

FURB Internet eXchange Point

Documento: Política de Uso Aceitável

Versão: 1.0.0

Última modificação: 30 de outubro de 2018

Créditos: Este documento foi baseado na Política de Uso Aceitável (PUA) do IX.br, disponível em <http://ix.br/documentacao>, Política de Uso Aceitável.

Sobre o conteúdo

1. O FURB-IX 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 FURB-IX não se responsabiliza por ele. O FURB-IX só pode ser responsabilizado por seu próprio conteúdo.

Itens Gerais

3. Onde for da sua alçada, os Participantes deverão tomar todas as medidas, inclusive aquelas que o FURB-IX venha a propor, para garantir o correto funcionamento do IX (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.
4. O FURB-IX reserva-se ao direito de modificar esta PUA, a qualquer momento com aviso prévio aos participantes, sendo que será válido o documento que estiver disponível no sítio internet do FURB-IX (<http://ix.furb.br/documents>).

5. As provisões contidas nesta PUA não encerram as restrições de uso da infraestrutura de redes e serviços do FURB-IX.

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

6. Os Participantes são responsáveis por monitorar apropriadamente suas redes em um regime 24 x 7 (24 horas, ou sete dias da semana) para garantir que sua utilização do FURB-IX não pretenda ou provoque inundação da rede (*flooding*) ou ataques de negação de serviço.
7. 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.furb.br/documents>) que especifica os tipos de tráfego e os tipos de pacotes que poderão ser encaminhados para o FURB-IX.

Acesso não autorizado ou tentativas maliciosas para comprometer a rede do FURB-IX

8. Nenhum serviço, sistema ou estrutura de rede do FURB-IX pode ser utilizado para finalidades ilegais e/ou não éticas que violem quaisquer leis locais, estaduais, nacionais ou acordos internacionais.
9. Os Participantes deverão tomar medidas razoáveis para prevenir o acesso não autorizado ou tentativas maliciosas para comprometer a rede do FURB-IX.
10. Os Participantes não deverão divulgar informações a terceiros não autorizados, que venham a auxiliá-los a comprometer a rede do FURB-IX, incluindo informações confidenciais privilegiadas fornecidas aos Participantes, assim como informações de uso geral, ainda não em

domínio público, sobre o FURB-IX que possam ser úteis a terceiros não autorizados.

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

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

- a. Utilizar o FURB-IX para comprometer ou manipular recursos de sistemas ou de contas na infraestrutura do FURB-IX 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;

13. O FURB-IX se reserva o direito de desconectar todas as portas envolvidas em atividades maliciosas, e/ou varredura de portas.