Internet Sectoral Overview

Number 2
July, 2026
Year 18

Internet in Brazil: Robustness, trust, and security

Building trust in the digital environment: The role of NIC.br in promoting a more secure Internet in Brazil[1]

The spread of the Internet and digital technologies has driven an increasingly rapid digital transformation in various dimensions of society, in the social and economic spheres, expanding its centrality in the daily activities of individuals, organizations, and governments. While the increasing incorporation of these technologies is associated with significant benefits for economic development and social well-being, their growing presence in everyday activities also introduces new challenges. Among these challenges, the growing exposure to digital risks and the potential security incidents associated with the use of Internet-connected devices stand out, which, to some extent, makes their users more vulnerable in the digital environment.

Since its inception, the Internet was developed in a context characterized by trust-based relationships among the participants connected through the computer network, which was initially composed of a limited number of academic, governmental, and research institutions with common ties or purposes. In this scenario, the fundamental network protocols were designed with a focus on interoperability and information exchange, without incorporating robust security mechanisms as central requirements of their design. With the network's expansion and its increasing use across different segments of society, the original premise of trust has proven insufficient in the face of contemporary digital security challenges.

[1] This article was written by Javiera F. Medina Macaya, a researcher at the Regional Center for Studies on the Development of the Information Society (Cetic.br), a department of the Brazilian Network Information Center (NIC.br), based on institutional materials from each of NIC.br's initiatives. Javiera holds a Ph.D. in Business Administration and a master's degree in Public Administration and Government from the Fundação Getulio Vargas's São Paulo School of Business Administration (FGV EAESP), with a bachelor's degree in Public Policy Management from the University of São Paulo (USP). The article was reviewed by managers involved in these initiatives.

There is no single solution for security and incident handling; as a result, the operationalization of these activities involves several areas of operation within NIC.br, with its various departments working together to foster a network in line with the governance principles approved by CGI.br.

Although the fundamental protocols of the Internet have evolved over time, incorporating new mechanisms and extensions, many continue to be based on an architecture conceived in a context where security was not a central requirement. With the increasing expansion of connectivity and the intensification of the digitalization of economic and social activities, security attacks are taking on new proportions, and the associated risks and incidents have assumed greater scale and complexity. While in the past carrying out attacks required high level of technical knowledge and tended to have relatively limited impacts, the widespread availability of automated tools has now lowered the barriers to entry for malicious actors, significantly increasing the potential impact on individuals, organizations, and critical infrastructure.

One of the principles[2] guiding Internet governance in Brazil concerns the preservation of the network's functionality, security, and stability. To ensure these three attributes, it is essential to adopt technical measures aligned with international standards and to encourage the implementation of best practices by the different stakeholders in the digital ecosystem. In this context, the NIC.br, an entity linked to the Brazilian Internet Steering Committee (CGI.br), is responsible for registering domain names and allocating Internet Protocol (IP) addresses in Brazil, as well as supporting the development of the Internet in the country, promoting its security, stability, and resilience. These activities promote the stability and robustness of the network in Brazil, including the production of studies, recommendations for technical standards and norms for Internet networks and services, and the handling of and response to security incidents.

There is no single solution for security and incident handling; as a result, the operationalization of these activities involves several areas of operation within NIC.br, with its various departments working together to foster a network in line with the governance principles approved by CGI.br. The following actions related to the promotion of security in the Internet in Brazil are presented below.

The Brazilian National Computer Emergency Response Team (CERT.br), a department of NIC.br, acts as a national Computer Security Incident Response Team (CSIRT) of last resort. With the mission of increasing security levels and incident handling capabilities of networks connected to the Internet in Brazil, CERT.br operates in the field of information security incident management, providing services to any network that uses resources managed by NIC.br; these services are structured around incident management, situational awareness, and knowledge transfer. In article II ("Security and incident handling in Brazil: History and role of CERT.br"), Cristine Hoepers, manager of CERT.br, presents the history, areas of activity, and the department's role in the incident handling process. One important initiative is the *Cartilha de Segurança para Internet*, which brings together a series of publications offering recommendations and tips for safer browsing and protection against potential threats, aimed at Internet users.

[2] The Principles for the Governance and Use of the Internet, developed and adopted by the CGI.br in 2009 (Resolution CGI.br/RES/2009/003/P), underpin and guide the committee's actions and decisions. More information about the resolution and principles can be found at: https://www.cgi.br/resolucoes-2009-003-en/ and https://principios.cgi.br/

Another important aspect concerns the robustness and quality of the country's infrastructure. Registro.br is the department of NIC.br responsible for registering and maintaining domain names under .br and publishing them via the Domain Name System (DNS). In addition to the security and robustness that characterize DNS services, since 2007, it has been possible to use Domain Name System Security Extensions (DNSSEC). This international standard confirms the content of the DNS and helps prevent attacks by validating the data and guaranteeing the origin of the information. Another aspect related to infrastructure is the maintenance of the country's mirrors of the Internet's root servers; one of its results is improved access quality through Brazilian networks, since the information about the Internet's root is duplicated and physically closer.

The robustness and quality of the network infrastructure in Brazil are also strengthened by IX.br (Brazil Internet Exchange), an initiative of the Centre of Study and Research in Network Technology and Operations (Ceptro.br), a department of NIC.br responsible for Internet Exchange Points (IXP), which promote direct and local interconnection among the Autonomous Systems (ASes) that compose the Internet in Brazil. With 39 IXPs distributed across metropolitan areas in all five regions of the country, IX.br is the largest network of IXPs in the world: It consists of approximately 3,800 participating ASes, generating over 7,000 connections across all locations. This shared infrastructure allows data traffic to remain regionalized, streamlining the path data travels and enabling a faster, more efficient, resilient, and lower-cost Internet for end users. In countries with large territories like Brazil, IXPs play an important role in the dissemination of the Internet across the country, as they facilitate local providers bringing broadband to areas less commercially attractive to large operators.

Beyond infrastructure, raising awareness about their importance, as well as training and coordinating stakeholders around IXPs, is crucial: The greater the number of participants, the denser the ecosystem of interconnected networks will be. Therefore, in addition to the IXPs, NIC.br created the OpenCDN project,[3] which aims to reduce the distance between Content Delivery Networks (CDNs) and Internet users by enabling infrastructure sharing. With OpenCDN, these content delivery networks can install their caching servers in the initiative's data centers, located in different regions of Brazil and connected to the local IXPs of the IX.br. The increasing concentration of traffic in local infrastructures illustrates this dynamic: In 2026, IX.br reached 50 Tbit/s of aggregate traffic, while OpenCDN surpassed 1 Tbit/s of content distribution in the country.[4]

In countries with large territories like Brazil, IXPs play an important role in the dissemination of the Internet across the country, as they facilitate local providers bringing broadband to areas less commercially attractive to large operators.

[3] Find out more: https://opencdn.nic.br/

[4] Available at: https://ix.br/noticia/releases/ix-br-bate-recorde-de-50-tbit-s-de-trafego-internet-agregado-impulsionado-por-conteudo-e-servicos-digitais/

Figure 1 – SOME NIC.br INITIATIVES PROMOTING THE SECURITY, STABILITY, AND ROBUSTNESS OF THE INTERNET IN BRAZIL

Secure Internet
https://internetsegura.br/
INTERNET SEGURA BR

A portal that brings together initiatives to raise awareness of security and the responsible use of the Internet in Brazil, with materials tailored to different audiences.

Program for a More Secure Internet
https://bcp.nic.br/i+seg/
PROGRAMA INTERNET +SEGURA

An initiative that promotes the dissemination and use of Internet standards and fosters educational initiatives and public policies related to the Internet.

BCOP Challenge
https://bcp.nic.br/desafiobcop/
BCOP

Award intended for institutions that adopt good operational and security practices, to give visibility and recognition to their effort.

Surveys on ICT use in Brazil
https://cetic.br/pt/pesquisas/
cetic.br

Robust data for monitoring aspects related to digital security and information security policies for individuals and organizations.

Cartilha de Segurança para Internet
https://cartilha.cert.br/

A portal composed of a set of documents with recommendations and tips for users about Internet security and ways to protect themselves from potential online threats.

BCP
https://bcp.nic.br/
BCP

A portal that brings together a set of operational best practices for ASes connected to the Internet.

SIMET
https://simet.nic.br/
SIMET

System available to the public to test and find information about Internet quality metrics, allowing for a better understanding of network capacity.

Source: Prepared by the author.

Another relevant initiative is the Portal of Good Practices for the Internet in Brazil (Portal de boas práticas para a Internet no Brasil [BCP]), maintained by professionals from various areas of NIC.br, such as CERT.br, Ceptro.br, and Registro.br, in collaboration with experts external to NIC.br. The portal focuses on raising awareness and disseminating Best Current Practices (BCPs) for Internet-connected ASes, offering technical recommendations. Although not exclusively, the portal is based on BCPs published by the Internet Engineering Task Force (IETF) aimed at ASes, through it, one can also stay up to date on the evolution of Internet standards. This initiative also includes the BCOP Challenge (Desafio BCOP), which rewards institutions for adopting BCPs and security measures.

The Program for a More Secure Internet (Programa por uma Internet mais Segura) is another NIC.br initiative focused on security, which encompasses some of the initiatives mentioned. Through various activities, it seeks to support the Internet technical community in reducing Distributed Denial of Service (DDoS) attacks on Brazilian networks, prefix hijacking, route leaks, spoofing of source IP addresses, vulnerabilities, and misconfigurations present in network elements. Furthermore, it also aims to bring together the different teams responsible for network security and stability to create a security culture among its operators. Given that security issues are complex and require joint action, the program directly involves four technical departments of NIC.br: CERT.br, Registro.br, Ceptro.br, and IX.br. In this edition of this publication, interview I ("Internet security in Brazil: A trajectory of cooperation"), featuring Gilberto Zorello, project coordinator at NIC.br, presents these initiatives, highlighting the importance of collaboration and their dissemination among different target audiences.

The production of relevant and reliable metrics is also an activity developed by NIC.br that contributes to guiding decision-making processes and the formulation of public policies. In addition to metrics related to network security aspects, NIC.br handles measurements and statistics through the Measurements team[5] of Ceptro.br | NIC.br and the Regional Center for Studies on the Development of the Information Society (Cetic.br | NIC.br).

Ceptro.br | NIC.br is responsible for initiatives and projects that support or improve the Internet infrastructure in Brazil, contributing to its development; specifically in the area of measurements, the Internet Traffic Measurement System (SIMET) was developed, through which initiatives are organized to improve Internet quality and foster actions that support and enhance the Internet infrastructure in the country. SIMET is a technology that enables users to perform accurate and reliable Internet quality measurements, assessing connection quality and explaining what each value means and how it impacts their Internet experience; in this way, it provides relevant information that helps users identify and resolve Internet connection problems. The aspects that should be highlighted are its reliability and independence, based on the possibility of performing measurements for SIMET servers inside and outside the providers' networks, on the neutral NIC.br's servers located in the IXPs. Furthermore, SIMET offers solutions for consumers, providers, the public sector (in areas such as education and health), and solution integrators to promote continuous network improvement.

The production of relevant and reliable metrics is also an activity developed by NIC.br that contributes to guiding decision-making processes and the formulation of public policies. In addition to metrics related to network security aspects, NIC.br handles measurements and statistics through the Measurements team of Ceptro.br|NIC.br and Cetic.br|NIC.br.

[5] Find out more: https://medicoes.nic.br/

The stability of the projects developed by the different departments of NIC.br allows for the continuity and permanence of the various services. (...) these initiatives enable the development of relationships based on trust and national and international recognition (...).

Cetic.br | NIC.br, in turn, is the department responsible for producing statistical data and analyses on access to and use of information and communication technologies (ICT) in Brazil. To this end, internationally defined methodological approaches are used to ensure the international comparability of the data produced, by conducting nationwide surveys conducted across various sectors of society, whether among individuals or organizations. Specifically, the center collects data on existing digital security policies and practices in Brazilian enterprises through the ICT Enterprises survey; security incidents and attacks through the ICT Providers survey; and information security policies through ICT in Health, ICT in Education, and ICT Nonprofit Organizations surveys. The Privacy and Personal Data Protection survey, which has institutional support from the National Data Protection Authority (ANPD), seeks to understand the challenges to building a digital ecosystem that guarantees privacy and the protection of personal data in Brazil. It gathers indicators collected from individuals, enterprises, and public organizations (government, health, and education) in order to identify their practices and perceptions on the subject. Finally, the ICT Households and ICT Kids Online surveys address issues related to digital security from the perspective of individuals.

