Disclaimer

This is an unofficial translation made for academic purposes only. The translator has been trustworthy to the original text in Portuguese, even when facing grammar mistakes or unusual word choices or verbal modes, avoiding corrections or changes that could mischaracterise the original choices of its authors. The only exceptions where in the cases of words wrongly spelled in Portuguese, and in the referencing of documents, not identifiable in the original text (in this English version put inside brackets).

NATIONAL CYBERSECURITY STRATEGY

This National Cybersecurity Strategy - E-Ciber is a manifest guidance from the Federal Government to Brazilian society on the main actions it intends, in national and international terms, in the area of cybersecurity and will be valid in the 2020-2023 quadrennium.

1. PRELIMINARY CONSIDERATIONS

1.1. EXECUTIVE SUMMARY

In 2015, the Federal Government publicised the Information and Communications Security and Cybersecurity Strategy of the Federal Public Administration [1], valid until 2018, as an important tool to support the planning of Government bodies and entities, whose objective was to improve the security and resilience of critical infrastructure and national public services. That document stimulated discussions on the topic within the scope of the Federal Public Administration, and in other sectors of society.

Decree 9.637, of December 26, 2018 [2], which instituted the National Information Security Policy and provides for principles, objectives, instruments, attributions and powers of information security for Federal Administration bodies and entities, under the prism of governance, foreseen, for its implementation, the elaboration of the National Information Security Strategy and its National Plans. Due to the scope of Information Security, Decree 9.637, of 2018, indicated, in its Article 6, that the National Information Security Strategy will be built in modules, in order to contemplate cybersecurity, cyber defence, the security of critical infrastructures, the security of confidential information and the protection against data leakage.

In compliance with the provisions of the National Information Security Policy, and considering Cybersecurity – Cyber Sec as the most critical and present area to be addressed, the Institutional Security Office of the Presidency of the Republic elected, in January 2019, the National Cybersecurity Strategy - E-Ciber as the first module of the National Information Security Strategy, under its responsibility, to be developed.

Thus, under coordination of the Institutional Security Office of the Presidency of the Republic, and with the participation of more than forty Government bodies and entities, as well as private institutions and the academic sector, which were distributed in three working subgroups, the present E-Ciber has been elaborated, after thirty-one meetings and seven months of studies and debates.

Using a bottom-up methodology, and based on the conclusions of the working subgroups, in comparative assessment - benchmarking on related strategies from other countries, and

in compliance with the National Information Security Policy – a diagnosis of global and Brazilian cybersecurity was developed. Following, the national strategic objectives and their respective strategic actions were established, according to seven lines of action, which demonstrate to Brazilian society the points considered relevant for the country in the area of cybersecurity.

1.2. INTRODUCTION

The digital revolution is deeply transforming our society. Over the last two decades, billions of people have benefited from the exponential growth of access to the Internet, the rapid adoption of information and communication technology resources, and the economic and social opportunities arising from the digital environment.

Rapid advances in the area of information technology and communication have resulted in intense use of cyberspace for a wide range of activities, including the provision of services by the Federal Government, consistent with global trends. However, new and growing cyber threats arise in the same proportion, and put public administration and society at risk.

Thus, protecting cyberspace requires attentive vision and leadership to manage continuous political, technological, educational, legal and international changes. In this sense, the Government, industry, academia and society in general shall encourage technological innovation and the adoption of cutting-edge technologies, and maintain constant attention to national security, the economy and free expression.

At a higher level than the debates on security in cyberspace is Information Security, a systemic area, directly related to the protection of a set of information and to the value it has for an individual or an organisation. Thus, according to Article 2 of Decree 9.637, of 2018, Information Security comprehends cybersecurity, cyber defence, physical security and the protection of organisational data, and has as fundamental principles confidentiality, integrity, availability and authenticity.

It is understood that the technological resources employed in systemic security shall support policies that ensure the fundamental principles of data authenticity and integrity, and provide mechanisms to protect its legitimacy against unauthorised change or disposal. Likewise, information collected, processed and stored in the information and communication technology infrastructure shall be accessible only to authorised persons, processes or entities, in order to ensure the confidentiality of that information. Additionally, information and communication technology resources must provide permanent availability and continuously support all authorised accesses.

E-Ciber, in addition to filling an important gap in the national normative framework on cybersecurity, establishes actions aimed at modifying, in a cooperative way and at the national level, characteristics that reflect the positioning of institutions and individuals on the subject. First, it turns out that there are good managerial initiatives in this area. However, they are fragmented and punctual, making it difficult to converge efforts in the sector. Second, there is a lack of normative, strategic and operational alignment, which often generates rework or results in the constitution of task forces for specific actions, impairing the absorption of lessons learned and jeopardising the prolonged effectiveness of these actions. Third, it is observed the existence of different levels of cybersecurity maturity in society, which results in varied perceptions of the real importance of the topic.

After this introductory part, it is presented the methodology adopted in the lines of analysis, which were based on the study of two sets of thematic axes: those of Protection

and Security, and the so-called Transformative. It is also addressed how the working subgroups were structured, according to the proposed topics.

In Part I, a diagnosis of cybersecurity is presented, based on the international scenario and the national scenario, with special attention to cyber threats, attacks and vulnerabilities, and to how these elements impact the society and institutions.

The thematic axes are presented separately in Part II. First, those related to protection and security are addressed: national cybersecurity governance, the connected and secure universe and strategic protection. Then, we analyse those which, by their nature, are called Transformative: the normative dimension; research, development and innovation; the international dimension and strategic partnerships; and education.

Due to the diagnostic analysis and the study of the thematic axes, the strategic objectives are presented and, then, the strategic actions, elaborated in order to achieve the specified objectives. Through these actions, for which plans are recommended, valuable directions are pointed out, capable of leading society and institutions to a prosperous, resilient and safe environment, as an ideal condition for economic growth and social development.

Finally, it is important to emphasise that during the presentation of the Strategy, several terms related not only to cybersecurity, but also to the larger field of information security studies are mentioned. In order to clarify them, if necessary, it is recommended to consult the Information Security Glossary, published by Ordinance 93, of September 26, 2019, of the Institutional Security Office of the Presidency of the Republic [3].

As a result of this Strategy, it is recommended that each body in the public and private sectors, plan and carry out administrations in order to put into practice the aspects that are appropriate and that are established in the strategic actions, in a joint and dedicated effort, for the full achievement of the country's strategic objectives, in the critical and current theme of national cybersecurity.

1.3. ADOPTED METHODOLOGY

The Strategy is the result of work carried out by representatives of public bodies, private entities, and academia, who participated in a series of technical meetings to discuss various aspects of cybersecurity. When considering the wide range of subjects, these representatives were divided into three subgroups, constituted as follows:

- Subgroup 1 - cyber governance, normative dimension, research, development and innovation, education, international dimension and strategic partnerships;

- Subgroup 2 - digital trust and prevention and mitigation of cyber threats; and

- Subgroup 3 - strategic protection - government protection and infrastructure protection.

Thirty-one meetings of the subgroups were held, with the effective participation of all these representatives of remarkable knowledge, which enabled the exchange of knowledge and ideas, and which contributed decisively to establish the strategic design.

In order to structure the debates, the work followed four stages:

First - Diagnosis - survey and mapping of initiatives, related actors and existing actions;

Second - Subgroup debates - weekly meetings with related actors and guests of notorious knowledge;

Third - Public consultation – provision of the document on the Internet for contributions and broad participation of society in general; and

Fourth - Approval and publication - finalisation of the proposal and submission to presidential approval.

Additionally, it was considered the cybersecurity capacity maturity model [4], which defines five dimensions:

- cybersecurity policy and strategy;

- cybernetic and societal culture;

- cybersecurity education, training and skills;

- legal and regulatory frameworks; and

- standards, organisations and technologies.

These dimensions, due to their transversality, cover the extensive areas that shall be considered in increasing cybersecurity capacity. When considering the five dimensions of the model, the structure of seven axes of the Strategy's, previously mentioned, which maintains a direct relationship with the cybersecurity capacity maturity model, was reached.

The thematic axes of E-Ciber have been considered in a transversal way, and can be described as:

- Protection and Security Axes:
    - national cybersecurity governance;
    - connected and secure universe: prevention and mitigation of cyber threats; and
    - strategic protection; and
- Transformative Axes:
    - normative dimension;
    - international dimension and strategic partnerships;
    - research, development and innovation; and
    - education.

The methodology described above allowed the gathering of relevant information, which resulted in a systemic national strategic conception.

The final conclusions of this work resulted in a first version of E-Ciber, which was made available for participation by society in the form of a public consultation, launched via the Internet on September 10, 2019, made available for twenty consecutive days and accessed by forty-one participants. Of this total, there were thirty-one individuals and ten public and private organisations that sent one hundred and sixty-six contributions. After analysing all the contributions received, the present version was approved by His Excellency the President of the Republic.

1.4. STRATEGIC CONCEPTION

From the analysis of the Thematic Axes contained in Part II, the present conception it was reached at this conception, which results from the interaction between the axes mentioned above, vision, and strategic objectives, in an approach that culminated in national strategic actions.

2. THE NATIONAL CYBERSECURITY STRATEGY

2.1. VISION FOR BRAZIL

Become a country of excellence in cybersecurity.

2.2. STRATEGIC OBJECTIVES

In order to meet the proposed vision, in the design of strategic objectives, the parameters established in the National Information Security Policy were considered: the maturity stage and the needs of the country in cybersecurity and aspects relating to the digital ecosystem, at the national and international level.

Thus, these strategic objectives aim to guide the country's strategic actions in cybersecurity, and represent basic macro-guidelines so that the public sector, the productive sector and society can enjoy a resilient, reliable, inclusive and secure cyberspace. These are the strategic objectives:

1. Make Brazil more prosperous and reliable in the digital environment;
2. Increase Brazilian resilience to cyber threats; and
3. Strengthen Brazilian performance in cybersecurity on the international stage.

2.3. STRATEGIC ACTIONS

In view of the aspects addressed in Part I - Diagnosis, and the considerations made about the situation of national cybersecurity in Part II - Analysis of Thematic Axes, ten strategic actions were established.

It is emphasised that it is absolutely essential that each public sector and private sector body identifies, plans and executes the actions of its competence, so that the Country makes the directions materialised by each strategic action a reality.

2.3.1. Strengthen cyber governance actions

Strengthen cybersecurity governance actions by the public and private sectors, which include initiatives related to people management, meeting cybersecurity requirements and the management of information assets. Among the actions that can be taken in this regard, mention is made of:

- hold governance forums;

- create controls for the treatment of information with restricted access;

- establish minimum requirements for cybersecurity in contracting by public agencies;

- implement cyber governance programmes and projects;

- adopt, in addition to the governance norms issued by the Institutional Security Office of the Presidency of the Republic, rules, standards and governance models recognised worldwide;

- adopt, in industry, international standards in the development of new products since its conception (privacy/security by design and default);

- recommend the adoption of national cryptographic solutions, observing, for this purpose, the specific legislation;

- intensify the fight against software piracy;

- adopt cybersecurity solutions that address integrative initiatives;

- designate the information security manager;

- recommend cybersecurity certification, according to international standards; and

- expand the use of the digital certificate.

