2025

# PROTEGENDO SEU DOMÍNIO CONTRA ATAQUES CIBERNÉTICOS

Um guia sobre SPF, DKIM, DMARC e mais.




WWW.LATUSEGUROS.COM

latú
Seguros

**PROTEJA SUA PRESENÇA ONLINE**

# Proteja seu domínio e a reputação da sua marca com **passos simples para evitar ameaças digitais**!

A proteção online da sua presença começa com medidas simples, mas incrivelmente eficazes. Configurar corretamente os **registros SPF, DKIM e DMARC** é um passo essencial para garantir que sua organização permaneça segura, confiável e respeitada no ambiente digital.

01

## **SPF** (Sender Policy Framework).

Um guia prático para configurar o SPF e proteger seu domínio contra spoofing, melhorar a entregabilidade de e-mails e preservar sua reputação digital.

02

## **DKIM** (Domain Keys Identified Mail).

Um passo a passo para configurar o DKIM, garantindo autenticidade, proteção contra falsificação e maior confiança nas suas comunicações por e-mail.

03

## **DMARC** (Domain-based Message Authentication, Reporting, and Conformance).

Um guia completo para configurar o DMARC, protegendo seu domínio contra spoofing e phishing, enquanto monitora e ajusta suas políticas de segurança.

04

## Consequências de **configurações ineficazes**.

Uma visão essencial sobre como proteger seu domínio e evitar riscos como phishing, baixa entregabilidade e impactos financeiros.

05

## Melhore a entregabilidade dos seus e-mails e evite o spam.

Uma abordagem estratégica para proteger sua marca, garantindo que cada mensagem enviada se transforme em uma conexão bem-sucedida.

**Boa leitura!**

# 1 SPF (Sender Policy Framework)

O SPF **previne a falsificação de e-mails, verificando se os servidores de envio são autorizados**. Ele funciona por meio de um registro DNS que lista os endereços IP permitidos para enviar mensagens em nome do seu domínio.

## Por que usar SPF?

**Evita spoofing:**
impede que invasores enviem e-mails falsos em nome do seu domínio.

**Melhora a reputação:**
as mensagens autenticadas têm menos chance de serem marcadas como spam.

**Aumenta a entregabilidade:**
garante que e-mails legítimos cheguem à caixa de entrada.

## Como funciona o SPF?

Simplificando, o Sender Policy Framework é um **mecanismo de segurança criado para evitar que terceiros mal-intencionados enviem e-mails em seu nome**. O mecanismo se baseia na comunicação entre servidores DNS. Por exemplo: você enviou um e-mail para o Bob. Mas como o servidor DNS do Bob sabe que o e-mail foi realmente enviado por você? A resposta é que ele não sabe, a menos que você tenha configurado o SPF no seu servidor DNS. O SPF define quais endereços IP podem ser usados para enviar e-mails a partir do seu domínio.

## **Como configurar** corretamente o SPF:

1 | **Defina servidores de envio autorizados:** liste todos os endereços IP e domínios autorizados a enviar e-mails em nome do seu domínio.

2 | **Use o mecanismo `"all"`:** especifique o que deve acontecer com e-mails de fontes não autorizadas. Por exemplo, usar `-all` indica que todas as outras fontes devem ser consideradas fraudulentas.

3 | **Crie um registro TXT no DNS do seu domínio.**

EXEMPLO DE REGISTRO SPF:

```
v=spf1 ip4:192.168.1.1 ip6:2001:db8::1 a mx -all
```

Este registro indica:

- Apenas o endereço IPv4 `192.168.1.1` e o IPv6 `2001:db8::1` estão autorizados a enviar e-mails em nome do domínio.
- A inclusão de `a` e `mx` permite que servidores associados ao domínio e registros MX (Mail Exchange) também enviem e-mails.
- O parâmetro `-all` especifica que qualquer outro servidor será considerado não autorizado.

Por exemplo, **se você estiver usando o Google Apps para enviar todos os e-mails do seu domínio**, a linha seria semelhante a esta:

```
v=spf1 include: _ spf.google.com ~all
```

Aqui, o `include:_spf.google.com` autoriza os servidores do Google a enviar e-mails em nome do seu domínio.

4 | **Inclua aplicativos que enviam e-mails em seu nome:** certifique-se de que quaisquer aplicativos que utilizem servidores SMTP próprios sejam adicionados ao seu registro SPF.