In addition to all these initiatives aimed at specialists and technicians, NIC.br also promotes awareness about Internet security and responsible use in Brazil, with support materials aimed at Internet users. The Secure Internet portal functions as a space that brings together information of interest and materials focused on different audiences: children, teenagers, parents and guardians, educators, elderly people, technicians, and the general public.

The stability of the projects developed by the different departments of NIC.br allows for the continuity and permanence of the various services. Always striving for a better Internet in Brazil, these initiatives enable the development of relationships based on trust and national and international recognition—a reputation that is essential for relations within the digital security ecosystem, as it enables valuable international partnerships with related institutions.

Together, these initiatives demonstrate NIC.br's comprehensive efforts to promote a more secure, stable, and resilient Internet in Brazil. By strengthening critical network infrastructure, coordinating incident prevention and response actions, disseminating best technical practices, training the operator community, and producing data and indicators on digital security, NIC.br contributes to building a more reliable digital environment for users, organizations, and public institutions.

By engaging different actors in the Internet ecosystem, promoting solutions aligned with international standards, and strengthening the security, stability, and resilience of the network, NIC.br promotes the expansion of the national capacity to address digital risks, improve the quality and security of Internet services, and strengthen trust in the digital environment. In this way, NIC.br creates conditions for the economic and social benefits of digital transformation to be enjoyed by the entire Brazilian society, with greater security and in a more sustainable way.

Article II

Security and incident handling in Brazil: History and role of CERT.br

By Cristine Hoepers

Photo: Klaus Steding-Jessen

Cristine Hoepers
Manager of CERT.br

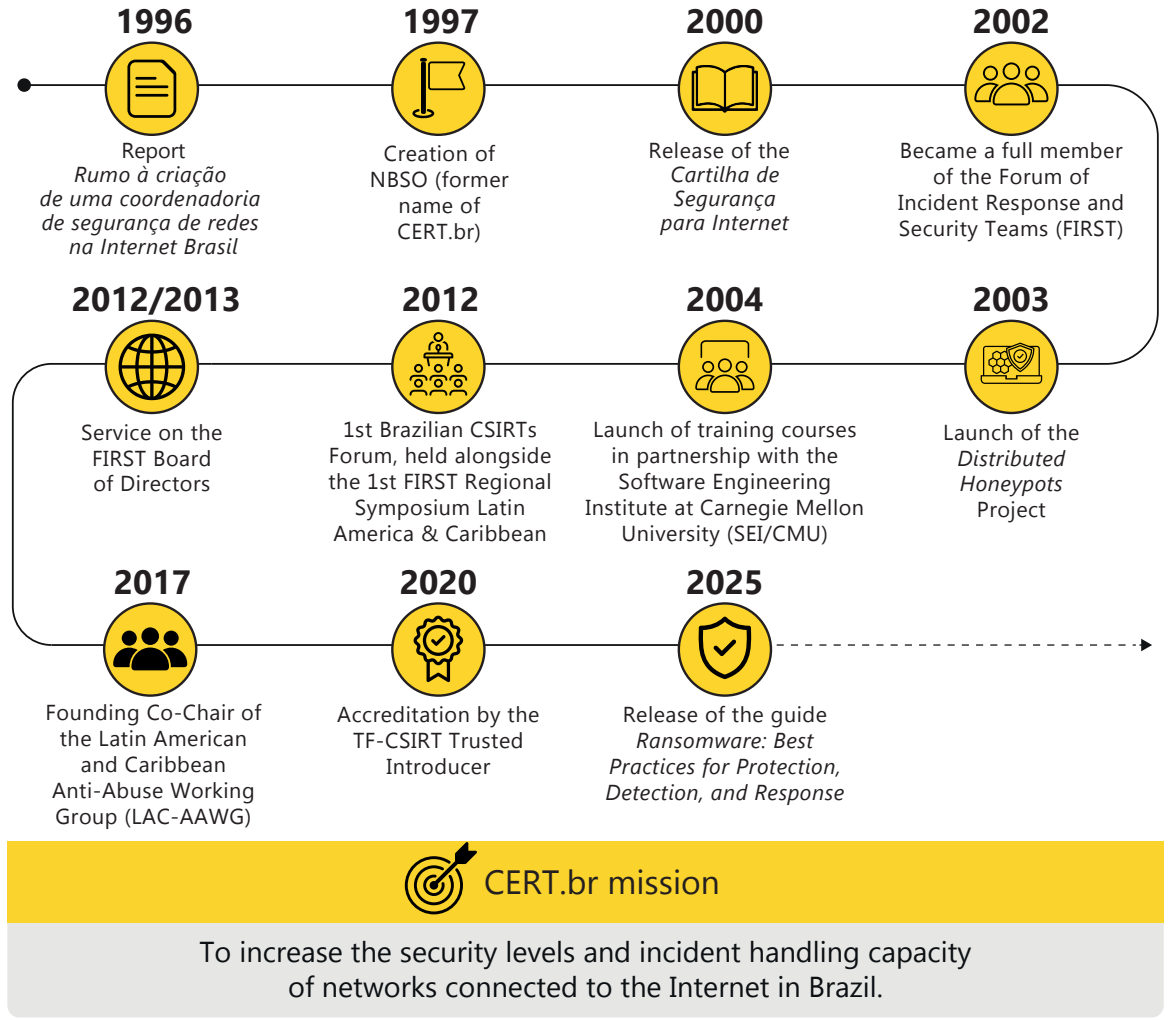
The Brazilian National Computer Emergency Response Team (CERT.br) is the national Computer Security Incident Response Team (CSIRT) of last resort, maintained by the Brazilian Network Information Center (NIC.br). Its mission is to increase the security levels and incident handling capacity of networks connected to the Internet in Brazil.

Its history began to take shape in August 1996 with the publication of the report *Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil* (Gomide et al., 1996), produced by the Security Working Subgroup of the Network Engineering Working Group (GTER) of the Brazilian Internet Steering Committee (CGI.br). This report was the result of a year of debate within the Brazilian Internet community, motivated by the need to address the growing number of computer security incidents that accompanied the rapid growth of the Internet in Brazil after its opening for commercial use in 1995. The report presented a diagnosis of the country's situation at that time and outlined paths to create a structure that would help organizations better handle incidents, given the complexity and scale of the national scenario. This diagnosis described the objectives and responsibilities sought by the community for a coordination center for issues related to digital security in Brazil:

> The goal of creating an organization responsible for coordinating network security is not for it to take on all the necessary tasks. This organization must possess a basic set of responsibilities from which it can assign or encourage the performance of such tasks by third parties, acting only as a coordinator of the activities. Therefore, it should possess the following attributes:
>
> - Receive and record reports of network security breaches;
> - Collect statistics on these occurrences and make them public;
> - Provide technical guidance to those who turn to it to resolve security flaws;
> - Mediate contact between networks involved in security incidents, serving as a legal witness to their actions;
> - Promote the creation of training and refresher programs in network security through close interaction with the Human Resources Training Working Group;
> - Promote the holding of network security meetings and conferences;
> - Represent Brazil as one of the security agencies at the national and international levels (Gomide et al., 1996, section Attributions).

This vision of needs and responsibilities guided the creation, on June 1, 1997, of the NIC.br Security Office (NBSO), the name by which CERT.br was known until December 2005 (Figure 1).

Figure 1 – CERT.br TIMELINE



Source: Prepared by the author.

The initial phase of the operation was dedicated to establishing the infrastructure, introducing the team to the national and international Internet communities, and building a network of contacts and cooperation. In 1999, the regular release of statistics on incidents reported to the team began, along with its first proactive activities, including security awareness presentations and the dissemination of best practices at specialized technical events on security and networks.

Looking back on its history, one of the factors that still fosters CERT.br's trust within the community and partnerships across sectors today is its inception, which involved a participatory, bottom-up approach. This approach did not originate from a single person or agency, but from professionals who already communicated and worked together, contributing to the building of strong cooperation and to the team being recognized as part of the Brazilian Internet community.

At the time, there were only a few dozen CSIRTs worldwide; FIRST,[6] for example, had only 53 members, drawn almost exclusively from Europe and North America. Setting up the CERT.br's operations and choosing the services that made the most sense for the Brazilian context was a gradual process that involved focusing the limited human resources available on the activities perceived as having the greatest impact on improving the country's security posture, namely: establishing itself as a focal point for receiving and forwarding incident notifications to those who needed to be involved in the resolution; maintaining statistics on these incidents to have data for situational awareness; and encouraging Autonomous Systems (ASes) and large organizations to define points of contact for handling incidents and, ideally, create their own CSIRTs.

Since then, incident response teams have matured, the field has gained global relevance, and operational frameworks and standards have been created, including contributions from CERT.br's professionals. In line with this evolution, the center's services were restructured according to these frameworks and are grouped into the following major areas: incident management, knowledge transfer, and situational awareness (Figure 2).

The main role of CERT.br is to act as a national point of contact of last resort for reporting security incidents, especially when a more specific contact is not known, assisting in the analysis and forwarding the matter to the correct contacts.

INCIDENT MANAGEMENT

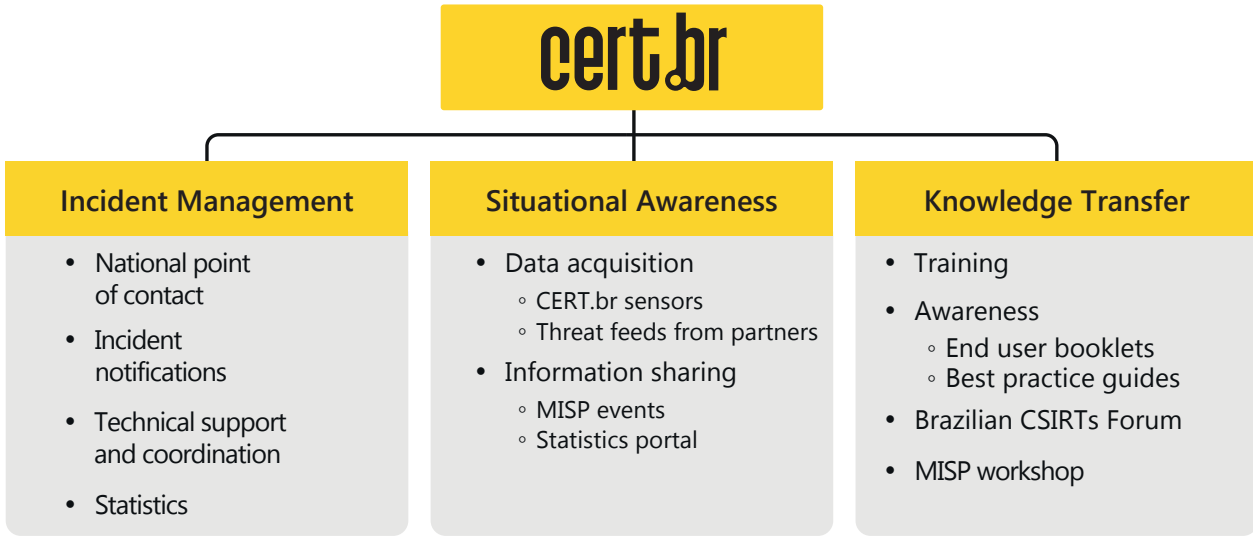
The main role of CERT.br is to act as a national point of contact of last resort for reporting security incidents, especially when a more specific contact is not known, assisting in the analysis and forwarding the matter to the correct contacts. This work aims to facilitate communication between professionals, specialists, and other teams, both domestically and internationally, who may be involved in handling a security incident.

