SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Renovação da solução de proteção de e-mail

Resumo: Renovação da solução de proteção de e-mail já existente na SCGÁS pelo período de 12 meses.

OBJETO:

Renovação da solução de proteção de e-mail *FortiMail Cloud* já existente na SCGÁS por um período de 12 meses.

1. Especificações técnicas mínimas necessárias:

1.1. Deve ser baseada em aplicação em nuvem (SaaS). Não serão considerados equipamentos ou máquinas virtuais em nuvem de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD ou GNU/Linux;

1.2. Deve possuir integração nativa com a solução FortiAnalyzer implementada no ambiente, permitindo a correlação de eventos entre as soluções Fortinet e análise centralizada dos logs gerados pelas ferramentas;

1.3. Deve possuir efetividade de detecção de 99,9% dos SPAMs, de acordo com testes independentes;

1.4. Deve atender até 225 (duzentas e vinte e cinco) caixa de e-mail pelo período de 12 meses;

1.5. Deve suportar integração com o Microsoft 365 através de API;

1.5.1. Esta integração deve suportar a varredura pós-entrega sob demanda de e-mails no Microsoft 365 e a varredura em tempo real, ou seja, as mensagens de e-mail devem ser verificadas logo após chegarem à caixa de correio do usuário;

1.6. Deve acompanhar a detecção de malwares comuns e do tipo zero-day através de sandboxing integrado em nuvem;

1.7. Deve oferecer proteção contra cliques em URLs encaminhadas por e-mail;

1.8. Deve ser fornecido também uma solução de DLP, para detectar informações sensíveis que podem estar vindo através de e-mail;

1.9. A funcionalidade de DLP deve permitir especificar a informação a ser detectada como palavras, frases e expressões regulares, possuir uma lista predefinida de tipos de informações, como números de cartão de crédito e outros, permitir a criação e armazenamento de impressões digitais (Fingerprint) de documentos e permitir a criação de filtros por arquivo;

1.10. A funcionalidade de DLP deve possuir uma lista predefinida de tipos de informações, como números de cartão de crédito e outros;

1.11. A funcionalidade de DLP deve permitir a criação e armazenamento de impressões digitais (Fingerprint) de documentos;

SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Renovação da solução de proteção de e-mail

Resumo: Renovação da solução de proteção de e-mail já existente na SCGÁS pelo período de 12 meses.

1.12. A solução deve ser capaz de funcionar como gateway SMTP para os servidores de correio existentes;
1.13. A solução deve ser capaz de funcionar como gateway, atuando como MTA (Mail Transfer Agent);
1.14. A solução deve ser capaz de operar em modo transparente, atuando como um proxy transparente para o envio de mensagens aos servidores de correio protegidos;
1.15. Deve poder ser instalado como um proxy SMTP transparente, para a análise do correio de saída, procurando evitar o relatório na Blacklist;
1.16. A solução deve ter uma API baseada em REST disponível para fins de monitoramento, automação e orquestração;
1.17. A solução deve suportar listas brancas e listas negras (White/Black List) por usuários, por domínio e globalmente para todo o sistema;
1.18. A solução deve permitir a substituição, edição e personalização de mensagens de notificação de antivírus e anti-spyware;
1.19. A solução deve ser capaz de atrasar o envio de e-mail de grandes dimensões aos horários que são de menos carga;
1.20. A solução deve ser capaz de definir o encaminhamento de correio (relay) para um IP específico baseado no IP de origem da mensagem;
1.21. A solução deve fornecer suporte para múltiplos domínios de e-mail;
1.22. A solução deve suportar a implementação de políticas por destinatário, domínio, por tráfego de entrada ou de saída;
1.23. A solução deve ser capaz de entregar o correio baseado em usuários existentes em uma base LDAP;
1.24. A solução deve suportar quarentena por usuário, possibilitando que cada usuário possa administrar sua própria quarentena, removendo mensagens ou liberando as que não são SPAM, diminuindo a responsabilidade do administrador e a possibilidade de bloqueio de e-mails legítimos. A quarentena deve ser acessada através de página Web e POP3;
1.25. A solução deve ser capaz de agendar o envio de relatórios de quarentena;
1.26. A solução deve ser capaz de realizar o armazenamento de e-mails (Archiving) baseado nas políticas de envio e recepção, com suporte também a armazenamento remoto;
1.27. A solução deve ser capaz de manter a filas de correio (Queue) em caso de falha na conexão de saída, atrasos ou erros de entrega;

Resumo: Renovação da solução de proteção de e-mail já existente na SCGÁS pelo período de 12 meses.

