



Requisitos da Certificação

2018 Return Path, Inc. Todos os direitos reservados

De e-mail a gente entende

returnpath.com/pt-br

Todos os requisitos válidos a partir de 2019

Sumário

Sumário

Introdução à certificação

Torne-se certificado

Permaneça certificado

Visão geral dos requisitos da certificação

Categorização dos requisitos

Parte 1 - Modelo de negócios

Parte 2 - Mensurabilidade

Parte 3 - Infraestrutura

Parte 4 - Conteúdo da mensagem de e-mail

Parte 5 - Pontos de coleta

Parte 6 - Consentimento

Exemplos de práticas de consentimento proibidas

Parte 7 - Política de privacidade

Parte 8 - Legalidade

Parte 9 - Segurança

Parte 10 - Feedback loops (FBLs)

Parte 11 - Comunicação

Parte 12 - Desempenho e conformidade

Precisa de ajuda?

Introdução à certificação

O Return Path Certification é a whitelist mais exclusiva e poderosa do setor. Mas também é muito mais do que isso. É um programa que oferece os dados exclusivos e as vantagens em termos de provedor de e-mail de que você necessita para entregar mais e-mails, atingir mais assinantes e aumentar seus lucros.

Torne-se certificado

Nosso programa de certificação foi desenvolvido para os melhores remetentes do ramo, que satisfazem as expectativas dos assinantes e dos principais provedores de e-mail e que seguem as melhores práticas padrão do setor. Ao longo do seu processo de certificação, trabalharemos com você para assegurar que o seu programa cumpra com os nossos requisitos de programa.

Estas são as principais etapas para se tornar certificado:

1. Envie este [formulário](#) caso esteja interessado na certificação e ainda não tenha entrado em contato com a Return Path. Se você já é cliente da Return Path, procure o seu Relationship Manager ou mande um email para clientes@returnpath.com.
2. No início do processo de certificação, nós realizamos uma auditoria abrangente do seu programa de e-mail para assegurar que ele satisfaz todos os requisitos detalhados abaixo.
3. Durante a auditoria, notificaremos você caso alguma parte do seu programa de e-mail não satisfaça nossos requisitos. Para continuar com a auditoria, você precisará concluir quaisquer atualizações no prazo de 30 dias a partir da nossa solicitação. (Não se preocupe, nós forneceremos informações adicionais sobre as alterações e sobre como concluí-las.)
4. Quando você tiver feito as alterações apropriadas, finalizaremos a sua auditoria e lhe enviaremos um e-mail de ativação de conta.
5. Após você se tornar certificado, os seus IPs começarão a receber vantagens na AOL, na Microsoft, no Yahoo! e em outros provedores globais de e-mail e de segurança de e-mail.

Permaneça certificado

Como remetente certificado, você será solicitado a cumprir consistentemente com os requisitos de certificação utilizados para avaliar o seu programa durante a auditoria. O cumprimento dos requisitos de forma consistente garante que você receberá todas as vantagens do programa em termos de entregabilidade. Realizaremos verificações periódicas das condições do seu programa de e-mail para assegurar que ele continue cumprindo com nossos requisitos e para proteger o programa de certificação.

Enquanto estiver certificado, você receberá vantagens como:

- Um aumento mensurável da entrega em caixa de entrada em provedores de e-mail como Microsoft, Yahoo!, AOL e outros, inclusive durante o período crucial de festas, quando os provedores de e-mail costumam retardar e filtrar remetentes de grande volume.
- Canais de dados exclusivos dos provedores de e-mail, com informações detalhadas sobre os seus KPIs, entrega e desempenho da certificação.
- Uma equipe de conformidade dedicada 24 horas por dia, sete dias por semana, ao monitoramento, oferecendo alertas de segurança e trabalhando com você na resolução de quaisquer comprometimentos.

Compreendemos que problemas acontecem e que você pode sair da conformidade de vez em quando, o que pode resultar em uma [suspensão](#) temporária do programa, até que você entre novamente em conformidade. Contudo, se você violar os requisitos excessivamente, repetidamente ou sistematicamente, nós o notificaremos e trabalharemos com você para fazer quaisquer atualizações necessárias. Nós nos reservamos o direito de removê-lo do programa, se necessário.

