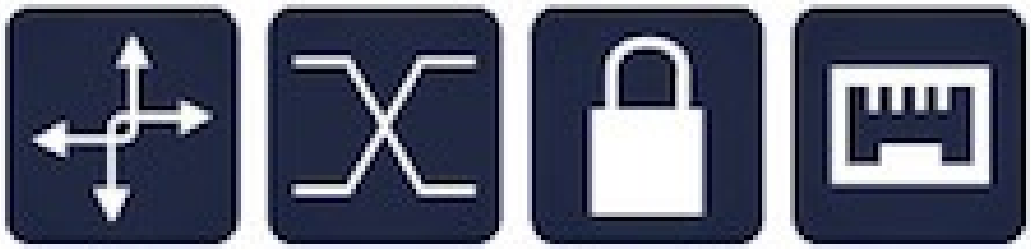
Marco Civil da Internet – Aplicações Práticas na Operação

22/05/2018

Fernando Frediani



GTER 45

GTS 31

Disclaimer

- **O material contido nesta apresentação é resultado de minha própria interpretação com base na aplicação no dia a dia de gestão técnica e operacional como também em consultas e discussões com outros colegas profissionais tanto da área técnica quando do direito acerca do assunto.**

- **Em caso de disputa judicial ou extrajudicial envolvendo o assunto aqui abordado recomenda-se fortemente a contratação de profissional do direito especialista no assunto.**

- **Eu não garanto que as informações apresentadas aqui são livres de erros e não posso me responsabilizar por perdas e danos causados pelo seu uso.**

Tópicos Abordados

- Histórico
- Sobre o Marco Civil / Objetivos
- Sobre o Marco Civil / Destaques
- Casos Práticos
  - Bloqueio da Porta 25 / Bloqueio de ataque DDoS
  - Bloqueio de Portas Entrantes
  - Redirecionamento de DNS Recursivo
  - Utilização de Serviços de cache HTTP e similares
  - Hospedagem de Servidores de CDN
  - Obrigações de quem fornece conexões de Internet mas não é AS.
  - Lei Estadual de SP
  - LOGs
    - O que deve ser logado ?
      - Provedores de Acesso
      - Provedores de Aplicação
      - CGNAT
    - O que NÃO deve ser logado ?
- Configurações de Aplicações
- Referências

Histórico

- Surgiu em 29/10/2009 através do lançamento de um processo colaborativo para construção de um marco regulatório da Internet no Brasil.
- Enviado pela Presidência da República à Câmara dos Deputados em 24/08/2011
- Aprovado pela Câmara dos Deputados em 25/03/2014
- Aprovado pelo Senado em 22/04/2014
- Sancionada pela Presidente da República em 23/04/2014 durante a conferência NETmundial (Lei 12.965 de 23 de Abril de 2014)
- Decreto de Regulamentação editado em 11/05/2016 (Decreto N°8.771 de 11 de Maio de 2016)

Sobre o Marco Civil / Objetivos

- **Contém 32 artigos divididos em 5 capítulos**
  - Disposições preliminares, Da provisão de conexão e aplicações de internet; Da atuação do poder público; Disposições finais

- **Princípio da Neutralidade (Art. 9°)**
  - Significa que todas as informações que trafegam na rede devem ser tratadas da mesma forma, sem distinção, navegando à mesma velocidade (velocidade de contratação).

- **Acesso à logs de aplicações e de conexões de acesso (Art. 13°)**
  - Deve ser condicionada à previa decisão judicial fundamentada.

- **Responsabilidade dos Provedores**
  - Isenta os provedores de serem responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros (Art. 18°).
  - Obriga os provedores de Acesso e Aplicação à guarda de logs com fins de identificação do usuário.

Sobre o Marco Civil / Destaques

- **Neutralidade**
- **Art. 9° O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.**

§ 1° A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.

(...)

§ 3° Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Sobre o Marco Civil / Destaques

- **Art. 13° - Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.**

- (…)

- § 2° A autoridade policial ou administrativa ou o Ministério Público poderá
- requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
- § 3o Na hipótese do § 2o, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.

- (…)

- § 5° Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

Sobre o Marco Civil / Destaques

- **Art. 14° Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.**

- **Art. 15° O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.**

- **Art. 19° Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente ressalvadas as disposições legais em contrário.**

Casos Práticos

- **Bloqueio da Porta 25 (Anti SPAM)**
- **Bloqueio e Prevenção de ataques DDoS**

  - Art. 9° proíbe a distinção por conteúdo, origem e destino e serviço utilizado porém o § 1° do mesmo artigo diz que as exceções serão regulamentadas em Decreto específico pelo Presidente da República, ouvidos o CGI.br e ANATEL.

  - Disciplina ainda que somente podem ocorrer por:
    - I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e
    - II - priorização de serviços de emergência.

