Núcleo de Informação e Coordenação do Ponto BR

Política de Uso Aceitável IX.br - V1.0

Sobre o Conteúdo

1. O NIC.br não exerce inspeção e controle sobre o conteúdo das informações originadas, armazenadas, ou mesmo transmitidas através de suas infraestruturas de rede. Os Participantes são responsáveis por certificar-se que suas informações estejam de acordo com as leis, normas e regulamentações aplicáveis, e por esta Política de Uso Aceitável (PUA).

2. Por não controlar o conteúdo gerado pelos Participantes, o NIC.br não se responsabiliza por ele. O NIC.br só pode ser responsabilizado por seu próprio conteúdo.

Geral

1. Todos os Participantes tem a responsabilidade de garantir que seus equipamentos de rede estejam disponíveis de maneira justa a todos os Participantes, significando que todos os Participantes terão acesso através da totalidade da banda disponível em suas portas para tráfego útil, sem impedimentos por qualquer ato acidental ou deliberado.

2. Onde for da sua alçada, os Participantes deverão tomar todas as medidas, inclusive aquelas que o IX.br venha a propor, para garantir o correto funcionamento do PTT (Ponto de Troca de Tráfego Internet), inclusive gerenciando o tráfego Internet de maneira proativa em suas próprias redes, independente de quem tenha gerado o tráfego Internet.

3. O NIC.br reserva-se ao direito de modificar esta PUA, a qualquer momento e sem aviso prévio, sendo que será válido o documento que estiver disponível no sítio internet do IX.br (http://www.ix.br/pua). As provisões contidas nesta PUA não encerram as restrições de uso da infraestrutura de redes e serviços do NIC.br.

Prevenção de inundação da rede (*flooding*) e de ataques de negação de serviço

1. Participantes são responsáveis por monitorar apropriadamente sua redes em um regime 24 x 7 (24 horas, ou sete dias da semana) para garantir que sua utilização do IX.br não pretenda ou provoque inundação da rede (*flooding*) ou ataques de negação de serviço.

2. Para reduzir a probabilidade da ocorrência de inundação da rede (*flooding*) não intencional, ou ataques de negação de serviço deliberados, os Participantes deverão obedecer a toda a Política de Requisitos Técnicos (http://www.ix.br/requisitos) que especifica os tipos de tráfego e os tipos de pacotes que poderão ser encaminhados para o IX.br.

Acesso não autorizado ou tentativas maliciosas para comprometer a rede do IX.br

1. Nenhum serviço, sistema ou estrutura de rede do NIC.br pode ser utilizado para finalidades ilegais e/ou não éticas que violem quaisquer leis locais, estaduais, nacionais ou acordos internacionais.

2. Os Participantes deverão tomar medidas razoáveis para prevenir o acesso não autorizado ou tentativas maliciosas para comprometer a rede do IX.br.

3. Os Participantes não deverão divulgar informações a terceiros não autorizados, que venham a auxiliá-los a comprometer a rede do IX.br, incluindo informações confidenciais privilegiadas fornecidas aos Participantes, assim como informações de uso geral, ainda não em domínio público, sobre o IX.br que possam ser úteis a terceiros não autorizados.

4. Violações de sistemas e segurança da rede são proibidas. Ao NIC.br se reserva o direito de divulgar os contatos dos Participantes envolvidos em violações de segurança aos outros Participantes, de forma a ajuda-los a resolver os incidentes de segurança. O NIC.br também irá cooperar com as investigações promovidas pelas autoridades legais.

5. Exemplos de violações de segurança de sistemas ou da rede:

    a. Utilizar o IX.br para comprometer ou manipular recursos de sistemas ou de contas na infraestrutura do IX.br ou em outro local;

    b. Uso ou distribuição de ferramentas projetadas para comprometer a segurança. Exemplos deste tipo de ferramentas são programas para o descobrimento de senhas, ferramentas de invasão ou ferramentas de sondagem (*probes*);

    c. Acesso não autorizado a, ou uso de dados, de sistemas ou redes. Isto inclui qualquer tentativa de sondagem, varredura ou teste de vulnerabilidades de sistemas, redes ou falhas de segurança;

    d. Monitoração não autorizada de dados ou tráfego em qualquer rede ou sistema sem a expressa autorização do proprietário do sistema ou da rede;

    e. Forjar qualquer pacote TCP/IP ou cabeçalho de pacote ou qualquer parte da informação do cabeçalho em postagem via e-mail ou grupo de notícias;

6. O NIC.br se reserva o direito de desconectar todas as portas envolvidas em atividades maliciosas, e/ou varredura de portas.