

CERT.br/NIC.br

Incident Management Activities

Cristine Hoepers, Ph.D.

General Manager, CERT.br/NIC.br
cristine@cert.br

Classification of AI Incidents, Institute of Advanced Studies – IEA/USP
São Paulo/SP – 14 de setembro de 2026

cert.br nic.br cgi.br

Services Provided to the Community

Incident Management

- ▶ Coordination
- ▶ Technical Analysis
- ▶ Mitigation and Recovery Support

Situational Awareness

- ▶ Data Acquisition
 - ▶ Distributed Honeypots
 - ▶ SpamPots
 - ▶ Threat feeds
- ▶ Information Sharing

Knowledge Transfer

- ▶ Awareness
 - ▶ Development of Best Practices
 - ▶ Outreach
- ▶ Training
- ▶ Technical and Policy Advisory

Affiliations and Partnerships:



SEI
Partner
Network



Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Constituency

Any network that uses Internet Resources allocated by NIC.br

- IP addresses or ASNs allocated to Brazil
- domains under the ccTLD .br

Governance

Maintained by **NIC.br** – The Brazilian National Internet Registry (NIR)

- all activities are funded by .br domain registration

NIC.br is the **executive branch of CGI.br** – The Brazilian Internet Steering Committee

- a multistakeholder organization
- with the purpose of coordinating and integrating all Internet service initiatives in Brazil

<https://cert.br/about/>
<https://cert.br/sobre/filiacoes/>
<https://cert.br/about/rfc2350/>

CERT.br's focus over 29 years:

Increasing the National Incident Handling Capacity

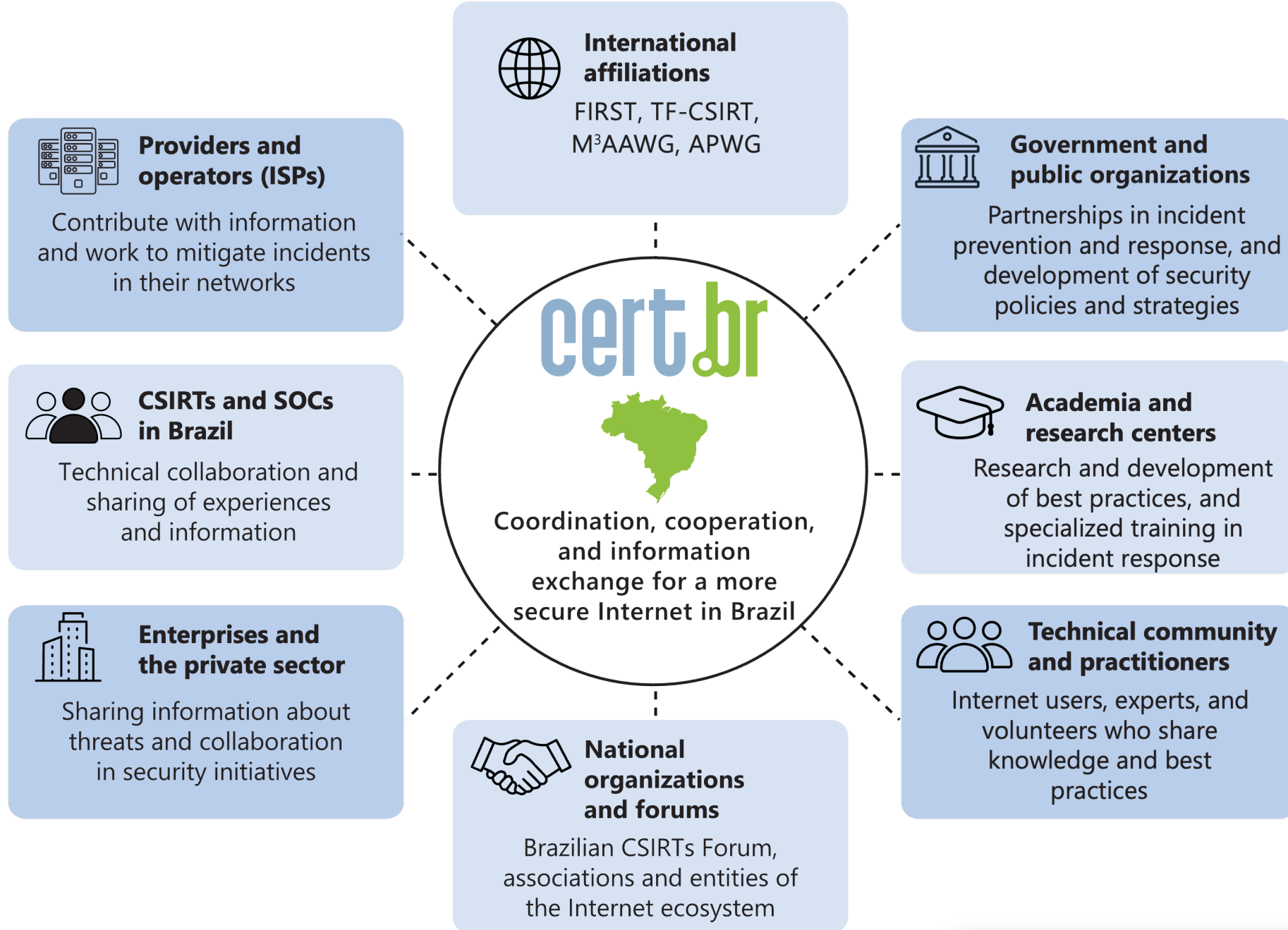
No single team or structure can do security or incident response alone

