Despacho de Pregoeiro n° 008/2018-SLC/ANEEL

Em 13 de setembro de 2018.

Processo: 48500.000180/2018-52
Licitação: Pregão Eletrônico nº 15/2018
Assunto: Análise do recurso interposto pela empresa SYBEX COMÉRCIO E SERVIÇOS EM INFORMÁTICA LTDA.

I – JUIZO DE ADMISSIBILIDADE

1. A empresa SYBEX COMÉRCIO E SERVIÇOS EM INFORMÁTICA LTDA registrou seu recurso contra a habilitação da empresa GLOBAL TTI SOLUCOES EM TECNOLOGIA LTDA no Pregão Eletrônico nº 15/2018. O registro ocorreu dentro do prazo fixado no sistema Comprasnet. A empresa vencedora do certame também se manifestou, apresentando suas contrarrazões.

2. A recorrente participou do certame, classificando-se em 5º lugar após a fase de lances.

3. O interesse de agir encontra-se evidentemente atendido, em vista do recurso ser manejado por aquele que o aproveita, caso esse seja julgado procedente.

4. O pressuposto da sucumbência recursal é atendido já que a adjudicação da recorrida representaria o insucesso definitivo no certame.

5. O recurso está regularmente motivado, devolvendo à Administração fatos e direitos.

6. O recurso foi apresentado conforme o previsto no inciso XVIII, art. 4º da Lei n. 10.520/02 e no caput do art. 26 do Decreto Federal n. 5.450/05.

7. Assim posto, conheço do recurso.

II – DA ANÁLISE DO JUÍZO DE RETRATAÇÃO

8. A peça recursal apresenta-se basicamente a irresignação da recorrente quanto a habilitação da proposta da empresa GLOBAL TTI, pois entende que alguns dos itens das especificações técnicas descritas para o objeto licitado, não foram atendidas pela proposta vencedora.

9. Ao todo, o recurso questionou 8 (oito) itens - quesitos, os quais serão tratados individualmente, e, por se tratarem de conteúdo eminentemente técnico, irei valer-me do posicionamento técnico da área de TI da ANEEL na análise de tais quesitos:

Item contestado	Alegações recursais	Contrarrazões	Reanálise técnica	Status final do item
7.1.1.4.1.8.2 - Arquivar qualquer mensagem que viole as políticas corporativas, podendo também enviá-la para a estrutura de arquivamento do órgão;	Motivo: A Solução Symantec Ofertada não possui o recurso de enviar mensagem para a estrutura de arquivamento do órgão. A alegação pode ser facilmente comprovada observando a interface da ferramenta.	*Content filtering policy actions* https://support.symantec.com/en_US/article.HOWTO126503.html#v30166150 *Specifying where to save archived messages* *https://support.symantec.com/en_US/article.HOWTO126815.html* *Content filtering policy actions and what they do* *https://support.symantec.com/en_US/article.HOWTO127817.html*	Evidenciado no trecho da url encaminhada: "*To specify where to save archived messages* *1.In the Control Center, click Content > Settings > Archive.* *2.In the Archive email address box, type a complete email address, such as kyi@symantecexample.com.* *3.In the Archive server host field, type the name of the archive server host.This server host is the host name or IP address for the archive email address that you provided in step 2.* *4.If you provided an Archive server host, in the Archive server port, type the server host's port number.* *5.If you want to route archive messages with MX Lookup to locate the information that corresponds to the archive server host, check Enable MX Lookup.* *6.To make the archive server information available to all of your existing policies, click Apply to all current policies.* *7.Click Save.*	Item atendido
7.1.1.4.2.2.7. - Disponibilizar opção de acesso remoto para eventual manutenção;	Motivo: A Solução Symantec ofertada não tem a opção de acesso remoto para manutenção. A alegação pode ser facilmente comprovada observando a interface da ferramenta.	*smg_10.6_administration_guide* - pág. 759	Não foi encontrado referências à possibilidade de acesso remoto na página 759 do documento informado pela licitante (a página informada trata de métodos utilizados para obter definições atualizadas de antivírus). Entretanto a área técnica encontrou a descrição de opções de acesso remoto disponível na pág. 846 do referido documento - "*Command line interface access methods for virtual appliances" If you configured the virtual appliance with a host name or IP address that resolves on your network, you can use an SSH client to access the command line interface. You can access the virtual appliance from any computer on your network, unless firewall rules prohibit access. For a Windows computer, use an SSH client such as PuTTY. On a UNIX computer you can use the ssh command that is typically included in the operating system.*	Item atendido
7.1.1.4.2.2.18. - Ser capaz de definir a quantidade de níveis de compactação no mesmo anexo que podem ser analisados pela solução;	Motivo: Não é possível definir a quantidade de níveis de compactação no mesmo anexo pela solução Symantec ofertada. A alegação pode ser facilmente comprovada observando a interface da ferramenta.	*Setting limits on nested files* *https://support.symantec.com/en_US/article.HOWTO92883.html*	Evidenciado no trecho da url encaminhada: *"Maximum container scan depth. The nested depth in a container file (such as a .zip file or email message) exceeds the number specified. Do not set this value too high. You can be vulnerable to denial-of-service attacks or zip bombs, which contain many levels of nested files."*	Item atendido
7.1.1.4.2.3.14.2. - Colocar em uma determinada área da quarentena definida pelo administrador;	Motivo: Não é possível determinar a área da quarentena definida pelo administrador.	*Configuring end-user quarantine* *https://support.symantec.com/en_US/article.HOWTO93102.html* *https://support.symantec.com/en_US/article.HOWTO77696.html* , *Smg_10.6_Administration Guide*	O item trata da capacidade da solução de realizar a ação de colocar uma mensagem com vírus em uma determinada área de quarentena definida pelo administrador. Entretanto, a ação é possível conforme informado na Table B-1 - *"Veredicts and actions for email messages"* da pág. 943 do documento *"Smg_10.6_Administration Guide"*, onde é possível verificar como "Action" a criação de um incidente quarentenado em uma pasta definida pelo administrador *"Create a Quarantine Incident"* com a seguinte *"Description"* : *"Hold the message for review in the content quarantine folder that you specify"*	Item atendido
7.1.1.4.2.4.5.1. - Limitar o número de conexões TCP permitidas através de um valor	Motivo: O administrador não consegue configurar o valor de números de conexões TCP	*https://support.symantec.com/en_US/article.HOWTO126458.html*	*"Maximum number of connections: Sets the maximum number of simultaneous inbound connections. The default is 2,000 connections."*	Item atendido

