurity, with varying levels of requirement and compliance-monitoring as a result. The Federal Public Administration (FPA), and financial and telecommunications sectors were considered by participants to be the most advanced sectors in this regard. Within the regulated CI sectors, operators implement good cybersecurity practice. Outside of these sectors, participants reported that there is implementation of cybersecurity good practice, and self-assessment against recognised industry standards, by many organisations, but the level of course varies across organisations.

Several policies and doctrines exist for cybersecurity in national defence. The Cyber Defence Policy was released in 2012, and the first Cyber Defence Doctrine was approved in 2014. Cyber has also been identified in the National Defence Strategy as one of three strategic priorities, alongside nuclear and space, since 2008. At the end of 2020, new doctrinal and organisational acts were established for cyber defence. Participants reported that important decrees and legal instruments since 2020 have led to more consistent implementation of doctrine, and a better capacity to engage internationally.

Cyber-defence capabilities and organisational structures are in place in Brazil. There are cyber units within each of the three forces (Navy, Army and Air Force), as well as a joint command (ComDCiber). The National Cyber Defence School provides training to the joint command and officers from the cyber units of the three forces, and training is also provided to the forces' cyber units individually, with exercising described as a critical part of training. Some challenges around insufficient budgets for cyber defence were described, with a reported aim to develop capacity-based planning to assess and put in place the resources needed.

It was reported that since the CMM 2020, the coordination between the civil and defence entities has been improved, through increased integration between CI and defence entities. The responsibility of the Ministry of Defence (MoD) in regard to protecting CI has been formalised through PlanSIC, although specific roles and budgets for this are not yet defined. Initiatives are also underway to improve understanding of the dependence of national security and military entities on the cybersecurity of other parts of the CI through technical groups that are studying the interdependence between CI sectors (including the military).

Cybersecurity Culture and Society

Stakeholder discussions indicated the presence of initiatives addressing the awareness of cybersecurity risks within all government agencies, including some agencies proactively anticipating new cybersecurity risks. However, external reports discussed in the media also

document some shortcomings: It criticises lack of activity by corporate managers in the public sector, flagging a mismatch between awareness raising initiatives within government agencies and the actual level of awareness with respect to cybersecurity risks. Actual prioritisation of cybersecurity in government agencies seems to vary strongly, including significant gaps within some agencies. Similarly, safe cybersecurity practice does not seem to be adequately implemented, despite guidance and procedures being present. For the reasons outlined, the public sector currently would be assessed as being on Established level.

With respect to the private sector, the level of awareness varies depending on the size of companies. Major public and private companies have a very high level of cybersecurity awareness, make cybersecurity a priority, also implement safe cybersecurity practices. However, small and medium businesses lack resources and knowledge with respect to cybersecurity practices and, due to financial reasons, cybersecurity is rarely a priority. With respect to Internet users' awareness, their knowledge with respect to safe practices, and their prioritisiation of cybersecurity, stakeholders did not point to any systematic surveys, metrics, or further indicators / sources of information. It is essential that Brazil conducts systematic surveys and collects metrics. Due to the absence of metrics or surveys, the level of maturity with respect to Internet users cannot be assessed as higher than Formative. A limited but growing proportion of Internet users have a minimum level of awareness with respect to cybersecurity risks and also follow safe practices.

As indicated, there is a general lack of systematic surveys and metrics in Brazil with respect to Internet users and their behaviour. Hence, the level of trust and confidence of Internet users cannot be assessed with certainty and respective surveys should be conducted, including relevant metrics. Due to various initiatives, it may be assumed that users' level of trust and confidence in online services is at a Formative stage. Systematic metrics and surveys as well as a broad campaign addressing the public would presumably quickly lead to achieving Established stage. The initiatives also address disinformation, which means that also with respect to this Aspect at least Formative stage is achieved. With respect to e-government, digital government, and e-commerce, Brazil had already reached a high level in the previous CMM (2020). Brazil's stage remains at the Established level. In 2019, 48% of all bank transactions took place online and the number has doubled since that time. Banks have introduced a new secure system for instant online transactions, which has been well received by users.

The users' understanding of personal information protection online has to be reviewed on the background of a new General Personal Data Protection Law (LGPD), which broadly aligns with the EU's GDPR.[5] ANPD is the national oversight body for personal data protection and also runs awareness initiatives; its activities and the implementation and oversight of LGPD

[5] "General Personal Data Protection Act (LGPD)", lgpd-brazil.info, accessed on 22 October 2023, https://lgpd-brazil.info/.

indicate that a growing proportion of users has skills to manage their privacy online.[6,7]. This is backed by media reports.[8]

CTIR and sectorial CERTs provide reporting mechanisms for the public and private sector. CERT.br acts as a national-level CSIRT of last appeal, where also generally users may report incidents. However, reporting mechanisms are not promoted to the general public. Hence, a platform and entity that specifically aims at Internet users in general, and potentially also SMEs, should be established.

Apart from larger cybersecurity incidents, media coverage is mostly dedicated to financial fraud. Media reporting could be broader and also aimed at increasing citizens' awareness and promote best practices. Discussions on social media happen in an ad-hoc manner. Brazil does not have a positive whistleblowing culture. Reports on whistleblowing are mostly not found in the media.

Building Cybersecurity Knowledge and Capabilities

A number of cybersecurity awareness campaigns exist in Brazil. Most importantly, *internetsegura.br*, an initiative by NIC.br and CERT.br, provides advice to the general public.[9] The campaigns and activities of the NIC.br and its sub-organisations could benefit from stronger government support, e.g., through stronger funding and government-supported promotion. The impact of these programmes is not monitored through outcome-oriented surveys or metrics. A systematic coordination and a dedicated portal for the general public would be beneficial. Stakeholders indicated that the private sector conducts many awareness raising campaigns, in particular in the banking sector since this is also driven by requirements of the regulator. Again, there are no systematic reviews by means of metrics and surveys and also the various private sector initiatives are not centrally coordinated. International cybersecurity training companies also provide courses for executives in Brazil.[10] The private sector could benefit from mandatory cybersecurity courses across all sectors for executives of companies.

Stakeholders indicated that Computer Science courses offered at universities are harmonised by means of a curriculum coordinated by the *Sociedade Brasileira de Computação* (SBC, the Brazilian Computation Society).[11] Stakeholders also indicated that SBC has finished preparing the definition of an undergraduate course in cybersecurity in 2022, enabling universities to offer a programme fully dedicated to cybersecurity. However, no evidence of this course

[6] "Autoridade Nacional de Proteção de Dados", ANPD, accessed on 22 October 2023, https://www.gov.br/anpd/pt-br.

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

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

[9] "Safe Internet", internetsegura.br, accessed on 22 October 2023, translated by *Firefox Fullpage Translation*, https://internetsegura.br/.

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

[11] "Sociedade Brasileira de Computação", SBC, accessed on 22 October 2023, https://www.sbc.org.br/.

programme is yet available online. In particular, cybersecurity is not yet a topic widely adopted in non-technical subjects and it is unclear, whether universities also offer lectures and seminars in cybersecurity aimed at a non-specialist audience, for example in law or ethics courses. While SBC is also concerned with computer education in the primary and secondary school curriculum, it is unclear whether cybersecurity is actually part of these levels–also, since primary and secondary education are partially within the responsibility of the communal and state level of government. Participants indicated that while many initiatives and activities exist, the educational system would benefit from a more coherent coordination of cybersecurity education.

With respect to vocational and professional training, stakeholders indicated there is currently no national coordination of such training. Many ad-hoc and industry initiatives exist. However, there is a significant gap in the workforce and a problem with qualified professionals moving abroad due to higher salaries. Stakeholders indicated that a main drawback of the professional training landscape is a cross-cutting approach integrating the requirements of the industry with the provision of professionally-focused education.

According to stakeholders, cybersecurity R&D activities mostly take place as part of conventional computer science research activities, e.g., as part of network security or systems security research and development. The main obstacle for reaching Established level is the lack of systematic national funding specifically for topics in cybersecurity and that also goes beyond the domain of technology and computer science. A next iteration of a national cybersecurity strategy should consider providing dedicated funding of this kind, which also addresses disciplines beyond technology and computer science. Furthermore, metrics should systematically be implemented, in order to measure the performance of R&D activities with respect to cybersecurity.

Legal and Regulatory Frameworks

Substantive cybercrime legislation has been thoroughly reviewed in the 2020 CMM Review of Brazil—the reader is referred to the 2020 report for a thorough listing of specific cybercrime and criminal law. Stakeholders have indicated that laws with respect to the digital chain of custody have been improved:[12] Due to secondary legislation the digital chain of custody can now be fully established, aiding criminal investigations and criminal procedural law (e.g., LEI Nº 14.155, DE 27 DE MAIO DE 2021[13] has been adapted in order to include the digital aspects). It follows ISO 17005. Brazil has signed the Budapest Convention and the implementation of of its requirements in national law is underway, although many requirements have already been implemented prior to signing the convention. The 2nd protocol of the Budapest Convention is of particular importance for Brazil, since it improves the possibilities for international cooperation and exchange of information for Brazilian authorities. Nevertheless, Brazil has already previously been integrated in police cooperation networks through, e.g., Interpol and G7. Brazil's general approach to cybercrime relies on treating cybercrime through

[12] The term "digital chain of custody" in this context refers to the documentation of ownership of a digital asset (e.g., data), and its transfer from a person or organization to another, including the exact date, time, and purpose of the transfer, etc.

[13] "LEI Nº 14.155, DE 27 DE MAIO DE 2021", GSI, accessed on 02 November 2023, https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm.

conventional law; law specific to cybercrime is only introduced where conventional law cannot adequately cover cybercrime cases. E.g., ransomware cases are handled as conventional extortion. Currently, Brazilian law does not require data breaches to be reported, as long as they do not include personal data. Where personal data is concerned, this is covered by the recently introduced General Personal Data Protection Law (LGPD), which is similar to the EU's GDPR.[14] Some sectors, for example, banking, require mandatory reporting. However, a general requirement for mandatory reporting would probably be useful across all sectors. Due to the ongoing activities in improving the legal and regulatory provisions, Brazil may be considered to already partially being on Strategic level. However, Stakeholders indicated that no systematic human rights impact assessment carried out with respect to cyber(crime) law, although some aspects are covered under LGPD.

As outlined, Brazil has implemented a comprehensive framework for personal data protection (LGPD). Oversight is guaranteed through a designated lead agency named ANPD. Brazil also has a functioning child protection law for the digital domain, which is regularly reviewed and adapted. Consumer protection online is covered mostly through conventional law. However, phishing is not currently considered a criminal act *per se*. Participants stated that criminalising Phishing would lead to a massive increase in criminal investigations–nevertheless, a law should be considered that could cover the systematic establishment of infrastructure for the purpose of Phishing. Furthermore, criminalising Phishing *per se* would presumably lead to a decrease in Phishing campaigns due to the deterrent effect of criminalisation. Intellectual Property is protected through conventional law. However, the law has not been designed specifically with respect to the risks online.

The institutional capability and capacity in Brazil varies strongly, depending on specific personnel and the level of administration. Brazil does not currently have a centralised competence centre for cybercrime cases, which would also be accessible to the state-level police; rather, this capability is integrated in the Federal Police. The state-level police also has to investigate cybercrime cases but there is no mechanism in place between states or between state and federal level, which would ensure sufficient capabilities and capacity and knowledge-sharing. According to stakeholders, the amount of experts within law enforcement has remained almost unchanged over the last 20 years, which is insufficient in order to address all cases of cybercrime. With respect to prosecutors, stakeholders have reported that resources, capabilities and capacities meet current needs. However, the situation seems to be different with courts. Stakeholders claimed that the courts seem to lack sufficiently trained judges for some cybercrime cases. According to stakeholders, regulatory bodies have an adequate level of staff and have the required capabilities and capacities.

As indicated previously, Brazil has signed and ratified the Budapest Convention. Current efforts include an integration of a 24/7 capacity, enabling Brazilian police to both seek and respond to requests for assistance. Stakeholders have also indicated that private-public collaborations work smoothly and that an information exchange between the private sector, intelligence, and the military is set up and works well. However, this statement could not be confirmed through external sources. The willingness to collaborate and openly exchange information, particularly of the private industry and NGOs, might be even greater in case the

[14] "General Personal Data Protection Act (LGPD)", lgpd-brazil.info, accessed on 22 October 2023, https://lgpd-brazil.info/.

information exchange is mandated to a cybersecurity agency separate from the intelligence, military, and law enforcement community.

Standards and Technologies

A nationally agreed baseline of cybersecurity-related standards and good practices has not yet been identified to guide organisations across the public and private sectors. The NCS establishes as a strategic action (within Strategic Action 2.3.1) improving the adoption of internationally recognised standards by the public and private sectors. Various standards are followed in the more advanced sectors and larger organisations. In the Federal Public Administration (FPA), and financial and telecommunications sectors, adherence to cybersecurity standards is driven by regulation. In other sectors, the implementation of cybersecurity standards is more ad-hoc, and is not monitored by an authority, although sources of guidance are available.

In order to promote consistent adoption of cybersecurity standards across organisations of all sectors and maturity levels, it may be beneficial to develop a nationally-agreed baseline of cybersecurity-related standards and good practices, against which organisations from the public and private sectors can in some cases be audited and in others self-assess. This should include standards for the procurement of technology, and standards for security in technology and service provision.

Technological security controls are deployed by public and private-sector organisations. Given the variability in the levels of standards adoption across organisations, the level of implementation of these controls varies significantly across different sectors and sizes of organisation. In the regulated sectors described above, there is a high level of technical and cryptographic control deployment in line with international standards. In sectors that are not regulated for the implementation of cybersecurity standards, there are, as might be expected, varying levels of implementation of technical and cryptographic security controls.

Some participants expressed the view that many organisations in the private sector are not implementing technical security controls at an adequate level to manage risks, with patchy controls and playbooks and processes that are missing or rarely updated. Participants also reported some concerns about lower levels of adoption of appropriate technical and cryptographic controls by SMEs, who usually have only limited financial resources to invest in cybersecurity. Many SMEs rely on cloud services, and concerns about a lack of awareness of how to securely configure and maintain cloud instances, potentially leading to vulnerability, were cited.

Internet-service providers, particularly the larger providers, offer a range of technical security controls for their downstream customers. There are current campaigns being run to increase the adoption of anti-DDoS and anti-spoofing controls by ISPs to protect their downstream customers. Tools such as TLS are deployed by some service providers to secure communications between servers and users, and the government is seeking to increase adoption of digital certificates and the security protocols they enable.

There is no catalogue for assured software platforms and applications currently available for organisations across the public and private sectors, nor is guidance given consistently to all organisations on secure software development and maintenance. In some sectors, there is

guidance given and regulatory requirements in place around software security. For example, For the FPA, there is an inventory of secure software, and secure software development and maintenance processes are in place in line with regulation. The financial and telecommunications sectors also have some regulatory requirements for software security. In other sectors such as Electricity, there are provisions stating that companies should have policies for secure software development and maintenance; these criteria are not regulated.

Outside of the more mature sectors described above, software quality and security is variable. Participants were not aware of recommendations given by government on the secure development of software, selection of secure software applications, or secure maintenance of software, that would extend to private-sector organisations. Participants expressed the view that guidance for all organisations on assured software platforms and applications would be beneficial, which guide all organisations in Brazil in selecting software for use. Furthermore, guidance extending to all organisations on secure software development and maintenance processes may be beneficial.

Reliable Internet services are widely available in Brazil and widely used, including for conducting e-commerce and electronic business transactions, with appropriate authentication processes established for most transactions. Participants generally agreed that there is a high level of resilience of the Brazilian Internet infrastructure, with reportedly no events in Brazil having caused major interruptions to Internet services. This is largely due to the decentralised structure, with a large number of Internet Service Providers (ISPs) operating in Brazil, and the presence of a large number of Internet eXchange Points (IXPs).

The telecommunications sector is regulated in general and for cybersecurity by the Brazilian National Telecommunications Agency, Anatel, which sets various cybersecurity requirements. Participants reported that Anatel's cybersecurity requirements are not yet mandatory, but are intended to be. These regulations apply in theory to all telecommunications operators. Anatel noted that, in practice, with approximately 1,500 ISPs in the country, it is not possible to perform audits for all operators. As such, it is not clear that these practices – the management of deployed technologies, risk assessments, network monitoring and resilience testing, and incident-response plans – will be consistently achieved across all Internet-infrastructure providers. Participants generally agreed that operational cybersecurity is strong amongst larger ISPs, but that there may be gaps in regard to smaller and medium-sized ISPs.

Participants generally agreed that the majority of cybersecurity technologies in Brazil are imported from abroad, often via domestic integrators. While there is some domestic production of cybersecurity technologies, and the domestic market is perceived to be growing, domestically produced cybersecurity products are not currently the market leaders. There is variability in the extent to which, currently, organisations are able to identify and manage the security implications of reliance on foreign technologies. This could create risk in the context of an international supply chain.

There are widespread cybersecurity consultancy services available for private and public organisations in Brazil. Participants described an active marketplace, with many national companies as well as large international companies offering consultancy services. Organisations' understanding of how to assess risk and reliability in procuring a cybersecurity-service provider varies dependent on their maturity and risk appetite. There is not currently any accreditation of cybersecurity-service providers by a national body. This may be beneficial

to guiding organisations in selecting reliable and secure service providers; particularly for organisations with limited cybersecurity expertise to inform their decisions.

There is widespread use of cloud services by Brazilian organisations. Some organisations conduct risk assessments to determine how to mitigate the risks of outsourcing IT to a third party or cloud services; in particular larger organisations tend to have security requirements in place when procuring services. For some sectors including the FPA and financial sector, this is driven by regulation. Potential issues for SMEs were highlighted: many SMEs rely on cloud services for IT and cybersecurity services. Participants described a lack of understanding of how to use the cloud securely in organisations that do not have a dedicated IT or cybersecurity team, leading to mistakes in configuration or failure to update, and resulting in vulnerability. It might be beneficial to extend a more substantial awareness-raising or training offering to SMEs for the secure use of cloud and assessment of the risks, or to issue specific cloud-security guidelines suitable to organisations that have lower cybersecurity capability and resource.

The cyber-insurance market in Brazil is in its early stages. Most cyber-insurance product offerings, it was reported, are by multi-national insurance companies, with participants aware of few local companies offering cyber-insurance products. The uptake of cyber-insurance offerings until recently has mainly been by large multi-national companies, but demand from Brazilian organisations is reportedly beginning to grow. The need for specific cyber-insurance products was recognised, with participants reporting that business-continuity insurance in Brazil would not tend to cover cyber-incidents. An issue around the affordability of the cyber-insurance products currently offered was raised, preventing some organisations from taking up cyber-insurance policies. While some working-group discussions on the affordability of cyber-insurance offerings were reported, It is also not clear that there has yet been strategic identification of the cyber-insurance market needs. Identifying the needs of organisations in Brazil in this area through assessment of financial risks for the public and private sectors, as well as cost-related challenges, would be beneficial to informing the development of the cyber-insurance market.

INTRODUCTION

In collaboration with the UK's Foreign, Commonwealth and Development Office (FCDO) and the Organization of American States (OAS), the Global Cyber Security Capacity Centre (GCSCC, or "the Centre") undertook a review of the maturity of cybersecurity capacity in Brazil at the invitation of the Institutional Security Cabinet of the Presidency of the Republic (GSI). The objective of this review was to determine areas of capacity in which the Government might strategically invest, so that it may improve its national cybersecurity status.

Over the period 28th-30th August 2023, a three-day consultation process took place in Brazil. This was preceded by a desk-research phase in which the GCSCC researchers gathered information from documents available online and provided by the GSI. Stakeholders from the following organisations participated in person in the consultations:

- Public-sector entities:
    - Institutional Cabinet of the Presidency of the Republic (GSI)
    - Ministry of Defence
    - Ministry of Education
    - Ministry of Agriculture
    - Ministry of Management and Innovation in Public Services
    - Ministry of Justice and Public Security
    - Ministry of Communications
    - Ministry of Foreign Affairs
    - Ministry of Mines and Energy
    - Ministry of Development, Industry, Trade and Services
    - Ministry of Planning and Budget
    - Ministry of Labour and Employment
    - Brazilian Intelligence Agency (ABIN)
    - National Electric Energy Agency
    - National Telecommunications Agency (ANATEL)
- Federal police
- Defence and military representatives
- Universities
- Professional societies
- Telecommunications service providers and Internet service providers (ISPs)
- Operators of Critical Infrastructures (CIs)
- National and subnational Computer Emergency Response Teams (CERTs)
- Cybersecurity technology and service providers

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were based around the GCSCC Cybersecurity Capacity Maturity Model (CMM),[15] which is composed of five distinct *Dimensions* of cybersecurity capacity (see Figure 3).

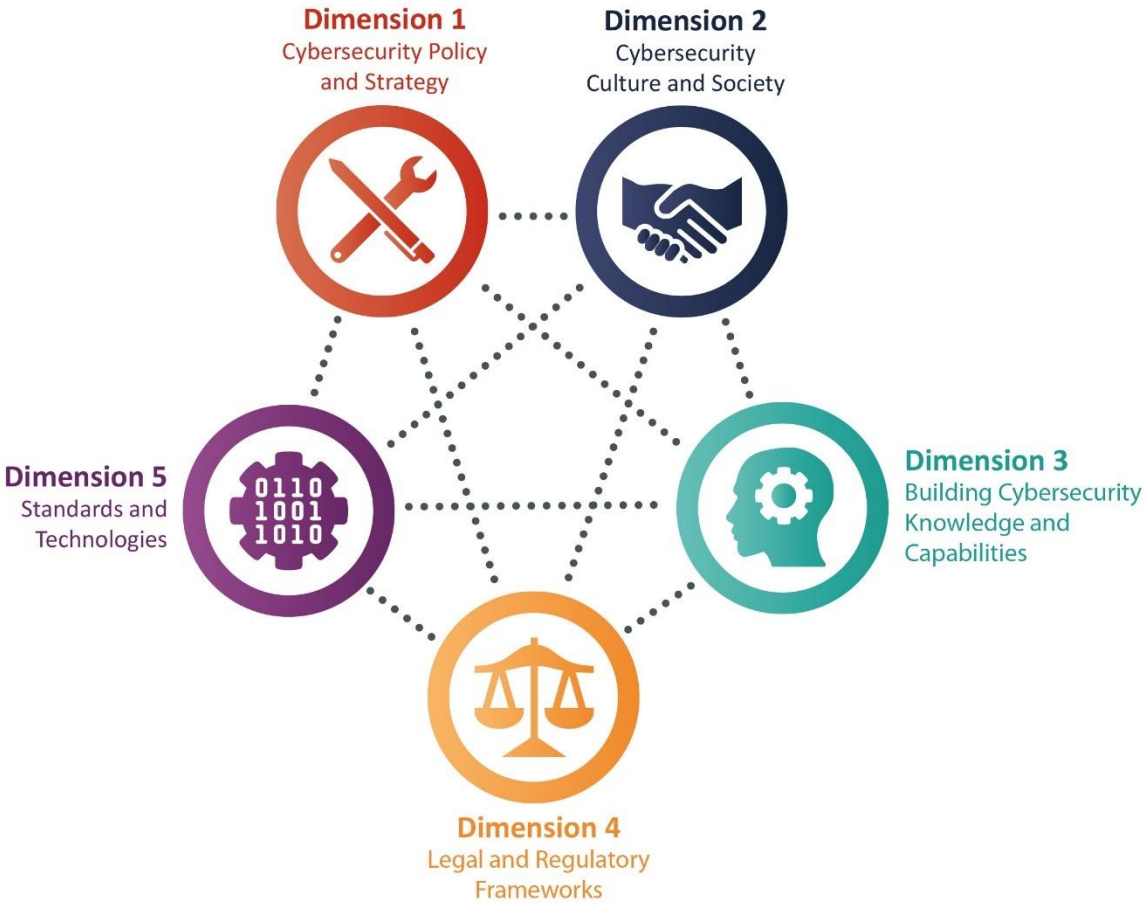


Figure 3: Dimensions of CMM.

[15] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), 2021 Edition," March 2021, https://gcscc.ox.ac.uk/the-cmm#/.