Foster and Strengthen the National Community

- Actions with key sectors to create and train Security Incident Response Teams (CSIRTs)
- **Assist in technical analysis and facilitate** incident handling by other CSIRTs
- Generate critical mass to enable **cooperation** and improved network security
- Gain **insight** into the main attack **trends** in Brazil

Participate in the International Community

- Establish **trust relationships**
 - facilitate communication in cases of incidents
 - provide access to information that helps the local community
- **Contribute** to the standards and certifications under construction for CSIRTs
- Take the **national vision** to the relevant forums



AI Incident

*An **AI incident** is an event, circumstance or series of events where the development, use or malfunction of one or more AI systems directly or indirectly leads to any of the following harms:*

- (a) injury or harm to the health of a person or groups of people;*
- (b) disruption of the management and operation of critical infrastructure;*
- (c) violations of human rights or a breach of obligations under the applicable law intended to protect fundamental, labour and intellectual property rights;*
- (d) harm to property, communities or the environment.*

Source: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/defining-ai-incidents-and-related-terms_88d089ec/d1a8d965-en.pdf

Security Incident

NIST:

“An occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.”

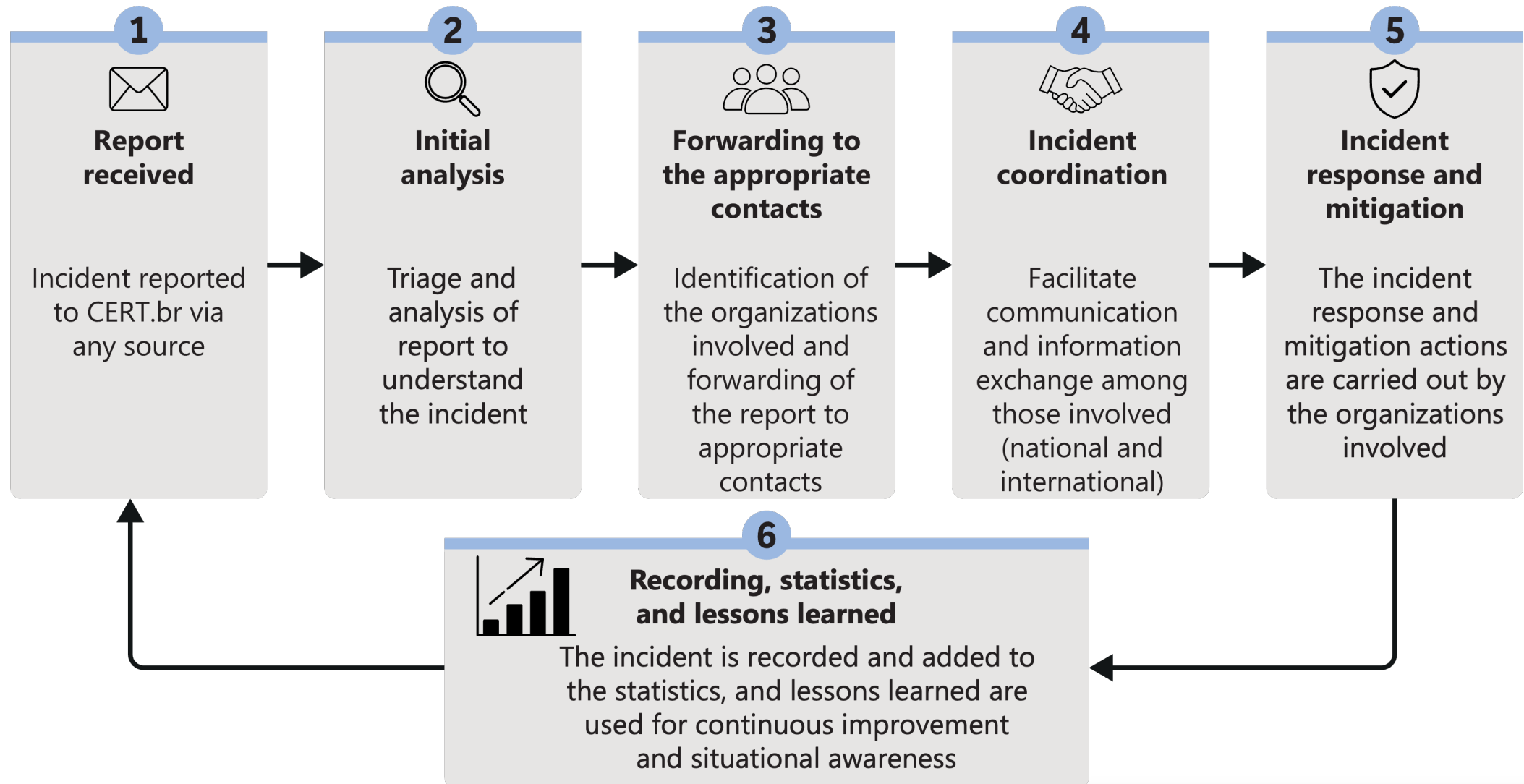
ISO/IEC 27035-1:2023:

“related and identified information security event(s) that can harm an organization's assets or compromise its operations”

information security event: “occurrence indicating a possible breach of information security or failure of controls”

Source: https://csrc.nist.gov/glossary/term/security_incident | <https://www.iso.org/obp>

Lifecycle of a Security Incident Reported to CERT.br



Thank You

@ cristine@cert.br

@ Incident notifications to: cert@cert.br

X @certbr

<https://cert.br>

nic.br cgi.br

www.nic.br | www.cgi.br