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

MAILINSPECTOR

powered by HSC

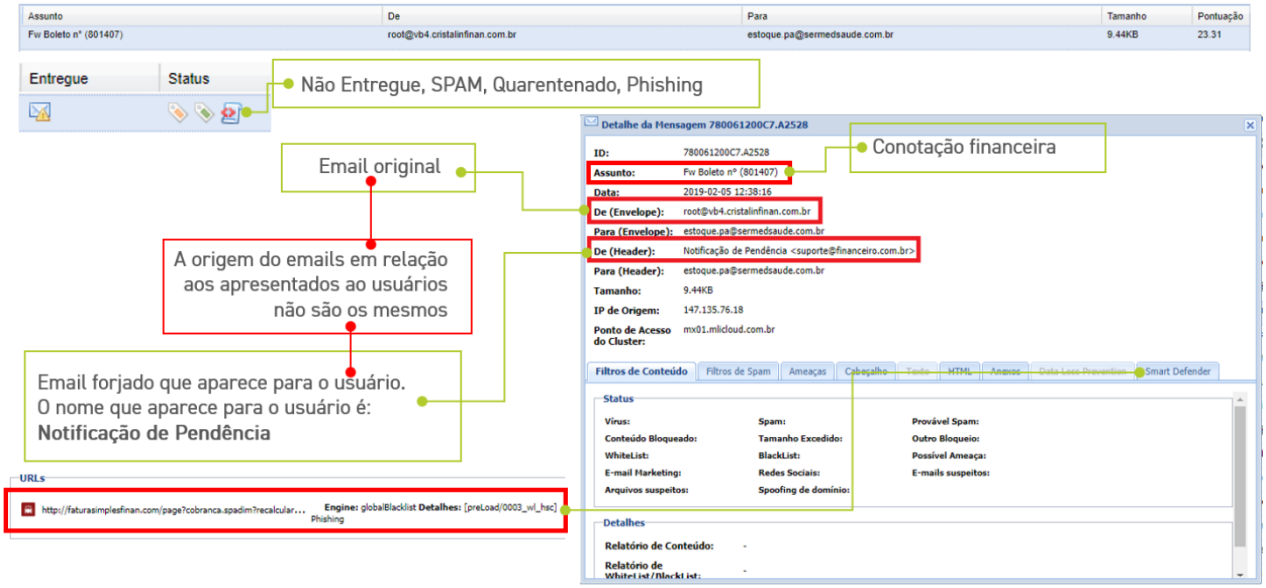
Configuração de uso com proteção a VIP (Very Important Person)

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



1. Criação de Display Name customizados

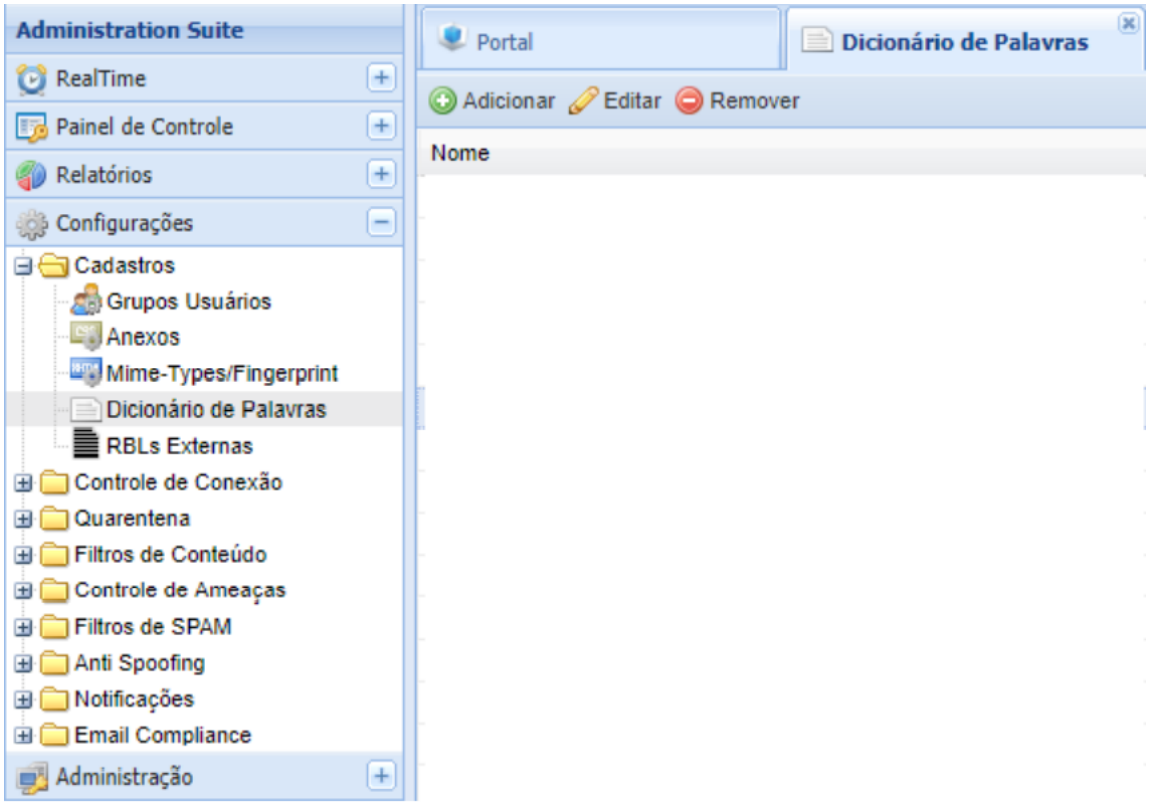
Configurações > Cadastro > Dicionário de Palavras