It is important to emphasize that CERT.br does not have access to third-party facilities or systems; its role is to enable other teams to respond to incidents as effectively as possible. In this process, the technical team assists with effective communication to achieve incident resolution through collaborative work, preferably with CSIRTs or Security Operation Centers (SOCs) established by the entities involved, which may be enterprises, universities, Internet access and service providers, government agencies, or other ASes that are part of the national Internet ecosystem. In this process, the team also assists those involved in analyzing malicious activities and compromised systems, and in recommending courses of action that can help recover systems and mitigate the damage caused. The CERT.br statistics portal[7] includes general data on these voluntary incident reports received through the

[6] Find out more: https://www.first.org/
[7] Available at: https://stats.cert.br/

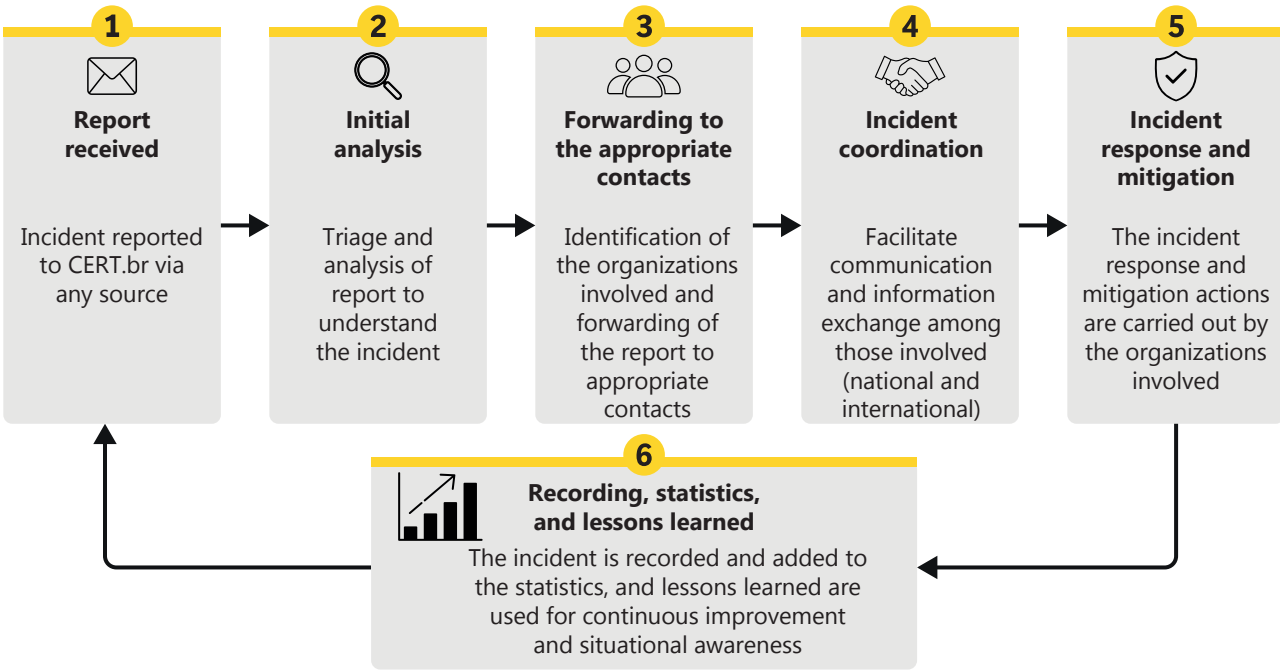
contact e-mail address used for this purpose, as well as specific statistics on fake pages used in phishing attempts, which are derived from these notifications (Figure 3).

Figure 2 – STRUCTURE OF CERT.br AREAS OF OPERATION



Source: Prepared by the author.

Figure 3 – INCIDENT MANAGEMENT: OPERATIONAL PROCESS FLOW



Source: Prepared by the author.

KNOWLEDGE TRANSFER

CERT.br also invests in activities that allow it to transfer to the community the knowledge acquired through experience in the field and through the analysis of threats and vulnerabilities observed in day-to-day activities. These activities include courses, encouraging the development of a CSIRT community in the country, and disseminating best practices and awareness materials, with the goal of better preventing and handling security incidents.

The first end user awareness material published by CERT.br was the result of a community demand: the *Cartilha de Segurança para Internet*.[8] Its history began at a meeting with representatives from the Internet Brazilian Association (Abranet) and the Federation of Industries of the State of São Paulo (Federação das Indústrias do Estado de São Paulo [FIESP]) in the first quarter of 2000, when the Internet service providers present expressed difficulty in finding reliable and concise material that could be used by their customer service departments to assist them when they had security problems. After the publication of the first version, its use went beyond the technical community and began to spread directly among Internet users. Since then, the guide has undergone several revisions that have kept pace not only with technological evolution and the threat environment, but also with evolution in how to communicate security tips in a simpler, more concise, direct way, and with illustrations.

Another key activity in this area is the partnership with SEI/CMU to deliver training courses in Brazil developed by the CERT Coordination Center (CERT/CC), now the CERT Division, which was the first CSIRT created in the world. In a country as large and diverse as Brazil, focusing on training and supporting other teams is a much more effective approach than offering hands-on incident response services. Additionally, instead of trying to create its own training program, the partnership with SEI/CMU allows CERT.br to focus on conveying the content of global best practices, but with an emphasis on how to apply them to the national context.

Moreover, the partnership went much further, as the training materials now include significant content contributions from the CERT.br team and are also used in the United States and other countries. These training sessions[9] have been offered since 2004 and have already resulted in the training of more than 2,000 specialized professionals to work in incident response teams. With this growing community, another important activity is the annual Brazilian CSIRTs Forum,[10] which has been held since 2012 and currently brings together around 800 professionals at each edition, in an event dedicated to community-building and discussing issues related to the organizations' resilience in the face of security incidents.

Other noteworthy materials include the technical recommendations and best practices published by the team, especially the material *Ransomware: Best Practices for Protection, Detection, and Response* (CERT.br, 2025), which focuses on basic steps that organizations of any size can take to prevent and, if affected, mitigate the impacts of this type of attack.

CERT.br also invests in activities that allow it to transfer to the community the knowledge acquired through experience in the field and through the analysis of threats and vulnerabilities observed in day-to-day activities. These activities include courses, encouraging the development of a CSIRT community in the country, and disseminating best practices and awareness materials (...).

[8] The publication is an Internet security guide (available only in Portuguese). Find out more: https://cartilha.cert.br/
[9] Find out more: https://cursos.cert.br/
[10] A Brazilian forum dedicated to community building and the discussion of topics related to organizational resilience in the face of security incidents. Find out more: https://forum.cert.br/

In order to better understand the threat landscape and complement the insights gained from voluntary notifications, CERT.br proactively works to obtain more data sources, aiming to increase its capacity to detect incidents and determine trends in attacks affecting organizations connected to the Internet in Brazil.

SITUATIONAL AWARENESS

In order to better understand the threat landscape and complement the insights gained from voluntary notifications, CERT.br proactively works to obtain more data sources, aiming to increase its capacity to detect incidents and determine trends in attacks affecting organizations connected to the Internet in Brazil.

The first activities related to this area began in 2003, with the start of the implementation of the Distributed Honeypots Project (CERT.br, n.d.), which consists of a network of passive sensors (honeypots) distributed across various networks in the country. This project provides a barometer of malicious activity in the Brazilian Internet space and enables the detection of Brazilian devices that have been compromised and abused by attackers.

In addition to its own source of data on attacks targeting networks in Brazil, CERT.br has established a network of global partners that share threat data related to ASes allocated to Brazil, generally indicating systems that may be misconfigured (allowing abusive use), vulnerable, or showing signs of compromise. Examples of CERT.br's global partners in this area include: Team Cymru,[11] ShadowServer Foundation,[12] and Spamhaus.[13]

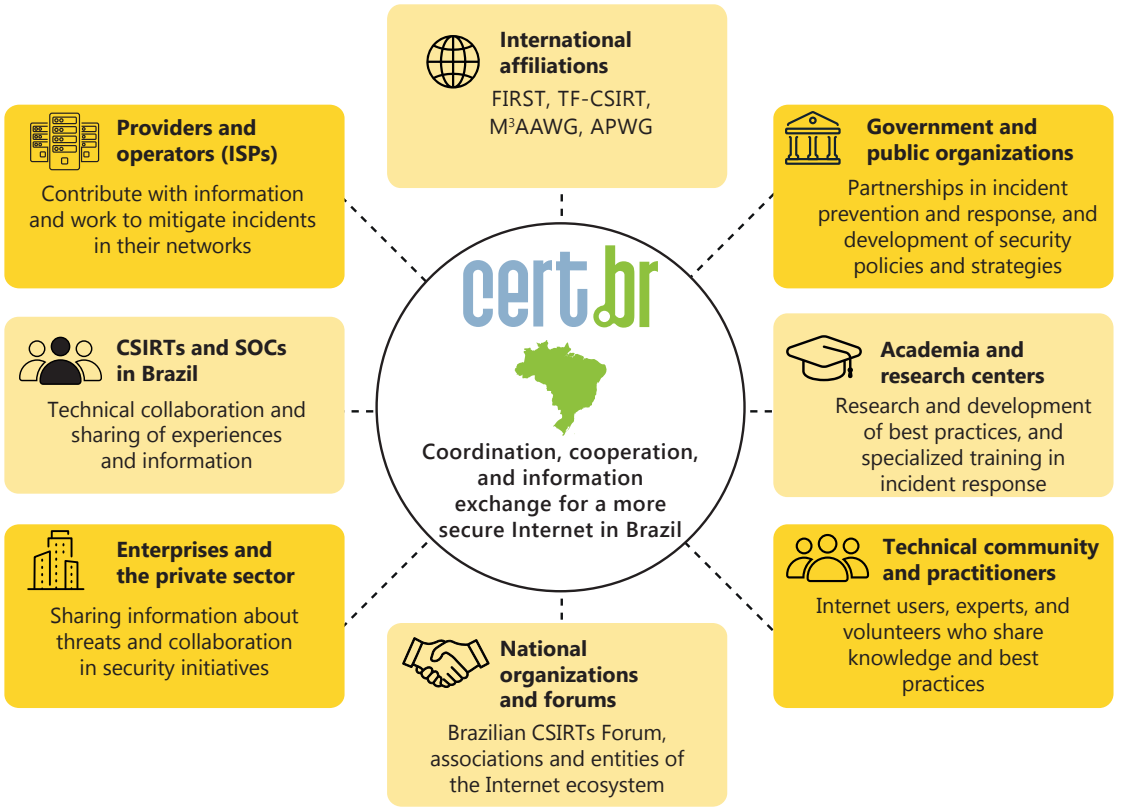
This data is not just used for sharing statistics about the profile of attacks on the CERT.br statistics portal. Potentially affected networks are regularly notified by CERT.br with instructions on how to test for problems and how to recover. Additionally, CERT.br shares more detailed information with industry communities through the MISP platform,[14] a platform for sharing threat data widely used among CSIRTs. To foster the growth of this sharing and ensure that it increasingly benefits the country, CERT.br annually promotes a free workshop (MISP Workshop), held in conjunction with the Brazilian CSIRTs Forum.[15]

International impact

CERT.br has strong integration with the national and international CSIRT communities, which leads to the formation of trust relationships, the establishment of a network of contacts with key stakeholders, and recognition of the competence and quality of its work. Figure 4 illustrates the collaboration networks in which CERT.br participates.

[11] Find out more: https://www.team-cymru.com/
[12] Find out more: https://www.shadowserver.org/
[13] Find out more: https://www.spamhaus.org/
[14] Find out more: https://www.misp-project.org/
[15] Find out more: https://forum.cert.br/

Figure 4 – CERT.br, INSTITUTIONAL PLAYERS, AND COLLABORATION NETWORKS



Source: Prepared by the author.

Over the years, numerous professionals have contributed to (and in many cases led) the development of best practices, standards, and frameworks that are now global benchmarks. Examples of this impact include:

- *Computer Security Incident Response Team (CSIRT) services framework* (FIRST, 2019);
- *Team Types Within the Context of Services Frameworks* (FIRST, 2025);
- *CSIRT Roles and Competences (Addendum)* (FIRST, 2022);
- *LACNOG-M³AAWG Joint Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition LAC-BCOP-1* (Latin American and Caribbean Network Operators Group [LACNOG] & Messaging, Malware and Mobile Anti-Abuse Working Group [M³AAWG], 2019).

CERT.br is also an active collaborator with FIRST, and its professionals have participated in various ways over time, most notably holding a seat on the Board of Directors (2012/2013) and serving as chair of the annual conference (2020).[16] Currently, its professionals participate in the Membership Committee, coordinate the "capture-the-flag" event at the annual conference, and are involved in various special interest groups (SIG) within the organization.