configurável pelo administrador;	permitidas. A alegação pode ser facilmente comprovada observando a interface da ferramenta.			
7.1.1.4.2.4.6. - Ser capaz de limitar o fluxo de mensagens automaticamente, de acordo com o volume de mensagens indevidas recebidas de um endereço IP, controlando com base em: volume de vírus, de spam e de remetentes inválidos;	Motivo: Não é possível limitar o fluxo de mensagens, com base em IP, volume de vírus, spam e de remetentes inválidos, pela solução Symantec Ofertada. A alegação pode ser facilmente comprovada observando a interface da ferramenta.	A solução Symantec preenche o referido requisito, conforme consta na Planilha Ponto a Ponto enviada na Fase de Habilitação e reforçada nas páginas do Admin Guide número 107.	As informações a seguir foram obtidas do documento *"Smg_10.6_Administration Guide* ". Na pag. 107 foi verificado que é possível bloquear emails enviados para destinatários inválidos *"You can configure Symantec Messaging Gateway to accept, reject, or drop any messages that are sent to invalid recipients..."* . Na Pág. 157 verificou-se a possibilidade de bloqueio de emails em ataques de DHA - *"A directory harvest attack works by sending a large quantity of possible email addresses to a site. To enable or disable directory harvest attack recognition 1. In the Control Center, click Reputation > Policies > Bad Senders . 2. To enable or disable directory harvest attack recognition on this page, check Directory Harvest Attack and click Enable or Disable. Or, continue with the next step. 3 Click Directory Harvest Attack"*. Na pag. 155 foi verificado também que é possível barrar ataques de vírus conforme o volume de vírus na mensagem *"Configuring email virus attack recognition - In an email virus attack, a specified quantity of infected email messages has been received from a particular IP address*" indicando ainda na Pág. 156 como especificar o volume mínimo de virus que a mensagem deverá conter para execução de determinada ação em "*email virus recognition - To configure email virus attack recognition: 1 In the Control Center, click Reputation > Policies > Bad Senders. 2 Click Email Virus Attacks. 3 Accept the defaults or modify the values under Email Virus Attack Configuration: Minimum number of virus messages - Number of virus messages from a single server that must be exceeded to trigger the specified action*. Por fim, na pág. 160 foi verificado que por meio da *"Global Bad Sender List da Symantec"* é possível bloquear remetentes por meio do uso dessa lista que já tenham encaminhado um grande volume de spams - *"Symantec Global Bad Senders consists of IP addresses that have sent large amounts of spam to mail servers protected by Symantec"*	Item atendido
7.1.1.4.2.4.7. - Ser capaz de controlar o número máximo de destinatários de um determinado emissor, por endereço IP, domínio, nome reverso, saudação de SMTP ou país;	Motivo: Não é possível controlar o número máximo de destinatários de um determinado emissor por endereço IP, domínio, nome reverso, saudação de SMTP ou país. A alegação pode ser facilmente comprovada observando a interface da ferramenta.	https://support.symantec.com/en_US/article.HOWTO126458.html	A figura inserida nas contrarrazões da licitante demonstrou que é possível limitar o número máximo de destinatários por mensagem. Tal ponto também foi confirmado na pág. 73 do documento *"smg_10.6_Administration Guide"* no trecho *"Maximum number of recipients per message"*. Complementarmente foi verificado nas págs. 387 e 388 , table 14-9 , que é possível configurar em *"content filtering policies"* condições de verificação de partes da mensagem, tais como: endereço de email do sender, envelope HELO, domain names e country codes que poderão resultar em ações de bloqueio de mensagem.	Item atendido
7.1.1.4.2.5.1. Suportar a criação de áreas de quarentena personalizadas para grupos de usuários, bem como para	Não é possível criar áreas de quarentena personalizadas para grupos de usuários ou usuários específicos. A alegação pode ser facilmente comprovada	https://support.symantec.com/en_US/article.HOWTO93102.html	A figura inserida nas contrarrazões da licitante demonstrou inicialmente que é possível permitir que membros de uma "*policy group*" tenham acesso à quarentena de usuário. Complementarmente, foi verificado na pág. 201 da documentação "*smg_10.6_Administration Guide*" que uma determinada "*policy group*" pode conter membros baseados em endereços de email, domínio, ou grupo LDAP (este último inclusive pode até mesmo conter	Item atendido

usuários específicos;	observando a interface da ferramenta.		apenas um usuário) - *"Adding members to a policy group: You can assign members to a policy group based on email addresses, domain names, or LDAP groups for the purpose of applying policies. Once you have created your policy group and added members you can select the policies that you want your group to have.*" Isto posto, na pág. 943, Table B-1 verificou-se ainda que é possível configurar *"filtering policies actions"* pertencentes as eventuais *"content filtering policies"* que , por sua vez estão definidas para determinados *"policies groups"* com as características já descritas acima e que pode ser configuradas com a ação de armazenamento da mensagem em uma determinada área de quarentena especificada pelo administrador denominada de "*quarantine incidents folders*" ou *"content incident folders"* conforme indicado na pág. 407 - *"Create an informational incident - The violation incident is created in the Informational Incidents folder that you specify" e " Create a quarantine incident - The violation incident is created in the Quarantine Incidents folder that you specify".*	

10. Entendo que as reanálises implementadas pela área técnica ratificaram plenamente o entendimento de que a solução apresentada pela licitante vencedora do certame, atende às exigências do instrumento convocatório.

III – CONCLUSÃO

11. Assim, decido por não exercer o juízo de retratação, mantendo a empresa GLOBAL TTI SOLUCOES EM TECNOLOGIA LTDA como vencedora do Pregão Eletrônico nº 15/2018.

ANGELICA LUISA PINTO NOGUEIRA PINHEIRO
Pregoeira

Angélica Luisa Pinto Nogueira (SLC)

De: Igo Rodrigues de Castro (SGI)
Enviado em: quarta-feira, 5 de setembro de 2018 14:31
Para: Angélica Luisa Pinto Nogueira (SLC)
Assunto: RES: recursos - Pregão 15/2018
Anexos: Reanálise técnica - razões do recurso SYBEX contra proposta técnica GlobalTTI.XLSX

Sinalizador de acompanhamento: Acompanhar
Status do sinalizador: Sinalizada

Angélica, boa tarde

Segue a minha análise acerca das contrarrazões apresentadas pela licitante GLobalTTI no recursos em questão.
Por meio dos pontos apresentados (*links* na página do fabricante Symantec) e da realização de uma busca detalhada de funcionalidades da solução descritas na própria documentação inicialmente entregue "*Smg_10.6_Administrtion Guide.pdf*" , que possui 1084 páginas, os itens contestados foram considerados atendidos.