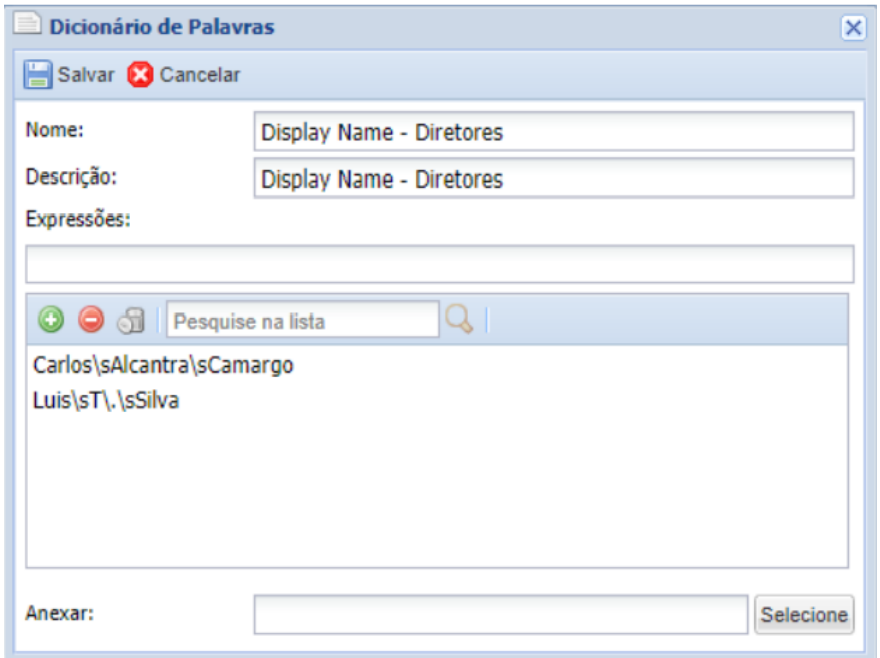
Clique em Adicionar

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





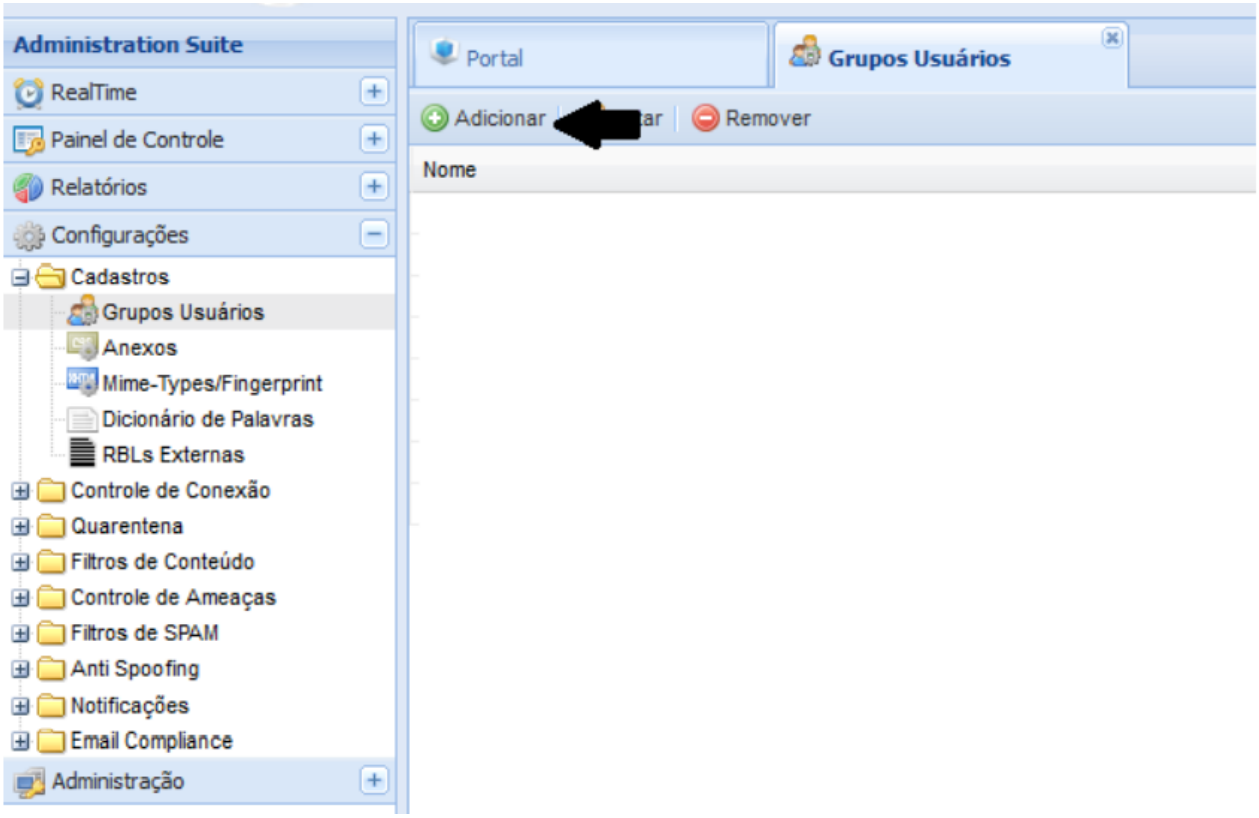
Após inserida toda as **expressões regulares**, clique em Salvar.

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 e-mails dos diretores/emails sensíveis a ataques.