Each *Dimension* consists of a set of *Factors*, which describe and define what it means to possess cybersecurity capacity therein. Table shows the five *Dimensions* together with the *Factors* which each presents:

DIMENSIONS	***FACTORS***
Dimension 1 ***Cybersecurity Policy and Strategy***	D1.1 National Cybersecurity Strategy D1.2 Incident Response and Crisis Management D1.3 Critical Infrastructure (CI) Protection D1.4 Cybersecurity in Defence and National Security
Dimension 2 ***Cybersecurity Culture and Society***	D2.1 Cybersecurity Mindset D2.2 Trust and Confidence in Online Services D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Online Platforms
Dimension 3 ***Building Cybersecurity Knowledge and Capabilities***	D3.1 Building Cybersecurity Awareness D3.2 Cybersecurity Education D3.3 Cybersecurity Professional Training D3.4 Cybersecurity Research and Innovation
Dimension 4 ***Legal and Regulatory Frameworks***	D4.1 Legal and Regulatory Provisions D4.2 Related Legislative Frameworks D4.3 Legal and Regulatory Capability and Capacity D4.4 Formal and Informal Co-operation Frameworks to Combat Cybercrime
Dimension 5 ***Standards and Technologies***	D5.1 Adherence to Standards D5.2 Security Controls D5.3 Software Quality D5.4 Communications and Internet Infrastructure Resilience D5.5 Cybersecurity Marketplace D5.6 Responsible Disclosure

Table 2: the Dimensions *and their* Factors *that are considered in CMM.*

STAGES OF CYBERSECURITY CAPACITY MATURITY

Each *Dimension* contains a number of *Factors* which describe what it means to possess cybersecurity capacity. Each *Factor* presents a number of *Aspects* grouping together related *Indicators*, which describe steps and actions that, once observed, define *the Stage* of maturity of that *Aspect*. There are five *Stages* of maturity, ranging from the start-up stage to the dynamic stage. The start-up stage implies an *ad-hoc* approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. The five *Stages* are defined as follows:

- **Start-up:** at this *Stage*, either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There may be an absence of observable evidence at this *Stage*;

- **formative:** some features of the *Aspect* have begun to grow and be formulated, but may be *ad hoc*, disorganised, poorly defined or simply new. However, evidence of this activity can be clearly demonstrated;

- **established:** the Indicators of the *Aspect* are in place, and evidence shows that they are working. There is not, however, well-thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in the various elements of the *Aspect*. But the *Aspect* is functional and defined;

- **strategic:** choices have been made about which parts of the *Aspect* are important, and which are less important for the particular organisation or nation. The strategic *Stage* reflects the fact that these choices have been made, conditional upon the nation or organisation's particular circumstances; and

- **dynamic:** at this *Stage*, there are clear mechanisms in place to alter national strategy depending on the prevailing circumstances, such as the technology of the threat environment, global conflict, or a significant change in one area of concern (e.g. cybercrime or privacy). There is also evidence of global leadership on cybersecurity issues. Key sectors, at least, have devised methods for changing strategies at any stage during their development. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this *Stage*.

The assignment of maturity stages is based upon the evidence collected, including the general or consensus view of accounts presented by stakeholders, desktop research and the professional judgement of GCSCC researchers. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of Brazil and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

CYBERSECURITY CONTEXT IN BRAZIL

Brazil is a large country covering approximately 8.5 million square kilometres (approximately half of the total area of South America). It is home to a population of approximately 216 million people. At the beginning of 2023, there were an estimated 181.8 million Internet users in Brazil: an Internet penetration rate of 84.3 percent, with an estimated 70.6 percent the population also using social media.[16] There is also widespread usage of cellular mobile connections, with the number of connections in early 2023 equivalent to 102.4 percent of the population.

Brazil is divided into 26 states and one federal district. These federative units each have their own government and constitution, with a substantial degree of autonomy.[17] The states are further divided into municipalities. The local governments share responsibility with the federal government for the provision of public services, taking primary responsibility for services such as education, healthcare and law enforcement, with financial and technical assistance from the federal government. There are aspects, such as higher education and law enforcement relating to organised crime, for which greater responsibility is taken at the federal level.

The federal system, as well as the large size of the country (in terms of land and population), are important to consider when assessing Brazil's cybersecurity, since they lead to significant variation across the country in the implementation measures taken and the levels of cybersecurity capacity and resource.

In terms of Brazil's readiness to take advantage of the opportunities offered by digital technologies, the Network Readiness Index 2022 ranked Brazil Cambodia 44th out of the 131 economies it includes, performing above the upper-middle income group average in all four pillars: Technology, People, Governance and Impact. Its main strength related to People, while the greatest scope for improvement related to Impact.[18]

Brazil participates in the Global Cybersecurity Index (GCI) by the International Telecommunication Union (ITU), having recently submitted responses to the questionnaire for the fifth edition. In the fourth edition of 2020, Brazil was ranked at 18th globally, and 3rd out of 35 countries in the Americas region.[19] Legal measures were indicated as an area of relative strength, while technical and organisational measures were an area of potential growth.

[16] https://datareportal.com/reports/digital-2023-brazil
[17] https://forumfed.org/document/federal-republic-of-brazil/
[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

As a member state of the Association of the Organisation of American States (OAS), Brazil participates in the OAS cybersecurity programme[20] and its CSIRTAmericas Network, as well as various cybersecurity training initiatives, discussions and bodies with other countries in the region. Brazil also actively participates in relevant international bodies and forums, with participation by representatives from the Ministry of Foreign Affairs (MFA), GSI, and Cyber Defence Command (ComDCiber) and other agencies. This includes attendance at ITU and G20 cybersecurity discussions, and active participation at the United Nations (UN) Open Ended Working Group (OEWG) on Information and Communication Technologies (ICTs), UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE), and UN ad-hoc working groups, including on cybercrime[21]. Brazil has twice chaired the UN GGE, (2014-15 and 2019-21)[22]. Relevant stakeholders reported Brazilian representatives making active contributions around the enforcement of international law in cyberspace, evolving cyber threats, and protection of CI, as well as the need to ensure that UN processes focus on the need to build cybersecurity capacity globally.

There have been a number of interventions made since the last CMM review conducted by the GCSCC, which was published in 2020. Key interventions include developing legal plans for the protection of the critical infrastructure (CI), formalising incident-response coordination within the federal government, and signing the Budapest Convention on Cybercrime.

These interventions are at varying stages of implementation, and have not all yet had enough time to create significant enough progress to lead to an increase in the maturity stage assessed according to the CMM. Furthermore, political challenges including a change of government have led to some delays, particularly in the renewal of the national cybersecurity strategy (NCS) which was due in 2023 but has been postponed by a year. These interventions do, however, represent strong progress towards reaching higher levels of cybersecurity maturity in the country, as is described throughout this report.

The recommendations we make in this report provide our view on the cybersecurity capacity and capability maturity enhancements that Brazil ought to consider for prioritisation. In some cases, work is already underway as part of ongoing projects but we still include the recommendation since the capacity is not yet fully achieved. The timing of this CMM review also provides an opportunities to make recommendations that may support the upcoming renewal of the NCS.

[20] https://www.oas.org/en/topics/cyber_security.asp

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

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

REVIEW REPORT

OVERVIEW

This section provides an overall representation of the cybersecurity capacity in Brazil. Figure 4 below presents the maturity estimates in each *Dimension*. Each *Dimension* represents one fifth of the graphic, with the five stages of maturity for each *Factor* extending outwards from the centre of the graphic; start-up is closest to the centre of the graphic and dynamic at the perimeter.

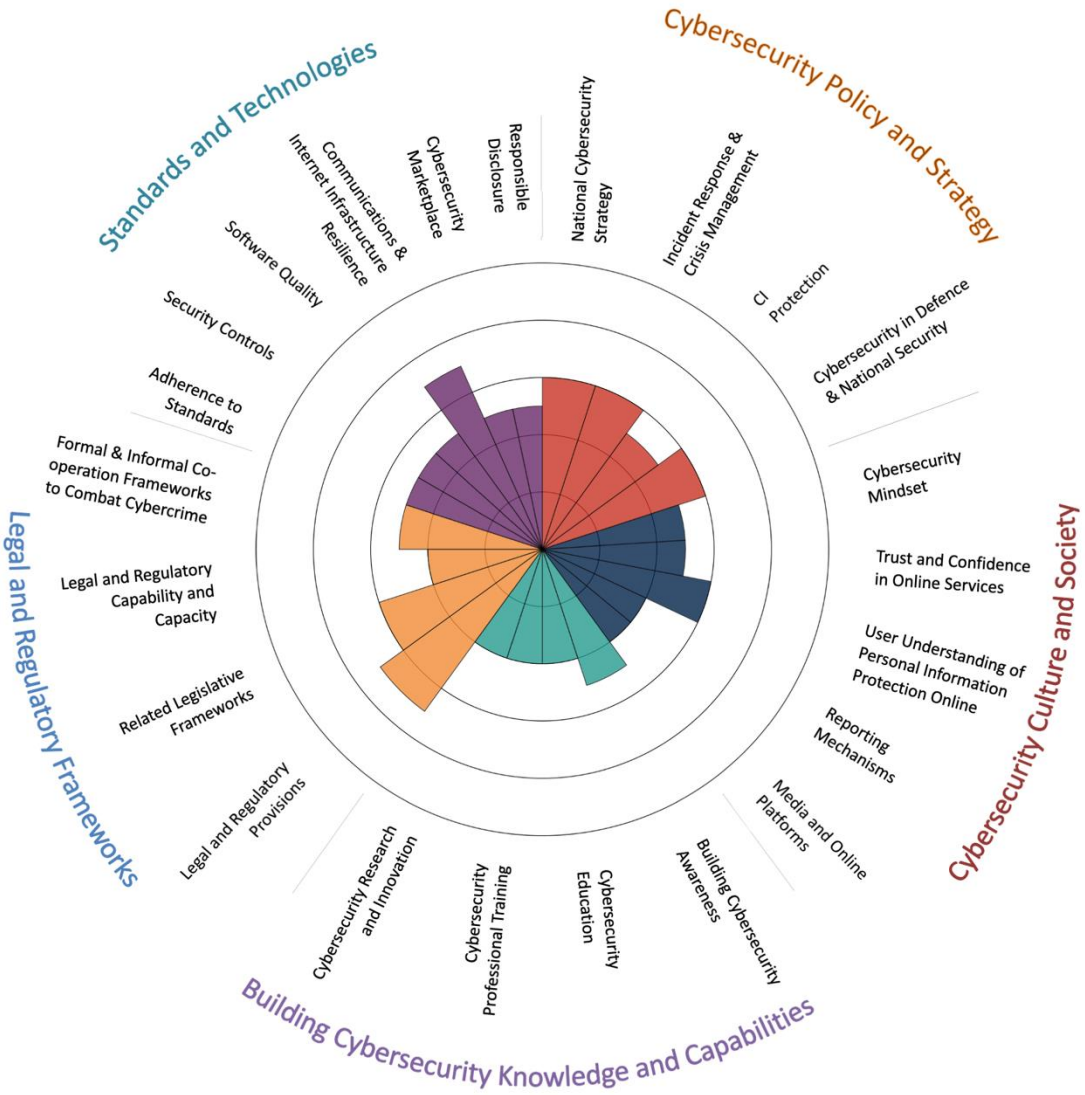


Figure 4: Overall representation of the cybersecurity capacity in Brazil – CMM review 2023

This was the second CMM review of Brazil, following the first in 2020. Brazil' cybersecurity capacity was also assessed using a questionnaire based on the CMM in the Regional Study conducted by the Organization of American States (OAS) and Inter-American Development Bank (IDB) in 2016, and again in 2020 (the results of the 2020 Regional Study were informed by the 2020 CMM review).

Figure 5 below shows the overall representation of the cybersecurity capacity in Brazil as presented in the 2020 CMM report. The CMM was revised in 2021 to reflect the continuously changing cybersecurity risk and control landscape, and the changing operational environment in which nations have to deliver cybersecurity. There are, therefore, some differences between the CMM used in the 2020 review and in the 2023 review; differences in the structure of dimensions and phrasing of *Factor* names can be seen from the graphs.

A comparison of Figure 4 and Figure 5 indicates the extent to which cybersecurity capacity in Brazil measured according to the CMM has changed during the last four years.

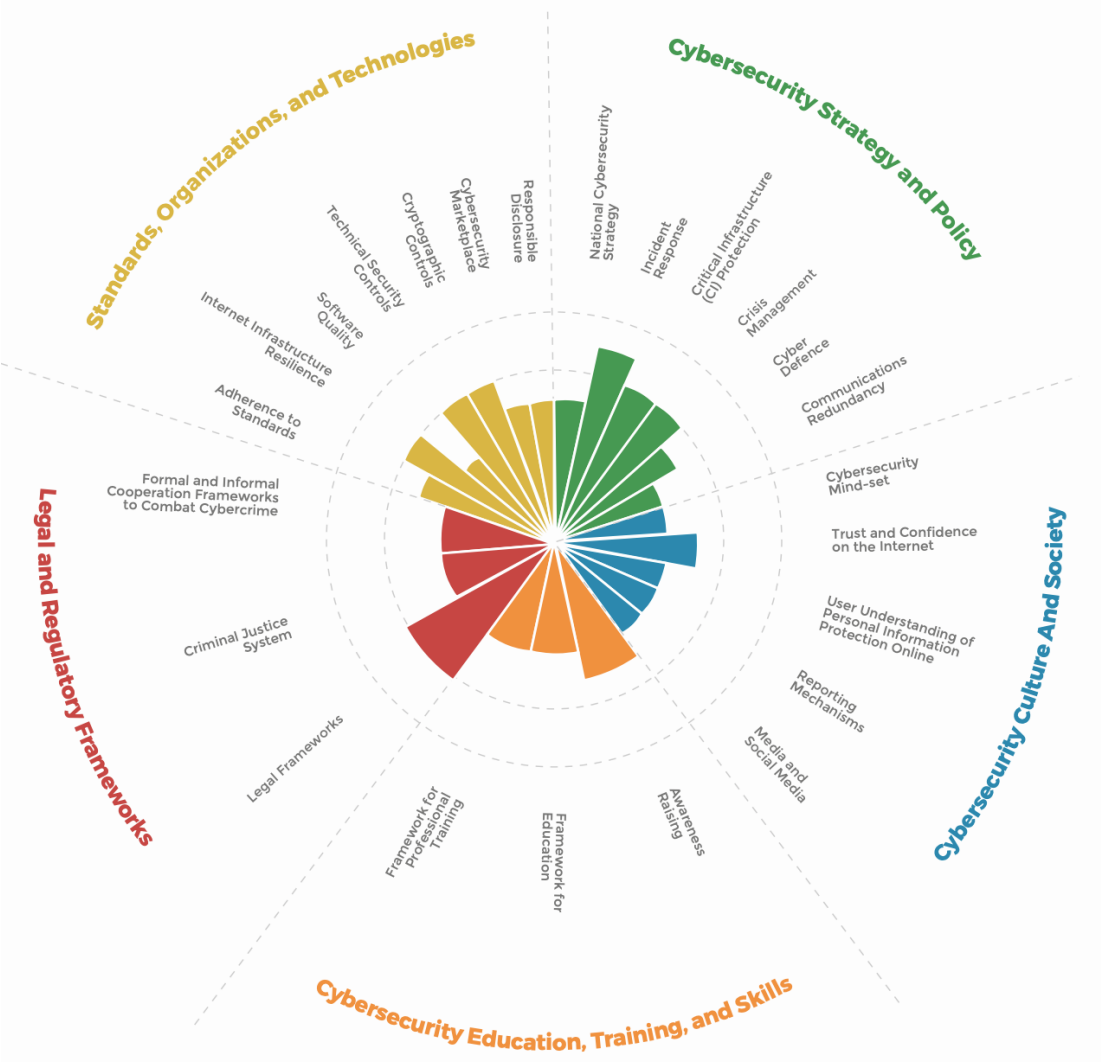


Figure 5: Overall representation of the cybersecurity capacity in Brazil – CMM review 2020

Table 2 provides a summary overview of capacity developments for all factors assessed both in 2020 and 2023.

Factors based on CMM 2017	Maturity Stage‡ 2020	Maturity Stage‡ 2023	Capacity Changes*
D1 Cybersecurity Policy and Strategy			
D1.1 National Cybersecurity Strategy	Formative to Established	Established	++
D1.2 Incident Response	Established to Strategic	Established	-
D1.3 Critical Infrastructure Protection	Established	Formative to Established	-
D1.4 Crisis Management	Established	Established	o
D1.5 Cyber Defence	Formative to Established	Established	++
D1.6 Communications Redundancy	Formative	Established	++
D2 Cybersecurity Culture and Society			
D2.1 Cybersecurity Mind-Set	Formative	Formative to Established	++
D2.2 Trust and Confidence on the Internet	Formative to Established	Formative to Established	o
D2.3 User Understanding of Personal Information	Formative	Established	++
D2.4 Reporting Mechanisms	Formative	Formative	o
D2.5 Media and Social Media	Formative to Established	Formative	-
D3 Cybersecurity Education, Training, and Skills			
D3.1 Awareness Raising	Formative to Established	Formative to Established	o
D3.2 Framework for Education	Formative	Formative to Established	++
D3.3 Framework for Professional Training	Formative	Formative to Established	++
D4 Legal and Regulatory Frameworks			
D4.1 Legal Frameworks	Established	Established to Strategic	++
D4.2 Criminal Justice System	Formative	Formative to Established	++

‡ For reasons of backward compatibility, this overview presents maturity levels observed in the 2023 CMM assessment in the framework of a previous version of the CMM that had served as the basis for the CMM review of Brazil conducted in 2020.

* Factors that have advanced to the next maturity stage have received the mark «+ +». Factors that have seen improvements in some of its indicators but not sufficient progress to warrant an upgrade in the next maturity stage have been marked «+». Factors without notable progress have been registered with the neutral mark «o». Any regression has been marked «- -»/«-», correspondingly. It is important to note that the CMM 2021 revision has created some new requirements that must be met in order to reach maturity stages. Regression occurs as a result of these new requirements, rather than an actual regression in practice.

D4.3 Formal and Informal Cooperation Frameworks	Formative	Formative to Established	++
D5 Standards, Organisations, and Technologies			
D5.1 Adherence to Standards	Formative to Established	Formative to Established	o
D5.2 Internet Infrastructure Resilience	Established	Established to Strategic	++
D5.3 Software Quality	Formative	Formative to Established	++
D5.4 Technical Security Controls	Established	Formative to Established	-
D5.5 Cryptographic Controls	Established	Formative to Established	-
D5.6 Cybersecurity Marketplace	Formative to Established	Formative to Established	o
D5.7 Responsible Disclosure	Formative to Established	Formative to Established	o

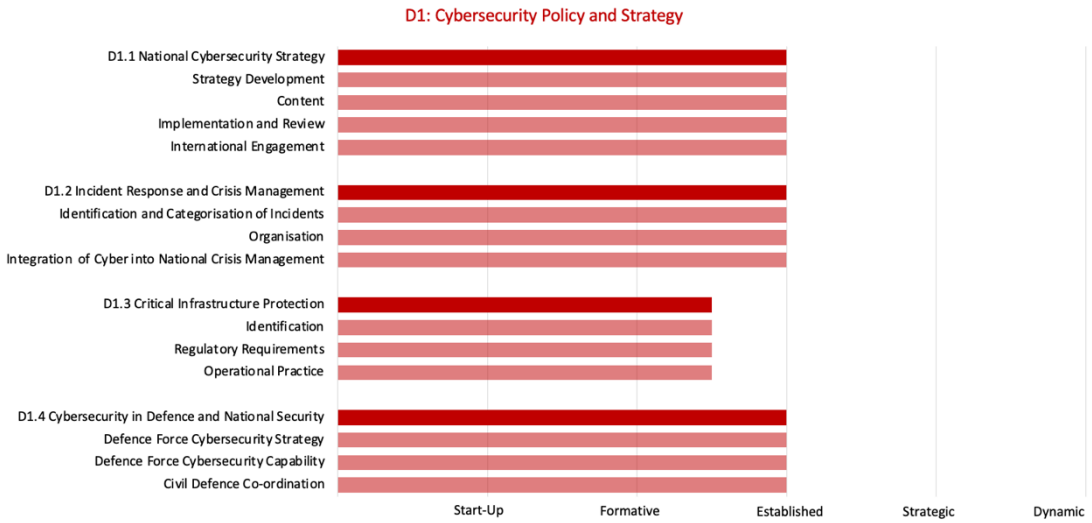
Table 2: Capacity developments comparing CMM assessments of Brazil in 2020 and 2023

DIMENSION 1
CYBERSECURITY POLICY AND STRATEGY

This *Dimension* explores Brazil's capacity to develop and deliver cybersecurity strategy and enhance its cybersecurity resilience through improving its incident response, cyber defence and critical infrastructure protection capacities. It considers effective strategy and policy in delivering national cybersecurity capability, while maintaining the benefits of a cyberspace vital for government, international business and society in general.

Figure 6: Factors and aspects examined in Dimension 1

OVERVIEW OF RESULTS



D1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key cybersecurity government and non-governmental actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities.

***Stage*: Established**

The first Brazilian national cybersecurity strategy (NCS), E-Ciber[23], has been published. The NCS was approved by Presidential Decree no. 10.222[24] and adopted in February 2020. The development of the NCS was led by the Institutional Security Cabinet of the Presidency of the Republic (GSI), which proposes guidelines and strategies for cybersecurity through the Department of Information and Communication Security (DSIC). This was in compliance with the provisions of the National Information Security Policy (PNSI, Decree no. 9,637 of December 26th 2018), which provided for the preparation of a NCS built in modules covering cybersecurity, cyber defence, security of critical infrastructures (CI), security of confidential information, and protection against data leakage.

The NCS was developed through a process of consultations with a range of stakeholders from the government, public- and private-sector organisations, academia and civil society. The

[23] https://ciberseguranca.igarape.org.br/en/national-cybersecurity-strategy-e-ciber-2020/
[24] http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm

consultation process and groups of stakeholders consulted are detailed in the NCS introduction, and during the CMM review sessions, stakeholders confirmed their participation in the process and resulting representation of their needs and interests in the NCS. Consultations were divided into three subgroups, with 31 meetings of the subgroups held in total: 1) cybernetic governance; normative dimension; research, development and innovation; education; international dimension and strategic partnerships; 2) digital trust, threat prevention and mitigation; 3) strategic protection – government and infrastructure. A draft was then made available online for public comment; at this stage, participation was received from 31 individuals and 10 public and private organisations.

The NCS was originally developed to be valid for a four-year cycle: 2020-2023, after which renewal was planned. A change in the Brazilian administration has led to delay in this renewal, leading to an agreement to expand the term of the existing NCS for another year. The process of revision is planned to begin at the end of 2023, and GSI is the body responsible for reviewing the current NCS and drafting the renewal. GSI described plans to engage a wide range of stakeholders in consultations for the NCS renewal process, including public- and private-sector organisations, academia, civil society, as well as engaging cybersecurity research and development institutions to consider how to account for the impact of emerging technologies. GSI also described plans for a supporting review of current legislation related to cybersecurity.

The strategic objectives are defined in the NCS: to make Brazil more prosperous and reliable in the digital environment; increase Brazilian resilience to cyber threats; and strengthen the Brazilian role in cybersecurity on the international stage. The 2020-2023 NCS content is divided into 10 strategic actions: 1) Strengthen cyber governance actions; 2) Establish a centralised model of governance at the national level; 3) Promote a participatory, collaborative, reliable and safe environment between the public sector, the private sector and society; 4) Raise the level of government protection; 5) Raise the level of protection of Critical National Infrastructures; 6) Enhancing the legal framework on cybersecurity; 7) Encourage the design of innovative cybersecurity solutions; 8) Expand Brazil's international cooperation in cybersecurity; 9) Expand the partnership in cybersecurity between the public sector, the private sector, academia and society; 10) Raise the level of maturity of society in cybersecurity. Participants reported that the CMM's five dimensions were considered in the process of developing the NCS content.

The NCS was developed based on an assessment of country-specific national cybersecurity risks. The results are summarised in the "diagnosis" section of the NCS. This considers the specific cybersecurity risks to Brazil, and was formulated based on the stakeholder consultations and existing statistics (e.g., from a third-party survey of 200 Brazilian companies in 2019 on the key cybersecurity concerns and attacks experienced). For the upcoming NCS renewal, it will be important to ensure that this national cybersecurity risk assessment is refreshed, to support development of NCS content. This should include taking account of the cybersecurity risks arising from the use of emerging technologies within critical infrastructure and wider society, and may also draw on insights on cyber-incidents and threats shared within information-sharing networks.

Consideration has been given to how the NCS can support wider online policy objectives: the NCS describes the need to align with the Civil Rights Framework for the Internet (Law No. 12,965 of 2014), which "*regulates the use of the Internet in Brazil through the provision of principles, guarantees, rights and duties for those who use the world wide web, and guidelines*

for the action of the State, protecting the personal data and privacy of users in the online environment", and explicitly considers how this should inform the development of legal frameworks as well as the terms of engagement at the international level. Stakeholders involved in planning the NCS renewal process also described the need for the upcoming consultations to consider issues observed in international discussions, including gender inclusion and social inclusion: how to promote cybersecurity culture to a society that is diverse socially and economically. Plans to focus on reviewing existing legal provisions for child protection online and the protection of personal information as part of the NCS renewal process were also described.

There is a programme of activity designed to deliver the NCS, according to an NCS Action Plan, which was not provided to the CMM review team, but reportedly described the actions needed to implement the NCS. The NCS delivery programme includes a series of "National Plans" that are focused on creating the legislations and budgets needed to execute the strategic objectives of the NCS. Alongside the NCS, these National Plans were provided for by the PNSI of 2018. The various components of the National Plans are not yet formally adopted but are at various stages in the congress approval process; some, such as the National Critical Infrastructure Security Plan (PlanSIC) have already been passed (see Section D1.3).

