Como tratar arquivos criptografados no MailInspector

O sistema de proteção a e-mails MailInspector, possui múltiplas formas de tratar e-mail com anexo compactado com senha.

1. Controle de anexos compactados com senha;
2. Sistema de DLP;
3. Sistema de análise sobre arquivos CONTIDOS no arquivo compactado com senha;
4. Mecanismo Heurístico de Análise de Senha

Sobre arquivos contidos em Anexos com Senha

Arquivos criptografados podem ser arquivos que passaram por sistema de criptografia ou arquivos compactados e inserida senha sobre os mesmos. O MailInspector trabalha com todas as formas arquivos criptografados.

No MailInspector, ao selecionar uma ação a ser tomada sobre arquivos, os mesmos são indicados sobre estes arquivos mesmo se estiver dentro de arquivos compactados com senha, como por exemplo ZIP, ARJ, RAR, entre outros compactadores. Dessa forma uma vez identificado o arquivo, o MailInspector irá tomar a ação configurada.

O MailInspector considera como arquivo compactado, arquivos que passaram pelos seguintes sistemas de compactação:

• ZIP	• RAR	• CAB	• ACE	• ARJ	• BH	• HA
• JAR	• PAK	• LHA	• PKZIP	• BZIP	• GZIP	• ZOO
• 7Z	• TZH	• TGZ	• TAR			

O sistema de detecção de conteúdo em anexos, consegue verificar arquivos contidos dentro de anexos compactados com senha, dessa forma já impedindo passagem de arquivos perigosos, tais como arquivos executáveis (.EXE, .LNK, .SRC, etc) dentro de ZIP's, RAR, 7Z, entre os outros modelos de compactação. Para esse processo o MailInspector faz nativamente, sem necessidade de dicionário de senhas ou heurística, dessa forma bloqueando conteúdos indesejados e/ou arquivos possivelmente perigosos.

O MailInspector também detecta arquivos criptografados com senha, sem necessariamente terem sidos compactados, tais como documento padrão Office, por exemplo: .DOC, .DOCX, .XLS, .XLSX, .PPT, .PPTX, .PDF, etc.

Controle de anexos compactados com senha

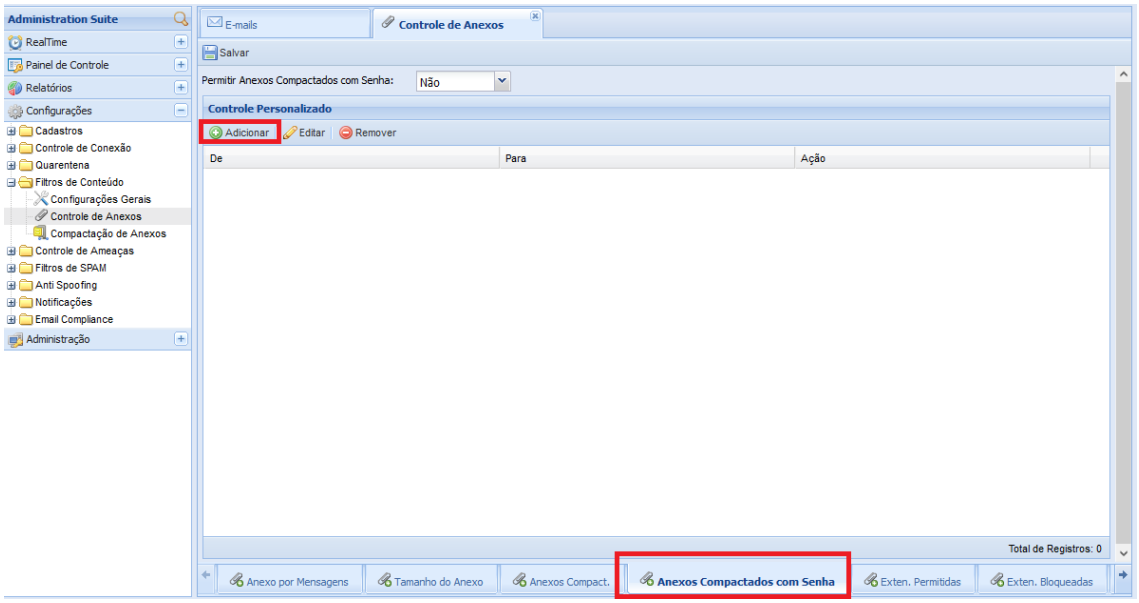
É possível fazer controle sobre anexos compactados com senha em:

Configurações > Filtros de Conteúdo > Controle de Anexos > Anexos Compactados com Senha

Na parte superior onde tem o campo Permitir Anexos Compactados com Senha é o que foi configurado como padrão para a TODA a empresa. Caso você queira fazer alguma exceção, basta clicar em Adicionar e indicar o Grupo Origem e Grupo Destino.