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



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

Regra de DLP - Diretoria

Configurações > Email Compliance > Regras

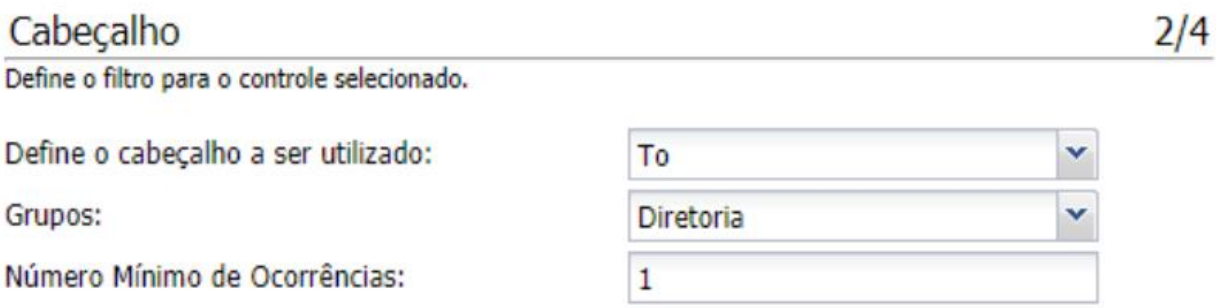
Clique em Adicionar

Seleção de Controle: Cabeçalho

Define o cabeçalho a ser utilizado: To

Grupos: Diretoria

Número Mínimo de Ocorrências: 1



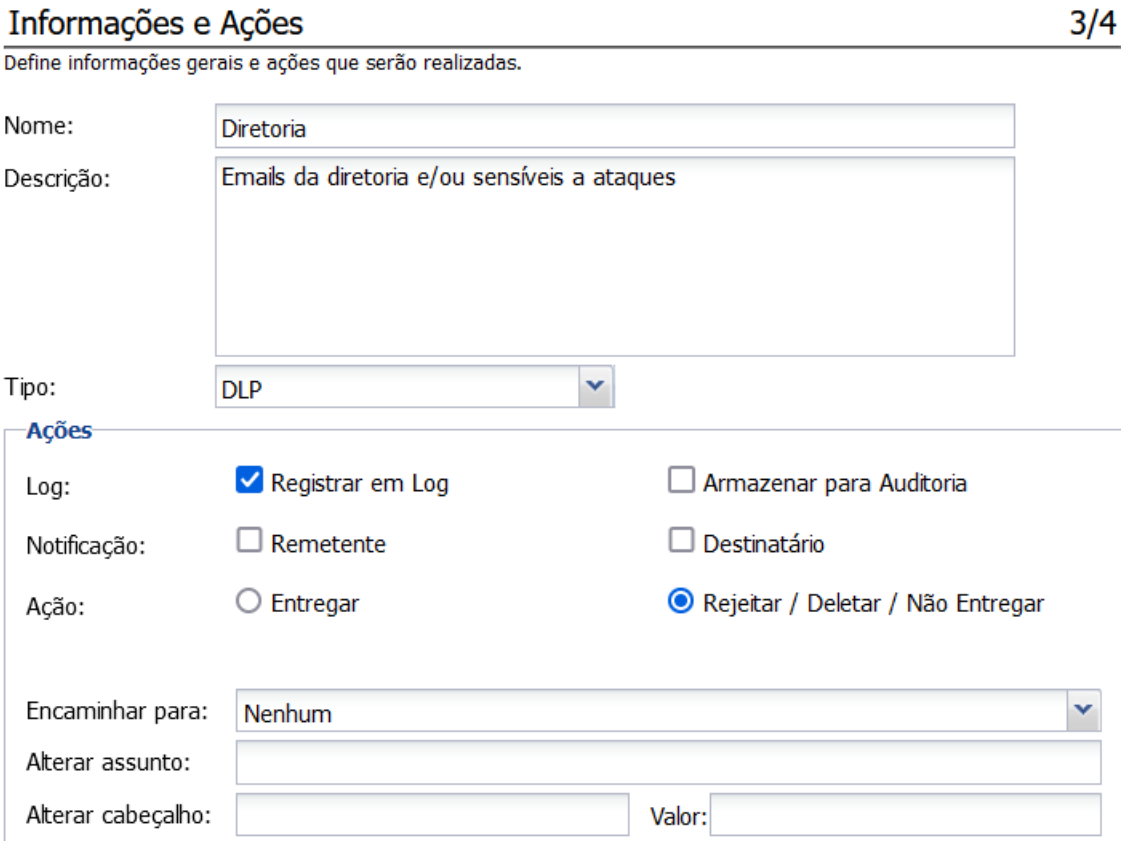
Na etapa de informações e ação

Nome: Diretoria

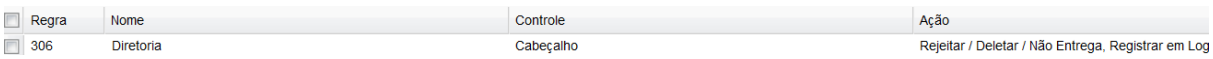
Descrição: Emails da diretoria e/ou sensíveis a ataques

Tipo: DLP

Ações:
Log: Marque a opção Registrar em Log
Notificação: Não marque nada
Ação: Rejeitar / Deletar / Não Entregar
Encaminhar para: Nenhum