Visão geral dos requisitos da certificação

Agora que você foi apresentado ao programa de certificação e sabe como se tornar e permanecer certificado, é hora de conhecer nossos requisitos de certificação. As informações listadas abaixo descrevem os requisitos que o seu programa de e-mail precisa cumprir para concluir a auditoria inicial e permanecer certificado após você ser aceito no programa.

Categorização dos requisitos

Os requisitos da certificação dividem-se em 12 partes diferentes do seu programa de e-mail, como infraestrutura ou política de privacidade. Juntos, eles proporcionam uma visão completa do seu programa de e-mail e determinam se você está qualificado para o nosso programa de certificação.

Veja a seguir as diferentes partes que verificamos e o que elas significam:

- O **modelo de negócios** explica quem você é e o que você faz
- A **mensurabilidade** ilustra quantos e-mails você envia e com que frequência os envia
- A **infraestrutura** mostra como você envia, autentica e gerencia os e-mails
- O **conteúdo da mensagem de e-mail** é como você se apresenta para os seus assinantes

- Os **pontos de coleta** mostram como você coleta endereços de e-mail
- O **consentimento** explica como os assinantes manifestam estar de acordo com o recebimento dos seus e-mails
- A **política de privacidade** documenta todos os detalhes do seu programa de e-mail
- A **legalidade** é importante para os seus negócios e confirma que você cumpre todas as leis aplicáveis, referentes a spam e privacidade dos dados, que afetam você e os seus assinantes
- A **segurança** demonstra como você cuida dos seus sistemas e dos dados de seus assinantes
- A **comunicação** indica a sua disposição e a sua capacidade de se comunicar com a Return Path
- O uso de **Feedback loops (FBLs)** mostra que você se preocupa em manter uma lista de assinantes limpa e saudável
- **Desempenho e conformidade** demonstram se o seu programa de e-mail é capaz de permanecer dentro dos limites estabelecidos pelos provedores de e-mail e assinantes

Leia a seguir para obter detalhes sobre cada seção listada acima.

Parte 1 - Modelo de negócios

Para iniciar a sua auditoria de certificação, nós examinamos o seu **modelo de negócios**. O seu modelo de negócios nos dá informações importantes sobre o seu programa de e-mail em geral e nos ajuda a determinar se você é um bom candidato à certificação.

Seguem os requisitos que o seu modelo de negócios deve preencher para se tornar e permanecer certificado:

1. Registro da empresa

- a. A sua empresa deve ser verificável por uma fonte terceirizada através de um site on-line legítimo, como um cadastro nacional, ou por um aplicativo como o Dun & Bradstreet.
- b. O registro deve incluir o endereço físico atual da sua empresa.
- c. É preciso que a sua empresa esteja operacional há pelo menos um ano.
- d. A sua empresa não deve utilizar um agente registrado para ocultar qualquer das suas informações.

2. Presença em um site

- a. A sua empresa deve estar mantendo, há pelo menos seis meses, um site válido e com páginas iniciais válidas para todas as marcas cujos e-mails de marketing serão enviados pelos IPs certificados.

3. Endereços IP e conteúdo

- a. Atualmente só certificamos IPs dedicados. Endereços IP compartilhados não se qualificam.
- b. IPs certificados só podem enviar e-mails próprios. Isso significa que IPs certificados não podem enviar e-mails de terceiros, ou seja, e-mails enviados em nome de entes não relacionados à sua marca.
- c. IPs certificados só podem enviar e-mails transacionais e comerciais. Isso significa que você não pode usar IPs certificados para enviar e-mails corporativos, que frequentemente incluem comunicações internas entre colegas de trabalho ou e-mails de suporte ao cliente.
- d. Os IPs certificados devem enviar e-mails baseados em templates e devidamente identificados com a marca. Eles não podem enviar conteúdo de formulário livre, como formulários Web ou caixas de texto abertas.

IMPORTANTE: Nós não certificaremos seus endereços IP se a sua empresa se enquadrar em uma das categorias seguintes:

- Agências
- Remetentes terceirizados
- Geração de leads
- Sites de leilão de centavos
- Atividades ilegais
- Tráfico de pessoas

Parte 2 - Mensurabilidade

Se o seu modelo de negócios satisfizer nossos requisitos, nós examinaremos a **mensurabilidade** do seu programa de e-mail. A mensurabilidade nos ajuda a compreender os seus padrões gerais de envio, incluindo a frequência com que você envia e-mails para os seus assinantes.

