Adicionar DMARC ao cpanel

Objetivo

Descrever, de forma clara e concisa, o processo de implementação e configuração do registro DMARC em domínios hospedados, visando aumentar a segurança dos e-mails, reduzir tentativas de fraude (spoofing) e melhorar a reputação e entregabilidade das mensagens.

Escopo e Público

Aplica-se a:
- Configuração de DNS para domínios hospedados.
- Implementação de autenticação de e-mail.
- Adequação às boas práticas de segurança de e-mail.

Não cobre:
- Configuração de servidores SMTP.
- Correção de SPF e DKIM.
- Análise detalhada dos relatórios DMARC.

Público-alvo:
- Analistas de suporte.
- Técnicos de hospedagem.
- Administradores de sistemas.
- Equipe de infraestrutura.

Pré-requisitos

- Acesso ao painel de hospedagem do domínio.
- Permissão para gerenciar registros DNS.
- Conhecimento básico sobre DNS.
- Sender25.

Materiais/Recursos

- Painel de gerenciamento DNS.
- Domínio ativo.
- Ferramenta de validação DMARC.
- Sender25.

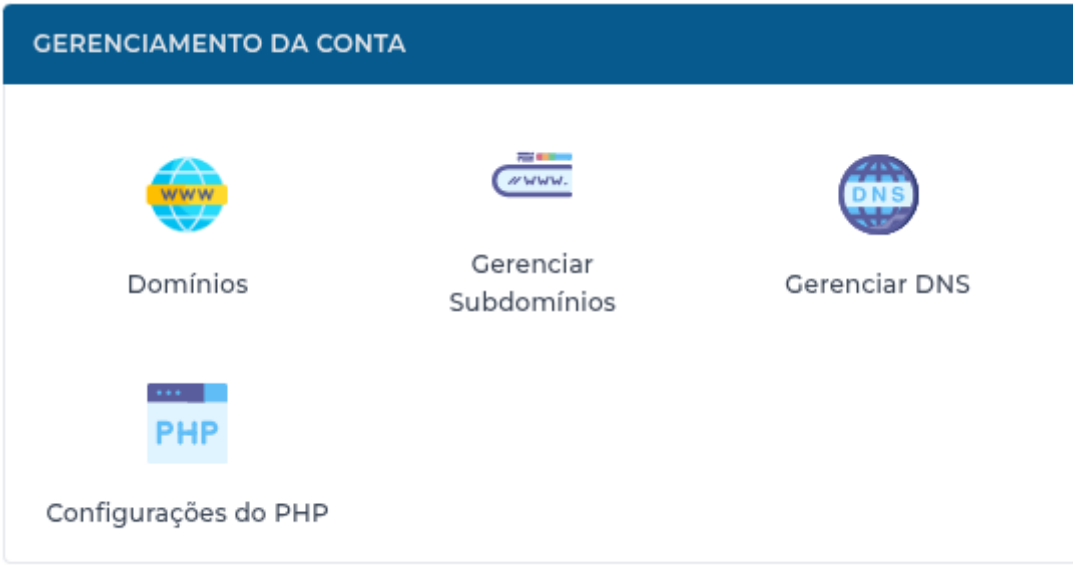
O que é DMARC?

A sigla **DMARC** significa **Domain-based Message Authentication, Reporting and Conformance**.
Trata-se de um mecanismo de autenticação de e-mails baseado no domínio, utilizado para validar mensagens enviadas em nome de uma organização.
Seu principal objetivo é impedir que terceiros utilizem o domínio para envio de mensagens fraudulentas, protegendo usuários contra golpes, phishing e spam.
Com o DMARC configurado corretamente, os provedores de e-mail conseguem verificar se uma mensagem realmente foi enviada por servidores autorizados pelo domínio, aumentando a confiança dos provedores e melhorando a taxa de entrega dos e-mails legítimos.
Além disso, o DMARC permite o recebimento de relatórios que auxiliam na identificação de possíveis tentativas de uso indevido do domínio.

Passos

Passo 1 – Acessar o gerenciamento DNS

Acesse o painel de hospedagem do domínio.
No menu principal localize e clique em:
Gerenciar DNS



Passo 2 – Verificar se já existe um registro DMARC

Na lista de registros DNS, procure por um registro com o nome:

```
_dmarc
```

Caso o registro já exista, revise sua configuração antes de realizar alterações.

> Importante: Não crie registros DMARC duplicados.

