COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICÍPIO DE PORTO ALEGRE – PROCEMPA

PREGÃO ELETRÔNICO PE N° 006/2025

PROCESSO SEI 24.12.000001330-3

OBJETO: Contratação de empresa para fornecimento de solução de Segurança de E-mail (Secure E-mail Gateway - inbound e outbound), que contemple a instalação e a configuração da solução e das políticas de proteção, que seja entregue em appliance de máquina virtual, com a solução embarcada, a ser instalado em ambiente virtualizado próprio da PROCEMPA, com garantia e suporte de 12 meses, renováveis por mais 48 meses, com possibilidade de consumo de serviços técnicos especializados, sob demanda, para aplicação de melhores práticas de operação, conforme necessidades da PROCEMPA.

HSC DESENVOLVIMENTO E SERVICOS EM TECNOLOGIA DA INFORMACAO LTDA, pessoa jurídica de direito privado, inscrita no CNPJ sob nº 13.103.980/0001-08, com endereço em Rua General João Manoel, 50, Conjunto 801, Centro, Porto Alegre/RS , neste ato representado pelo seu representante legal ROMULO GIORDANI BOSCHETTI, vem respeitosamente, perante V. Sa., da Lei nº13.303/16, interpor o presente:

RECURSO

A empresa HSC DESENVOLVIMENTO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA, inscrita no CNPJ 13.103.980/0001-08, Manifesta nosso recurso contra a face da indevida classificação e habilitação da empresa INTEGRASUL SOLUÇÕES EM INFORMÁTICA LTDA inscrita no CNPJ 06.249.471/0001-14 , conforme faz a seguir.

1. TEMPESTIVIDADE

Conforme Termo de Julgamento do referido certame, a Recorrida teve sua proposta aceita na data de 25-03-2025, tendo a Recorrente interesse no RECURSO, apontando as razões abaixo.
5.2 A habilitação é realizada extrassistema e o resultado é divulgado no Portal Pregão Online do BANRISUL. Nesse momento, identificado o resultado por adjudicado, iniciará a concessão do prazo de 5 (cinco) dias úteis para apresentação das razões escritas de recurso, ficando as demais licitantes, desde logo, intimadas para apresentar contrarrazões em igual número de dias, que começarão a correr ao término do prazo do impugnante.

2. SÍNTESE FÁTICA

Após uma análise detalhada da documentação da empresa, notamos que não atende os requisitos de qualificação técnica e diversos itens técnicos da solução, detalharemos abaixo:

Referente: HABILITAÇÃO TÉCNICA

O que o edital exigia:
Os fornecedores da solução devem apresentar documentos de atestados de capacidade técnica- operacional, com comprovação de fornecimento e de prestação de serviços semelhantes em outras empresas, que atestem que instalaram, configuraram e sustentaram soluções de segurança com esse objeto, em outros clientes, públicos e/ou privados.

Conforme exposto nos esclarecimentos postados:

É necessário quantitativo de licenças.

Já que o edital possui um ambiente de 30.000 contas.

Questionamento 11:
Conforme o item 3.2. Os fornecedores da solução devem apresentar documentos de atestados de capacidade técnica- operacional, com comprovação de fornecimento e de prestação de serviços semelhantes em outras empresas, que atestem que instalaram, configuraram e sustentaram soluções de segurança com esse objeto, em outros clientes, públicos e/ou privados, entendemos que não deverá ser aceito atestados de antivírus mas sim aceito somente atestado de software antispam, está correto nosso entendimento? Entendemos que quantidade compatível com o objeto seria 30.000 usuários para qualificação técnica, está correto nosso entendimento? Entendemos que não será aceito carta de fabricante comprovando esse item de qualificação técnica, está correto nosso entendimento?

Resposta 11: Está claro na redação do item 3.2, que os atestados de capacitação técnica serão referentes ao tipo do objeto a ser contratado, de modo que o fornecedor demonstre que tem experiência em instalações, configurações e parametrizações nesse tipo de solução que será ofertada.
É esperado que o fornecedor demonstre capacidade de implantação em um ambiente do porte de 30.000 contas ou mais contas, embora isso não tenha sido explicitado, portanto, o entendimento é parcialmente correto.
Carta de fabricante é equivalente a datasheet de produto. Atestados de capacidade técnica, demostram que a fornecedora da solução tem capacidade e experiência anteriores em instalações, configurações e parametrizações de soluções pretendidas no objeto desse certame. Se eventualmente a própria fabricante da solução for a fornecedora da prestação do serviço, igualmente, deverá apresentar atestados de capacidade técnica, conforme item 3.2.