It is not currently clear how investments in all of the different interventions that form the national cybersecurity programme are being coordinated. The national cybersecurity programme does not currently have a process for allocating budget, nor for identifying and escalating budget shortfalls that could undermine the delivery of the NCS. Participants noted the importance of allocating the budget needed by various components of the national cybersecurity programme, to ensure that adequate investments in cybersecurity are made to support ongoing digital transformation. The intention is reportedly that the National Plans will eventually create a national dedicated budget for cybersecurity, assigned to a coordinating body. Currently, to deliver the actions of the programme, organisations invest in various campaigns in a decentralised manner. Government departments have autonomy to decide their investments in cybersecurity, and awareness-raising campaigns are run to encourage each government department to allocate resources to invest in cybersecurity. There are reportedly plans to create a new expenditure type within government that enables the government departments to formally allocate resources for cybersecurity.

It is also unclear how the collective impact of the interventions being made is being monitored. The NCS Action Plan does not define metrics or key performance indicators (KPIs) for monitoring the achievement of outcomes of the national cybersecurity programme. As such, there is only limited monitoring of success or review of processes. GSI described current difficulties in measuring the strategic actions for the NCS, and reported current efforts to validate progress in the NCS implementation programme via a third-party consultancy, that will be both validating current progress and identifying metrics and indicators to assess achievement of objectives.

As part of the next NCS revision, it will be important to ensure that a process is in place for allocating budget to the implementation of the various NCS actions, and for identifying any budget shortfalls so that they can be escalated to the coordinating body. Developing programme review processes and metrics that are adequately resourced will also be important to enabling a coordinating body to comprehensively ensure that those responsible for implementing various aspects of the NCS are held to account. They will also provide an

approach to identifying risks, implementation issues and dependencies, which can be escalated to the coordinating body as necessary. It will therefore be important to include the definition of NCS review processes and metrics in the upcoming NCS revision, supported by the findings from current validation efforts.

In terms of national cybersecurity governance, the political and strategic level of cybersecurity governance is assigned to GSI, while cyber defence is assigned to the Ministry of Defence (MoD). Discussions are ongoing on which organisations should be part of the coordinating body for the national cybersecurity programme that implements the NCS. The NCS sets actions for the establishment of a centralised model of cybersecurity governance, noting the centralised models adopted in the US, UK, Portugal, France, India, Malaysia, Singapore, South Korea and Japan: "*it is important to grant a government body the responsibility of guiding the theme at the national level, organizing it, and proposing measures and regulations, with the participation of representatives from all sectors of society. Only exceptions are made to aspects related to cybernetic defense and warfare, which are the responsibility of the Ministry of Defense, which in no way prevents the necessary interaction, in this regard, between the areas of security and defense*".

In this regard, there is ongoing discussion around establishing a new national cybersecurity agency to coordinate cybersecurity activity across sectors, and consideration of which organisations will form part of this agency. This new agency is proposed in the Bill for a new National Cybersecurity Policy (PNCiber), which also proposes the establishment of a new National Cybersecurity Committee, and a National Management Office of Cyber Crises. The Bill for PNCiber is currently in the discussion phase (with documented consultation outcomes having been provided to the CMM review team) to improve the text and carry out legal analysis. It will then be submitted to Congress for approval.

The role and operating model of the agency has not yet been fully determined; there is ongoing discussion amongst stakeholders in the country, and consideration of aspects of international models that it might draw on. It is anticipated that this agency might in future hold a national budget for cybersecurity, and coordinate the actions of various 'owners' of the NCS actions. There is debate on whether this agency might take on a cross-sector regulatory role, or whether its role should focus on promoting collaboration, trust and engagement between stakeholders. Some participants noted concerns about the potential conflict between this agency enforcing mandatory requirements and imposing penalties, and the need to promote an environment with which stakeholders are willing to engage and collaborate. It is important that the role of the agency is clearly defined: the extent to which is has a strategic oversight role, an operational delivery role, or both. It is also important to clearly define how its responsibilities interact with other security and regulatory functions in government: for example, if the agency is to have a regulatory role, it needs to be clear how this interacts with the existing regulatory structures within the country.

Brazil actively participates in relevant international bodies and forums, with participation by representatives from the Ministry of Foreign Affairs (MFA), GSI, and Cyber Defence Command (ComDCiber) and other agencies. This includes attendance at ITU and G20 cybersecurity discussions, and active participation at the United Nations (UN) Open Ended Working Group (OEWG) on Information and Communication Technologies (ICTs), UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of

International Security (GGE), and UN ad-hoc working groups, including on cybercrime[25]. Brazil has twice chaired the UN GGE, (2014-15 and 2019-21)[26]. Relevant stakeholders reported Brazilian representatives making active contributions around the enforcement of international law in cyberspace, evolving cyber threats, and protection of CI, as well as the need to ensure that UN processes focus on the need to build cybersecurity capacity globally.

The national-level Brazilian Cyber Security Incident Response Teams (CSIRTs) are members of the global Forum of Incident Response and Security Teams (FIRST) , and Brazilian experts make a leading contribution to the activities and development of FIRST and other international CERT forums such as the UN Internet Governance Forum (IGF) Best Practice Forum on CERTs.

At the regional level, Brazil is a member of the Organization of American States (OAS) and participates in its cybersecurity programme[27] and its CSIRTAmericas Network[28]. Participants reported that Brazil and OAS are considering jointly hosting events on cybersecurity for the region. Brazil also participates in the Cyber Committee of the Digital Agenda project of the Southern Common Market (Mercosul), of which Brazil is holding the presidency this year, which is reportedly negotiating an agreement on cybersecurity and discussing the possibility of developing a common cybersecurity taxonomy for the region. Participants viewed Brazil as a reference for the region, sharing its experience in developing national cybersecurity capacity at regional events to help other countries in the region.

Brazil is also beginning to actively engage in supporting regional capacity-building initiatives. For example, in September 2022, Brazil signed a memorandum of understanding (MoU) to collaborate on the EU CyberNet project. This project intends to establish and operationalise the Latin America and Caribbean Cyber Competence Centre (LAC4). Brazil will contribute to "*the identification of cyber capacity-building needs and the development of the LAC4 training curricula to support the cybersecurity endeavours of Brazil and the LAC4 region*".[29]

In terms of engagement at the international level, the NCS content explicitly details the need to be guided by Brazilian constitutional principles and fundamental values that must guide the national cybersecurity programme, including respect for democracy and human rights, identifying as relevant the Civil Rights Framework for the Internet (Law No. 12,965 of 2014) and the General Law for the Protection of Personal Data (Law No. 13,709 of 2018), combined with policies for the development of the Brazilian Internet. In practice, participants reported that Brazil chooses to engage widely in international discussions, and that departments or ministries that are representing Brazil at international fora would consult with and be coordinated by the MFA. There have also been steps taken to advance the capacity and coordination of cyber diplomacy: Brazil designated its first cyber diplomat in 2019, who has participated in two editions of the UN GGE.[30]

It is important to ensure that there is regular validation that the objectives in this area are clear and understood by all participants involved, and that there is a process in place to

[25] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home
[26] https://disarmament.unoda.org/group-of-governmental-experts/
[27] https://www.oas.org/en/topics/cyber_security.asp
[28] https://csirtamericas.org/en
[29] https://www.eucybernet.eu/celebrating-the-signature-of-the-memorandum-of-understanding-with-brazil-to-establish-cooperation-in-lac4-activities/
[30] https://directionsblog.eu/unpacking-brazils-cyber-diplomacy/

monitor the achievement of objectives. Continuous refinement of the objectives is also important: for example, Brazil might aim to eventually expand its objectives around building international communities of interest around specific cybersecurity policy goals, and more active involvement in building cybersecurity capacity in other countries.

D1.2 INCIDENT RESPONSE AND CRISIS MANAGEMENT

This Factor *addresses the capacity of the Government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the Government's capacity to organise, co-ordinate, and operationalise incident response, and whether cybersecurity has been integrated into the national crisis management framework.*

***Stage*: Established**

Brazil is a large country with a range of distributed structures that have evolved to deal with various aspects of cybersecurity, including multiple CERTs to provide incident response. This distributed arrangement is reported to function effectively. It is important to remain cognisant that cyber incidents are inherently often cross-cutting, and as such cyber incident response often needs to function across sectors and institutions. It is therefore especially important, for incident response related to cyber in particular, that the ability of the various parts involved to respond as a whole is effective and regularly tested. In this section, we describe Brazil's distributed setup of highly capable incident-response teams, and make some observations about the potential benefits of testing collaboration and rapid information-sharing capabilities between the various national, regional and sectoral entities.

Two main CERTs provide incident response services on a national scale in Brazil: CTIR.gov and CERT.br. The Brazilian Center for the Prevention, Handling, and Response of Government Cyber Incidents (CTIR.gov) is responsible for coordinating response to cybersecurity incidents relating to the networks of the Brazilian Federal Public Administration (FPA).[31] Each body within the FPA is required to have its own cyber incident-response team or CSIRT and responsible IT body. CTIR.gov provides a single point of contact for FPA institutions' incident notification, which is mandatory for all FPA institutions. CTIR.gov was established in 2006 and is part of the Department of Information Security and Cybersecurity (DSIC) of GSI. In addition to receiving notification and providing incident-response support, CTIR.gov actively monitors the government networks for threats and vulnerabilities using sensors and honeypots.

CERT.br is the Brazilian National Computer Emergency Response Team, which provides incident-management services to any network connected to the Brazilian Internet. It is described as a "National CSIRT of last resort",[32] providing a focal point for incident notification, technical incident-management support to analyse and recover compromised systems, and facilitating any necessary coordination among security professionals for response to an incident, especially for "*cases where no incident handling contact is known for a given*

[31] https://www.gov.br/ctir/pt-br/assuntos/rfc-2350-1/rfc-2350
[32] https://www.cert.br/

network". It is a free service for the Brazilian Internet community, funded by domain registration, and maintained by the Brazilian Network Information Center (NIC.br), which is the executive branch of the Brazilian Internet Steering Committee (CGI.br). Reporting to CERT.br is voluntary for all organisations. Public statistics are maintained of incidents handled and reports received from CSIRTs, network administrators and users.[33]

The activities of CERT.br have the strategic goal of increasing the level of security and incident-handling capacity of the networks connected to the Internet in Brazil. Alongside incident-handling services, CERT.br provide training and guidance in incident response for CSIRT staff, and conduct initiatives to encourage the adoption of security best practices. They engage in the formation of trust-based communities to share threat-intelligence, including groups in the energy sector run by Petrobras and in the financial sector, and encourage the use of Open Source Threat Intelligence and Sharing Platforms (MISP) for sharing information (including running MISP workshops). CERT.br also actively monitor the Brazilian Internet for incident detection and analysis of current and emerging threat trends, using a network of honeypots and sensors, as well as running a set of honeypots in other countries to analyse threat trends.

There are various subnational CERTs in Brazil, many of which are listed on the CERT.br website[34]). This includes the CERTs of bodies within the FPA (as described above), and CERTs across the various sectors. For example, for academic institutions, the Brazilian Academic and Research Network CSIRT, CAIS/RNP, is a mature Security Incident Management Maturity Model (SIM3)-certified CSIRT that maintains and analyses a registry of incidents, publishes training and alerting information to academic institutions in Brazil, engages in incident response and promotes security practice, and is a member of the Forum of Incident Response and Security Teams, FIRST[35]. CERTs also exist within the financial, energy, telecommunications and healthcare sectors, amongst others. The subnational CERTs vary in their capacity, with some having achieved SIM3 accreditation, while others have more limited resources.

Both CTIR.gov and CERT.br coordinate with international partners to share threat information and cooperate on responding to cyber incidents. Both CTIR.gov and CERT.br are members of FIRST[36], and representatives from CERT.br make key contributions to the development of FIRST policies and initiatives. CTIR.gov is also affiliated with the regional CSIRT Americas Network run by the Organization of American States (OAS),[37] and with the Latin America and Caribbean Anti-Abuse Working Group (LAC-AAWG), and handles international. At the sectoral level, there is also some international collaboration on incident response; for example, Anatel is a member of the Cybersecurity Alliance for Mutual Progress (CAMP), which provides a global network for information sharing and collective response.[38]

Registries of incidents are maintained by CTIR.gov and CERT.br, as well as various subnational CERTs, who classify and analyse their incident registries to gain insights informing their actions and to enable dissemination of warnings and recommendations to their constituents, and

[33] https://stats.cert.br/
[34] https://www.cert.br/csirts/brasil/
[35] https://www.first.org/members/teams/cais-rnp
[36] https://www.first.org/members/teams/
[37] https://csirtamericas.org/en/member_teams),
[38] https://www.cybersec-alliance.org/camp/index.do

publish trend information online. CTIR.gov also reported using analysis of their registry to establish public policies for improving the level of security in the networks of the FPA.

The level of incident notification by organisations varies according to their regulatory requirements and capacity to identify incidents. Although all FPA bodies are required to have a CSIRT, and report incidents to CTIR.gov, participants reported that their capacity and expertise to identify and respond to incidents varies. In the financial sector, organisations are required to report incidents to the Central Bank of Brazil (BACEN), according to their sectoral regulation (as is described further in D1.3), although participants again noted variation in the capability of financial-sector organisations to identify and report incidents. Similarly, telecommunications providers are required to notify cybersecurity incidents to their regulator, Anatel, by Resolution No. 740 of 2020, and organisations within the sector have varying capability to do so. CERT.br described variation in the levels of reporting and information shared by organisations within their constituency to them, with more mature organisations tending to systematically report and participate in information sharing, while smaller organisations may report only in cases where they require assistance.

There are some initiatives to support organisations in developing their incident-response capability. Participants reported that there is an initiative to create a centre of expertise to provide support to government organisations in identifying and addressing incidents, especially for organisations with lower levels of maturity and limited expert staff. Furthermore, subnational CERTs are supported in developing their capacity through events such as the Brazilian CSIRTs Forum, organised by CERT.br, which includes workshops and tutorials on topics such as SIM3 accreditation.[39] CERT.br possesses qualified SIM3 auditors and is working with the OpenCSIRT Foundation to create profiles for SIM3, against which CERT.br plans to accredit Brazilian CSIRTs starting from next year. CERT.br also assists new CSIRTs in establishing their activities in Brazil.

Since the 2020 CMM review, there have been initiatives to formalise the coordination of federal cyber incident management, and extend it voluntarily to public companies, mixed capital companies and their subsidiaries. The Federal Cyber Incident Management Network (ReGIC) was formally established in 2021 by Decree 10,748 of July 16th 2021,[40] in accordance with the provisions of the 2018 National Information Security Policy (although participants reported that in practice this network has been developing since 2006). This is a cross-government network of cyber incident response teams, coordinated by CTIR.gov, the aim of which is to improve coordination of incident-response between entities of the FPA.

According to the Decree that establishes ReGIC, the participation of "*direct, autonomous and foundational federal public administration bodies and entities*" in ReGIC is mandatory; the participation of "*public companies and federal mixed-capital companies and their subsidiaries*" is voluntary and occurs through membership. ReGIC aims *"to improve and maintain coordination between bodies and entities of the public administration for the prevention, handling, and response to cyber incidents to raise the level of cybersecurity resilience of its information assets. It aims to publicize cyber incident prevention, handling, and response measures; share alerts about cyber threats and vulnerabilities; disclose information*

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

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

about cyber-attacks; promote cooperation among Network participants and encourage speed in responding to cyber incidents".

In addition, in 2022 the Cyber Incident Management Plan for the federal public administration (PlanGIC) was approved by Ordinance GSI/PR 120[41] and came into force. This plan establishes the cyber incident-manag dement procedures to be observed by participants in the ReGIC network. According to PlanGIC, all participants in ReGIC must notify cyber incidents to CTIR.gov (or in the case of entities outside of the FPA that are voluntarily members, report to the sectoral coordination team to which they are linked). CTIR.gov shares alerts, information on threat and vulnerabilities, recommendations and statistics related to cyber incidents to members of the ReGIC network.

Outside of ReGIC, there is regular sharing of threat and vulnerability information within some sectors; however, this varies according to the level of regulation and cybersecurity capacity within the sector. For the telecommunications sector, the regulator Anatel reported maintaining a constant forum for the exchange of cyber threat intelligence (CTI) and vulnerability information amongst operators, with the involvement of other bodies such as the intelligence service, ABIN, via anonymised, efficient channels. The finance sector also reported a high level of CTI exchange amongst operators.

The Defence sector has its own Cyber Incident Management Sectorial Plan (PSGIC-Def), established through the MoD Ordinance #4174 of 16th August 2023, intended to guide the coordination of incident response between the incident-response teams of the MoD and the three armed forces. The plan reportedly seeks alignment with the best practices provided for in the SIM3 Model. A further MoD Ordinance (#4138 of 14th August 2023) establishes coordination roles between the Defence sector and ReGIC.

There is not yet an incident-reporting requirement consistent across all CI organisations in Brazil. As is described further in D1.3, progress towards cybersecurity regulation of the CI is being made under the National Critical Infrastructure Security Plan (PlanSIC), which outlines responsibilities and states that GSI is the coordinating body for CI cybersecurity activity. The requirements of PlanSIC are not yet fully implemented, but, it was reported, will eventually result in a regulated requirement for the CI to report cyber incidents. The ReGIC Decree also established in 2021 that the regulatory agencies in Brazil, Central Bank of Brazil and National Nuclear Energy Commission are responsible for establishing or designating a sectoral coordination team for "*prevention, treatment and response team to cyber incidents*" and that these bodies are responsible for "*coordinating cyber security activities and centralising incident notifications from other teams in the regulated sector*". Implementation of this requirement is underway.

Since reporting is not yet mandatory across the CI, CTIR.gov does not yet reliably receive cyber incident reports across the CI. Reports are received on an ad-hoc basis via voluntary participation of entities outside of the FPA in ReGIC, through informal relationships with sectoral CERTs and regulators (e.g., regular incident reports from Anatel, the authority for the telecommunications sector, to GSI were described), and through notification of relevant incidents by CERT.br. Representatives from the sectoral authorities in the review stated that currently, if a sectoral authority or CSIRT felt that an incident might have a cross-sector impact,

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

they would coordinate on an informal basis with the relevant sectors, supported by CERT.br or CTIR.gov.

This informal set of relationships is seen to be working well, but consideration needs to be given to whether these informal relationships would work in a complex cross-cutting cyber incident, how the roles of CTIR.gov and CERT.br could evolve to provide better collaboration across sectors, and whether there would be benefit in formalising CERT.br's cross-sector remit (i.e., the types of organisations that they are responsible for supporting). Table-top exercises might help to clarify these processes.

Further, while various mature CERTs have incident registries, these are not currently consolidated into a single list. This could make it harder to assess trends across the economy, or to reliably gain early warning of an incident that might affect multiple organisations. In practice, participants reported, strong coordination and trust-based relationships between the CSIRTs, particularly CERT.br and CTIR.gov, interacting on an as-needed basis (for example, with CERT.br notifying CTIR.gov of any incidents or threats identified that might impact government networks), mean that relevant information is exchanged and a sufficient overall picture is maintained by these two entities. There are reportedly also strong relationships between CTIR.gov and CERT.br, and the subnational CERTs, in terms of information exchange.

It is nonetheless important to verify that the current distributed registries are sufficiently coordinated to enable identification and categorisation of, and response to, a national-level cyber incident (i.e., an incident that leads or contributes to a crisis scenario) under the full range of possible scenarios and conditions. Further, it is important to ensure that visibility of cybersecurity incidents in Brazil is sufficiently coordinated to allow analysis of trends that can inform national strategy and the allocation of resources to cybersecurity activities.

Based on the findings from testing these aspects of the current arrangement, it might be beneficial to consider whether CTIR.gov or CERT.br should be given responsibility for maintaining a central registry. It is important to note that the provisions of PlanSIC describe reporting requirements for the CI that should eventually lead to a stronger ability of CTIR.gov to maintain a comprehensive registry of incident reports within the CI; these provisions are not yet fully implemented, however. It may also be beneficial to formalise the conditions and thresholds for information exchange and escalation, and the processes, and points of contact in place for exchange of information between CSIRTs, including points of contact and responsibilities, in order to ensure that all necessary functionality is institutionalised and can continue to operate in the case of a change of personnel, for example. The potential for the planned national cybersecurity agency to take on a facilitating role in regard to rapid information sharing and effective collaboration between the various national, regional and sectoral entities was suggested by participants in the CMM review.

Review participants reported that crisis management in Brazil is not centralised, but organised by sector, with each sector having its own crisis-management team that responds to crises affecting its sector. In addition, in the event of a cybersecurity-related crisis, GSI noted that an inter-agency committee would be created, with CTIR.gov also responsible for providing advice to GSI and the President's Office, and that they may provide support to activate a crisis room bringing together key stakeholders across sectors. There is, however, no formal integration of cybersecurity national crisis-management framework, nor has a cyber incident management authority been assigned.

Participants in the CMM review generally viewed the integration of cybersecurity into crisis management as being effective, having being strengthened through practice in both real-world events and exercising. In the last decade, Brazil has hosted several major world events, including the Pope's visit (2013), football World Cup (2014) and the Olympic Games (2016). The high level of coordination required to protect the CI against potential targeting has reportedly created strong expertise and relationships that, participants reported, underpin an effective system. It was also reported that Brazil has assisted other countries with capacity in this area: the example was given of assisting Peru in preparing their centre of cyber operations ahead of hosting the Pan-American Games in 2019.

The approach to cross-sector coordination is also tested regularly via a strong programme of crisis exercising. In particular, the Cyber Guardian Exercise, organised by the Cyber Defence Command (ComDCiber) in partnership with GSI, has been conducted annually since 2018. The exercise focuses on protection of the CI against cyber crisis scenarios, and on testing and training coordination between the public and private sectors in these scenarios. Scenarios are developed through discussions with stakeholders to agree on the most important incidents and conditions to test. Emergency-communications systems are in place and their effectiveness and resilience are tested through the exercise. Participants reported that this is the largest exercise of this type in the region, and that other countries in the region are frequent observers of the Brazilian exercise.

The first Cyber Guardian exercise in 2018 brought together the energy, nuclear and defence sectors; this has now expanded to involve a wide range of stakeholders (with reports of involvement from many of the stakeholders present in our CMM review) from the defence forces, CI (an objective of PlanSIC is to ensure that all CI sectors are involved in these exercises), government, private sector, and intelligence services. Participants reported that in the edition of the exercise running in October 2023, the intention is to involve the regulatory agencies, CSIRTs and representative organisations from all 14 CI sectors that have been identified in PlanSIC (see D1.3).

Cyber incidents can be cross-cutting and evolve very quickly, and as such the level of coordination necessary may require a higher degree of coordination than in other types of crisis. While the decentralised, regularly exercised approach is reported to be strong, it is therefore critical to continue to regularly test the capabilities of the various relevant entities to coordinate in the face of a wide range of potential cybersecurity scenarios. The findings from these exercises should be evaluated to establish regularly updated lessons learned. In establishing lessons learned, consideration should be given to whether it would be beneficial to assign a body responsible for coordinating cyber crisis management (and for supporting wider crisis-management processes in which there is a cybersecurity element), and/or to formally integrate cybersecurity into a broader crisis-management framework.

D1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

This Factor *studies the Government's capacity to identify CI assets, the regulatory requirements specific to the cybersecurity of CI, and the implementation of good cybersecurity practice by CI operators.*

***Stage*: Formative to Established**

The National Critical Infrastructure Security Plan (PlanSIC) was approved by Decree 11,200 in September 2022.[42] This describes implementation details and responsibilities for achieving the objectives of the National Critical Infrastructure Security Policy (Decree 9,573 approved in November 2018), and the National Critical Infrastructure Security Strategy (Decree 10,569 of December 2020), which details the strategic objectives in line with the Policy. GSI is stated to be the coordinating body for CI Security activity.

Through PlanSIC, progress is being made towards identifying the CI, coordinating and assigning responsibilities for its protection, and developing recommended cybersecurity standards for all CI sectors. Many elements of PlanSIC are not yet fully implemented, and as such cybersecurity is not yet regulated across all CI sectors. Technical groups composed of the relevant ministries and organisations for each of the CI sectors have been established to work towards these aims. We begin this section by describing the progress being made through PlanSIC, before describing the current state of CI regulation in Brazil.

PlanSIC identifies seven priority areas, within which 14 CI sectors are identified: Waters (CI sectors: Dams, Urban Water Supply. Responsible: Ministry of Regional Development); Energy (Electricity; Peganbio – Oil, Natural Gas and Biofuels. Responsible: Ministry of Mines and Energy); Transport (Terrestrial, Air, Waterway. Responsible: Ministry of Infrastructure); Communications (Telecommunications, Broadcasting, Postal Services. Responsible: Ministry of Communications); Finance (Responsible: Ministry of Economy); Biosafety and Bioprotection (Responsible: Ministry of Health), Defence (Responsible: Ministry of Defence). There are reportedly plans for the Digital Government sector to also be included as a priority area. It is intended that under PlanSIC, all of these identified CI sectors will eventually be regulated for cybersecurity.

In terms of cybersecurity standards for the CI, various responsibilities are outlined in PlanSIC. GSI is responsible for preparing guidance and regulation to encourage the adoption of standards and good practices in the CI. In particular, GSI reported work towards a bill of law to create a national policy on cybersecurity requirements. The policy that exists currently applies only for federal government organisations; it is intended that the new policy will expand this policy to create an overarching framework of minimum cybersecurity requirements for all CI sectors. GSI is also responsible for providing a consolidated guidance on regulations identified as relating to CI security on their institutional website.