Atenciosamente,

Igo Rodrigues de Castro
Analista Administrativo
Superintendência de Gestão Técnica da Informação - SGI
Telefone: (61) 2192-8671
igocastro@aneel.gov.br
www.aneel.gov.br

De: Angélica Luisa Pinto Nogueira (SLC)
Enviada em: terça-feira, 4 de setembro de 2018 16:58
Para: Igo Rodrigues de Castro (SGI) <igocastro@aneel.gov.br>
Assunto: RES: recursos - Pregão 15/2018

Igo,

Recebi a visita do pessoal da GLOBAL TI que apresentou as contrarrazões por escrito acrescidas de telas reproduzidas, que não poderiam ser colocadas no Sistema Compras Governamentais.
O documento é este do sicnet 48535.003799/2018.

Veja se acrescenta algo, por favor.

Atenciosamente

Angelica Luisa Pinto Nogueira Pinheiro
Analista Administrativo
Superintendencia de Licitações e Controle de Contratos e Convênios - SLC
Telefone: (61) 2192-8654
Fax: (61) 2192- 8666
www.aneel.gov.br

De: Igo Rodrigues de Castro (SGI)
Enviada em: terça-feira, 4 de setembro de 2018 10:46
Para: Angélica Luisa Pinto Nogueira (SLC) <angelicanogueira@aneel.gov.br>
Cc: Rodrigo Vargas Bezerra (SGI) <rvargas@aneel.gov.br>; Herbert Lima Monteiro (SGI) <herbert@aneel.gov.br>
Assunto: RES: recursos - Pregão 15/2018

Angélica,

Seguem as minhas considerações acerca dos recursos da BTM e SYBEX.

Aproveito para solicitar a realização de diligências acerca da proposta técnica da BTM, no sentido de:

a) Apresentar comprovações acerca dos pontos não atendidos na planiha em anexo;
b) Diligenciar o atestado de capacidade técnica de 2011 apresentado pela empresa BTM.

Atenciosamente,

Igo Rodrigues de Castro
Segurança da Informação
Superintendência de Gestão Técnica da Informação - SGI
Telefone: (61) 2192-8671
igocastro@aneel.gov.br
www.aneel.gov.br

De: Angélica Luisa Pinto Nogueira (SLC)
Enviada em: quinta-feira, 30 de agosto de 2018 11:05
Para: Igo Rodrigues de Castro (SGI) <igocastro@aneel.gov.br>
Assunto: recursos - Pregão 15/2018

Igo,

Seguem as razões recursais dos três recursos, para sua avaliação
Atenciosamente

Angelica Luisa Pinto Nogueira Pinheiro
Analista Administrativo
Superintendencia de Licitações e Controle de Contratos e Convênios - SLC
Telefone: (61) 2192-8654
Fax: (61) 2192- 8666
www.aneel.gov.br