[16] Find out more: https://www.first.org/about/organization/directors

Over the course of nearly three decades, CERT.br has established itself as one of the main technical pillars of Internet security in Brazil, playing a strategic role in incident coordination, disseminating best practices, and strengthening the country's digital resilience.

Final considerations

The trajectory of CERT.br mirrors the evolution of the Internet in Brazil and highlights the importance of specialized technical structures to strengthen the security and resilience of the Brazilian digital ecosystem. CERT.br has established itself as a national focal point for incident coordination, fostering cooperation networks between providers, companies, academia, government, and technical communities, always based on a collaborative and multi-sectoral approach, aligned with the multi-sectoral nature of NIC.br and CGI.br.

Throughout its history, CERT.br has contributed not only to incident response but also to strengthening national cybersecurity capabilities through awareness-raising activities, knowledge production, training of specialized professionals, and dissemination of best practices. Simultaneously, initiatives to collect and share threat data have broadened situational awareness of the country's security landscape and strengthened the prevention and response capabilities of organizations connected to the Internet.

In a context marked by the increasing complexity of digital threats, the expansion of the adoption of emerging technologies such as the Internet of Things (IoTs), and the advancement of Artificial Intelligence (AI), the experience of CERT.br demonstrates that trust, cooperation, and continuous training are essential elements for the sustainability of digital transformation. Its international recognition and contribution to global frameworks and best practices reinforce Brazil's strategic role in international discussions on cybersecurity.

Over the course of nearly three decades, CERT.br has established itself as one of the main technical pillars of Internet security in Brazil, playing a strategic role in incident coordination, disseminating best practices, and strengthening the country's digital resilience. Its collaborative efforts and continuous work have contributed to making the Internet infrastructure in Brazil progressively more secure, reliable, and resilient, expanding the national capacity for prevention, detection, and response to cyber threats.

Furthermore, CERT.br has become an international benchmark by promoting cooperation between national and global players, supporting the development of technical capabilities, and strengthening trust in the Brazilian digital ecosystem. In a scenario of increasing complexity of digital threats, preserving and strengthening the multi-stakeholder governance model represented by CGI.br|NIC.br, which is based on technical coordination, cooperation, community participation, and consensus building, is fundamental to guaranteeing an increasingly secure, stable, and reliable Internet for the future.

References

Brazilian National Computer Emergency Response Team. (n.d.). *Distributed Honeypots Project.* HoneyTARG. https://honeytarg.cert.br/honeypots/index-po.html

Brazilian National Computer Emergency Response Team. (2025). *Ransomware: Best Practices for Protection, Detection, and Response*. https://cert.br/docs/ransomware/en/

Forum of Incident Response and Security Teams. (2019). *Computer Security Incident Response Team (CSIRT) Services Framework*. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Forum of Incident Response and Security Teams. (2022). *CSIRT Roles and Competences (Addendum). https://www.first.org/standards/frameworks/csirts/csirt_roles_competences*

Forum of Incident Response and Security Teams. (2025). *Team types within the context of services frameworks*. https://www.first.org/standards/frameworks/csirts/team-type_1.2

Gomide, A. C., Pinheiro, C. A. C., & Vazquez, P. A. M. (1996). Rumo a criação de uma coordenadoria de segurança de redes na Internet Brasil. CERT.br. https://www.cert.br/sobre/estudo-cgibr-1996.html

Latin American and Caribbean Network Operators Group, & Messaging, Malware and Mobile Anti-Abuse Working Group. (2019). *LACNOG-M^{3}AAWG Joint best current operational practices on minimum security requirements for customer premises equipment (CPE) Acquisition LAC-BCOP-1*. https://www.m3aawg.org/sites/default/files/doc_files/lac-bcop-1-m3aawg-v1.pdf

Interview I

Internet security in Brazil: A trajectory of cooperation

Photo: Ricardo Matsukawa

Gilberto Zorello
Project coordinator at NIC.br

In this interview, Gilberto Zorello, project coordinator at the Brazilian Network Information Center (NIC.br), reflects on the creation and evolution of the Program for a More Secure Internet (Programa por uma Internet mais Segura), highlighting its main milestones, strategies, and best practices for promoting digital security in Brazil. He also addresses the role of collaboration between different actors in the ecosystem in strengthening trust and advancing Internet security in the country.

Internet Sectoral Overview (I.S.O.)_ To begin, could you introduce us to the Program for a More Secure Internet? In what context was this program created, when did it begin, and what were the main objectives that guided its design?

Gilberto Zorello (G.Z.)_ In recent years, the number of Internet security incidents has grown steadily, directly or indirectly impacting the stability, performance, and reliability of services that depend on network infrastructure. Security incidents can cause significant losses, such as downtime, the need for debugging and reconfiguration of equipment, and the undue consumption of bandwidth by Distributed Denial of Service (DDoS) attacks originating from other networks and, often, from the networks themselves. The cause of these problems often lies in poorly configured equipment or equipment compromised by malicious code, which is then used in attacks against third parties.

The targets of these attacks may face service unavailability, damage to their reputation, financial and credibility losses, and difficulties in the continuity of their operations. One of the main reasons for the success of these malicious actions is the lack of attention to the security settings of the equipment used by network operators, as well as the numerous vulnerabilities present in these devices. Maintaining network functionality is essential to the operations of telecommunications operators, Internet access providers, corporations, and data service providers. Given this scenario, at the end of 2017 during the

"The [Program for a More Secure Internet] was created to support the Internet technical community in reducing DDoS attacks originating from Brazilian networks, and decreasing prefix hijacking, route leaks, and spoofing of source Internet Protocol (IP) addresses."

IX Forum 11,[17] the Brazilian Internet Steering Committee (CGI.br) and NIC.br launched the Program for a More Secure Internet, with the support of the National Union of Telephone and Mobile, Cellular and Personal Service Companies (Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel, Celular e Pessoal [Conexis Brasil Digital][18]), the Internet Brazilian Association (Abranet) and the Brazilian Association of Internet and Telecommunication Service Providers (Abrint), and in partnership with the Internet Society (an international organization dedicated to the development of standards and the promotion of educational initiatives and public policies related to the Internet). The program was created to support the Internet technical community in reducing DDoS attacks originating from Brazilian networks, and decreasing prefix hijacking, route leaks, and spoofing of source Internet Protocol (IP) addresses. Furthermore, it seeks to reduce vulnerabilities and misconfigurations in network elements, and to bring together the teams responsible for Internet security and stability, strengthening this security culture among operators.

To achieve these goals, NIC.br provides the technical community with a series of practical actions (lectures, courses, training sessions, and technical meetings) that help operators and providers improve their security processes and enhance the configuration of their network. The program also maintains constant interaction with provider and operator associations that support its initiatives, expanding the reach of best practices and promoting a collaborative environment among the various actors in the Internet ecosystem.

Through these actions, the Program for a More Secure Internet contributes to reducing incidents, strengthening network resilience, and promoting a more stable, reliable, and secure Internet for all.

I.S.O._ How has the program evolved since its inception, what have been the main milestones along the way, and how have they contributed to defining its current areas of focus, strategic objectives, and best practices for promoting a more secure Internet? And how are these practices disseminated and encouraged among the different audiences and actors in the ecosystem?

G.Z._ The Program for a More Secure Internet is an internal initiative of NIC.br involving several of its technical departments: the Brazilian National Computer Emergency Response Team (CERT.br), Registro.br, the Center for Study and Research on Network Technology and Operations (Ceptro.br), and IX.br (Brazil Internet Exchange). Each area performs specific actions that contribute to the success of the program:

- **CERT.br:** A national-level Computer Security Incident Response Team (CSIRT) of last resort that defines the best security practice guidelines that the program should follow. CERT.br is also responsible for notifying about services exposed on networks that can be abused in reflection and amplification attacks, and for publishing various security statistics.

[17] Find out more: https://forum.ix.br/2017/
[18] Previously called SindiTelebrasil.

- **Registro.br:** Responsible for the registration and maintenance of .br domain names, and also for allocation IPv4 and IPv6 addresses and Autonomous System Numbers (ASNs) in the country. Furthermore, it hosts the program coordination and has an engineering and operational group that develops and maintains a tool for verifying the adoption of security best practices, operating the Domain Name System (DNS) infrastructure, the DNS Security Extensions (DNSSECs), and the Resource Public Key Infrastructure (RPKI) repository, which are important for the security of name resolution and Internet routing, among other activities;
- **Ceptro.br:** Responsible for initiatives and projects that support or improve the Internet infrastructure in Brazil, contributing to its development. The center's initiatives include providing tools to measure Internet quality in the country, disseminating best operational and network security practices through courses, training, lectures, and in-person and online events, and promoting IPv6.br among network operators and carrying out projects such as the distribution of the official Brazilian time, which is fundamental to network security;
- **IX.br:** Responsible for the Internet Exchange Points (IXPs) maintained by NIC.br, implements best security practices in its 39 interconnection points spread across the country.

In this context, the program develops its actions through notifications of exposed services performed, by including security content in face-to-face training and workshops in different regions of the country, by including security content in online training, workshops, and podcasts, by holding technical meetings with network operators on the best security practices that should be applied to their networks and, more recently, by a competition or challenge for the implementation of best security practices by network operators.

The program coordination team produces statistics to monitor the actions. Initially, there were over 750,000 exposed services in the country, and in April 2026, even considering the network's growth during that period and attacks that began to exploit new services, the number of exposed services was below 116,000, with a downward trend, a result of notification, training, and clarification actions regarding the importance of adopting best security practices across networks.

The Program for a More Secure Internet began with actions targeting large operators and, subsequently, medium and small Internet providers, encouraging them to adopt configurations that prevent services from being exposed on their networks. Subsequently, the program began to disseminate the best security practices recommended by the Mutually Agreed Norms for Routing Security (MANRS), an initiative operated by the Global Cyber Alliance (GCA) and aimed at reducing routing security problems in networks. These practices include implementing filtering for incorrect network advertisements and false origin addresses, publicizing contact points that respond to notifications and take necessary actions promptly, and disclosing network routing policies in accessible and secure databases that assist in filtering network advertisements. Today, more than 320 networks in the country participate in MANRS, and many others have implemented the recommended actions.

"Initially, there were over 750,000 exposed services in the country, and in April 2026, even considering the network's growth during that period and attacks that began to exploit new services, the number of exposed services was below 116,000, with a downward trend, a result of notification, training, and clarification actions regarding the importance of adopting best security practices across networks."

"At the end of 2021, the Test the Standards (Teste os Padrões [TOP]) tool was developed to verify whether the end-user's connection follows security best practices and whether the accessed website or email service follows the most important security best practices for its service."

At the end of 2021, the Test the Standards (Teste os Padrões [TOP]) tool was developed to verify whether the end-user's connection follows security best practices and whether the accessed website or e-mail service follows the most important security best practices for its service.
In 2023, the program incorporated dissemination of best security practices for domain name resolution proposed by the Knowledge-Sharing and Instantiating Norms for DNS and Naming Security (KINDNS), an initiative of the Internet Corporation for Assigned Names and Numbers (ICANN), which are fundamental to the security of users' Internet browsing.
Thus, various best security practices have been defined over time by the technical areas of NIC.br in response to the increasing number of attacks and security incidents, and the technologies developed to protect networks.

I.S.O._ We know that collaboration is a central element in digital security initiatives. How does it materialize in the program? How does this collaborative arrangement contribute to strengthening trust between stakeholders and driving progress in Internet security in Brazil?

G.Z._ The collaboration of the Program for a More Secure Internet is realized through cross-cutting action within NIC.br, bringing together its technical areas and support teams—such as Development system and Communication teams—in integrated and complementary actions. This internal coordination ensures coherence, agility, and consistency in the implementation of security initiatives.
The program also relies on collaboration with leading Internet provider associations, including Abranet, Abrint, the National Association of Companies for Internet Solutions and Telecommunications (RedeTelesul), the Association of Internet Service and Information Providers (Associação dos Provedores de Serviços e Informações da Internet [InternetSul]), the Brazilian Association of Internet Providers and Multimedia Data Communication Operators (Abramulti), the Santa Catarina Association of Internet Providers (Associação Catarinense de Provedores de Internet [Apronet]), and the Brazilian Association of Competitive Telecommunications Service Providers (Telcomp), expanding its reach and strengthening dialogue with network operators throughout the country.
Furthermore, institutions such as the National Education and Research Network (RNP) and the Brazilian Internet technical community actively contribute, bringing expertise, legitimacy, and reach to the initiatives developed. This support is essential for disseminating and implementing best security practices, promoting trust among stakeholders, and driving concrete progress in Internet security in Brazil.

