

Configuração de Proteção a  
VIP (Very Important Person) e  
Look-aLike Domains

**MAILINSPECTOR**  
powered by **HSC**

# Configuração de uso com proteção a VIP (Very Important Person)

Essa proteção se dá a nível de Display Name, uma vez que o criminoso não tem acesso ao Display Name correto utilizado pela empresa e com isso, acaba colocando um Display Name **similar ao original**.

## Passo-a-passo

1. Criar um dicionário de palavras chamado Display Name e incluir o Display Name dos Diretores nesta lista.
2. Criar um grupo de usuários chamado Diretoria e incluir os emails deles nesta lista.
3. Crie regra de SPAM.
4. Crie regra de Display Name.
5. Case as regras e ajuste a pontuação necessária

## Características de Fraude de Email

Assunto: Fw: Boleto nº (801407) De: root@vb4.cristalinfinan.com.br Para: estoque.pa@sermedsaude.com.br Tamanho: 9.44KB Pontuação: 23.31

Entregue Status

Não Entregue, SPAM, Quarentenado, Phishing

Assunto: Fw: Boleto nº (801407) Data: 2019-02-05 12:38:16 De (Envelope): root@vb4.cristalinfinan.com.br Para (Envelope): estoque.pa@sermedsaude.com.br De (Header): Notificação de Pendência <support@financeiro.com.br> Para (Header): estoque.pa@sermedsaude.com.br Tamanho: 9.44KB IP de Origem: 147.135.76.18 Ponto de Acesso do Cluster: mx01.mildcloud.com.br

Conotação financeira

Email original

A origem do emails em relação aos apresentados ao usuários não são os mesmos

Email forjado que aparece para o usuário. O nome que aparece para o usuário é: Notificação de Pendência

Detalhes da Mensagem 780061200C7.A2528

URLS

http://fatursimplesfinan.com/page?cobranca.spadmin?recalcula... Engine: globalBlacklist Details: [preLoad/0003\_wl\_hsc] phishing

Filtros de Conteúdo Filtros de Spam Ameaças Cabeçalho Tabela HTML Anexos Data Lixo Prevenção Smart Defender

Status

Virus:	Spam:
Conteúdo Bloqueado:	Tamanho Excedido:
WhiteList:	BlackList:
E-mail Marketing:	Redes Sociais:
Arquivos suspeitos:	Spoofing de domínio:

Provável Spam:

Outro Bloqueio:
Possível Ameaça:
E-mails suspeitos:

Detalhes

Relatório de Conteúdo: -

Relatório de WhiteList / BlackList: -

## 1. Criação de Display Name customizados

Configurações > Cadastro > Dicionário de Palavras

Clique em Adicionar

Insira no nome do Dicionário (no exemplo foi **Display Name - Diretores**), descrição as expressões regulares que comporiam o Display Name.

Obs: Não esqueça de clicar em + para incluir a Expressão na lista.

No exemplo, vamos considerar 2 diretores:

- Carlos Alcantra Camargo
- Luis T. Silva

**Administration Suite**

RealTime

Painel de Controle

Relatórios

Configurações

Cadastros

- Grupos Usuários
- Anexos
- Mime-Types/Fingerprint
- Dicionário de Palavras**
- RBLs Externas

Controle de Conexão

Quarentena

Filtros de Conteúdo

Controle de Ameaças

Filtros de SPAM

Anti Spoofing

Notificações

Email Compliance

Administração

**Dicionário de Palavras**

Nome:

Display Name - Diretores

Descrição:

Display Name - Diretores

Expressões:

Carlos\sAlcantra\sCamargo

Luis\sT\sSilva

Anexar:  Selecionar

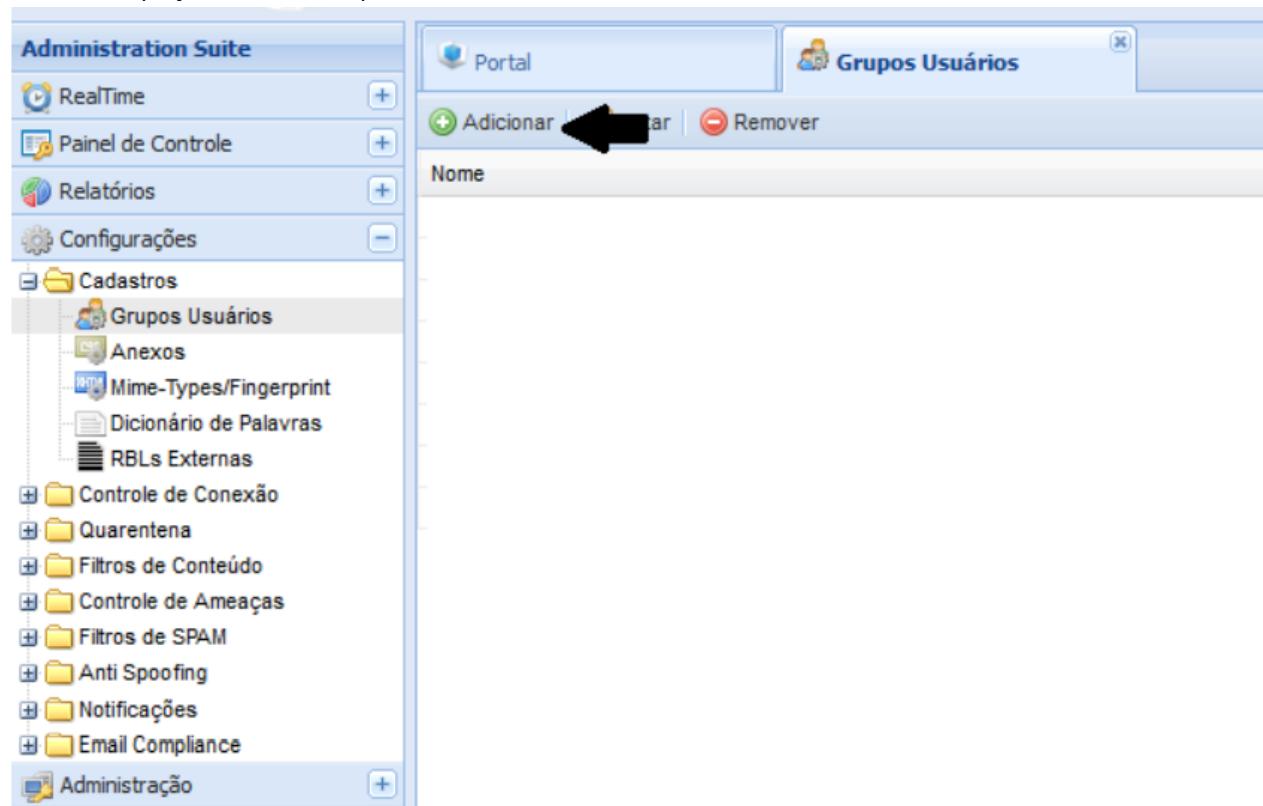
Após inserida toda as **expressões regulares**, clique em Salvar.

## 2. Criação de Grupo de Emails dos Diretores

Configurações > Cadastro > Grupo de Usuários

Clique em Adicionar Insira no nome do Grupo (no exemplo foi Diretoria), descrição e inclua neste grupo os emails dos diretores/emails sensíveis a ataques.

Obs: Não esqueça de clicar em + para incluir o email na lista.



The screenshot shows the 'Administration Suite' interface. On the left, a navigation tree includes 'RealTime', 'Painel de Controle', 'Relatórios', 'Configurações' (selected), 'Cadastros' (selected), 'Grupos Usuários' (selected), 'Anexos', 'Mime-Types/Fingerprint', 'Dicionário de Palavras', 'RBLs Externas', 'Controle de Conexão', 'Quarentena', 'Filtros de Conteúdo', 'Controle de Ameaças', 'Filtros de SPAM', 'Anti Spoofing', 'Notificações', 'Email Compliance', and 'Administração'. The 'Grupos Usuários' item is highlighted. On the right, a 'Grupos Usuários' panel is open, showing a 'Nome' (Name) input field and a toolbar with 'Adicionar' (Add) and 'Remover' (Remove) buttons. A green arrow points to the 'Adicionar' button.