Nome	TTL	Tipo	Valor
ftp	3600	A	170.247.60.100
ingacontabil.com.br.	3600	A	170.247.60.100
mail	3600	A	170.247.60.100
pop	3600	A	170.247.60.100
smtp	3600	A	170.247.60.100
webmail	3600	A	170.247.60.100
www	3600	A	170.247.60.100
ingacontabil.com.br.	86400	NS	ns.br53.eu.
ingacontabil.com.br.	3600	NS	ns.br53.net.
ingacontabil.com.br.	3600	NS	ns.br53.org.
ingacontabil.com.br.	86400	NS	ns.br53.pro.
ingacontabil.com.br.	86400	NS	ns.br53.us.
ingacontabil.com.br.	3600	MX	10 mail.ingacontabil.com.br.

Passo 3 – Adicionar um novo registro DMARC

Caso não exista nenhum registro DMARC:

1. Clique em **Adicionar Registro**.
2. Selecione o tipo **TXT**.

Passo 4 – Preencher as informações do registro

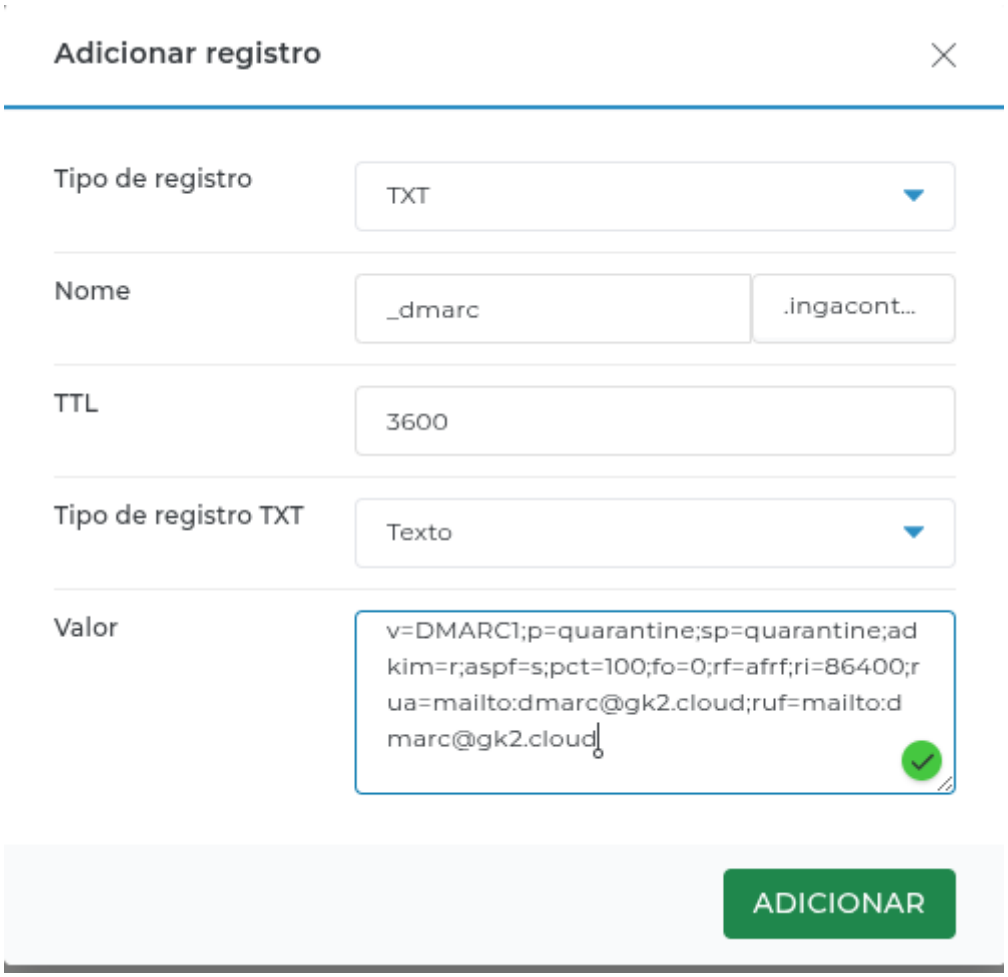
Configure os campos conforme abaixo:

Campo	Valor
Tipo de Registro	TXT
Nome	_dmarc
TTL	3600
Tipo de Registro TXT	Texto

No campo **Valor**, informe:

```
v=DMARC1;p=quarantine;sp=quarantine;adkim=r;aspf=s;pct=100;fo=0;rf=afrf;ri=86400;rua=mailto:dmarc@gk2.cloud;ruf=mailto:dmarc@gk2.cloud
```

Após preencher os dados, clique em **Adicionar**.