Razões do Recurso (SYBEX)		Contrarrazões encaminhadas (GlobalTTI)	Reanálise Técnica (ANEEL)	
Item constestado	**Alegações**	**Evidências complementares**	**Verificação realizada pela área técnica**	**Status final do item**
7.1.1.4.1.8.2 - Arquivar qualquer mensagem que viole as políticas corporativas, podendo também enviá-la para a estrutura de arquivamento do órgão;	Motivo: A Solução Symantec Ofertada não possui o recurso de enviar mensagem para a estrutura de arquivamento do órgão. A alegação pode ser facilmente comprovada observando a interface da ferramenta.	Content filtering policy actions https://support.symantec.com/en_US/article.HOWTO126503.html#v30166150 Specifying where to save archived messages https://support.symantec.com/en_US/article.HOWTO126815.html Content filtering policy actions and what they do https://support.symantec.com/en_US/article.HOWTO127817.html	Evidenciado no trecho da url encaminhada : *"To specify where to save archived messages* *1.In the Control Center, click Content > Settings > Archive.* *2.In the Archive email address box, type a complete email address, such as kyi@symantecexample.com.* *3.In the Archive server host field, type the name of the archive server host.This server host is the host name or IP address for the archive email address that you provided in step 2.* *4.If you provided an* ***Archive server host*** *, in the Archive server port, type the server host's port number.* *5.If you want to route archive messages with MX Lookup to locate the information that corresponds to the archive server host, check Enable MX Lookup.* *6.To make the archive server information available to all of your existing policies, click Apply to all current policies.* *7.Click Save.*	Item atendido
7.1.1.4.2.2.7. - Disponibilizar opção de acesso remoto para eventual manutenção;	Motivo: A Solução Symantec ofertada não tem a opção de acesso remoto para manutenção. A alegação pode ser facilmente comprovada observando a interface da ferramenta.	smg_10.6_administration_guide - pág. 759	Não foi encontrado referências à possibilidade de acesso remoto na página 759 do documento informado pela licitante (a página informada trata de métodos utlizados para obter definições atualizadas de antivírus). Entretanto a área técnica encontrou a descrição de opções de acesso remoto disponível na pág. 846 do referido documento - "*Command line interface access methods for virtual appliances" If you configured the virtual appliance with a host name or IP address that resolves on your network, you can use an SSH client to access the command line interface. You can access the virtual appliance from any computer on your network, unless firewall rules prohibit access. For a Windows computer, use an SSH client such as PuTTY. On a UNIX computer you can use the ssh command that is typically included in the operating system.*	Item atendido
7.1.1.4.2.2.18. - Ser capaz de definir a quantidade de níveis de compactação no mesmo anexo que podem ser analisados pela solução;	Motivo: Não é possível definir a quantidade de níveis de compactação no mesmo anexo pela solução Symantec ofertada. A alegação pode ser facilmente comprovada observando a interface da ferramenta.	Setting limits on nested files https://support.symantec.com/en_US/article.HOWTO92883.html	Evidenciado no trecho da url encaminhada: *"Maximum container scan depth. The nested depth in a container file (such as a .zip file or email message) exceeds the number specified. Do not set this value too high. You can be vulnerable to denial-of-service attacks or zip bombs, which contain many levels of nested files."*	Item atendido
7.1.1.4.2.3.14.2. - Colocar em uma determinada área da quarentena definida pelo administrador;	Motivo: Não é possível determinar a área da quarentena definida pelo administrador.	Configuring end-user quarantine https://support.symantec.com/en_US/article.HOWTO93102.html https://support.symantec.com/en_US/article.HOWTO77696.html, Smg_10.6_Administration Guide	O item trata da capacidade da solução de realizar a ação de colocar uma mensagem com vírus em uma determinada área de quarentena definida pelo administrador. Entretanto, a ação é possível conforme informado na *Table B-1 -" Veredicts and actions for email messages"* da **pág. 943** do documento "Smg_10.6_*Administration Guide"* , onde é possível verificar como *"Action"* a criação de um incidente quarentenado em uma pasta definida pelo administrador *"Create a Quarantine Incident"* com a seguinte "*Description* " : "*Hold the message for review in the* ***content quarantine folder that you specify*** **"**	Item atendido