Casos Práticos / Bloqueio porta 25 e Ataques DDoS

- **Do Decreto de Regulamentação do Marco Civil**
- (Decreto 8.771 de 11 de Maio de 2016)
- Art. 5° Os requisitos técnicos indispensáveis à prestação adequada de serviços e aplicações devem ser observados pelo responsável de atividades de transmissão, de comutação ou de roteamento, no âmbito de sua respectiva rede, e têm como objetivo manter sua estabilidade, segurança, integridade e funcionalidade.

§ 1° Os requisitos técnicos indispensáveis apontados no caput são aqueles decorrentes de:

I - tratamento de questões de segurança de redes, tais como restrição ao envio de mensagens em massa (spam) e controle de ataques de negação de serviço;
II - tratamento de situações excepcionais de congestionamento de redes, tais como rotas alternativas em casos de interrupções da rota principal e em situações de emergência.

Casos Práticos / Bloqueio porta 25 e Ataques DDoS

- **Exemplos de aplicação de bloqueios legítimos a fim de mitigar ataques DDoS (na entrada e saída)**:
  - Limitação do número de conexões por segundo à determinado IP ou bloco de IPs
  - Aplicação de Access Lists a fim de bloquear tráfego malicioso destinado a causar indisponibilidade do serviço.
  - Anúncios de Blackhole dos IPs alvos de ataque.
  - Redirecionamento do tráfego destinado ao(s) IP(s) à serviço de mitigação de terceiro.
  - Bloqueio de tráfego sainte que não deveria existir na Internet (e.g; SSDP)
  - Aplicação de técnicas para evitar a falsificação do endereço de origem (IP Source Address Spoofing) – BCP 38

  - **Obs**: Algumas técnicas são válidas apenas como forma de mitigar ataques de negação pelo tempo de duração do mesmo e não podem ser utilizadas para retirar funcionalidades da conexão à internet do usuário de maneira permanente com o pretexto de proteção.

Casos Práticos

Bloqueio de Portas Entrantes

- Art. 9° O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

- Também faz parte da Internet poder receber conexões entrantes mesmo em uma conexão residencial, independente do serviço ou protocolo, com exceção dos casos descritos anteriormente.

- A distinção comercial de serviços Residencias, PME, Dedicados deve ser feita através de outros detalhes como: simetria de velocidade, IP fixo, SLA maior, canal de atendimento diferenciado

Casos Práticos

Redirecionamento de DNS Recursivo

- Art. 9° O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

- Tecnicamente é recomendado ao usuário utilizar o DNS Recursivo do próprio provedor de acesso, mas e se ele deseja utilizar outro ?

- Mesmo que a intenção seja boa de baixar a latência da consulta DNS não se pode retirar a escolha do usuário de alcançar o destino desejado.

Casos Práticos

- **Utilização de serviços de Cache HTTP e similares**

  - Art. 9° O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.
  - Mesmo que a intenção seja boa de entregar o conteúdo de maneira mais rápida e eficiente ao usuário não se pode redirecioná-lo a um destino para onde ele não desejava ir.
  - Não confundir com servidores de CDNs.

Casos Práticos

Hospedagem de Servidores de CDN

- Servidores de CDN pertencem às empresas geradoras de conteúdo que os hospedam dentro do backbone do provedor através de contrato particular e mantém total controle sobre o direcionamento do usuário para consumo do próprio conteúdo portanto NÃO há nenhuma violação ao Marco Civil por parte do provedor que fornece a infraestrutura necessária.

Casos Práticos

- **Empresa Privada com Link Dedicado fornecendo conexão aos funcionários para desempenho de suas funções são obrigados a guarda de logs ?**

  - *Art. 13° - Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão*...
  - Aos olhos do Marco Civil não sendo a empresa detentor de sistema autônomo não há obrigatoriedade.

  - Art. 5°, item IV disciplina o que é um administrador de sistema autônomo: "*a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País*;"

Casos Práticos

- **E o caso de padarias, cafés, restaurantes e similares que disponibilizam conexões Wifi para seus clientes ?**

  - Mesmo caso do Art. 13° - Por não serem administradores de sistemas autônomos aos olhos do Marco Civil não há a obrigatoriedade.

  - Caberá apenas ao provedor de acesso identificar a origem daquela conexão caso requisitado na forma da lei para auxílio da investigação.

  - O contratante de conexão também não pode ser responsabilizado caso alguém utilize aquela conexão para cometimento de algum ilícito, a não ser que o responsável tenha ciência e consenta com aquele ato.

Casos Práticos / Lei Estadual - SP

- **No Estado de São Paulo existe a Lei Estadual 12.228 de 11/01/2006**

- A lei foi feita para regular a atividade de “lan houses”, “cyber offices”, cibercafés, entre outros, e que é descrito de maneira clara em seu Art. 1°

- Porém já foi aplicada pelo Judiciário de maneira equivocada para obrigar fornecedores de acesso público a internet (ex: Wifi público) a guardarem registro do cadastro dos usuários.

