

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

Email original

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

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

Conotação financeira

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 <suporte@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.milcloud.com.br

Filtros de Conteúdo

Filtros de Spam

Ameaças

Cabeçalho

Texto

HTML

Anexos

Outra Lista de Exceções

Smart Defender

Status:

Vírus:

Contido Bloqueado:

WhiteList:

E-mail Marketing:

Arquivos suspeitos:

Spam:

Tamanho Excedido:

BlackList:

Redes Sociais:

Spoofing de domínio:

Provável Spam:

Outro Bloqueio:

Possível Ameaça:

E-mails suspeitos:

URLs:

http://fatursimplesfinan.com/paga?cobranca.spadim?recalcular...

Engines: globalBlacklist Details: [preLoad/0003_vil_hsc] Phishing

1. Criação de Display Name customizados

Configurações > Cadastro > Dicionário de Palavras

Clique em Adicionar

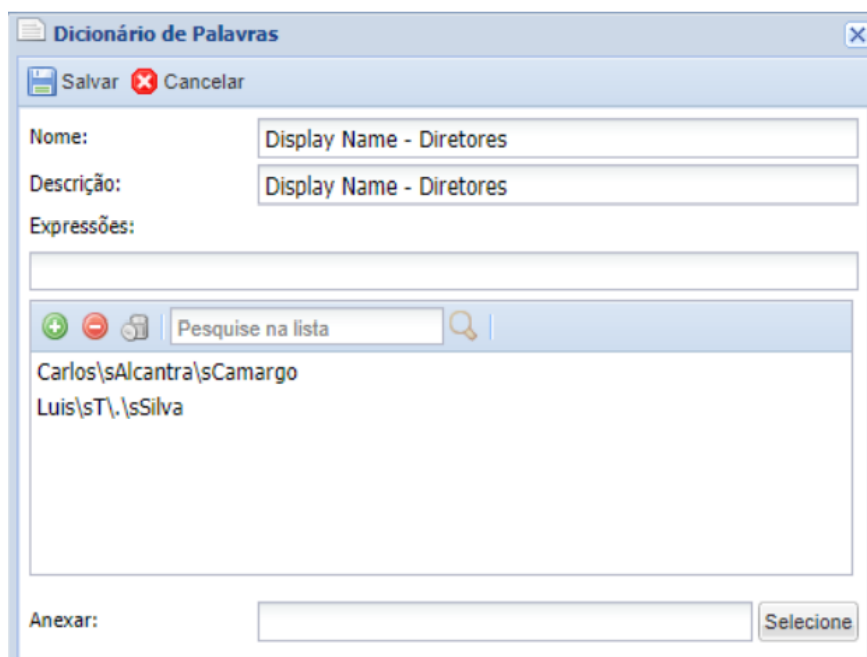
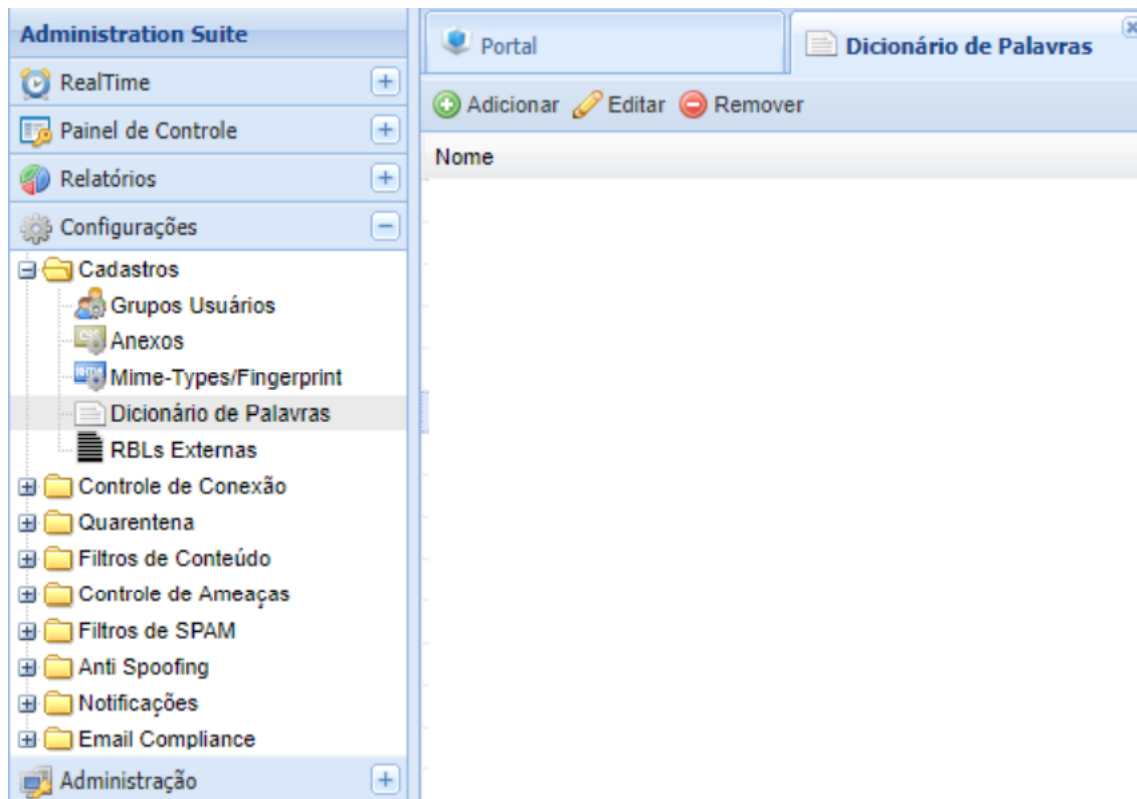
Insira no nome do Dicionário (no exemplo foi **Display Name - Diretores**), descrição as expressões regulares que comporiam o Display Name.