Interview II

Cooperation and trust in cybersecurity incident management

Photo: Caleff

Olivier Caleff
Chair of FIRST, CSIRT and cyber-resilience expert at CSIRT.FR, and SIM3 auditor at Open CSIRT Foundation

In this interview, Olivier Caleff, chair of the FIRST,[19] CSIRT manager at the CSIRT.FR,[20] and certified SIM3 auditor at Open CSIRT Foundation,[21] reflects on the challenges of cybersecurity incident management in the context of technological transformation, highlighting the importance of cooperation among Computer Security Incident Response Teams (CSIRTs) and Computer Emergency Response Teams (CERTs), trust-building within cybersecurity communities, and the role of the Security Incident Management Maturity Model (SIM3) in strengthening incident response capabilities.

Internet Sectoral Overview (I.S.O.)_ In your view, what are the main challenges posed to cybersecurity incident management in a technological transformation context? To what extent have these challenges changed over the last decades?

Olivier Caleff (O.C.)_ First and foremost, the main challenge is the mismatch between the pace of change and the organization's ability to adapt its security and incident response capabilities. New technologies, architectures, and business processes are often deployed faster than governance, incident response plans, and procedures can evolve.

A second major challenge is visibility and control. Effective incident management requires a clear understanding of the environment being protected: assets, which soon translates into "attack surface," dependencies, business processes, and data flows. During wide-scale transformations, inventories, documentation, and architectural mappings are often incomplete or outdated. As a result, the attack surface expands, while defenders may lose visibility over critical assets and interconnections.

Transformation also increases technical complexity. Cloud services, Software as a Service (SaaS) platforms, AI-enabled systems, containerized environments, and third-party integration introduce new technologies, components, and attack vectors. CSIRTs—alongside cybersecurity or cyberdefense teams—may not yet have sufficient experience with these technologies. As a consequence, qualification, risk assessment, and security validation processes often struggle to keep pace.

[19] Find out more: https://first.org/
[20] Find out more: https://csirt.fr/
[21] Find out more: https://opencsirt.org/

"The challenges faced by cybersecurity incident management teams have not fundamentally changed in nature: Organizations still need visibility, detection, response, communication, and recovery capabilities. What have dramatically changed over the last decades are the scale, the complexity, and the business criticality underlying these challenges."

Another significant challenge is organizational. Incident response depends on strong collaboration between technical, security, operational, and business teams. However, cybersecurity is sometimes perceived as a constraint rather than an enabler, which can hinder cooperation and delay the establishment of effective communication and escalation channels. At the same time, roles, responsibilities, and decision-making authority are not always clearly defined during transformation programs, creating uncertainty when incidents occur.

Human factors should not be underestimated. Security Operations Centers (SOCs) and CSIRTs frequently face alert fatigue, increasing workloads, and skills shortages. When training and knowledge transfer lag behind technological change, teams may feel overwhelmed and less capable of responding effectively to incidents involving unfamiliar technologies.

Finally, the threat landscape is evolving alongside technological transformation. Adversaries are increasingly leveraging automation and Artificial Intelligence (AI) to accelerate reconnaissance, phishing campaigns, vulnerability discovery, and attack execution. This raises the issues of speed and the sophistication of threats while defenders are already coping with a rapidly changing environment.

To address these challenges, organizations should invest in strong asset management, Configuration Management Database (CMDB), Software Bill of Materials (SBOM), continuous training, stakeholder engagement, and governance frameworks that integrate cybersecurity into transformation programs from the outset. While there is no single solution, many of these areas are covered by maturity models such as Security Incident Management Maturity Model (SIM3) for the OpenCSIRT Foundation (OCF).

The challenges faced by cybersecurity incident management teams have not fundamentally changed in nature: Organizations still need visibility, detection, response, communication, and recovery capabilities. What have dramatically changed over the last decades are the scale, the complexity, and the business criticality underlying these challenges.

Let's now highlight five major evolutions: architecture, scale, complexity, speed, and business impact.

The first is architecture, from centralized to distributed ecosystems. When I started my career forty years ago, most assets were concentrated in centralized environments, such as mainframes and private networks. Incident response focused on a relatively well-defined perimeter and a very limited number of critical systems. Over time, organizations adopted distributed computing, client-server architectures, the Internet, cloud services, SaaS platforms, mobile devices, remote work, and interconnected supply chains. As a result, incident responders no longer investigate a contained environment but instead an ecosystem spanning multiple providers, technologies, and administrative domains. One consequence is that visibility has become a major challenge. Critical logs, telemetry, and forensic evidence may be owned by third parties—think cloud—creating dependencies that did not exist in earlier generations of information technology (IT).

The second is scale, from hundreds to millions of events. The sheer number of assets, users, applications, Application Programming Interface (API), containers, cloud services, and connected devices has increased exponentially. As attack surfaces expanded, the volume of security events exploded as well: What could once be investigated manually—remember Unix "grep," "awk," and the likes—now requires centralized logging, computing power for correlation platforms, Security Information and Event Management (SIEM) platforms, threat intelligence, and analytics. Thus, incident management has evolved from analyzing isolated events to operating at a large scale.

The third is complexity, from known systems to interconnected dependencies. Today, environments contain countless layers of abstraction and dependencies. Organizations increasingly rely on software components, open-source libraries, cloud-native services, third-party API, and supply chains that are not always fully understood. Identity has become particularly critical. While network security was once the primary focus, modern incident investigations frequently revolve around identity systems, privileged access, session tokens, federated authentication, and cloud permissions. Identity and Access Management (IAM) is now among the most valuable sources of evidence during an investigation, so have been logging and DNS for decades. This complexity makes root-cause analysis, containment, and recovery significantly more difficult than in previous decades.

The fourth is speed, from days and weeks to minutes and hours. Perhaps the most dramatic change is the speed at which incidents unfold. Threat actors increasingly leverage automation, industrialized attack frameworks, and AI-assisted techniques. Vulnerabilities are weaponized rapidly after disclosure, and compromise-to-exfiltration timelines continue to shrink. Cases where attackers move from initial compromise to data theft within hours or even less are no longer exceptional. Usual manual response processes are often too slow to cope with such a fast pace. Incident management increasingly tends to depend on real-time detection, automation and orchestration, and fast decision-making.

Finally, the fifth is business impact, from technical disruption to enterprise risk. Historically, cybersecurity incidents were often viewed as technical or operational problems. Today, they directly affect revenue, operations, regulatory compliance, legal exposure, reputation, and customer trust for the long term. The convergence of IT and operational technology, the growth of digital business models, and increasingly stringent regulations have elevated cyberresilience to a board-level concern. Incident management now involves executives, legal teams, communications departments, regulators, insurers, and business leaders in addition to technical teams.

Over the last decades, I have seen cybersecurity incident management evolving from a domain that was mostly focused on protecting IT systems with a purely technical approach into a strategic business capability concerned with organizational resilience.

The core objective remains the same: prevent, detect, contain, eradicate, and recover. Unfortunately, the environment has become more distributed, larger, more complex, faster, and directly impacting business. As a result, success is no longer measured solely by preventing incidents but by how quickly and effectively an organization can respond, recover, and maintain business continuity. Recovery and resilience have become just as important as prevention. CSIRTs definitely have a role there too by participating in such activities.

"Historically, cybersecurity incidents were often viewed as technical or operational problems. Today, they directly affect revenue, operations, regulatory compliance, legal exposure, reputation, and customer trust for the long term."

"The CSIRT-CERT cooperation model is a collaborative cybersecurity framework built on trust, information sharing, and coordinated incident response. While CSIRTs and CERTs are the primary actors, they operate alongside complementary entities (...). The foundation of the model is trust."

I.S.O._ How does the CSIRT-CERT cooperation model work? Additionally, how can the existing cooperation mechanisms improve the prevention and management of cyberincidents?

O.C._ The CSIRT-CERT cooperation model is a collaborative cybersecurity framework built on trust, information sharing, and coordinated incident response. While CSIRTs and CERTs are the primary actors, they operate alongside complementary entities such as Product Security Incident Response Teams (PSIRTs), Information Sharing and Analysis Centers (ISACs), SOCs, and Cyber Threat Intelligence (CTI) teams.

The foundation of the model is trust. Security teams organize themselves into communities based on common interests such as geography, language, sector, or mission. Some communities are open to qualified members, while others are restricted to governmental, national, or accredited teams. These communities foster trusted relationships through conferences, working groups, training sessions, exercises, and day-to-day collaboration.

At the global level, organizations such as FIRST, founded in 1990, provide a framework for international cooperation and bring together incident response teams from over 110 countries as of today. Regional organizations, such as TF-CSIRT[22] in Europe, AfricaCERT,[23] and TrustBroker Africa,[24] strengthen cooperation within their respective regions and many countries have also established national CSIRT associations, such as InterCERT-France,[25] the Brazilian CSIRTs Forum[26] in Brazil, and the Nippon CSIRT Association[27] (NCA) in Japan.

The operational aspect of cooperation relies on agreed governance rules, common terminology, and standardized sharing mechanisms. Information can be exchanged manually or through automated platforms such as the MISP.[28] To ensure that shared information is handled appropriately, communities use established standards and frameworks, including the following:

- the Traffic Light Protocol (TLP)[29] and Permissible Actions Protocol (PAP)[30] for information handling and dissemination;
- the Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII) for structured and automated threat intelligence exchange; and
- the Common Vulnerability Scoring System (CVSS)[31] and Exploit Prediction Scoring System (EPSS)[32] for vulnerability assessment and prioritization.

[22] Find out more: https://tf-csirt.org/
[23] Find out more: https://www.africacert.org/
[24] Find out more: https://www.trustbroker.africa/
[25] Find out more: https://intercert-france.fr/
[26] Find out more: https://forum.cert.br
[27] Find out more: https://www.nca.gr.jp/en/index.html
[28] Find out more: https://www.misp-project.org/
[29] Find out more: https://www.first.org/tlp/
[30] Find out more: https://www.cert.ssi.gouv.fr/csirt/sharing-policy/
[31] Find out more: https://www.first.org/cvss/v4.0/
[32] Find out more: https://www.first.org/epss/

These mechanisms enable teams to rapidly share indicators and intelligence, including Indicators of Future Attack (IOFA), Indicators of Attack (IOA), Indicators of Behavior (IOB), Indicators of Compromise (IOC), and adversary Tactics, Techniques, and Procedures (TTPs).

When incidents cross organizational or national boundaries, trusted relationships established through these communities enable direct communication and coordinated response activities. For major cyberincidents, large-scale campaigns, or critical vulnerabilities, multiple teams may form ad hoc task forces to coordinate analysis, mitigation, disclosure, and communication efforts.

Let me conclude by insisting on that the CSIRT-CERT cooperation model is global and based on trust, standards, and collaboration, making it a TSC triad. It then facilitates the secure exchange of actionable information,[33] improves collective situational awareness, and enables coordinated responses to cybersecurity threats and incidents.

Existing cooperation mechanisms significantly improve both the prevention and the management of cyberincidents by enabling organizations to anticipate threats, coordinate responses, and continuously strengthen collective resilience.

The first benefit is anticipation. Effective prevention depends on having timely visibility into emerging threats. Through trusted cooperation networks, it is possible for CSIRTs, CERTs, ISACs, CTI teams, and other security stakeholders to rapidly exchange threat intelligence, vulnerability information, indicators, adversary TTPs, and lessons learned from incidents. Early awareness allows organizations to raise their alert level, strengthen monitoring, fine-tune detection capabilities, deploy mitigation strategies, patch vulnerable systems, and prepare response plans before an attack materializes. In many cases, it also enables proactive activities such as threat hunting and targeted risk assessments.

Cooperation also improves situational awareness. Individual organizations typically observe only a small portion of the threat landscape, whereas a community of trusted partners can collectively identify larger attack campaigns, emerging trends, and systemic risks. By correlating observations from multiple sectors, regions, or countries, communities can detect threats earlier and understand their potential impact more accurately.

