

Estudo Técnico Preliminar 5/2023

1. Informações Básicas

Número do processo: 028/2023

2. Descrição da necessidade

Contratação de Solução de Filtragem de Conteúdo de E-mail na Nuvem (Antispam Corporativo), para proteção de caixas postais, contemplando serviços de instalação, manutenção, atualização e suporte técnico especializado da plataforma ofertada, conforme as condições e especificações constantes neste instrumento, observado o quadro abaixo:

Item	Descrição	Quantidade / Unidade de Medida
01	Solução de Filtragem de Conteúdo de E-mail na Nuvem (Antispam Corporativo), para proteção de 300 caixas postais, contemplando serviços de instalação, manutenção, atualização e suporte técnico especializado da plataforma ofertada.	12 meses

3. Área requisitante

Área Requisitante	Responsável
Centro de Informática	Luis Eduardo Pires Monte Maior

4. Descrição dos Requisitos da Contratação

A empresa deverá apresentar no mínimo 01 (um) Atestado de Capacidade Técnica fornecido por pessoa jurídica de direito público ou privado, declarando ter fornecido bens, compatível com o objeto deste Termo de Referência;

5. Levantamento de Mercado

Foi realizada pesquisa de preço junto ao mercado, conforme consta na planilha de estimativa de despesa, onde foram discriminados os valores unitários estimados deste serviço, e as fontes consultadas para estimativa de valores de referência.

6. Descrição da solução como um todo

1. ESPECIFICAÇÕES TÉCNICAS DOS MATERIAIS OU SERVIÇOS

1.1. DO MODELO

1.1.1. *O produto deve ser ofertado como serviço em nuvem, SaaS – Software as a Service*

1.2. DO CONSOLE DE GERENCIAMENTO

1.2.1. A solução deve possuir console e acesso em plataforma totalmente *WEB*

.

1.2.2. A CONTRATANTE deve possuir acesso de forma ilimitada a quarentena dos usuários, criação de filtros regras, geração de relatórios e acesso a gráficos de análise para tomada de decisões.

1.3. DA PLATAFORMA

1.3.1. A licença de uso deve suportar usuários de correio eletrônico de forma ilimitada;

1.3.2. Deve suportar usuários “alias” de forma ilimitada

1.3.3. Deve ser capaz de filtrar o tráfego de correio, bloqueando a entrada de vírus, SPAM e Malwares.

1.

1.1. FILTRO DE ENTRADA

1.1.1. Deve suportar a filtragem de no mínimo 100.000 (cem mil) mensagens mensais

1.1.2. Deve suportar tamanho de mensagens de no mínimo 400 mb.

1.2. FILTRO DE SAÍDA

1.2.1. Deve suportar a transmissão de no mínimo 15.000 (quinze mil mensagens mês)

1.3. DAS FUNÇÕES GERAIS

1.3.1. A CONTRATANTE terá direito de uso da versão mais atual do produto licenciado caso esta esteja disponível pelo fabricante, atualizações de recursos e melhorias dentro da mesma versão;

1.3.2. Garantia de software contra mau funcionamento e correção de Bugs e falhas;

1.3.3. Deve ser uma solução completa com registro de LOGS de todas as atividades realizadas dentro da plataforma.

1.3.4. Ter a capacidade de processar o tráfego de entrada de mensagens filtrando e protegendo contra ameaças e conteúdos indesejados;

1.3.5. Deve possuir ferramenta de auditoria de e-mail, com facilidade de pesquisa por origem, destino, assunto e conteúdo da mensagem.

1.4. DA ALTA DISPONIBILIDADE E SISTEMAS CONTRA FALHAS

Em caso de indisponibilidade do provedor de correio eletrônico a solução de Antispam deve reter as mensagens pelo período mínimo de 7 (sete) dias.

1.

1.1.

1.1.1. A solução deve ser replicada em diversos Data Centers para maior resiliência.

1.2. DA PROTEÇÃO CONTRA ATAQUES

1.2.1. A solução deve ser capaz de efetuar a filtragem do tráfego de correio eletrônico bloqueando a entrada de:

1.2.1.1. Vírus;

1.2.1.2. Malwares;

1.2.1.3. Spam;

1.2.2. A solução Deve realizar atualização automática das assinaturas de antivírus, antispam e outras assinaturas necessárias para o bom funcionamento da solução.

1.2.3. A solução deve permitir criação de listas negras e listas brancas.

1.3. DO MONITORAMENTO E LOGS

1.3.1. Possuir registro de log de TODAS as ações executadas na interface de administração para fins de auditoria. Esse log deve ser de fácil acesso e para obtenção dele.