2.3.2. Establish a centralised governance model at the national level

Establish a centralised governance model for the country, by creating a national cybersecurity system, with the following attributions:

- promote the coordination of the various actors related to cybersecurity, in addition to the federal sphere;

- promote a joint analysis of the challenges faced in combating cybercrime;

- assist in the formulation of public policies;

- create a national cybersecurity council;

- create cybersecurity discussion groups, in different sectors, under the coordination of the Institutional Security Office of the Presidency of the Republic, to foster discussions on the subject, through informal participation mechanisms;

- establish routine cybersecurity compliance checks, internally, in public agencies and private entities; and

- allow the convergence of efforts and initiatives, and act in a complementary manner to receive complaints, investigate incidents and promote the awareness and education of the society on the subject. To make its implementation feasible, the Institutional Security Office of the Presidency of the Republic will be responsible for coordinating cybersecurity at the national level, which will enable it to act in a broad, cooperative, participatory manner, and in line with cyber defence actions, in charge Ministry of Defence.

2.3.3. Promote a participatory, collaborative, reliable and safe environment, between the public sector, the private sector and society

Promote a participatory, collaborative and secure environment among public organisations, private institutions, academia and society, through the continuous and proactive monitoring of threats and cyberattacks, with the aim of:

- stimulate the sharing of information about cyber incidents and vulnerabilities;

- conduct cyber exercises with the participation of multiple actors;

- establish mechanisms that allow interaction and information sharing at different levels;

- strengthen the Centre for Treatment and Response to Government Cyber Incidents - CTIR Gov and keep it updated in personnel and material;

- highlight the role of the Cyber Incident Treatment and Response Centres - national CSIRTs;

- improve the national cybercrime investigation infrastructure;

- stimulate the creation and action of a team to deal with and respond to cyber incidents - ETIRs, with emphasis on the use of emerging technologies;

- issue alerts and recommendations; and

- stimulate the use of cryptographic resources, within the scope of society in general, for the communication of matters considered sensitive.

2.3.4. Raise the level of government protection

Raise the level of Government protection, through actions in the cyber field, such as:

- include cybersecurity requirements in contracts established by Government bodies and entities;

- improve and encourage the use of the Government's secure communication devices;

- improve and maintain up-to-date information systems, infrastructures and communication systems of public agencies, in relation to cybersecurity requirements;

- recommend that public agencies have updated and automatically segregated backup copies in a protected location;

- elaborate specific cybersecurity requirements related to the use of endpoints in public organisations, understood here, in short, as final equipment connected to a terminal of some network or to some communication system;

- include, in cybersecurity policies, requirements related to supply chain management;

- include cybersecurity requirements in the privatization processes, when involving essential services; and

- monitor the implementation of minimum cybersecurity requirements by suppliers that are part of the supply chain.

2.3.5. Raise the level of protection for National Critical Infrastructures

Provide critical infrastructures with greater resilience that enables the continuous provision of essential services, through the following actions:

- promote interaction between critical infrastructure regulatory agencies to address issues related to cybersecurity;

- stimulate the adoption of cybersecurity actions by critical infrastructures;

- encourage these organisations to implement cybersecurity policies, which include, among other aspects, metrics, evaluation mechanisms, and periodic review;

- encourage the constitution of ETIRs*;

- encourage critical infrastructures to notify CTIR Gov† of cyber incidents; and

- encourage the participation of critical infrastructure in cybernetic exercises.

2.3.6. Enhance the legal framework on cybersecurity

To improve the legal framework on cybersecurity, review and update existing regulations, address new topics and develop new instruments. In this sense, the following actions can be adopted, such as:

- identify and address issues absent from current legislation;

- make efforts to include, in Decree-Law 2,848, of December 7, 1940 - Penal Code, new types of cybercrimes;

- develop norms on emerging technologies;

- create incentive policies for hiring skilled labour in cybersecurity;

---

* Incident emergency response teams.

† Government Computer Incident Response Centre.

- define cybersecurity requirements in remote work programmes; and

- develop, under the coordination of the Institutional Security Office of the Presidency of the Republic, a draft law on cybersecurity, with guidelines that will provide macro-strategic alignment to the sector and contribute decisively to increase the security of organisations and citizens.

2.3.7. Encourage the design of innovative cybersecurity solutions

Seek the alignment between academic projects and the needs of the production area, in order to encourage research and development of cybersecurity solutions, which bring the necessary innovation to national products in this critical, current and essential area. Among the actions to be considered, it can be mentioned:

- propose the inclusion of cybersecurity in research promotion programmes;

- encourage the creation of cybersecurity research and development centres within the federal executive branch and in the private sector;

- enable investments in research, through public and private funds;

- create programmes to encourage the development of cybersecurity solutions;

- stimulate the creation of start-ups in the cybersecurity area;

- stimulate the development and innovation of cybersecurity solutions in emerging technologies;

- encourage the adoption of global technology standards, which will allow interoperability on an international scale;

- encourage the development of skills and solutions in cryptography;

- encourage further research on the use of spectral intelligence; and

- establish minimum cybersecurity requirements that ensure the full, responsible and safe use of the fifth-generation mobile connection technology - 5G.

2.3.8. Expand Brazil's international cooperation in Cybersecurity

Expand Brazil's cooperation in cybersecurity with the largest possible number of countries, in a transparent manner, and reinforce the country's position in the constant search for peace and international security, according to the tradition of national diplomacy based on the principles established in Article 4 of the Constitution. To make this intent feasible, the following measures can be adopted:

- stimulate international cooperation on cybersecurity;

- encourage discussions on cybersecurity in international organisations, forums and groups of which Brazil is a member;

- expand the international relationship with Latin American countries;

- promote international events and exercises on cybersecurity;

- participate in international events of interest to the country;

- expand cooperation agreements on cybersecurity;

- expand the use of international mechanisms to combat cybercrimes;

- stimulate the country's participation in future normative structuring initiatives, such as those related to the creation of security standards in emerging technologies, and

- identify, stimulate and take advantage of new business opportunities in cybersecurity.

2.3.9. Expand the partnership, in cybersecurity, between public sector, private sector, academia and society

Expand partnerships between the various sectors of society, with a view to raising, in general, the level of cybersecurity. It is visualised the effective cooperation of the productive sector with academia, through financial and material resources, and according to their needs, investing in the training of university students. Among the possible actions, the following stand out:

- expand cooperation between Government, academia and private initiative to promote the implementation of E-Ciber;

- maintain a collaborative environment that allows for the study and wide use of emerging technologies;

- establish partnerships to encourage the private sector to invest in cybersecurity measures;

- encourage meetings with prominent players in cybersecurity;

- stimulate the establishment, if necessary, of working groups and forums on cybersecurity;

- encourage the creation of mechanisms for sharing information on cyber risks; and

- establish partnerships between the Union, the States, the Federal District, the Municipalities, the Public Ministry and the academia, for the implementation of programmes, projects and actions in cybersecurity, which reach the whole society.

2.3.10. Raise the level of maturity in cybersecurity society

Raise the level of maturity in cybersecurity in society, in order to provide an understanding of threats and risks in cyberspace, and enable people to use the appropriate and timely procedures and tools for the safe use of the digital environment. In this sense, the following are identified as initiatives:

- encourage public agencies and private companies to carry out internal awareness campaigns;

- carry out public awareness actions;

- create public policies that promote society's awareness of cybersecurity;

- propose the inclusion of cybersecurity, through its basic skills, and the ethical use of information in basic education - early childhood education, elementary school and high school;

- encourage the creation of higher education courses in cybersecurity;

- propose the creation of incentive programmes for undergraduate and graduate students in Brazil and abroad in cybersecurity;

- foster research and development in cybersecurity;

- create continuous training programmes for professionals in the public and private sectors;

- encourage the training of professionals to act in the fight against cybercrimes;

- hold cybersecurity training events;

- encourage participation in national and international cybersecurity forums and events;

- improve mechanisms for integration, collaboration and incentives between universities, institutes, research centres and the private sector in relation to cybersecurity;

- encourage cybersecurity simulation exercises; and

- promote cybersecurity knowledge management, in conjunction with the main players in the field, in order to optimize the identification, selection and use of talents.

PART I

DIAGNOSIS

In 2018, more than half of the world population used the Internet (four billion and one hundred million users, representing fifty-four per cent of the world population), with ninety-three per cent of access to social networks via mobile devices [5]. According to an estimate by the statista.com portal, there will be more than thirty billion Internet of Things (IoT) devices connected by 2020.

This scenario of progressive connectivity, in which thousands of devices have simultaneous access to data networks and the Internet, offers users a wide variety of online services, and provides citizens with comfort and convenience in daily life.

However, while the growth of this connectivity results in benefits for users, it also brings with it a wide range of cyber vulnerabilities, which pose threats and attacks that can cause damage of all kinds, with different levels of impact for people and institutions.

In financial terms, considering cyberattacks, global losses of US$ 600,000,000,000.00 (six hundred billion dollars) are estimated per year [6]. The 2019 International Monetary Fund's Report highlighted that, in all economies, the guideline is the implementation of actions that strengthen resilience, while electing, as necessary, the search for greater multilateral cooperation to manage cybersecurity risks [7].

The almost complete digitisation of business models has made the global economy more efficient and dynamic, and also more vulnerable to cyberattacks. The variety and complexity of threats put at risk the essential trust in the digital world, a key factor for online activities. This scenario leads to increasing joint investments between Governments and productive sectors. As a result, it is estimated that, in 2020, the global cybersecurity market will be valued at US$ 151,000,000,000.00 (one hundred and fifty-one billion dollars) [8]. By way of comparison, it can be seen that, currently, the Brazilian cybersecurity market moves close to US$ 2,000,000,000.00 (two billion dollars) per year with the sale of software, hardware and services [9].

The Brazilian case is highlighted below. The report on the ranking of information and communication technology of the United Nations - UN analyses the world development index in information technologies and their application in the advances of the Internet. It also studies how modern technologies will allow innovations and "fundamentally" transform businesses, governments and societies. In the regional ranking of the Americas, Brazil is only in tenth place, behind countries like Barbados, Bahamas, Argentina and Chile. According to the report, however, Brazil is one of the largest telecommunications markets in the region. The expectation is that the quality and coverage of services will "significantly" improve in the coming years [10].

The risk to the Brazilian economy, generated by the intrusion into computers and the spread of malicious codes practised by organised crime is already a reality, as can be seen

from the data below, regarding the connectivity of the Government, the private sector and citizens, to the indexes and cybercrimes [11]:

- Brazil ranks 66th in the ranking of the United Nations - UN of information and communication technology (1);

- Only 11% of federal agencies have a good level of IT governance (2);

- Brazil ranks 70th in the Global Security Index, from ITU (3);

- 74.9% of households (116 million people) with Internet access (4);

- 98% of companies use the Internet (5);

- 100% of federal and state agencies use the Internet (6);

- In 2017, there were seventy million and four hundred thousand victims of cybercrimes (7);

- In 2018, 89% of executives were victims of cyber fraud (8);

- Security issues discourage electronic commerce (9);

- In 2017, cybercrime resulted in US$ 22,500,000,000.00 (twenty-two billion and five hundred million dollars) of loss (10); and

- Brazil is the second most affected by cyberattacks (11).

According to the report of the “Internet Organised Crime Threat Assessment - IOCTA” [12], 2018, of the European Union Agency for Law Enforcement Cooperation - Europol, “the lack of adequate legislation on cybercrimes has made Brazil the number one target and the main source of online attacks in Latin America; 54% of cyberattacks reported in Brazil are supposed to originate from within the country”. The document goes on to state that, "similarly to the USA, Brazil is one of the main hosts of phishing sites, with some reports placing Brazil as one of the top ten global sources of cyberattacks".