It is intended that the sector regulators will adapt the cross-CI guidance and regulation prepared by GSI according to the needs of their sector. According to PlanSIC, the responsible ministries are responsible for preparing complementary guides for their respective priority

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

areas, as well as sectoral Critical Infrastructure Security plans, which will be forwarded to a new Critical Infrastructure Security Steering Committee for approval. These sectoral plans are intended to be complementary documents to PlanSIC, that address CI security actions according to the specificities of each sector, providing guidance on "*the desirable levels of protection, on the security activities to be carried out and on prioritization in resource allocation*".

Participants stated that the regulatory structure has not yet been decided; this is currently in the study phase included in the work of the established technical groups, and will be taken to congress for discussion. Some intended oversight responsibilities are described in PlanSIC, which states that GSI will be responsible for carrying out technical visits to monitor CI security activities, which may include the completion of checklists or questionnaires to guide follow-up actions. The National Critical Infrastructure Security Strategy also includes as a strategic objective to establish a governance structure for CI security; PlanSIC states that this objective will be met by establishing the Critical Infrastructure Security Steering Committee, which "*will be composed of a set of bodies responsible for articulating, guiding, proposing and managing the implementation of actions related to the Security of Critical Infrastructures, which will also seek to ensure compliance with the goals established in this Plan [PlanSIC]*". It is anticipated that this year (2023) a further decree will be approved, which formally establishes this management structure for CI security.

During the CMM review sessions, there was some debate amongst participants as to the relative benefits of assigning the competence to regulate cybersecurity across the CI sectors to a single body such as the planned national cybersecurity agency or GSI, or to developing the regulatory structure per sector. In the latter case, participants expressed the view that the agency or GSI might still play a valuable role in coordinating and supporting the individual CI-sector regulators, for example in the form of recommending minimal cross-sector cybersecurity standards. If the new national cybersecurity agency is to have a regulatory role, it will be important that its remit is clear, particularly in regard to how any cybersecurity regulatory responsibilities it takes on align with the regulatory activities of the sector regulators.

PlanSIC further states the aim to establish the Integrated Critical Infrastructure Security Data System (and further integration protocols between this system and CTIR.gov), an operational structure for the country's CI security, including secure information-sharing mechanisms to support cooperation between the public and private sector, tools for analysis of risks and interdependencies of CIs, and methodologies for identifying the CI continuously. This structure may therefore eventually be important to ensuring that the list of CI assets is kept up to date and can be adapted as necessary, and that interdependencies between sectors, in which digital infrastructures from one sector such as Finance may depend on the provision of services from another sector such as Telecommunications or Energy, for example, can be managed. Participants in the review reported ongoing work towards the identification and management of interdependencies between sectors, within the technical groups created on CI security. It was not clear from the review sessions or documented plans the extent to which cross-border dependencies (where which Brazilian CI assets may depend on the infrastructure of other nations) are being considered.

In practice, currently the level of cybersecurity regulation varies across different CI sectors. Cybersecurity requirements are provided by some sector regulators, each of which has autonomy in terms of the management of their sector in relation to cybersecurity, with

varying levels of requirement and compliance-monitoring as a result. The FPA, and financial and telecommunications sectors were considered by participants to be the most advanced sectors in this regard.

The DSIC of GSI proposes mandatory requirements for the cybersecurity of the FPA. Cybersecurity in the FPA is overseen by the Federal Court of Accounts (TCU), which performs audits in line with the regulation. All federal institutions are required to conduct cyber risk assessments, updated annually based on lessons learned from larger incidents. Normative Instruction GSI/PR 3 (May 2021) provides for processes related to information-security risk management in FPA bodies and entities. According to PlanGIC, all participants in the Federal Cyber Incident Management Network (ReGIC, which, as described in D1.2, mandatorily includes all entities of the FPA) must notify cyber incidents to CTIR.gov. Regular benchmark exercises are also conducted by the Bureau of Information Technology Audit (Sefti/TCI) to measure cybersecurity development in the FPA.

For the financial sector, the Central Bank (BACEN)'s Resolutions No. 4,658[43] (2018), No. 4,893 and No. 85 (both enacted in 2021) regulate the adoption of cybersecurity measures. The regulations require financial institutions to adopt controls and procedures for preventing and responding to cybersecurity incidents, and appoint an officer responsible for overseeing their cybersecurity policies. Financial institutions' compliance with the regulation is audited by BACEN. Financial institutions are also required to notify BACEN in case of data breach (although deadlines are not specified), and to report annually to BACEN disclosing any cybersecurity incidents.[44] Resolution No. 4,658 also establishes requirements for contracting services of data processing, data storage and cloud computing.

For the telecommunications sector, which is regulated by Anatel, Resolution No. 740 of 2020 established cybersecurity regulation which, participants reported, was an evolution of previous regulations for the sector.[45] Each telecommunications company in Brazil is required to identify its assets, perform regular vulnerability tests, adopt standards and good practices in cybersecurity, and develop a cyber risk-management plan, cybersecurity training policy, and clear incident-response processes. The Resolution also establishes that cybersecurity incidents must be notified to Anatel, and includes provisions on audit for the supply chain of the major telecommunications service providers. Anatel runs a working group with the major telecommunications operators to keep up-to-date on the management of cybersecurity risks, including analysing risks relating to more recent technological developments such as 5G. Anatel noted that, with approximately 1,500 telecommunications service providers in the country, it is not possible to perform audits for all operators, and audit is prioritised from a risk-management perspective.

In both the financial and telecommunications sectors, the guidelines do not contain prescriptive technical requirements, but state that each institution should establish its own cybersecurity policy and maintain an incident-response plan. Some participants from the financial sector noted that it might be beneficial to have a more prescriptive basis that could be used by different sectors and infrastructures in terms of technical and cryptographic standards and controls.

[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
[45] https://www.in.gov.br/web/dou/-/resolucao-n-740-de-21-de-dezembro-de-2020-296152776

Outside of the finance and telecommunications sectors, mandatory requirements for cybersecurity are not yet implemented. In some sectors, requirements have been set, but compliance is not yet monitored. For example, for the Energy sector, Resolution 964 of December 2021 came into force in July 2022, and sets requirements for the adoption of standards and good practices, cyber-incident notification, and threat-information sharing.[46] Compliance is not yet assessed; the Resolution states that it will be subject to regulatory assessment after seven years of validity. All sectors have mandatory requirements for case of breaches of personal data: under the General Personal Data Protection Law which took effect in August 2020 (see D4.2), breaches of personal data must be reported by any Brazilian institution to the National Data Protection Authority (ANPD) and the data subject.

In terms of sharing threat and vulnerability information, direct, autonomous and foundational federal public administration institutions are mandated to participate in the Federal Cyber Incident Management Network, ReGIC, through which threat, incident and vulnerability information is shared, with some other organisations, such as federal public companies and mixed-capital companies, participating voluntarily. Threat-information sharing mechanisms are also in place within some sectors outside of the FPA. For example, for the telecommunications sector, there is a working group established by Anatel run using a MISP platform in which major and medium-sized operators share information about threats and vulnerabilities. This working group was established by regulation and promotes cooperation of different operators. For the financial sector, the Brazilian Federation of Banks (Febraban) creates working groups for cyber-threat intelligence (CTI) sharing using platforms such as MISP, and reported also sharing information with other sectors. Similarly, companies from the oil and gas sector reported participating in CTI-sharing networks through MISP platforms, sharing with a number of other institutions from the sector as well as organisations from the financial, educational and retail sectors. Participants from the financial sector also reported participating in international CTI-sharing networks: the Financial Services Information Sharing and Analysis Center (FS-ISAC). As described, it is intended that the Integrated Critical Infrastructure Security Data System will also eventually support and formalise the channels for CTI sharing across CI organisations.

Within the regulated CI sectors, operators implement good cybersecurity practice. Outside of these sectors, participants reported that there is implementation of cybersecurity good practice, and self-assessment against recognised industry standards, by many organisations, but the level of course varies across organisations. As described in D1.2.3, CI operators participate fully in national incident response and crisis-management exercises; in particular, the Cyber Guardian exercise.

[46] https://www.in.gov.br/en/web/dou/-/resolucao-normativa-aneel-n-964-de-14-de-dezembro-%20de-2021-369359262

D1.4 CYBERSECURITY IN DEFENCE AND NATIONAL SECURITY

This Factor explores whether the government has the capacity to design and implement a strategy for cybersecurity within national security and defence. It also reviews the level of cybersecurity capability within the national security and defence establishment, and the collaboration arrangements on cybersecurity between civil and defence entities.

Stage: Established

Several policies and doctrines exist for cybersecurity in national defence. The Cyber Defence Policy was released in 2012, and the first Cyber Defence Doctrine was approved in 2014. Cyber has also been identified in the National Defence Strategy as one of three strategic priorities, alongside nuclear and space, since 2008. According to the National Defence Strategy, the key national defence capabilities are protection, prompt response, and deterrence, and this is the basis for defining the priorities for cyber defence. These key strategic documents are supported by operational doctrines and field manuals.

At the end of 2020, new doctrinal and organisational acts were established for cyber defence: in particular, the new joint operations manual (Normative Ordinance #84/GM-MD, of 15 Sep 2020), which includes chapters on cyber defence: Chapter VII – Cyber Defense Command and Chapter XII – Cyber Warfare in Joint Operations. These chapters define the priority of using cyber as an operational tool, in addition to its alignment with Intelligence concepts, Command and Control (C2) and Information Operations. Participants also stated that the Cyber Defence Policy of 2014 is currently being updated. Participants reported that important decrees and legal instruments since 2020, in particular Normative Ordinance #3781/GM-MD, of 17 Nov 2020, have led to more consistent implementation of doctrine, and a better capacity to engage internationally.

Cyber-defence capabilities and organisational structures are in place in Brazil. There are cyber units within each of the three forces (Navy, Army and Air Force). The Army created its Strategic Programme for Cyber Defence in 2010, establishing its Cyber Defence Center (CDCiber). The MoD created the Cyber Defence Programme in 2014, which sought to improve the interoperability of cyber defence among the forces. Based on directives issued by the MoD within the framework of this programme, the Cyber Defence Command (ComDCiber, the joint cyber operational command operational since 2016) and the National School of Cyber Defence were established. Participants noted that the expansion of cyber-defence capabilities around this time was motivated in part by the major sporting events hosted by Brazil (the 2014 football world cup and 2016 Olympics).

The role of ComDCiber as a joint command in cyber defence has been boosted by developments in the last few years; in particular, definition of the organisation of ComDCiber in the 2020 joint operations manual, and provisions made in Normative Ordinance #3781/GM-MD of 17 Nov 2020, which affirms ComDCiber as a joint command, permanently activated, and the central body of the SMDC. The budget provided to ComDCiber through the MoD has reportedly also improved.

The Cyber Defence Military System (SMDC) was created be the MoD to set up the overarching institutional structure to coordinate Brazil's cyber defence efforts. It is composed of ComDCiber, the National School of Cyber Defence, and CDCiber. SMDC organises training of the cyber defence forces, and develops and updates the cyber-defence doctrines and policies.

The National Cyber Defence School via the SMDS provides training to the joint command and officers from the cyber units of the three forces, by contracting specialised trainers and programmes from Brazil and overseas. There is also training provided separately to the cyber units of the three forces: the Air Force for example has performed and catalogued a training needs assessment and reported providing additional training to its officers on this basis. The Brazilian Intelligence Agency (ABIN) also reported applying specialist intelligence resources to provide support for cyber training and operations of the defence forces. Participants described cyber training delivered by Brazilian teaching institutions, mainly from the Army's training school, to foreign military officers, with approximately 75 foreign officers having been trained in Brazil as of last year.

There are currently no cybersecurity elements included in the training of the wider military forces, outside of these cyber units, but this is reportedly planned for the future in order to increase the defence force cybersecurity awareness. Training the wider forces will be increasingly important as cyber becomes increasingly relevant to a whole range of different military scenarios.

Exercises were highlighted as a critical part of cyber-defence training. The AZUVER exercise is an annual exercise for the joint training of the three services and involves cyber scenarios. Participants reported that joint Capture-the-Flag (CTF) exercises are run for the three forces' cyber units. The Cyber Guardian exercise, organised by ComDCiber in partnership with GSI, is another critical training exercise for the defence forces alongside various other Brazilian stakeholders from the CI, government, private sector, and ABIN which is described in further detail in D1.2, in the context of crisis management. Participants described this as the most important training exercise for the cyber defence forces in regard to engaging with and assisting in the protection of CI.

Mechanisms to facilitate collaboration with allies on cyber defence are trained and tested through international exercises. Since 2018, Brazil has engaged in the annual Locked Shields cyber defence exercise organised by the North Atlantic Treaty Organisation (NATO) Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn. ComDCiber also participates in international meetings including the annual meetings of the Iberoamerican Cyberdefence Forum, of which Brazil is currently holding the secretariat, and other meetings between Cyber Defence Commanders that are organised in different countries. As was described in D1.1, Brazilian representatives, including the joint cyber operational command of the defence forces, ComDCiber, are actively engaged in the global debate on international humanitarian law and norms of behaviour via the UN OEWG and GGE. Going forward, to reach the higher stages of maturity of the CMM, it is important to consider how Brazilian cyber-defence strategy can be designed to contribute to promote stability in cyberspace, including measures to predict and influence the strategies, actions and reactions of potential allies and adversaries.

Resources for cyber defence are arranged between the various forces and institutions and the MoD on an annual basis. Participants described challenges arising from not yet having a multi-annual budget for cyber defence. Challenges were also described arising from more limited budget being given to cyber defence compared with other programmes (comparison with the strategic programmes for the Army and Air Force were given, which reportedly have much larger, more stable budgets), leading to limited resource available to purchase training programmes and equipment.

Participants reported an aim to develop capacity-based planning to allocate dedicated resources for cyber defence. It will be important to establish these processes, enabling review of current resourcing against a range of plausible scenarios (which might be supported by the broader national assessment of cybersecurity risks, and consideration of other demands that might be placed on the cyber forces) in order to ensure that the right budgets are in place. To increase the availability of skilled personnel, it may be beneficial to consider establishing a cyber reserve force or other mechanism that would enable the defence community to draw on the cybersecurity skills and capabilities of the broader society.

It was reported that since the CMM 2020, the coordination between the civil and defence entities has been improved, through increased integration between CI and defence entities. The responsibility of the MoD in regard to protecting CI has been formalised through the CI Security Plan (PlanSIC), which, although not yet fully implemented, states that the implementation of PlanSIC and the developing sectoral security plans (described in D1.3) will have the support of the MoD. PlanSIC also assigns the MoD as responsible for involving the CI sectors in the Cyber Guardian exercises, which the MoD carries out through ComDCiber.

Given that the sectoral CI security plans are currently under development, the specific responsibilities of the defence entities in regard to the assisting in the protection of the various CI sectors have not yet been formalised. Similarly, the respective roles of the defence entities within cyber crisis-management are not yet formalised. As such (and also due to a lack of capacity-based resource planning for the cyber defence programme currently, as described above) the resources required by the cyber defence entities to support civil and CI authorities have not yet been formally assigned.

Despite the specific responsibilities and budget not having yet been formalised, various examples of coordination between defence and civil entities were given; for example defence entities having assisted CI sectors and the government in the case of significant cyber-incidents. The intelligence service, ABIN, exchanges information on threats, including relating to cyber-espionage and Advanced Persistent Threats (APTs) with international counterparts, and supports the defence forces as well as CTIR.gov, the CI and other organisations with intelligence as relevant. This reportedly includes two-way information-exchange partnerships with public and private companies, as well as participation in various CTI-exchange groups including for the government, financial and academic sectors. Participants described the benefits of the annual Cyber Guardian exercise to training and testing the various roles of the CI and defence stakeholders for the event of a cyber crisis.

Initiatives are underway to improve understanding of the dependence of national security and military entities on the cybersecurity of other parts of the CI. As described in D1.3, various technical groups are currently studying security for the CI sectors identified in PlanSIC; defence being one identified CI sector under the responsibility of the MoD. The technical

groups that are currently involved in studying the interdependence between CI sectors, including the dependence of the military on other sectors, include representatives from the MoD and three armed forces. It was reported that these studies will produce an output in the next few years. The studies should eventually inform the Cyber Defence Policy or Doctrine, as well as the development of formal mechanisms to regularly identify and manage these interdependencies.

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the Government of Brazil. These recommendations provide advice and steps aimed at increasing existing cybersecurity capacity in line with the considerations of the GCSCC's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each *Factor*.

NATIONAL CYBERSECURITY STRATEGY

Since the NCS renewal processes are soon to begin, the following recommendations are made for the renewal of the NCS:

R1.1.1 Develop and publish a revised NCS through a process that involves consultations with key stakeholder groups including representatives from the government, private sector, civil society and international partners. The development of the new NCS should also be guided by an evaluation of the progress made against the current NCS, and a refreshed assessment of national cybersecurity risk (which updates the "diagnosis" of risk that is included in the current NCS). The development of the NCS may also be guided by recommendations from this CMM review.

R1.1.2 When refreshing the assessment of national cybersecurity risk, consult with relevant stakeholders from groups including the CI, national security community and private sector, and ensure that the process takes into account the cybersecurity risks arising from the use of emerging technologies within critical infrastructure and wider society. The process may also draw on insights on cyber-incidents and threats shared within information-sharing networks. Consider putting in place a process for regularly refreshing the risk assessment in light of a changing threat and technology landscape.

R1.1.3 In drafting the NCS and as part of the consultation processes, give consideration to how the NCS might incorporate or support wider online policy objectives such as: child protection; the promotion of human rights; the promotion of equality, diversity and inclusion; and managing disinformation. Ensure that this is clearly indicated in the NCS.

R1.1.4 Develop and publish a detailed NCS Action Plan for the new NCS, describing an implementation programme that covers the scope of the strategy. This plan should assign actions within the programme to specific "owners" (relevant stakeholders across government and other sectors). Ensure that a process is in place to allocating budget to delivering the various components of the strategy, and for identifying, escalating and mitigating the impact of any budget shortfalls.

R1.1.5 Assign a coordinating body for the national strategy implementation programme, and ensure that this body has sufficient authority to ensure that action "owners" are held to account. Noting the potential for the new national cybersecurity agency to take on this coordinating role, it is important that the role of the agency is clearly defined: the extent to which is has a strategic oversight role, an operational delivery role, or both. It is also important to clearly define how its responsibilities interact with other security and regulatory functions in government.

R1.1.6 Define within the NCS key outcomes against which success can be measured, and put in place review processes and mechanisms to enable strategy 'owners' to monitor achievement of these NCS outcomes, address implementation issues and escalate risks, issues and dependencies to the relevant authorities. The NCS validation efforts that are currently taking place might provide support for the definition of progress metrics and review processes. Ensure that these processes are adequately funded.

R1.1.7 Define outcome-oriented metrics that can be used to monitor the impact that the programme is having on risk and harm reduction. Use these metrics to continuously refine the Action Plan, and to inform funding and priority decisions.

R1.1.8 Ensure review and renewal processes for the next NCS are formally in place. These processes should describe how to identify lessons learnt from the current implementation of the strategy.

R1.1.9 Ensure that the NCS content takes account of the cybersecurity risks arising from the use of emerging technologies within critical infrastructure, and the wider economy and society. Put in place processes to regularly assess emerging cybersecurity risks and use the results to update the NCS and Action Plan.

R1.1.10 Regularly consult all relevant stakeholders to refine and update international-engagement objectives: for example, Brazil might aim to eventually expand its objectives around building international communities of interest around specific cybersecurity policy goals, and more active involvement in building cybersecurity capacity in other countries. Ensure that there is regular validation that the objectives in this area are clear and understood by all participants involved, and that there is a process in place to monitor the achievement of objectives.

R1.2.1 Test the ability of the distributed system of CERTs to function in the event of a major cross-sector cyber incident or crisis. Practical and table-top exercises might help to clarify these processes. It is important that this capability is tested against the wide range of potential cybersecurity scenarios that the country could face, and that exercises take account of changes in the technology and threat landscape. Based on continuous evaluation of lessons learned from these tests, it might be valuable to:

- Consider how the roles of CTIR.gov and CERT.br could evolve to provide better collaboration across sectors, including whether there would be benefit in formalising CERT.br's cross-sector remit (i.e., the types of organisations that they are responsible for supporting);
- Consider formalising the conditions, thresholds and processes for information exchange and escalation between CERTs, including definition of the points of contact and responsibilities, in order to ensure that all necessary functionality is institutionalised and can continue to operate in the case of a change of personnel, for example.

R1.2.2 Verify that the current distributed cyber-incident registries are sufficiently coordinated to enable identification and categorisation of, and response to, a national-level cyber incident under the full range of possible scenarios and conditions. This assessment might be included in the tests described in D1.2.1. Further, it is important to ensure that visibility of cybersecurity incidents in Brazil is sufficiently coordinated to allow analysis of threat trends, risks, harms and losses that can inform national strategy and the allocation of resources to cybersecurity activities.

R1.2.3 Based on the findings from the assessment described in D1.2.3, it might be valuable to consider whether CTIR.gov or CERT.br should be given responsibility for maintaining a central registry of cyber incidents.

R1.2.4 Consider what facilitating role the planned national cybersecurity agency might play in regard to Recommendations R1.2.1 to R1.2.3.

R1.2.5 Continue to regularly exercise the capabilities of the various relevant entities to coordinate in the face of a wide range of potential cybersecurity crisis scenarios, and to coordinate with other sectors in the case of a wider crisis with cybersecurity components. The findings from these exercises should be evaluated to establish regularly updated lessons learned. In establishing lessons learned, consideration should be given to whether it would be beneficial to assign a body responsible for coordinating cyber crisis management (and for supporting wider crisis-management processes in which there is a cybersecurity element), and/or to formally integrate cybersecurity into a broader crisis-management framework.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.3.1 Finalise and issue cybersecurity regulatory requirements for all of the CI sectors identified in PlanSIC. These requirements should include appropriate cybersecurity standards that must be met, and mandatory breach reporting and vulnerability-disclosure requirements.

R1.3.2 Put in place formal processes to evaluate CI operator compliance with regulatory standards and incident and vulnerability disclosure. As noted, discussions are ongoing as to the regulatory structure that will be adopted. It will be important to consider the following in establishing the regulatory structure:

- Ensuring that sufficient consultation processes are undertaken to meet the needs of the regulators of and organisations within the CI sectors, particularly in regard to the potential benefits of a cross-CI regulation monitored by a single body versus sector-based regulation.
- If any body is to take on a cross-sector regulatory role, as was suggested might be the case, ensuring that its remit is clear, particularly in regard to its responsibilities it takes on align with the existing regulatory activities of the sector regulators.

R1.3.3 Continue work on identifying interdependencies between CI sectors, to understand potential supply-chain and systemic risks and improve the ability to quickly identify risk aggregation. Formally document these dependencies and the approach to managing them.

R1.3.4 Identify cross-border dependencies, in which Brazilian CI assets may depend on the infrastructure of other nations. Formally document these dependencies and the approach to managing them.

R1.3.5 Consider how to increase the sharing of threat and vulnerability information between all CI sectors, in order to ensure that all necessary CI organisations are in receipt of relevant information. This might involve consultations to understand current strengths and challenges. Approaches might include creating further formal structures for information sharing between all CI sectors automatically (e.g., using MISP platforms); approaches to building relationships and trust to support information sharing; and regulatory requirements.

R1.3.6 Put in place regular review processes to ensure that the list of CI assets identified in PlanSIC can adapt to shifts in the technical and the socio-economic environment.

CYBERSECURITY IN DEFENCE AND NATIONAL SECURITY

R1.4.1 Put in place regular consultation and review processes to ensure that cyber-defence strategy and doctrine are adaptive to changing capabilities and to the evolving geo-political and threat environment.

R1.4.2 Consider how Brazilian cyber-defence strategy can be designed to contribute to promote stability in cyberspace, including measures to predict and influence the strategies, actions and reactions of potential allies and adversaries.

R1.4.3 Develop cybersecurity elements within the wider operational and command training within the military forces, in order to increase cybersecurity awareness across the defence forces.

R1.4.4 Establish capacity-based planning processes to support the allocation of resources for cyber defence. These might include a review of current resourcing against a range of plausible scenarios (which might be supported by the broader national assessment of cybersecurity risks, and consideration of other demands that might be placed on the cyber forces) in order to ensure that the right budgets are in place.

R1.4.5 Consider establishing mechanisms that enable defence and the national security community to draw on the cybersecurity skills and capabilities of the broader economy and society (for example, via a formal cyber reserve force).

R1.4.6 Formalise the specific roles and responsibilities of the cyber-defence entities in regard to assisting in the protection of the various CI sectors, and within the country's crisis-management procedures. Ensure that the budget allocated in R1.4.5 includes the resources required to support civil and CI authorities.