Furthermore, cooperation mechanisms accelerate response and recovery. Trusted communication channels allow teams to quickly exchange technical findings, indicators of compromise, remediation measures, and operational guidance. This reduces duplication of effort, improves decision-making, and enables coordinated actions across affected organizations. During major cybercrises or large-scale vulnerabilities, communities can establish dedicated task forces to synchronize analysis, mitigation, disclosure, and communication activities.

"Effective prevention depends on having timely visibility into emerging threats. Through trusted cooperation networks, it is possible for CSIRTs, CERTs, ISACs, CTI teams, and other security stakeholders to rapidly exchange threat intelligence, vulnerability information, indicators, adversary TTPs, and lessons learned from incidents."

[33] See ENISA's 2015 "Actionable Information for Security Incident Response", available at: https://www.enisa.europa.eu/publications/actionable-information-for-security.

"While not every incident requires judicial involvement, collaboration between incident response teams and law enforcement can help better understand the context of some types of malicious activities, support investigations, facilitate evidence preservation, and, last but not least, contribute to the disruption of criminal infrastructures."

Cooperation with law enforcement agencies is another important aspect. While not every incident requires judicial involvement, collaboration between incident response teams and law enforcement can help better understand the context of some types of malicious activities, support investigations, facilitate evidence preservation, and, last but not least, contribute to the disruption of criminal infrastructures. Strong relationships established before an incident or a crisis occurs greatly improve the effectiveness of such collaboration; this is the point of participating in events and conferences organized by the community.

Preparedness is also strengthened through joint exercises, cyber-ranges, tabletop simulations, and crisis management drills. These activities allow organizations to test procedures, identify weaknesses, validate communication channels, and improve coordination among stakeholders. Equally important, they create personal relationships and trust between practitioners, which often prove invaluable during real incidents.

Finally, cooperation mechanisms contribute to long-term community and capacity building. Mature CSIRT communities invest significant effort in sharing knowledge, publishing best practices, mentoring new teams, and developing training programs. This helps raise the overall maturity of the ecosystem and increases the number of capable defenders available to respond to future threats. Initiatives such as FIRST's Community and Capacity Building Program (CCB),[34] CORE Program,[35] and Fellowship Program,[36] as well as InterCERT-France's incubator program,[37] demonstrate how investing in people and organizations today strengthens the collective resilience of the cybersecurity community in the future.

Keep in mind these five cooperation mechanisms: anticipation (again), situational awareness, preparedness, coordinated response, and community capacity. For four decades, incident management fundamentals relied on collective efforts, in the belief that defenders achieve greater effectiveness when they collaborate and share. Guess what? Threat actors also do so, for at least as long as us. They increasingly collaborate and exchange knowledge among themselves too.

You do not measure cooperation by volume of information shared, but by the ability to transform shared information into actionable measures and coordinated operational decisions. Quality, therefore, is better than quantity.

[34] Find out more: https://www.first.org/global/ccb-initiatives/
[35] Find out more: https://www.first.org/global/core/
[36] Find out more: https://www.first.org/global/fellowship/
[37] Find out more: https://www.intercert-france.fr/incubateur-intercert-france/

I.S.O._ What are the minimum shared values of global and regional CSIRT communities, and what role does the community play in fostering trust among participants?

O.C._ Global and regional CSIRT communities are generally built around three fundamental values: trust, cooperation, and secure information sharing.
Trust is the foundation of the entire ecosystem. Members are expected to handle shared information responsibly, respect confidentiality requirements, and comply with the community's rules of engagement. Breaches of trust are taken seriously and can ultimately lead to exclusion from the community. Beyond confidentiality, members are expected to demonstrate professionalism, integrity, and ethical conduct in their incident response activities, operational practices, and communications.
Cooperation is the mechanism through which the community delivers value. It encompasses the sharing of knowledge, expertise, threat intelligence, lessons learned, best practices, and technical capabilities. Effective cooperation depends on timely communication, responsiveness to requests for assistance, and the ability to coordinate activities across organizational and national boundaries. In this sense, accuracy, reliability, and relevance of the information exchanged are critical; ultimately, the goal is to provide actionable information that enables informed decision-making and effective response.
Secure information sharing underpins both trust and cooperation. Whether information is exchanged verbally, through written communications, or via automated platforms such as the MISP, members are expected to follow agreed governance rules and information-handling procedures. While technologies, platforms, and communication channels continue to evolve, the underlying principles remain consistent: Ensuring that the right information reaches the right people, at the right time, with the appropriate level of protection and dissemination controls.
CSIRT communities play a central role in establishing, strengthening, and maintaining trust among their members through a combination of governance, operational practices, and interpersonal relationships.
At the governance level, communities define codes of conduct, membership requirements, operational standards, and information-sharing frameworks. They establish common rules for handling sensitive information, typically based on protocols such as TLP and PAP in some cases. These shared rules create a predictable and trusted environment in which members can exchange information with confidence.

"Global and regional CSIRT communities are generally built around three fundamental values: trust, cooperation, and secure information sharing. Trust is the foundation of the entire ecosystem."

"Valuable time is not lost establishing legitimacy, negotiating communication paths, or validating relationships; those foundations have already been built through community engagement. (...) Valuable time is not lost establishing legitimacy, negotiating communication paths, or validating relationships; those foundations have already been built through community engagement."

In addition, the communities also invest heavily in relationship building. Conferences, workshops, working groups, training sessions, capture-the-flag (CTF) events, tabletop exercises, and cybercrisis simulations provide valuable opportunities for participants to interact regularly and develop both professional and personal relationships. These interactions help transform organizational trust into human trust, which often becomes a decisive factor during major incidents.

Some communities go even further by implementing peer-review, accreditation, certification, or mentoring mechanisms. These initiatives allow teams to better understand each other's capabilities, operating models, and constraints, while also increasing credibility and confidence within the community. Trust grows more naturally when organizations have worked together, reviewed each other's practices, and demonstrated their commitment to common standards.

A core responsibility of any CSIRT community is to facilitate coordinated incident response and crisis management. When a significant incident occurs, the existence of preestablished trust and communication channels allows teams to cooperate immediately and effectively. Valuable time is not lost establishing legitimacy, negotiating communication paths, or validating relationships; those foundations have already been built through community engagement.

Finally, one of the most impactful contributions of CSIRT communities is capacity building through mentorship, fellowship, and knowledge-sharing programs. Experienced teams and practitioners support newer or developing teams by sharing expertise, best practices, lessons learned, and operational experience. This accelerates capability development, helps avoid common pitfalls, and strengthens the overall resilience of the ecosystem.

Having participated in and supported such initiatives for two decades, both in national and international contexts, I consider mentorship one of the most valuable aspects of our community. It benefits everyone involved: Mentees gain knowledge, confidence, and support, while the mentor broadens their views, refines their own practices, and continues learning through such experience.

I.S.O._ How would you describe the SIM3, and what are the main challenges currently identified for CSIRTs based on this model?

O.C._ SIM3 is the most widely adopted maturity assessment framework used in the international CSIRT community, used by organizations and communities such as TF-CSIRT, FIRST, and the CSIRTAmericas Network,[38] and its principles are being applied beyond CSIRTs to related operational teams such as PSIRTs, SOCs, and ISACs. It provides a structured, objective, and measurable method to assess the maturity of an incident response capability.

SIM3 can be used for self-assessment, capability development, external audits, certification programs, and the definition of improvement roadmaps. Rather than evaluating technical expertise alone, SIM3 evaluates whether a team's capabilities are properly organized, documented, formalized, managed, measured, and continuously improved.

A common misconception is that SIM3 measures how technically advanced a CSIRT is. But it is not designed to measure a team's technical strength or establish a "guruness" rating. SIM3 measures operational maturity and sustainability. A highly skilled team can still score poorly if its mandate is unclear, processes are undocumented, knowledge resides with only a few individuals, or governance mechanisms are weak. A mature team is one that can consistently deliver services regardless of staff turnover, organizational change, and that can rely on written, validated, and well understood processes and procedures.

The model evaluates 45 parameters organized into four domains:

- **Organization (O):** 11 parameters covering governance, mandate, constituency, service definition, management support, strategic positioning, etc.;
- **Human (H):** 7 parameters covering staffing, competencies, training, resilience, succession planning, team development, etc.;
- **Tools (T):** 10 parameters covering technical capabilities, infrastructure, monitoring, automation, supporting technologies, etc.;
- **Processes (P):** 17 parameters covering operational workflows, incident handling procedures, escalation mechanisms, coordination, communication, quality assurance, continuous improvement, etc.

As a certified SIM3 auditor conducting assessments and audit for almost a decade, I have found that the model's greatest value is not certification itself but its ability to guide improvement. SIM3 provides a common language for discussing maturity, identifying gaps, prioritizing investments, and building realistic roadmaps. It is equally valuable when designing a new CSIRT from the ground up and when helping an established team implement a continuous improvement or quality management approach. The model also facilitates the creation of measurable objectives, indicators, and Key Performance Indicators (KPIs) that can be tracked over time.

"SIM3 measures operational maturity and sustainability. A highly skilled team can still score poorly if its mandate is unclear, processes are undocumented, knowledge resides with only a few individuals, or governance mechanisms are weak."

[38] Find out more: https://csirtamericas.org/

"From an organizational perspective, the most common challenge remains the lack of a clearly defined mandate and governance framework. Many teams still operate with ambiguous authority, insufficient top-management sponsorship, unclear constituency definitions, or overlapping responsibilities with other security functions."

One of SIM3's strengths is its balance between these four dimensions. Experience shows that weaknesses in one area often limit maturity in the others. Let me offer three quick examples:

- highly skilled analysts struggle to operate effectively without "O" clear governance, mandate, and organizational support;
- initial phases of incident handling are slow or inefficient if the constituents' IT or operational technology (OT) environment cartography is poor and relationships with stakeholders are not well established ("O," "T," and "P");
- investing in advanced tools will not deliver expected benefits if "P" is not defined, as technology is often easier to acquire than sustainable operational maturity.

Several SIM3 baselines have been developed to address specific operational contexts. In addition to the original certification baseline started by TF-CSIRT, tailored profiles have been defined for national and governmental CSIRTs within ENISA's CSIRTs Network,[39] for FIRST, and more recently within the CSIRTAmericas Network. These baselines help ensure that maturity expectations are aligned with the missions and responsibilities of the teams being assessed.

Regarding the main challenges identified through SIM3 assessments, the specific findings vary between organizations, but several recurring themes emerge.

- From an organizational perspective, the most common challenge remains the lack of a clearly defined mandate and governance framework. Many teams still operate with ambiguous authority, insufficient top-management sponsorship, unclear constituency definitions, or overlapping responsibilities with other security functions. These issues are major obstacles during incident coordination and crisis situations.
- From a human perspective, many teams remain highly dependent on a small number of key experts. This concentration of knowledge creates operational risks, limits scalability, and increases stress, and may lead to burnout. At the same time, fast technological evolution, including cloud-native environments, AI-related technologies, industrial systems, and increasingly sophisticated threat actors, continues to create skills gaps that are difficult to close.
- From a tooling perspective, organizations frequently struggle with visibility and integration. Modern infrastructures are increasingly distributed across on-premises, cloud, SaaS, and third-party environments, making comprehensive monitoring difficult. In addition, many teams still rely on fragmented toolsets that require significant manual processing despite advances in orchestration and automation.
- From a process perspective, recurring weaknesses include outdated escalation procedures, incomplete contact directories, insufficient coordination with external stakeholders, limited coverage of supply-chain and third-party incidents, and lessons-learned activities that are inconsistently performed. Many organizations also struggle to maintain playbooks and runbooks at the same pace as operational reality, resulting in procedures that no longer accurately reflect how incidents are handled.

[39] Find out more: https://csirtsnetwork.eu/

Across all four domains, two major challenges appear consistently. The first is the gap between documented processes and actual operational practices. The second is maintaining continuous improvement over time. Some teams successfully establish processes and documentation during their initial development phase but struggle to keep them updated as their environment, technologies, and mission evolve.

SIM3 is not merely an assessment or certification framework with "compliance" as the sole objective. It is a management and improvement tool that helps CSIRTs build sustainable operational capabilities.

Challenges most frequently identified through SIM3 assessments are rarely technical in nature; they are usually global and relate to governance, people, process discipline, knowledge management, and the ability to adapt continuously to an evolving threat landscape.

Let me conclude that SIM3 can be used as an eye-opener highlighting issues, and a building or improvement support tool, enabling maturity improvement. SIM3 is much more than yet another "pass or fail" certification: It can support your growth and your team ability to adapt to technical transformation.