It is also verified that the number of cyberattacks practically doubled in Brazil in 2018 compared to 2017. According to information from the specialised cybersecurity laboratory at PSafe [13], one hundred and twenty million and seven hundred thousand attacks were detected in the first half of 2018. This number represents an increase of 95.9% in relation to the same period of the previous year. In the last three months of 2018, sixty-three million and eight hundred thousand malicious links were registered, an increase of 12% in relation to the beginning of that year, with links sent through messaging applications like WhatsApp being the champions of scams. In all, 57.4% of the attacks were carried out through phishing, while, second, were the scams with suspicious advertising, which accounted for 19.2% of the cases.

The Cyber Review 2019 survey by consultancy JLT [14], carried out with 200 medium and large Brazilian companies, showed that 55.4% of these companies are totally dependent on the use of technology in their activities and that another 35% may have severe paralysation in the face of a technology-related problem. Other relevant research data are highlighted below:

- 80% of respondents estimated that a cyber incident would have an operational impact with an impact on the entire company;

- 29% have already financially assessed what this impact would have on their organisations;

- 34% of companies that responded to the survey reported having experienced some type of cyber incident in the last twelve months;

- 29% of companies that suffered attacks had operational impacts;

- 27.8% had high systemic reconstruction costs; and

- 4% suffered reputation impacts with customers.

Data from this research demonstrate that Brazilian companies, especially those considered as critical infrastructures, need to consider cybersecurity as a priority investment action, develop risk management and incident response and treatment plans, as well as plan an adequate budget to combat security incidents. In more than half of the companies surveyed in the Tempest/EZ-Security [15] survey, the annual information security budget represents up to 2% of annual revenue. In 34.5% of these companies, this percentage does not exceed 1%, according to the same survey.

A major cyberattack, if not properly dealt with, can profoundly affect the organisation's reputation, cause loss of revenue, lead to operational losses with the stoppage of services, result in loss of information and also lead to the application of legal and regulatory or administrative sanctions.

Thus, it is important that organisations, public or private, establish cybersecurity policies and procedures that are periodically reviewed, meet technological developments, process improvement and the need for continuous and structured training for all employees, through qualification and training programmes. According to the JLT CyberView 2019 survey, in 2017, 35% of organisations mentioned not having a cybersecurity contingency plan; in 2019, 44.2% stated that, in addition to not having a contingency plan, they also did not provide for a possible crisis in their budgets.

In the last decade, not only in Brazil, but in several countries, there has been a significant increase in the number of services provided to citizens through the Internet. Among the various services, the following stand out: registration, obtaining negative certificates, paying taxes, the duplicate of documents and consultations, which are provided on online platforms at the federal, state and municipal levels.

Initiatives such as the Digital Governance Policy - Decree 8,638, of January 15, 2016, the recent Brazilian Strategy for Digital Transformation - E-Digital - Decree 9,319, of March 21, 2018 [16] and governance in data sharing - Decree 10,046, of October 9, 2019, highlight the strong digitalisation process of the Federal Government and the parameters that underpin it throughout its implementation.

Furthermore, these initiatives, with an emphasis on technological change, mean, for the financial system, the adoption of processes called 4D: democratisation, digitalisation, de-bureaucracy and demonetisation [17], which will favour the concept of Open Insurance [18], in which, in relation to the financial market, bank data will now belong to customers and not to financial institutions.

Due to this process, and in line with more advanced initiatives already adopted, for example, by the countries of the European Union, embodied in reports such as the eGovernment Benchmark 2018 [19], the importance of regulatory instruments appropriate to the Brazilian reality is emphasised, which, in fact, contribute to the protection of government systems and networks, since the services supported by these resources cannot suffer interruptions, data leakages or be targets of other harmful actions.

In recent cyberattacks, hacker groups have regarded government systems as compensating targets, in order to cause different impacts, such as the potential damage to the Government's image before its internal public and before the international community, the discredit of the population in public services, the distrust of international investors in the capacity of the public administration to protect their own systems, the distrust in electoral processes, and the population's discontent in relation to public administration.

In addition to the protection of the Government itself, another critical point refers to the cyber protection of companies representing critical infrastructure. For the sake of understanding, we can conceptualise them as facilities, services and goods that, if interrupted or destroyed, will have a serious social, economic, political, international or national security impact. These companies need to take a consistent and evolutionary approach to cybersecurity to identify and assess vulnerabilities, and manage threat risk, by looking, for example, at the five functions provided for in the cybersecurity framework of the National Institute of Standards and Technology - NIST, which are: Identify, Protect, Detect, Respond and Restore [20].

The main types of threats against these organisations are considered to be phishing attacks, large-scale denial of service, private information leaks, cyber espionage and terrorism, and service disruption.

The need for protection of these companies is growing in relevance. As information and communication infrastructures become globally interconnected, they become the target of malware, hackers, hacktivists and adverse state operations. In addition, the global interconnectivity of some critical infrastructures means that a vulnerable party can become the weakest link and therefore a risk to other nations.

PART II

ANALYSIS OF THE THEMATIC AXES

In order to assist in the formulation of strategic actions, the thematic axes that belong to the area of protection and security were analysed, which are: national cybersecurity governance, the sub-connected and secure universe, prevention and mitigation of threats cybernetics, and strategic protection. Then, the transformative thematic axes were approached, thus named for their potential to modify, in a decisive and structuring way, the themes influenced by them. These are: the normative dimension, research, development and innovation, the international dimension and strategic partnerships, and education.

1. THEMATIC AXES: PROTECTION AND SECURITY

1.1. National Cybersecurity Governance

In the analysis of this thematic axis, aspects related to mechanisms and measures that can be adopted in favour of cyber governance, the risk management methodology, trust and security in the use of the digital certificate, the implementation of a centralised model for cybersecurity coordination will be addressed. national level, and monitoring the cyber scenario.

With regard to mechanisms and measures in favour of cyber governance, the concept of governance is initially analysed. It is noted that this set of management processes, in any area, is of vital importance to align an organisation's planning with its strategic actions, optimise the use of resources, increase the quality of the services provided and allow the successful conduct of projects and processes. In cybersecurity, this aspect acquires special relevance, due to the profusion of actors related to the theme, the capillarity and

transversality of the subject in different areas of society, and the multilateral nature of planned and ongoing actions.

In this sense, cyber governance encompasses the development and application of common principles, standards, procedures and programmes that shape the evolution and use of digital tools.

Information security is achieved through the implementation of controls, processes, policies and procedures, which together strengthen business objectives by minimising their risks, and promoting the security of the organisation (NBR ISO/IEC 17799: 2005).

Actions aimed at communicating cyberattacks and malicious actions are also addressed, strengthening the institutional capacity of public agencies in cybersecurity, leadership mechanisms, good practice manuals, minimum requirements and recommendations, monitoring of public policies, risk management, meeting the interests of society, the custody of data by public bodies and certificates in cybersecurity, as well as to actions aimed at other topics.

To support and guide the analysis of the thematic areas of protection and security, the following aspects were considered:

- public confidence in online public services;

- ensuring, by the public administration, that its bodies protect their networks and systems, in accordance with the legislation on the subject;

- government investment in the provision of digital services;

- compliance with cybersecurity standards, by suppliers of goods and services to government agencies; and

- the need for up-to-date information to support current government policy, the planning of new guidelines and the future design of programmes.

Governance in the cyber area is related to actions, mechanisms and measures to be adopted in order to simplify and modernise the management of human, financial and material resources, and to monitor performance and evaluate the results of efforts undertaken in this field.

This governance aims to incorporate high standards of conduct into cybersecurity, and to guide the actions of public agents and private agents, when considering the role they play in their organisations, according to the purpose and nature of their business.

It also includes planning aimed at executing programmes, projects and processes, and establishing guidelines that will guide risk management. In this context, it guides people and organisations on compliance of existing norms, requirements and procedures in cybersecurity.

According to Decree 9,203, of November 22, 2017, in its Article 17 [21], it is said that “senior management officers of organisations of the direct, autarchic and foundational federal public administration shall establish, maintain, monitor and improve the risk management system and internal controls with a view to the identification, evaluation, treatment, monitoring and the critical analysis of risks that may impact the implementation of the strategy and the achievement of the organisation's objectives in fulfilling its institutional mission ”.

In this context, is emphasised the importance of companies, which produce or sell services in the field of cybersecurity, in adopting national and international standards in the

development of new solutions, since their conception, which is internationally known by the terms **privacy by design and default** and **security by design and default**. To this end, the role of the State in guaranteeing companies the flexibility to continue to create improvement mechanisms, with the use of cutting-edge technology to guarantee the security of their products, services and solutions, and thus protect their users, stands out.

It is seen that cyber governance, considered at the national level, guides the rights, obligations and responsibilities of different segments of society, and leads public bodies and private organisations to prioritise the safe use of cyberspace.

In this sense, it is verified the importance of the institutions implementing cybersecurity programmes, using recognised models, that provide an adequate diagnosis of the stage they are in, which identify the most vulnerable points of their systems, the most probable cyber threats, and the biggest risk factors that consider the adoption of appropriate protections, attack detection mechanisms, incidents response methodologies and cyber ecosystem restoration procedures.

Regarding the definition of roles and responsibilities, it is seen that the Brazilian citizen needs to increase his participation in the digital ecosystem, not only through the use of technologies, but mainly, in the fight against cybercrimes, the so-called software piracy [22] and malicious actions, by reporting, through specific reporting channels, all cybercrime of which he is a victim of.

With regard to risk management, it is found that it is one of the main points of support of cyber governance, since it indicates the adoption of better policies and methodologies, which allows managing, in an optimised way, the acceptable risk limits. This management boils down to the principles, objectives, structures, skills and processes necessary to know the vulnerabilities, and thus allow them to be dealt with effectively, being, therefore, a tool that allows each institution, among others benefits, have the perfect dimension of their critical points and the most relevant assets to protect.

On October 13, 2008, the Institutional Security Office of the Presidency of the Republic published Complementary Norm 02/IN01/DSIC/GSI/PR, which provides for the information security management methodology and provides guidance on risk definition, procedures to identify risks and their acceptable levels, analysis of impacts and probabilities and risk treatment options. Additionally, on February 15, 2013, the Institutional Security Office of the Presidency of the Republic published Complementary Norm 04/IN01/DSIC/GSI/PR, which establishes guidelines for the information and communications security risk management process in the bodies or entities of the Federal Public Administration, direct and indirect. This standard allows each public body or entity to adopt an information security risk management methodology that meets the objectives, general guidelines and the defined scope, and that contemplates, at least, the risk assessment and acceptance criteria.

Over time, it was found that each institution adopts different international methodologies and frameworks, which, among other things, provide: security guidance policies, recommendations of good practices and a guide to assist companies in assessing and improving their systems internal control, which includes risk assessment.

The adoption of these frameworks differently among public bodies and entities and private sector companies, makes it difficult to analyse the degree of maturity in the country's cybersecurity in general, since the criteria and requirements of each standard are not the same, which makes it necessary to standardise best practices and allow even small organisations to adopt efficient measures to protect their information. In this way,

cybersecurity risk assessment and management stand out as key factors for the protection of cyberspace, services and information in it.

However, it was found that the adoption of unique and excluding governance standards would not necessarily produce positive results, when considering the transversality and capillarity of cybersecurity actions in public and private institutions and society in general. It is also emphasised that cyber governance policies must correspond to continuous processes that are part of the culture of public and private entities.

Consequently, in the broader context of governance, it is recommended, as an initial step, to observe the rules issued by the Institutional Security Office of the Presidency of the Republic. However, it is known that these standards are not exhaustive, and shall be consulted and, when relevant, also adopted the related standards of the International Organisation for Standardization (ISO), in addition to other methodological standards, such as the Control Objectives for Information and related Technology – COBIT [23], the National Institute of Standards and Technology – NIST [24] and the one by the Centre for Internet Security – CIS [25]. In this way, companies are encouraged to adopt customised security measures and tools to address the risks faced by their specific business model.