**Grupos Usuários**

Nome do Grupo:  
Diretoria

Descrição do Grupo:  
Emails internos sensíveis a ataques

Ativo:  
 Sim  Não

E-mail:  
cfo@hscbrasil.com.br

diretor@hscbrasil.com.br

Domínio:

Após inserida toda a lista de email diretoria, clique em Salvar.

## Regra de DLP - Diretoria

Configurações > Email Compliance > Regras

Clique em Adicionar

Seleção de Controle: Cabeçalho

Define o cabeçalho a ser utilizado: To

Grupos: Diretoria

Número Mínimo de Ocorrências: 1

### Cabeçalho

2/4

Define o filtro para o controle selecionado.

Define o cabeçalho a ser utilizado:

To

Grupos:

Diretoria

Número Mínimo de Ocorrências:

1

Na etapa de informações e ação

Nome: Diretoria

Descrição: Emails da diretoria e/ou sensíveis a ataques

Tipo: DLP

Ações:

Log: Marque a opção Registrar em Log

Notificação: Não marque nada

Ação: Rejeitar / Deletar / Não Entregar

Encaminhar para: Nenhum

## Informações e Ações

3/4

Define informações gerais e ações que serão realizadas.

Nome:

Diretoria

Descrição:

Emails da diretoria e/ou sensíveis a ataques

Tipo:

DLP

### Ações

Log:

Registrar em Log

Armazenar para Auditoria

Notificação:

Remetente

Destinatário

Ação:

Entregar

Rejeitar / Deletar / Não Entregar

Encaminhar para:

Nenhum

Alterar assunto:

Alterar cabeçalho:

Valor:

Clique em Avançar e depois de apresentado o resumo, clique em Salvar

Regra	Nome	Controle	Ação
306	Diretoria	Cabeçalho	Rejeitar / Deletar / Não Entrega, Registrar em Log

## Regra de DLP – Display Name

Configurações > Email Compliance > Regras

Clique em Adicionar

Seleção de Controle: Cabeçalho

Define o cabeçalho a ser utilizado: Customizad

Cabeçalho Customizado: From

Dicionário de Palavras: Display Name - Diretores

Número Mínimo de Ocorrências: 1

### Cabeçalho

2/4

Define o filtro para o controle selecionado.

Define o cabeçalho a ser utilizado:

Customizado

From

Dicionário de Palavras:

Display Name - Diretores

Número Mínimo de Ocorrências:

1

Clique em Avançar

Na etapa de Informações e Ações

Nome: Display Name Diretores

Descrição: Nomes de Apresentação utilizados pelos diretores em Seus Emails Profissionais

Tipo: DLP

Ações:

Log: Marque a opção Registrar em Log

Notificação: Não marque nada

Ação: Rejeitar / Deletar / Não Entregar

Encaminhar para: Nenhum

**Regras**

**Informações e Ações** 3/4

Define informações gerais e ações que serão realizadas.

Nome:

Descrição:

Tipo:

**Ações**

Log:	<input checked="" type="checkbox"/> Registrar em Log	<input type="checkbox"/> Armazenar para Auditoria
Notificação:	<input type="checkbox"/> Remetente	<input type="checkbox"/> Destinatário
Ação:	<input type="radio"/> Entregar	<input checked="" type="radio"/> Rejeitar / Deletar / Não Entregar

Encaminhar para:

Alterar assunto:

Alterar cabeçalho:  Valor:

Clique em Avançar e depois de apresentado o resumo, clique em Salvar.

 307 Display Name Diretores Cabeçalho Rejeitar / Deletar / Não Entrega, Registrar em Log

## Casando as Regras

Selecione as duas regras que você criou e clique em Conectar

Regra	Nome	Controle	Ação
<input type="checkbox"/>	306	Diretoria	Rejeitar / Deletar / Não Entrega, Registrar em Log
<input checked="" type="checkbox"/>	307	Display Name Diretores	Rejeitar / Deletar / Não Entrega, Registrar em Log

 Conectar



A ideia é para quando os emails foram para os diretores, mas o Display Name não se casar, é porque foi alguém que colocou um Display Name diferente do que é usado na empresa para aquele diretor, portanto, é email forjado.