1.3.2. A solução deve apresentar gráficos referente as cinco fontes de SPAM por país.

1.3.3. A solução deve apresentar gráficos referente as cinco fontes de e-mails limpos.

1.3.4. A solução deve ser capaz de apresentar diagnósticos dos serviços em execução.

1.3.5. Os logs da solução deverão apresentar no mínimo os seguintes dados:

1.3.5.1. ID do Email;

1.3.5.2. Assunto;

1.3.5.3. Data/Hora;

1.3.5.4. E-mail de destino;

1.3.5.5. E-mail de origem;

1.3.5.6. IP de Origem;

1.3.5.7. Status da mensagem.

1.3.6. O rastreamento deve ser a partir de uma única interface de gerenciamento, não sendo aceito pesquisa via linha de comando;

1.4. DAS INTEGRAÇÕES SISTÊMICAS

1.4.1. A solução deve disponibilizar painéis gráficos com estatísticas instantâneas.

1.4.2. A solução deve prover lista de e-mail validos

- 1.4.3. A solução deve prover lista de emissores de e-mail válidos
- 1.4.4. A solução deve prover lista de emissores de e-mail bloqueados
- 1.4.5. A solução deve possuir integração com Microsoft Active Directory
- 1.4.6. A solução deve possuir integração com LDAP Sync
- 1.4.7. A solução deve permitir a configuração de alias por domínio
- 1.4.8. A solução deve possuir característica de *CATCH-ALL*
- 1.4.9. A solução deverá prover comunicação criptografada entre a solução e o provedor de e-mail com encriptação TLS com característica (OE) *Opportunistic encryption*.
- 1.4.10. A solução deve suportar “etiquetas” nos e-mails para que os e-mails possam possuir alias ilimitados.

1.5. DA PROTEÇÃO CONTRA MALWARES

- 1.5.1. A solução deve permitir regras de bloqueio para o recebimento de arquivos compactados.
- 1.5.2. Deve suportar a criação de regras sem limites
- 1.5.3. Deve possuir o monitoramento de no mínimo 100.000.000 (cem milhões) de senders.
- 1.5.4. Deve possuir políticas de filtragem *Domain-wide*
- 1.5.5. Deve possuir políticas de filtragem *Custom-Domain*
- 1.5.6. Deve possuir a filtragem de vírus e malwares

1.6. DA PROTEÇÃO CONTRA SPAM E PHISHING

- 1.6.1. A solução deve possuir filtro de anti-spam para detecção de spams
- 1.6.2. A solução deve permitir a criação de regras de filtro de URL: Filtragem por URL contidas na no corpo da mensagem, dessa forma combatendo possível email Phishing;
- 1.6.3. A solução deve permitir a criação de filtros de URL de forma ilimitada, podendo restringir quaisquer assuntos de interesse da CONTRATANTE.

1.7. DOS RELATÓRIOS

- 1.7.1. Deve permitir a geração de relatórios da solução de forma centralizada através de uma única interface web no console de gerenciamento;
- 1.7.2. Permitir a seleção de dados para a formulação de relatórios por data ou por um intervalo de tempo específico;
- 1.7.3. Capacidade de criar relatórios globais e por domínio.
- 1.7.4. Deve permitir a exportação dos relatórios no formato CSV, PDF e/ou HTML;
- 1.7.5. Permitir filtros de relatórios com definição de origem (email de origem) e destinos (email de destino) específico;
- 1.7.6. Deve permitir filtragem das mensagens selecionado a quarentena indicada, por exemplo filtrar mensagens selecionando a quarentena PROVÁVEL SPAM.

1.7.7. Deve permitir a configuração de no mínimo período de 1 mês para a retenção de dados para a formulação de relatórios;

1.8. DA QUARENTENA

1.8.1. Permitir ao administrador da solução executar pesquisa nas áreas de quarentena de todos os usuários através de interface web.

1.8.2. A solução deve prover quarentena ilimitadas por usuário.

1.8.3. A solução deve prover quarentena por domínios compartilhados

1.8.4. A solução deve prover relatórios de quarentena por hora, diário ou semanais.

1.8.5. A solução deve prover a visualização e recuperação de e-mails em quarentena por no mínimo 30 (trinta) dias

1.8.6. A solução deve prover a possibilidade de reenvio de e-mails em quarentena por no mínimo 30 (trinta) dias.

1.8.7. A solução deve prover a possibilidade leitura de *logs*.

1.8.8. A solução deve prover o provisionamento de quarentena de forma automática.

1.9. DA QUALIFICAÇÃO TÉCNICA

1.9.1. A empresa deverá apresentar no mínimo 1(hum) Atestado de Capacidade Técnica fornecido por pessoa jurídica de direito público ou privado, declarando ter fornecido bens, compatível com o objeto deste Termo de Referência;

1.9.2. Não será aceito pela CONTRATANTE atestado ou declaração emitido pela própria CONTRATADA, sob pena de infringência ao princípio da moralidade, pois a CONTRATADA não possui a impessoalidade necessária para atestar sua própria capacitação técnica;

1.10. DA IMPLANTAÇÃO

1.10.1. Entende-se como fase em que se dará a instalação e configuração dos produtos, ou seja, efetiva implementação do projeto especificado;

1.10.2. A instalação e testes dos produtos devem estar inclusos no custo do produto;

1.10.3. A implementação deverá ser realizada de tal forma que as interrupções no ambiente de produção sejam as mínimas possíveis e estritamente necessárias, e, ainda, não causem transtornos aos usuários finais do órgão;

1.10.4. A **CONTRATADA** deverá executar uma série de testes funcionais básicos para verificar o perfeito funcionamento do ambiente.

