

# POSTMASTER

Com o objetivo de reduzir o volume de spam e vírus que circula na rede, e seguindo a tendência dos principais provedores da Internet, adotamos alguns mecanismos de proteção e segurança para o tráfego de e-mails, dentre eles o SPF e Reverse Lookup.

Assim, para obter garantia de entrega de mensagens em nossa rede, é importante que os servidores remetentes observem os seguintes critérios:

1 – O endereço IP do servidor precisa ser fixo e válido para a Internet.

2 – O IP do servidor de origem deve possuir configuração de DNS Reverso (PTR) apontando para um nome de domínio, que por sua vez deve cruzar para o mesmo IP, conforme RFC 1912.

3 – Caso o servidor possua registro de SPF (Sender Policy Framework) em seu DNS, o IP de origem das mensagens precisa ser, obrigatoriamente, cadastrado e autorizado nesse registro, do contrário as mensagens retornarão ao remetente acusando problemas.

3.1 – Nos casos de mensagens redirecionadas, é necessário que o servidor que efetua esse redirecionamento assuma a responsabilidade pela transmissão, ou seja, que através do sistema de SRS (Sender Rewriting Scheme), reescreva o cabeçalho do e-mail como se tivesse originando o envio, e não apenas espelhando.

4 – Mensagens com anexos de extensões que normalmente contém vírus, são automaticamente filtradas, minimizando assim a possibilidade de infecção de sua rede.

4.1 – Dentre elas: .ade, .adp, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .hta, .inf, .ins, .isp, .js, .jse, .lnk, .mdb, .mde, .msc, .msi, .msp, .mst, .pcd, .pif, .reg, .scr, .sct, .shs, .url, .vb, .vbe, .vbs, .wsc, .wsf, .wsh

4.2 – Caso necessite enviar ou receber arquivos com esses formatos, por questões de segurança indicamos o serviço de FTP, ao invés de e-mail, ou ainda envie o arquivo compactado com senha.

5 – O servidor de origem deve garantir que somente usuários autenticados consigam enviar mensagens, além de primar pelas normas básicas de segurança. Servidores que possuam relay aberto têm o acesso bloqueado.

6 – Os administradores devem configurar seus servidores para garantir o recebimento das mensagens de retorno (bounces), além de e-mails de comunicação de abusos ([abuse@seu.dominio.com.br](mailto:abuse@seu.dominio.com.br)).

7 – O número de conexões geradas pelo servidor de origem é controlado e, caso torne-se abusivo, o envio é interrompido e temporariamente bloqueado, até que o problema seja corrigido.

8 – O servidor de envio deve identificar-se de forma adequada nas conexões com nossos servidores, obedecendo as normas descritas nas RFC's 2142 e 2821.

9 – Os servidores de e-mail da G2 não permitem o acesso direto como relay para a Internet.

Casos específicos devem ser encaminhados para nossa equipe de atendimento que fará uma avaliação e indicará a melhor solução para o caso.

No interesse em conhecer mais sobre os assuntos tratados, você poderá encontrar material complementar sobre RFC no site da IETF (Internet Engineering Task Force) e sobre SPF na WIKIPEDIA, além de diversos sites de comunidades técnicas na Internet.