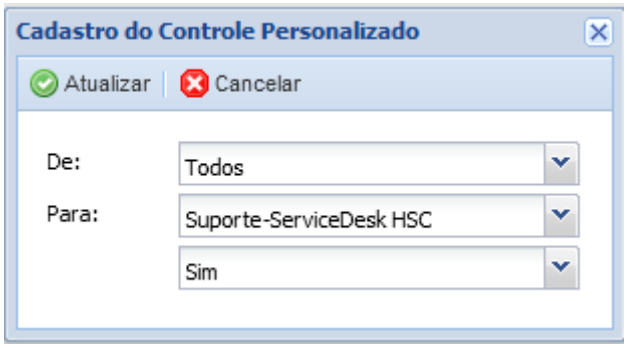
Conforme indicado no manual do MailInspector, consideramos como anexos compactados aplicações utilizando os seguintes compactadores:

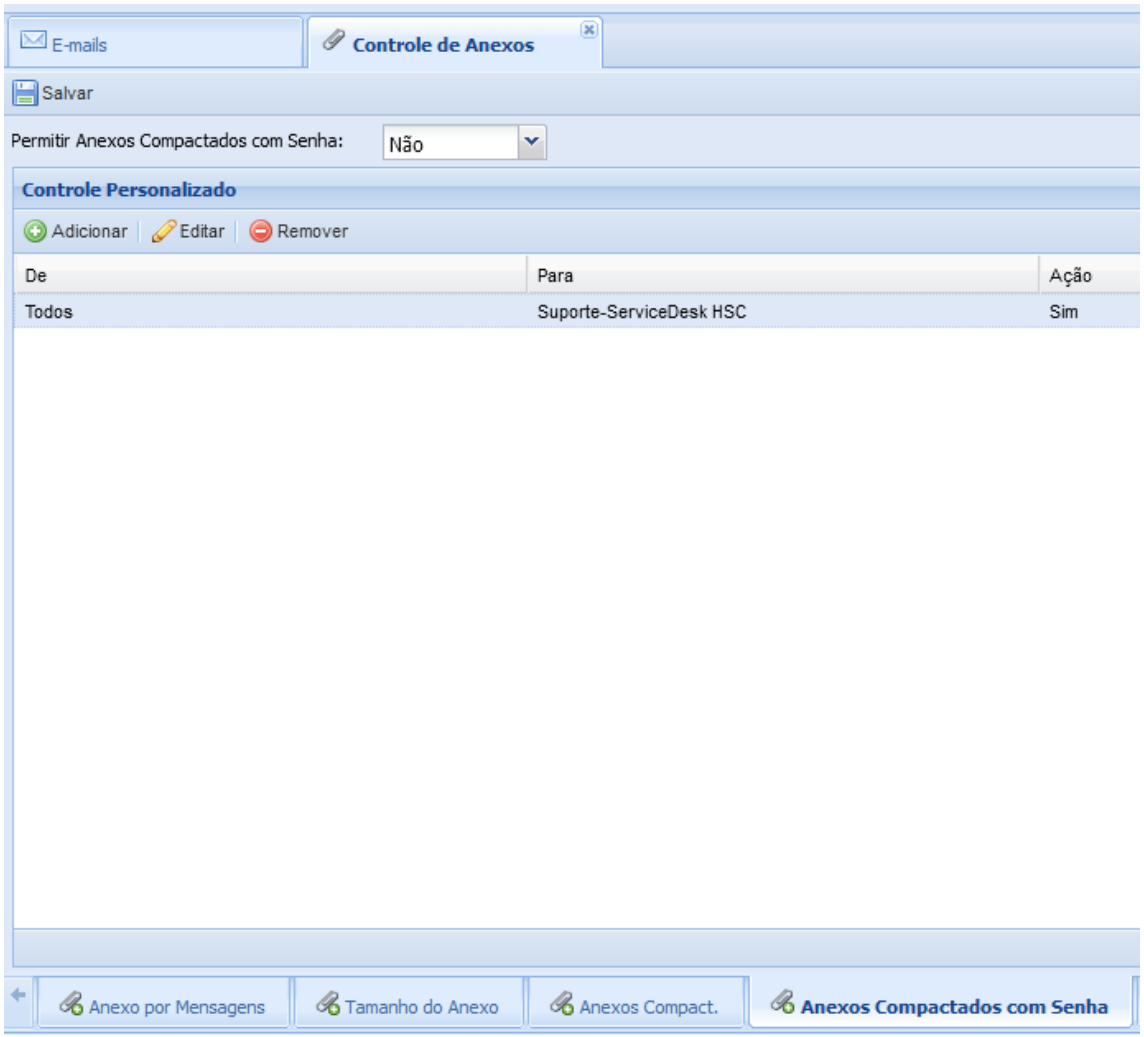
• ZIP	• RAR	• CAB	• ACE	• ARJ	• BH	• HÁ
• JAR	• PAK	• LHA	• PKZIP	• BZIP	• GZIP	• ZOO
• 7Z	• TZH	• TGZ	• TAR			



Dessa forma, é possível deixar configurado por exemplo:

Todo e qualquer e-mail que tiver conteúdo anexo compactado com senha, se for enviado ao sistema de suporte da HSCBRASIL, será aceito.