1.28. A solução deve ser capaz de realizar a autenticação SMTP via LDAP, RADIUS, POP3 ou IMAP;
1.29. A solução deve ser capaz de manter listas de reputação do remetente com base em: quantidade de vírus enviados, quantidade de e-mails considerado spam, quantidade de destinatários equivocados;
1.30. A solução deve suportar direcionamento em IPv4 e IPv6;
1.31. Permitir a aplicação de políticas através dos filtros de conexões: Limite de número de mensagens por conexão, limite de número de destinatários por mensagem, limite do tamanho de mensagens e filtros de Reputação
1.32. A solução deve permitir o armazenamento de e-mail e quarentena localmente ou servidor remoto;
1.33. A solução deve possuir funcionalidades de AntiSpam, Antivírus, Anti-Spyware e Anti-Phishing;
1.34. A solução deve ser capaz de realizar a inspeção de correio da Internet de entrada e saída;
1.35. A solução deve possuir um assistente (wizard) para o provisionamento fácil e rápido de configurações básicas e domínios para proteger;
1.36. A solução deve fornecer controle de DNS reverso para proteção contra ataques de Anti-Spoofing;
1.37. A solução deve se conectar em tempo real com a base de dados do fabricante para baixar atualizações AntiSpam;
1.38. A solução pode detectar se a origem de uma conexão é legal com base em um banco de dados de reputação de IP fornecido pelo fabricante;
1.39. A solução pode detectar se um e-mail é spam, verificando os URLs que contém, comparando-os com o banco de dados de reputação fornecido pelo fabricante;
1.40. A revisão de URLs deve permitir selecionar as categorias de URL que serão permitidas ou não, nos e-mails analisados. Este banco de dados de categorias será atualizado pelo fabricante;
1.41. A solução deve ter novos mecanismos de detecção de SPAM, através da análise contínua do correio recebido e sua correlação posterior com eventos ocorridos em todo o mundo, permitindo assim definir e detectar novas regras de SPAM;
1.42. A solução deve ser capaz de realizar a análise heurística e definir limites máximos de acordo com o compartilhamento de mensagens e assim determinar se um e-mail é spam;

Resumo: Renovação da solução de proteção de e-mail já existente na SCGÁS pelo período de 12 meses.

1.43. A solução deve ser capaz de realizar análise Bayesiana para determinar se um e-mail é spam;
1.44. A solução deve ser capaz de detectar se o e-mail é um boletim de informação (Newsletter);
1.45. A solução deve ser capaz de filtrar e-mails baseados na URIs (Uniform Resource Identifier) contidos no corpo da mensagem;
1.46. A solução deve ser capaz de realizar análise com base em palavras proibidas (Banned Word);
1.47. A solução deve ter uma técnica que detecta SPAM através do uso de Greylist, que classifica o correio com base na sua entrada no início da sessão, como bloquear todos os e-mails e permitir apenas aqueles reenviados;
1.48. A solução permite criar uma Whitelist ou Blacklist de palavras;
1.49. A solução deve permitir o gerenciamento de spam com capacidade de aceitar, encaminhar (Relay), rejeitar (Reject) ou descartar (Discard);
1.50. A solução deve ser capaz de realizar análise de imagem e documentos PDF para a procura de spam;
1.51. A solução deve ser capaz de suportar listas negras (Blacklist) de terceiros;
1.52. A solução deve suportar greylist para contas de e-mail em IPv4 e IPv6;
1.53. A solução permite identificar imagens que fazem referência ao conteúdo SPAM. Ele deve suportar a análise das seguintes extensões GIF, JPEG e PNG;
1.54. A solução deve suportar Sender Policy Framework (SPF);
1.55. A solução deve suportar Domain Keys Identified Mail (DKIM);
1.56. A solução deve suportar Domain Based Message Authentication (DMARC);
1.57. A solução deve permitir sua configuração através de interface para acesso à Web (HTTP, HTTPS);
1.58. A solução deve ser capaz de permitir a criação de administradores exclusivos para a administração e configuração da solução por domínio, sendo também possível restringir o acesso por endereço IP e máscara de rede de origem;
1.59. A solução deve ser capaz de fornecer, pelo menos, dois níveis de acesso de gestão: leitura/gravação (Read/Write) ou somente leitura (Read Only);
1.60. A solução deve permitir a criação de perfis de configuração de forma granular, onde para cada perfil pode adicionar configurações

Resumo: Renovação da solução de proteção de e-mail já existente na SCGÁS pelo período de 12 meses.

específicas de funcionalidades como AntiSpam, antivírus, autenticação, entre outros;

1.61. Quando a solução estiver implementada em alta disponibilidade, deve ser capaz de detectar e notificar a falha de algum dispositivo;

1.62. A solução deve ser capaz de filtrar anexos e conteúdo de e-mails;

1.63. A solução deve ser capaz de executar análise de antivírus/antispyware em arquivos compactados;

1.64. A solução deve ter uma base de informações de malware fornecida pelo fabricante atualizadas de forma recorrente;

1.65. Após a detecção de um malware, a solução pode executar as seguintes ações: envie uma mensagem de notificação, reenviar mensagens e malwares para uma conta definida, reescreva o destinatário;

1.66. A solução deve ser capaz de verificar os e-mails que são liberados da quarentena SPAM pelo usuário em busca de conteúdo malicioso;

1.67. A solução deve suportar criptografia da mensagem baseada em identidade (Identity Based Encryption IBE) para que o destinatário não requeira uma PSK ou certificado instalado anteriormente para a descriptografado;