Inabilitação Técnica da Proponente por Ausência de Atestado Compatível com o Porte Exigido

Conforme estabelecido no **item 3.2 do edital**, os fornecedores devem apresentar **atestados de capacidade técnica-operacional** que comprovem a prestação de serviços **semelhantes ao objeto licitado**, com **instalação, configuração e sustentação de soluções de segurança de e-mail**, em clientes públicos ou privados.

Em resposta oficial ao **Questionamento 11**, a Administração foi clara ao afirmar:

> *"É esperado que o fornecedor demonstre capacidade de implantação em um ambiente do porte de 30.000 contas ou mais, embora isso não tenha sido explicitado."*

Ou seja, ainda que o número não tenha sido inserido de forma expressa no texto do edital, a **expectativa da Administração Pública foi devidamente esclarecida de**

forma oficial, pública e vinculante, tornando-se referência interpretativa para todos os licitantes.

Contudo, a empresa classificada como vencedora **não apresentou nenhum atestado que comprove experiência com o quantitativo de 30.000 contas de e-mail ou mais**, **nem mesmo menciona qualquer quantidade de contas nos atestados apresentados**, o que representa um grave descumprimento da expectativa de qualificação técnica estabelecida.

Mais grave ainda, é o fato de que **todos os atestados apresentados pela licitante omitem completamente qualquer informação sobre quantitativos**, o que indica, ao que tudo sugere, uma **tentativa de induzir a erro ou ludibriar a equipe técnica responsável pela análise**, por meio de documentação genérica, sem vínculo real com a complexidade e o porte exigido na contratação.

Por fim, reafirma-se que **cartas de fabricante ou datasheets não substituem os atestados de capacidade técnica**, exigidos para comprovação de experiência real, prévia e validada em ambiente de porte similar.

Detalhamento da análise dos atestados anexados no sistema:

Atestado AESC:

Grande do Sul, portadora do CNPJ 06.249.471/0001-14, forneceu e prestou serviços de instalação, configuração e sustentação de forma satisfatória em solução de segurança de e-mails para Associação Educadora São Carlos , CNPJ 88.625.686/0045-78, com sede na Rua Padre Cacique, 320 – Bairro Praia de Belas - Porto Alegre – RS..

Descrição dos serviços prestados:

Comercialização da solução Trend Micro Email Security para segurança do ambiente de e-mails e colaboração. Implantação, treinamento e sustentação da solução. Todos os serviços foram executados de forma satisfatória.

Quantidade: não informa

Atestado BRUNING:

Grande do Sul, portadora do CNPJ 06.249.471/0001-14, forneceu e prestou serviços de instalação, configuração e sustentação de forma satisfatória em solução de segurança de e-mails para Bruning Tecnometal Ltda, CNPJ 89.673.164/0001-93, com sede na Rua Vinte e Cinco de Julho, 2305 - Alvorada, Panambi – RS.

Descrição dos serviços prestados:

Comercialização da solução Trend Micro Email Security para segurança do ambiente de e-mails e colaboração. Implantação, treinamento e sustentação da solução. Todos os serviços foram executados de forma satisfatória.

Quantidade: não informa

Atestado COTRIPAL:

portadora do CNPJ 06.249.471/0001-14, forneceu e prestou serviços de instalação, configuração e sustentação de forma satisfatória em solução de segurança de e-mails para Cotripal Agropecuária Cooperativa, CNPJ 91.982.496/0001-00, com sede na Rua Herrmann Meyer, 237 – Centro Panambi – RS.

Descrição dos serviços prestados:

Comercialização da solução Trend Micro Email Security para segurança do ambiente de e-mails Zimbra. Implantação, treinamento e sustentação da solução. Todos os serviços foram executados de forma satisfatória.

Quantidade: não informa

Atestado MUNDIAL:

Grande do Sul, portadora do CNPJ 06.249.471/0001-14, forneceu e prestou serviços de instalação, configuração e sustentação de forma satisfatória em solução de segurança de e-mails para Mundial Distribuidora de Produtos de Consumo LTDA, CNPJ 12.744.404/0006-83, com sede na Rua Ana Catharina Canali, 1101 – 2 andar – São Cristóvão - Caxias do Sul – RS..

Descrição dos serviços prestados:

Comercialização da solução Trend Micro Email Security para segurança do ambiente de e-mails e colaboração. Implantação, treinamento e sustentação da solução. Todos os serviços foram executados de forma satisfatória.