MAILINSPECTOR

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

No exemplo, vamos considerar 2 diretores:

- Carlos Alcantra Camargo
- Luis T. Silva



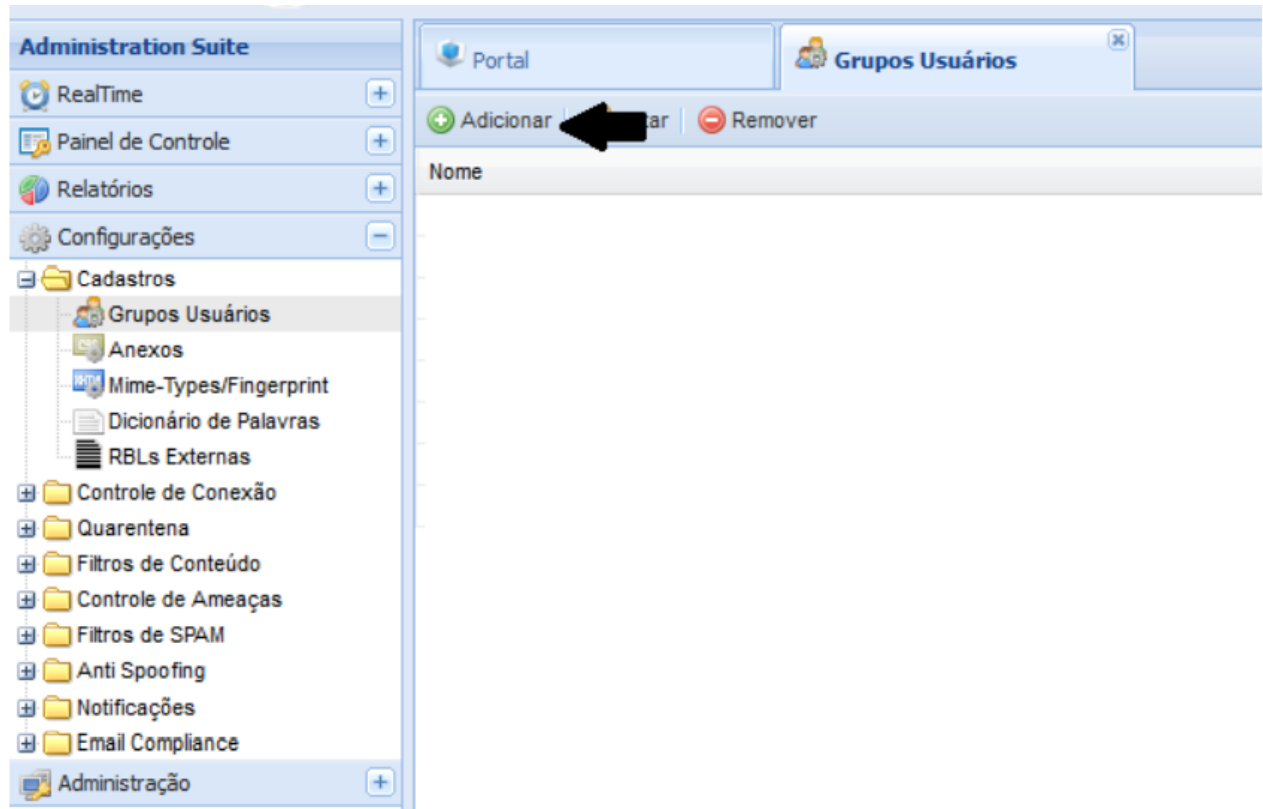
Após inserida toda as **expressões regulares**, clique em Salvar.