Seguem os requisitos de mensurabilidade que você deve cumprir para se tornar e permanecer certificado:

1. Volume consistente e mensurável

- a. O seu endereço IP deve ter enviado pelo menos 100 mensagens de e-mail para endereços Microsoft e Yahoo! (100 para cada) ao longo do período de 30 dias mais recente, conforme evidenciado nas fontes de dados da Return Path.

- b. O seu endereço IP deve manter um volume mensurável e consistente para permanecer certificado. A consistência é determinada com base no seu programa específico e no seu comportamento de envio. Os endereços IP sem volume mensurável e consistente serão suspensos após 30 dias e excluídos do programa ou do processo de candidatura após 90 dias.

2. Visando os provedores de e-mail

- a. A sua empresa não pode utilizar um único endereço IP para enviar e-mail exclusivamente para um provedor de e-mail específico da rede de consumidores ou da rede de provedores da Return Path.
*Envios ocasionais e temporários para um único destinatário podem ser tolerados em determinadas circunstâncias, mas somente mediante aprovação por escrito da Return Path.

Parte 3 - Infraestrutura

Se o seu modelo de negócios satisfizer nossos requisitos, nós examinaremos a **infraestrutura** de envio de e-mails. Isso se refere ao hardware e ao processo utilizados para a distribuição de e-mails. É fundamental que você envie e-mails a partir de sistemas de infraestrutura com boa manutenção e que utilizem as melhores práticas.

Tenha em mente que talvez seja necessário trabalhar com o seu provedor de serviços de e-mail (ESP) ou com a sua equipe interna de TI para cumprir com os requisitos listados abaixo e, com isso, tornar-se e permanecer certificado.

1. Endereço IP dedicado

- a. A sua empresa deve ser a única entidade a ter enviado e-mails pelos endereços IP dedicados por pelo menos 60 dias.

2. Retransmissão aberta

- a. A sua infraestrutura não deve ter servidor algum com [retransmissão aberta](#).

3. FCrDNS

- a. As entradas de Reverse DNS (rDNS) do seu endereço IP devem coincidir com as entradas de Forward DNS, o que se conhece como [Forward-Confirmed reverse DNS](#) (FCrDNS).

4. Blacklists

- a. Os seus domínios ou endereços IP não devem estar em uma blacklist monitorada pela Return Path. Inclusões excessivas ou reiteradas em blacklists podem resultar na suspensão ou no término dos seus benefícios de certificação. [Saiba mais sobre limites de blacklist a seguir](#)

5. SPF

- a. Todos os seus domínios “Mail From” e “Return-Path” devem ter registros [Sender Policy Framework](#) (SPF) publicados. [Saiba como configurar SPF aqui](#)
- b. Os seus registros SPF devem passar pelas verificações de autenticação dos provedores de e-mail com uma tolerância operacional razoável, conforme determinado pela Return Path.
- c. Nenhum dos domínios de envio ou de “Return-Path” deve utilizar uma diretiva `+all` ou `?all`.
- d. Nenhum dos domínios de envio ou de “Return-Path” deve incluir um registro PTR.

6. DKIM

- a. Todos os e-mails enviados pelos IPs certificados devem ter a autenticação [DomainKeys Identified Mail](#) (DKIM) configurada. [Saiba como configurar DKIM aqui](#).
- b. A sua autenticação DKIM deve passar pelas verificações de autenticação dos provedores de e-mail com uma tolerância operacional razoável, conforme determinado pela Return Path.

7. DMARC (apenas recomendação)

- a. Consideramos *altamente recomendável* implementar o DMARC ([Domain-based Message, Authentication, Reporting & Conformance](#)). Porém, isso atualmente não é um requisito para a certificação. [Saiba como configurar um registro DMARC aqui](#).

8. Contas de função

- a. Você pode configurar e manter [contas de função](#) `abuse@` e `postmaster@` em todos os domínios de envio ou de “Return-Path” para lidar com reclamações e outros problemas.
- b. Também recomendamos que você dê suporte e manutenção a outras contas de função padrão, como `support@` ou `help@`.