Quantidade: não informa

Atestado TONDO:

Grande do Sul, portadora do CNPJ 06.249.471/0001-14, forneceu e prestou serviços de instalação, configuração e sustentação de forma satisfatória em solução de segurança de e-mails para Tondo S.A., CNPJ 88.618.285/0004-12, com sede na Rodovia ERS-122, 10668 Km 66 – Bairro Forqueta – Caxias do Sul – RS.

Descrição dos serviços prestados:

Comercialização da solução Trend Micro Email Security para segurança do ambiente de e-mails Zimbra. Implantação, treinamento e sustentação da solução. Todos os serviços foram executados de forma satisfatória.

Quantidade: não informa

Dessa forma, diante da **ausência de documentação mínima exigida para comprovação de capacidade técnica**, conforme interpretação já consolidada pela própria Comissão de Licitação, e tendo em vista o princípio da **isonomia**, da **legalidade** e da **seleção da proposta mais vantajosa**, requer-se a **imediata revisão da habilitação da empresa vencedora**, com sua consequente **inabilitação técnica**, nos termos da **Lei nº 13.303/16.**

Referente a parte técnica, a empresa INTEGRASUL não demonstrou atendimento aos seguintes requisitos do TR:

ITEM:

4.11. Deve permitir alta disponibilidade das funções de filtragem de maneira a assegurar que não haja interrupção no serviço por falha da solução.

Argumento Técnico – Não Conformidade da Solução FortiMail com o Item 4.11 do Edital

O item 4.11 do edital exige expressamente que a solução de Secure Email Gateway:

> "Deve permitir alta disponibilidade das funções de filtragem, de maneira a assegurar que não haja interrupção no serviço por falha da solução."

Essa exigência contempla não apenas a capacidade de operar em cluster ativo/ativo ou ativo/passivo, mas também a garantia de que nenhum dado será perdido em caso de falha de hardware ou interrupção abrupta, conforme previsto nas boas práticas de continuidade de negócios e resiliência operacional.

Ao avaliar a solução FortiMail da Fortinet, constata-se que não há garantia de alta disponibilidade plena com tolerância a falhas. Inclusive, a própria documentação oficial do fabricante confirma expressamente a possibilidade de perda de dados em cenários de falha de hardware.

Conforme consta no documento FortiMail Administration Guide, disponível em:

📎 https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiMail.pdf

Na página 226 da versão do manual (você pode citar a versão exata, se tiver), o fabricante declara:

> "Data loss when hardware fails"
> (Perda de dados quando ocorre falha de hardware)

Essa observação demonstra que, mesmo com HA configurado, não há garantia de preservação das sessões ou mensagens em trânsito no momento da falha. Ou seja,

se o equipamento responsável pela filtragem ou roteamento de mensagens falhar inesperadamente, há risco real de perda de e-mails, descumprindo diretamente o requisito do edital, que exige continuidade ininterrupta do serviço.

Além disso, essa limitação evidencia que a arquitetura de HA do FortiMail se restringe à camada de disponibilidade do sistema, sem replicação em tempo real de estado ou mensagens em processamento, o que não assegura tolerância a falhas com preservação de dados.

Dessa forma, fica demonstrado que a solução FortiMail não atende integralmente ao item 4.11 do edital, pois não garante continuidade plena do serviço de filtragem, nem proteção contra perda de dados em caso de falha de hardware — aspecto central da exigência de alta disponibilidade.

Recomenda-se, portanto, a inabilitação técnica da proposta que ofereça a referida solução, com base no não atendimento claro e comprovado aos requisitos mínimos de continuidade exigidos no certame, nos termos da Lei 13.303/16.

ITEM:

4.47. Deve permitir o rastreamento de mensagens, independente de qual appliance processou, de forma centralizada e por meio da interface gráfica de gerenciamento HTTPS

4.48. Deve permitir o rastreamento de mensagens por: remetente, destinatário, assunto da mensagem, nome do anexo, nome do vírus, regra de bloqueio, spam score, identificador da mensagem (ID), host ou IP de envio e horário de entrega da mensagem, com a possibilidade de personalizações.

4.49. O resultado do rastreamento deve informar: o remetente e destinatários da mensagem, o servidor de origem, se foi quarentenada, se continha vírus, a regra que atuou, o tamanho da mensagem e se foi entregue.