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.



Grupos Usuários

Salvar Cancelar

Nome do Grupo:
Diretoria

Descrição do Grupo:
Emails internos sensíveis a ataques

Ativo:
☒ Sim ☐ Não

E-mail:
cfo@hscbrasil.com.br

Pesquise na lista

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

MAILINSPECTOR

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:

Descrição:

Tipo:

Ações

Log: ☒ Registrar em Log ☐ Armazenar para Auditoria

Notificação: ☐ Remetente ☐ Destinatário

Ação: ☐ Entregar ☒ Rejeitar / Deletar / Não Entregar

Encaminhar para:

Alterar assunto:

Alterar cabeçalho: Valor:

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

<input type="checkbox"/> Regra	Nome	Controle	Ação
<input type="checkbox"/> 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

MAILINSPECTOR

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

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

MAILINSPECTOR

 **Regras** 

Informações e Ações 3/4

Defina informações gerais e ações que serão realizadas.

Nome:

Descrição:

Tipo:

Ações

Log: ☒ Registrar em Log ☐ Armazenar para Auditoria

Notificação: ☐ Remetente ☐ Destinatário

Ação: ☐ Entregar ☒ 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

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

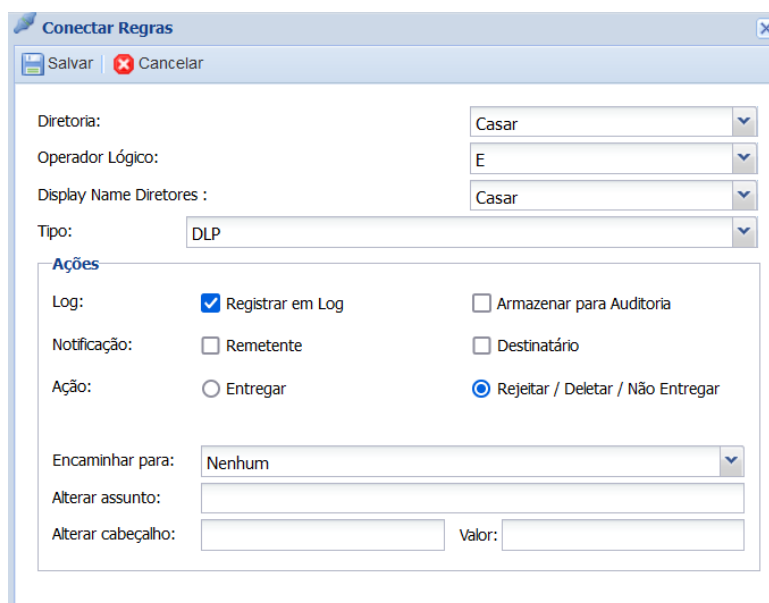
Notificação: Não marque nada

MAILINSPECTOR

Ação: Rejeitar / Deletar / Não Entregar

Encaminhar para: Nenhum

Clique em Salvar



The image shows a 'Conectar Regras' (Connect Rules) dialog box. It has a title bar with a close button. Below the title bar are two buttons: 'Salvar' (Save) and 'Cancelar' (Cancel). The dialog contains several fields: 'Diretoria:' with a dropdown menu showing 'Casar'; 'Operador Lógico:' with a dropdown menu showing 'E'; 'Display Name Diretores :' with a dropdown menu showing 'Casar'; 'Tipo:' with a dropdown menu showing 'DLP'. Below these fields is a section titled 'Ações' (Actions) which contains three rows of checkboxes: 'Log:' with 'Registrar em Log' checked and 'Armazenar para Auditoria' unchecked; 'Notificação:' with 'Remetente' and 'Destinatário' both unchecked; 'Ação:' with 'Entregar' unchecked and 'Rejeitar / Deletar / Não Entregar' checked. Below the 'Ações' section are three more fields: 'Encaminhar para:' with a dropdown menu showing 'Nenhum'; 'Alterar assunto:' with an empty text box; and 'Alterar cabeçalho:' with two empty text boxes labeled 'Alterar cabeçalho:' and 'Valor:'.

<input type="checkbox"/>	Regra	Nome	Controle	Ação
<input checked="" type="checkbox"/>	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



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](#)

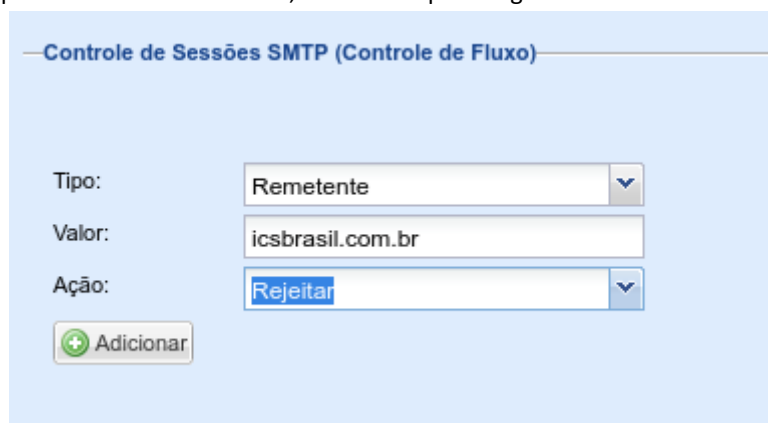
É possível também verificar os domínios que ainda não foram registrados (possíveis domínios similares), para isso, basta clicar no botão SHOW UNRESOLVED DOMAINS.

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:



The screenshot shows the 'Controle de Sessões SMTP (Controle de Fluxo)' configuration page. It features three input fields: 'Tipo' with a dropdown menu set to 'Remetente', 'Valor' with the text 'icsbrasil.com.br', and 'Ação' with a dropdown menu set to 'Rejeitar'. Below these fields is a green button with a plus icon and the text '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:

Pesquise na lista

Domínio:

Pesquise na lista 3 / 3 registros

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

MAILINSPECTOR

Controle Avançado

Cabeçalho 2/4

Define o filtro para o controle selecionado.