9. Registros WHOIS

Os seus registros WHOIS devem satisfazer os seguintes critérios em todos os domínios de

envio, domínios de “Return-Path” e domínios de sites associados ao e-mail enviado a partir dos seus endereços IP.

- a. A sua empresa deve manter registros WHOIS atualizados.
- b. Os seus registros WHOIS devem conter a razão social da sua empresa. Para os registros WHOIS do seu domínio de “Return-Path”, a razão social pode ser a do seu provedor de serviços de e-mail (ESP), se aplicável.
- c. Os seus registros WHOIS devem listar pelo menos um método de contato, como um telefone ou um endereço de e-mail.
- d. Os seus registros WHOIS devem conter um endereço postal atual da sua empresa, que não seja uma caixa postal.
- e. O seu registro WHOIS não deve ocultar informações da sua empresa por meio do uso de serviços de proxy ou privacidade.
- f. [Veja um exemplo e saiba mais sobre registros WHOIS aqui](#)

10. Manutenção da lista

- a. A sua empresa deve utilizar sistemas de manutenção de lista de endereços para receber e processar confiavelmente erros de entrega, mensagens devolvidas e outras respostas das redes receptoras (bounces).
- b. Você deve processar as devoluções permanentes (bounces definitivos) das mensagens de e-mail enviadas através dos seus endereços IP removendo de todos os envios futuros esses endereços de e-mail para os quais não é possível entregar mensagens.

Parte 4 - Conteúdo da mensagem de e-mail

Se a sua infraestrutura satisfizer nossos requisitos, nós examinaremos o **conteúdo das suas mensagens de e-mail**. Basicamente, nós asseguramos que o seu e-mail siga as melhores práticas, conforme determinado pelos provedores de e-mail. Isso inclui transparência com os seus assinantes quanto a quem você é.

Seguem os requisitos de conteúdo da mensagem de e-mail que você deve cumprir para se tornar e permanecer certificado:

1. Marca

- a. Os e-mails enviados devem utilizar claramente a marca da sua empresa para identificá-la para os assinantes.

2. Linha de assunto

- a. Todas as linhas de assunto devem ser precisas.
- b. Todas as linhas de assunto devem estar claramente relacionadas ao conteúdo do corpo da mensagem de e-mail, de maneira não enganosa e inequívoca.
- c. Nenhuma linha de assunto deve incluir “RES:” ou “ENC:”. O uso dessas abreviações costuma ser visto como uma tática enganosa para induzir os assinantes a abrir o e-mail como se o mesmo tivesse sido enviado por uma pessoa em vez de um remetente comercial.

3. Conteúdo do corpo do e-mail

- a. Todo o conteúdo do corpo do e-mail deve ser verdadeiro e exato.
- b. Em qualquer e-mail comercial, promocional ou transacional, você deve incluir um endereço postal válido da sua empresa.
- c. Você não deve utilizar abreviadores de URL no conteúdo do corpo do e-mail. Isso inclui, por exemplo, o uso de serviços como Bitly, TinyURL e Google URL Shortener, entre outros.
- d. Você não deve utilizar um link do tipo “denunciar spam/lixo” dentro do conteúdo do corpo do e-mail. Isso costuma ser feito por remetentes em uma tentativa de evitar reclamações por parte do provedor de e-mail.

4. Cabeçalhos de mensagem

- a. Os cabeçalhos das mensagens de e-mail não devem ser falsificados, ocultados, dúbios ou enganosos de forma alguma. Como exemplos, podemos citar o cabeçalho “Return-Path”, o cabeçalho “From”, o nome e o endereço “Friendly From” e outros.

5. Conteúdo de terceiros

[Conforme listado acima na Parte 1](#), o e-mail próprio que inclui conteúdo de terceiros (por exemplo, conteúdo patrocinado por anúncios) qualifica-se para a certificação, mas deve cumprir com os seguintes requisitos:

- a. As linhas de assunto devem fazer referência ao conteúdo próprio.
- b. Todas as mensagens de e-mail devem ser claras e inequivocamente identificadas por marca de maneira a informar serem originárias de você, o remetente certificado.
- c. A maior parte do conteúdo do e-mail deve ser marketing da sua empresa, incluindo links e logotipos.
- d. Os endereços “From” e “Friendly From” devem identificar o remetente certificado e não devem incluir nomes de terceiros.