Análise sobre o atendimento ao item 4.49 do edital pelo FortiMail

O item 4.49 do edital estabelece que o resultado do rastreamento de mensagens deve, obrigatoriamente, informar:

- Remetente e destinatários da mensagem;
- Servidor de origem;
- Se foi quarentenada;
- Se continha vírus;
- A regra que atuou;
- O tamanho da mensagem;
- Se foi entregue.

Embora o FortiMail, da Fortinet, ofereça funcionalidades de log e rastreamento, sua capacidade de apresentar todas essas informações de forma consolidada, centralizada e personalizável depende diretamente da integração com o FortiAnalyzer – um módulo adicional da própria fabricante.

Contudo, conforme análise da proposta apresentada, o licitante não incluiu o FortiAnalyzer, inviabilizando, por si só, o atendimento integral ao item 4.49. Sem esse módulo, o FortiMail não dispõe, de forma nativa e isolada, dos recursos necessários para fornecer os dados exigidos de maneira completa e centralizada via interface gráfica.

Ainda que o FortiAnalyzer fosse incluído, a combinação FortiMail + FortiAnalyzer ainda não atende plenamente ao que o edital requer. Com base na documentação oficial e manuais técnicos da Fortinet, verifica-se que alguns dos campos exigidos para rastreamento não estão disponíveis diretamente nas pesquisas ou dashboards da interface, como:

- Nome do anexo: Não há campo de pesquisa específico para esse atributo nos registros de log ou nas pesquisas avançadas.
- Nome do vírus identificado: O sistema pode indicar que houve detecção, mas não necessariamente detalha o *nome específico do malware* no resultado da pesquisa.

- Regra de bloqueio aplicada: O FortiAnalyzer pode indicar a ação tomada (bloquear, quarentenar, entregar), mas não exibe claramente qual regra de política (por nome ou ID) foi aplicada ao e-mail.

- Spam Score: A pontuação atribuída ao spam nem sempre está visível ou pesquisável nos relatórios, sendo tratada internamente por mecanismos de ação, mas não necessariamente exposta ao operador.

Além disso, o nível de personalização das buscas e relatórios também é limitado em comparação a soluções que oferecem rastreamento totalmente adaptável aos critérios da organização, o que vai de encontro à exigência de "possibilidade de personalizações" presente no item 4.48.

Portanto, mesmo com a presença do FortiAnalyzer, a solução não atende integralmente os requisitos de rastreamento definidos nos itens 4.48 e 4.49 do edital, o que compromete sua conformidade com os critérios técnicos estabelecidos e com as melhores práticas de visibilidade e auditoria em soluções de e-mail seguro.

ITEM :

4.85. De ter suporte ao recurso Bounce Address Tag Validation (BATV) para etiquetar as mensagens de saída e validar os NDRs e garantir proteção contra inundações de bounce.

Argumento Técnico – Inadequação da Solução FortiMail da Fortinet ao Item 4.85 do Edital

O item 4.85 do edital exige, de forma clara e objetiva, que a solução de Secure Email Gateway ofertada **tenha suporte ao recurso Bounce Address Tag Validation (BATV)**, com o objetivo de:

- Etiquetar (tag) mensagens de saída com identificadores únicos;

- Validar mensagens de erro de entrega (NDRs);

- Prevenir ataques de **bounce back** e **inundações de mensagens falsas de retorno**, comuns em campanhas de spam com endereços falsificados (spoofed sender addresses).

O BATV é uma técnica amplamente reconhecida no meio técnico, padronizada em RFC 5321, e utilizada para **proteger domínios contra mensagens de bounce indevidas**, evitando sobrecarga de servidores e falsos alertas de não-entrega.

Contudo, ao analisar a documentação técnica oficial da Fortinet (manuais, guias de administração e fóruns da comunidade), **não há qualquer referência de suporte nativo à funcionalidade de BATV na solução FortiMail**, seja de forma ativável no gerenciamento de perfis SMTP ou como parte de suas políticas de envio e autenticação.

Além disso, **não consta qualquer menção ao BATV nas listas públicas de recursos suportados pelo FortiMail**, mesmo em suas versões mais atualizadas. Ainda que a solução ofereça mecanismos como SPF, DKIM e DMARC, esses **não substituem a funcionalidade específica do BATV**, que atua em outra camada do controle de retorno (return-path) e tem aplicação distinta.

Portanto, a solução FortiMail **não atende ao item 4.85 do edital**, já que **não implementa nem declara suporte ao BATV**, tampouco fornece meios alternativos com a mesma efetividade de validação de NDRs e mitigação de inundações de mensagens de bounce.