Define o cabeçalho a ser utilizado: From

Grupos: Dominios Similares

Número Mínimo de Ocorrências: 1

Voltar Avançar

Clique em Avançar

Nome: Domínios Similares

Descrição: Domínios similares detectados pelo DNSTwister



Pontuação: 7

Clique em Avançar

Clique em Salvar

Clique em Aplicar Configurações

MAILINSPECTOR

 **Controle Avançado** 

Informações e Pontuação 3/4

Define informações gerais e ações que serão realizadas.

Nome:

Descrição:

Ações

Pontuação:

[< 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

The screenshot shows the 'Quarentena Customizada' (Custom Quarantine) dialog box. It has a title bar with a close button. Below the title bar are 'Salvar' (Save) and 'Cancelar' (Cancel) buttons. The form contains the following fields and sections:

- Nome:** A text field containing 'Domínio similar'.
- Definições:** A section containing:
 - Tipo:** A dropdown menu set to 'Armazenamento'.
 - Tempo de Armazenamento das Mensagens:** A text field with a value of 3, followed by a unit dropdown menu set to 'Horas'.
- Tamanho:** A text field with a value of 0.
- * Para tamanho ilimitado deixe o campo em branco (0 GB).
- Tempo de Armazenamento das Mensagens:** A text field with a value of 3.
- Tempo de Armazenamento dos Logs:** A text field with a value of 90.
- Permissões:** A section containing three checked checkboxes: 'Administradores', 'Usuários locais', and 'Usuários remotos (LDAP)'. Below these is the text 'Seleção manual dos usuários:' followed by a dropdown menu labeled 'Selecione'.
- At the bottom, there is a search bar with a magnifying glass icon and the text 'Pesquise na lista'.