6. Processo de descadastramento

- a. Todo e-mail comercial, promocional ou na forma de um convite enviado através do seu endereço IP deve incluir um [cabeçalho “list-unsubscribe”](#) e um link de descadastramento.
- b. As instruções para descadastramento devem ser claras, visíveis e de fácil entendimento.
- c. Os mecanismos de descadastramento devem ser de fácil uso para o destinatário que não quiser mais ser assinante do seu programa de e-mail. Mecanismos de descadastramento fáceis de usar incluem responder ao e-mail comercial ou promocional com a solicitação ou selecionar um link para descadastrar através de um processo on-line.
- d. O processo de descadastramento não deve exigir que o destinatário forneça informação alguma além de seu endereço de e-mail. Recomendamos utilizar um processo de um só clique, como ao clicar em um link.
- e. Assim que um destinatário se descadastrar do seu programa de e-mail, você não deverá mais enviar a ele qualquer e-mail comercial ou promocional. Além disso, você não deverá vender, alugar ou informar a terceiros o endereço de e-mail ou informações pessoais do destinatário.
- f. Você deve processar e concluir todas as solicitações de descadastramento no prazo de até três dias após receber a solicitação.
- g. Você deve honrar solicitações de descadastramento do seu programa de e-mail originárias de qualquer um, em caráter permanente, independentemente de terem sido iniciadas na forma de um convite. Ou até que o assinante se inscreva novamente no seu programa de e-mail. [Conheça os requisitos de adesão da certificação aqui](#)
- h. Os links de descadastramento enviados através de qualquer e-mail devem permanecer ativos e funcionais por pelo menos 60 dias a partir da data em que forem enviados.
- i. Se algum destinatário pedir para se descadastrar do seu programa de e-mail através de mecanismos de descadastramento não padronizados, você ainda assim processará prontamente a solicitação. Exemplos de mecanismos de descadastramento não padronizados são carta postal, endereços de e-mail do tipo “alias”, endereços de postmaster ou de abuso e ligações telefônicas.
- j. Você precisa incluir um link de descadastramento válido em toda pesquisa por e-mail que peça algum retorno por parte dos destinatários. No entanto, você não precisa incluir um mecanismo de descadastramento caso envie a um destinatário uma pesquisa relacionada a uma transação anterior que tenha ocorrido entre a sua empresa e o destinatário.

Parte 5 - Pontos de coleta

Uma vez que tenhamos determinado que o conteúdo e os processos de descadastramento da sua mensagem de e-mail cumprem com nossos requisitos, nós examinaremos como você coleta endereços de e-mail, ou seja, o que se entende como seus **pontos de coleta**. É

fundamental que você informe diretamente aos assinantes o tipo de e-mail no qual eles estão se inscrevendo, o que eles devem esperar e mais.

Os seus pontos de coleta devem satisfazer os seguintes requisitos:

1. Clareza e simplicidade

- a. Você deve ter uma divulgação clara e simples em todos os pontos de coleta. A inclusão de um link para a sua política de privacidade em vez de explicitar as informações não constitui cumprimento desse requisito.
- b. Você deve divulgar informações ao assinante sobre o e-mail que ele receberá quando ele entrar e enviar seu endereço de e-mail. Isso deve incluir uma definição precisa do conteúdo e de sua frequência.
- c. Você deve explicitar claramente, em todos os pontos de coleta, se compartilha ou aluga os endereços de e-mail dos seus assinantes ou quaisquer outras informações pessoais relacionadas.

2. Política de privacidade

- a. A sua política de privacidade deve ser citada clara, aberta e diretamente em todos os pontos de coleta, incluindo em aplicativos móveis. [Saiba mais sobre nossos requisitos de política de privacidade aqui](#)

Parte 6 - Consentimento

Se seus pontos de coleta passam nossos requisitos, nós revisaremos suas práticas de **permissão**. Nós queremos saber se você está pedindo e recebendo permissão de forma adequada dos seus assinantes de acordo com esses requisitos.