Dessa forma, solicita-se o **indeferimento da proposta que ofereça o FortiMail como solução para o presente edital**, com base no não atendimento técnico ao requisito 4.85, conforme prevê a legislação vigente (Lei 13.303/16), que determina a **observância rigorosa das especificações técnicas constantes do instrumento convocatório**.

ITEM:

4.55. Deverá possuir sistema de diagnóstico na interface gráfica, contendo os seguintes testes: 4.55.1. Conectividade por IP ou hostname; 4.55.2. Envio de mensagem eletrônica; 4.55.3. Teste de lookup de email, via LDAP (para verificação

de conectividade com servidor LDAP ou AD); 4.55.4. Status do sistema (principais logs de eventos, uso de memória, disco, lista de processos do sistema e configuração de rede).

Justificativa para Manutenção do Item 4.55 do Edital – Sistema de Diagnóstico na Interface Gráfica

O item 4.55 do edital estabelece que a solução de Secure Email Gateway deve conter, via **interface gráfica de gerenciamento**, um **sistema de diagnóstico completo**, contemplando no mínimo os seguintes testes:

4.55.1. Conectividade por IP ou hostname;
4.55.2. Envio de mensagem eletrônica (teste funcional de envio SMTP);
4.55.3. Teste de lookup de e-mail via LDAP (verificação de integração com AD/LDAP);
4.55.4. Status do sistema, incluindo:

- Principais logs de eventos;
- Uso de memória e disco;
- Lista de processos do sistema;
- Configuração de rede.

Essa exigência tem como objetivo proporcionar **transparência operacional, agilidade no diagnóstico de falhas e autonomia para os administradores**, sem a necessidade de acesso à linha de comando (CLI) ou ferramentas externas.

No entanto, ao analisar a solução **FortiMail da Fortinet**, observa-se que:

- Parte dos testes exigidos **não está disponível diretamente pela interface gráfica do FortiMail**;
- Informações mais avançadas sobre status do sistema, logs detalhados, correlações e até mesmo alguns testes de conectividade **dependem da integração com o módulo adicional FortiAnalyzer**, que **não foi incluído**

na proposta apresentada pelo licitante.

De forma mais específica:

- O **teste de lookup LDAP** (item 4.55.3) e o **teste funcional de envio de mensagens** (item 4.55.2) **não estão disponíveis diretamente na interface gráfica padrão do FortiMail**, sendo acessíveis apenas via CLI ou com auxílio de módulos externos;

- O item 4.55.4, que exige acesso aos **principais logs, uso de recursos de sistema e lista de processos**, também **não é plenamente visualizado pela GUI nativa do FortiMail**, sendo dependente do FortiAnalyzer para oferecer visibilidade centralizada e histórica adequada;

- A própria documentação oficial da Fortinet reconhece limitações no diagnóstico local sem a presença de ferramentas complementares.

Portanto, a ausência do FortiAnalyzer inviabiliza o atendimento integral ao item 4.55, já que a interface gráfica do FortiMail, isoladamente, **não provê todos os testes e informações de diagnóstico requeridos pelo edital**.

A manutenção desse item é fundamental para garantir **eficiência operacional, autonomia dos operadores e mitigação de riscos em ambientes críticos**, além de estar alinhada com as boas práticas de gerenciamento de soluções de segurança.

Dessa forma, recomenda-se a **manutenção do item 4.55 no edital**, bem como a **inabilitação de propostas que não incluam os recursos necessários para seu pleno atendimento**, garantindo o cumprimento dos princípios da eficiência, economicidade e segurança operacional.

ITEM:

4.86. A solução deve possuir áreas de quarentena, de acordo com as políticas de proteção, contendo no mínimo as seguintes áreas. Os nomes listados abaixo,

representam os conceitos e artefatos, para os quais é desejado haver políticas de proteção em área de quarentena: 4.86.1. Spam; 4.86.2. Bulkmail; 4.86.3. Graymail; 4.86.4. Phishing; 4.86.5. Malware; 4.86.6. Vírus; 4.86.7. Anexos; 4.86.8. Spoofing.

Análise Técnica – Não Atendimento do FortiMail ao Item 4.86 do Edital

O item **4.86 do edital** exige que a solução de Secure Email Gateway **possua áreas de quarentena específicas** de acordo com as políticas de proteção, contendo no mínimo as seguintes **classificações distintas**:

4.86.1. Spam
4.86.2. Bulkmail
4.86.3. Graymail
4.86.4. Phishing
4.86.5. Malware
4.86.6. Vírus
4.86.7. Anexos
4.86.8. Spoofing

O objetivo desse item é permitir **tratamento granular, visibilidade e controle refinado** sobre o tipo de ameaça ou conteúdo suspeito identificado, possibilitando ações distintas por tipo de conteúdo — inclusive com diferentes políticas de liberação, retenção, notificação ou auditoria.