Em Configurações > Email Compliance > Regras

Clique em Adicionar

Seleção de Controle: Cabeçalho

Define o cabeçalho a ser utilizado: From

Grupos: Domínio Similar

MAILINSPECTOR

Número Mínimo de Ocorrências: 1

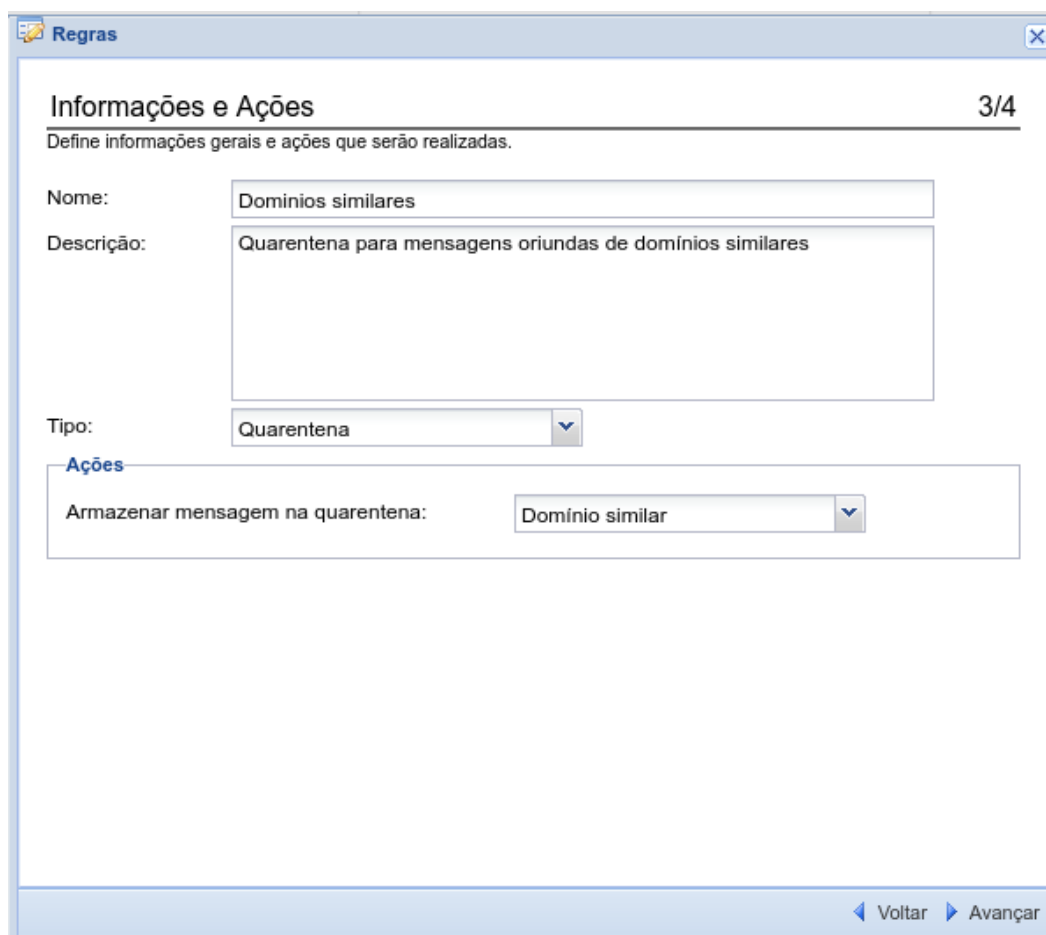
Clique em Avançar

Nome: Domínios similares

Descrição: Domínios similares

Tipo: Quarentena

Armazenar na Quarentena: Domínio similar



Regras 3/4

Define informações gerais e ações que serão realizadas.

Nome: Domínios similares

Descrição: Quarentena para mensagens oriundas de domínios similares

Tipo: Quarentena


Ações