Aqui estão os requisitos de permissão que você deve alcançar para se tornar e se manter Certificado:

1. Métodos aceitáveis de opt-in

Você deve usar um dos seguintes métodos de opt-in quando solicitar a permissão dos seus assinantes:

- a. **Opt-in Confirmado (duplo):** Após seus assinantes fazerem o opt-in no seu programa de email, você deve enviar um email de verificação para confirmar esse cadastramento. Os assinantes devem clicar no link fornecido no email para confirmar sua inscrição antes de você enviar emails adicionais.

- b. **Opt-in com Notificação:** Após um cliente fazer o opt-in no seu programa de email, você deve enviar um email de notificação afirmando a inscrição e fornecendo claras instruções de opt-out, antes de enviar emails adicionais.

Para **Opt-in Confirmado** e **Opt-in com Notificação** você pode ter uma caixa de seleção pré-marcada que os usuários podem desmarcar no momento da criação de sua conta para não receber seus emails promocionais.

- c. **Outros métodos de Permissão:** se o seu programa de email se apóia em um método de permissão alternativo como sua base legal para processar dados pessoais, você precisará nos enviar a documentação para esse método, como por exemplo uma avaliação completa de interesse legítimo ou outra avaliação.

Lembrete: também é importante revisar e estar em conformidade com as leis e regulamentações aplicáveis que impactam você, sendo que estas podem ser maiores que os Requisitos do Programa de Certificação Return Path.

2. Inscrição compartilhada

Ao dar aos usuários a opção adicional de se inscreverem para receber um e-mail de terceiros ou de afiliados no seu site, você precisa cumprir com os requisitos seguintes. Esses requisitos também se aplicam a quaisquer marcas que operem sob o mesmo nome que a empresa controladora.

- a. No ponto de coleta, você deve indicar, de maneira clara e explícita, o nome da empresa cujos e-mails o destinatário está se inscrevendo para receber.
- b. Você deve definir claramente cada marca cujos e-mails o destinatário pode estar se inscrevendo para receber. Você também deve ter opções de adesão separadas, como caixas de seleção previamente desmarcadas. Esse requisito também se aplica a marcas que operem sob o mesmo nome que a empresa controladora.
- c. Você deve ter a capacidade de produzir provas de consentimento onde quaisquer endereços sejam coletados. As provas de consentimento devem incluir data, hora, endereço IP de origem e localização (URL).

3. E-mails encaminhados para amigos e iniciados na forma de um convite

- a. O formulário de inscrição deve incluir CAPTCHA ou reCAPTCHA para verificar a legitimidade do amigo que iniciou o e-mail. CAPTCHA e reCAPTCHA ajudam a evitar bots ou usuários exploradores.
- b. Você pode enviar apenas um e-mail promocional ou comercial de encaminhamento para um amigo para o endereço especificado.

- c. Se um destinatário do e-mail de encaminhamento para um amigo não responder, você só poderá enviar um único e-mail adicional.
- d. Os domínios “Return-Path” e “Mail-From” (MFrom), listados no cabeçalho do e-mail, devem ser domínios de sua propriedade.
- e. Você deve oferecer aos destinatários uma maneira destes se descadastrarem de todos os e-mails futuros, o que normalmente se chama de descadastramento global.
- f. Os e-mails não devem conter links ou URLs para endereços Web externos.
- g. Os e-mails podem incluir comentários personalizados de até 140 caracteres.
- h. Um usuário individual só pode utilizar esse recurso para enviar, no máximo, 100 mensagens em um período de 24 horas.
- i. Para enviar mais e-mails comerciais ou promocionais para destinatários de e-mail de encaminhamento para um amigo, é preciso que o destinatário se inscreva no seu programa de e-mail utilizando um dos métodos de adesão indicados acima.

Exemplos de práticas de permissão proibidas

- Opt-in simples pré-marcado (sem notificação)
- Opt-in simples (sem notificação)
- Colheita de lista
- Compra ou aluguel de lista, assim como acrescentar email em uma lista
- Prospecção de Email

Parte 7 - Política de privacidade

Se as suas práticas de consentimento satisfizerem nossos requisitos, nós examinaremos a sua **política de privacidade**. É importante observar que as suas políticas de privacidade devem respeitar quaisquer leis aplicáveis. Além disso, nós asseguramos sua total transparência com assinantes em potencial no que se refere ao seu programa de e-mail, a como eles podem contactar você e a quais dados você coleta.