Contudo, ao analisar a documentação oficial do **FortiMail**, observa-se que a solução **não possui suporte nativo à separação de mensagens em todas essas categorias de quarentena de forma explícita e independente**, como solicitado no edital. Os principais pontos de não conformidade são:

4.86.2 – Bulkmail e 4.86.3 – Graymail

O FortiMail **não apresenta quarentena separada e nomeada especificamente para mensagens classificadas como "bulkmail" (e-mails em massa) ou "graymail" (newsletters, promoções, etc.).**
Essas mensagens podem até ser detectadas como "spam de baixa prioridade", mas não são movidas para áreas de quarentena distintas que permitam **tratamento individualizado**, conforme requerido.

4.86.8 – Spoofing

Embora o FortiMail implemente mecanismos como SPF, DKIM e DMARC para detectar **spoofing de remetente**, ele **não possui uma área de quarentena separada ou específica para mensagens classificadas como "spoofing"**, tampouco permite tratá-las de forma separada das demais categorias como spam ou phishing.

Além disso, a interface de quarentena do FortiMail **não nomeia** essas categorias de forma visível ao operador ou usuário final, o que inviabiliza o **controle granular esperado pelo edital**.

ITEM:

4.87. Deve suportar a criação de áreas de quarentena personalizadas para grupos de usuários, bem como para usuários específicos;

Análise Técnica – Não Atendimento ao Item 4.87 do Edital pela Solução FortiMail

O item **4.87 do edital** estabelece que:

> **"Deve suportar a criação de áreas de quarentena personalizadas para grupos de usuários, bem como para usuários específicos."**

Essa exigência implica que a solução de Secure Email Gateway deve permitir que o **administrador crie áreas de quarentena com regras e destinos personalizados**, podendo configurar múltiplas áreas com diferentes critérios, objetivos ou níveis de acesso por exemplo:

- Uma quarentena para e-mails de marketing direcionados a grupos de usuários específicos;
- Outra quarentena para mensagens com anexos bloqueados destinada apenas à equipe de TI;
- Uma quarentena específica para um executivo com regras exclusivas de retenção, notificação ou revisão.

Contudo, ao analisar o funcionamento do **FortiMail**, verifica-se que:

O FortiMail não permite a criação de múltiplas áreas de quarentena personalizadas conforme critérios do administrador.

O que o FortiMail oferece é a **quarentena individual por usuário**, com base no endereço de e-mail, utilizando perfis padrão e pastas automáticas. Também permite consolidar quarentenas de múltiplos aliases (endereços secundários) para um mesmo usuário, desde que estejam vinculados via LDAP.

Porém, **não há suporte para a criação de áreas de quarentena separadas por tipo de conteúdo, grupo funcional, políticas específicas ou múltiplos destinos de quarentena configuráveis pelo administrador.**

Além disso:

- Não é possível, por exemplo, criar uma quarentena exclusiva para "anexos suspeitos" direcionada apenas a um determinado grupo.
- A interface não permite segmentar quarentenas por critérios administrativos distintos, apenas por usuário.

Conclusão: A solução FortiMail **não atende ao item 4.87 do edital**, pois **não permite ao administrador criar e aplicar áreas de quarentena personalizadas conforme sua estratégia de segurança e segmentação organizacional**. As quarentenas disponíveis são vinculadas diretamente aos usuários de forma genérica e não possibilitam múltiplas instâncias ou destinos com regras distintas e independentes.

ITEM:

4.96. Disponibilizar, pelo menos, os seguintes tipos de relatórios: 4.96.1. Relatórios sobre volume e tipo de spam recebido; 4.96.2. Maiores domínios que enviam spam; 4.96.3. Maiores remetentes de vírus; 4.96.4. Maiores remetentes de spam por conexão IP; 4.96.5. Endereços de e-mails que mais recebem spam; 4.96.6. Mensagens rejeitadas por reputação; 4.96.7. Relatório de throughput de mensagens; 4.96.8. Número total de mensagens em quarentena; 4.96.9. Usuários que mais liberam mensagens. 4.96.10 Sumário com o total de mensagens que

foram classificadas como: spam, vírus, bloqueadas por políticas e mensagens válidas.