Compliance with these standards by the different national actors, for the elaboration of their cybersecurity standards, is relevant, since they provide widely evaluated and consensus-based structures to define and implement effective cybersecurity approaches that can meet common challenges, and thus enable collaboration and interoperability.

Governance actions shall, also, according to the context of each institution, include cybersecurity concepts that address integrative initiatives and that allow the macro-management of different assets and different technologies, such as a SOAR - Security Orchestration Automation and Response platform, which consists of a set of solutions [26] of compatible software that allows an organisation to collect data about security threats from various sources.

A SOAR platform includes a series of security management, analytics and reporting features [27] that use readable data from multiple sources to provide reports, analysis and workflow automation functions for multiple security teams, and offer the intelligence that point solutions, such as SIEM (security information and event management software [28]) - incident response and vulnerability scanning solutions, do not offer. Therefore, based on solutions such as SOAR, it is expected to respond adequately to security events, and to improve the effectiveness of operations in the digital scenario.

A SOAR platform can therefore manage several resources [29], such as: portable devices, endpoint protection systems, servers, e-mail security, routers, switches, wireless systems, access points, firewalls, file systems, DNS (Domain Name System) servers, DHCP (Dynamic Host Configuration Protocol) protocols, IDS (Intrusion Detection System), IPS (Intrusion Prevention System) and SIEM solutions.

Seizing the opportunity, it is understood that the certification of products and solutions in cybersecurity is an objective to be pursued, when considering the complexity of the equipment and computational tools, which require a high degree of specialisation and technological resources available, and of structured and equipped bodies to conduct it. It is noteworthy that, before fostering and developing its own certification, it is recommended to seek to leverage the existing certification mechanisms, to avoid the creation of trade barriers.

However, there is a growing understanding, in the productive environment, that product certification - more specifically, of equipment - does not prove to be something simple, since certification occurs on the type, model and firmware of an equipment, which prevents its firmware update or that the manufacturer makes security patches available, under penalty of causing the product to lose its initial certification.

Another aspect to consider when addressing protection and security in the cyber environment is the trust provided by the digital certificate, which can be understood as a secure electronic identity for people or organisations, and with authenticity guaranteed by complex encryption. With it, it is possible to unequivocally guarantee the identity of an individual or an institution, without a face-to-face presentation [30].

The digital certificate guarantees confidentiality, authenticity, and proof of authorship in signed electronic transactions through its use.

This feature is very relevant and encourages the standardisation of validation and authentication practices, since several certificates are internationally accepted. Thus, the adoption of digital certification shall be encouraged. It is noteworthy that its use in public documents (identity card, voter registration and CPF[*]), can be a way of spreading a more secure and reliable access environment.

In Brazil, digital certification was introduced in 2001. Among the pioneers in its use, the Central Bank of Brazil stands out, through the Brazilian Payment System - SPB, and the Federal Revenue of Brazil, which used it in services such as the Virtual Taxpayer Service Centre - e-CAC, and for the issuance of the Electronic Invoice - NF-e, which collaborates to optimise processes and enables greater control to reduce fraud and tax evasion.

The Brazilian judiciary also extensively uses certification, from the edition of the *Diário da Justiça*[†] in electronic format to the electronic petition available in several courts. There are several applications that make use of the ICP-Brasil digital certificate, and enable digital trust and security.

According to the National Institute of Information Technology, until April 2019, the issuance of certificates exceeded 35.6% of the number registered in the same period of 2018. However, of the total emissions in 2019, certificates issued to individuals represented only 8.4%, while, for legal entities, they represented 45.9% [31].

Today, virtually all legal entities have at least one digital certificate. However, digital certification is still not widely used in corporations, due to certain difficulties, such as the high number of processes for issuing certificates, the high cost to citizens and the low number of certifying units per inhabitant. In order to solve these issues, the Federal Government has been adopting actions to optimise the processes aimed at obtaining them, with the purpose of significantly expanding the offer of this resource. However, care must be taken for, in the name of acceleration and dissemination of digital certification, not weakening the security measures related to its concession, which lead to the compromise of this valuable resource.

---

[*] The Brazilian federal individual registration number, similar to the NIN (National Identification Number) in the UK.

[†] The official journal of the Brazilian Judiciary where justice decisions are published daily in Brazil.

Regarding the study of the most appropriate model for the coordination of cybersecurity actions, it is important to highlight that the management of these actions involves multiple actors. Both nationally and internationally, an effective mobilisation for the consolidation of cybersecurity, as vital for the development of Brazilian society, will be more successful through assertive political coordination, which includes the private sector and society.

According to a report by the Parliamentary Committee of Inquiry for Espionage [32], the distribution and handling of matters related to cybersecurity in the country, has not contributed to the Government having an overview of the subject, which makes it difficult to carry out more effective actions in this field. This is because each public agency adopts definitions, criteria and different actions for the protection of the digital environment, without sharing information, good practices and the solutions adopted for each cyber incident.

In this sense, the creation of a system that brings together all state and non-state actors under the aegis of cybersecurity, may contribute to the necessary strategic, doctrinal and operational alignment in the actions concerning this field, and it is up to the Federal Government to encourage discussion of alternatives that lead to the institutional strengthening of Brazilian cybersecurity. In this context, it is important to grant to a government agency the responsibility to guide the issue at the national level, organise it, and propose measures and regulations, with the participation of representatives from all sectors of society. Exception is made only to aspects related to cyber defence and warfare, which are in charge of the Ministry of Defence, which in no way prevents the necessary interaction, in this bias, between the areas of security and defence.

The centralised model of cybersecurity management presents itself as a viable and effective alternative, and has been adopted by countries such as the United States of America, the United Kingdom, Portugal, France, India, Malaysia, Singapore, South Korea and Japan. The experience of these countries demonstrates that the creation of central structures to address this issue, with authority to establish specific regulations and actions, presents good results for the coordination and consolidation of cybersecurity as a state issue, promotes synergy between Government, the private sector, society and academia, and highlights the strategic character of protecting cyberspace.

In the Brazilian case, when considering the Federal Government, the Institutional Security Office of the Presidency of the Republic stands out, which, since 2006, through the Information Security Department, studies and prepares several norms, which consist of General Instructions, Complementary Norms, Strategies and Policy, within the scope of the Federal Public Administration, by gathering, since then, vast experience in relation to several areas of information security, especially with regard to cybersecurity.

Thus, it seems not the case of creating new and expensive governmental bodies, being enough to resize the current structure of the Institutional Security Office of the Presidency of the Republic, in order to enable it to act at the national level. Therefore, there is an urgent need for a law that regulates cybersecurity actions, specifying attributions, pointing out mechanisms for dialogue with society and which makes it possible for the Institutional Security Office of the Presidency of the Republic, with the participation of representatives of all national entities, to play the role of macro strategic coordinator, by providing alignment to cybersecurity actions and by contributing to the evolution of the whole country in this field, in a convergent and structured manner. It is also concluded that it is necessary and urgent that the Federal Government prioritise the application of resources in the area of cybersecurity.

Furthermore, as mentioned in the previous paragraph, mechanisms that enable the participation of society shall be considered. Among the possible instruments, this Strategy recommends the creation of a national cybersecurity council, which brings together several state and non-state actors, with the aim of thinking about cybersecurity under a comprehensive, inclusive, modern prism and with an emphasis on real national needs.

In addition to this Council, as a stimulus to the debate on the subject, E-Ciber encourages the creation of several discussion groups, under the coordination of the Institutional Security Office of the Presidency of the Republic, in order to ensure the involvement of professionals with sectorial knowledge and relevant specialities for a better understanding of the challenges to be addressed to the various sectors according to specific realities.

Regarding the monitoring of the cyber scenario, there is a need for continuous verification of the effectiveness of the normative instruments, which necessarily involves monitoring and constant evaluation. Evaluations that produce reliable results allow policy improvement and justify investments or savings in resources, since they show if the expected results are achieved and if the resources are used efficiently. According to the public governance guidelines established in Decree 9,203, of 2017 [33], it is observed the importance of also foreseeing metrics and indicators that allow, in the future, the monitoring of actions, programmes and projects aimed at cybersecurity, in order to obtain continuous effectiveness in the management of actions related to this area.

Within this perspective, three important aspects are highlighted: the measurement of the effectiveness and efficiency of treatment centres and response to computer incidents, the development of indicators to measure the country's performance in cybersecurity and the establishment of routine cybersecurity compliance checks within public bodies and private entities, conducted by them, so that it is possible to establish the correct relationship between the technical aspects of information technology, such as vulnerability analysis, technical threat reports and a list of solutions in technology, business aspects, such as continuity of services provided, image risks and decision-making processes. Therefore, compliance verification is understood as a natural process, based on programmes established by public and private entities themselves, which aims at the continuous improvement of cybersecurity systems.

It shall be noted that compliance checks must be planned in moderation, and must be based on principles of reasonableness, so that public and private institutions do not employ time and large amounts of resources in excessive compliance procedures, to the detriment of their use in dealing with cyber threats.

1.2. Connected and secure universe: prevention and mitigation of cyber threats

The process of preparing the country towards the new digital economy, will experience a strong impact of various technologies, such as the Internet of things, quantum computing, artificial intelligence, machine learning, cognitive science, robotics, biotechnology, nanotechnology or 5G telephony. To provide support for this process, actions are needed to enable its viability in a safe and resilient manner.

To face this challenge, this axis of E-Ciber will deal with the management of computer incidents, which involves detection, screening, analysis and response to these incidents.

Preventive activities based on risk assessments can reduce the growing number of cyber incidents. However, they cannot entirely prevent them. Therefore, a response feature is needed to detect them quickly, minimise the loss and destruction they can cause, mitigate the weaknesses exploited and restore information and communication technology

services, always considering that the monitoring of cybersecurity threats must be global in nature.

In this context, we highlight the relevance of resources and mechanisms that allow the interaction and sharing of information at different levels, between public and private institutions, and between these and international organisations, who have experience monitoring threat trends and cyberattacks, in order to consider the regional, multilateral and global impacts of incidents occurring in the digital environment.

It is widely known that every organisation, public or private, must have a team for handling and responding to cyber incidents - ETIR, also known by the acronym - CSIRT, from Computer Security Incident Response Team. This team must be trained, and must have computer tools appropriate to their needs, and systems based on emerging technologies, consistent with international standards. Currently, Brazil has eight types of treatment centres and response to cyber incidents, according to their sectors:

- Centres of National Responsibility - CERT.br and CTIR Gov.

- International Coordination Centres - CERT/Coordination Centre, FedCirc and FIRST.

- Critical Infrastructure CSIRTs - Energy - CSIRTCemig - Financial - CSIRTs of BB, Caixa, BASA, BNB, BRB and BANESE - Telecom - CTIR/DATAPREV, GRA/SERPRO and CSIRT PRODESP.

- Providers CSIRTs - CSIRT Locaweb and CSIRT HP.

- Corporate CSIRTs - CERT-RS, SEGTIC UFRJ and CSIRT Unicamp.

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

- Government CSIRTs - Executive - CTIR Gov, Legislative - GRIS-CD and Judiciary - GATI, CLRI and TRF-3.

- Military CSIRTs - Navy - CTIM, Army - CCTIR/EB and Aeronautics - CTIR.FAB.

These centres operate in constant communication, and keep records of national incidents, to evaluate statistical data regarding threats and such incidents. Current efforts focus on simplifying information sharing among all CSIRTs, as the number of actors in the Government and the private sector is increasing, alongside the growing challenges in the cyber field.