Seguem os requisitos de política de privacidade que você deve cumprir para se tornar e permanecer certificado:

1. Estar facilmente acessível

- a. A sua política de privacidade deve estar facilmente acessível na página inicial do seu site.

2. Instruções de descadastramento

- a. A sua política de privacidade deve incluir instruções claras e diretas que digam aos usuários como eles podem se descadastrar do seu programa de e-mail.

3. Endereço físico

- a. A sua política de privacidade deve incluir um endereço físico da sua empresa e de quaisquer empresas parceiras. Caixas postais são aceitáveis, embora os assinantes prefiram endereços postais.

4. Ponto de coleta

- a. A sua política de privacidade deve refletir com precisão as práticas da sua empresa, quando citada nos pontos de coleta. Por exemplo, você deve divulgar como um endereço de e-mail será utilizado após coletá-lo.

5. Divulgação dos dados

- a. A sua política de privacidade deve informar aos destinatários todas as informações pessoais que a sua empresa coleta e como elas podem ser compartilhadas.

6. Propriedade da marca

- a. Caso represente uma empresa controladora detentora de diversas marcas, você deve incluir uma lista de quaisquer outras marcas de sua propriedade em cada política de privacidade.
- b. Caso represente uma marca pertencente a uma empresa controladora, você precisa incluir o nome da empresa controladora na sua política de privacidade.

Parte 8 - Legalidade

Como empresa, é importante que você cumpra quaisquer **leis e regulamentos** aplicáveis que possam afetá-lo. Cada país e cada território têm uma legislação relacionada a práticas de dados e de e-mail. É imperativo que você cumpra e obedeça plenamente essas leis e regulamentos, onde quer que você atue.

Exemplos incluem, sem se limitar a:

- Estados Unidos da América: [Lei “Controlling the Assault of Non-Solicited Pornography And Marketing” \(CAN-SPAM\) de 2003](#)
- Canadá: [“Canada's Anti-Spam Legislation” \(CASL\)](#)
- União Europeia: [GDPR \(Regulamento Geral sobre a Proteção de Dados\)](#)

- Austrália: [“Spam Act” de 2003](#)

Parte 9 - Segurança

Continuando com a sua auditoria, nós examinaremos as suas **práticas de segurança**. É importante que a sua empresa adote medidas adequadas e específicas do setor para manter o seu banco de dados e seus sistemas seguros, de modo a proteger sua infraestrutura e seus assinantes.

Seguem os requisitos de segurança que você deve cumprir para se tornar e permanecer certificado:

1. Infraestrutura

- a. A sua infraestrutura de e-mail deve ser mantida e operada de maneira responsável.

2. Proteção dos assinantes

- a. A sua empresa deve utilizar políticas e procedimentos padrão do setor para resguardar e proteger os endereços de e-mail de seus assinantes e quaisquer outras informações de identificação pessoal (PII).

3. Sistemas seguros

- a. A sua empresa deve seguir procedimentos padrão do setor para evitar proxies abertos, retransmissões abertas, vírus de computador, worms, spyware, adware, cavalos de Troia, recursividade de DNS ou qualquer outro item identificado como malware na sua infraestrutura.

4. Comprometimentos

- a. Você deverá notificar à Return Path por escrito, em até dois dias úteis, caso descubra que o seu IP ou domínio foi comprometido.
- b. Caso o seu IP ou domínio venha a ser comprometido, você concorda que o IP ou domínio não deverá ser reativado no programa de certificação até que um funcionário da Return Path conclua uma revisão e determine que a causa do comprometimento foi devidamente mitigada.

Parte 10 - Feedback loops (FBLs)

Como uma melhor prática, nós recomendamos que você se inscreva em todos os feedback loops (FBLs) disponíveis para gerenciar e reduzir efetivamente as reclamações. Uma lista completa de FBLs pode ser encontrada [aqui](#).