---

## Quais **aplicativos** devem fazer parte do seu registro SPF?

O conceito principal é garantir que quaisquer aplicativos que enviem e-mails em seu nome, utilizando seus próprios servidores SMTP em vez do seu, sejam incorporados ao seu registro SPF. Por exemplo, se você usa o Google Workspace para enviar e-mails do seu domínio, é essencial incluir o Google no seu registro SPF. No entanto, **é crucial garantir que apenas os aplicativos autorizados sejam incluídos** para evitar vulnerabilidades.

### **Confira o guia oficial dos fornecedores aqui:**

- Se seu fornecedor de e-mails é Microsoft, **clique aqui**.
- Se seu fornecedor de e-mails é Google, **clique aqui**.

# 2 DKIM (Domain Keys Identified Mail)

O Domain Keys Identified Mail (DKIM) **adiciona uma assinatura digital aos seus e-mails enviados, permitindo que o servidor do destinatário verifique a autenticidade do remetente**. Ele protege contra modificações nas mensagens durante o envio.

## Por que usar DKIM?

**Garante autenticidade:**
verifica que a mensagem foi enviada e não alterada pelo remetente legítimo.

**Protege contra falsificação:**
evita que terceiros manipulem suas mensagens.

**Melhora a entregabilidade:**
aumenta a confiança nos servidores de destino.

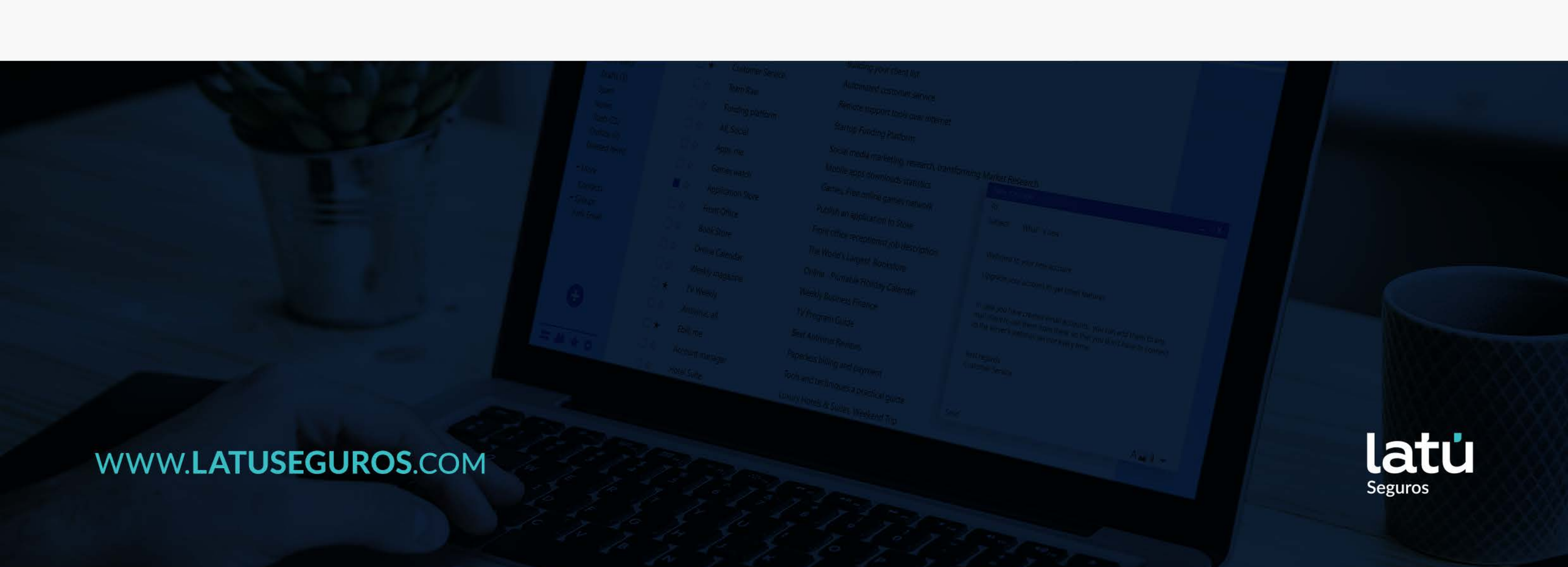
## Como funciona o DKIM?