"Let me conclude that SIM3 can be used as an eye-opener highlighting issues, and a building or improvement support tool, enabling maturity improvement. SIM3 is much more than yet another "pass or fail" certification: It can support your growth and your team ability to adapt to technical transformation."

Domain Report

Domain registration dynamics in Brazil and around the world

The Regional Center for Studies on the Development of the Information Society (Cetic.br), department of the Brazilian Network Information Center (NIC.br), carries out monthly monitoring of the number of country code top-level domains (ccTLD) registered in countries that are part of the Organisation for Economic Co-operation and Development (OECD) and the G20.[40] Considering members from both blocs, the 20 nations with the highest activity sum more than 98.40 million registrations. In May 2026, domains registered under .de (Germany) reached 17.96 million, followed by China (.cn), United Kingdom (.uk), and Russia (.ru), with 12.12 million, 8.98 million, and 6.11 million registrations, respectively. Brazil had 5.75 million registrations under .br, occupying 6th place on the list, as shown in Table 1.[41]

[40] Group composed by the 19 largest economies in the world and the European Union. More information available at: https://g20.org/

[41] The table presents the number of ccTLD domains according to the indicated sources. The figures correspond to the record published by each country, considering members from the OECD and G20. For countries that do not provide official statistics supplied by the domain name registration authority, the figures were obtained from: https://research.domaintools.com/statistics/tld-counts. It is important to note that there are variations among the date of reference, although the most up-to-date data for each country is compiled. The comparative analysis for domain name performance should also consider the different management models for ccTLD registration. In addition, when observing rankings, it is important to consider the diversity of existing business models.

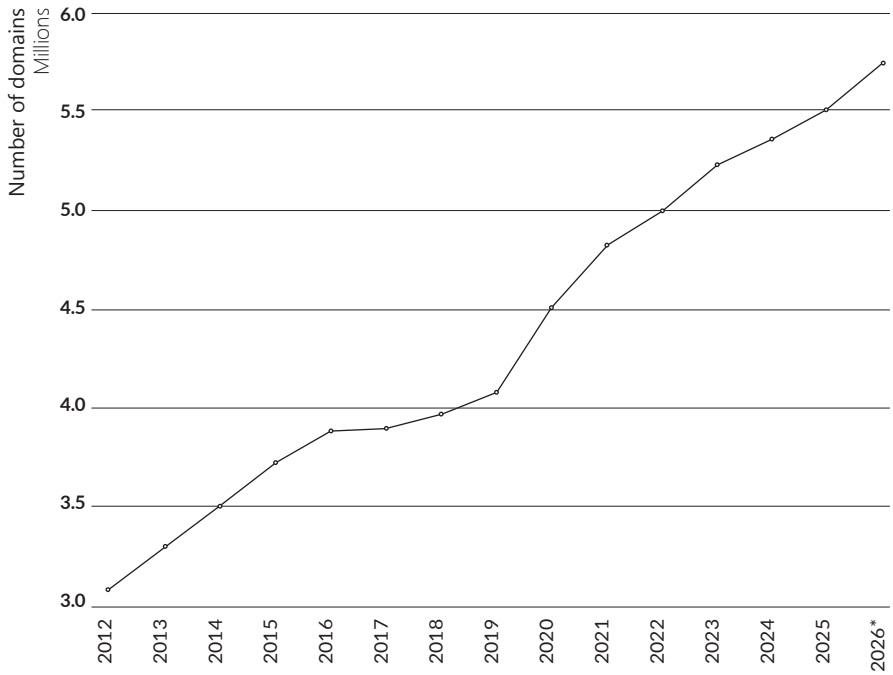
Table 1 – TOTAL REGISTRATION OF DOMAIN NAMES AMONG OECD AND G20 COUNTRIES

Position	Country	Number of domains	Date of reference	Source (website)
1	Germany (.de)	17,968,945	01/06/2026	https://www.denic.de
2	China (.cn)	12,125,420	01/06/2026	https://research.domaintools.com/statistics/tld-counts/
3	United Kingdom (.uk	8,986,855	30/04/2026	https://nominet.uk/reports-and-statistics/
4	Russia (.ru)	6,114,524	01/06/2026	https://cctld.ru
5	Netherlands (.nl)	6,081,616	31/05/2026	https://stats.sidnlabs.nl/en/registration.html
6	**Brazil (.br)**	**5,755,795**	**31/05/2026**	**https://registro.br/dominio/estatisticas/**
7	France (.fr)	4,466,907	30/05/2026	https://www.afnic.fr/en/observatory-and-resources/statistics/
8	Australia (.au)	4,368,740	01/06/2026	https://www.auda.org.au/
9	European Union (.eu)	3,683,208	01/06/2026	https://research.domaintools.com/statistics/tld-counts/
10	Italy (.it)	3,592,180	01/06/2026	http://nic.it
11	Canada (.ca)	3,575,127	01/06/2026	https://www.cira.ca
12	India (.in)	3,419,117	01/06/2026	https://research.domaintools.com/statistics/tld-counts/
13	Colombia (.co)	3,151,207	01/06/2026	https://research.domaintools.com/statistics/tld-counts/
14	Switzerland (.ch)	2,614,611	15/05/2026	https://www.nic.ch/statistics/domains/
15	Poland (.pl)	2,573,378	01/06/2026	https://research.domaintools.com/statistics/tld-counts/
16	Spain (.es)	2,183,603	30/04/2026	https://www.dominios.es/es/sobre-dominios/estadisticas
17	Portugal (.pt)	2,148,852	01/06/2026	https://www.dns.pt/en/statistics/
18	United States (.us)	2,036,354	28/02/2026	https://www.about.us/stats-trends
19	Japan (.jp)	1,860,215	01/06/2026	https://jprs.co.jp/en/stat/
20	Belgium (.be)	1,702,749	01/06/2026	https://www.dnsbelgium.be/en

Collection date: June 1, 2026.

Chart 1 shows the performance of .br since 2012.

Chart 1 – TOTAL NUMBER OF DOMAIN REGISTRATIONS FOR .BR – 2012 to 2026*



*Collection date: May 31, 2026.
Source: Registro.br
Retrieved from: https://registro.br/dominio/estatisticas

In May 2026, the five generic Top-Level Domains (gTLD) totaled more than 201.65 million registrations. With 163.19 million registrations, .com ranked first, as shown in Table 2.

Table 2 – TOTAL NUMBER OF DOMAINS AMONG MAIN gTLD

Position	gTLD	Number of domains
1	**.com**	163,198,805
2	**.net**	12,248,331
3	**.org**	11,909,496
4	**.xyz**	7,823,909
5	**.top**	6,478,286

Collection date: June 1, 2026.
Source: DomainTools.com
Retrieved from: research.domaintools.com/statistics/tld-counts

Internet markers in Brazil

Indicators of the Internet Traffic Measurement System (SIMET)

The Center for Study and Research on Network Technology and Operations (Ceptro.br),[42] a department of the Brazilian Network Information Center (NIC.br), is responsible for the Internet Traffic Measurement System (SIMET).[43]

The platform allows you to assess the quality of Internet connection by collecting metrics such as latency, jitter, packet loss, and download and upload speeds.

SIMET was developed to provide an independent assessment of connection quality. To achieve this, it uses a methodology focused on the impartiality and neutrality of the measurements. Currently, due to the distribution of its server network, most tests are performed outside the operator's or access provider's network, thereby reducing the influence of the provider's own infrastructure on the results.

Measurements can be performed using SIMET Web or the SIMET Mobile app, available for Android and iOS. Over the past six months, 447,559 measurements have been recorded, considering both modalities. In addition to performing tests, SIMET Mobile helps users interpret the results, indicating whether the connection is suitable for activities such as remote work, videoconferencing, streaming, and online gaming.

The app also explains the meaning of key quality indicators, provides guidance when performance issues are identified, and keeps a history of measurements organized by usage location, allowing users to track connection evolution over time and compare performance in different environments, such as home and work.

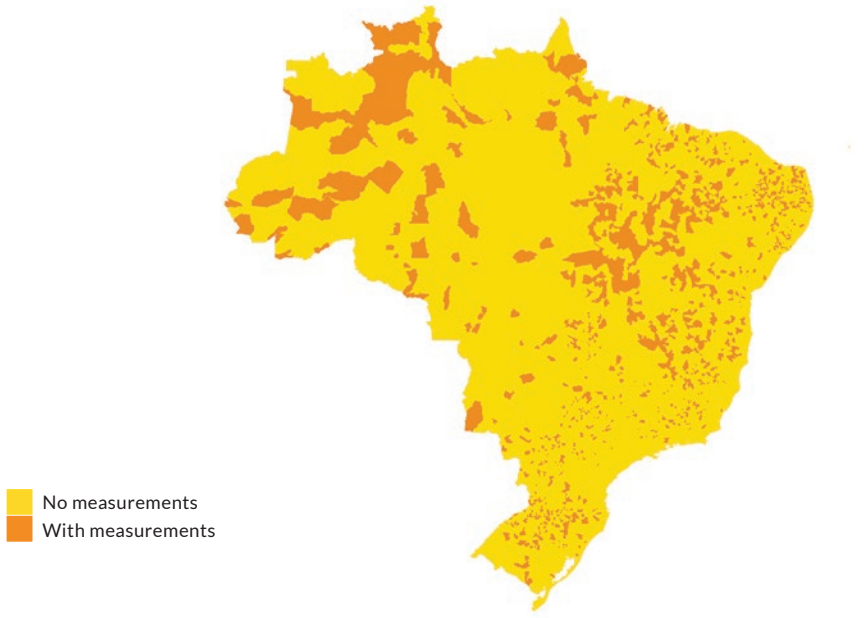
By using SIMET, users not only receive a diagnosis of their connection quality but also contribute to a database that supports connectivity monitoring in Brazil. In an anonymous and aggregated manner, these measurements support NIC.br initiatives to monitor Internet quality in essential public services, such as schools and health units, contributing to the production of indicators that support studies and public policies. Figure 1 illustrates the extent of voluntary measurements using SIMET: Out of the 5,571 municipalities in Brazil (including the Federal District), 4,374 (78.51%) had at least one measurement recorded during the period, while Figure 2 shows the number of measurements per municipality.

Measurements performed by SIMET users support the production of indicators and studies that contribute to monitoring connectivity and improving digital public policies.

[42] Find out more: https://ceptro.br/
[43] Find out more: https://medicoes.nic.br/

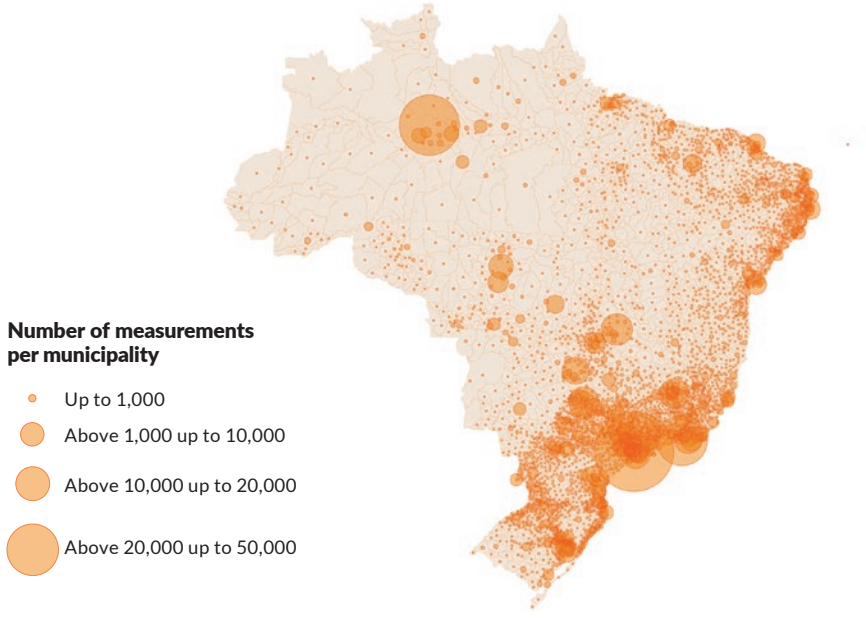
Each measurement with user-authorized location data expands knowledge about connectivity in Brazil and contributes to identifying regional inequalities in Internet access.