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



Regra de DLP – Display Name

Configurações > Email Compliance > Regras

Clique em Adicionar

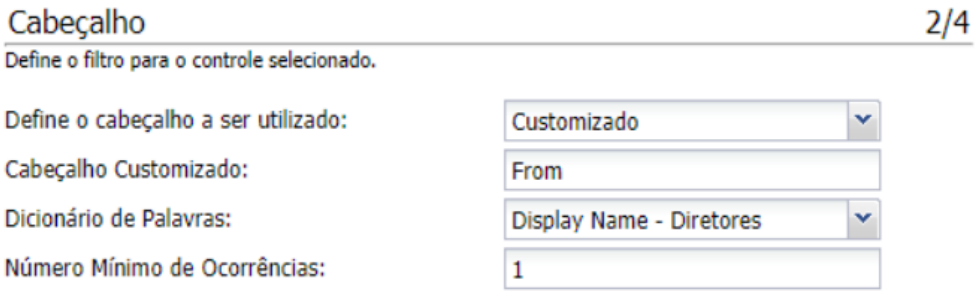
Seleção de Controle: Cabeçalho

Define o cabeçalho a ser utilizado: Customizad

Cabeçalho Customizado: From

Dicionário de Palavras: Display Name - Diretores

Número Mínimo de Ocorrências: 1



Clique em Avançar

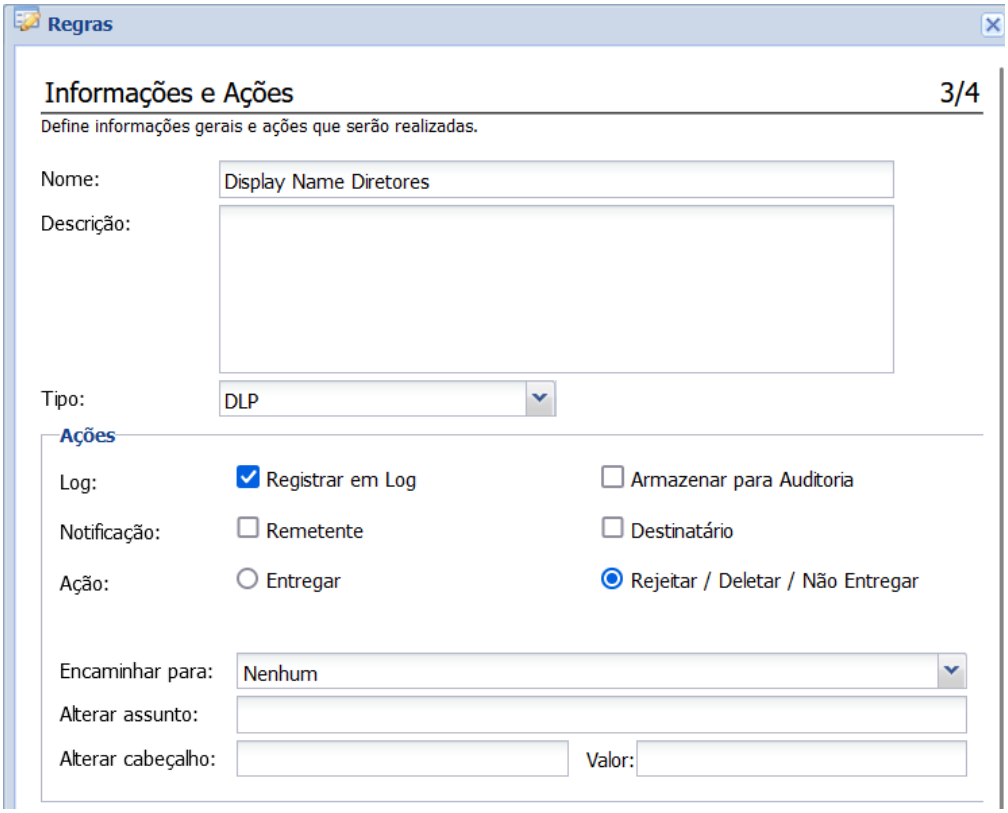
Na etapa de Informações e Ações

Nome: Display Name Diretores

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

Tipo: DLP

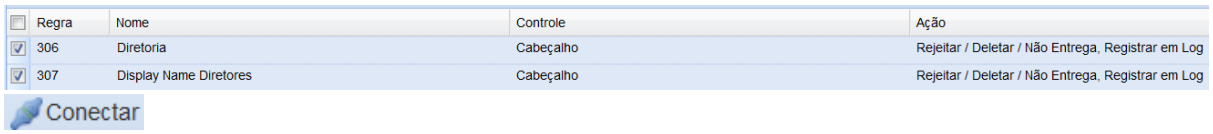
Ações:
Log: Marque a opção Registrar em Log
Notificação: Não marque nada
Ação: Rejeitar / Deletar / Não Entregar
Encaminhar para: Nenhum



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

Casando as Regras

Selecione as duas regras que você criou e clique em Conectar



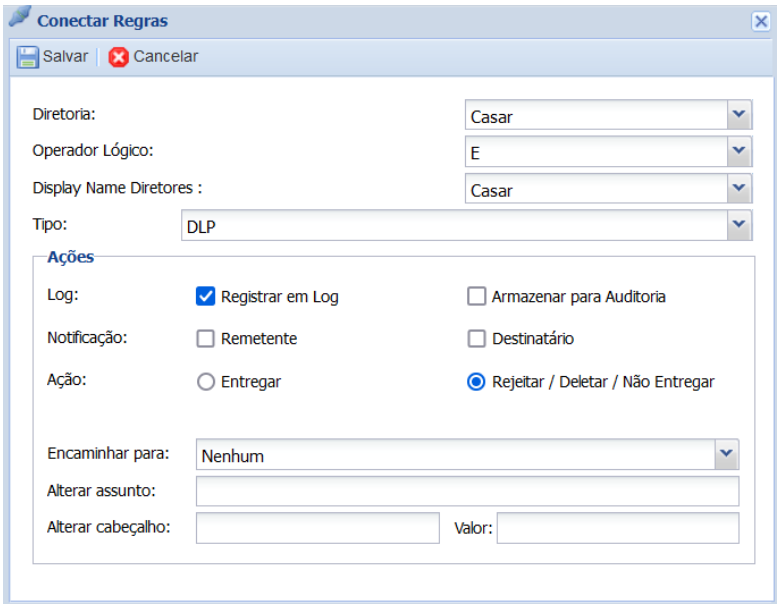
A ideia é para quando os emails foram para os diretores, mas o Display Name não se casar, é porque foi alguém que colocou um Display Name diferente do que é usado na empresa para aquele diretor, portanto, é email forjado.

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



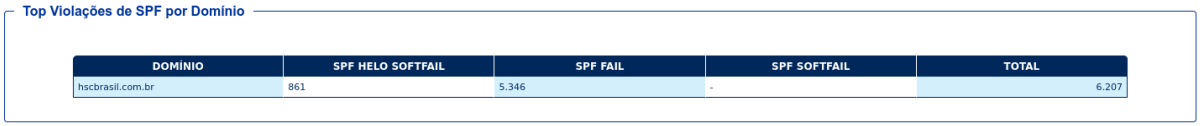
Regra	Nome	Controle	Ação
308	(Diretoria) **E** (Display Name Diretores)	(Cabeçalho) **E** (Cabeçalho)	Registrar em Log, Rejeitar / Deletar / Não Entregar, DLP, Encaminhar para:

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

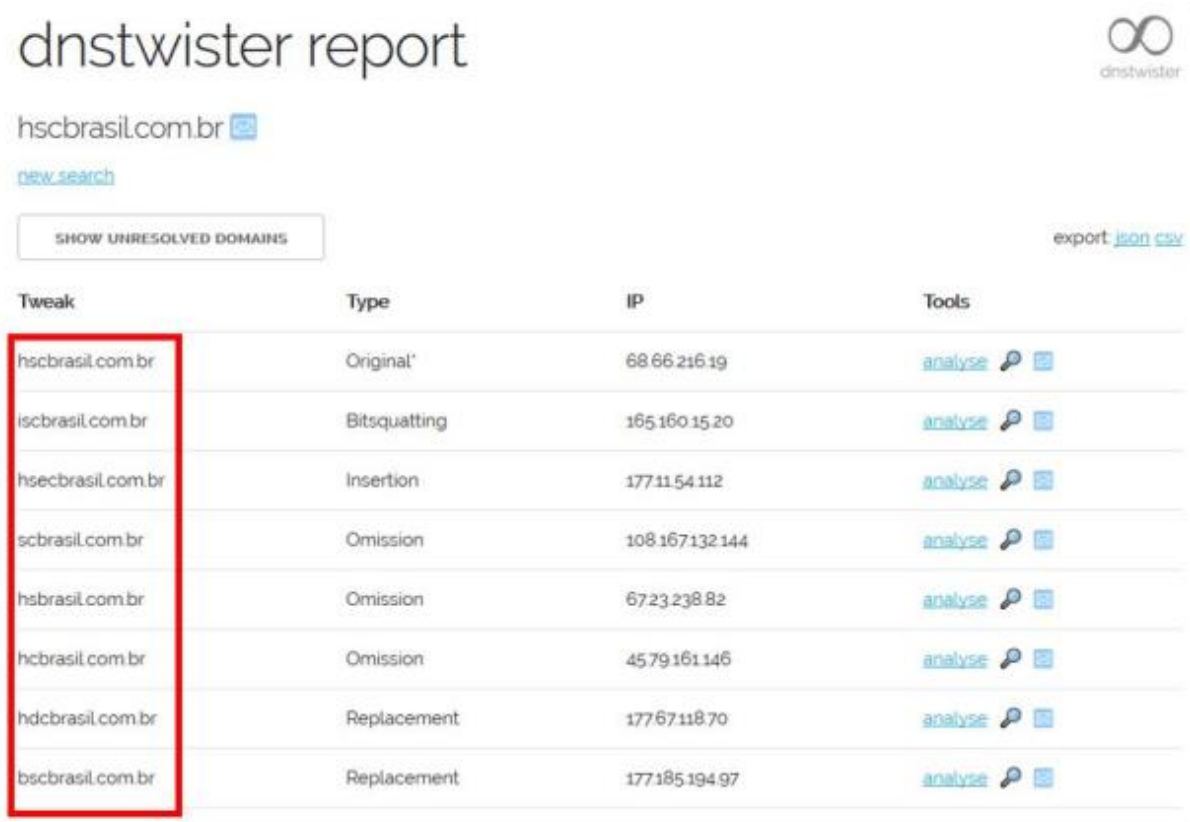
Os domínios primos geralmente são criados como uma ferramenta de phishing para falsificar sua marca e seu nome de domínio.

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

dnstwister

hscbrasil.com.br

new search

SHOW UNRESOLVED DOMAINS

export: json csv

Tweak	Type	IP	Tools
hscbrasil.com.br	Original*	68.66.216.19	analyse
iscbrasil.com.br	Bitsquatting	165.160.15.20	analyse
hsecbrasil.com.br	Insertion	177.11.54.112	analyse
scbrasil.com.br	Omission	108.167.132.144	analyse
hsbrasil.com.br	Omission	67.23.238.82	analyse
hcbrasil.com.br	Omission	45.79.161.146	analyse
hdcbrasil.com.br	Replacement	177.67.118.70	analyse
bscbrasil.com.br	Replacement	177.185.194.97	analyse

Então temos os domínios variantes:

- icsbrasil.com.br
- hsebrasil.com.br
- hdcbrasil.com.br
- scbrasil.com.br
- scbrasil.com.br
- hscbrasil.com.br

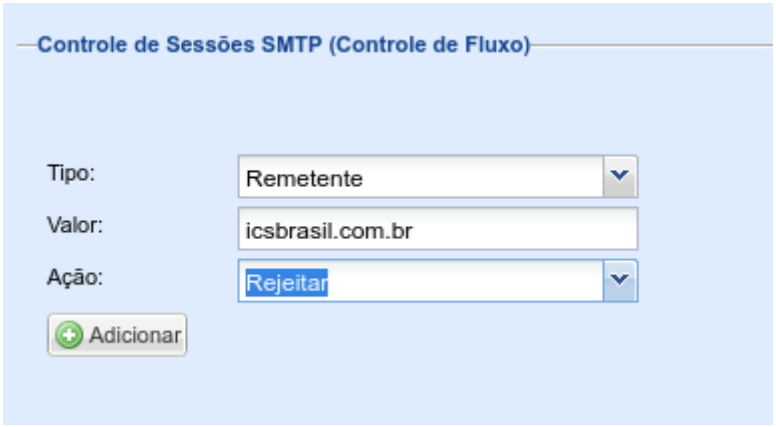
É possível também verificar os domínios que ainda não foram registrados (possíveis domínios similares), para isso, basta clicar no botão SHOW UNRESOLVED DOMAINS.