Conectar Regras:

Diretoria: Casar

Operador Lógico: E

Display Name Diretores: Casar

Tipo: DLP

Ações:

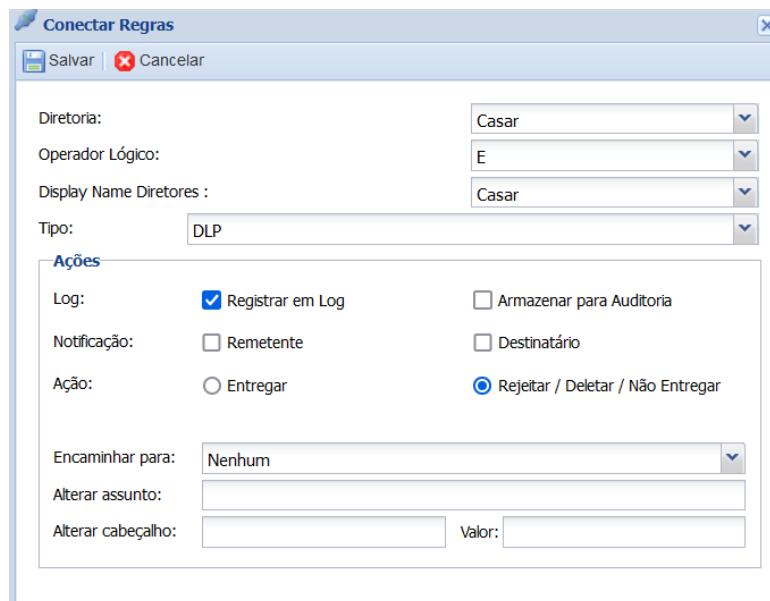
Log: Marque a opção Registrar em Log

Notificação: Não marque nada

Ação: Rejeitar / Deletar / Não Entregar

Encaminhar para: Nenhum

Clique em Salvar



**Resumo da regra:** O que vier destinado a Diretoria, será verificado o Display Name e caso o Display Name não case com nenhum dos nomes cadastrados pelas expressões regulares cadastradas, o sistema bloqueará o email pelo DLP.

# Configuração de uso com proteção a Look-alike Domains/Cousin Domains

Look-aLike Domains ou Cousin Domains é Uma técnica de ataques muito utilizada por hackers, ao qual consistem em compra de domínios “parecidos/similares” em relação ao domínio alvo.

O MailInspector consegue verificar se a origem do e-mail é similar ao domínio aplicado no remetente e ainda compara com eventual problema de SPF em relação ao domínio.

Top Violações de SPF por Domínio

DOMÍNIO	SPF HELO SOFTFAIL	SPF FAIL	SPF SOFTFAIL	TOTAL
hscbrasil.com.br	861	5.346	-	6.207

Além da proteção já mencionada, podemos utilizar o sistema de DNSTwister para verificar domínios parecidos com o domínio original.

O cousin domain ou domínios primos, também chamado de look-alike domain (também conhecidos como domínios similares), é um domínio DNS (sistema de nome de domínio) semelhante a outro nome quando processado por um agente de usuário de email (MUA).

Por exemplo, [americanas1.com](#) ou [americamas.com](#) são domínios primo de [americanas.com](#).

Outros exemplos incluem erros de ortografia de um domínio, como [americamas.com](#) e [americanas.com](#)

Os domínios primos geralmente são criados como uma ferramenta de phishing para falsificar sua marca e seu nome de domínio.

No MLI existem **3 (três) formas de bloqueio** a domínios similares:

1. Bloqueio a nível de conexão;
2. Bloqueio a nível de pontuação de SPAM;
3. Bloqueio em quarentena customizada;

Em qualquer uma das formas de bloqueio, primeiramente o administrador deverá acessar o DNSTwister e verificar as variações do domínio já registradas.