Também podemos restringir mais ainda essa autorização, sendo que em vez de Todos para Suporte da SHCBRASIL, poderíamos ter limitado a um único e-mail, um único domínio ou a um grupo de e-mail ou a um grupo de hosts específicos como Origem do e-mail, com destino ao suporte da HSCBRASIL.

Sistema de DLP

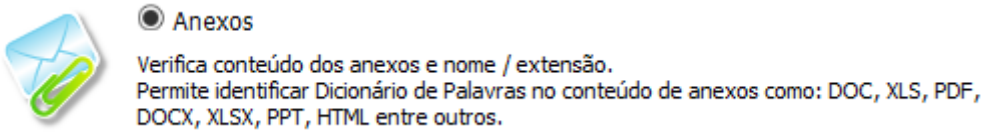
Também é possível fazer controle sobre anexos com senha pelo sistema de DLP, onde irá detectar o anexo por heurística, dicionário e Mime-Type, dessa forma ela já atua verificando a senha do anexo.

Importante salientar que o sistema de DLP identifica além dos sistemas de compactação, também detecta senha dentro de arquivos padrão Office, ou seja, se algum arquivo do tipo Office (SCR, DOC, DOCX, DOCM, XLS, XLSX, SLK, PPT, PPS, PPTX, PDF, XML, HTML, etc, ou similar), o DLP do MailInspector consegue verificar a senha atuar sobre a mesma.

Para utilizar regras de DLP, vá em:

Configurações > E-mail Compliance > Regras

Clique em Adicionar e Selecione o seguinte cabeçalho: Anexos



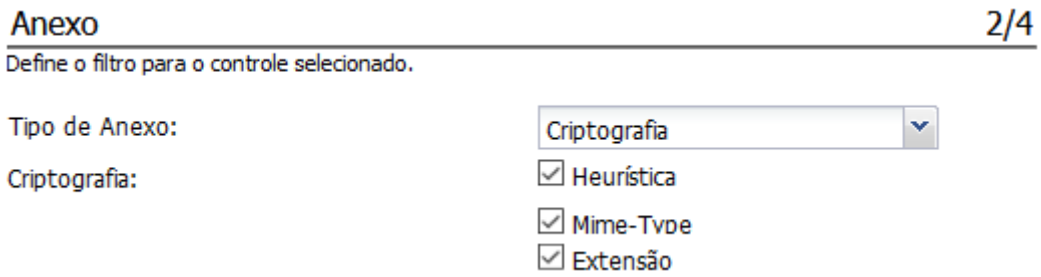
Clique em Avançar

No Tipo de Anexo selecione: Criptografia – Dessa forma o MailInspector irá determinar a forma de detecção do anexo criptografado.

Em Criptografia, marque as formas de criptografia que você deseja que o MLI irá operar sobre o anexo:

- Heurística;
- Mime-Type;
- Extensão

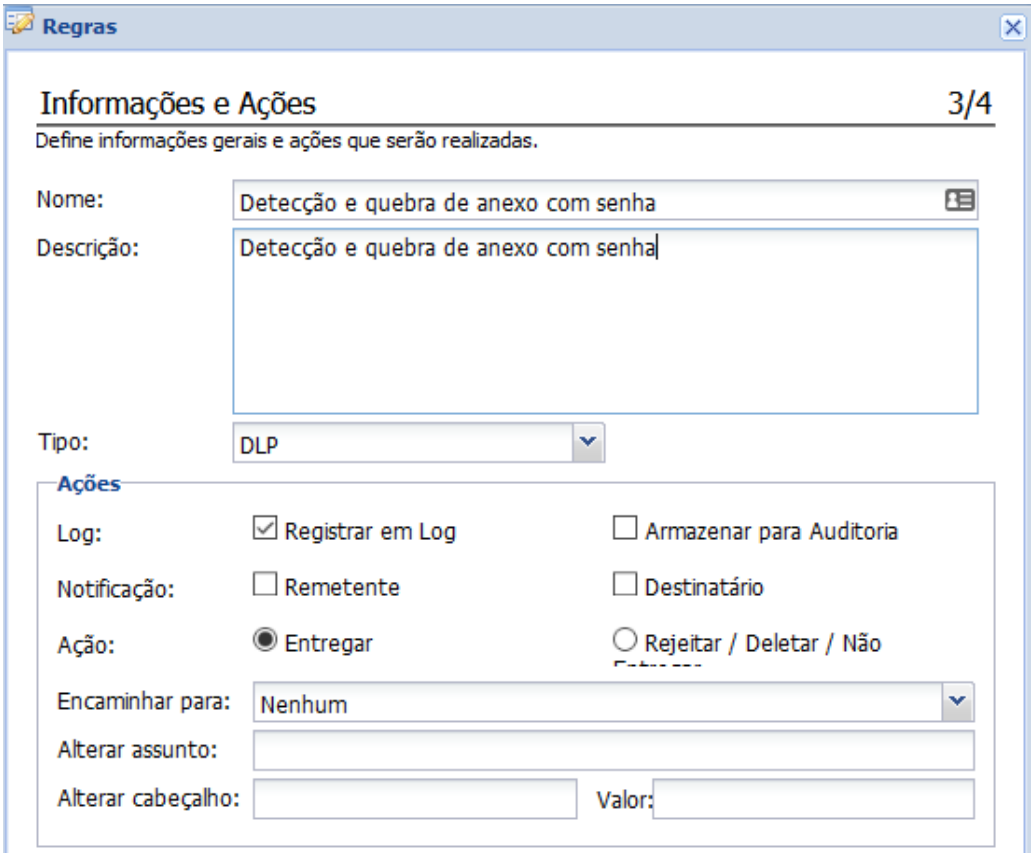
É possível marcar todas para que o MailInspector detecte a forma de trabalha com as três simultaneamente.



Clique em avançar

Dê um nome e descrição a regra e selecione a ação a ser tomada.

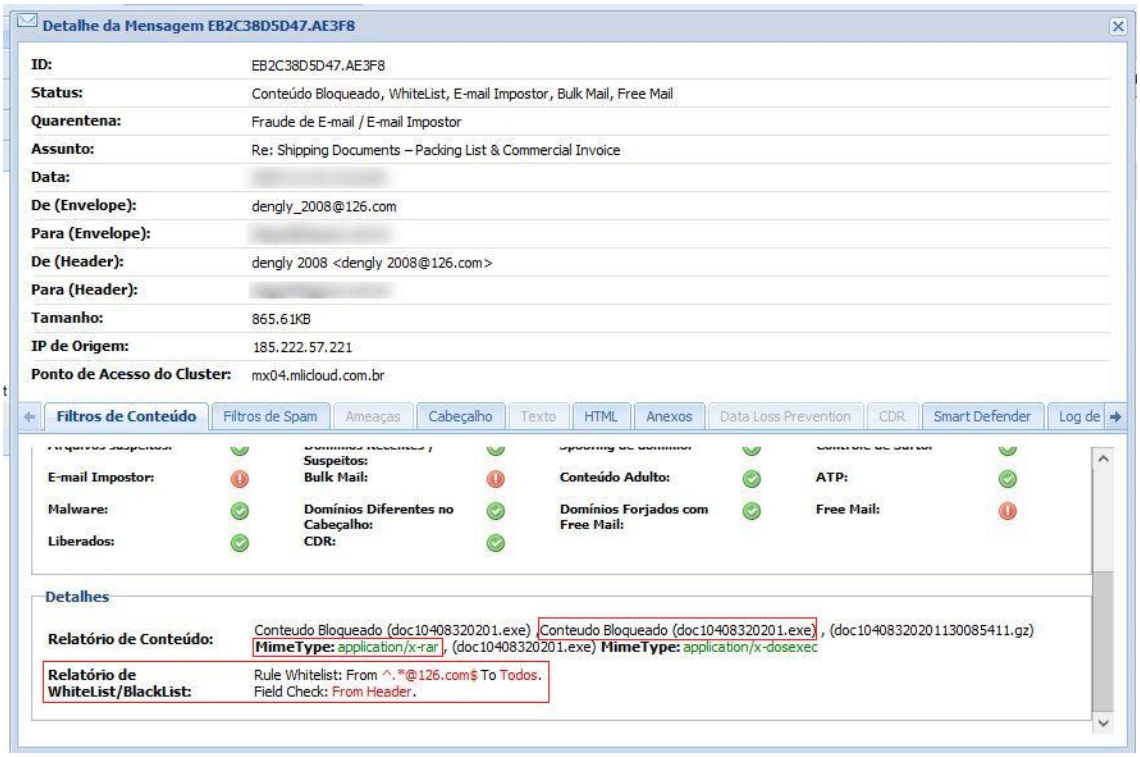
Lembre-se que regras de DLP, podem casar com outras regras de DLP, para deixar mais afinada com o ambiente, tendo controle sobre o FROM, o TO, ou mesmo sobre Subject, tudo isso casando com a regra sobre E-mail Compactado com Anexos com senha.



