nic.br cgi.br

cert.br

First Forum for Law Enforcement Agencies (LEAs)

LACNIC 32

October 09, 2019 – Panamá

CSIRTs and LEAs Cooperation

Dr. Cristine Hoepers
General Manager
cristine@cert.br

cert.br nic.br cgi.br

Incident Management

- ▶ Coordination
- ▶ Technical Analysis
- ▶ Support for recovery

Training and Awareness

- ▶ Courses
- ▶ Presentations
- ▶ Best Practices
- ▶ Meetings

Trend Analysis

- ▶ Distributed Honeypots
- ▶ SpamPots
- ▶ Processing of threat feeds

SEI
Partner
Network

Creation:

August/1996: report with a proposed model for incident management for the country is published by the Brazilian Internet Steering Committee – CGI.br[1]

June/1997: CGI.br creates CERT.br (at that time called NBSO – *NIC BR Security Office*) based on the report's recommendations[2]

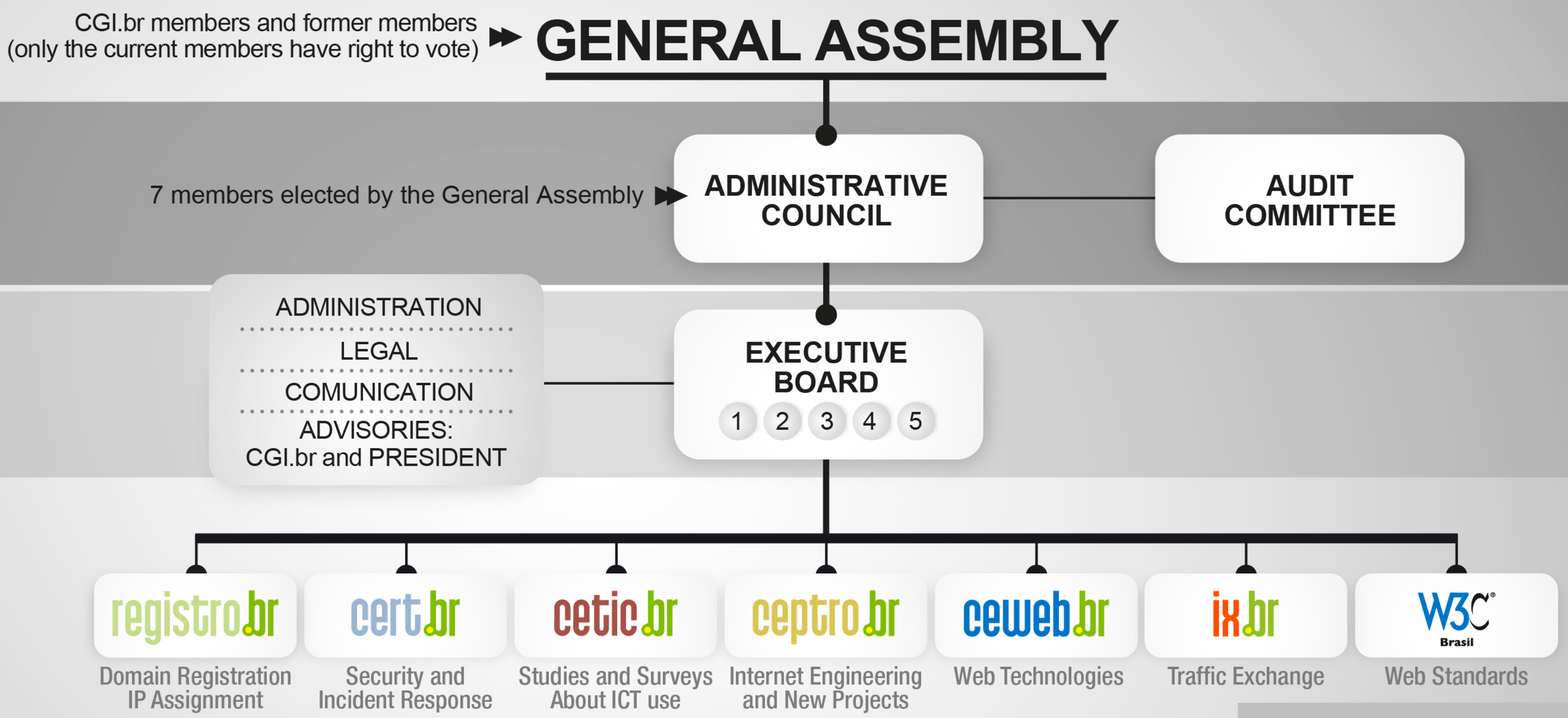
[1] https://www.nic.br/grupo/historico-gts.htm | [2] https://www.nic.br/pagina/gts/157