No exemplo, vamos considerar o domínio HSCBRASIL.COM.BR

<https://dnstwister.report/>

# dnstwister report



hscbrasil.com.br 

[new search](#)

[SHOW UNRESOLVED DOMAINS](#)

export: [json](#) [csv](#)

Tweak	Type	IP	Tools
hscbrasil.com.br	Original*	68.66.216.19	<a href="#">analyse</a>  
iscbrasil.com.br	Bitsquatting	165.160.15.20	<a href="#">analyse</a>  
hsecbrasil.com.br	Insertion	177.11.54.112	<a href="#">analyse</a>  
scbrasil.com.br	Omission	108.167.132.144	<a href="#">analyse</a>  
hsbrasil.com.br	Omission	67.23.238.82	<a href="#">analyse</a>  
hcbrasil.com.br	Omission	45.79.161.146	<a href="#">analyse</a>  
hdcbrasil.com.br	Replacement	177.67.118.70	<a href="#">analyse</a>  
bscbrasil.com.br	Replacement	177.185.194.97	<a href="#">analyse</a>  

Então temos os domínios variantes:

- [icsbrasil.com.br](#)
- [hsebrasil.com.br](#)
- [hdcbrasil.com.br](#)
- [scbrasil.com.br](#)
- [scbrasil.com.br](#)
- [hsbrasil.com.br](#)

É possível também verificar os domínios que ainda não foram registrados (possíveis domínios similares), para isso, basta clicar no botão SHOW UNRESOLVED DOMAINS.

Com as variações dos domínios em mãos, é possível bloquear os domínios similares pelas três formas anteriormente citados.

## 1. Bloqueando na camada de conexão

Em Configurações > Cadastros > Configurações do MTA > Filtragem

Inclua toda a lista apresentada no DNSTwister, como exemplo a seguir:

Controle de Sessões SMTP (Controle de Fluxo)

Tipo:	Remetente
Valor:	icsbrasil.com.br
Ação:	Rejeitar

 Adicionar

Repita o processo acima até finalizar com todos os domínios similares.

Clique em Salvar.

Clique em Aplicar Configurações.

## 2. Bloqueando na camada de SPAM

Em Configurações > Cadastros > Grupos de Usuários

Crie um Grupo de usuários (domínios), com toda a lista dos domínios similares indicados pelo DNSTwister, conforme imagem abaixo:

Nome do Grupo: **Domínios Similares**

Descrição do Grupo: **Lista obtida no DNSTwister**

Ativo:  Sim  Não

E-mail:

Domínio:

hdcbrasil.com.br  
hsebrasil.com.br  
icsbrasil.com.br

IP/Rede:

Clique em Salvar

Depois vá em: Configurações > Filtros de SPAM > Controle Avançado

Clique em Adicionar

### Regras do Controle Avançado:

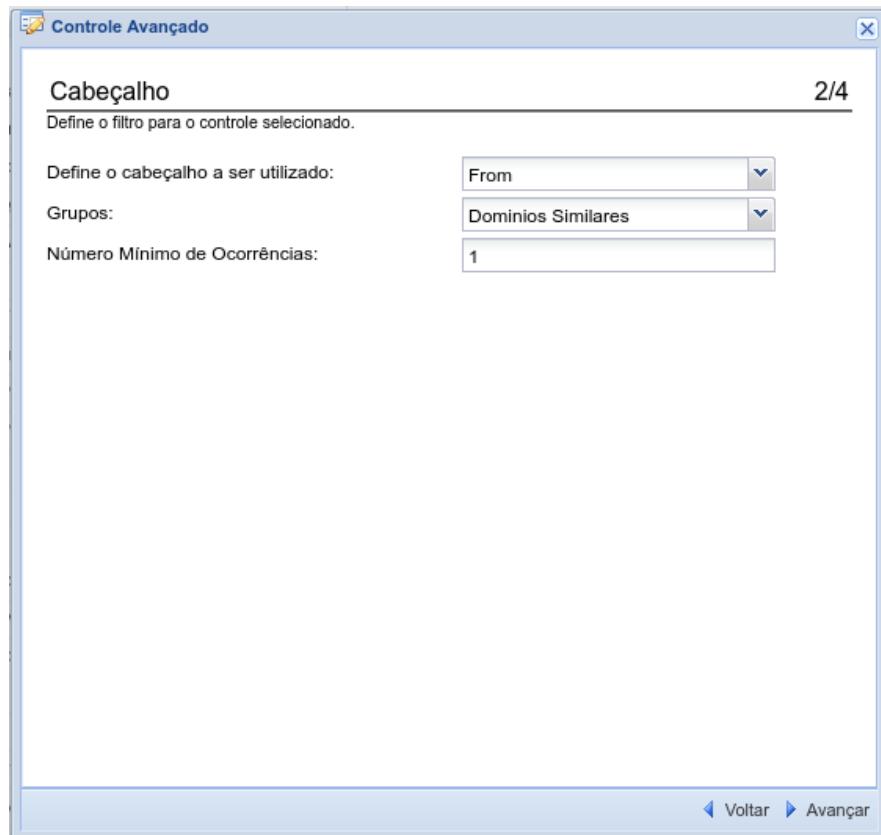
Seleção de Controle: Cabeçalho

Clique em Avançar

Define o Cabeçalho a Ser Utilizado: From

Grupos: Domínios Similares

Número Mínimo de Ocorrências: 1



Clique em Avançar

Nome: Domínios Similares

Descrição: Domínios similares detectados pelo DNSTwiester

Pontuação: 7

Clique em Avançar

Clique em Salvar

Clique em Aplicar Configurações

 **Controle Avançado** X

**Informações e Pontuação** 3/4

Define informações gerais e ações que serão realizadas.

Nome:	Domínios Similares
Descrição:	Domínios similares detectados pelo <del>DNSTwiester</del>
<b>Ações</b>	
Pontuação:	<input type="text" value="7"/>