7.1.1.4.2.4.5.1. - Limitar o número de conexões TCP permitidas através de um valor configurável pelo administrador;	Motivo: O administrador não consegue configurar o valor de números de conexões TCP permitidas. A alegação pode ser facilmente comprovada observando a interface da ferramenta.	https://support.symantec.com/en_US/article.HOWTO126458.html	*"Maximum number of connections: Sets the maximum number of simultaneous inbound connections. The default is 2,000 connections."*	Item atendido
7.1.1.4.2.4.6. - Ser capaz de limitar o fluxo de mensagens automaticamente, de acordo com o volume de mensagens indevidas recebidas de um endereço IP, controlando com base em: volume de vírus, de spam e de remetentes inválidos;	Motivo: Não é possível limitar o fluxo de mensagens, com base em IP, volume de vírus, spam e de remetentes inválidos, pela solução Symantec Ofertada. A alegação pode ser facilmente comprovada observando a interface da ferramenta.	A solução Symantec preenche o referido requisito, conforme consta na Planilha Ponto a Ponto enviada na Fase de Habilitação e reforçada nas paginas do Admin Guide número 107.	As informações a seguir foram obtidas do documento "Smg_10.6_Administration Guide ". Na **pag. 107** foi verificado que é possível bloquear emails enviados para destinatários inválidos " *You can configure Symantec Messaging Gateway to accept, reject, or drop any messages* ***that are sent to invalid recipients*** *..."* . Na **Pág. 157** verificou-se a possibildade de bloqueio de emails em ataques de DHA - *"A directory harvest attack works by sending a large quantity of possible email addresses to a site. To enable or disable directory harvest attack recognition 1. In the Control Center, click Reputation > Policies > Bad Senders . 2. To enable or disable directory harvest attack recognition on this page, check Directory Harvest Attack and click Enable or Disable. Or, continue with the next step. 3 Click Directory Harvest Attack".* Na **pag. 155** foi verificado também que é possível barrar ataques de vírus conforme o volume de vírus na mensagem *"Configuring email virus attack recognition - In an email virus attack, a specified* ***quantity of infected email messages has been received from a particular IP address"*** indicando ainda na **Pág. 156** como especificar o volume mínimo de virus que a mensagem deverá conter para execução de determinada ação em *"email virus recognition - To configure email virus attack recognition: 1 In the Control Center, click Reputation > Policies > Bad Senders. 2 Click Email Virus Attacks. 3 Accept the defaults or modify the values under Email Virus Attack Configuration:* ***Minimum number of virus messages - Number of virus messages from a single server that must be exceeded to trigger the specified action.*** *Por fim,* na **pág. 160** foi verificado que por meio da "*Global Bad Sender List* da Symantec" é possível bloquear remetentes por meio do uso dessa lista que já tenham encaminhado um grande volume de spams - *"Symantec Global Bad Senders consists of IP addresses that have sent large amounts of spam to mail servers protected by Symantec"*	Item atendido
7.1.1.4.2.4.7. - Ser capaz de controlar o número máximo de destinatários de um determinado emissor, por endereço IP, domínio, nome reverso, saudação de SMTP ou país;	Motivo: Não é possível controlar o número máximo de destinatários de um determinado emissor por endereço IP, domínio, nome reverso, saudação de SMTP ou país. A alegação pode ser facilmente comprovada observando a interface da ferramenta.	https://support.symantec.com/en_US/article.HOWTO126458.html	A figura inserida nas contrarrazões da licitante demonstrou que é possível limitar o número máximo de destinatários por mensagem. Tal ponto também foi confirmado na **pág. 73** do documento "*smg_10.6_Administration Guide* " no trecho "*Maximum number of recipients per message* ". Complementarmente foi verificado nas **págs. 387 e 388 , table 14-9 ,** que é possível configurar em "*content filtering policies* " condições de verificação de partes da mensagem, tais como: endereço de email do *sender* , envelope HELO, *domain names* e *countrycodes* que poderão resultar em ações de bloqueio de mensagem.	Item atendido
7.1.1.4.2.5.1. Suportar a criação de áreas de quarentena personalizadas para grupos de usuários, bem como para usuários específicos;	Não é possível criar áreas de quarentena personalizadas para grupos de usuários ou usuários específicos. A alegação pode ser facilmente comprovada observando a interface da ferramenta.	https://support.symantec.com/en_US/article.HOWTO93102.html	A figura inserida nas contrarrazões da licitante demonstrou inicialmente que é possível permitir que membros de uma "*policy group* " tenham acesso à quarentena de usuário. Complementarmente, foi verificado na **pág. 201** da documentação "*smg_10.6_Administration Guide* " que uma determinada *"policy group* " pode conter membros baseados em endereços de email, domínio, ou grupo LDAP (este último inlcusive pode até mesmo conter apenas um usuário) - "*Adding members to a policy group: You can assign members to a policy group based on email addresses, domain names, or LDAP groups for the purpose of applying policies. Once you have created your policy group and added members you can select the policies that you want your group to have.* " Isto posto, na **pág. 943, Table B-1** verificou-se ainda que é possível configurar *"filtering policies actions"* pertencentes as eventuais *"content filtering policies"* que , por sua vez estão definidas para determinados "*policies groups* " com as características já descritas acima e que pode ser configuradas com a ação de armazenamento da mensagem em uma determinada área de quarentena especificada pelo administrador denominada de "*quarantine incidents folders" ou "content incident folders"* conforme indicado na **pág. 407 -** "*Create an informational incident - The violation incident is created in the* ***Informational Incidents folder that you specify*** " e " *Create a quarantine incident - The violation incident is created in the* ***Quarantine Incidents folder that you specify*** ".	Item atendido