You are here: CERT.br > **About CERT.br**

About CERT.br

CERT.br is the Brazilian National Computer Emergency Response Team, maintained by NIC.br – the executive branch of the Brazilian Internet Steering Committee. CERT.br is responsible for handling computer security incident reports and activity related to Brazilian networks connected to the Internet.

CERT.br provides a focal point for incident notification in the country, providing the coordination and necessary support for organizations involved in incidents.

Besides doing Incident Handling activities, CERT.br also works to increase security awareness in our community, maintains an early warning project with the goal of identifying new trends and correlating security events, as well as alerting Brazilian networks involved in malicious activities. CERT.br also helps new Computer Security Incident Response Teams (CSIRTs) to establish their activities in the Country.

These activities have the strategic goal of increasing the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

The activities performed by CERT.br are in accordance to the CGI.br attributions, as defined in the Presidential Decree 4829, from 2003:

- **I -** to establish strategic directives related to the use and development of the Internet in Brazil;
- **IV -** to promote studies and recommend procedures, rules and technical and operational standards for the security of the network and services in the Internet, as well as for its growth and adequate use by the society;
- **VI -** to be represented at national and international forums related to the Internet;

This activities are also in accordance to the NIC.br objectives, according to is Statute:

- **IV -** to address the security and emergency requisites of the Brazilian Internet, in articulation and cooperation with other entities;
- **VII -** to promote and collaborate in the organization of courses, symposiums, seminars, conferences and congresses, with the objective of contributing for the development and improvement of teaching opportunities in its areas of expertise.

Main Activities

Incident Handling

- Support in the analysis of compromised systems and in their recovery process;

- Establish collaborative relationships with other entities, such as other CSIRTs, universities, Internet service and access providers and telecommunication companies;
- Maintain public statistics of incidents handled and spam complaints received.

Training and Awareness

- Provide training in Incident Response, specially for CSIRT staff and for institutions starting the creation of a CSIRT;
- Develop support documentation in Portuguese for system administrators and Internet users;
- Promote meetings among key stakeholders to foster cooperations and adoption of security best practices.

Network Monitoring and Trend Analysis

- Increase the capacity of incident detection, event correlation and trend analysis in the country, trough a network of distributed honeypots in the Brazilian Internet space.
- Obtain details about the abuse of the Internet infrastructure by spammers, using low-interaction honeypots distributed in several countries.

$Date: 2012/03/19 21:46:50 $