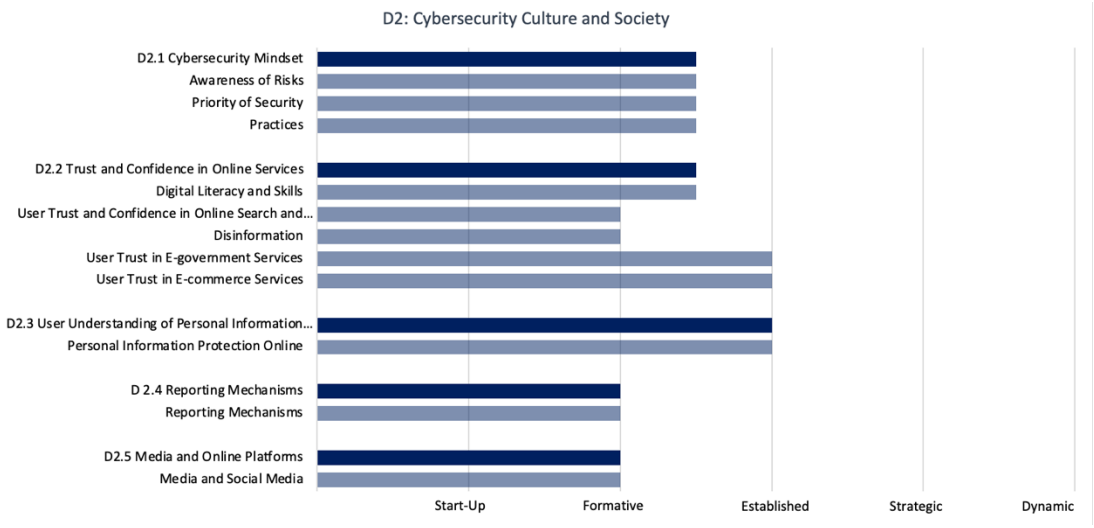
R1.4.7 Complete the ongoing identification of the dependence of national security and military entities on the cybersecurity of other parts of the CI. Develop formal mechanisms for regularly revisiting the identification and management of these dependencies. Use the results to inform cyber-defence policy and doctrine.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

This *Dimension* reviews important elements of a responsible cybersecurity culture such as the understanding of cyber-related risks in society, the level of trust in Internet services, e-government and e-commerce services, and users' understanding of personal information protection online. Moreover, this *Dimension* explores the existence of reporting mechanisms that function as channels for users to report cybercrime. In addition, this *Dimension* reviews the role of media and social media in shaping cybersecurity values, attitudes and behaviour.

Figure 7: Factors and aspects examined in Dimension 2.

OVERVIEW OF RESULTS



D2.1 CYBERSECURITY MINDSET

This Factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society at large. A cybersecurity mindset consists of values, attitudes and practices–including habits of individual users, experts, and other actors–in the cybersecurity ecosystem that increase the capacity of users to protect themselves online.

***Stage*: Formative to Established**

Stakeholder discussions indicated the presence of initiatives addressing the awareness of cybersecurity risks within all government agencies. Furthermore, several discussions with stakeholders also indicated that some agencies proactively attempt to anticipate new cybersecurity risks. A materialisation thereof may, for example, be seen in the plans to establish a central government agency for cybersecurity, in order to better coordinate government agencies' cybersecurity activities including anticipation of risks.

While the legal provisions and government procedures back this view, more critical perceptions of the cybersecurity risk awareness within government agencies may also be found. For example, a report released by the *Tribunal de Contas de União* lists shortcomings in many public agencies where basic cybersecurity mechanisms are concerned.[47] The report

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

"points to cybersecurity actions that need to be urgently implemented by federal agencies. These include the need for public managers to take inventory and control of corporate IT equipment and software; the provision of ongoing vulnerability and incident response management; and the establishment of programs for security awareness and training".[48] The criticised lack of activity by corporate managers in the public sector points toward a mismatch between awareness raising initiatives within government agencies and the actual level of awareness with respect to cybersecurity risks. Furthermore, it indicates that while overall the government is aiming at making cybersecurity a priority within the public sector, the actual situation within some government agencies varies strongly, including significant gaps within some agencies.

Similarly, safe cybersecurity practice does not seem to be adequately implemented, despite guidance and procedures being present. Therefore, it would be useful to implement a monitoring framework across all public sector entities, which could for example be coordinated by a central cybersecurity agency.

For the reasons outlined, the public sector currently would be assessed as being on Established level, with some outliers towards Formative on the one side but also strong indicators for some agencies having reached Strategic level. With respect to the level of Federal States with respect to cybersecurity, no consistent picture could be presented. Some states are more advanced that others and, therefore, cybersecurity awareness, priority of security, and practices should not only be considered on a federal level but also a higher level of systematic and coordinated activities are required on the state and even communal level– in particular. Initiatives on the state and communal level should also be registered and monitored by a federal level entity, such as a designated cybersecurity agency.

With respect to the private sector, the level of awareness varies depending on the size of companies, as is often the case in most countries. Stakeholders indicated that major public and private companies have a very high level of cybersecurity awareness, make cybersecurity a priority, also implement safe cybersecurity practices. In particular, publicly owned private companies have a very high level of compliance with respect to cybersecurity practices and have indicated implementing cybersecurity with priority and working on a general level of awareness across their enterprises.

However, small and medium businesses lack resources and knowledge with respect to cybersecurity practices and, due to financial reasons, cybersecurity is rarely a priority. Furthermore, no specific awareness raising campaigns were mentioned that target small and medium enterprises. With respect to larger companies Brazil's level for this factor might be Established to Strategic. However, with respect to smaller companies, the level may not be assessed as higher than Formative. It is unclear, whether the responsibility for small and medium businesses should lie with the federal or the state level–in any case, systematic monitoring, including surveys and metrics, should be collected and collated through a designated entity on the federal level.

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

The varying level of cybersecurity awareness and practice depending on the federal state has also been highlighted by cybersecurity professionals quoted in an article in *Intelligent CIO*:[49] *"The cause of the irregularity in cybersecurity investments in different national territories is a consensus among specialists"*, highlighting a *"lack of communication between the public and private sectors"*. The article further claims there is a lack of collective awareness with respect to cybersecurity awareness and adequate measures between military forces, intelligence, government agencies, and companies.

Other countries have encountered a reserved attitude from private companies to collaborate directly with the military or intelligence sectors, which might also be the case for Brazil. Therefore, it might be useful to attempt establishing a collective approach towards cybersecurity awareness and good practices by means of a (semi-)governmental entity separate from these institutions, within which such a collaboration can take place. Furthermore, stakeholders have raised the issue of bringing all entities from different sectors together, despite legislation supporting such an approach. This might be resolved by means of the approach outlined earlier. Additionally, due to Brazil's federal structure, it might be useful to consider setting up similar bodies with dedicated responsibilities on the state level, which collaborate with a federal-level entity.

With respect to Internet users' awareness, their knowledge with respect to safe practices, and their prioritisation of cybersecurity, stakeholders did not point to any systematic surveys, metrics, or further indicators / sources of information that could provide a partial or complete picture. Therefore, it is essential that Brazil conducts systematic surveys and collects metrics on this–while the ownership for this problem could lie with a dedicated cybersecurity entity on the federal level, the conduct of such surveys could be outsourced to universities and federal states could also conduct state-level surveys in order to receive a clearer picture of the situation within their respective state. Such a set-up would also enable states to add aspects to surveys and metrics relevant for their specific environment.

Due to the absence of metrics or surveys, the level of maturity with respect to Internet users cannot be assessed as higher than Formative. According to participants at the stakeholder meetings, many people do not assign sufficient importance to the problem of cybersecurity. Due to various initiatives aiming also at end-users listed under Dimension 3, it may be assessed that a limited but growing proportion of Internet users have a minimum level of awareness with respect to cybersecurity risks and also follow safe practices. Surveys may be available in an ad-hoc manner, for example with respect to cybercrime cases in the broad population (see Dimension 4) but they lack the depth and breadth envisioned within Factor D 2.1 Cybersecurity Mindset. Therefore, the level of maturity with respect to Internet users for this Factor cannot be assessed higher than Formative.

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

D2.2 TRUST AND CONFIDENCE IN ONLINE SERVICES

This Factor *reviews critical skills, the management of disinformation, the level of users' trust and confidence in the use of online services in general, and of e-government and e-commerce services in particular.*

***Stage*: Formative to Established**

As outlined under the previous Factor, no large-scale surveys or metrics are available that would provide information on users' awareness and behaviour online, and how they might vary across different segments of the public. Therefore, also, the level of trust and confidence of Internet users cannot be assessed with certainty and respective surveys should be conducted, including relevant metrics.

Due to various initiatives, it may be assumed that users' level of trust and confidence in online services is at a Formative stage. These initiatives are often aimed at younger people, for example students of university or pupils of schools and teenagers in general but also parents. However, some programmes also include awareness for users in general as well as for people above the age of 60, who often exhibit higher levels of uncertainty over the use of the internet and social media. Some major actors with respect to these initiatives are shortly outlined in the following:

- *CGI.br* is the Internet Steering committee in Brazil and *"has the task of establishing strategic guidelines related to the use and development of the Internet in Brazil and guidelines for the execution of the registration of Domain Names, allocation of IP Address (IP) Address (Internet Protocol) and administration relevant to the First Level Domain ".br". It also promotes studies and recommends procedures for Internet security and proposes research and development programs";*[50]
- *CERT.br* is a national CSIRT *"of Last Appeal, maintained by NIC.br, and provides services in the area of information security incident handling for any network that uses resources managed by NIC.br"*;[51]
- *RNP.br* is *"the Brazilian network for education and research"* and connects *"more than 4 million Brazilian students, professors and researchers in universities, educational and cultural institutes, research agencies, teaching hospitals, technological parks and hubs"*.[52]

NIC.br runs a portal promoting safe Internet use called *internetsegura.br*.[53] It addresses children, adolescents, parents and educators, people above the age of 60, technicians and

[50] "About CGI.br", CGI.br, accessed 22 October 2023, translated by *Firefox Fullpage Translation*, https://cgi.br/sobre/.

[51] "About CERT.br", CERT.be, accessed 22 October 2023, translated by *Firefox Fullpage Translation*, https://cert.br/.

[52] "Who we are", RNP.br, accessed 22 October 2023, https://www.rnp.br/en/about/who-we-are.

[53] "Safe Internet", internetsegura.br, accessed on 22 October 2023, translated by *Firefox Fullpage Translation*, https://internetsegura.br/.

generally interested Internet users. A presentation by CERT.br further lists a number of awareness initiatives addressing a semi-technical audience and referring to the aforementioned awareness raising initiatives for the general public.[54] Due to this evidence, the level of maturity for Factor D 2.2 Trust and Confidence in Online Services with respect to users' general behaviour when interacting with online services may be assessed to be minimally Formative.

Systematic metrics and surveys as well as a broad campaign addressing the public would presumably quickly lead to achieving Established stage. The initiatives also address disinformation, which means that also with respect to this Aspect at least Formative stage is achieved. A stronger involvement of the government in programmes to strengthen the public's preparedness against online disinformation would be helpful. Such an involvement could, for example, materialise by means of stronger financial support and broad promotion also through government channels of the aforementioned initiatives by NIC.br and CERT.br.

With respect to e-government and digital government, Brazil already reached a high level in the previous CMM Report dating back to 2020. No particular additions were mentioned by stakeholders and a major assessment basis, a report by the OECD on Brazil's digital government from 2018, has not yet been updated.[55] With respect to user trust in e-government services, Brazil's stage remains at the Established level.

Also with respect to e-commerce services the situation remains on a high level, as already indicated by the CMM Report in 2020. Stakeholders have indicated that, in particular, the high level of electronic bank transactions speaks for a high level of users' trust in e-commerce services. According to stakeholders, in 2019, 48% of all bank transactions took place online and the number has doubled since that time. Furthermore, banks have introduced a new and secure system for instant online transactions. It has been well received by users. It would be useful if the private sector would conduct surveys and define metrics in order to underpin and refine these claims and for Brazil to reach Strategic stage with respect to e-commerce.

D2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

This Factor *looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protecting personal information online, and whether they are sensitive of their privacy rights.*

***Stage*: Established**

[54] "Security Awareness Initiatives in Brazil", CERT.br, accessed on 22 October 2023, https://cert.br/docs/palestras/certbr-natcsirt2023.pdf.
[55] "Digital Government Review of Brazil: Towards the Digital Transformation of the Public Sector", OECD, 2018.

The users' understanding of personal information protection online has to be reviewed on the background of a new General Personal Data Protection Law (LGPD).[56] It is a comprehensive personal data protection law and broadly aligns with the EU's GDPR. The law requires privacy policies to be developed, both for the private and public sector. The development as well as the implementation of the law has led to a public debate on data protection taking place.

The *Autoridade Nacional de Proteção de Dados* (ANPD) is the national oversight body for personal data protection and also runs awareness initiatives.[57,58] The activities of ANPD together with the implementation and oversight of LGPD indicate that a growing proportion of users has skills to manage their privacy online. This is also backed by media reporting on the issue.[59] Therefore, Brazil clearly reached an Established stage with regards to this Factor.

D2.4 REPORTING MECHANISMS

This Factor *explores the existence of reporting mechanisms that function as channels for users to report Internet-related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.*

***Stage*: Formative**

The Centre for Prevention, Treatment, and Response to Cyber Government Incidents (CTIR) provides reporting mechanisms for governmental institutions.[60] Furthermore, sectorial CERTs provide reporting mechanisms for the private sector. CERT.br acts as a national-level CSIRT of last appeal, where also generally users may report incidents. However, these reporting mechanisms for the general public are not widely promoted and its target audience is not the general public, it is rather the last resort that "catches all" who have no other place to turn to. Therefore, a platform and entity that specifically aims at Internet users in general, and potentially also SMEs, should be established. A dedicated cybersecurity agency could, for example, take up this role and also promote this service among Internet users. There are also no centralised metrics available that would concatenate all incidents reported systematically from the private sector, public sector, and Internet users in general. Therefore, Brazil currently sits at a Formative stage.

[56] "General Personal Data Protection Act (LGPD)", lgpd-brazil.info, accessed on 22 October 2023, https://lgpd-brazil.info/.
[57] "Autoridade Nacional de Proteção de Dados", ANPD, accessed on 22 October 2023, https://www.gov.br/anpd/pt-br.
[58] "How to protect your personal data", ANPD, accessed on 22 October 2023, https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_senacon_ingles.pdf.
[59] Angelica Mari, "Data privacy awareness grows in Brazil", ZDNET, 15 May 2020, https://www.zdnet.com/article/data-privacy-awareness-grows-in-brazil/.
[60] "Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo", CTIR, accessed on 22 October 2023, https://www.gov.br/ctir/pt-br.

D2.5 MEDIA AND ONLINE PLATFORMS

This Factor *explores whether cybersecurity is a common subject of discussion across mainstream media, and an issue for broad discussion on social media. Moreover, this* Factor *looks at the role of media in conveying information about cybersecurity to the public, thus shaping citizens' cybersecurity values, attitudes and online behaviour.*

***Stage*: Formative**

Stakeholders indicated that media coverage is mostly dedicated to financial fraud. Furthermore, larger cybersecurity incidents in the private and public sectors are covered by the media. However, media reporting could be broader and also inform citizens in order to increase their awareness and promote best practices. Furthermore, the discussions on social media happen in an ad-hoc manner. Brazil does not have a positive whistleblowing culture and, therefore, reports on whistleblowing are mostly not found in the media.

RECOMMENDATIONS

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of *Cybersecurity Culture and Society*. These aim to provide possible next steps to be followed to enhance existing cybersecurity capacity in line with the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

CYBERSECURITY MINDSET

R2.1.1 Consider implementing a monitoring framework, in order to ensure awareness, implementation of safe practices, and cybersecurity as a priority across all public sector entities. The oversight for ensuring implementation should be assigned to a dedicated, centralised agency, such as a national cybersecurity agency or CIRT.

R2.1.2 Consider mandating states to ensure similar activities to the federal level within their sovereignty and on the communal level.

R2.1.3 Ensure awareness raising campaigns targeted at SMEs, in order to address cybersecurity as a priority and promote safe cybersecurity practices. Consider delegating this responsibility to the state-level and coordinate activities across states through a dedicated federal-level cybersecurity entity.

R2.1.4 Consider setting up a body that can coordinate a collective approach toward cybersecurity awareness and safe practices across the private sector, public sector, and the defence and intelligence community. The body should be led by a civilian authority, in order to ensure the willingness of the private sector to fully and openly collaborate.

R2.1.5 Ensure metrics are defined and surveys conducted, in order to gain a full picture with respect to the mind-set among users in general and across the private sector, including SMEs.

TRUST AND CONFIDENCE ON THE INTERNET

R2.2.1 Ensure metrics are defined and surveys conducted, in order to gain a full picture with respect to users' trust and confidence on the Internet.

R2.2.2 Ensure the promotion of campaigns currently led by CERT.br and NIC.br, in order to inform society-at-large.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.3.1 Ensure the further promotion of data protection online among users in general, independent of their demographic background.

R2.3.2 Implement mechanisms that ensure that privacy and security do not compete.

REPORTING MECHANISMS

R2.4.1 Set up a dedicated entity and platform that provides reporting mechanisms to Internet users in general and SMEs; such an entity could also be federalised, being implemented on the state-level and coordinated through a federal-level cybersecurity agency.

R2.4.2 Ensure metrics for all reporting (SMEs, large businesses, public sector, Internet users in general) is collated in metrics and surveys, in order to gain a full picture of any reporting activities.

MEDIA AND ONLINE PLATFORMS

R2.5.1 Encourage media to report not only on major cybersecurity incidents but also on best practices and increase their personal cybersecurity awareness. The media could also be encouraged to promote a positive whistleblowing culture through reporting on whistleblowing examples that had a positive impact on the cybersecurity culture.

R2.5.2 Encourage NGOs to set up for a on social media for discussions on cybersecurity.

DIMENSION 3
BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

This *Dimensio*n reviews the availability, quality and uptake of programmes for various groups of stakeholders, including the Government, the private sector and the population as a whole, and relates to cybersecurity awareness-raising programmes, formal cybersecurity educational programmes, and professional training programmes.

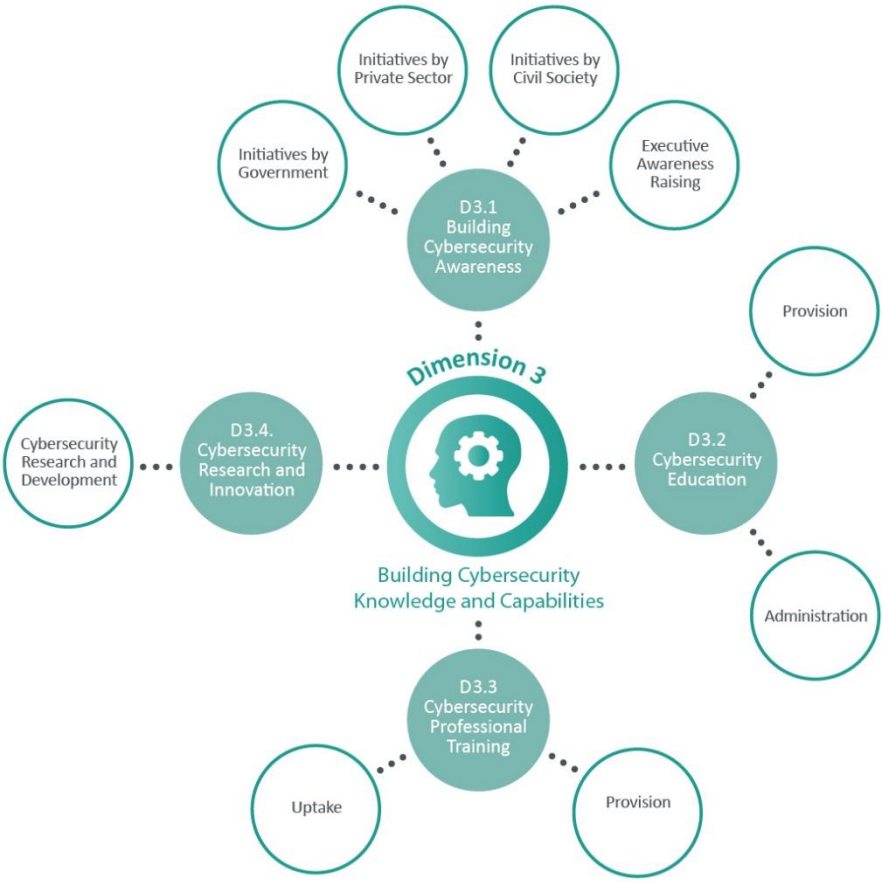
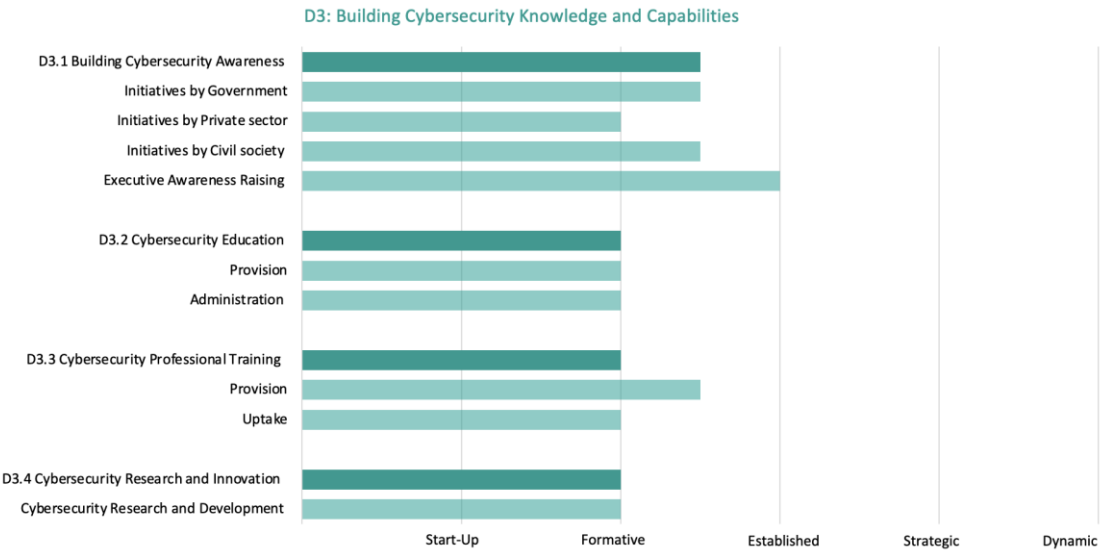


Figure 8: Factors and aspects examined in Dimension 3.

OVERVIEW OF RESULTS



D3.1 BUILDING CYBERSECURITY AWARENESS

This Factor *focuses on the availability of programmes that raise cybersecurity awareness throughout the country, concentrating on cybersecurity risks and threats, and ways in which to address them.*

***Stage*: Formative to Established**

Brazil's NCS *E-Ciber* identifies cybersecurity awareness as one of three areas of activity under section *2.4 Education*. It recommends the establishment of awareness plans in schools and institutions, good practice portals, and educational campaigns. However, E-Ciber does not provide an overview of specific actions that should be implemented–it generally recommends raising awareness by means of outlining various possibilities for doing so including examples from other countries. Therefore, this review mostly relies on the statements of stakeholders and evidence of awareness activities available online.

A number of cybersecurity awareness campaigns have already been listed in Dimension 2. Most importantly, *internetsegura.br*, an initiative by NIC.br and CERT.br, provides advice to the general public.[61] CERT.br and NIC.br are organisations functioning under the umbrella of government mandates and may be characterised as multistakeholder organisations. The

[61] "Safe Internet", internetsegura.br, accessed on 22 October 2023, translated by *Firefox Fullpage Translation*, https://internetsegura.br/.

governance structure of these organisations is shortly outlined in the following, based on the information provided on the website of NIC.br.[62]

CGI.br is the Brazilian Internet Steering Committee, which *"was created by Interministerial Ordinance 147, of May 31st, 1995, which was amended by Presidential Decree 4,829 of September 3rd, 2003, with the purpose of coordinating and integrating all Internet service initiatives in Brazil, as well as promoting technical quality, innovation and the dissemination of the services available".*[63] While established by means of national ordinance and presidential decree, the committee is not a government institution *per se*. It includes nine representatives from the federal government, four representatives from the corporate sector, four representatives from the third sector (i.e., NGOs), three representatives from the science and technology community, and one Internet expert. Therefore, it may be characterised as a multistakeholder body, including representatives from government, the private sector, civil society / NGOs, science and technology, as well as a subject matter expert. As is shown in Figure 9, CGI.br functions as the body governing NIC.br by means of constituting the members with voting rights in NIC.br's General Assembly. NIC.br is further subdivided in different organisational entities, including CERT.br.