Brazil has two centres of treatment and response of national responsibility. The Centre for Studies, Response and Treatment of Security Incidents in Brazil - CERT.br [34], is responsible for dealing with security incidents on computers involving networks connected to the Internet in the country, more focused on commercial and private institutions. With a similar assignment, but focused on government networks, there is the Centre for Treatment and Response to Cyber Government Incidents - CTIR Gov [35]. Today, the services provided by CTIR Gov basically include: incident notification, incident analysis, support for incident response, coordination in incident response, distribution of alerts, recommendations and statistics, and cooperation with other ETIRs.

As an example of the Alert issued by CTIR Gov, there is Alert 03/2019 - Silex Malware on IoT devices, a document that can be found on that Centre's website.

To perform its functions, the CTIR Gov has mechanisms that monitor vulnerabilities, tampering and unavailability of sites, advertisements for information leaks, and that check

open social networks. In addition, it works in cooperation with cybersecurity partner agencies, by integrating an international network of CSIRTs, with a strong role in the analysis of possible massive actions.

It is noteworthy that the work of a CSIRT can be improved through research and consultation to global standards, which can facilitate communication between other incident analysts, information technology operators, information technology equipment manufacturers, and other representatives of the private initiative and academia. In this sense, models like the one described by Common Vulnerabilities and Exposures – CVE [36], can be of great use.

In this context, it is considered essential to adopt actions that allow the continuous and proactive monitoring of threats and cyberattacks, and that allow the establishment of adequate means of communication with groups internal and external to the organisation itself. Communication channels can also be expanded internationally, through participation in forums such as the following:

- FIRST: Forum of Incident Response and Security Teams

- Creation: 1990.

- Members: four hundred and eighty-three CSIRTs, in ninety-two countries, from all sectors.

- APWG: Anti-phishing Working Group

- Creation: 2003.

- Members: more than two thousand organisations, participants from all sectors, including international organisations.

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

- creation: 2004.

- Members: more than two hundred CSIRTs, belonging to the industrial sector.

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

- Creation: 2017.

- Members: Internet community in general.

In order to demonstrate the action of CTIR Gov in the face of the notifications received, according to the incidents reported and confirmed by that Centre, from 2011 to 2018, it is observed that, among the notifications received, 26.23% correspond to abuse of site, 20.04% correspond to leakage, and 15.95% correspond to fraud, these being the largest categories of incidents.

In this sense, according to a publication by CERT.br, in 2018, one thousand and seventy-five notifications of compromised machines were received. This total was 168% higher than that received in 2017. More than 98% of notifications were related to web servers that had their pages defaced [37]. However, as cases are reported on a voluntary basis, the actual number of incidents is likely to be much higher, as cyber incidents targeted to users are mostly related to fraud.

In the current scenario of cyber threats, organisations will likely experience the same type of attack, which highlights the importance of information about the fact, the treatment performed and the lessons learned. In this context, the aim is for joint action in favour of cybersecurity, and the creation of a collaborative environment, in which the public

administration, the private sector, academia and society in general, participate, is of paramount importance.

An example of collaborative action is the Cyber Guardian exercise, organised annually by the Cyber Defence Command, in partnership with the Institutional Security Office of the Presidency of the Republic. The activity consists of training cyber protection actions, through cooperation between the Armed Forces, partner agencies and representatives of critical infrastructures, by adopting virtual simulation techniques and incident management practices. The exercise employs crisis offices in the areas of information and communication technology, social communication, legal and senior management of the participants, who are led to present solutions for cyber events with an impact on organisations, including the decision-management level (crisis management) and the technical level (incidents response) of companies and government agencies.

Another approach in this context, with the objective of promoting a collaborative, participatory and secure environment, can be the implementation of a platform for sharing threats or cyber trends, where the exchange of information occurs in a standardised, fast and secure manner.

It is noteworthy that information sharing is a way of showing the strategic partnership between the main actors interested in cybersecurity, in all sectors of society. Thus, those actors responsible for the management of critical infrastructures - be they public administration bodies or private sector companies - have better conditions for sharing information that can assist in mitigating risks, analysing threats and studying emerging vulnerabilities, while public agencies specialised in cybersecurity are able to provide vital information on aspects related to national security status.

The country still needs to strengthen and improve its government agencies that deal with threats and that fight cybercrime. Since the CTIR Gov is the central government agency that coordinates and carries out actions aimed at the management of computer incidents, it is recommended to grant this agency national reach, which shall be strengthened. In the same direction, it is recommended to improve the national structure for investigating cybercrimes.

Currently, communication can be subject to illegal interception that, occasionally, may not be avoided by cybersecurity policies adopted by both telecommunications service providers and other actors, and promoted by agents with different intentions, such as searching information, harassment of people with a certain profile or attempt to hinder the realisation of a project, among other reasons. Thus, digital communication can be monitored or intercepted, in the following ways:

- personal or organisational devices, infected with malware or directly monitored;

- Wi-Fi router, infected with malware or controlled by third parties;

- infected Internet providers, either for their own purposes or for third parties;

- national network bridge (gateway), regardless of the interceptor's location;

- tapped cables for diverting communications;

- website of the service used; and

- any of the services that store or route communication.

While some recommendations on digital security are tailored to a specific tool, network technology or communication medium, other recommendations are universal. In this regard, it is recommended to establish protocols and requirements regarding prevention,

monitoring, treatment, and response to computer incidents, aimed mainly at specialised teams that deal with cyber threats.

In addition, it is recommended to mitigate risks, considering the details of the environment, in order to keep devices up-to-date, and to avoid malicious codes, pay attention to phishing attacks, prefer reliable services, create strong passwords, use encryption and share these practices with those agents involved in the communication process. It is also considered that the proper use of cryptographic resources has proven to enable an additional security layer of extreme relevance to achieve the desired levels of data protection at rest or in transit.

1.3. Strategic Protection

In the analysis of this thematic axis, aspects related to the government's cyber protection and the cyber protection of critical infrastructures will be addressed.

The country is in an accelerated process of digitisation of public services, which confers progressive critical character to government networks and systems, which support the provision of these services to citizens. The same process is observed in relation to the communication structures between government entities, whose level of protection must be adequate and proportional to their relevance.

To effectively support E-Digital and at the same time provide cyber protection to the management systems and other systems used by government agencies, it is necessary to reduce the vulnerability of government organisations against any type of cyber threat, by providing the public administration with adequate levels of security and resilience against cyberattacks.

Since the mitigation of attacks involves the articulation of different actors at the national level and, sometimes, at the international level, grows in relevance the need for the short, medium and long term actions to deal with these attacks effectively, in order to consider that they can be carried out by countries, groups or individuals, who seek political interests, economic advantages or even harm the provision of essential services to society, causing damages of all kinds.

Brazil lacks training actions that reach different spheres of government, while it needs to devote special attention to the protection of national critical infrastructures. It is also necessary to specify actions that protect the structure related to the Internet, such as large servers, traffic exchange points and datacentres, since they provide the functioning of the critical sectors of the network.

With regard to the protection of government networks and systems, due to the increasing integration of services, databases and digital platforms, there is an increase in vulnerabilities, which can be exploited by hackers. In this sense, it is noteworthy that the Government must use resources so that cybersecurity is implemented and adequate to protect its computational structures, so that the provision of services to citizens does not suffer a continuity solution. It is emphasised that these resources must compose a structured set of investments in knowledge, policies, professionals and technologies, among others.

In this context, the information held by public agencies is sensitive, due to the potential for negative impact on the provision of services to the population, in case of compromise. With respect to this information, it is recommended that public agencies have backup copies that are frequently updated, automatically segregated and stored in a protected location. This practice aims to restrict malicious attacks to the original productive

environment, and to reduce the risks of data hijacking, financial losses, negative impacts on the image, and disruption of services for unacceptable periods.

Corporative mobile devices, connected to the Internet and used frequently by public authorities, can be targets of cybercrime, and deserve attention, especially in the case of bodies that allow, in their security policies, the use of such equipment in the modality known as BYOD, abbreviation for Bring Your Own Device, in which system administrators allow the connection of a private device to the government body network.

In this regard, it is vital to consider endpoint security, the security of devices used by final users[38] and connected to a network, basically any device that is connected to a network, internal or external.

The modern and agile flow of information in an organisation requires quick response, which does not always come from a corporate workstation - a desktop computer -, since it can come from smartphones, notebooks or tablets connected to the corporate network. Therefore, these endpoints shall be part of a set of measures that aim to block them against cyber threats and keep them free from attacks. By blocking network terminals[39], endpoint security prevents hackers and vulnerabilities from connected devices from being exploited by hackers to steal corporate data.

The concern and protection actions aimed at endpoints are fully justified, given the growth of cyber threats against them. According to AVTEST, more than nine million new cases of malware are observed each month [40], targeting not only Windows® systems, but also [41] macOS®, Linux and Android®.

Another point that has been highlighted among the government's cybersecurity concerns refers to the sophisticated and targeted attacks on supply chains. A Supply Chain Attack occurs when there is an infiltration in a system through a supplier, a partner company or an external provider with access to systems and data. This type of attack, in general, causes financial losses and reflects negatively on suppliers' image, in order to lead to loss of confidence and profoundly affect business.

In this sense, it is recommended to establish minimum cybersecurity requirements in contracts by Government agencies and entities, which would perform dual function: first, to improve cybersecurity in the public sector, and second, to encourage a more effective security in the entire market, that, in order to trade with the Government, must pay attention to these requirements in the provision of services and in the sale of equipment.

In preparing contractual instruments, it is recommended that government entities, when establishing these requirements, ensure that they are market-oriented, consistent with the national private universe and aligned with internationally known standards.

The protection of critical infrastructures, due to their relevance, deserves a specific approach. In Brazil, these organisations, the scope of this Strategy, belong to the Telecommunications sector, the Transport sector, the Energy sector, the Water sector and the Financial sector.

Although the Health sector has not been contemplated in the list of critical infrastructures, we can consider it in an analogous scope, since its representative institutions provide essential services to society. Therefore, we consider the same recommendations on cybersecurity dedicated to the other five sectors addressed by this Strategy to be valid and appropriate.

Similarly, it is noteworthy the strategic relevance of the pharmaceutical industry, and the impact that successful cyberattacks can have on it and on Brazilian society. According to

Portal CSO [42], pharmaceutical organisations are preferred targets for cybercrime, mainly due to the possibility of obtaining intellectual property related to business processes, which can provide a profitable competitive advantage.

Decree 9,573, of November 22, 2018 [43], approved the National Policy for the Security of National Critical Infrastructures. This Policy aims to ensure the security and resilience of the country's critical infrastructure and the continuity of the provision of its services. In this sense, it establishes the Integrated Critical Infrastructure Security Data System, the National Critical Infrastructure Security Strategy and the National Critical Infrastructure Security Plan. In its principles, the Policy mentioned above points out the importance of prevention and precaution, based on risk analysis, which reflects the need to adopt security procedures in all of their aspects, including cybersecurity. This, in many cases, is considered vital for the full functioning of critical infrastructures and as a guarantee of adequate provision of services for the entire Brazilian society.

In 2018, the risks of cyberattacks grew significantly, especially the breaches of information accessed by third-party suppliers and the theft of information (personally identifiable information, intellectual property and trade secrets). According to the study "2018 Cost of Data Breach Study: Global Overview" [44], carried out by IBM in partnership with the Ponemon Institute, in 2018, there was a 350% increase in ransomware attacks, with an expansion of 250 % in spoofing attacks or commercial email compromises and there was an increase of 70% in spear-phishing attacks in companies in general. The average cost of a cyber data breach increased from US$ 3,620,000.00 (three million six hundred and twenty thousand dollars) in 2017 to US$ 3,860,000.00 (three million eight hundred and sixty thousand dollars) in 2018. In Brazil, the average cost of a breach reached US$ 1,240,000.00 (one million two hundred and forty thousand dollars).