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:



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

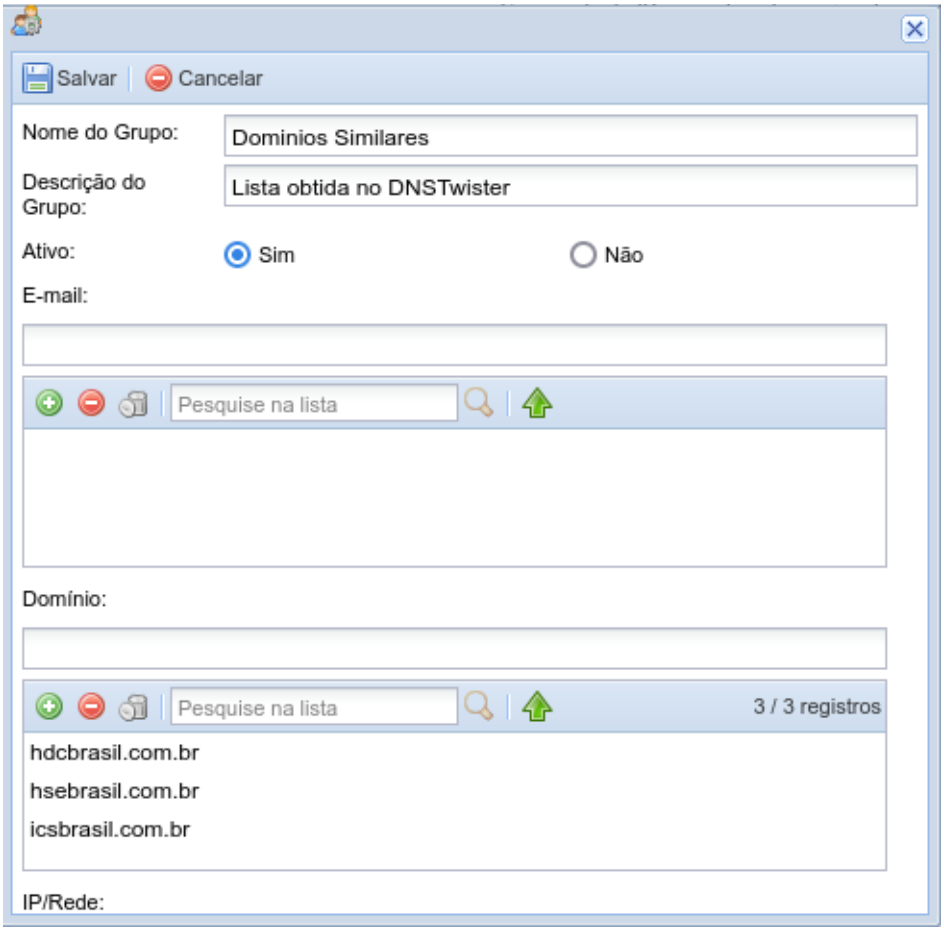
Clique em Salvar.

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:

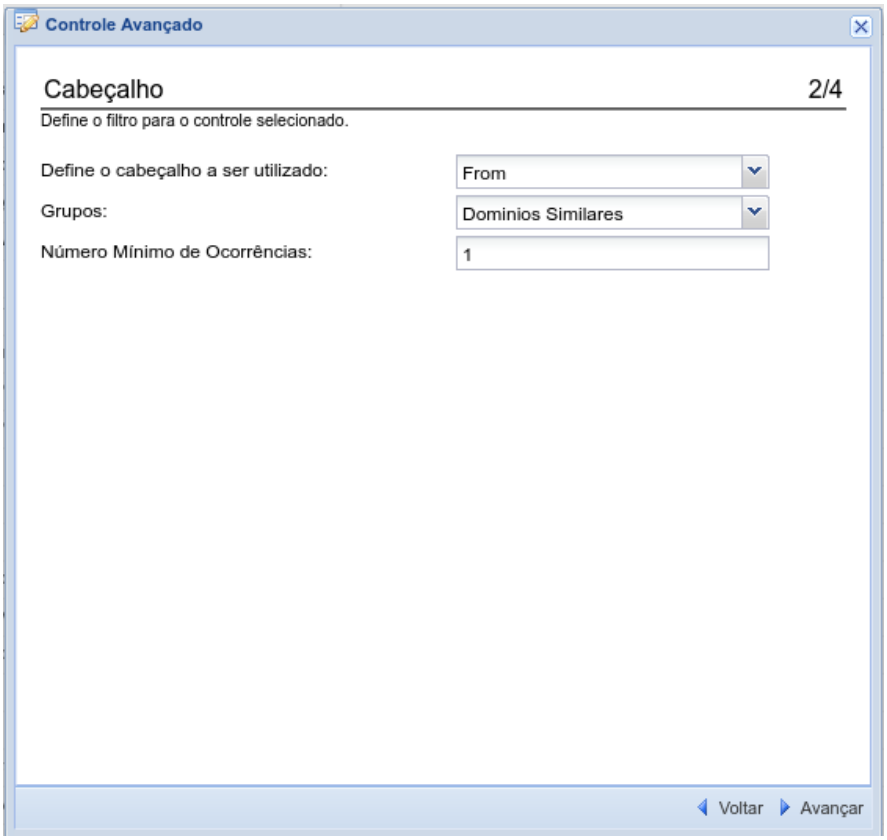


Clique em Salvar

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

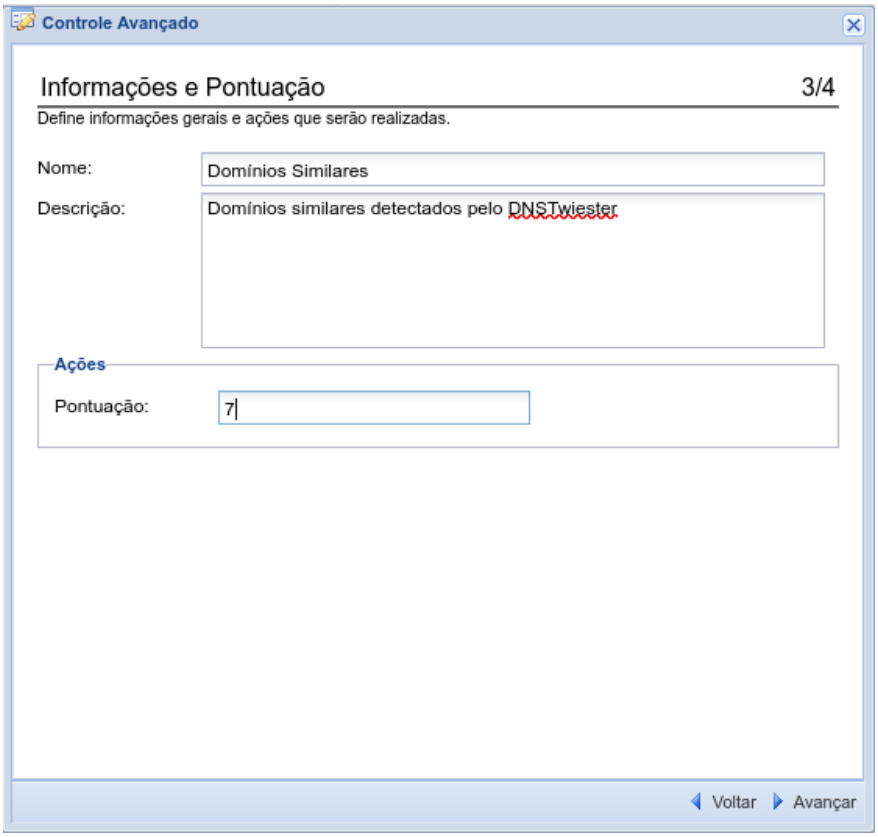
Descrição: Domínios similares detectados pelo DNSTwiester

