

Política Anti-Spam

Envie mensagens que as pessoas esperam receber.

O essencial para consulta

- Envio legítimo exige origem e finalidade justificadas.
- Lista comprada não prova autorização.
- Protegemos a entrega sem prometer bloqueio perfeito.

Resumo de consulta. As cláusulas completas abaixo prevalecem.

1. Escopo e mensagens proibidas

A política vale para e-mail, formulários, contas e automações nos recursos Zovvi. É proibido enviar spam, phishing, malware, golpes, falsificar origem ou abusar de encaminhamentos. Spam não se define apenas pela quantidade: mensagem individual também pode ser abusiva. Contas comprometidas devem ser contidas e corrigidas, mesmo sem intenção do titular.

2. Base de destinatários e identificação

O remetente deve demonstrar origem legítima da lista, finalidade compatível e base legal adequada. Consentimento, quando usado, deve ser verificável e específico. Listas compradas, extraídas automaticamente ou de origem desconhecida não provam autorização para marketing.

Identifique corretamente remetente, domínio e assunto. Não oculte publicidade como mensagem urgente de segurança ou cobrança. Mensagens transacionais devem corresponder a uma relação real e não servir de pretexto para campanha não solicitada.

3. Descadastro e higiene

Marketing deve permitir recusa simples e funcional, sem exigir senha para sair da lista. A oposição ou revogação aplicável precisa ser respeitada antes de novos envios. Lista de supressão pode manter o mínimo necessário para não reincorporar quem recusou.

Remova endereços inválidos e trate devoluções e reclamações. Não tente reenviar continuamente a quem bloqueou ou se descadastrou. A ausência de reclamações não comprova origem legítima da base.

4. Autenticação e limites

Configure SPF, DKIM e DMARC conforme o provedor e proteja credenciais e formulários. A hospedagem comum não equivale a plataforma de disparo em massa. Quantidades, horários e recursos dependem do plano informado; não existe autorização para contornar filas com múltiplas contas.

Filtros, reputação e políticas do destinatário podem afetar entrega. Não garantimos chegada à caixa principal nem ausência completa de spam. Liberação de remetentes não deve desativar indevidamente proteções contra malware e falsificação.

5. Investigação e regularização

Diante de indícios, podemos limitar envio, colocar mensagens em fila ou isolar a conta proporcionalmente ao risco. A análise considera cabeçalhos, logs necessários, origem, reclamações e comprometimento, com confidencialidade e minimização. Não se deve suspender toda a operação se uma medida menor for suficiente.

O responsável recebe orientação de causa, correção e revisão quando possível. Reativação pode exigir troca de credenciais, correção da aplicação, comprovação da origem e ajuste de volume. Fraude ou reincidência grave podem levar a encerramento conforme AUP e lei.

6. Como denunciar

Use Denunciar Abuso ou ola@zovvi.com.br. Informe data, remetente, destinatário e cabeçalhos relevantes, removendo senhas, códigos e informações desnecessárias. Não encaminhe anexos maliciosos para provar o caso. O relato é analisado; recebimento não comprova infração. O afetado pode apresentar contexto e pedir revisão, preservados os direitos legais.