Se por algum motivo você não puder se inscrever em todos os FBLs dessa lista, eis alguns feedback loops que você deve acompanhar para se tornar e permanecer certificado:

- Feedback loop sobre IPs e domínios do Comcast
- Yahoo! Feedback loop
- JMRP (Junk Mail Reporting Partner Program) da Microsoft
- Feedback loop da AOL

Parte 11 - Comunicação

Esteja você apenas iniciando sua auditoria ou candidatura à certificação ou já esteja certificado, é importante que haja uma comunicação clara e aberta entre a sua empresa e a Return Path.

Seguem os requisitos de comunicação que você deve cumprir para se tornar e permanecer certificado:

1. Resolução de problemas

- a. Para resolver quaisquer problemas relacionados à certificação, você e qualquer equipe envolvida com o envio de e-mail deverão cooperar com os administradores da certificação.
- b. Você deve responder a qualquer notificação do programa no prazo de três dias e deve iniciar quaisquer ações necessárias no prazo de 10 dias a partir da notificação.

2. Informações de contato

- a. Você deve manter informações de contato atualizadas com a Return Path.

Parte 12 - Desempenho e conformidade

Permanecer certificado de maneira regular e consistente depende muito de assegurar que o seu programa de e-mail se mantenha dentro de nossos limites de desempenho. Mantendo-se dentro dos limites listados abaixo, você obtém vantagens junto aos provedores de e-mail

correspondentes, melhorando sua entregabilidade geral e, em última instância, atingindo mais dos seus assinantes.

Observação: Nós trabalhamos ativamente com nossos parceiros para determinar limites e suspensões.

Você precisa cumprir os seguintes requisitos de desempenho para se tornar e permanecer certificado:

Limites de conformidade Microsoft SRD para IPs individuais

Volume SRD	0-4	5-10	11 ou mais
Taxa SRD	Não imposta	5 votos de lixo	45%

Limites de conformidade do Microsoft SRD em grupo

Volume SRD	0-9	10-30	31-50	51 ou mais
Taxa SRD	Não imposta	75%	65%	55%

Observação: Nós imporemos o padrão SRD em grupo caso você tenha dois ou mais Ips certificados.

Dica: Problemas com as suas taxas Microsoft SRD? Confira [estes materiais](#).

Limites de conformidade para reclamações, traps e blacklists

Microsoft: Taxa de reclamações (média de 30 dias)	Todos os volumes de envio 0,2%
Yahoo!: Taxa de reclamações de caixa de entrada (média de 30 dias)	Todos os volumes de envio 0,6%
AOL: Taxa de reclamações (média de 30 dias)	Não é mais obrigatório*
Comcast: Taxa de reclamações (média de 30 dias)	Todos os volumes de envio 0,3%
Spam Traps (acumulado de 30 dias)	Três ocorrências de traps críticas Cinco ocorrências de traps significativas

Rede de traps 1 da RP (acumulado de 30 dias)	100 ocorrências de traps
Traps do Cloudmark (acumulado de 30 dias)	100 ocorrências de traps
Taxa de reclamações do Cloudmark (média de 30 dias)	Todos os volumes de envio 1,0%
Blacklists (inclusão atual)	Uma inclusão crítica Duas inclusões significativas

*A Return Path parou de impor a conformidade para a AOL em 18/1/19 devido à migração da empresa Oath ou à consolidação das infraestruturas do Yahoo e AOL. Os dados da AOL continuarão aparecendo na interface do usuário de Certificação e no DPR, embora os dados da AOL diminuam com o tempo até que não haja mais dados específicos a serem relatados. Você notará uma diminuição constante nos dados da AOL juntamente com um aumento constante nos dados do Yahoo. Para mais informações sobre a migração, clique [aqui](#).

Observação: A certificação só impõe limites de taxa de reclamações do provedor de e-mail quando você recebe um número mínimo determinado de reclamações em provedores de e-mail específicos:

- Microsoft: 200 reclamações
- Yahoo!: 200 reclamações
- Comcast: 100 reclamações
- Cloudmark: 100 reclamações

Precisa de ajuda?

Para obter mais insights sobre a certificação e seus requisitos ou para saber como resolver problemas de entregabilidade e reputação, visite nossa [Central de ajuda](#).