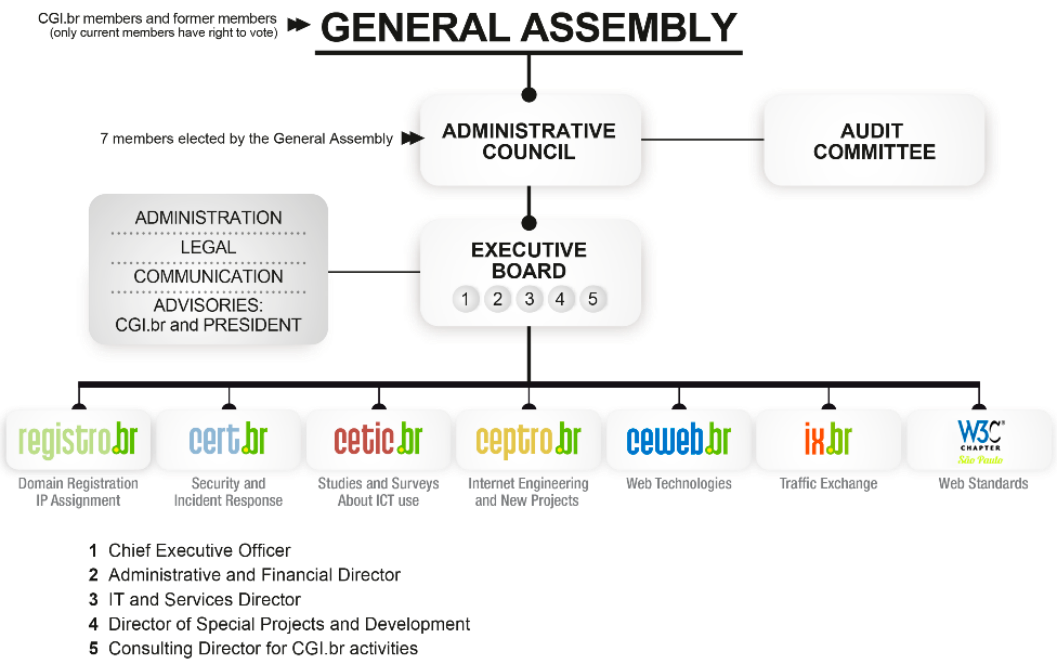


Figure 9: The governance structure of NIC.br and ist sub-organisations, as listed on the website of NIC.br.[64]

The campaigns and activities of the NIC.br and its sub-organisations could benefit from stronger government support, e.g., through stronger funding and government-supported

[62] "Who we are", NIC.br, accessed on 2 November 2023, https://nic.br/who-we-are/.
[63] "About the CGI.br", CGI.br, accessed on 2 November 2023, https://cgi.br/about/.
[64] "Who we are", NIC.br, accessed on 2 November 2023, https://nic.br/who-we-are/.

promotion. The impact of these programmes is not monitored through outcome-oriented surveys or metrics. Furthermore, a systematic coordination and a dedicated portal for the general public, for example provided through a dedicated cybersecurity agency, would be beneficial, as has also been formulated under section 2.4 of E-Ciber. The awareness raising activities by CERT.br and NIC.br also address technical personnel in the private sector, as outlined by an overview presentation provided earlier in Dimension 2.[65] For example, the *Programa Internet+Segura* provides best practices with respect to configurations useful against common network attacks.[66] While the activities clearly fulfil the requirements for Formative stage, they also indicate advances towards Established stage. The most important requirements for fully reaching Established stage that yet need to be fulfilled are the provision of metrics and surveys as well as a systematic coordination of government and civil society initiatives.

Stakeholders indicated that the private sector conducts many awareness raising campaigns, in particular in the banking sector since this is also driven by requirements of the regulator. However, there are no systematic reviews by means of metrics and surveys and also the various private sector initiatives are not centrally coordinated. While the indicators for reaching Formative stage are clearly provided, a systematic coordination and review of private sector activities would be required, in order to reach Established stage.

International cybersecurity training companies also provide courses for executives in Brazil.[67] Stakeholders indicated that there is knowledge exchange among executives of larger companies with respect to cybersecurity. Furthermore, companies traded on the stockmarket have adopted protocols for VPs, boards, and CEOs, including investment decisions with respect to addressing cybersecurity risks. In the banking sector, there is an executive committee for cybersecurity, where executives meet on a regular basis to discuss aspects of cybersecurity. Larger firms also conduct cybersecurity simulation exercises at all levels. Therefore, Established stage is reached. However, stakeholders also indicated that smaller companies are not aware of the risks and lack training. The private sector could benefit from mandatory cybersecurity courses across all sectors for executives of larger companies and a stronger promotion and provision of executive-level courses for SMEs. Currently, the cyber strategy of Brazil does not assign a dedicated budget for establishing a training programme for managers. This should be considered for a next iteration of the strategy and a budget should be allocated for setting up coordinated training programmes in the mean time.

[65] "Security Awareness Initiatives in Brazil", CERT.br, accessed on 22 October 2023, https://cert.br/docs/palestras/certbr-natcsirt2023.pdf.

[66] "Para fazermos uma Internet mais Segura", Programa Internet+Segura, accessed on 22 October 2023, https://bcp.nic.br/i+seg/.

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

D3.2 CYBERSECURITY EDUCATION

This Factor *addresses the availability and provision of high-quality cybersecurity education programmes and having sufficient qualified teachers and lecturers. Moreover, this* Factor *examines the need to enhance cybersecurity education at national and institutional levels, and the collaboration between government and industry to ensure that educational investments meet the needs of the cybersecurity education environment across all sectors.*

***Stage*: Formative**

Similarly to the previous Factor, cybersecurity education is listed as an area of activity under the term "Formation" in section 2.4 of E-Ciber. The NCS mentions the necessity of creating courses and the insertion of cybersecurity as a subject in school curricula of all levels, inclusing universities. However, no specific actions are listed in E-Ciber as to how this should be achieved. Although an action plan exists, no access to this action plan was provided to the authors of this report. Therefore, the assessment mostly relies on statements from the stakeholders and evidence gathered online. E-Ciber does mention that cybersecurity *"in Brazilian schools is still very incipient, if not non-existent"*.[68]

Stakeholders indicated that Computer Science courses offered at universities are harmonised by means of a curriculum coordinated by the *Sociedade Brasileira de Computação* (SBC, the Brazilian Computation Society).[69] Systems security is a standard component of the curriculum not only of computer science but also further computer and software related undergraduate degrees defined by SBC in 2017.[70] Stakeholders also indicated that SBC has finished preparing the definition of an undergraduate course in cybersecurity in 2022, enabling universities to offer a programme fully dedicated to cybersecurity. However, no evidence of this course programme is yet available online. While these are indicators required for reaching Established stage, some further indicators of this stage yet remain to be reached. In particular, cybersecurity is not yet a topic widely adopted in non-technical subjects and it is unclear, whether universities also offer lectures and seminars in cybersecurity aimed at a non-specialist audience, for example in law or ethics courses. Some participants indicated that a number of universities in certain regions offers such courses, lectures, and seminars. However, this does not yet seem to be the case across the whole country.

While SBC is also concerned with computer education in the primary and secondary school curriculum, it is unclear whether cybersecurity is actually part of these levels–also, since primary and secondary education are partially within the responsibility of the communal and state level of government. Participants indicated that while many initiatives and activities exist, the educational system would benefit from a more coherent coordination of cybersecurity education. Furthermore, a dedicated budget for education in cybersecurity

[68] See section 2.4 of E-Ciber.

[69] "Sociedade Brasileira de Computação", SBC, accessed on 22 October 2023, https://www.sbc.org.br/.

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

should be reserved. There is currently no dedicated national funding for cybersecurity research and also funding for competitions and student stipends in this domain is limited and not nationally coordinated. Since the cybersecurity curriculum for undergraduate university degrees has only just been established there are also no metrics available–similarly, no metrics exist for primary or secondary cybersecurity education. No data could be provided on the availability of qualified teachers for cybersecurity. Discussions with stakeholders imply that teaching expertise is probably available in higher education but mostly missing on primary and secondary school levels. Therefore, it may be stated that a small cadre of existing qualified educators exists but that it requires further initiatives in order to establish broad availability of educators.

D3.3 CYBERSECURITY PROFESSIONAL TRAINING

This Factor *addresses and reviews the availability and provision of affordable cybersecurity professional training programmes to build a cadre of cybersecurity professionals. Moreover, this* Factor *reviews the uptake of cybersecurity training, and horizontal and vertical cybersecurity knowledge and skills transfer within organisations, and how this transfer of skills translates into a continuous increase of cadres of cybersecurity professionals.*

***Stage*: Formative**

As with the previous Factors of this Dimension, cybersecurity professional training is mentioned in the NCS under section 2.4. The NCS outlines the difficulty of acquiring qualified personnel: 34 percent of Brazilian employers are said to have difficulty recruiting talent. The greatest difficulties for Brazilian companies in the hiring process are a lack of technical skills (33 percent), lack of experience (23 percent), and a lack of interpersonal skills (19 percent).E-Ciber further states that *"the private sector focuses intensely on the development of the workforce"*.[71] Furthermore, the strategy formulates "brain drain" as a problem for the Brazilian economy with respect to trained personnel. Again, no specific actions are listed in order to address the situation outlined and no access to the implementation / action plan of the NCS was provided to the authors, which is why the following assessment mainly relies on stakeholder discussions and evidence found online.

With respect to vocational and professional training, stakeholders indicated there is currently no national coordination of such training. Many ad-hoc and industry initiatives exist. However, there is a significant gap in the workforce and a problem with qualified professionals moving abroad due to higher salaries. Common international certifications exist for cybersecurity professionals. However, there are only limited provisions of training provided nationally that would provide sufficient depth with respect to technological and practical skills. Stakeholders indicated that many professional courses do not go beyond concepts and do not offer hands-on training. Certain sectors provide their own training programmes, which are not coordinated with other sectors or nationally. In order to fill the gap, institutions such as NIC.br

[71] See section 2.4 of E-Ciber.

provide training and initiatives to onboard young people and get them to know the domain of cybersecurity as a possible area for employment. Examples are programmes such as *Hackers do Bem* ("Hackers for Good")[72], aimed at young people, or free seminars on cybersecurity offered by *Escola Superior de Redes*[73].

Stakeholders reported the availability of a practically-focused cybersecurity college course. However, people struggle with the integration on the employment market since they lack practical experience. Therefore, it would be useful to increase the interconnection between the cybersecurity colleges and the industry as part of the courses, in order to provide graduates with practical work experience before they graduate. Stakeholders indicated that a main drawback of the professional training landscape is a cross-cutting approach integrating the requirements of the industry with the provision of professionally-focused education. While informal coordination exists, a dedicated body should take over the coordination of requirements from the industry and the curricula of local training providers.

While the discussions showed, that the required indicators for Formative stage are met, Brazil yet has to coordinate its activities for professional training more broadly. In particular, the needs of society have to be systematically analysed and fed into vocational and professional training programmes that have to be nationally and sectorially coordinated. Furthermore, the government should fund and encourage initiatives for trained professionals to stay in the country upon successful completion of courses and also after gaining experience in the industry. Furthermore, many programmes seem to be focused on youth; Brazil could explore the possibility of career-transition programmes for non-cybersecurity professionals. Finally, professional training programmes should be regularly and systematically reviewed by means of metric in order to assess whether the training provided meets the demands of the public and private sector and whether the funding is sufficient.

D3.4 CYBERSECURITY RESEARCH AND INNOVATION

This Factor *addresses the emphasis placed on cybersecurity research and innovation to address technological, societal and business challenges, and to advance the building of cybersecurity knowledge and capabilities in the country.*

***Stage*: Formative**

Brazil's NCS lists its approach towards research, development, and innovation in Section 2.2. It outlines that research, development and innovation initiatives in the area of cybersecurity require greater priority . The NCS identifies gaps in the cybersecurity research activities and also defines the requirement to foster a national coordination of activities and funding. E-Ciber states the requirement to implement master and doctoral degree programmes in order

[72] "Hackers do Bem", Hackers do Bem, accessed on 22 October 2023, https://conteudo.hackersdobem.org.br/oprograma.
[73] "Escola Superior de Redes, Instituto SANS", Escola Superior de Redes, accessed on 22 October 2023, https://esr.rnp.br/.

to improve cybersecurity research, development, and innovation. However, it is unclear how this should be specifically implemented, although this might be defined in an action plan that the authors did not receive access to. The following assessment, therefore, is mainly based on evidence found online and stakeholder discussions.

According to stakeholders, cybersecurity R&D activities mostly take place as part of conventional computer science research activities, e.g., as part of network security or systems security research and development. Examples of such activities are listed in the following:

- *SBSeg* is an annual Brazilian research symposium on information security and computational systems.[74] It focuses on technological aspects of cybersecurity, as is for example evident from its programme in 2023;[75]
- *RNP.br*, the national research network provider, offers an innovation and research grant for technologically innovative projects that also covers cybersecurity;[76]
- Stakeholders mentioned several research projects at universities on topics in cybersecurity, which have been taken up in the past 3-5 years. These projects bear a technological focus.

Stakeholders also highlighted that the research is integrated in international and, in particular, regional research collaboration in Latin America. No systematic metrics exist to assess the R&D performance with respect to cybersecurity but ad hoc metrics exist.

Therefore, Brazil clearly fulfils all indicators required for Formative stage. Some indicators for Established level may also be present. The main obstacle for reaching Established level is the lack of systematic national funding specifically for topics in cybersecurity and that also goes beyond the domain of technology and computer science. A next iteration of a national cybersecurity strategy should consider providing dedicated funding of this kind, which also addresses disciplines beyond technology and computer science. Furthermore, metrics should systematically be implemented, in order to measure the performance of R&D activities with respect to cybersecurity.

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

[75] "Programação SBSeg 2023", SBSeg, accessed on 22 October 2023, https://sbseg2023.ufjf.br/programacao/.

[76] Research, Development and Innovation Incentive Grant Programme", RNP.br, accessed on 22 October 2023, https://www.rnp.br/en/node/7766.

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Building Cybersecurity Knowledge and Capabilities*, the following set of recommendations are provided to Brazil. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

BUILDING CYBERSECURITY AWARENESS

R3.1.1 Programme review processes and outcome-oriented metrics should be implemented for cybersecurity awareness initiatives in the government, civil society, and the private sector, mandated and monitored by a dedicated cybersecurity agency.

R3.1.2 A systematic coordination of private sector awareness raising iniatives should be implemented. This could, for example, be supported by a dedicated national cybersecurity agency and integrated into the existing portal *internetsegura.br*.

R3.1.3 Mandatory cybersecurity courses for executives of larger companies should be considered and coordinated by a mandated budy, such a national cybersecurity agency or NIC.br. For SMEs, such courses should be provided free of charge of at low cost, in order to reflect the economic pressures SMEs often face.

R3.1.4 A future iteration of the national cybersecurity strategy should allocate a dedicated budget for training programmes for managers, in particular for SMEs who face economic limitations. Before the next iteration of a cybersecurity strategy, the financial gap could be filled by allocating part of the government budget for this purpose.

CYBERSECURITY EDUCATION

R3.2.1 Consider introducing cybersecurity as part of non-specialist courses at universities across the country, for example in ethics or law. Consider providing cybersecurity seminars and lectures for a non-specialist audience by means of adding cybersecurity to the subject curricula of other courses with a topical overlap. Introduce, with high priority, dedicated cybersecurity degree

programmes (bachelor, master, and doctoral) broadly across universities. These tasks should be mandated to a dedicated body, such as the Brazilian Computing Society or a national cybersecurity agency.

R3.2.2 Consider coordination of cybersecurity education below university level (e.g., primary and secondary education and vocational training) through the Ministry of Education in collaboration with further stakeholders, such as NIC.br and a national cybersecurity agency.

R3.2.3 Consider introducing a dedicated national and state-level budget for all levels of cybersecurity education (primary, secondary, higher education, etc). This task should be taken up by a dedicated body, e.g., an entity in the Ministry of Education.

R3.2.4 Allocate a national budget for cybersecurity student stipends and cybersecurity competitions. This should be tasked to a dedicated body, such as a national research council or the Ministry of Education.

R3.2.5 Implement metrics and surveys in order to monitor the effectivity of and demand for cybersecurity education, mandated by a national cybersecurity agency in collaboration with the Ministry of Education.

CYBERSECURITY PROFESSIONAL TRAINING

R3.3.1 Consider national coordination of vocational and professional training through a dedicated body, such as the Ministry of Education or a national cybersecurity agency. The coordination should encompass a cross-cutting approach, feeding the requirements of the industry into the training curricula.

R3.3.2 Establish a strong interconnection between cybersecurity college degree programmes and the industry; for example by enabling students to gain practical work experience in the industry as part of cybersecurity college courses. This should be included as a strategic vision in a future iteration of a National Cybersecurity Strategy and mandated to a dedicated body, e.g., within the Ministry of Education or a national cybersecurity agency.

R3.3.3 Establish, through a mandate from the Ministry of Education to a dedicated entity, mechanisms and dedicate funds to encourage trained professionals and professionals with work experience to remain in the employment market of the country.

R3.3.4 Consider establishing and funding career-transition programmes for non-cybersecurity professionals. This should be mandated by the government to a dedicated private sector or NGO institution, or NIC.br.

R3.3.5 Conduct reviews and studies and establish metrics in order to monitor whether the training programmes provided meet the demands of the public and private sector. This task should be mandated by a dedicated cybersecurity agency.

CYBERSECURITY RESEARCH AND INNOVATION

R3.4.1 Include dedicated national funding for cybersecurity R&D activities, including topics beyond technology and computer science, as part of the next iteration of a national cybersecurity strategy and assign responsibility to a dedicated body, such as a national research council.

R3.4.2 Systematically collect metrics on all cybersecurity R&D activities and research demands on a national level, in order to inform on the performance of R&D activities and the funding provided. This should be mandated by the Ministry of Education to a dedicated entity, such as a national statistics office or similar.

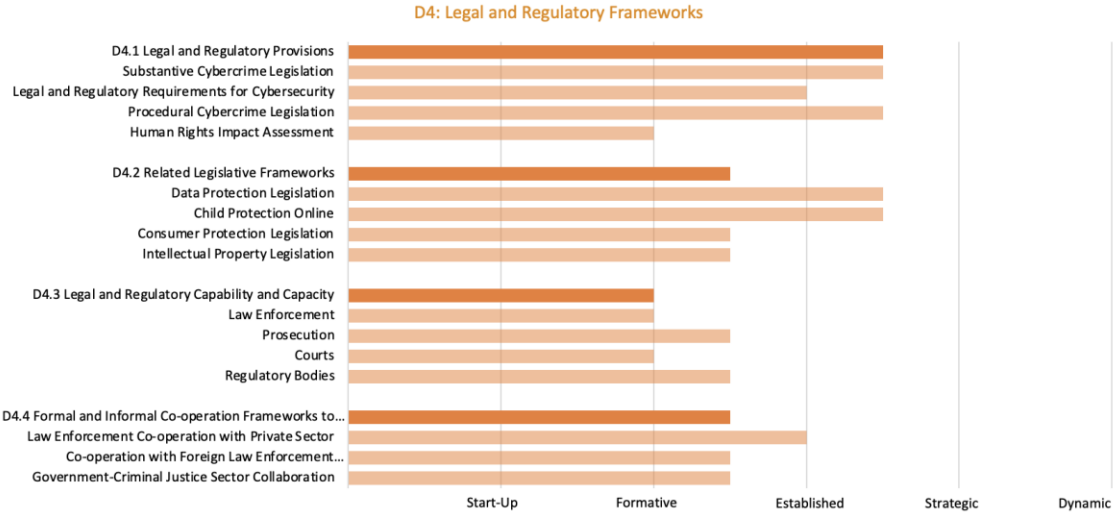
R3.4.3 Consider initiating a national forum or symposium on cybersecurity, which addresses both technological and non-technological topics, such as cyber law, cybersecurity and international politics, or cyber ethics. This task should be mandated to a dedicated body, e.g., a national research council or a national cybersecurity agency, in collaboration with academia and the private sector.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This *Dimension* examines the Government's capacity to design and enact national legislation that directly and indirectly relates to cybersecurity, with a particular emphasis placed on the topics of regulatory requirements for cybersecurity, cybercrime-related legislation, and related legislation. The capacity to enforce such laws is examined through law enforcement, prosecution, regulatory bodies and court capacities. Moreover, this *Dimension* observes issues such as formal and informal co-operation frameworks to combat cybercrime.

Figure 9: Factors and aspects examined in Dimension 4.

OVERVIEW OF RESULTS



D4.1 LEGAL AND REGULATORY PROVISIONS

This Factor *addresses various legislation and regulatory provisions relating to cybersecurity, including legal and regulatory requirements, substantive and procedural cybercrime legislation, and human rights impact assessment.*

***Stage*: Established to Strategic**

Substantive cybercrime legislation has been thoroughly reviewed in the 2020 CMM Review of Brazil—the reader is referred to the 2020 report for a thorough listing of specific cybercrime and criminal law. Changes to the law since the previous CMM Review are provided in the following, where applicaple.

Stakeholders have indicated that laws with respect to the digital chain of custody have been improved:[77] Due to secondary legislation the digital chain of custody can now be fully established, aiding criminal investigations and criminal procedural law (e.g., LEI Nº 14.155, DE 27 DE MAIO DE 2021[78] has been adapted in order to include the digital aspects). It follows ISO 17005. Participants stated that the criminal law reflects cybercrime adequately; matters such as unauthorised access are well regulated. The Budapest Convention was signed in 2023. According to stakeholders, national law previously already largely covered its implementation–the aforementioned establishment of a digital chain of custody being one of

[77] The term "digital chain of custody" in this context refers to the documentation of ownership of a digital asset (e.g., data), and its transfer from a person or organization to another, including the exact date, time, and purpose of the transfer, etc.

[78] "LEI Nº 14.155, DE 27 DE MAIO DE 2021", GSI, accessed on 02 November 2023, https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm.

the major changes implemented in order to further ensure complaince. However, a process needs to be initiated to ensure that the requirements of the Budapest Convention are fully coherent with Brazilian national law. This process is currently underway. The 2nd protocol of the Budapest Convention is of particular importance for Brazil, since it improves the possibilities for international cooperation and exchange of information for Brazilian authorities. Nevertheless, Brazil has already previously been integrated in police cooperation networks through, e.g., Interpol and G7. The Budapest Convention should enable Brazil to exchange information very swiftly and to obtain data required for investigations very quickly. The federal police is further involved in the No More Ransom project as a "Supporting Partner", offering time and resources to help promote the project nationally and internationally.[79] The goal of the project is to *"help victims of ransomware retrieve their encrypted data without having to pay the criminals"*.[80] The project also aims at crime prevention by means of educating users and businesses. This is supported by the Federal Police by promoting the project and sharing knowledge within Brazil.

Generally, Brazil's approach relies on treating cybercrime through conventional law; law specific to cybercrime is only introduced where conventional law cannot adequately cover cybercrime cases. E.g., ransomware cases are handled as conventional extortion.

Currently, Brazilian law does not require data breaches to be reported, as long as they do not include personal data. Where personal data is concerned, this is covered by the recently introduced General Personal Data Protection Law (LGPD), which is similar to the EU's GDPR.[81] A detailed guide on the similarities and differences between LGPD and GDPR may be found on the European Commision's website.[82] The guide outlines how most aspects of LGDP are consistent with GDPR, with some exceptions in the domain of research and discrimination protection. With respect to personal data protection for children, LGPD is stricter than GDPR but the age limit for providing is set lower than in GDPR. Further differences outline by the guide often state that LGPD is in fact often more restrictive, i.e., provides a stricter level of personal data protection.

Some sectors, for example, banking, require mandatory reporting. However, a general requirement for mandatory reporting would probably be useful across all sectors–as a minimum reporting requirement for incidents for sectors where a regulatory body does not exist or does not require reporting.

Due to the ongoing activities in improving the legal and regulatory provisions, Brazil may be considered to already partially being on Strategic level. However, particular care should be given to considering further mechanisms for mandatory reporting. A legal requirement for reporting should be outlined for all sectors in the form of a minimum incident reporting requirement. In non-critical sectors, and in case no personal data is concerned, such reporting

[79] "No More Ransom", nomoreransom.org, accessed on 22 October 2023, https://www.nomoreransom.org/cs/index.html.

[80] "About the Project", nomoreransom.org, accessed on 02 November 2023, https://www.nomoreransom.org/en/about-the-project.html.

[81] "General Personal Data Protection Act (LGPD)", lgpd-brazil.info, accessed on 22 October 2023, https://lgpd-brazil.info/.

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

might even be anonymised, with the benefit of providing law enforcement with a clearer picture of malevolent activities experienced in the private sector.

Stakeholders also indicated that there is no systematic human rights impact assessment carried out. Participants also stated that due to the introduction of LGDP many aspects concerning human rights are already reflected in the legal and regulatory provisions. Nevertheless, a systematic review of cybercrime law on its impact on human rights should be conducted, in order to ensure that the benevolent aim of fighting cybercrime does not impact citizens' rights online.

D4.2 RELATED LEGISLATIVE FRAMEWORKS

This Factor *addresses the legislative frameworks relating to cybersecurity, including data protection, child protection, consumer protection, and intellectual property.*

***Stage*: Formative to Established (with elements of Strategic)**

As stated previously, Brazil has introduced a comprehensive General Personal Data Protection Law (LGPD), designed similarly to the EU's GDPR. [83] The designated lead agency is the *Autoridade Nacional de Proteção de Dados* (ANPD).[84] Therefore, Established stage is clearly reached with respect to this aspect. Since the law is new it has probably not yet been reviewed since its introduction. In order to reach Strategic level, Brazil would benefit from a regular review of its personal data protection legislation and it should also aim to enact mechanisms in its framework, such that the law can quickly adapt to emerging technologies. This could be defined as the responsibility of ANPD.