Mission

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

Focus of the Activities

- National focal point for security incident reports
- Support technical analysis and the understanding of attacks and threats
- Develop collaborative relationships with other entities
- Increase the capacity of incident detection, event correlation and trend analysis in the country
- Transfer the acquired knowledge through courses, best practices and awareness materials



CGI.br members and former members
(only the current members have right to vote)

GENERAL ASSEMBLY

7 members elected by the General Assembly

ADMINISTRATIVE COUNCIL

AUDIT COMMITTEE

ADMINISTRATION

LEGAL

COMUNICATION

ADVISORIES:
CGI.br and PRESIDENT

EXECUTIVE BOARD

1 2 3 4 5

registro.br
Domain Registration
IP Assignment

cert.br
Security and
Incident Response

cetic.br
Studies and Surveys
About ICT use

ceptro.br
Internet Engineering
and New Projects

ceweb.br
Web Technologies

ix.br
Traffic Exchange

W3C Brasil
Web Standards

1 Chief Executive Officer
2 Administrative and Financial Director
3 IT and Services Director
4 Director of Special Projects and Development
5 Consulting Director for CGI.br activities

NIC.br:

Not for profit organization that implements all services and decisions of CGI.br.

Internet Governance in Brazil:
The Brazilian Internet Steering Committee – CGI.br

CGI.br is a **multi-stakeholder organization created in 1995** by the Ministries of Communications and Science and Technology **to coordinate all Internet related activities in Brazil**.

Among the responsibilities reinforced by the Presidential Decree 4.829, it has as the main attributions:

- to propose policies and procedures related to the regulation of Internet activities
- **to recommend standards for technical and operational procedures**
- to establish strategic directives related to the use and development of Internet in Brazil
- **to promote studies and technical standards for the network and services' security in the country**
- to coordinate the allocation of Internet addresses (IP) and the registration of domain names using <.br>
- to collect, organize and disseminate information on Internet services, including indicators and statistics.