 Voltar  Avançar

### 3. Quarentena Customizada

Em Configurações > Quarentena > Customizada

Clique em Adicionar

Nome: Domínio similar

Tipo: Armazenamento

Tamanho: 0

Tempo de Armazenamento de Mensagens: 3

Tempo de Armazenamento dos Logs: 90

Clique em Salvar

Em Configurações > Email Compliance > Regras

Clique em Adicionar

Seleção de Controle: Cabeçalho

Define o cabeçalho a ser utilizado: From

Grupos: Domínio Similar

Número Mínimo de Ocorrências: 1

Clique em Avançar

Nome: Domínios similares

Descrição: Domínios similares

Tipo: Quarentena

Armazenar na Quarentena: Domínio similar

 **Regras**

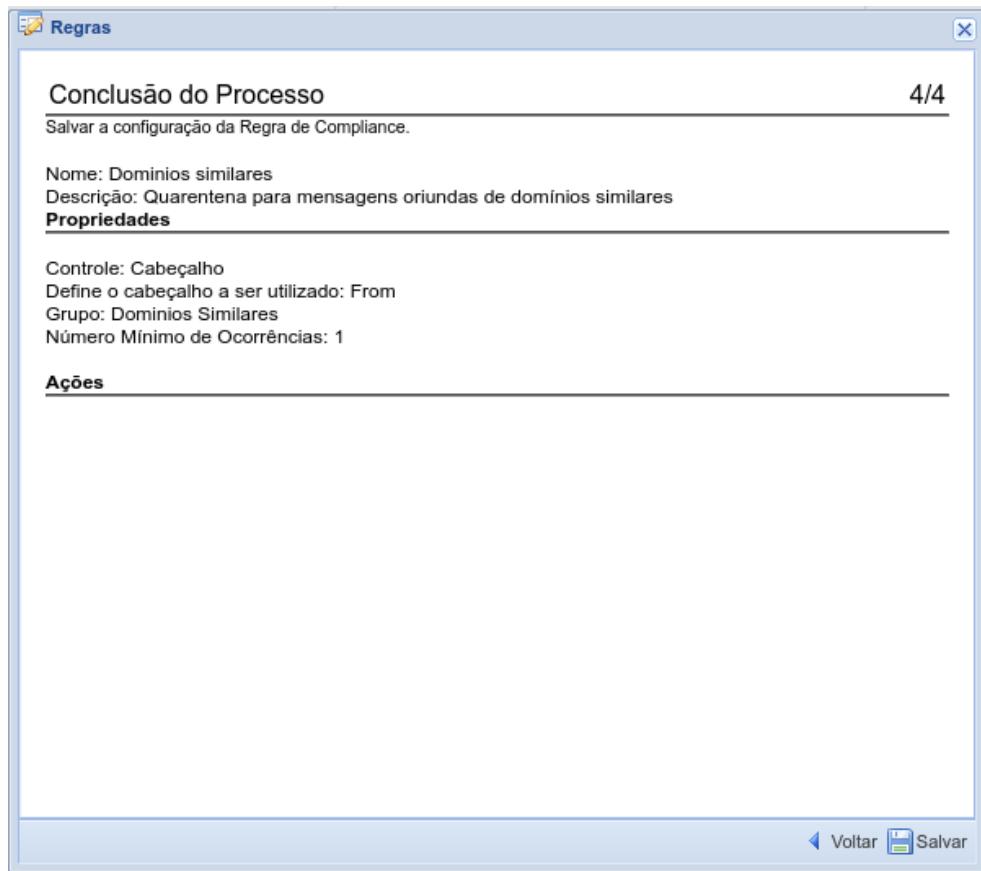
**Informações e Ações** 3/4

Define informações gerais e ações que serão realizadas.

Nome:	Domínios similares
Descrição:	Quarentena para mensagens oriundas de domínios similares
Tipo:	Quarentena
<b>Ações</b>	
Armazenar mensagem na quarentena:	Domínio similar

◀ Voltar ▶ Avançar

Clique em Avançar



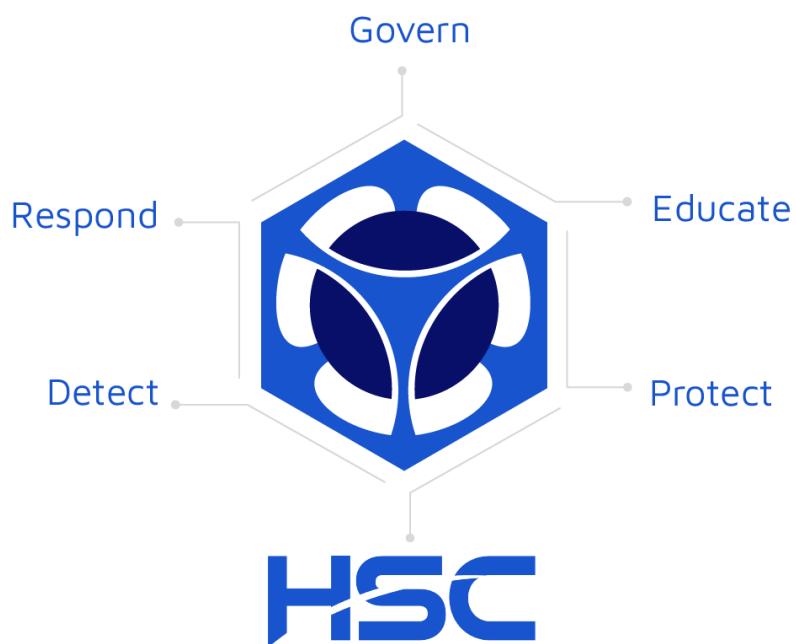
Por último, clique em Salvar e depois em Aplicar Configurações.

## Sobre a **HSC**

A HSC tem quase duas décadas de atuação em cibersegurança e conscientização de usuários, atendendo organizações de vários segmentos, dos setores público e privado.

Atualmente atuamos no Brasil, nos EUA e na América Latina.

Nossa experiência se reflete em números: todos os dias, protegemos mais de 10 milhões de mailboxes e filtramos mais de 100 milhões de e-mails



**Material exclusivo** da  
HSC, referente ao  
MailInspector.

Copyright © 2024 HSC.  
Não copie sem permissão.



[hsclabs.com](http://hsclabs.com)  
+55 51 3500 8255