1.68. Criptografia de mensagens com IBE, deve suportar tanto o método push e pull, em que a mensagem criptografada é armazenada na plataforma de e-mail para acesso remoto autenticado ou ser enviado como anexo para o destinatário;

1.69. Em ambos os métodos da criptografia IBE, deve ter um registro do usuário do destino na plataforma de e-mail, de modo que, para ver as mensagens criptografadas, um processo de autenticação é necessário;

1.70. Deve suportar criptografia de e-mail usando S / MIME;

1.71. Suportar criptografado SMTPS e SMTP over TLS;

1.72. A solução deve analisar o conteúdo e anexos de uma mensagem em busca de palavras que indicam que o correio deve ser em quarentena, criptografado, arquivado, bloqueado, marcado, substituído ou encaminhado para outro host;

1.73. Deve inspecionar arquivos protegidos por senha, usando senhas predefinidas, uma lista de senhas ou pesquisar a palavra “password” no corpo;

1.74. A solução deve permitir o relato de atividade, analisando os arquivos de eventos (logs) e apresentá-los na tabela ou formato gráfico;

Resumo: Renovação da solução de proteção de e-mail já existente na SCGÁS pelo período de 12 meses.

1.75. A solução deve permitir gerar relatórios sob demanda ou programados em intervalos de tempo específicos.

2. CONDIÇÕES DE PAGAMENTO

Items	Cronograma
01	Após recebimento das licenças

2.1. As Condições de Pagamento deste Edital obedecerão sempre ao pré-requisito de haver uma entrega homologada previamente, conforme estipulado pela Legislação vigente.

2.2. As etapas de pagamento estão estipuladas conforme o cronograma abaixo:

ITEM	PRAZO
Licenciamento	À vista, conforme cronograma de pagamentos da SCGÁS, após o recebimento formal das licenças.
Serviços de Atualização e Configuração	À vista, conforme cronograma de pagamentos da SCGÁS, após a Entrega Total do Projeto.

3. CONDIÇÕES GERAIS:

3.1. O CONTRATADO deverá fornecer as subscrições com validade para 12 meses.

3.2. A solução ofertada deverá funcionar em período de 24x7 durante todos os dias de vigência do contrato.

3.3. O prazo de entrega das subscrições e das novas chaves é de até 7 (sete) dias após assinatura do contrato.

3.4. O serviço de atualização tecnológica e configuração da solução ofertada deverá ser realizado durante o período de vigência do contrato conforme necessidade da SCGÁS.

Resumo: Renovação da solução de proteção de e-mail já existente na SCGÁS pelo período de 12 meses.

3.5. O serviço de atualização tecnológica e configuração da solução ofertada poderá ser realizado de forma on-site ou remoto.

3.6. Se o serviço de atualização tecnológica e configuração da solução ofertada for realizado de forma on-site, o CONTRATADO deverá levar em consideração:

- As despesas de deslocamento (passagens, táxi, traslados, pedágios, estacionamentos etc.), estadia e alimentação ficam sob responsabilidade do CONTRATADO.

- Serão responsabilidade integral do CONTRATADO todos os serviços a serem realizados em horário não comercial, eventuais acréscimos sobre o valor-hora normal de seus profissionais, atividades realizadas em Sábados, Domingos e Feriados etc.

3.7. O CONTRATADO deverá manter durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

3.8. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, de acordo com o Termo de Confidencialidade disposto no Anexo do Contrato.

3.9. Estar em conformidade com a Lei Nº 13.709, de 14 de agosto de 2018, a LGPD – Lei Geral de Proteção de Dados.

3.10. O CONTRATADO deverá disponibilizar o acesso ao suporte imediatamente após a assinatura do contrato.

3.11. O CONTRATADO deverá disponibilizar por um período de 24 (vinte e quatro) meses durante o período de validade do contrato um canal de comunicação (0800, e-mail, site) para suporte técnico ilimitado quando necessário.

3.12. O CONTRATADO deverá disponibilizar durante período de vigência do contrato qualquer versão nova da solução ofertada sem custos para a SCGÁS.

SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Renovação da solução de proteção de e-mail

Resumo: Renovação da solução de proteção de e-mail já existente na SCGÁS pelo período de 12 meses.

3.13. O CONTRATADO deverá encaminhar as chaves de acesso por e-mail, ou disponibilizar via download ao fiscal do contrato ou pelo correio para a SEDE da SCGÁS, 2º Andar, Gerência de Finanças e Sistemas de Informação, localizada na Rua Antônio Luz, 255 - Centro Empresarial Hoepcke - 88010-410 - Florianópolis - SC.

ASSINADO DIGITALMENTE
Validade jurídica assegurada conforme MP 2.200-2/2001, que instituiu a ICP-Brasil
BRyTecnologia

ALISON LUIZ MARTINS SCHVEITZER:91992362919.923.629-04

Emitido por: AC SyngularID Multipla

Data: 10/11/2025

Alison Luiz Martins Schveitzer
Analista de Tecnologia da Informação