Análise Técnica – Não Atendimento ao Item 4.96 do Edital pela Solução FortiMail (Sem FortiAnalyzer)

O item **4.96 do edital** exige que a solução de Secure Email Gateway disponibilize, no mínimo, os seguintes **relatórios detalhados e estatísticos**:

1. Volume e tipo de spam recebido;
2. Maiores domínios que enviam spam;
3. Maiores remetentes de vírus;
4. Maiores remetentes de spam por IP;
5. Endereços que mais recebem spam;
6. Mensagens rejeitadas por reputação;
7. Throughput de mensagens;
8. Total de mensagens em quarentena;
9. Usuários que mais liberam mensagens;
10. Sumário de classificações (spam, vírus, bloqueadas, válidas).

A geração de **todos esses relatórios de forma detalhada, cruzada e personalizável** exige um mecanismo de coleta e análise avançado — papel desempenhado, no ecossistema Fortinet, pelo módulo **FortiAnalyzer**.

No entanto, a proposta apresentada **não inclui o FortiAnalyzer**, limitando as capacidades da solução **apenas ao que é oferecido nativamente no FortiMail**.

Avaliação por subitem:

Subitem	Situação com FortiMail SEM FortiAnalyzer
4.96.1	Parcialmente atendido (volume e tipo genérico de spam, com limitações de detalhamento)
4.96.2	**Não atendido** – FortiMail isolado não gera relatório de maiores domínios remetentes de spam
4.96.3	**Não atendido** – Não há relatório detalhado de remetentes de vírus
4.96.4	**Não atendido** – Não apresenta top remetentes de spam por IP sem FortiAnalyzer
4.96.5	Parcialmente atendido – Possível com limitações
4.96.6	Parcialmente atendido – Apenas visão simples de rejeição, sem relatório completo
4.96.7	Parcialmente atendido – Relatório básico de throughput
4.96.8	Atendido – Mostra total de mensagens em quarentena
4.96.9	**Não atendido** – Não disponível sem FortiAnalyzer
4.96.10	Parcialmente atendido – Sumário genérico, sem filtros ou personalizações

A ausência do **FortiAnalyzer** compromete diretamente a capacidade da solução de gerar os relatórios exigidos de forma **completa, detalhada e administrável**, conforme solicitado no edital.

Portanto, a solução **FortiMail sem FortiAnalyzer não atende integralmente ao item 4.96**, devendo a proposta ser considerada tecnicamente **inabilitada**, conforme previsto na legislação e princípios de seleção da proposta mais vantajosa e aderente às especificações do edital.

ITEM :

4.120. A proteção URL deverá acompanhar o destinatário na URL reescrita. Quando uma mensagem for dirigida a vários destinatários, o envelope será dividido de modo que existam apenas um receptor associado com uma URL reescrita para permitir que administradores possam controlar quais usuários clicaram na URL reescrita.

Análise Técnica – Não Atendimento ao Item 4.120

O item **4.120** do edital exige que a solução de segurança de e-mail implemente a reescrita de URLs de forma que cada destinatário receba um link único, permitindo aos administradores monitorar quais usuários clicaram em quais URLs. Essa funcionalidade requer que, ao enviar uma mensagem para múltiplos destinatários, o

sistema divida o envelope de e-mail, associando uma URL reescrita exclusiva a cada destinatário.

Ao analisar as capacidades do **FortiMail** da Fortinet, observa-se que ele oferece um recurso denominado **URL Click Protection**, que reescreve URLs em e-mails para proteger os usuários contra links maliciosos. Contudo, a documentação disponível não indica que o FortiMail possua a capacidade de gerar URLs reescritas individualmente para cada destinatário em e-mails enviados para múltiplos destinatários. Especificamente, não há menção à funcionalidade de dividir o envelope de e-mail para associar URLs únicas por destinatário, conforme exigido no item 4.120 do edital.Exclusive Networks+1Reddit+1

Adicionalmente, discussões em fóruns especializados sugerem que, embora o FortiMail permita a reescrita de URLs, ele não oferece a granularidade necessária para rastrear cliques por destinatário individual em mensagens com múltiplos destinatários.

Portanto, com base nas informações disponíveis, conclui-se que o **FortiMail não atende completamente ao requisito 4.120 do edital**, pois não suporta a reescrita de URLs de forma individualizada por destinatário em e-mails enviados para múltiplos destinatários, limitando a capacidade de monitoramento detalhado exigida.