Figure 1 – MUNICIPALITIES WITH MEASUREMENT RECORDING FROM WEB AND MOBILE METERS



Collection Period: December 2025 to May 2026.
Source: Ceptro.br | NIC.br

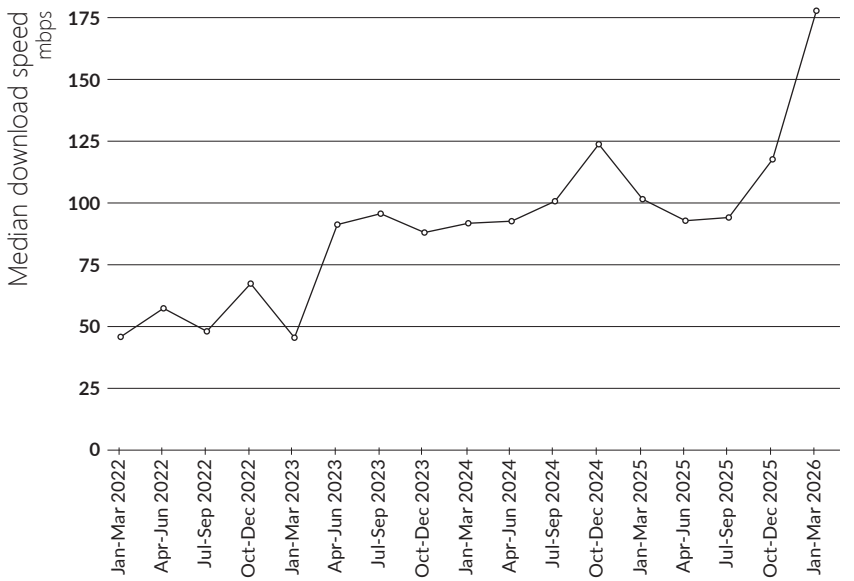
Figure 2 – NUMBER OF WEB AND MOBILE METER MEASUREMENTS, BY MUNICIPALITY



Collection Period: December 2025 to May 2026.
Source: Ceptro.br | NIC.br

Download speed, one of the metrics for analyzing the quality of the Internet, refers to the data transmission rate or speed at which transactions take place between the measuring servers and the measured device. The higher the speed, the better the connection. Chart 1 presents the median of total download speed measurements per quarter since 2022, while Figure 3 shows the median download speed for the last six months for each Federation Unit (FU).

Chart 1 – DOWNLOAD SPEED MEDIAN BY QUARTER - 2022 TO 2023[44]

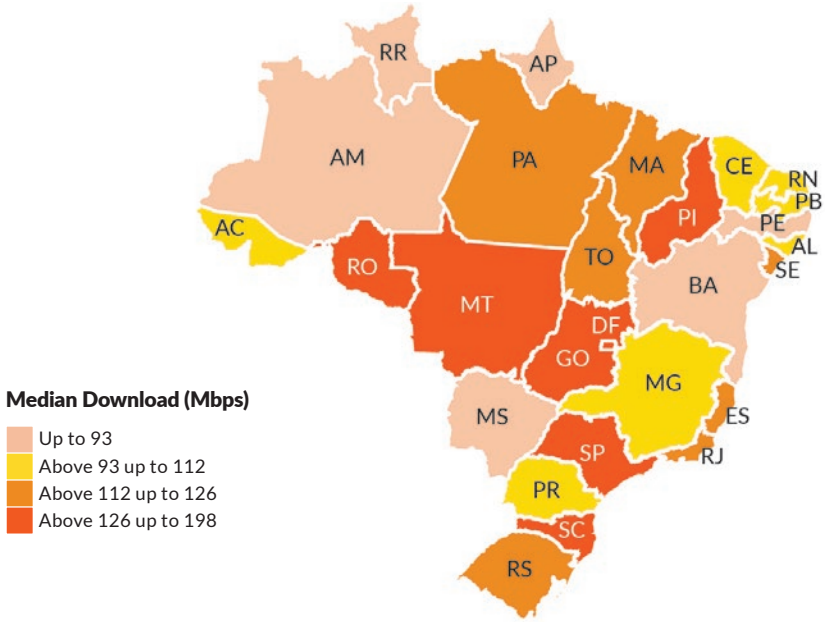


Collection Period: January 2022 to March 2026.
Source: Ceptro.br | NIC.br

The evolution of download speed is an important indicator of the development of Internet infrastructure. Faster and more stable connections expand access to digital services, improve user experience, and promote the adoption of applications that require greater data transmission capacity. Monitoring this indicator over time allows us to track the progress of connectivity in the country.

[44] The fluctuations observed reflect existing variations in the proportion of measurements performed by mobile and web meters in each quarter. Despite this, there is a clear general trend toward an increase in download speed over time.

Figure 3 – DOWNLOAD SPEED MEDIAN, BY FEDERATIVE UNIT



Collection Period: December 2025 to May 2026.
Source: Ceptro.br | NIC.br

Internet quality is not uniform. Differences among regions reflect characteristics of infrastructure, service offerings, and access technologies. Mapping these variations is an essential step in understanding the challenges of connectivity and guiding evidence-based public policies.

Measurements performed by users provide an essential contribution to studies, analyses, and public policies. The greater the number of measurements distributed across Brazilian municipalities, the more accurate the estimates of Internet quality in the country.

What you need to know about

Security and incident response teams

With the increasingly important role of technology and connectivity in all activities of society, attacks on Internet systems have increased in both frequency and complexity. To detect attacks and handle security incidents, there are various types of teams, each with specific characteristics related to the public they serve and the types of services they provide.[45] These teams use acronyms in their names that are globally associated with the services they provide and, in most cases, the team names themselves serve as necessary calling cards for interactions with peers. There is some confusion and misinformation surrounding the roots and meanings of these acronyms, so what follows is a discussion of the community's origins and uses of these terms.

CERT

Computer Emergency Response Team

The first team created was the CERT Coordination Center (CERT/CC), in 1988, based on one of the needs identified in response to the Morris Worm.[46] A few years later, the acronym became a registered trademark of the Software Engineering Institute at Carnegie Mellon University (SEI/CMU) after attackers attempted to use it to impersonate a CERT and gain privileged access to target organizations. Since then, it has been standard practice to request permission from the CERT Division of SEI/CMU to use the acronym. Apart from that, there is no difference between a team called a CERT, a Computer Security Incident Response Team (CSIRT), a Computer Incident Response Team (CIRT), an Incident Response Team (IRT), or any other acronym referring to incident handling teams.

CSIRT

Computer Security Incident Response Team

A CSIRT offers security incident management services focused on prevention, incident handling (i.e., detection, analysis, and response), and/or coordination of actions necessary for effective handling of incidents. Other frequently used acronyms include CERT, CIRT, and Computer Incident Response Center (CIRC), or variations thereof, depending on the objectives of the organization that created the team. It is important to note that the acronym CSIRT was created in 1998, when the SEI/CMU published the *Handbook for Computer Security Incident Response Teams (CSIRTs)*,[47] a seminal document that, for the first time, defined and formalized incident handling procedures. The acronym CSIRT and its expansion were created by the authors to refer, in a generic sense, to incident handling teams, since CERT is a registered trademark.

[45] The definitions of the team types are based on the document Team types within the context of services frameworks by the Forum of Incident Response and Security Teams. Available at: https://www.first.org/standards/frameworks/csirts/team-type_1.2

[46] Find out more: https://www.fbi.gov/history/cases-and-criminals/morris-worm and https://alumni.cornell.edu/cornellians/morris-worm/

[47] Find out more: https://cisre.egr.uh.edu/wp-content/uploads/2023/09/csirt.pdf

Since then, CSIRT has become one of the most widely used acronyms to refer to incident response and handling teams. For pragmatic reasons, many teams simply adopt the name "CSIRT Organization" to indicate the type of work they do. Depending on the organization's choices, the CSIRT can also perform tasks that are typically handled by a SOC.

ISAC

Information Sharing and Analysis Center

An ISAC is a center dedicated to a specific sector (e.g., financial, electrical, or industrial) that focuses on collecting, analyzing, and sharing information on cyber threats specific to that sector. It can also facilitate sectoral cooperation.

SOC

Security Operations Center

A SOC is a team that focuses on managing security events, that is, monitoring and detecting attacks. To do so, a SOC needs to have access to the organization's event logs. It is the team that generally handles alerts from intrusion detection and endpoint monitoring systems (such as security information and event management [SIEM], endpoint detection and response [EDR], extended detection and response [XDR], firewalls, etc.). Some organizations choose to implement incident handling functions as part of their SOC activities.

PSIRT

Product Security Incident Response Team

A PSIRT is a team that focuses on identifying, assessing, and addressing risks associated with security vulnerabilities in products developed by an organization and is generally associated with a software vendor, whether commercial or open source.

CTIR and ETIR

Computer Incident Response Team and Equipe de Tratamento e Resposta a Incidentes Cibernéticos

In Brazil, these are two acronyms used by government-affiliated entities to designate their CSIRTs. CTIR was the acronym chosen when CTIR Gov[48] was created, a CSIRT maintained by the Institutional Security Office, which was originally expanded to the Federal Government Network Incident Response Center (Centro de Tratamento de Incidentes em Redes do Governo Federal), and has now been expanded to the Cyber Incident Prevention, Handling, and Response Center of Brazilian Government. The acronym ETIR began to be used after the publication of Normative Instruction No. 1 of the GSI/PR,[49] which stipulates that every agency or entity of the Federal Public Administration should establish an ETIR. Since these acronyms are not widely known internationally, many teams that use them in Brazil need to identify themselves in other ways when communicating with international counterparts.

[48] Find out more: https://www.gov.br/gsi/pt-br/assuntos/ctir

[49] Find out more: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao/copy_of_IN01_consolidada.pdf

/Credits

TEXT

DOMAIN REPORT

Thiago Meireles (Cetic.br | NIC.br)

GRAPHIC DESIGN

Andre Martini Martins (Comunicação | NIC.br)

PUBLISHING

Grappa Marketing Editorial

ENGLISH REVISION AND TRANSLATION

Prioridade Consultoria Ltda.: Isabela Ayub, Lorna Simons, Luana Guedes, Luísa Caliri, and Maya Bellomo Johnson

EDITORIAL COORDINATION

Alexandre F. Barbosa, Graziela Castello, Javiera F. M. Macaya, Manuela Cortez da Cunha Cruz, Rodrigo Brandão, and Mariana Galhardo Oliveira (Cetic.br | NIC.br)

ACKNOWLEDGMENTS

Javiera F. Medina Macaya (Cetic.br | NIC.br)

Cristine Hoepers (CERT.br | NIC.br)

Olivier Caleff (FIRST, CSIRT.FR, and Open CSIRT Foundation)

Gilberto Zorello (NIC.br)

ABOUT CETIC.br

The Regional Center for Studies on the Development of the Information Society – Cetic.br (https://www.cetic.br/en/), a department of NIC.br, is responsible for producing studies and statistics on the access and use of the Internet in Brazil, disseminating analyzes and periodic information on the Internet development in the country. Cetic.br acts under the auspices of UNESCO.

ABOUT NIC.br

The Brazilian Network Information Center – NIC.br (http://www.nic.br/about-nic-br/) is a non-profit civil Entity in charge of operating the .br domain, distributing IP numbers, and registering Autonomous Systems in the country. It conducts initiatives and projects that bring benefits to the Internet infrastructure in Brazil.

ABOUT CGI.br

The Brazilian Internet Steering Committee – CGI.br (https://cgi.br/about/), responsible for establishing strategic guidelines related to the use and development of the Internet in Brazil, coordinates and integrates all Internet service initiatives in the country, promoting technical quality, innovation, and dissemination of the services offered.

*The ideas and opinions expressed in the texts of this publication are those of the respective authors and do not necessarily reflect those of NIC.br and CGI.br.

unesco
Centre under the auspices of UNESCO

cetic.br
Regional Center for Studies on the Development of the Information Society

nic.br
Brazilian Network information Center

cgi.br
Brazilian Internet Steering Committee

STRIVING FOR A BETTER INTERNET IN BRAZIL

CGI.br, MODEL OF MULTISTAKEHOLDER GOVERNANCE

www.cgi.br

nic.br cgi.br

PHOTOS: RICARDO MATSUKAWA AND SHUTTERSTOCK