https://www.cgi.br/sobre/

CGI.br Members

As established by the presidential decree Nº 4.829, 03/09/2003

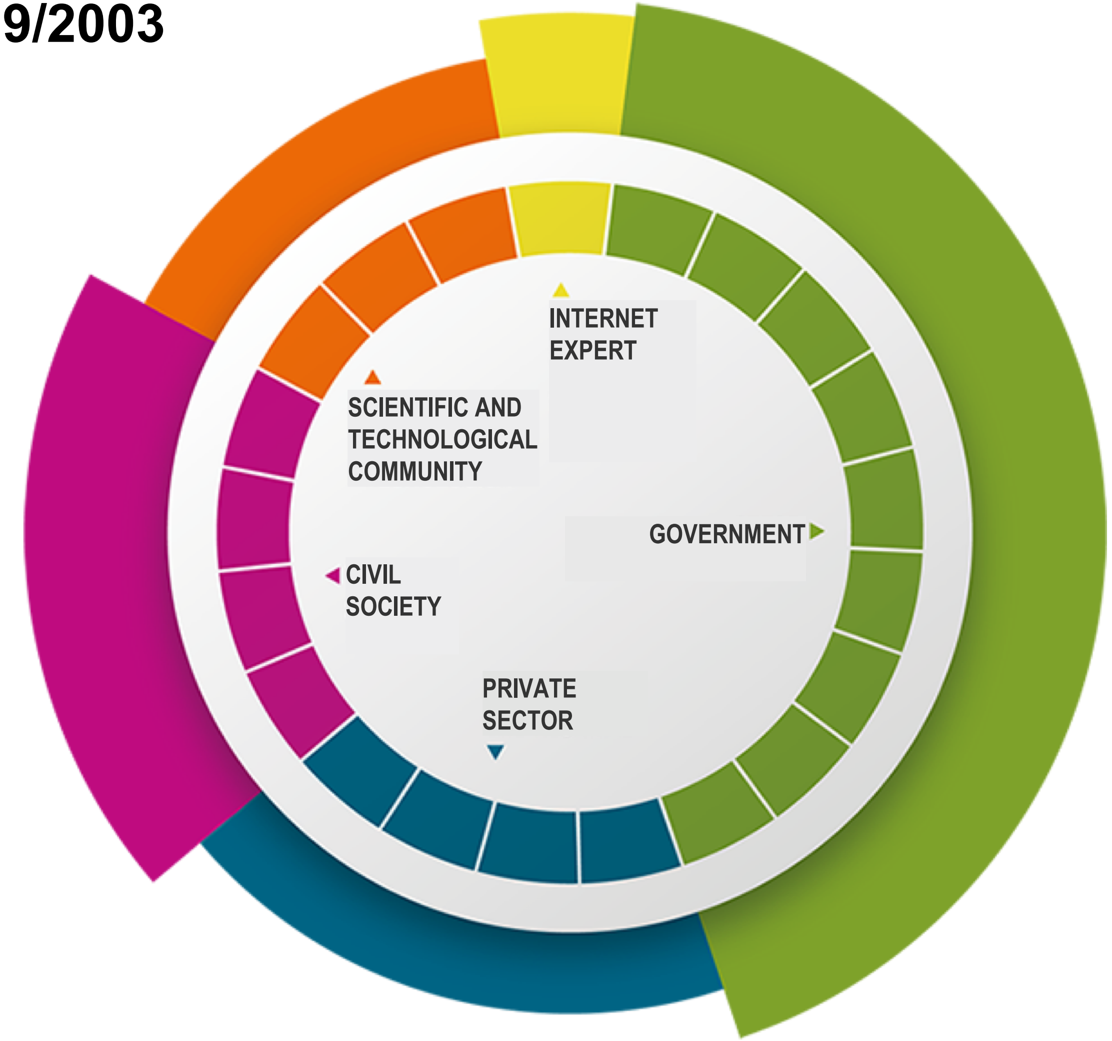
9 representatives from the Government

Ministry of Science, Technology and Innovation (coordination)
Ministry of Communications
Presidential Cabinet
Ministry of Defense
Ministry of Development, Industry and Foreign Trade
Ministry of Planning, Budget and Management
National Telecommunication Agency
National Council for Scientific and Technological Development
National Council of State Secretariats for Science, Technology and Information

12 representatives from private sector & civil society

Private Sector (4)
- Internet access and content providers
- Telecommunication infrastructure providers
- Hardware, telecommunication and software industries
- Enterprises that use the Internet

Civil Society (4)
Scientific and technological community (3)
Internet Expert (1)



Agenda

– Context

  – CSIRT and Incident Definitions

  – CSIRT Services Framework

– CSIRT Services that can help or enable law enforcement work

– Final considerations

Context

cert.br nic.br cgi.br

What is a CSIRT?

A Computer Security Incident Response Team (CSIRT) is

- an organizational unit (which may be virtual) or a capability
- that provides services and support to a defined constituency
- for preventing, detecting, handling, and responding
- to computer security incidents,
- in accordance with its mission.