Passo 5 – Confirmar a criação do registro

Após a inclusão, o registro deverá aparecer na listagem DNS semelhante ao exemplo abaixo:

```
_dmarc    TXT    v=DMARC1;...
```

Passo 6 – Aguardar a propagação

Após a criação do registro, será necessário aguardar a propagação DNS.
O tempo pode variar entre alguns minutos e até 24 horas, dependendo da infraestrutura de DNS utilizada.

Como implementar relatórios DMARC personalizados

Caso deseje receber relatórios específicos do domínio monitorado:

Criar um e-mail para relatórios

Exemplo:

```
dmarc-reports@dominio.com
```

Criar o registro TXT

Nome:

```
_dmarc
```

Valor:

```
v=DMARC1;p=quarantine;sp=quarantine;adkim=r;aspf=s;pct=100;fo=0;rf=afrf;ri=86400;rua=mailto:dmarc-reports@dominio.com;ruf=mailto:dmarc-reports@dominio.com
```

Passo 7 – Validar a configuração

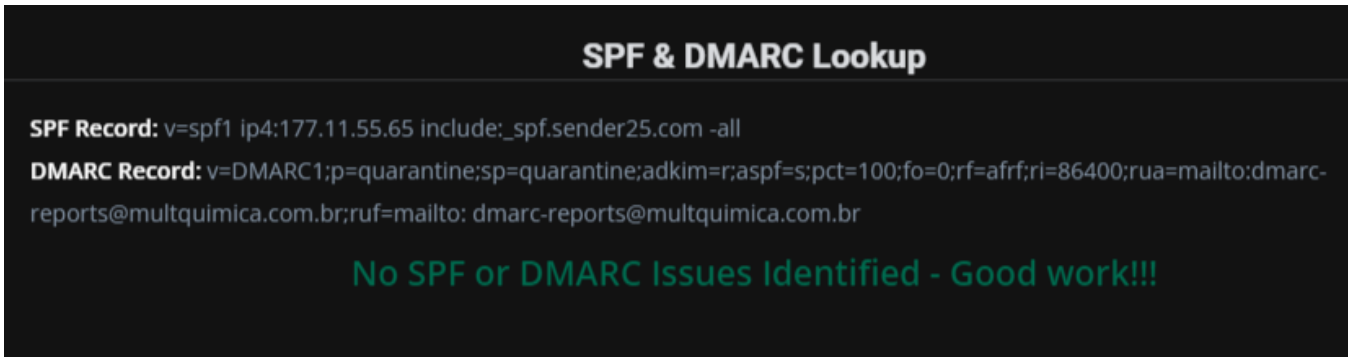
Após a propagação DNS, realize um teste para validar o funcionamento do DMARC.
Verifique se o domínio apresenta:

- SPF válido.
- DKIM válido.
- DMARC válido.

Resultado esperado:

```
No SPF or DMARC Issues Identified - Good Work!!!
```

Testar segurança do DMARC **aqui**



Critérios de Aceitação

- Registro DMARC criado com sucesso.
- Não existem registros DMARC duplicados.
- O registro está propagado corretamente.
- A validação retorna status positivo.
- O domínio passa nos testes de SPF, DKIM e DMARC.

Riscos e Mitigações

Risco	Probabilidade	Impacto	Mitigação
Registro DMARC duplicado	Média	Alto	Verificar previamente a zona DNS
Erro de digitação no valor do registro	Média	Alto	Copiar e revisar o valor antes de salvar
Propagação DNS demorada	Média	Baixo	Aguardar o tempo necessário antes de validar

Risco	Probabilidade	Impacto	Mitigação
Ausência de SPF ou DKIM	Média	Alto	Configurar SPF e DKIM antes da validação final

Controle de Mudanças

Versão	Data	Descrição
2.0	Junho/2026	Upgrade do procedimento
1.0	Abril/2025	Criação inicial do procedimento

Notas Adicionais

- O DMARC complementa as proteções fornecidas pelo SPF e DKIM.
- Recomenda-se monitorar regularmente os relatórios recebidos.
- Alterações incorretas podem afetar a entregabilidade dos e-mails.

Revision #4
Created 2023-05-04 14:27:05 UTC by Ewerton Henrique
Updated 2026-06-15 14:32:12 UTC by Rafael Herreiro