Armazenar mensagem na quarentena: Domínio similar

Voltar Avançar

Clique em Avançar

MAILINSPECTOR

 **Regras** ✕

Conclusão do Processo

4/4


Salvar a configuração da Regra de Compliance.

Nome: Domínios similares
Descrição: Quarentena para mensagens oriundas de domínios similares

Propriedades

Controle: Cabeçalho
Define o cabeçalho a ser utilizado: From
Grupo: Domínios Similares
Número Mínimo de Ocorrências: 1

Ações

◀ Voltar  Salvar

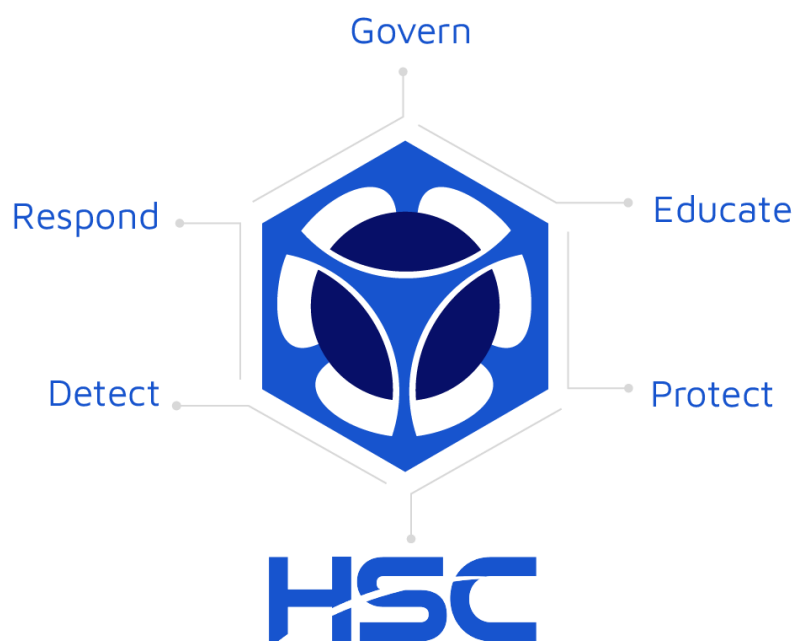
Por último, clique em Salvar e depois em Aplicar Configurações.

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

+55 51 3500 8255