Pontuação: 7

Clique em Avançar

Clique em Salvar

Clique em Aplicar Configurações



3. Quarentena Customizada

Em Configurações > Quarentena > Customizada

Clique em Adicionar

Nome: Domínio similar

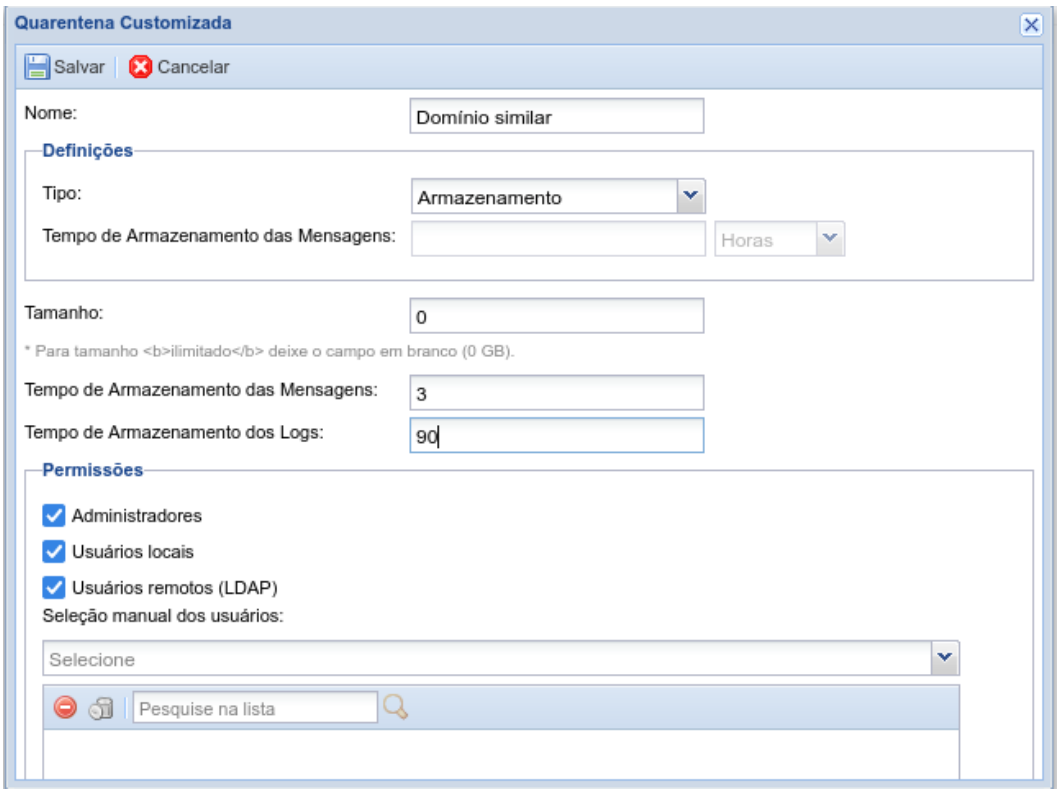
Tipo: Armazenamento

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

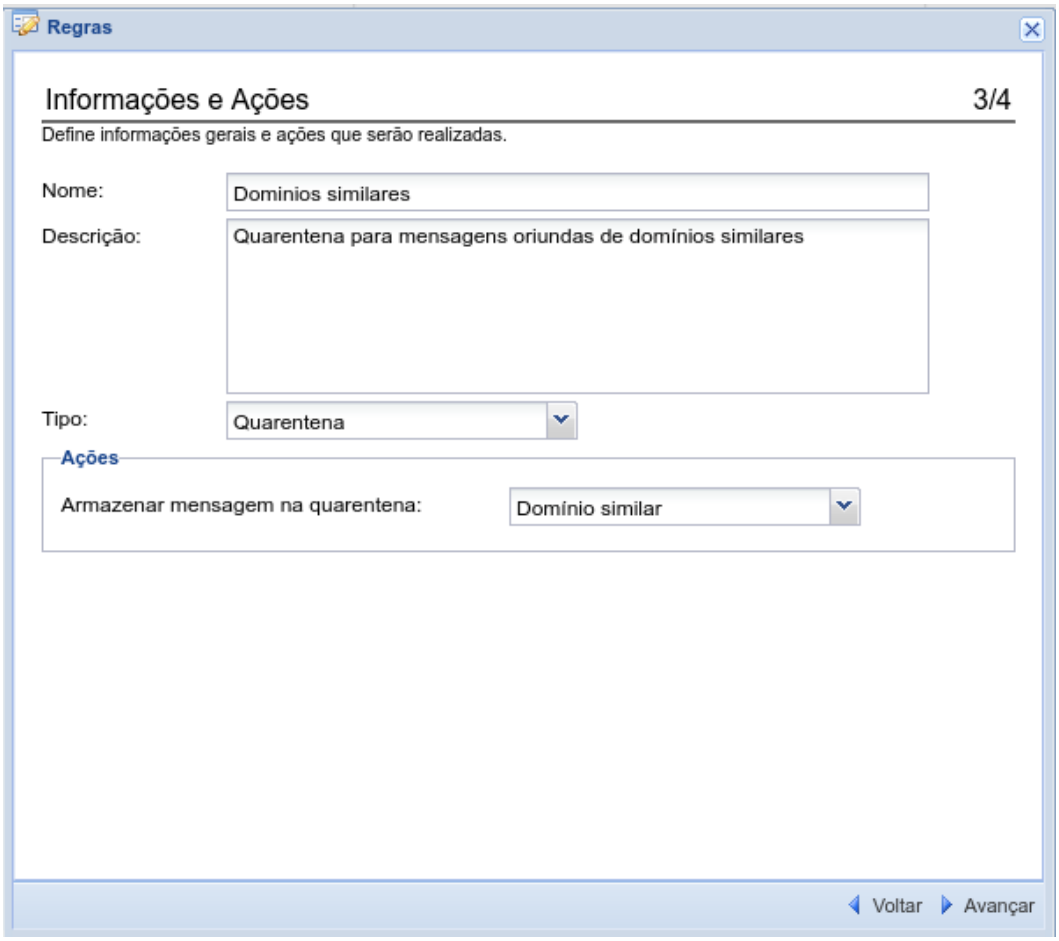
Clique em Avançar