- Uma lei portanto controversa e que embora exista jurisprudência a respeito carece de revisão por parte de instâncias superiores da justiça quanto à sua aplicabilidade.

Casos Práticos / LOGs / Acesso

O que deve ser logado ?

- **Provedor de Acesso**
  - *Art. 13° Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.*

  - **Definição de "registros de conexão" no Art. 5°**
    - *Art. 5° Para os efeitos desta Lei, considera-se:*
    - *VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;*

Casos Práticos / LOGs / Aplicação

O que deve ser logado ?

- **Provedor de Aplicação**
  - *Art. 15° O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.*

  - **Definição de "registros de acesso a aplicações de internet" no Art. 5°**
    - *Art. 5° Para os efeitos desta Lei, considera-se:*
    - *VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP;*

Casos Práticos / LOGs

O que deve ser logado ?

- **Válido para ambos os casos, Acesso e Aplicação:**
  - O Art. 5° especifica de maneira mais detalhada o que é um endereço IP em seu item III.
  - *III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;*
  - No caso de uso de CGNAT um endereço IP é suficiente para identificar um terminal de uma rede para permitir sua identificação ?

Casos Práticos / LOGs / CGNAT

- **O que deve ser logado ?**
  - **Para permitir a identificação do usuário atrás de CGNAT é necessário possuir também o log da Porta de Origem da conexão.**
  - **Existem 2 formas mais comuns de realizar CGNAT em provedores de acesso:**
    - **Com intervalo fixo de portas**
      - Neste caso bastar guardar os logs de autenticação informando data e hora do início e término de uma conexão e qual IP de CGNAT foi atribuído àquele usuário.
    - **Com atribuição dinâmica de portas**
      - Neste caso é necessário guardar o log de todas as conexões originadas pelo usuário contendo a informação da porta de origem alocada para acesso à conexão.

Casos Práticos / LOGs / CGNAT

- **Além da Lei para aqueles detentores de SCM ou Registro na ANATEL existe também disposição administrativa da ANATEL para que os logs sirvam à identificação do usuário contemplando de maneira mais clara o CGNAT. (Resolução n° 614 de 28 de Maio de 2013).**
- Art. 53. A Prestadora deve manter os dados cadastrais e os Registros de Conexão de seus Assinantes pelo prazo mínimo de um ano.
- Art. 4º Para os fins deste Regulamento, aplicam-se as seguintes definições:
- III - Assinante: pessoa natural ou jurídica que possui vínculo contratual com a Prestadora para fruição do SCM;

XVII - Registro de Conexão: conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados, entre outras que permitam identificar o terminal de acesso utilizado;

De acordo com a Resolução 680 de 27 de Junho de 2017 que isentou pequenos provedores do SCM a mesma regras acima são válidas nesses casos, portanto independente do tamanho do provedor o log é obrigatório.

Casos Práticos / LOGs / CGNAT

- **O que NÃO deve ser logado ?**
  - **Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.**
    - Ou seja, é proibido guardar logs que identifiquem detalhes como endereço ou porta de **destino** da conexão

Configurações Aplicações

- Por padrão o Apache e o NGINX não logam a porta de origem da conexão no /var/log/ apenas o IP
- **Apache**
  - Para adicionar a porta de origem da requisição aos logs edite o arquivo **/etc/apache2/apache2.conf** e adicione o parâmetro **%{remote}p** após o %h nos Logformats vhost_combined, combined e common. Exemplo:
  - `LogFormat "%h %{remote}p %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined`
  - Exemplo do output:
  - `203.0.113.10 50181 - fernando [19/May/2018:08:31:46 -0300] "GET /index.html HTTP/1.1" 201 1126 "-" ""Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0"`
- **NGINX**
  - Edite o arquivo /etc/nginx/nginx.conf e adicione as linhas conforme o exemplo abaixo que contempla o parâmetro **$remote_port**
  - `log_format mycombined '$remote_addr $remote_port - $remote_user [$time_local] "$request" $status $body_bytes_sent "$http_referer" "$http_user_agent"';`
  - `access_log /var/log/nginx/access.log mycombined;`

Referências

- **Marco Civil da Internet**
  - http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
- **Decreto de Regulamentação do Marco Civil**
  - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm
- **Regulamentação do SCM (Resolução 614 de 28/05/2013)**
  - http://www.anatel.gov.br/legislacao/resolucoes/2013/465-resolucao-614
- **Alteração da Regulamentação do SCM (Resolução 680 de 27/06/2017)**
  - http://www.anatel.gov.br/legislacao/resolucoes/2017/936-resolucao-680
- **Lei Estadual de SP**
  - https://www.al.sp.gov.br/repositorio/legislacao/lei/2006/lei-12228-11.01.2006.html

Perguntas ?

Obrigado

Contato: fhfrediani@gmail.com