A ideia central é baseada em criptografia e descriptografia.

**O DKIM utiliza duas chaves:**

- **Chave privada:** exclusiva para o seu domínio, usada para assinar os cabeçalhos das mensagens.
- **Chave pública:** adicionada aos registros DNS, usada pelos servidores destinatários para verificar a assinatura.

Quando você configura o DKIM, cada mensagem enviada inclui uma assinatura que pode ser validada pela chave pública.



# **Como configurar** corretamente o DKIM:

1 | **Gere as chaves DKIM:** use um gerador de chaves para criar um par de chaves (privada e pública). Armazene a chave privada com segurança no servidor de envio.

2 | **Publique a chave pública no DNS:** adicione um registro TXT.

EXEMPLO DE REGISTRO DKIM:

```
default._domainkey.example.com. IN TXT "v=DKIM1; k=rsa; p=MIGf..."
```

Este registro informa:

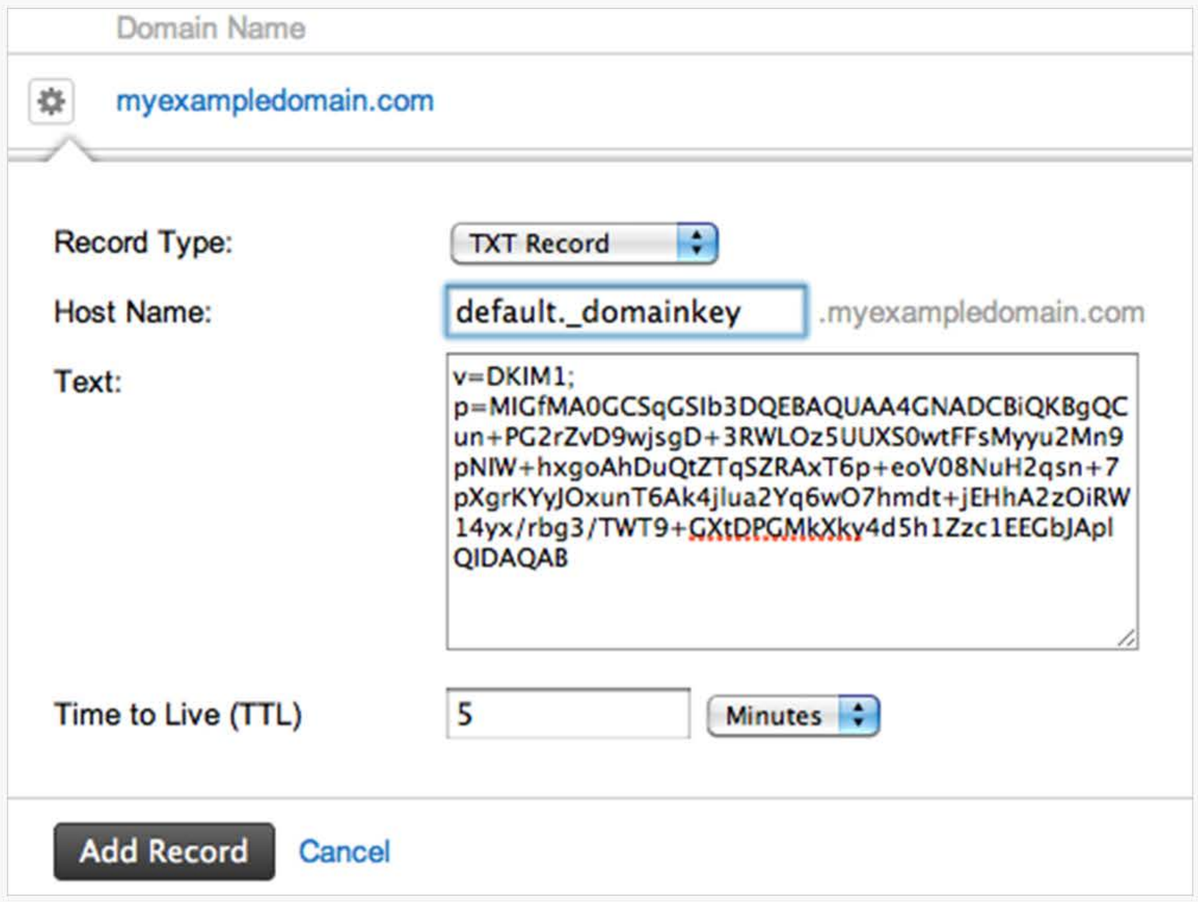
- `v=DKIM1` indica a versão do DKIM utilizada.
- `k=rsa` especifica o método de criptografia (RSA).
- `p=MIGf...` contém a chave pública que será usada para validar os e-mails.