Brazil also has a functioning child protection law for the digital domain, which is regularly reviewed and adapted. For example, recent adaptations enhance the fight against child pornography online. Similarly to data protection, Brazil could benefit from a mechanism that takes into account emerging technologies in its online child protection legislation.

Consumer protection online is covered mostly through conventional law, as is outlined in the 2020 CMM Report. However, phishing is not currently considered a criminal act *per se*. This provides for a gap in the legal framework and Brazil may want to consider closing this gap. In particular, since Brazil is characterised as a leading in phishing attacks worldwide in an article by zdnet.com.[85] Participants stated that criminalising Phishing would lead to a massive increase in criminal investigations–nevertheless, a law should be considered that could cover the systematic establishment of infrastructure for the purpose of Phishing. Furthermore, criminalising Phishing *per se* would presumably lead to a decrease in Phishing campaigns due

[83] "General Personal Data Protection Act (LGPD)", lgpd-brazil.info, accessed on 22 October 2023, https://lgpd-brazil.info/.

[84] "Autoridade Nacional de Proteção de Dados", ANPD, accessed on 22 October 2023, https://www.gov.br/anpd/pt-br.

[85] Angelica Mari, "Brazil leads in phishing attacks", ZDNET, 24 March 2021,

to the deterrent effect of criminalisation, even if not every Phishing campaign would be investigated. The current rationale for not covering Phishing in the criminal law is that sending Phishing emails is not yet a materialisation of a harmful effect–only the exploitation of a users' action responding to a Phishing email is considered as such. This materialisation is already covered under conventional criminal law concerning fraud. A criminal network systematically operating infrastructure for Phishing, however, could be prosecuted in case of a Phishing legislation and could have a preventive effect with respect to online fraud.

Intellectual Property is protected through conventional law. However, the law has not been designed specifically with respect to the risks online. While it may provide the basis for protection and prosecution for most online cases, it may be useful to conduct a specific review in order to identify potential cases online, which are not covered under the current legislation. In particular, since stakeholders were unsure as to whether the current legislation is sufficient for cyberspace.

Due to the advanced level of the law *Factor D4.2 Related Legislative Frameworks* this Factor may be assessed as meeting all requirements for Established stage and even some of Strategic stage, with the exception of points referring to intellectual property and consumer protection in cyberspace. Furthermore, the ongoing changes of the law with respect to the online environment reflect a strategic vision of cybercrime legislation and legal protection from cybersecurity risks online in Brazil.

D4.3 LEGAL AND REGULATORY CAPABILITY AND CAPACITY

This Factor *studies the capacity of law enforcement to investigate cybercrime, the prosecution's capacity to present cybercrime and electronic evidence cases, and the court's capacity to preside over cybercrime cases and those involving electronic evidence. Finally, this* Factor *reviews the existence of cross-sector regulatory bodies to oversee compliance with specific cybersecurity regulations.*

***Stage*: Formative**

The institutional capability and capacity in Brazil varies strongly, depending on specific personnel and the level of administration. While the federal police level has adequate law enforcement capabilities, such capability may not be present at state and local level. The distribution of responsibility between the federal and state police level depends on the severity and impact of a case: Large cases and cases with international connection (e.g., international cybercrime networks) are investigated by the Federal Police. Smaller cases fall within the responsibility of the state-level Civil Police. Brazil does not currently have a centralised competence centre for cybercrime cases, which would also be accessible to the state-level police; rather, this capability is integrated in the Federal Police. The state-level police also has to investigate cybercrime cases but there is no mechanism in place between states or between state and federal level, which would ensure sufficient capabilities and capacity and knowledge-sharing. Stakeholders have indicated that in practice, presumably

collaboration does happen among state-level police units and with the Federal Police However, this collaboration should be formalised and a competence centre for the exchange of knowledge and experiences should be established, which could also provide investigative capacity to states which lack sufficient resources in terms of personnel or infrastructure. Even though police forces may have a sufficient the capability in terms of knowledge, they often lack sufficient personnel for smaller cases including digital crime. This particularly applies to state-level police units. While the Federal Police provides training for its officers, the situation on the state level is unclear, since it is within the sovereignty of the respective states. According to stakeholders, the amount of experts within law enforcement has remained almost unchanged over the last 20 years, which is insufficient in order to address all cases of cybercrime. Furthermore, due to the career structure of the police, trained personnel may get moved into a different domain and so knowledge and experience may be lost. As outlined, the provisions for establishing a digital chain of custody are well established.

With respect to prosecutors, stakeholders have reported that resources, capabilities and capacities meet current needs; i.e., prosecutors usually have sufficient resources and expertise for conducting cybercrime cases. However, the situation seems to be different with courts. Stakeholders claimed that the courts seem to lack sufficiently trained judges for some cybercrime cases. Such training is conducted, if at all, ad hoc. While improving this situation is difficult, since the courts are independent from the legislative and executive branches of the state, the legislative and government should attempt to encourage courts to increase their expertise with respect to cybercrime, for example by means of ensuring funding for courses or seminars for judges.

According to stakeholders, regulatory bodies have an adequate level of staff and have the required capabilities and capacities in order to address cybersecurity within their responsibility.

Overall, particularly law enforcement capabilities and capacities should be more strongly coordinated on the federal level and among states, in order to reach Established level. Especially, staffing issues and training should be addressed, as well as collaboration mechanisms in case of shortages among states and between the state and federal level.

D4.4 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This Factor *addresses the existence and function of formal and informal mechanisms that enable co-operation between domestic actors and across borders to deter and combat cybercrime.*

***Stage*: Formative to Established**

As indicated previously, Brazil has signed and ratified the Budapest Convention and has already previously collaborated internationally and regionally (with Latin American Countries

and the US) on issues of cybercrime. Recently, legislation has been introduced to ensure full compliance with requirements of the Budapest Convention.[86] The efforts include an integration of a 24/7 capacity, enabling Brazilian police to both seek and respond to requests for assistance. When this process is completed, Established stage is reached with respect to these indicators. As the process is currently underway, however, Established stage cannot yet be fully granted.

Stakeholders have also indicated that private-public collaborations work smoothly and that an information exchange between the private sector, intelligence, and the military is set up and works well. However, this statement could not be confirmed through external sources (e.g., from the private sector). GSI currently acts as the information exchange point between law enforcement, military, intelligence, and the central government / president's office. It may be useful to review this arrangement with respect to a potential establishment of a dedicated cybersecurity agency on the federal level. The willingness to collaborate and openly exchange information, particularly of the private industry and NGOs, might be even greater in case the information exchange is mandated to a cybersecurity agency separate from the intelligence, military, and law enforcement community.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Legal and Regulatory Frameworks*, the following set of recommendations are provided to Brazil. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

LEGAL AND REGULATORY PROVISIONS

R4.1.1 Consider implementing a broader requirement for mandatory reporting of cybersecurity incidents, in particular for large businesses and CNI.

R4.1.2 Consider carrying out a systematic human rights impact assessment for cybercrime legislation, which goes beyond aspects of privacy and data protection.

[86] This has already been outlined in *Factor D4.1 Legal and Regulatory Provisions*. In particular, the introduction of *LEI Nº 14.155* in May 2021 has been an important step towards compliance.

RELATED LEGISLATIVE FRAMEWORKS

R4.2.1 Consider enacting mechanisms for adapting to legal protections with respect to emerging technologies with respect to data protection, consumer protection, intellectual property protection, and child protection online.

R4.2.2 Consider bringing under the criminal law large-scale Phishing campaigns and the establishment of infrastructural readiness for large-scale Phishing campaigns.

R4.2.3 Review whether the (conventional) intellectual property legislation covers aspects specific to the online environment, such as streaming and file sharing platforms or digital copies of intellectual property.

LEGAL AND REGULATORY CAPABILITY AND CAPACITY

R4.3.1 Consider setting up a national centre for police investigations of digital / cybercrime cases, which could act as a centre of competence, knowledge exchange and last resort in case of resource limitations for federal-level and state-level police. In particular, the current set-up of a cybersecurity competence centre for police investigations on the federal level should be accessible to the state-level police units. Collaboration mechanisms should be formalised.

R4.3.2 Provide sufficient funding for the adequate staffing of experts in cyber-related law enforcement on the federal level and ensure the states provide sufficient funding and personnel resources to build an adequate law enforcement capacity and capability with respect to law enforcement. Furthermore, the bureaucratical provisions within the state-level and federal level police should be reviewed, in order to retain experts with skills in the departments where these skills are best placed.

R4.3.3 Consider setting up training for judges and further court professionals with respect to cybercrime. Similar trainings should also be provided for the legal profession in Brazil in general, either through a public entity or a mandated private entity.

FORMAL AND INFORMAL CO-OPERATION FRAMEWORKS TO COMBAT CYBERCRIME

R4.4.1 Ensure the review of compliance with the Budapest Convention is completed and legislation adapted accordingly, including the establishment of a solid 24/7 capability for exchange with international networks.

R4.4.2 Consider assigning the responsibility for formal relationships between the government and criminal justice systems, as well as information exchange with the private and public sector in general, to a (future) dedicated national cybersecurity agency.

DIMENSION 5
STANDARDS AND TECHNOLOGIES

This *Dimension* addresses the effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The *Dimension* specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

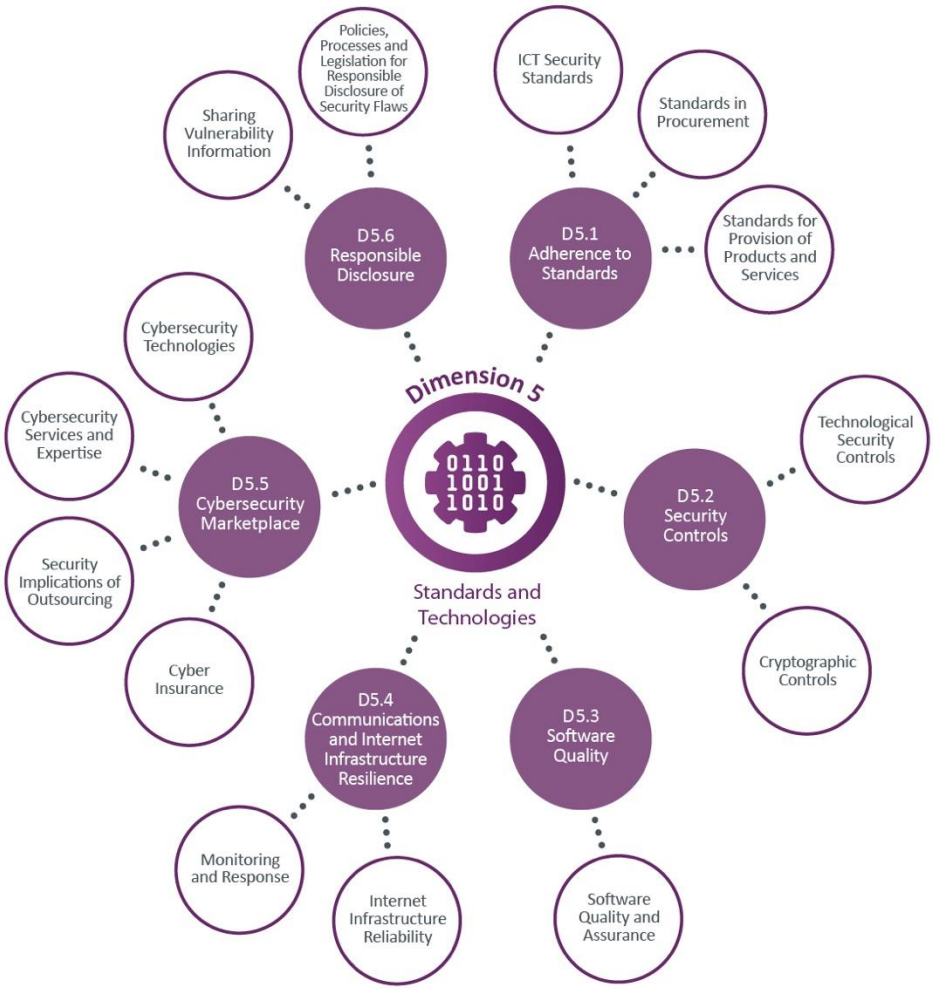
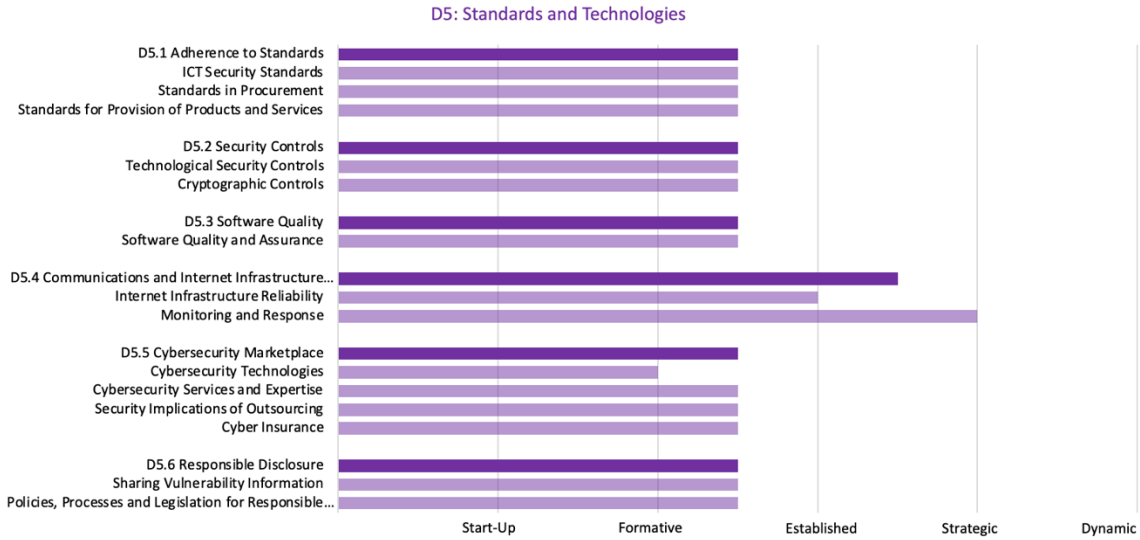


Figure 10: Factors and aspects examined in Dimension 5.

OVERVIEW OF RESULTS



D5.1 ADHERENCE TO STANDARDS

This Factor *reviews the Government's capacity to promote, assess implementation of, and monitor compliance with international cybersecurity standards and good practices.*

***Stage*: Formative to Established**

A nationally agreed baseline of cybersecurity-related standards and good practices has not yet been identified to guide organisations across the public and private sectors. The NCS establishes as a strategic action (within Strategic Action 2.3.1) improving the adoption of internationally recognised standards by the public and private sectors.

Various standards are followed in the more advanced sectors and larger organisations. In a number of sectors, adherence to cybersecurity standards is driven by regulation. For the FPA, cybersecurity standards requirements are established and the implementation of standards is audited; these are largely based on the International Organization for Standardization (ISO) 27000 suite of cybersecurity standards. For the financial and telecommunications sectors, institutions are required to establish their own cybersecurity policy based on international standards; the regulations are not prescriptive about which standards must be used. Participants stated that the international standards most commonly followed include the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF); ISO 27001, and the Center for Internet Security (CIS) Critical Security Controls. For the financial sector, this is also driven by the standards requirements to operate in the international financial system. Some participants from the financial sector noted that it might be beneficial

to be provided with a more specific basis that could be used by different sectors and infrastructures in terms of technical and cryptographic standards and controls.

In other sectors, the implementation of cybersecurity standards is more ad-hoc, and is not monitored by an authority, although sources of guidance are available. The Digital Government department has published a framework of 33 cybersecurity controls, adapting the CIS Critical Security Controls, to guide the digital government institutions (of which there are over 250). The academic network CERT (CAIS) work with the academic sector to give guidance on cybersecurity standards, based on international standards such as ISO 27001, which are adapted meet the realities of the sector. CERT.br provides links on its website to a wide range of guidance materials on the implementation of technical and cryptographic security controls, which can be accessed by any organisation.[87] CERT.br also described engaging with ISPs to promote the adoption of cybersecurity standards and best practices.

Some measures are in place to support SMEs; in particular, recommendations ("Information Security for Small Processing Agents"[88]) are issued by the National Data Protection Authority (ANPD) to help SMEs that are processing personal data to achieve a minimum security level to comply with the General Personal Data Protection Law (LGPD), including guidance on strong passwords and two-factor authentication when using cloud services. Industry associations reported ongoing discussions on how to elevate the cybersecurity maturity of SMEs, and having produced guidance for this audience. Participants expressed the view that further work along these lines would be beneficial, establishing broader cybersecurity guidelines for smaller companies to use in the adoption of technical and cryptographic controls.

In order to promote consistent adoption of cybersecurity standards across organisations of all sectors and maturity levels, it may be beneficial to develop a nationally-agreed baseline of cybersecurity-related standards and good practices, against which organisations from the public and private sectors can in some cases be audited and in others self-assess. As participants noted, the set of baseline standards would need to account for varying contexts and organisations' varying maturity and resource levels, and would need to complement and interact appropriately with the existing sectoral guidelines and regulations. The view was expressed that developing and promoting a national cybersecurity standards baseline might be a role of the new National Cybersecurity Agency (which, as described in D1, is in development).

In terms of cybersecurity standards and best practices in guiding procurement processes, there is again variation according to regulation and organisations' level. As part of the cybersecurity regulation of the FPA, cybersecurity requirements are placed on FPA institutions in regard to procurement of hardware and software, lifecycle management, and the use of cloud services. GSI in August 2021 established normative instructions for agencies of the FPA on the procurement of cloud services, including security requirements.[89] The Central Bank (BACEN) also sets requirements for the financial sector on the procurement of data-processing, data-storage and cloud-computing services, via Resolution No. 4,658 of 2018.[90]

[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

[89] https://digitalpolicyalert.org/event/4032-normative-instructions-on-cloud-computing-services

[90] https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf

In some other sectors and smaller organisations, requirements for cybersecurity practices in procurement are not set, and adherence to standards guiding cybersecurity-related aspects of procurement processes (including risk management, lifecycle management, software and hardware assurance, outsourcing, and use of cloud services) is ad-hoc. Sectors including Electricity noted the need for improved management of supply-chain risks arising from a lack of cybersecurity practices guiding procurement processes. Establishing and promoting guidance in this area that extends to a wider set of sectors and sizes of organisation may be beneficial.

Core activities and methodologies for secure development and lifecycle management for software, hardware and provision of managed services and cloud services are being identified and discussed within professional communities. For example, there is some strategic consideration of requirements for cybersecurity of the software produced by Brazilian companies. The Brazilian Association of Software Companies (ABES) runs a number of working groups to discuss specific issues related to software companies, including working groups on Cybersecurity and Data Protection.[91] The Cybersecurity working group aims to establish a "*space for internal discussions and monitoring of specific regulations, engagement with stakeholders, in addition to promoting the exchange and dissemination of information between members and the most diverse segments of society*".

Participants also reported local cloud companies working with large multinational cybersecurity companies to create secure and robust cloud platforms to offer to clients[92]; a particular example of such a project that targets improving the cybersecurity, availability and quality of the municipal public services was highlighted.[93] Anatel sets requirements for providers of equipment to the telecommunications sector, which are not yet fully audited but aim to manage supply-chain risk.[94]

Standards for software development, hardware-quality assurance, provision of managed services and cloud security are not yet being promoted consistently by the government to providers. Identification and promotion of the relevant standards would help to promote more consistent adoption of security practices by providers.

[91] https://abes.com.br/en/servicos/comites-e-%20grupos-de-trabalho/
[92] https://www.loja.serpro.gov.br/en/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 SECURITY CONTROLS

This Factor *reviews evidence regarding the deployment of security controls by users and public and private sectors, and whether the technological cybersecurity control set is based on established cybersecurity frameworks.*

***Stage*: Formative to Established**

Technological security controls are deployed by public and private-sector organisations. Given the variability in the levels of standards adoption across organisations (as described in D5.1), the level of implementation of these controls varies significantly across different sectors and sizes of organisation.

Within the FPA, for which there are mandatory, audited cybersecurity-compliance requirements, the adoption and implementation of technical and cryptographic controls is reportedly advanced. Advances in the technical controls deployed have also been driven by the establishment of the General Personal Data Protection Law (LGPD), with more federal institutions establishing security operations centres (SOCs) and making use of cyber-threat intelligence (CTI). Participants noted that within state and municipal governments, where the FPA's regulation does not apply, the application of technical controls is much more variable, dependent on the institutions' cybersecurity capabilities and resources.

Another advanced example is the financial sector, where BACEN's regulation has driven institutions to create their own cybersecurity policies and adopt technical and cryptographic security controls in line with these. While BACEN's regulation is not prescriptive of the precise technical controls that should be implemented, there are specific requirements for security and encryption protocols used by institutions participating in the Brazilian payment and financial exchanges system.

In sectors that are not regulated for the implementation of cybersecurity standards, there are, as might be expected, varying levels of implementation of technical and cryptographic security controls. Some of the more advanced organisations adopt up-to-date technical controls in line with international standards, have established CERTs and SOCs, participate in CTI-sharing networks, and implement up-to-date encryption protocols for data in transit and at rest. Some participants expressed the view that many organisations in the private sector are not implementing technical security controls at an adequate level to manage risks, with patchy controls and playbooks and processes that are missing or rarely updated.

Participants reported some concerns about lower levels of adoption of appropriate technical and cryptographic controls by SMEs, who usually have only limited financial resources to invest in cybersecurity. Many SMEs rely on cloud services, and concerns about a lack of awareness of how to securely configure and maintain cloud instances, potentially leading to vulnerability, were cited. As described in D5.1.1, there are some initiatives, including from the National Data Protection Authority, that can serve as guidance for SMEs, but there is a general view that more support for SMEs in the area of cybersecurity-control deployment is needed.

Industry associations also reported ongoing discussions on how to elevate the cybersecurity maturity of SMEs (particularly given that some SMEs are providing services to larger organisations and may present vulnerabilities to them), and having produced guidance and delivering training on minimum security requirements targeting this audience.

Internet-service providers, particularly the larger providers, offer a range of technical security controls for their downstream customers. There are current joint campaigns being run between NIC.br, major telecommunications providers, and other stakeholder, to increase the adoption of anti-DDoS and anti-spoofing controls by ISPs to protect their downstream customers. Tools such as TLS are deployed by some service providers to secure communications between servers and users, and the government is seeking to increase adoption of digital certificates and the security protocols they enable.

Brazil established a national public key infrastructure (PKI), ICP-Brasil, in 2001. The National Institute of Information Technology (ITI) is the Root Certificate Authority (CA), which certifies other CAs and Registration Authorities (RAs) in the chain. There are strict requirements for Root CAs and CAs who handle PKI in Brazil, in order to become certified. The NCS states that digital certificates are still not widely used in corporations, "*due to certain difficulties, such as the high number of processes for issuing certificates, the high cost for citizens and the low number of certifying units per inhabitant*", and that the government is seeking to optimise processes and expand provision in order to enable greater adoption.

CERT.br have recently established a an openly available tool that allows organisations to test the implementation of cryptographic protocols such as TLS in their Internet services and websites. The tool is reportedly being used to assess the security of government websites.

D5.3 SOFTWARE QUALITY

This Factor *examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this* Factor *reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the critical nature of services.*

***Stage*: Formative to Established**

There is no catalogue for assured software platforms and applications currently available for organisations across the public and private sectors, nor is guidance given consistently to all organisations on secure software development and maintenance.

For the FPA, there is an inventory of secure software, recommendations are in place for the secure development of software for use by the government, and software-maintenance procedures including patching and KPIs to evaluate patching effectiveness are in place in line with the FPA's cybersecurity regulations. The finance sector is mandated to comply with regulation from BACEN on the security of software used, and on secure lifecycle management.

In the telecommunications sector, the supply-chain audit provisions (which are described further in D5.1) mean that software providers to the sector must have policies for cybersecurity in place. This is not yet fully regulated, but it is intended that Anatel will have competence to audit providers of software to telecommunications services. It was noted that this is of particular importance given a tendency towards incorporating software-defined networks (SDN) into telecommunications infrastructure. In other sectors such as Electricity, there are provisions stating that companies should have policies for secure software development and maintenance; these criteria are not regulated.

Outside of the more mature sectors described above, software quality and security is variable. Participants were not aware of recommendations given by government on the secure development of software, selection of secure software applications, or secure maintenance of software, that would extend to private-sector organisations. Participants expressed the view that guidance for all organisations on assured software platforms and applications would be beneficial, which guide all organisations in Brazil in selecting software for use. Furthermore, guidance extending to all organisations on secure software development and maintenance processes may be beneficial.

D5.4 COMMUNICATIONS AND INTERNET INFRASTRUCTURE RESILIENCE

This Factor *addresses the existence of reliable Internet services and infrastructure in the country, as well as rigorous security processes across private and public sectors. Also, this* Factor *reviews the control that the Government might have on its Internet infrastructure and the extent to which networks and systems are outsourced.*

***Stage*: Established to Strategic**

Reliable Internet services are widely available in Brazil and widely used, including for conducting e-commerce and electronic business transactions, with appropriate authentication processes established for most transactions. Participants generally agreed that there is a high level of resilience of the Brazilian Internet infrastructure, with reportedly no events in Brazil having caused major interruptions to Internet services. This is largely due to the decentralised structure, with a large number of Internet Service Providers (ISPs) operating in Brazil, and the presence of a large number of Internet eXchange Points (IXPs).