Source: CSIRT Services Framework v2.0
https://www.first.org/education/csirt_services_framework_v2.0

Some Computer Security Incident Definitions

IT Infrastructure Library (ITIL) 2011

- an unplanned interruption to an IT Service or reduction in the quality of an IT service

ISO/IEC 27035-1:2016

- single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

SANS Computer Security Incident Handling Step-by-Step Guide

- “an adverse event in an information system and/or network, or the threat of the occurrence of such an event”

NIST Computer Security Incident Handling Guide

- “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices”

How CSIRTs Operate:
FIRST CSIRT *Services Framework v2.0*

High level description of services that can be offered

- by a CSIRT
- by other teams that provide incident management services

It is the new "CSIRT Services" document

These are Best Practices from the FIRST perspective

- To help CSIRTs to
  - identify and choose main services
  - a starting point for standard's terms and definitions to be used by the community
- What this document is **not**
  - it does not explain how to create a CSIRT
  - does not cover CSIRT maturity issues

https://www.first.org/education/csirt_services_framework_v2.0

Computer Security Inciden

Services Framework

Version 2.0 (Review Releas

FIRST.Org, Inc. (www.first.org)

Forum of Incident Response and Security Teams

Table of Contents

Version 2.0.1 (Review) 3

CSIRT *Services Framework v2.0*: **Service Areas**

Information Security Event Management

- Monitoring and Detection
- Analyzing

Information Security Incident Management

- Accepting Reports
- Analyzing Incidents
- Analyzing artefacts and forensic evidence
- Mitigation and recovery
- Coordination

Vulnerability Management

- Vulnerability Discovery
- Report Intake
- Analysis
- Coordination
- Disclosure
- Response

Situational Awareness

- Data Acquisition
- Analysis and Synthesis
- Communication

Knowledge Transfer

- Awareness Building
- Training and Education
- Exercises
- Technical and Policy Advisory

CSIRT Services That can Help or Enable Law Enforcement Work

cert.br nic.br cgi.br

5.1 Service: Monitoring and detection

"List of functions which are considered to be part of the implementation of this service:

– Log and sensor management

– Detection use case management

– Contextual data management"

How this can help:

– Accurate logs

  – e.g. synchronized time and correct timezone

– Relevant logs

6.1 Service: Accepting information security incident reports

"6.1.2 Function: Information security incident report triage and processing

– ***Description:*** *The initial review, categorization, prioritization, and processing of a reported information security incident."*

How this can help:

– Policies should define clearly
  - what is an incident
  - which incidents could be a criminal activity and should be reported to LEA

6.2 Service: Analyzing information security incidents

"List of functions which are considered to be part of the implementation of this service:

- *Information security incident triage (prioritization and categorization)*
- *Information collection*
- *Coordinate any more detailed analysis*
- *Information security incident root cause analysis*
- *Cross-incident correlation"*

How this can help:

- Policies should define clearly how to trigger evidence collection and preservation

6.3 Service: Analyzing artefacts and forensic evidence

*“**Description:** Analyzing and gaining an understanding of artefacts related to a confirmed information security incident, **taking into consideration the need to preserve forensic evidence.**”*

Final Considerations

CSIRTs leave or die by their credibility, this means

– respecting confidentiality

– establishing trust relationships

Not all security incidents are crimes

– actually the vast majority of incidents handled by CSIRTs are not crimes

CSIRTs are not investigators

– but they are the “first responders”

– organizations with mature CSIRTs and policies can help LEAs in different ways

Additional References

IGF (United Nations Internet Governance Forum) Best Practices Forums

- Final reports of the working groups on “*Establishing and supporting CSIRTs*” and “*Fighting Spam*”

  2015: **http://www.intgovforum.org/cms/best-practice-forums/2015-best-practice-forum-outputs**

  2014: **http://www.intgovforum.org/cms/best-practice-forums/igf-2014-best-practices-forums**

- “*Best Practices Forum on Cybersecurity*”. 2019 topic: “*Exploring best practices in relation to recent international cybersecurity initiatives*”

  2016–2019: https://www.intgovforum.org/multilingual/content/bpf-cybersecurity

FIRST Internet Governance Initiative

https://www.first.org/global/governance/

FIRST Incident Handling for Policy Makers

https://www.first.org/education/trainings#Incident-Handling-for-Policy-makers

Thank You

@ cristine@cert.br

@ Incident reports to: cert@cert.br

@certbr

www.cert.br

October 09, 2019

nic.br cgi.br

www.nic.br | www.cgi.br