3 | **Ative a assinatura no servidor de envio:** configure o servidor para assinar os e-mails automaticamente.

---

## Se você utiliza o Google Workspace para enviar seus e-mails, aqui está um guia passo-a-passo:

1. Acesse o **Console de Administração do Google Workspace** e faça login com uma conta administrativa.
2. No painel, vá até **Apps > Google Workspace > Gmail > Configurações de autenticação de e-mail**.
3. Selecione o domínio no qual deseja configurar o DKIM.
4. Clique em **Gerar uma nova chave de autenticação**.
5. Configure o comprimento da chave (recomendado: 2048 bits para maior segurança).
6. Escolha o prefixo do seletor (por padrão, o Google sugere google, mas você pode personalizar, se necessário).
7. Copie o valor do registro TXT gerado pelo Google. Ele terá o mesmo formato do exemplo de registro acima.
8. Adicione este registro TXT no provedor de DNS do seu domínio. Isso pode ser feito acessando a configuração de DNS do seu provedor (como Cloudflare, GoDaddy ou outro).
9. Depois de publicar o registro DNS, volte ao Console de Administração do Google e clique em **Iniciar Autenticação**.




## Confira o guia oficial dos fornecedores aqui:

- Se seu fornecedor de e-mails é Microsoft, **clique aqui**.
- Se seu fornecedor de e-mails é Google, **clique aqui**.

# 3 DMARC (Domain-based Message Authentication, Reporting, and Conformance)

O DMARC é um **protocolo de autenticação de e-mails que trabalha em conjunto com o SPF e o DKIM** para validar a legitimidade das mensagens enviadas em nome de um domínio.

## Por que usar DMARC?

**Proteção contra spoofing e phishing:**
garante que apenas fontes autorizadas possam enviar e-mails em nome do seu domínio.

**Maior controle sobre a entregabilidade:**
permite especificar como os servidores devem lidar com mensagens não verificadas.

**Monitoramento detalhado:**
gera relatórios que ajudam a identificar fontes não autorizadas.

## Como funciona o DMARC?

O DMARC é configurado pelo proprietário do domínio por meio de um registro específico no DNS (Domain Name System), assim como os registros SPF e DKIM. Esse registro consiste em **uma única linha de texto que define a política de autenticação do e-mail, especificando como os servidores destinatários devem lidar com mensagens que falhem nas verificações de SPF e DKIM**. Ao integrar esses dois mecanismos, o DMARC cria uma camada adicional de proteção contra falsificação de e-mails, garantindo que apenas remetentes legítimos possam enviar mensagens em nome do domínio.

# **Como configurar** corretamente o DMARC:

1 | **Publique um registro DNS TXT para seu domínio, especificando sua política DMARC:** esse registro define a política DMARC e como os relatórios devem ser enviados.

EXEMPLO DE REGISTRO DMARC:

```
_ dmarc.example.com. IN TXT "v=DMARC1; p=quarantine; rua=mailto:relatorios@example.com"
```

Este registro informa:

- `v=DMARC1` indica que se trata de um registro DMARC.
- `p=quarantine` define a política de tratamento para e-mails não autenticados. Pode ser:
  - `none` apenas monitora os envios, sem ação punitiva.
  - `quarantine` direciona mensagens suspeitas para a caixa de spam.
  - `reject` bloqueia mensagens que falharem na autenticação.
- `rua=mailto:relatorios@example.com` define o e-mail para envio de relatórios agregados.

2 | **Configure o recebimento de relatórios:** os relatórios DMARC são fundamentais para entender quem está enviando e-mails em nome do seu domínio e identificar possíveis problemas de autenticação. Existem dois tipos:

- **Relatórios agregados** `rua`**:** fornecem uma visão geral de quais fontes estão enviando e-mails em nome do seu domínio.
- **Relatórios forenses** `ruf`**:** fornecem detalhes específicos sobre mensagens que falharam na verificação.