The cyber threats described above are intended to reach a large number of organisations, including representatives of critical infrastructures, which, since they provide essential services to society, have a high level of criticality. For this reason, these organisations need the means to identify, protect, detect, evaluate, respond, recover and thus manage the risk of cyber threats, as well as security automation tools that use artificial intelligence and machine learning, which allow to analyse, identify and contain cyberattacks.

The main types of threats against critical infrastructure are phishing attacks, large-scale denial of service, private or institutional information leaks, cyber espionage and service disruption. In this context, it is emphasised that the quantity and plurality of devices and applications, especially those belonging to the IoT category, present themselves as a challenge for critical infrastructures, considering the need for balancing security, privacy and non-confinement of resources to guarantee the promotion of the innovation environment.

It is also noted that in all cyber risk management approaches, in systems or critical functions, there are indications for using cryptography, which contains the appropriate recommendations for where, when, and how it shall be applied.

It is mentioned in many national cybersecurity strategies that attacks on critical infrastructures are among the greatest threats to national security, considering that a large part of national economies is increasingly dependent on information systems of essential sectors, based on automated controls.

Therefore, the protection of critical infrastructures against evolving cyber threats requires a broad approach, such as: monitoring issues relevant to these organisations, with priority to those referring to risk assessment, planning, coordinating and developing cybersecurity

actions and defining norms and methodological requirements for the implementation of cybersecurity actions.

During the elaboration of the Strategy, it was observed that:

- there is not, in Brazil, an autochthonous and comprehensive cybersecurity framework that contributes to the strengthening of national cyber resilience;

- the codes, norms, standards and guidelines in force have evolved with the development of projects, tools and practices related to cybersecurity, but have not been adequately absorbed by public and private entities;

- cybersecurity features have evolved;

- there is a need to increase coordination between representatives of critical infrastructures;

- it is important to establish models that make it possible to understand cyber risk for the provision of services and to assess the cost of an occurrence; and

- it is necessary to encourage these critical organisations to create a culture of cybersecurity.

One of the sectors of critical infrastructures that have regulations established for its regulated entities with specific actions for cyber protection is the financial sector. Published by the Central Bank of Brazil, Resolution 4,658, of April 26, 2018 [45], aimed at financial institutions, addresses the cybersecurity policy to be observed by those institutions. In addition, it provides for the premises for contracting cloud computing and data processing and storage services. Even though payment institutions are not part of the National Financial System, and are not considered as critical infrastructures, it is worth highlighting Circular 3,909, of August 16, 2018 [46], specific to these institutions, which addresses interesting aspects of cybersecurity.

One of the aspects of great relevance for critical infrastructures is business continuity. In relation to this topic, the Central Bank of Brazil requires that these organisations must define: the treatment for the relevant incidents, the procedures in the event of interruption of the relevant contracted services and the scenarios of incidents to be considered in tests.

Through joint action between the Government and the various critical infrastructure operators, it will be possible to protect the cyberspace in which they are inserted. In addition, the role of regulatory agencies in stimulating the adoption of cybersecurity procedures by their regulated entities is verified, such as:

- creation of a cybersecurity governance structure in critical infrastructure companies, with the establishment of manuals, guidelines, classifications and procedures for handling incidents, and security rules applicable to all employees, contractors and suppliers;

- insertion of cybersecurity annual external audit plans;

- adoption of cybersecurity practices and requirements in the development of new products, programmes, projects and actions;

- creation of CSIRTs by company and by sector, with collaboration and information exchange mechanisms between them.

- continuous training of its employees at all levels;

- notification to CTIR Gov, in the shortest possible time, about the occurrence of cyber incidents;

- communication to consumers in the event of an incident that compromises the security of their data, in accordance with existing legislation;

- promoting awareness campaigns on the importance of attitudes and care on the part of users;

- demand that equipment, software and service providers adopt the cybersecurity levels recommended by national and international standardisation bodies; and

- provision for the preparation of incident response plans and the recovery of critical environments that may be impacted by cyber incidents.

With regard to the modus operandi of cybersecurity procedures, technical and operational aspects related to the topic may be dealt with in more detail by regulatory agencies with support from the Institutional Security Office of the Presidency of the Republic, through working groups composed of representatives of the Government, the private sector, academia and society in general, in order to provide, for example, the preparation of operational manuals and specific cybersecurity procedures.

Finally, it is recommended that critical infrastructure managers, when designing their cybersecurity policies, include, among others, the following ideas:

- focus on security outcomes;

- use of a flexible structure based on risk analysis;

- emphasis on the continuity of its services;

- alignment of critical security with nationally and internationally recognised standards; and

- ensuring that certification processes are balanced, transparent and based on national and international standards.

2. THEMATIC AXES: TRANSFORMATIVE

2.1. Normative Dimension

The exponential increase in the number of Internet users and the strong expansion of online commerce have expanded the possibilities of malicious and illicit actions, and led to a rise in criminal offences known as cybercrimes or virtual crimes. These crimes range from crimes that offend a person's honour, such as slander, defamation, injury and bullying, to crimes that violate citizens' privacy or threaten their property.

Currently, with the intense use of the world wide web, such crimes expand rapidly. It is necessary to recognise the initiatives and efforts made so far, which resulted in the approval of important laws for the country, such as Law 12,965, of April 23, 2014 [47], known as Marco Civil da Internet and Law 13,709, of August 14, 2018 - General Law for the Protection of Personal Data (Lei Geral de Proteção de Dados Pessoais) – LGPD [48], however, the level of articulation and standardisation of Brazilian institutions on issues related to cybersecurity is still timid, and requires additional effort.

Establishing norms and possibly laws that govern cyberspace is always a significant challenge, due to the rapid development of information and communication technology and control systems. In this sense, coordinated action between governmental organisations and society in general is essential to proceed with legislative advances on the subject.

Two laws related to Internet crimes were enacted in 2012, which amended Decree-Law 2,848 of 1940 - Penal Code, which typified and established penalties for certain criminal conduct committed in the digital world.

The first is the Cybercrimes Law - Law 12,737, of November 30, 2012 [49], known as the “Carolina Dieckmann Law”, which typifies acts such as the invasion of computers - hacking, the theft of passwords, the violation of user data and the disclosure of private information (photos, messages, etc.). The second is Law 12,735, of November 30, 2012 [50], which determines the installation of specialised police stations to combat digital crimes.

In terms of E-digital: “it is opportune for Brazil to establish a legal framework, protecting citizens' rights and conferring legal certainty for investments in the digital economy. However, there are legal and infra-legal norms that currently address the issue at the sectoral level, such as: Consumer Protection Code, which protects consumers' personal data; the Access to Information Law, that protects personal data and at the same time promotes public authorities transparency; the Positive Registration Law, which safeguards personal data in the context of credit analysis; among others".

Law 12.965, of 2014 - Marco Civil da Internet (Civil Framework of the Internet), regulates the use of the Internet in Brazil by providing principles, guarantees, rights and duties for those who use the world wide web, and guidelines for action of the State, protecting the personal data and privacy of users in the online environment, which is dealt with, more directly and assertively, by LGPD. Despite being comprehensive and modern, the intense advance of technology and the consequent redesign of human relations in cyberspace calls for periodic analyses of this valuable legal instrument, in order to always preserve its noble democratic pillars of freedom of expression and free transit of opinions.

The publication, in August 2018, of the LGPD mentioned above, reinforced the need for organisations to make investments in their structure and to adopt internal policies that meet the security requirements aimed at the processing of personal data.

The other work front refers to the normative instruments of competence of the Information Security Department of the Institutional Security Office of the Presidency of the Republic, directed at the Federal Administration bodies, which aim at improving and updating the operational guidelines and requirements related to the topic. After the creation of the then Information and Communications Security Department, in 2006, the Office of Institutional Security of the Presidency of the Republic dedicated itself intensively to the theme. As a result, since 2008, three General Instructions and twenty-two Complementary Norms [51] have been published, in order to address matters related to Information Security. Due to the evolutionary characteristics of the theme, such instruments need constant assessment and review.

On December 26, 2018, the National Information Security Policy was published, under Decree 9.637, of 2018, which provides for principles, objectives, instruments, attributions and powers on information security for the bodies and entities of the Federal Administration, under the prism of governance. Despite being a significant instrument, it is recommended that a specific Law on Cybersecurity be drafted, capable of providing specific guidelines for the national cyber sector, and including the Powers of the Union, the States, the Federal District, the Municipalities, the private sector and society in general.

A law would be designed to discipline various aspects of the national dimension of cybersecurity, since the entire existing regulatory framework is insufficient for the proper

confrontation of the issue by the country. This insufficiency stems from the infra-legal nature of the existing instruments, making them restricted to the Federal Public Administration, so as not to apply, in this way, to the other entities of the Public Power, and not to contemplate, yet, the productive sector, among which the suppliers of essential services, and the society in general.

In addition, it is noteworthy that cybersecurity presents a new paradigm in terms of security for the State, since all national actors have vulnerabilities that can be exploited by a cyber threat that acquires great repercussion, in order to put at risk even the stability of national institutions.

One of the major challenges in terms of cybersecurity is that it needs to be understood in a holistic and multisectoral way, not being appropriate to address it as restricted to government agencies, without the proper engagement of the private sector and without looking at the end-user of all technologies that use the cyberspace.

In this sense, a cybersecurity law would be able to align governance and compliance actions on this subject, from a single standpoint, by linking the various national actors to the proposed principles and rules. The digital economy, the insertion of Brazil in Industry 4.0 and the achievement of the Sustainable Development Goals [52] elected by the United Nations, demand the country to be able to build the confidence and security necessary for national development in the information age.

From this perspective, actions are recommended for improving the legal framework of national cybersecurity, believing that this initiative might provide the necessary strategic and normative alignment to the country's actions in this area, in order to emphasise that special attention shall be given to cybersecurity policies aimed at the productive sector, which, due to the natural strength of the market, tend to be more successful than those dedicated exclusively to public sector and regulatory oversight.

It is also recommended, in order to allow the elaboration of instruments with the greatest possible legitimacy, the creation of mechanisms that allow the participation of the private initiative and the academia for exchanging experiences, exploring international practices, discussing standards and best practices on the topic and supporting decisions by the central entity.

2.2. Research, Development and Innovation

The last decades have been marked by intense transformations and an impacting technological revolution, which have promoted important changes in people's daily lives, especially with regard to forms of communication, interaction and access to information. In this sense, technological advances have highlighted the relevance of encouraging research and innovation in favour of development, and demonstrated the essential role of these areas for society.

The role that the Government must play in this scenario also becomes relevant, so that the country continues in an economic growth guided by innovation, in an inclusive and sustainable way. In this context, the Research, Development and Innovation initiatives - RD&I, in the area of cybersecurity, need higher priority, in order to obtain greater investment, more qualified researchers in the area, and new projects, along the lines of other countries, of in order to even contemplate cryptology as a matter of extreme relevance to be incorporated into research and innovation projects nationwide.

The focus of this axis is to encourage the search for security solutions in the digital environment, in line with the E-Digital, of 2018. Smart cities, which widely use

technologies from IoT, and integration of government systems, which use BigData resources, for example, must have cybersecurity concerns at the centre of the debates.

E-Digital encourages RD&I, and the modernisation of a productive structure, in areas such as: microelectronics, in particular, actions aimed at training in house design, sensors, automation and robotics, supercomputing, artificial intelligence, BigData and analytics, high-performance networks, cryptography, 5th generation mobile networks and cloud computing.