Nome: Domínios similares

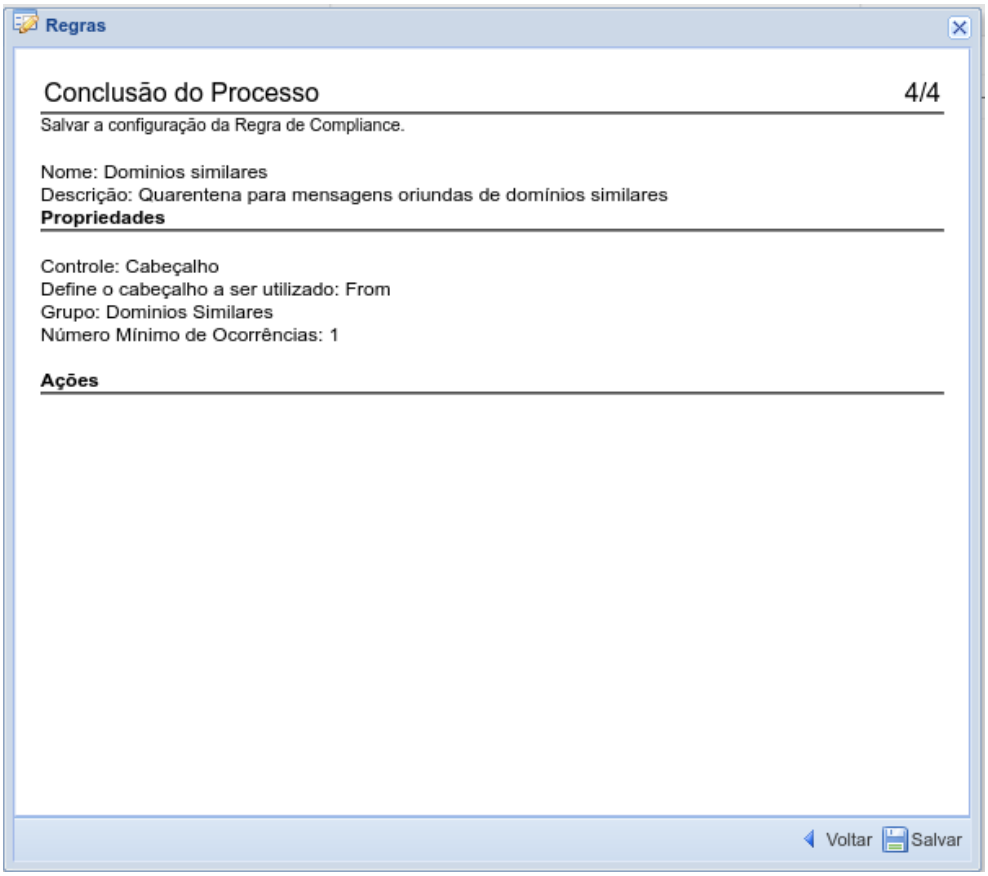
Descrição: Domínios similares

Tipo: Quarentena

Armazenar na Quarentena: Domínio similar



Clique em Avançar



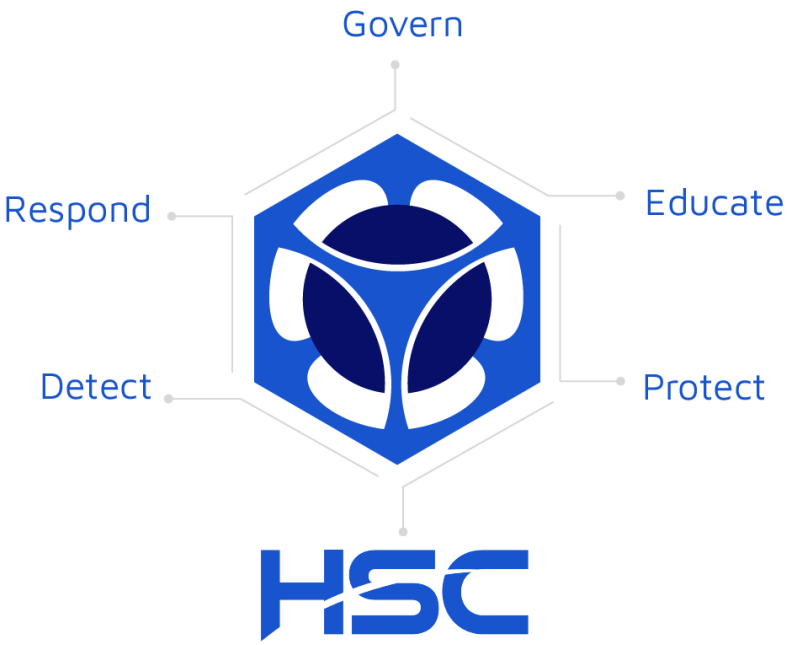
Por último, clique em Salvar e depois em Aplicar Configurações.

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.

hsclabs.com

+55 51 3500 8255