Sistema de análise sobre arquivos CONTIDOS no arquivo compactado com senha

No MailInspector, ao selecionar uma ação a ser tomada sobre arquivos, os mesmos são indicados sobre estes arquivos mesmo se estiver dentro de arquivos compactados com senha, como por exemplo ZIP ou ARJ ou RAR. Dessa forma uma vez identificado o arquivo, o MailInspector irá tomar a ação configurada.

Repare no exemplo abaixo:



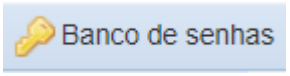
O e-mail foi bloqueado, por haver executável dentro de um arquivo compactado por RAR com senha e mesmo estando em Whitelist do usuário.

Sistema de Banco de Senhas

O MailInspector possui um sistema de controle de senhas, ao qual permite ao administrador cadastrar as senhas utilizadas pela empresa e automaticamente as mesmas serão utilizadas para descriptografar um anexo com senha.

Para acessar o Banco de Senhas, vá em:

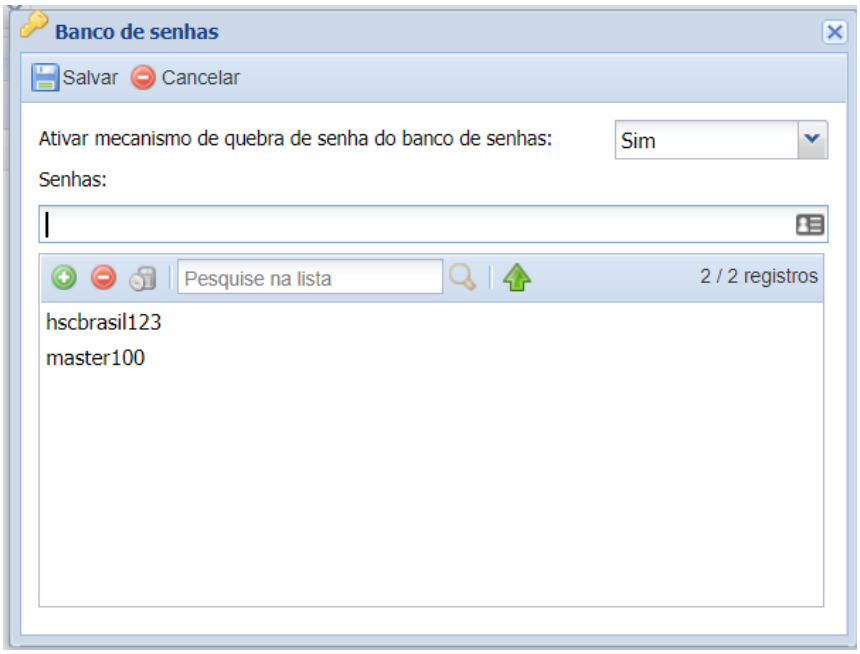
Configurações > Filtro de Conteúdo > Controle de Anexos

No lado direito superior tem o botão Banco de senhas 

O Sistema de Banco de Senhas é responsável pela quebra da senha em arquivos criptografados.

Para efetivar o uso do Sistema Banco de Senhas, o administrador deve ativar a funcionalidade em **Ativar mecanismo de quebra de senha no banco de senhas: Sim**

Ao clicar nele, será aberto o Banco de senhas da sua empresa, sendo possível gerenciar as senhas cadastradas nela.



Serão as senhas que estiverem no Banco de Senhas que serão primeiramente testadas para descriptografar anexos com senha.

Importante salientar que o Banco de Senhas não é somente uma tabela contendo senhas utilizadas pela empresa. O administrador ao ativar o Banco de Senhas, ele estará automaticamente ativando as seguintes funcionalidades:

- Banco de Senhas: Tabela de senhas previamente cadastrado pelo administrador e alimentado automaticamente com novas senhas detectadas pelo sistema ou manualmente pelo administrador;
- Dicionário de senhas: Dicionário de palavras pré-concebidas que são historicamente mais utilizadas por usuários;
- Similaridade do Banco de Senhas: Variantes das senhas cadastradas no Banco de Senhas;
- Similaridade do Dicionário de senhas: Variantes de senhas do dicionário de senhas;
- Heurística de Senhas: Verifica no histórico do usuário senhas anteriormente utilizadas e/ou enviadas, bem como senhas encontradas no corpo de e-mails;

Mecanismo Heurístico de Análise de Senha

O MailInspector faz a verificação das senhas na seguinte sequência:

1. Banco de Senhas: Utiliza as senhas contidas no Banco de Senhas para tentar descriptografar o arquivo;
2. Dicionário de Senhas: Utiliza o dicionário de palavras que contém senhas comumente utilizadas;
3. Similaridade do Banco de Senhas: Combinações possíveis do Banco de Senhas;
4. Similaridade do Dicionário de Senhas: Combinações possíveis do Dicionário de Senhas;

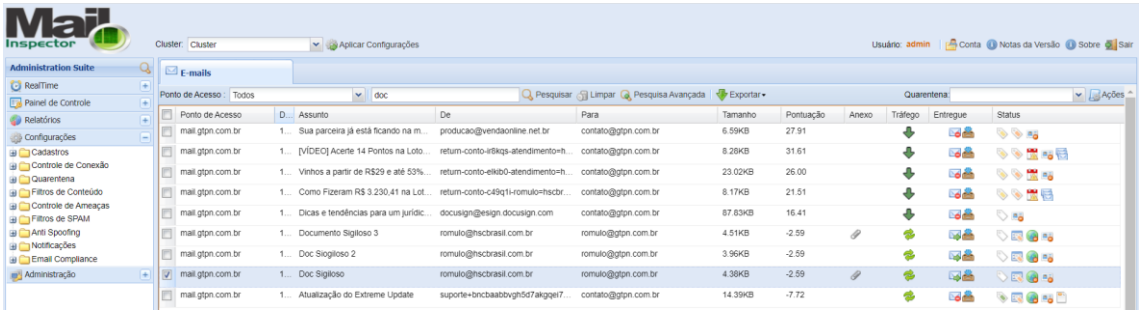
5. Heurística de Senha: O MailInspector irá verificar de forma automática usando heurística o corpo do e-mail, tomando como base todas possíveis senhas que já foram enviadas anteriormente para o usuário, dessa forma, engloba todo o histórico, bem como análise no corpo da mensagem, para verificar se possui alguma senha digitada, incluindo senhas “escondidas”.

Ao utilizar todas as técnicas de combinação de senhas, o MailInspector faz o teste sobre o arquivo criptografado e em caso de sucesso na quebra da senha, o sistema adiciona automaticamente a senha no Banco de Senhas.

Analisando senha em E-mail Específico

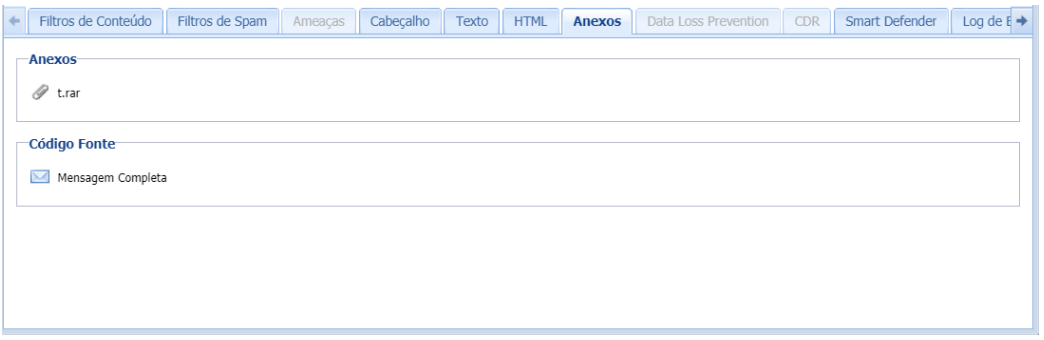
Também é possível efetuar a análise de senha de um e-mail específico com anexo criptografado.

O administrador seleciona o e-mail com anexo criptografado:

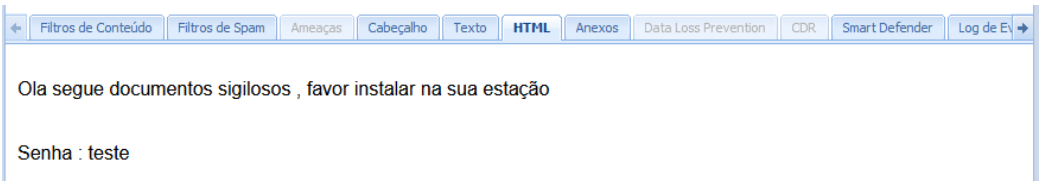


Dados do CORPO do e-mail selecionado:

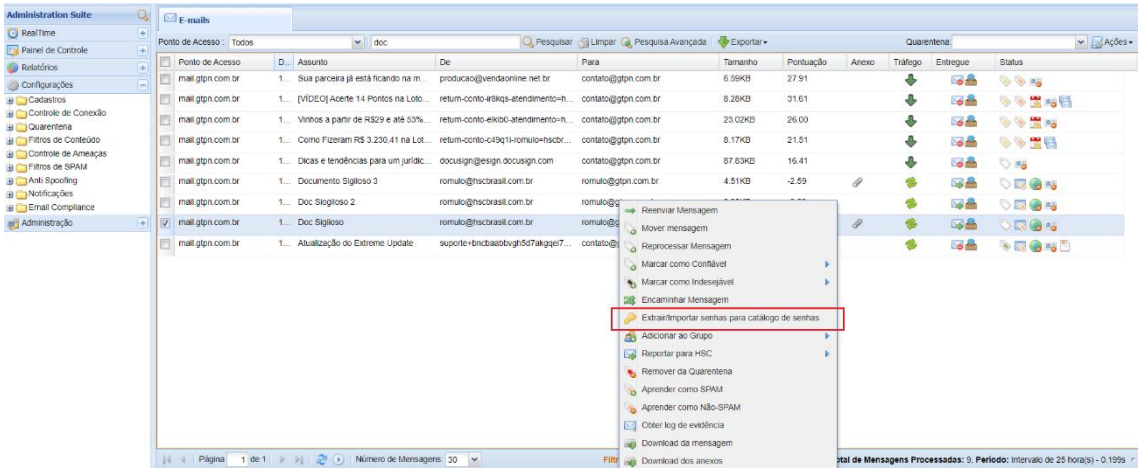
Como pode observar, ele possui um arquivo RAR com senha em anexo.

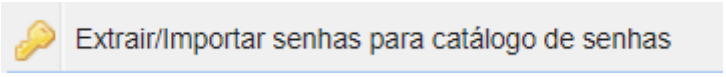


A seguir, veja o e-mail no formato HTML. Repare que a senha está no corpo do e-mail:

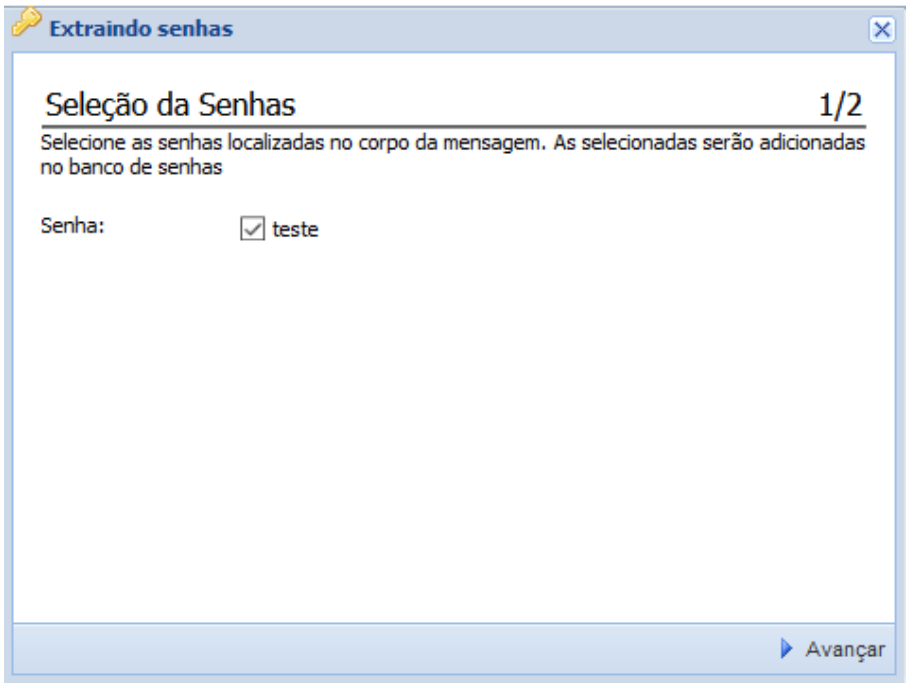


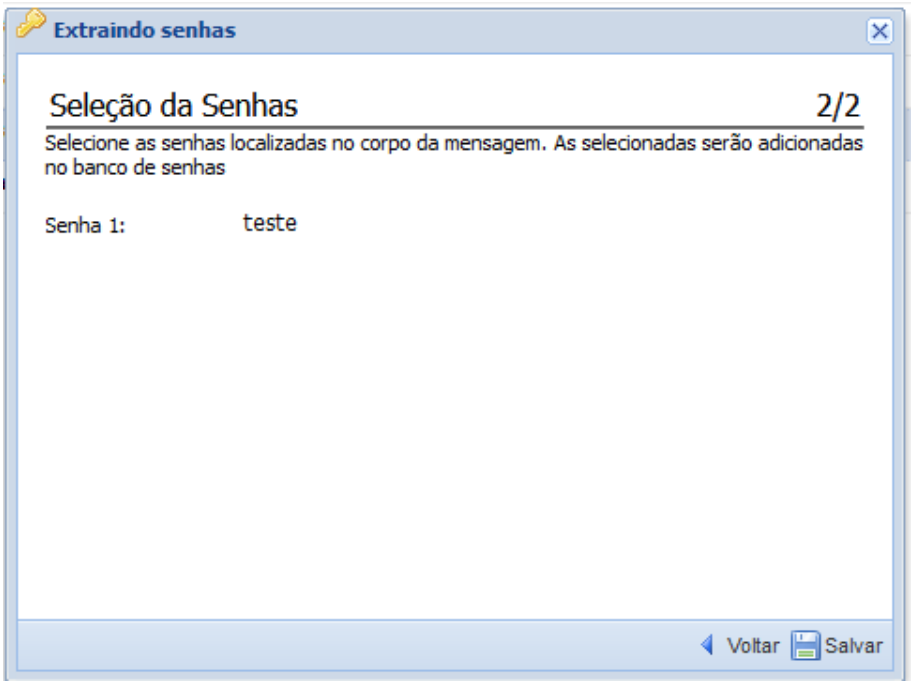
Para ativar o a extração manual da senha, basta clicar o botão direito do mouse sobre o e-mail e selecionar a opção **Exportar/Importar senhas para catálogo de senhas**

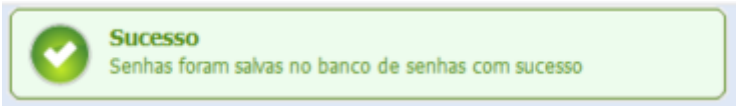


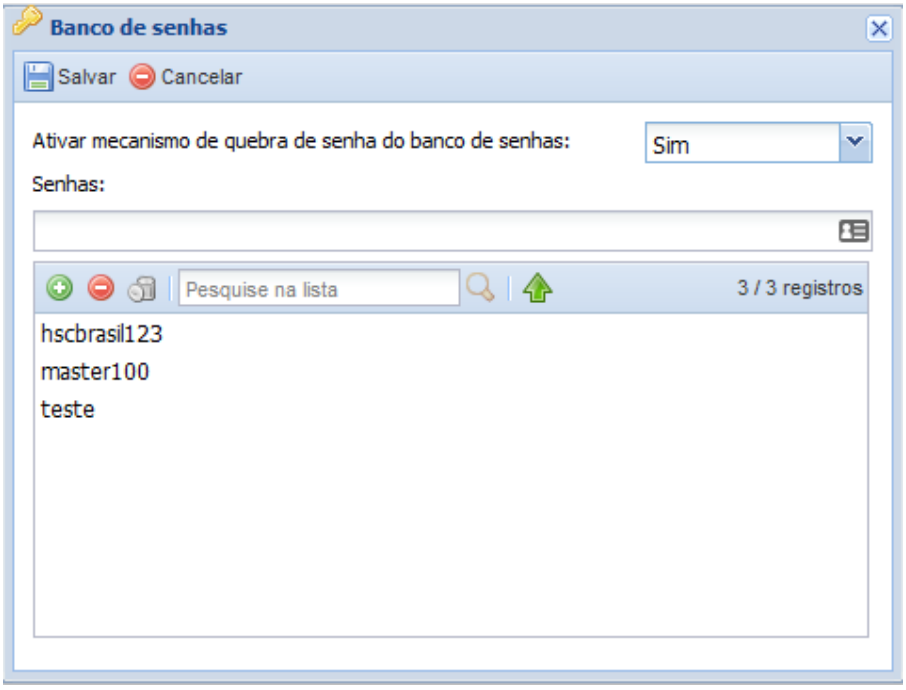


Ao selecionar a opção indicada, o sistema apresentará a senha extraída, permitindo ao administrador adicionar a senha no Banco de Senhas de forma manual, ou simplesmente visualizar a senha do arquivo criptografado. Caso o administrador opte por adicionar a senha ao Banco de Senhas, é só marcar a senha e mandar Salvar a senha no Banco de Senhas, conforme opção indicada a seguir:




Extraindo senhas
Seleção da Senhas
2/2
Selecione as senhas localizadas no corpo da mensagem. As selecionadas serão adicionadas no banco de senhas
Senha 1:
teste
Voltar
Salvar


Sucesso
Senhas foram salvas no banco de senhas com sucesso


Banco de senhas
Salvar
Cancelar
Ativar mecanismo de quebra de senha do banco de senhas:
Sim
Senhas:
Pesquise na lista
3 / 3 registros
hscbrasil123
master100
teste