It is recommended, in this sense, the investment in the search for innovative solutions in new types of cryptography, in order to consider its varied potential for applicability and its strategic value for information security and cybersecurity in the country.

Brazil has a diversified scenario in terms of research and development in technology. There are centres of excellence highly qualified and recognised for their activities, which however produce little innovation or technology applicable to the cyber environment. The country needs an innovative cybersecurity industry, supported by high-level research and scientific productions, capable of retaining talents that can contribute to the national industry and feed the knowledge production cycle.

There is a dissonance between the projects carried out by public and private universities and the productive sector needs for cybersecurity solutions. This framework demonstrates the need for a closer and more effective dialogue between the business sector and the academia, so that efforts and projects converge to positively and constructively impact society.

In this sense, it is recommended to establish partnerships with the Ministry of Education, aiming at the implementation of programmes to encourage the development of cybersecurity capacities for students of basic education, with the objective of identifying talents, and it is advised that universities develop projects in alignment with the needs of the productive sector.

The approximation of the master's and doctoral programmes, not only in applied computing, but in other areas of knowledge, can be an effective route for training, improvement and qualification of personnel interested in the theme, in addition to generating knowledge.

In the context of innovation, E-Ciber encourages the adoption of global and voluntary technology standards, which will allow interoperability on an international scale and, consequently, will ensure that not only organisations located in Brazil but also those outside the country can adopt our practices and processes in order to serve as a model for international cooperation in cybersecurity strengthening. Therefore, it is emphasised that public policies on this topic contemplate the relevance of taking advantage of global advances and technologies, to guarantee, in all ways, the use of the best tools available for cybersecurity.

One of the indicators used to measure a country's performance in terms of technological innovation is the World Competitiveness Yearbook ranking of the IMD Foundation Board [53] business school. In its 2019 edition, Brazil ranked fifty-ninth among sixty-three in the world. The research indicates that Brazil has been losing positions in this technological innovation indicator since 2010, when it ranked 38th. In 2011, it dropped to forty-fourth place. In 2012, it had already lost two more positions in the ranking and, in the last edition, it fell fifteen more positions.

With regard to the use of funds, the largest one is the National Fund for Scientific and Technological Development – FNDCT [54], formally created in 1969, with the objective of financially supporting national priority programmes and projects for scientific and technological development. FNDCT resources are used to support innovation and research activities in companies and scientific and technological institutions. However, there is no specific focus for projects in cybersecurity. In this perspective, the use of this and other funds to encourage cybersecurity innovation programmes and actions is considered relevant.

In the current scenario of innovation and technological revolution, companies that arise with a technological base – start-ups play a relevant role as the main sources of innovation. The perception of its innovative potential has encouraged several countries to establish a wide range of support programmes for start-ups and small and medium-sized companies, a solution that Brazil must follow and encourage.

In this context, it is important to continue research on the use of spectral intelligence, due to the fact that sensors used in IoT networks, drones, smartphones, GPS devices and wireless routers may suffer malicious actions in the radio frequency spectrum, with serious impacts on privacy and even on security of people and critical infrastructure. Spectral intelligence is understood as the use and analysis of the radio frequency spectrum in wireless communication systems [55].

With regard, furthermore, to the Research and Development axis, it is highlighted the importance of considering the cybersecurity aspects related to the technology of 5G networks, since it represents a revolution in data communications, in the potential use of IoT equipment, and in the provision of new and disruptive services that require networks with very low latency for their operationalisation, implementation, effectiveness and resilience. In this context, E-Ciber recommends that minimum requirements for cybersecurity must be considered on the acquisition of 5G equipment to ensure the full, responsible and safe use of this technology for the development of society and national institutions.

2.3. International Dimension and Strategic Partnerships

Brazil experiences the phenomenon of the fourth industrial revolution, where technologies gain more integration, the physical world and the virtual environment achieve a high degree of interaction, and IoT devices proliferate in support to production processes. This automation tends, naturally, to increase the competitiveness and productivity of the industrial sector.

The so-called Industry 4.0, therefore, brings great possibilities of productivity gains for the industrial sector through the use of new technologies, such as IoT, advanced robotics, 3D printing, BigData, cloud computing, artificial intelligence and virtual simulation systems. In addition, the combination of technologies creates new possibilities, new businesses and solutions, in order to cross borders and eliminate distances. For a better visualisation of these technologies, there is a list of them, brought by Agência Mais [56]:

- Advanced Robotics: an educational and technological area that includes computers, robots and computing that are part of integrated circuits;

- BigData - analysis and interpretation of large volumes of varied data;

- 3D printing - a form of additive manufacturing technology where a three-dimensional model is created by successive layers of material;

- Cloud Computing - possibility to access files and perform different tasks over the Internet without the need to install applications, for example;

- Artificial intelligence - a branch of computer science that aims to create machines with intelligence similar to human;

- Virtual Simulation - systems capable of simulating the behaviour of the equipment to be reproduced; and

- Internet of Things - a technological revolution that aims to connect items used in people's daily lives to the world wide web.

Motivated by this phenomenon, there is an increasing incorporation of digital technologies in various daily activities, such as, for example, applications for scheduling consultations or performing banking operations, autonomous cars, machinery and products control through sensors or any other another technology that optimises the realisation of activities, in terms of financial costs and time, in order to corroborate, in the end, the process of digitalisation of the economy.

With the digitised economy, business opportunities arise at the national and international levels. However, new forms of crime and malicious actions are also emerging. Cybercrime is a global phenomenon, usually with multiple territorial connections. Because of these characteristics, it is impossible for a country to act alone in combating crimes in the cyber environment. In this sense, there is room for the search for greater international integration, especially among police forces, investigators, justice agencies and other actors related to criminal investigations in the digital environment. In all these actions, a collaborative environment must be maintained for allowing the study and wide use of emerging technologies.

It is noteworthy that cybersecurity is a global issue in which the interaction between different actors in the international community is paramount for the construction of a safe and reliable digital environment. In this sense, it is recommended that the country adopts guidelines that, through confidence-building measures, aim at interstate cooperation, intense information exchange, transparency, predictability of actions, reaffirmation of international peace and stability, in order to corroborate to reduce the risk of escalating cyber incidents globally.

At the international level, in relation to the cyber theme, the country must continue to be guided by Brazilian constitutional principles, by the fundamental values of our society - such as respect for democracy and human rights - by the emphasis on multilateralism, by respect for international law, by its vocation for dialogue and the peaceful settlement of disputes, including the identification of new commercial opportunities. The existence of regulations such as Law 12,965, of 2014 - Marco Civil da Internet, and Law 13,709, of 2018 - LGPD, combined with Brazilian Internet development policies, reinforce the country's actions in international forums for discussing information and communication technology and, in particular, cybersecurity.

Observing the international scenario, it is perceived an urgent need for cooperation between countries to mitigate threats such as: cybercrimes, cyberattacks on critical infrastructures, cyber-espionage, mass data interception and offensive operations designed for projecting power thru the improper and disproportionate application of force in peacetime. In this sense, it is necessary to reinforce Brazilian action in the preparation and review of international instruments related to cybersecurity, by stimulating debates and encouraging international cooperation on the subject. The need for greater integration

between Brazil and Latin America countries is also identified, with the country being an important regional driver.

It is noteworthy that the country intends to seek bilateral cooperation agreements in cybersecurity with as many countries as possible, as a demonstration of our intention to establish, in this field, relations that are adequate, fruitful, constructive and transparent. Therefore, it is considered that strategic partnerships are fundamental, and shall always be guided by principles such as trust, aggregating capacity, and effective contribution, in order to provide opportunities for other actors, besides the members of the Public Power, can also contribute.

International cooperation, therefore, must be made possible through actions that ensure its development and its continuous implementation, and shall include, among others, information sharing (benchmarking, technological knowledge, doctrine, threat analysis, cyber intelligence sharing, evaluation of major cyber crises) and the signing of instruments on the topic.

In this sense, E-Ciber recommends the country's participation in international efforts to develop standard operating procedures to be used for the sharing of information and responses to major transnational crises, and to encourage the participation of public and private entities in regional and international organisations as a way of supporting cooperation with strategic partners.

With regard to international acts related to the treatment of classified information, the Office of Institutional Security of the Presidency of the Republic has the competence to conduct negotiations, in conjunction with the Ministry of Foreign Affairs. Currently, the Institutional Security Office of the Presidency of the Republic follows dozens of agreements for the exchange and mutual protection of classified information.

Also with regard to bilateral agreements, Brazil shall encourage the negotiation of Mutual Legal Assistance Treaties (MLATs) in order to better combat cybercrime when it expands beyond our borders.

In the pursuit of this international engagement, it is essential that Brazil participates in future normative structuring initiatives, such as those related to the creation of standards that will guide security in emerging technologies, such as 5G communication networks, artificial intelligence and the Internet of Things. In this way, the country will be better able to work and influence these standards, recognising that they consist of international challenges.

It is a fact that the integration and cooperation between public administration, private sector and society, in several areas, usually bring beneficial results, and contributes to raising the citizen's trust in public and private institutions and improves the relationship between these actors. In the area of cybersecurity, this relationship is essential, since, as the theme is transversal, the best results will only be achieved if everyone acts in a coordinated manner, always aware that no actor can, in isolation, face all the challenges imposed by new technologies. In this sense, well-defined responsibilities are needed, and the Government has the central role of coordinating this complex ecosystem, by directing efforts towards the well-being of society.

The need to establish and consolidate strategic partnerships in the cyber environment becomes even more evident when it is found that a large part of critical infrastructures is under the responsibility of the private sector, which reinforces the need for common purposes, in cybersecurity, between Government, private companies, academia and society in general.

In Brazil, the coordination processes between the different players of the cyber environment, to date, comprise a wide range of arrangements that are not always institutionalised and perennial, nor linked to conventional regulatory mechanisms [57]. Added to this fact is the existence of a large number of institutions that deal directly or indirectly with cybersecurity, which poses great challenges for cooperation and coordination for the Brazilian State. Therefore, it is recommended to create appropriate communication channels, so that the largest number of segments of Brazilian society can be heard and contemplated when designing, implementing and promoting public policies related to cybersecurity.

It is important to highlight that partnerships in the cyber field tend to consolidate if they are based on trust, interests and common goals, where action plans are built together, and where coordination mechanisms are effective. In view of this, it is becoming more relevant to hold meetings with leading players in cybersecurity and the institution, if necessary, of working groups and forums on the topic.

Therefore, as cybersecurity is extremely important for public authorities and private institutions, it is understood as relevant the creation of a mechanism for sharing information on cyber risks, in order to contribute to the identification, management and mitigation of risks. This continuous exchange of knowledge will help organisations to avoid, assess and manage risks correctly, in addition to enabling a more effective and efficient coordinated approach.

2.4. Education

Building a connected society has been a challenge for the Brazilian State. However, thanks to technological modernisation and to the expansion of telecommunications networks, which resulted in a fast and massive access to the Internet by millions of Brazilians, as discussed in the Diagnosis, today 98% of the population has access to mobile networks and 60% of households have access through the wired network. However, this reality has raised a series of new concerns, especially with regard to vulnerabilities and cyber threats.

As a consequence of greater access to digital networks, and due to the lack of maturity in cybersecurity, Brazil occupies a prominent place in the ranking of countries that receive the most cyberattacks. The lack of culture in cybersecurity, qualification and knowledge in this topic by a large number of Brazilians connected to the digital world shows that our society is not prepared for the use of digital tools with the proper care related to cybersecurity.

