Núcleo de Informação e Coordenação do Ponto BR

Acceptable Use Policy IX.br - V1.1

About the Content

1. NIC.br does not make inspection and control over the content of information originated, stored, or even transmitted through its network infrastructures. Participants are responsible for ensuring that their information is in accordance with applicable laws, rules and regulations, and this Acceptable Use Policy (AUP).

2. By not controlling the content generated by the Participants, NIC.br is not responsible for it. NIC.br can only be held responsible for its own content.

General

1. All Participants have a responsibility to ensure that their network equipment is available in a fair manner to all Participants, meaning that all Participants will have access through the entire band available on their ports to useful traffic, without impdiment by any accidental or deliberate act.

2. Wherever it is within its competence, Participants shall take all measures, including those proposed by IX.br, to ensure the proper functioning of the IXP (Internet Traffic Exchange Point), including the management of Internet traffic in a proactive manner in their own networks, regardless of who has generated Internet traffic.

3. NIC.br reserves the right to modify this AUP at any time with 30 (thirty) days prior notice, and the valid document will be the one that is available on the IX.br website (http://www.ix.br/pua). The provisions contained in this AUP do not contain all restrictions on the use of NIC.br's network and service infrastructure.

Prevention of flooding and denial of service attacks

1. Participants are responsible for properly monitoring their networks on a 24 x 7 regime (24 hours, or seven days a week) to ensure that their use of IX.br does not intend or cause flooding or denial of service.

2. To reduce the likelihood of unintentional flooding or deliberate denial of service attacks, Participants shall abide by the entire Technical Requirements Policy (http://www.ix.br/requisitos) which specifies the types of traffic and the types of packages that can be forwarded to IX.br.

Unauthorized access or malicious attempts to compromise a IX.br network

1. No NIC.br service, system or network structure may be used for unlawful and / or unethical purposes that violate any local, state, national, or international agreements.

2. The Participants shall take reasonable measures to prevent unauthorized access or malicious attempts to compromise the IX.br network.

3. The Participants shall not disclose information to unauthorized third parties that may help them to compromise the IX.br network, including privileged confidential information provided to the Participants, as well as information of general use, not yet in the public domain, about IX.br which may be useful to unauthorized third parties.

4. System violations and network security are prohibited. NIC.br reserves the right to disclose the contacts of Participants involved in security breaches to other Participants in order to help them

resolve security incidents. The NIC.br will also cooperate with the investigations promoted by the legal authorities.

5. Examples of system or network security breaches:
    a. Use IX.br to compromise or manipulate system or account resources in the infrastructure of IX.br or elsewhere;
    b. Use or distribution of tools designed to compromise safety. Examples of this type of tools are password discovery programs, intrusion tools or probing tools;
    c. Unauthorized access to, or use of, data, systems or networks. This includes any attempt to poll, scan, or test vulnerabilities of systems, networks, or security holes;
    d. Unauthorized monitoring of data or traffic on any network or system without the express authorization of the system or network owner;
    e. Forge any TCP/IP packet or packet header or any piece of header information in post via e-mail or newsgroup;
6. NIC.br reserves the right to disconnect all ports involved in malicious activity, and/or port scanning.