Internet services in Brazil are coordinated by the Brazilian Internet Steering Committee (CGI.br), which "*is comprised of members from the government, the corporate sector, the third sector and the academic community, and as such constitutes a unique Internet governance model for the effective participation of society in decisions involving network implementation, management and use*".[95] The decisions of CGI.br are implemented by the Brazilian Network Information Center, NIC.br.[96] Through these bodies, the national Internet infrastructure is formally managed and the redundant, decentralised approach is promoted.

[95] https://www.cgi.br/about/
[96] https://nic.br/about-nic-br/

There are over 15,000 registered ISPs in Brazil; one of the largest such markets in the world.[97] Large operators including Claro, Telefonica and Oi operate alongside a wide range smaller-sized providers. The IX.br system is the IXP system of Brazil, with 31 IXPs in Brazil in metropolitan areas, under the centralised management of CGI.br. Management includes strategic decisions that have been made on the necessity of developing more IXPs to help create resilience. NIC.br play an active role in maintaining the IXP landscape, funding IXPs in areas that cannot yet afford to fund them.

The telecommunications sector is regulated in general and for cybersecurity by the Brazilian National Telecommunications Agency, Anatel. Anatel has established regulatory requirements via Resolution No. 740 of 2020 for telecommunications companies to identify their assets, perform regular vulnerability tests, adopt national or international norms and standards of good practices in cybersecurity, and develop a cyber risk-management plan, cybersecurity training policy, and clear incident-response processes. The Resolution establishes requirements for the technologies deployed by telecommunications service providers, stating that providers must use, "*within the scope of its networks and services, telecommunications products and equipment from suppliers that have a cybersecurity policy compatible with the principles and guidelines set out in this Regulation and carry out periodic independent audit processes*". The Cybersecurity Requirements for Telecommunications Equipment Act (No. 77 of 2021) establishes more detailed cybersecurity requirements for telecommunications equipment, through which providers can submit to Anatel for approval of their equipment, in order to be permitted to sell to Brazilian telecommunications providers.[98]

Anatel has also published Act 2346 (2023), which sets minimum cybersecurity requirements for providers of customer-premised equipment (CPE, including modems, routers, access points), including requirements for factory and user-defined passwords, and other controls such as cryptographic controls for protecting passwords and access keys.[99] The CPE regulation will come in force in March 2024.

Participants reported that Anatel's cybersecurity requirements are not yet mandatory, but are intended to be. These regulations apply in theory to all telecommunications operators. Anatel noted that, in practice, with approximately 1,500 ISPs in the country, it is not possible to perform audits for all operators. As such, it is not clear that these practices – the management of deployed technologies, risk assessments, network monitoring and resilience testing, and incident-response plans – will be consistently achieved across all Internet-infrastructure providers.

Amongst larger ISPs there is generally strong practice, guided by the regulation of Anatel, with established CERTs. Participants felt there may currently be gaps in some of these capabilities, particularly in regard to smaller and medium-sized ISPs. There is not yet full oversight of the technologies used and acquired by Internet infrastructure providers, leading to some

[97]https://www.bnamericas.com/en/features/snapshot-brazils-3-largest-isps-and-their-capex-plans#:~:text=With%20over%2015%2C000%20registered%20internet,such%20markets%20in%20the%20world.

[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_yI3XCuMz8fweImNoyttQO8pA5ey8n7x_4PlmD_H2Fc85VrG

penetration of vendors from abroad with potential security issues, or of vendors with lacking security maturity, although, as described, progress is being made towards management and controlled acquisition of these critical technologies.

A similar picture was described for the presence of security-monitoring technologies and incident-response plans, with variable levels of maturity across the wide array of Internet infrastructure providers. Given the significant importance of smaller and medium sized providers to maintaining a resilient national Internet infrastructure, it may be valuable to consider further measures to develop consistent cybersecurity practices, such as the development of specialised and more basic cybersecurity guidelines for smaller ISPs. Participants noted the peer support and guidance of the NIC.br network operators group, and training provided to ISPs by NIC.br and CERT.br (which is maintained by NIC.br), and training partnerships of NIC.br with the consultants that are frequently contracted to implement technologies and response processes for the smaller ISPs.

There are processes in place to maintain an up-to-date understanding of the threats to Brazilian Internet infrastructure, and to assess the risks related to emerging technologies. Participants reported that a key mission of NIC.br is to improve the security of the Brazilian Internet and increase incident-handling capability. CERT.br conduct comprehensive programmes to detect and analyse threats and incidents occurring within the Brazilian Internet, using honeypots and tracked feeds relating to Brazilian IP addresses from international partners. Infrastructure operators are notified by CERT.br of threats and vulnerabilities, along with information about how to mitigate them. Furthermore, Anatel runs a working group with the major telecommunications operators to keep up-to-date on the management of cybersecurity risks, including analysing risks relating to more recent technological developments such as 5G. Minimum cybersecurity requirements have also been established for when establishing 5G networks, by GSI Normative Instruction No.4 (2020).[100]

D5.5 CYBERSECURITY MARKETPLACE

This Factor *addresses the availability and development of competitive cybersecurity technologies, cyber-insurance products, cybersecurity services and expertise, and the security implications of outsourcing.*

***Stage*: Formative to Established**

Participants generally agreed that the majority of cybersecurity technologies in Brazil are imported from abroad, often via domestic integrators. While there is some domestic production of cybersecurity technologies, and the domestic market is perceived to be growing, domestically produced cybersecurity products are not currently the market leaders. The exception of the armed forces, defence and intelligence services was noted, where domestically developed technologies are prioritised. The NCS establishes as a strategic goal to

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

encourage the development of cybersecurity solutions and Brazilian cybersecurity start-up companies, and a range of initiatives to promote and fund technology start-ups exist in Brazil.

There is variability in the extent to which, currently, organisations are able to identify and manage the security implications of reliance on foreign technologies. This could create risk in the context of an international supply chain. As noted in the preceding Factors of D5, cybersecurity requirements and practice between sectors and organisations or different sizes; some regulators, for example in the telecommunications, sector, place requirements on the providers of technologies to their sector. These are yet to be fully implemented, and for this example sector some participants expressed concerns about the potential dangers of reliance on foreign technologies by Brazilian telecommunications providers.

There are widespread cybersecurity consultancy services available for private and public organisations in Brazil. Participants described an active marketplace, with many national companies as well as large international companies offering consultancy services. The market is perceived to be very active in providing Security Operations Centre (SOC) services, CSIRT as a service, and high-quality local Cyber Threat Intelligence (CTI) services. Participants also reported that Brazilian cybersecurity skills are exported internationally as Brazilian consultancy services are contracted abroad. Stakeholders from organisations that hire cybersecurity consultants described a receiving a high level of high-quality competition in response to their tenders. Providers generally provide details of the professional certifications that they possess.

Participants also reported that for a range of sectors, a security-as-a-service concept is available from the sector authority (sometimes via their business partners). For example, CAIS (for the academic network), the Digital Government department (for digital government institutions) and the Department of Defence offer services such as CSIRT, CTI exchange, vulnerability analysis, and penetration testing.

Larger organisations described the tender processes they run to select cybersecurity-service providers, which include checking accreditations, experience, technical skills, and cybersecurity standards followed (e.g., ISO 27001). Participants noted that organisations' consideration of such factors in procuring a cybersecurity-service provider varies dependent on their maturity and risk appetite. There is not currently any accreditation of cybersecurity-service providers by a national body. This may be beneficial to guiding organisations in selecting reliable and secure service providers; particularly for organisations with limited cybersecurity expertise to inform their decisions. Participants also expressed the view that the opportunity to achieve such accreditation might benefit the service providers.

The view was expressed that accreditation of businesses providing products and services in cybersecurity might be a role that the National Cybersecurity Agency (which, as described in D1, is under development) could take on. Another potential approach recommended by participants was a self-regulatory model, in which the larger companies can assess the smaller companies providing cybersecurity services to them, and issue seals of approval, which providers use as recognition.

Participants noted the cybersecurity workforce deficit (which is discussed further in D3, noting that this is an issue worldwide), which increases the cost of hiring cybersecurity consultants. Views were expressed that capacity in this area needs to continue to increase in order to meet the continuously growing demand for cybersecurity services.

There is widespread use of cloud services by Brazilian organisations. Some organisations conduct risk assessments to determine how to mitigate the risks of outsourcing IT to a third party or cloud services; in particular larger organisations tend to have security requirements in place when procuring services including cloud. As described in Sections 5.1 and 5.2, the level of cybersecurity maturity varies between sectors and organisations of different sizes, and this also impacts on organisations' capability of manage cybersecurity risks when outsourcing.

For some sectors, the management of the security implications of outsourcing is driven by regulation. GSI in August 2021 established normative instructions for agencies of the FPA on the procurement of cloud services, including cybersecurity and data-privacy requirements.[101] The Central Bank (BACEN) also sets requirements for the financial sector on the procurement of data-processing, data-storage and cloud-computing services, via Resolution No. 4,658 of 2018.[102] The Digital Government department, a central point of contact for over 250 digital-government institutions, has created models for the procurement of cloud services; reportedly in the upcoming months institutions will have access to this additional model to validate requirements and support bidding processes.

Potential issues for SMEs were highlighted: many SMEs rely on cloud services for IT and cybersecurity services. Participants described a lack of understanding of how to use the cloud securely in organisations that do not have a dedicated IT or cybersecurity team, leading to mistakes in configuration or failure to update, and resulting in vulnerability. It might be beneficial to extend a more substantial awareness-raising or training offering to SMEs for the secure use of cloud and assessment of the risks, or to issue specific cloud-security guidelines suitable to organisations that have lower cybersecurity capability and resource.

Local companies that provide cloud services reported offering guidelines and safeguards to help guide customers in securely adopting cloud services. For example, in some cases, local companies acting as an intermediary to several other cloud services perform the risk management for these providers, safeguarding their clients.

The cyber-insurance market in Brazil is in its early stages. Most cyber-insurance product offerings, it was reported, are by multi-national insurance companies, with participants aware of few local companies offering cyber-insurance products. Some of the international products on offer specify conditions (e.g., cybersecurity-control requirements) that organisations must meet in order to be insurable.

Many participants in the review were aware of cyber-insurance products, but these had not yet been adopted by their organisations. The uptake of cyber-insurance offerings until recently has mainly been by large multi-national companies, but demand from Brazilian organisations is reportedly beginning to grow. The need for specific cyber-insurance products was recognised, with participants reporting that business-continuity insurance in Brazil would not tend to cover cyber-incidents.

An issue around the affordability of the cyber-insurance products currently offered was raised, preventing some organisations from taking up cyber-insurance policies. There was no evidence of any cyber-insurance products suitable for smaller and medium-sized enterprises

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

being offered. While some working-group discussions on the affordability of cyber-insurance offerings were reported, It is also not clear that there has yet been strategic identification of the cyber-insurance market needs. Identifying the needs of organisations in Brazil in this area through assessment of financial risks for the public and private sectors, as well as cost-related challenges, would be beneficial to informing the development of the cyber-insurance market.

D5.6 RESPONSIBLE DISCLOSURE

This Factor *explores the establishment of a responsible disclosure framework for the receipt and dissemination of vulnerability information across sectors, and whether there is sufficient capacity to continuously review and update this framework.*

***Stage*: Formative to Established**

The presence of a responsible-disclosure policy or framework varies between organisations. There is a vulnerability-disclosure framework in place for the federal government, enabling researchers who find vulnerabilities in government websites to report them. The Federal Cyber Incident Management Network (ReGIC) supports the sharing of threat and vulnerability information between FPA institutions (and the participation of all FPA institutions is mandatory), with other organisations able to join on a voluntary basis. CTIR.gov publishes alerts on vulnerabilities and threats to the FPA on its website, supported by consultation of sources such as CERT.br and the vulnerability databases relating to the main providers of IT solutions.[103]

Outside of the government, participants reported the larger, more advanced companies tend to have their own channels and frameworks in place for responsible disclosure. These frameworks include policies for disclosure and clear guidelines on the process and timeline for resolution. Some of these more advanced companies run bug-bounty programmes; particular examples in the financial sector were cited. Some other companies use a proxy CERT to receive notification of vulnerabilities in their infrastructure and provide feedback for Brazilian and foreign researchers. Participants noted that, as is broadly the case around the world, sometimes the response and resolution by a company that has been notified of a vulnerability may not be prompt; this is dependent on the nature of the vulnerability and the maturity of the company.

CERT.br plays a significant role in disseminating vulnerability and threat-intelligence information to its client organisations (which, as is described in D1.2, may voluntarily include any organisation in Brazil) via formal channels. Vulnerability information is gathered using sensors, vulnerability and threat information shared by the organisations and CERTs they work

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

with, and international partnerships, published on the CERT.br portal,[104] and disseminated to various information-sharing groups via MISP platforms.

Other CERTs described playing a similar role; for example, CAIS, the CERT for the academic network receives and disseminates vulnerability information from its stakeholders, and also creates alerts on new vulnerabilities listed in the international Common Vulnerabilities and Exposures platform (CVEs) that are distributed to their stakeholders. In various other sectors, there are mechanisms in place for sharing vulnerability information: for the telecommunications sector, working groups established by Anatel allow operators to share threat and vulnerability information using MISP platforms; there are also trusted groups sharing threat and vulnerability information via MISP platforms in the financial and oil and gas sectors, for example.

There are no specific legal protections in place for parties disclosing security flaws responsibly. Participants described a general culture of the more mature companies, which run their own disclosure channels or receive disclosures via a CERT, understanding the benefits of responsible disclosure and welcoming responsible disclosure of vulnerabilities, and refraining from legal attempting legal action against a party disclosing information responsibly. Whereas fifteen years ago, it is perceived, companies might have felt threatened and challenged researchers disclosing such information to them, today larger companies tend to view these researchers as allies.

Some less mature companies, however, may not yet understand the benefits of responsible disclosure. In order to encourage a wider range of organisations to introduce responsible-disclosure policies, channels and resolution approaches, and bug-bounty programmes, it was perceived that awareness-raising on responsible disclosure (and how it is different from genuine attacks and extortion) would be beneficial.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Standards and Technologies*, the following set of recommendations are provided to Brazil. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

ADHERENCE TO STANDARDS

R5.1.1 Develop a nationally-agreed baseline of cybersecurity standards and good practices, against which organisations from the public and private sectors can self-assess. The baseline standards will need to account for varying contexts and organisations' varying cybersecurity capability and resource levels, and will need to complement and interact appropriately with the existing and upcoming CI

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

regulations (which are described further in D1.3). As well as ICT-security standards, the baseline should include:

- cybersecurity standards and best practices guiding procurement processes (including risk management, lifecycle management, software and hardware assurance, outsourcing, and use of cloud services).
- cybersecurity standards for the provision of products and services (including software development, hardware-quality assurance, provision of managed services and cloud security).

R5.1.2 Consider issuing guidance to smaller-and-medium sized organisations on how to deploy a more basic level of cybersecurity controls that is achievable with more limited financial and personnel resources. The UK's Cyber Essentials scheme may be a useful example.

R5.1.3 Assign an entity responsibility for measuring (for example, collecting and analysing statistics on) the use of cybersecurity standards across the public and private sectors.

R5.1.4 Establish government programmes for promoting adherence to the identified standards across organisations in Brazil. Use insights into adoption (generated through R5.1.3) to identify and promote awareness within groups of organisations with lower levels of adoption.

SECURITY CONTROLS

R5.2.1 Promote the use of cybersecurity standards across public and private organisations in Brazil, so that the technological cybersecurity control sets used by organisations consistently reflect established cybersecurity frameworks, standards and good practices.

R5.2.2 Issue guidance or support to SMEs to increase their awareness of how to securely adopt cloud services.

R5.2.3 Consider how to increase the use of digital certificates by organisations in Brazil. This might include running awareness campaigns, or putting in place to measures prohibitive practical factors.

R5.2.4 Promote the use of tools to test the implementation of cryptographic protocols, such as the tool made openly available by CERT.br.

SOFTWARE QUALITY

R5.3.1 Issue guidance for all organisations on how to identify secure and reliable software platforms and applications. This may take the form of a catalogue of assured software, or of guidance on how to assess software quality, functional and security requirements.

R5.3.2 Issue guidance for all organisations on software updates and maintenance (including patch management).

R5.3.3 Develop a framework for measuring the security of software and application of software-maintenance policies across organisations (for example, collecting and analysing statistics).

R5.3.4 Assign a body responsible for gathering evidence of software security and deficiencies, and characterisation software applications as to their reliability, usability, performance and security in adherence to international standards and good practices. The information gathered can be used to issue guidance to organisations in Brazil.

COMMUNICATIONS AND INTERNET INFRASTRUCTURE RESILIENCE

R5.4.1 Identify (for example, through consultations with stakeholders from the telecommunications sector) how to maintain oversight of cybersecurity practice and the acquisition of technologies across the very large number of ISPs in Brazil. Consider whether implementing automated approaches to reporting and analysing practice may be beneficial.

R5.4.2 Given the importance of small-and-medium-sized ISPs to maintaining a resilient national Internet infrastructure, consider further measures to develop consistent cybersecurity practices, such as the development of specialised and more basic cybersecurity guidelines for smaller ISPs

R5.4.3 Ensure that Anatel's regulation is kept up-to-date through regular assessments of the impacts of emerging technologies, the risks to the telecommunications sector, and processes for compliance with international standards.

CYBERSECURITY MARKETPLACE

R5.5.1 Convene relevant stakeholders to consider the security implications of using foreign cybersecurity technologies, and consider whether any actions are needed to mitigate potential risks.

R5.5.2 Issue and promote guidance for organisations in Brazil on how to identify and manage the security implications of reliance on foreign technologies.

R5.5.3 In promoting the growth of the domestic cybersecurity-technology marketplace, ensure that secure development processes are promoted, according to internationally accepted standards.

R5.5.4 Review the supply and demand for cybersecurity-service providers to Brazilian companies, to ensure that the offering meets the continuously growing demand.

R5.5.5 Create an approach to accrediting cybersecurity-service providers. Accreditation may come from a central body (such as the new national cybersecurity agency), or may follow a self-regulatory model, as suggested by participants, in which the larger companies can assess the smaller companies providing cybersecurity services to them, and issue seals of approval, which providers use as recognition.

R5.5.6 Extend awareness-raising or training offerings to SMEs on the secure use of cloud and assessment of associated risks, and/or issue cloud-security guidelines suitable to organisations that have lower cybersecurity capability and resource.

R5.5.7 Identify the cyber-insurance needs of organisations in Brazil through consultations to assess the financial risks for the public and private sectors as well as cost-related challenges, to inform the development of the cyber-insurance market.

RESPONSIBLE DISCLOSURE

R5.6.1 Conduct awareness-raising for organisations on responsible disclosure of vulnerabilities (and how it is different from genuine attacks and extortion), in order to increase awareness and ensure understanding of benefits of responsible disclosure.

R5.6.2 Promote the development of responsible-disclosure policies, channels and resolution approaches, and bug-bounty programmes amongst a wider range of Brazilian organisations. This might be supported by improved awareness as recommended in R5.6.1.

R5.6.2 Consider putting in place specific legal protections for parties disclosing security flaws responsibly.

ADDITIONAL REFLECTIONS

The level of stakeholder engagement in the review was good, and the representation and composition of stakeholder groups was, overall, balanced and broad. This enabled the review team to collect comprehensive evidence to support this CMM review.

APPENDICES

METHODOLOGY - MEASURING MATURITY

Deploying the CMM involves data-gathering both through in-country stakeholder consultation (typically over the course of three days) and remotely through desk research. It is designed to produce an evidence-based report which is submitted to the government representatives for the country being studied and will include recommendations to:

- benchmark the maturity of a country's cybersecurity capacity;
- provide a detailed a set of pragmatic actions to contribute towards the advancement of cybersecurity capacity
- identify maturity gaps; and
- identify priorities for investment and future capacity-building.

During the review of a country, specific dimensions are discussed with relevant groups of stakeholders. Each group of stakeholders is asked to respond to one or two dimensions of the CMM, depending on their expertise. For example, Academia, Civil Society and Internet Governance groups would all be invited to discuss both Dimension 2 'Cybersecurity Culture and Society' and Dimension 3 'Building Cybersecurity Knowledge and Capabilities' of the CMM.

Data collection

The Review Team gathers the evidence necessary to identify the stages of maturity across the CMM through desk research, in-depth interviews, and modified-focus group discussions, utilising the CMM Structured Field Coding (SFC) Tool to capture the results. The functions of the Review Team include that of a facilitator to lead the group sessions, and a note-taker.

The CMM uses a **modified focus-group discussion methodology** that elicits data that complements and helps validate in-depth interviews and desk research.[105] As with interviews, focus-group discussions are an interactive methodology with the advantage that during the process of collecting data, diverse viewpoints and conceptions can emerge as participants follow the discussion. Rather than posing questions to specific participants, the researcher(s) facilitate a discussion among the participants, encouraging them to adopt, defend or explain

[105] Williams, M. (2003). Questionnaire design. In *Making sense of social research* (pp. 104-123). SAGE Publications, 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* (pp. 35-50). SAGE Publications, Inc., https://www.doi.org/10.4135/9781483349008; Richard A. Krueger, R. A., & Mary Anne Casey, M. A., (2009) Focus-groups: A Practical Guide for Applied Research. SAGE Publications, London.

different perspectives.[106] It is this interaction that offers advantages over other methodologies, making it possible for the participants to reach a mutual understanding and to raise everyone's awareness of cybersecurity practices and capacities.[107] During CMM reviews, the Review Team leads the discussion to get onto all the aspects within the relevant dimensions.

To determine the level of cybersecurity capacity maturity, each *Aspect* has a set of indicators corresponding to all five stages of maturity. A consensus method is used to drive the discussions within sessions, for the stakeholders to provide evidence on how many indicators have been implemented by the country and to determine the maturity level of every aspect of the model. During focus-group discussions, researchers use semi-structured questions to keep discussions around relevant indicators. The discussion among stakeholders provides evidence regarding the implementation of indicators. In gauging the maturity level, if there is no evidence for all the indicators being met at a particular stage, then that country has not yet reached that stage of maturity.

Inconsistencies between stakeholders will inevitably occur. Equally, information known to a stakeholder in one sector might not be familiar in other sectors. Accordingly, it will fall to the Review Team to perceive these information gaps and then investigate them.

Desk research and modified focus groups inevitably raise some additional questions and possible inconsistencies. For this reason, and to a gain more in-depth understanding of key and sometimes unique policies and practices, a set of in-depth interviews are also conducted during and on some occasions following the field research.

Data analysis

With the prior consent of participants, all sessions are recorded. Individual responses are treated as confidential with the Chatham House Rule applied in reporting our results.[108] After conducting a country review, the **data collected during consultations** with stakeholders and the notes taken during the sessions are used to find evidence and **define the stages of maturity** for each *Aspect* of the CMM. The CMM report aggregates this information and determines the maturity for each Factor of the CMM.

In the course of the review further desk research is undertaken to bridge any gaps that emerge during the in-country data-collection process and to validate the evidence provided. While drafting the **CMM report**, further desk research and interviews are often necessary to address any missing information, and to validate and verify the results. For example, stakeholders might not always be aware of recent developments in their country, or if the country has signed a particular convention on personal data protection policy. Therefore, official

[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, E. F. (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. *Bmj*, *311*(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299

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

government or ministry websites, annual reports of international organisations, university websites, in-depth interviews, etc. can be used as supplementary sources for information. This type of additional research helps to ensure that the report accurately reflects the Host Country's cybersecurity capacity. In each case, the team does not privilege any particular source of information but seeks to reach a consensus on the most valid status of each indicator of the model.

Developing recommendations

For each *Dimension*, **recommendations** are provided for the next steps to be taken for the country to enhance its cybersecurity capacity. If a country's capacity for a certain *Aspect* is, for example, at a formative stage of maturity then by looking at the CMM the indicators which will help the country move to the next stage can be easily identified. Recommendations might also arise from discussions with and between stakeholders. The recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the CMM. The recommendations are provided specifically for each *Factor.*

After a review by the GCSCC Technical Board, the draft report is submitted to the Local Host to secure feedback. If new evidence arises, the draft report is revised and the maturity stages of each *Aspect* and *Factor* in the CMM are updated correspondingly. Once all parties approve the draft report, the Local Host will take the lead in the publication process. Publication approval rests with the Host Country and if this is agreed the Local Host is encouraged to publish it via an official government portal or other outlet.

Data management and ethical considerations

Focus-group discussions are conducted online on Microsoft Teams™ and Zoom™ platforms. *(depending on platforms preferred by each nation)* The discussions are recorded using external recorders to guarantee confidentiality of the data and information collected, and for future transcription for the purpose of writing the CMM report. The recordings remain anonymised. The findings from the desktop study, in-depth interviews, and focus group discussions are consolidated during the analysis.

Global Cyber Security Capacity Centre

Department of Computer Science, University of Oxford

Wolfson Building, Oxford OX1 3QD,

United Kingdom

Tel: +44 (0)1865 287434

Email: cybercapacity@cs.ox.ac.uk

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

Sponsored by

UK Government