1.10.5. Durante a execução dos serviços, pelo menos um representante do **CONTRATANTE** participará e fará composição na equipe designada para as atividades.

1.11. DA GARANTIA E SUPORTE TÉCNICO

1.11.1. O prazo de garantia das licenças da solução ofertada deverá ser de, no mínimo, 12 (doze) meses, contados a partir da data do aceite definitivo;

1.11.2. O suporte técnico deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes aos componentes que compõem a solução.

1.11.3. A CONTRATADA deverá disponibilizar uma ferramenta de abertura de chamado com os seguintes pré-requisitos:

1.11.3.1. Abertura de chamado por correio eletrônico.

1.11.3.2. Abertura de chamado por comunicador instantâneo que permita transformar a conversa em um chamado de forma automática.

1.11.3.3. Console com acesso via internet via navegador.

1.11.3.4. A ferramenta deverá apresentar uma pesquisa de satisfação ao término de cada atendimento. A CONTRATANTE poderá solicitar uma cópia do nível de atendimento a qualquer momento.

1.11.4. A CONTRATADA deverá fornecer os níveis de atendimento conforme abaixo indicado:

1.11.4.1. Os chamados de severidade ALTA (quando há indisponibilidade de uso da solução) deverão ter o início do atendimento em até 2 (duas) horas após a abertura da solicitação;

1.11.4.2. Os chamados de severidade MÉDIA (quando há falha, simultânea ou não, de uma ou mais funcionalidades que não cause indisponibilidade, mas apresente problemas de funcionamento e/ou performance da solução) deverão ter o início do atendimento em até 8 (oito) horas após a abertura da solicitação;

1.11.4.3. Os chamados de severidade BAIXA (para instalação, configuração, atualização de versões e implementações de novas funcionalidades) deverão ter o início do atendimento em até 12 (dois) horas após a abertura da solicitação;

1.11.4.4. Os chamados de severidade INFORMATIVO (informações ou dúvidas) deverão ter o início do atendimento em até 12 (dois) horas após a abertura da solicitação;

1.11.5. A CONTRATADA deverá ter especialistas na ferramenta proposta fisicamente na mesma cidade que a CONTRATANTE ou até no máximo 150km para melhor atendimento presencial se necessário.

1. MIGRAÇÃO

1.1. Garantir a importação de todas as informações compatíveis e bases do sistema de antispam atual utilizado pela CONTRATANTE para o novo sistema.

1.2. Sistema deverá ser testado em Homologação antes de ir para Produção.

1. PRAZO E LOCAL DE EXECUÇÃO DO SERVIÇO

1.1. O serviço deverá estar integralmente implementado na sede do CREMERS na cidade de Porto Alegre/RS dentro do prazo de 10 (dez) dias uteis após a assinatura do contrato.

7. Estimativa das Quantidades a serem Contratadas

Os quantitativos foram estimados com base na necessidade atual do CREMERS sendo o tempo de contratação e 12 meses podendo ser renovado por sucessivos períodos nos termos da lei .

8. Estimativa do Valor da Contratação

Valor (R\$): 26.921,00

VINTE E SEIS MIL, NOVECENTOS E VINTE E UM REAIS

9. Justificativa para o Parcelamento ou não da Solução

O objeto será licitado em item único, contemplo o objeto de forma global.

10. Contratações Correlatas e/ou Interdependentes

Para viabilizar a contratação desta demanda não foi identificado contratações com interdependência.

11. Alinhamento entre a Contratação e o Planejamento

A contratação deste objeto é imprescindível ao Conselho Regional de Medicina, para suprir às necessidades de filtragem de ameaças cibernéticas aos emails do CREMERS, tendo em vista o contrato anterior não foi renovado a licitante vencedora da última licitação.

12. Benefícios a serem alcançados com a contratação

Busca-se com esta contrata atender a necessidade do CREMERS relacionadas a filtragem de ameaças cibernéticas, através de proposta mais vantajosa em relação aos valores de mercado.

13. Providências a serem Adotadas

Definições das rotinas por parte da equipe de TI.

14. Possíveis Impactos Ambientais

Não foram identificados impactos ambientes nesta contratação, mas para o bom atendimento das melhores práticas de sustentabilidade ambiental no âmbito das contratações públicas, a presente contratação poderá, sem

restrição do caráter competitivo do certame, preferencialmente solicitar que o contrato seja encaminhado e assinado por meio eletrônico, a fim de evitar a impressão de papel.

15. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

15.1. Justificativa da Viabilidade

Esta contratação é viável.

16. Responsáveis

Porto Alegre, 07 de fevereiro de 2023

ALFREDO ROSA DA SILVA
Assistente