PARA ATIVAR OS RELATÓRIOS FORENSES, ADICIONE O SEGUINTE PARÂMETRO AO SEU REGISTRO DMARC:

```
ruf=mailto:forense@example.com
```

3 | **Monitore e ajuste as configurações:** após a implementação, monitore os relatórios regularmente para:

- **Identificar fontes não autorizadas** enviando e-mails em nome do seu domínio.
- Ajustar configurações para **incluir ou excluir fontes específicas**.
- **Refinar a política DMARC gradualmente**, iniciando com p=none para monitoramento e depois migrando para `quarantine` e `reject` conforme necessário.

## **Confira o guia oficial dos fornecedores aqui:**

- Se seu fornecedor de e-mails é Microsoft, **clique aqui**.
- Se seu fornecedor de e-mails é Google, **clique aqui**.

# 4 Consequências de **configurações ineficazes**

Garantir a segurança do seu domínio é essencial para proteger sua marca, clientes e parceiros contra ataques cibernéticos. **Configurações inadequadas podem abrir brechas para invasores explorarem seu e-mail**, resultando em diversos problemas.

## **Principais riscos** de configurações ineficazes:

### Phishing e Spoofing:

se seu domínio não estiver corretamente autenticado, **criminosos podem falsificar e-mails em seu nome, enganando clientes e parceiros**. Isso pode levar a golpes financeiros, vazamento de dados e danos à reputação da sua empresa.

### Comprometimento da Reputação:

Provedores de e-mail (como Gmail, Outlook e Yahoo) utilizam autenticação para decidir se um e-mail é confiável. **Mensagens enviadas sem SPF, DKIM e DMARC podem ser classificadas como spam**, afetando diretamente sua capacidade de comunicação e credibilidade no mercado.

### Comprometimento da Reputação:

**Sem configurações adequadas, até e-mails legítimos podem ser bloqueados ou marcados como suspeitos.** Isso pode impactar comunicações internas, transacionais e de marketing, reduzindo a eficiência do seu negócio.

### Impactos Financeiros:

A falta de segurança no e-mail pode resultar em:

- **Multas** por não conformidade com regulamentações de proteção de dados.
- **Perda de oportunidades de negócios** devido à comunicação falha.
- **Custos adicionais** para remediar ataques ou ajustar configurações após um incidente.

## **Ferramentas** para verificação e otimização:

Para garantir que seu domínio esteja configurado corretamente, **utilize ferramentas especializadas para análise e diagnóstico**:

- **MxToolbox:** Permite verificar registros SPF, DKIM e DMARC, identificando falhas e sugerindo melhorias.
- **Google Apps Toolbox:** Analisa configurações de e-mail do Google Workspace para detectar problemas de autenticação.

Utilizar essas ferramentas regularmente ajuda a evitar vulnerabilidades e otimizar a segurança do seu e-mail.

# 5 Melhore a entregabilidade dos seus e-mails e **evite o spam**

Os provedores de e-mail analisam diversos fatores para decidir se uma mensagem será entregue, enviada para a caixa de spam ou bloqueada. **Cada e-mail não entregue representa uma oportunidade perdida.** Se suas mensagens forem marcadas como spam, sua marca perde credibilidade, e seus resultados de negócio podem ser impactados negativamente.

## **Proteja seu domínio** com SPF, DKIM e DMARC:

### SPF (Sender Policy Framework):

Permite que você defina **quais servidores estão autorizados a enviar e-mails em nome do seu domínio**, reduzindo o risco de falsificação de remetente.

### DKIM (DomainKeys Identified Mail):

**Adiciona uma assinatura digital às mensagens**, garantindo que elas não foram alteradas durante o envio e que realmente vieram do seu domínio.

### DMARC (Domain-based Message Authentication, Reporting, and Conformance):

O DMARC vai além: ele i**nstrui os provedores de e-mail sobre como lidar com mensagens que falham na autenticação SPF e DKIM**. Com ele, você pode monitorar tentativas de fraude usando seu domínio e reforçar a segurança da entrega.

## Principais **benefícios**:

### Aumento da taxa de entrega:

Suas mensagens têm mais chances de chegar à caixa de entrada do destinatário.

### Proteção contra phishing e spoofing:

Evita que hackers utilizem seu domínio para enganar clientes e parceiros.