In this context, stands out the importance of digital literacy, a concept that, according to Western Sidney University [58], means “having the necessary skills to live, learn and work in a society in which communication and access to information occur increasingly through digital technologies, such as Internet platforms, social media and mobile devices”. This digital education effort, which includes technological inclusion, aims to fill a huge gap between current users of these technologies and those belonging to the group of so-called “digital natives”, an expression created in 2001 by Marc Prensky [59], an American education specialist, who used the term to refer to all those born after 1980, whose biological and social development took place in direct contact with technology.

Thus, it is recommended to develop a culture of cybersecurity, through education, that reaches all sectors of society and levels of education, in order to prevent incidents and allow the responsible use of technologies, as one of the key factors for the development of the country.

Cybersecurity education is conceived in three areas, with an increasing degree of content specialisation, and with a decreasing degree of coverage of society, as follows:

- Training - professionals in the field or with functions that require skills in the field;

- Formation - portion of society found in school banks; and

- Awareness - society and its sectors.

Awareness is obtained through actions aimed at sensitising specific sectors of society, or this as a whole. In a more restricted focus, formative education covers the teaching of cybersecurity directed to the part of society that is in early childhood education, elementary school, high school and higher education. Finally, Training includes education, in the professional and technological modality, aimed at continuing education for professionals in the area, or for those whose job or function require deeper and specialised technical cybersecurity knowledge. Training is the most specialised form of action and can be carried out through short-term training, security certifications, among other means.

With regard to the implementation of these three strands of cybersecurity education, responsibility must be shared between state agencies, the educational sector, social services in commerce and industry, and national learning systems. It shall be noted that, for this, there are a number of educational resources available, as shown below:

- Training - Training Plans for teachers, managers and specialists and the Talent Banks;

- Formation - the creation of courses and the insertion of the theme in school curricula;

- Awareness - Awareness Plans in schools and institutions, Portals of good practices and Educational Campaigns.

In the context of awareness, it is encouraged the design of public policies, which lead to situational awareness in the current scenario of cyber threats, and encourage responsible and safe behaviour on the part of Internet users.

Awareness actions have become an essential tool for behavioural changes related to the cyber environment, and are relevant, as they lead individuals to realise, in their personal or professional routine, what attitudes need to be corrected in the digital world.

As an example, the National Cybersecurity Awareness Month, held every October, is a collaborative effort between the United States Government and the industry, for increasing awareness regarding the importance of cybersecurity and ensuring that all Americans have the resources they need to be safer online.

Awareness shall reach wide audiences, among individual and corporate users, from children to the elderly. It must also be continuous, creative and motivating, in order to grab the attention of the target audience, for changing the behaviour favourably in the cyber environment, being important the promotion of periodic actions, within the society, with the objective of a more secure and responsible use of information and communication technology resources, and the protection against typical risks in cyberspace.

An awareness programme can include the following tasks:

- define the target of the awareness campaign;

- develop mechanisms to reach this target audience;

- identify common behavioural problems that affect the target audience or that they must know;

- improve the content of government websites, especially the most accessed ones, with material related to cybersecurity; and

- consider translating the material into other languages.

It is recommended the strengthening of cybersecurity training and education programmes. Such a suggestion is a current demand from public and private organisations. According to the Centre for Strategic and International Studies, it is estimated that there are between one and two million unfilled jobs worldwide in the area of cybersecurity [60].

The rapid technological advance, accompanied by the proposed digital transformation of modern societies, made essential the development of educational and pedagogical actions for training in favour of the judicious, safe and responsible use of technologies. In this sense, it is considered that the priority of investments in education programmes related to cybersecurity is an essential pillar to reduce risks to companies and society.

In the context of training, the approach to cybersecurity in Brazilian schools is still very incipient, if not, non-existent. In the context of higher education, cybersecurity, as a discipline or study programme, is still difficult for students to access. Cybersecurity, in general, is not an isolated academic topic, but part of the curriculum of the Computer Science undergraduate courses, being an ever-changing topic that requires constant training and education. However, it is noteworthy that there are already educational initiatives in areas related to cybersecurity, such as the recent creation of the Higher Technology in Cyber Defence course, in the National Catalogue of Higher Technology Courses.

In this sense, according to McAfee Reporter, “continuous learning is vital to retaining talent in cybersecurity. Although employers may be cautious about investing in expensive training programmes that make employees more attractive in the talent market, our research shows that the absence of such training is often a significant factor in people's decisions to seek alternative employment.”

Currently, universities and institutions do not train enough experts in cybersecurity to meet the growing needs of the sector; however, the theme has become so relevant that it cannot remain restricted to those entities, but must be known and dominated by all levels of education.

It is recommended to place emphasis on cybersecurity in the curricula of technical courses, particularly those involving software development, at the levels of high school and higher education, and in the curricula of the “technological education and professional training” [61] modality.

In the context of cybersecurity training, the situation is no different. A survey conducted in 2018 by ManpowerGroup [62], a world leader in innovative workforce solutions, with approximately forty thousand employers from forty-three countries, shows that almost half of them (45%) have difficulty finding qualified people, including in the cybersecurity segment. Among Brazilian employers, 34% say they have difficulty recruiting talents. The digital age has transformed work models, which demand new skills.

The greatest difficulties for companies in the hiring process in Brazil are the lack of technical skills (33%), followed by the lack of experience (23%) and the lack of interpersonal skills (19%). The first has to do with the Brazilian educational gaps. The second is related to the resistance of recruiters to give an opportunity to newbies. And the

third one is related to behavioural competencies, which are not innate, being possible to develop them. Such difficulties in hiring demonstrate the mismatch between the situation of existing professionals and the needs of the labour market.

Despite the educational efforts undertaken so far in the field of information and communication technology, it appears that they have been insufficient in the face of national demand. “According to a study released by Brasscom - Brazilian Association of Information and Communication Technology Companies, the technology market in Brazil will need approximately 70 thousand professionals per year until 2024, a number that may represent a deficit of 260 thousand qualified people in the period” [63].

The study adds that today, in the country, “the ICT sector - information and communication technology is responsible for 845 thousand jobs and trains 46 thousand students per year with a technological profile in higher education”. The report also states that "the most requested specialisations that need immediate manpower are those of web and mobile developers, cloud computing, data sciences, cybersecurity and artificial intelligence".

It is verified that the private sector is intensely concentrated in the development of the workforce, but needs the support of the State in the formation of the future workforce. To this end, governmental actions are recommended in order to provide greater training and education opportunities for information technology and cybersecurity professionals, in order to improve the training required for the implementation of multiple digital technologies and solutions. This objective can be achieved, for example, through partnerships with universities for the development of cybersecurity curricula; training in the area, through seminars and workshops; and the creation of programmes aimed at areas internationally known as STEM - Science, Technology, Engineering and Mathematics [64].

Despite the current cyber scenario, companies continue to suffer from the lack of better-qualified professionals and the retention of their talents, according to the State of Cybersecurity: 2019 study, from the global association of information technology, security and cyber audit – ISACA [65], released in early 2019. According to the survey, retaining cybersecurity professionals is very difficult, and the training and certifications promoted and paid for by the employer are not enough to guarantee retention. Cybersecurity professionals are migrating more frequently from their jobs to those who offer higher pay, prospects for career advancement and a perception of healthier work environments.

Finally, according to ISACA research, companies are implementing several strategies to retain cybersecurity professionals, including providing additional training. Fifty-seven per cent of respondents indicate that their companies invest in more training, as an incentive for their employees to remain in them.

As the forecasts for 2020 indicate that small and medium-sized enterprises are the next target of cyberattacks, the need for awareness actions is emphasised. The first step is the recognition by companies that their data is not 100% secure. This means that attacks, reduced productivity and damage can be avoided if there is a change in attitude. The subject is common, and concepts such as the Zero Trust, reflected in greater rigidity in the access to the network, in the inspection and in the registration of traffic, have been discussed and applied in the corporate environment.

The trend is that cybercrimes occur more frequently in the niche of small and medium-sized companies, since, in general, these companies do not adopt the appropriate

preventive measures and actions. As smaller companies are often the service providers for larger companies, this makes smaller companies a connection channel for large organisations that allow infiltration attacks.

In this sense, it is emphasised the importance of raising managers' cybersecurity awareness, both in the public and private sectors, since most of them decide on the allocation of resources and the time allocated to projects defined as priorities. This initiative grows in importance with the urgent compliance of public and private entities with the recent Law 13,709, of 2018 - General Law for the Protection of Personal Data (LGPD), which highlights the need for such institutions to invest in training programmes on the protection and privacy of such data.

In this context, it is recommended to encourage initiatives to increase interest and access to education in computer science for students of basic education, with the possibility of expanding public-private partnerships, rethinking professional education and training more teachers to qualify them properly on the subject.

It is also identified the need to develop cybersecurity training programmes for workers of the public and private sectors, so that they can improve their knowledge and develop new skills in this area.

Data from the Organisation for Economic Cooperation and Development - OECD reveals that by 2021 there will be three and a half million vacancies in the cybersecurity job market worldwide. In Brazil, a survey by the Brazilian Association of Information and Communication Technology Companies - Brasscom estimates that, by 2024, the market will demand four hundred and twenty thousand professionals in the area of information and communication technology, with forty-five thousand specifically for the cybersecurity segment. Such numbers lead to the understanding that the greatest deficiency in the fight against cybercrimes will not be technological, but rather the lack of human resources.

A recent survey conducted by the Centre for Strategic and International Studies – CSIS [66], with information technology decision-makers from eight countries, revealed that 82% of employers report a lack of skills of their employees in cybersecurity, and 71% believe that this talent gap causes direct damage to their organisations.

In Brazil, the following gaps have been identified:

- few professionals specialised in cybersecurity;

- low awareness of users; and

- few educational programmes focused on the area.

Combating cyberattacks requires continuously trained professionals. In this sense, there is an urgent need for a nationwide training programme aimed at technical training and the improvement of human resources with a view to strengthening cybersecurity in government agencies and private companies. In this context, public institutions shall seek articulation and strengthening in the cybersecurity area, through collaborative actions and partnerships with the private sector, with academia and with the third sector, in Brazil and abroad, to stimulate the continuous development of critical mass and talent. It is viewed as one of the possible alternatives, the availability of free cybersecurity training on virtual government platforms.

The investment in training security professionals - managers, analysts and even operators - aims to adopt not only a preventive or reactive attitude in face of threats and cyber

incidents, but also a consultative attitude, which will result in greater confidence on the part of the final areas of their institutions, and in less resistance, in case of recommendations.

It is also noted that, in general, security teams face a disparity between the availability of qualified labour and the sophistication of threats, being highly important the investment in training professionals so that they can effectively face these constant challenges.

Finally, the effectiveness of the development of cybersecurity culture through awareness, training and capacity building depends on well-structured knowledge management, in order to continue all the processes involved, to train professionals in the state-of-the-art and to depend on the dynamics of the emergence and obsolescence of cybersecurity skills.

REFERENCES (not translated)

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

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

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

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

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

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

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

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

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

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

11. References of sources used for composing the scenario described on Annex I - Diagnosis:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

49. BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em julho de 2019.

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

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

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

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

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

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

56. *ALAGOAS: INDÚSTRIA 4.0 TAMBÉM SERÁ NECESSIDADE PARA PEQUENAS EMPRESAS*. AGÊNCIA DO RÁDIO MAIS. 05 Out 18. Disponível em:

<https://www.agenciadoradio.com.br/noticias/alagoas-industria-4-0-tambem-sera-necessidade-para-pequenas-empresas-mrin180127>. Acesso em agosto de 2019.

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

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

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

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

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

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

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

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

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

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