

ANEXO 9

TRATAMENTO CONJUNTO DE COMBATE E PREVENÇÃO A FRAUDE

1. OBJETIVO

- 1.1 Disciplinar o tratamento a ser dispensado às Fraudes e Ataques relacionados ao tráfego objeto do Contrato, especialmente nos aspectos da ação coordenada de sua prevenção e controle.
- 1.2 Será premissa para essa ação a identificação de todos os terminais classificados em situação de fraude, conforme definições abaixo, bem como definir procedimentos para a identificação de tráfego fraudulento, seja esse de origem ou destino.

2. DEFINIÇÕES, TIPOS E TERMOS

2.1 Definição de Fraude:

Conceito Objetivo

Subterfúgio para alcançar um fim ilícito, ou ainda, o engano dolosamente provocado, o malicioso induzimento em erro ou aproveitamento de pré-existente erro alheio, para o fim de enriquecimento ilícito.

Conceito Subjetivo

Obtenção ou uso de um produto/serviço de telecomunicações com a pré-disposição de não realizar o pagamento integral ou parcial do produto/serviço utilizado ou ainda gerar cobrança indevida a terceiros.

A fraude pode objetivar o benefício do anonimato, ganho financeiro ou apenas economia para o usuário.

A fraude se distingue da inadimplência.

- 2.2 Fraude – obtenção ou uso de um produto/serviço de Telecomunicações com a pré-disposição de não realizar o pagamento integral do produto/serviço utilizado ou ainda gerar cobrança indevida à terceiros. A fraude pode objetivar o benefício do anonimato, ganho financeiro e/ou economia para aquele que se utiliza da fraude.
- 2.3 Ataque – consiste na origem indiscriminada de ações de acesso a endereços IP de qualquer ponto da rede Internet, com a finalidade de congestionar redes de clientes corporativos, provedores ou usuários da Internet, através de sobrecarga aplicada à infraestrutura ou elemento de rede.
- 2.4 Ataque de Negação de Serviço – ataque provocado por “*hacker*” com o objetivo de tornar inacessível, ou mesmo bloqueado, um servidor ou elemento de rede IP, por solicitação excessiva de processos, resultando na paralisação de sua operação.
- 2.5 Lista Negra – lista de terminais de cada PARTE que estão sofrendo ação de restrição pelas áreas de Anti-Fraude das PARTES.

3. OBRIGAÇÕES DAS PARTES

- 3.1.** Manter pessoal técnico capacitado para interagir na detecção, localização e isolamento de Fraudes, Ataques e ações prejudiciais à segurança das redes, observado o disposto no Anexo 7 do Contrato.
- 3.2.** Atuar, quando requisitada pela outra PARTE, nos procedimentos de controle e no desenvolvimento de ações, tão logo venha ocorrer e sejam identificadas situações de fraude relacionadas ao tráfego entre as redes IP das PARTES.
- 3.3.** Atender por telefone às solicitações de ações cooperativas da outra PARTE, sempre que solicitada pela outra PARTE, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e durante todo o ano, incluindo sábados, domingos e feriados.

4. COMUNICAÇÕES ENTRE AS PARTES

- 4.1** Todas as notificações, relatórios e outros comunicados relacionados a este Anexo deverão ser efetuados por e-mail, ou, na indisponibilidade deste, por telefone, para os seguintes destinatários:

| TIM | | | |
|-------------|---------|---------|----------|
| Nível | Contato | Posição | Telefone |
| Primeiro | | | |
| Segundo | | | |
| Terceiro | | | |
| Quarto | | | |
| | | | |
| ¢OPERADORA¢ | | | |
| Nível | Contato | Posição | Telefone |
| Primeiro | | | |
| Segundo | | | |
| Terceiro | | | |
| Quarto | | | |

5. PROCEDIMENTOS OPERACIONAIS

4.1. Cada PARTE adotará os Procedimentos Operacionais descritos abaixo:

- 4.1.1.** Manter Sistema de Controle de Ataques e Fraudes na sua rede, investigando ou tratando os incidentes de forma pragmática, informando a outra PARTE e bloqueando quando do comprometimento da infra-estrutura de rede.
- 4.1.2.** Comunicar à outra PARTE sempre que os incidentes de Ataque ou Fraude identificados em sua rede possam afetar a rede da outra PARTE, com as informações mínimas necessárias, conforme modelo e procedimentos definidos entre as PARTES.
- 4.1.3.** A PARTE que identificou o incidente de Ataque ou Fraude (“PARTE Fraudada”) deverá enviar comunicação à outra PARTE (“PARTE Fraudadora”) em até 24 (vinte e quatro) horas, para que a mesma efetive o saneamento do incidente no prazo de 5 (cinco) dias úteis.
- 4.1.4.** A PARTE Fraudadora deverá buscar a identificação das fontes dos Ataques ou Fraudes com base na comunicação da outra PARTE, fazendo os bloqueios cabíveis para sanear seus efeitos.
- 4.1.5.** Caso a PARTE Fraudadora não resolva o incidente de Ataque ou Fraude no prazo estipulado no item 4.1.3 acima, ficará sujeita ao bloqueio do respectivo tráfego nas rotas de interconexão pela PARTE Fraudada.
 - 4.1.5.1.** O bloqueio referido no item 4.1.5 acima deverá ser precedido de denúncia pela PARTE Fraudada junto à ANATEL.
- 4.1.6.** Sempre que houver necessidade, as PARTES poderão informar suas Listas Negras, conforme modelo e procedimento a ser definido entre as PARTES.

6. DISPOSIÇÕES GERAIS

- 6.1.** Os Procedimentos Operacionais podem ser revistos a qualquer momento, desde que acordados mutuamente entre as PARTES.
- 6.2.** Quaisquer alterações nos Procedimentos Operacionais, definidos neste Anexo, antes de serem aplicados, deverão ser formalizadas por meio de aditivo ao Contrato.
- 6.3.** Qualquer acionamento de agências de segurança pública ou privada, por qualquer das PARTES, quando de atuação de investigação em terminais da outra PARTE para tratamento de casos de Fraude, deverá ser reportado previamente à outra PARTE, com objetivo de dar conhecimento e buscar informações adicionais, mantendo-se o devido sigilo destas informações.