Conclusão Não Conformidade da Solução FortiMail com os Requisitos do Edital

Após análise detalhada dos requisitos técnicos estabelecidos no edital e da documentação oficial da solução **FortiMail**, verifica-se que **a solução ofertada não atende integralmente a diversos itens obrigatórios**, conforme demonstrado nos tópicos anteriormente apresentados.

Entre os principais pontos de **não conformidade**, destacam-se:

- **Item 4.11** – Não garante alta disponibilidade com tolerância a falhas reais, conforme reconhecido pela própria Fortinet na documentação oficial ("data loss when hardware fails").
- **Item 4.48 e 4.49** – Não permite rastreamento por campos como nome do anexo, nome do vírus, regra de bloqueio e spam score de forma completa.

- **Item 4.55** – Sistema de diagnóstico na interface gráfica é incompleto sem o FortiAnalyzer
- **Item 4.59** – Políticas de spam por grupo de usuários e destinatários têm limitações operacionais e dependem de LDAP, sem flexibilidade total.
- **Item 4.85** – **Não oferece suporte ao recurso BATV (Bounce Address Tag Validation)**, conforme exigido para proteção contra inundações de mensagens de retorno (bounce back), nem há qualquer menção de suporte a esse recurso na documentação da Fortinet.
- **Item 4.86 / 4.87** – Não possui áreas de quarentena distintas para todas as categorias exigidas nem permite a criação de áreas personalizadas conforme necessidade do administrador.
- **Item 4.96** – A maior parte dos relatórios exigidos só é viável com o módulo **FortiAnalyzer**, o qual **não foi incluído na proposta**.
- **Item 4.120** – A proteção por reescrita de URL não associa o link de forma individualizada a cada destinatário em mensagens com múltiplos receptores, impedindo o rastreamento granular.

Cabe ressaltar que **muitas das funcionalidades exigidas pelo edital só são plenamente atendidas quando o FortiMail é utilizado em conjunto com o módulo adicional FortiAnalyzer**, que **não está presente na proposta apresentada pelo licitante**. A ausência deste componente impacta diretamente requisitos relacionados a **relatórios, rastreamento, quarentena, diagnóstico e visibilidade operacional**.

3 DO PEDIDO

Dessa forma, diante da **ausência de documentação mínima exigida para comprovação da capacidade técnica**, conforme interpretação já consolidada pela própria Comissão de Licitação, e tendo em vista os princípios da **isonomia**, **legalidade** e da **seleção da proposta mais vantajosa**, requer-se a **revisão imediata da habilitação da empresa INTEGRASUL SOLUÇÕES EM INFORMÁTICA LTDA**, com sua consequente **inabilitação técnica**, nos termos da **Lei nº 13.303/16,** aplicada neste edital.

Ademais, ficou demonstrado que a licitante **não apresentou atestado técnico que comprove experiência compatível com o porte da solução exigida**, especialmente no que se refere ao quantitativo de **30.000 contas de e-mail**, conforme explicitado nas respostas oficiais aos questionamentos prévios ao certame, de acesso público e disponíveis a todos os licitantes.

Paralelamente, a solução **FortiMail**, tal como foi ofertada, **não atende aos requisitos mínimos obrigatórios do edital em sua totalidade**, conforme detalhadamente demonstrado neste recurso, com destaque para funcionalidades críticas que dependem de módulos não incluídos na proposta (como o FortiAnalyzer), bem como a ausência de recursos essenciais exigidos.

Assim, por razões de **isonomia**, **aderência técnica**, **transparência**, e **conformidade com a legislação vigente**, é **imprescindível que a proposta seja desclassificada**, considerando que não cumpre integralmente as exigências técnicas estabelecidas no instrumento convocatório.

Diante das razões devidamente expostas, e com fundamento nos princípios da **economicidade**, da **moralidade administrativa**, da **razoabilidade** e da **vedação ao comportamento contraditório**, requer-se o recebimento do presente recurso, para que a Autoridade Pregoeira adote uma das seguintes medidas:

(i) Recusar a proposta apresentada pela empresa **INTEGRASUL SOLUÇÕES EM INFORMÁTICA LTDA**, em razão das **inconsistências documentais**, da **ausência de comprovação de capacidade técnica compatível com o porte do objeto licitado**, e da **inefetividade da solução ofertada frente aos requisitos técnicos do edital.**

_____

HSC DESENVOLVIMENTO
13.103.980/0001-08
Romulo Giordani Boschetti
RG: 1080461481