### Reforço na reputação do domínio:

Evita que seu e-mail seja tratado como spam e reduz o risco de ser incluído em listas de bloqueio.

Manter a reputação do seu domínio é essencial, especialmente se sua empresa envia grandes volumes de e-mails. **Implementar SPF, DKIM e DMARC é um passo fundamental** para garantir que suas comunicações cheguem ao destino certo.

**Tome a iniciativa agora:** proteja seu domínio, otimize a entrega de e-mails e transforme cada mensagem em uma conexão bem-sucedida!

# Guia de **termos técnicos**

**SPF (Sender Policy Framework):** informa aos servidores de e-mail quais servidores estão autorizados a enviar e-mails em seu nome.
Se não configurado corretamente: E-mails podem ser marcados como spam ou rejeitados se vierem de servidores não autorizados. Além disso, qualquer pessoa pode enviar e-mails em seu nome.

**DMARC (Domain-based Message Authentication, Reporting & Conformance):** Funciona com SPF e DKIM para informar aos servidores de e-mail como lidar com e-mails não autorizados (rejeitar, colocar em quarentena ou aceitar). Se não configurado corretamente, você perde o controle sobre e-mails não autorizados e fica mais difícil proteger contra phishing ou spoofing.

**Spoofing:** Técnica usada por cibercriminosos para falsificar informações de remetentes em e-mails, criando a aparência de que uma mensagem veio de uma fonte confiável, quando, na verdade, é um ataque.

**Blacklists (Listas Negras)::** Listas de endereços IP ou domínios conhecidos por enviar e-mails indesejados, ou maliciosos. Se seu domínio for incluído em uma blacklist, seus e-mails podem ser bloqueados por servidores de e-mail de terceiros.

**TLS (Transport Layer Security):** Protocolo criptográfico que protege as comunicações na internet. Quando configurado corretamente, o TLS pode garantir que seus e-mails sejam criptografados durante o envio e recebimento, aumentando a segurança.

**MX Records (Mail Exchange Records):** Registros DNS que definem os servidores de e-mail responsáveis pela recepção das mensagens enviadas para o seu domínio. Eles são importantes para a configuração de SPF e DMARC.

**DKIM (DomainKeys Identified Mail):** Adiciona uma assinatura digital aos seus e-mails para provar que eles não foram alterados durante o envio.
Se não configurado corretamente, os destinatários não conseguem verificar a autenticidade do e-mail, o que pode fazê-lo parecer suspeito ou não confiável. Qualquer e-mail pode ser alterado durante o envio por um atacante.

**DNS (Domain Name System):** Sistema que traduz os nomes de domínio (como example.com) em endereços IP. É essencial para o funcionamento do SPF, DKIM e DMARC, pois essas autenticações dependem de registros DNS.

**Phishing:** Ataque cibernético em que criminosos tentam enganar usuários para que revelem informações confidenciais, como senhas ou dados bancários, geralmente por meio de e-mails falsos.

**SMTP (Simple Mail Transfer Protocol):** Protocolo de comunicação utilizado para o envio de e-mails entre servidores. Ele é fundamental para a entrega de mensagens e, quando combinado com SPF, DKIM e DMARC, ajuda a autenticar e garantir a segurança do envio de e-mails.

**Reputação de Domínio:** Refere-se à credibilidade do seu domínio em relação aos servidores de e-mail. Uma boa reputação ajuda a garantir que seus e-mails não sejam marcados como spam, enquanto uma má reputação pode reduzir a entregabilidade e a confiança nas suas comunicações.

# Conclusão

**Proteger seu domínio com SPF, DKIM e DMARC vai muito além de uma recomendação técnica.** Imagine seus clientes recebendo um e-mail falso da sua empresa, solicitando dados confidenciais. Ou, pior, seu domínio sendo usado para enganar centenas de pessoas.

Com essas configurações, você cria uma barreira poderosa contra práticas como spoofing e phishing, garantindo que seus e-mails cheguem com credibilidade e segurança. Elas atuam como guardiões invisíveis, validando cada mensagem enviada em nome do seu domínio e preservando a integridade das suas comunicações.

Dê o próximo passo agora: **configure essas soluções e transforme sua comunicação em um diferencial competitivo**. Proteja sua marca e ofereça tranquilidade a quem confia em você. Segurança é uma escolha que faz toda a diferença — para sua empresa, seus clientes e o futuro do seu negócio.

---