Secretaria de Estado da Segurança Pública

ESTADO DE GOIÁS
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA
GERÊNCIA DE TELECOMUNICAÇÕES

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de solução de Filtro de Conteúdo de E-mail para proteção de 27.000 caixas postais, incluindo sistema de segurança contra ataques dirigidos, bem como treinamento, implantação, manutenção preventiva e suporte técnico especializado 24x7, pelo período de 12(doze) meses para a segurança e proteção da plataforma de e-mail da SSPGO.

2. JUSTIFICATIVA DA CONTRATAÇÃO

2.1. A Gerência de Telecomunicações da SSPGO tem entre suas principais atribuições conforme DECRETO Nº 9.690, DE 06 DE JULHO DE 2020 que Aprova o Regulamento da Secretaria de Estado da Segurança Pública:

2.1.1. "Gestão de Segurança da Informação, definição de Política de Segurança, controle de acesso, análise e correção de vulnerabilidades em aplicações e rede corporativa."

2.1.2. "Disponibilização e Gerência de Acesso Internet e Intranet, Correio Eletrônico, Armazenamento de Arquivos, Hospedagem de Sites Web, Banco de Dados, Servidores de Análise de Dados/BI e Aplicações."

2.1.3. "Gerenciar e configurar servidores de virtualização, antivírus, firewall, antispam, filtro de conteúdo web e Sistema de Prevenção de Intrusão / IntrusionPrevention System(IPS);"

2.1.4. "Análise e especificação de ferramentas, equipamentos e serviços de TI e de Telecomunicações para aquisição ou contratação. "

2.2. A Lei Geral de Proteção de Dados Pessoais (LGPD) - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, já em vigor em todo Brasil, torna obrigatório a definição de mecanismos formais que visem auxiliar no controle sobre o tratamento de dados nas instituições conforme abaixo:

"Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

"Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios."

"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais

ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

"Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término."

2.3. Esta contratação tem por objetivo a contratação de solução de segurança do tipo AntiSpam para promover o aumento dos níveis de segurança no ambiente de e-mail institucional. Refere-se ao objetivo de identificar e bloquear, em tempo real, ataques, invasões ou abusos direcionados ao ambiente de e-mail, de forma a reduzir os riscos relacionados à imagem institucional, perda de informações e descumprimento de normas e regulamentos. Visa também atender a necessidade de possuir uma infraestrutura mais robusta, necessária para atender às demandas de envio e recebimento de mensagens institucionais, internas e externas, através da implementação de recursos de segurança da informação. Visa atender as áreas finalísticas com melhor qualidade, em menor espaço de tempo, diminuindo o período de inatividade dos usuários, causados por incidentes de segurança, aumentando assim a produtividade; prover melhores serviços aos usuários finais, oferecendo maior qualidade, ampliando a eficiência e a segurança das atividades executadas.

2.4. Em decorrência disso, é fundamental a definição de estratégias que unifiquem os propósitos desses pilares da Segurança da Informação. Dentre as medidas de segurança que garantem a proteção e a preservação das informações da Instituição, destaca-se a utilização de uma ferramenta de detecção e de prevenção de contaminações ou ataques de programas maliciosos, como vírus e malwares em geral, que possam vir a comprometer os dados e informações do negócio.

2.5. O correio eletrônico é o canal mais usado para ataques oportunistas e direcionados, além de um ponto importante de saída para conteúdo confidencial, sendo assim, uma solução integrada de AntiSpam e mecanismo de prevenção de perda de dados se mostra um componente crítico da estratégia de segurança em um ambiente de correio eletrônico onde ameaças estão sempre em evolução.

2.6. A contratação mostra-se imprescindível em razão da necessidade de manutenção dos serviços de segurança da informação e de correio eletrônico, sendo de suma importância a adoção da solução de segurança para tratamento de mensagens não solicitadas (SPAM e PHISHING), de modo a evitar a disseminação de softwares maliciosos.

2.7. Objetivos a Serem Alcançados:

2.7.1. Reduzir riscos de segurança associados à TI, diminuindo a possibilidade de ataques direcionados diretamente à rede e seus componentes e proprietários de contas de correio, a partir de e-mails contendo trojans, vírus ou ataques que utilizem engenharia social;

2.7.2. Aumentar a disponibilidade dos sistemas de correio eletrônico;

2.7.3. Reduzir quantidade de incidentes relacionados a ameaças oriundas da Web;

2.7.4. Prevenir eventuais falhas e antecipar soluções de possíveis problemas;

2.7.5. Obter ganho de tempo na identificação e correção de problemas com análise especializada que direcionará as soluções;

2.7.6. Garantir a disponibilidade do serviço de correio eletrônico contra ataques provenientes da Internet.

2.7.7. Melhoria na reputação do domínio de correio eletrônico: Refere-se a melhoria da reputação externa da instituição, que recebe e envia uma quantidade significativa de mensagens eletrônicas, atendendo aos trabalhos de pesquisa, coleta e divulgação de dados para a população e órgãos públicos. Com a implantação de controles efetivos, a instituição fica menos suscetível a penalidades como inserção em Blacklists, que são cadastros utilizados para disparadores de e-mails classificados como Spammers (disparadores se Spam).

2.8. Benefícios Diretos e Indiretos:

2.8.1. Diminuir a incidência de e-mails indesejáveis na caixa postal dos usuários;

2.8.2. Melhorar o controle, reduzindo ocorrências ou incidentes com agentes maliciosos;

2.8.3. Reduzir a perda de produtividade, na medida em que seja diminuído o tempo pelo usuário com procedimentos de abertura de mensagens, verificação e registro de ocorrência por suspeita ou confirmação de SPAM;

2.8.8. Automatizar algumas tarefas de gerenciamento na filtragem de mensagens, como por exemplo interface para usuário para avaliar e liberar mensagens quarentenadas, envio de relatórios de bloqueios e mensagens quarentenadas (digest), etc.

2.8.9. A redução do tráfego de mensagens não solicitadas (spam) diminui custos de armazenamento de disco dos servidores e também das estações de trabalho. Reduz, também, a disseminação de vírus e de outros "softwares" maliciosos nocivos à segurança das estações e da rede institucional.

2.9. Da Justificativa do quantitativo solicitado:

2.9.1. Atualmente a GETEL mantém solução de correio eletrônico para as Unidades da SSPGO.

2.9.2. Abaixo é listado a quantidade de caixas postais existentes e administradas pelo corpo técnico da Unidade:

Unidade	CAIXAS
Corpo de Bombeiro Militar	3015
Polícia Civil	5601
Polícia Militar	15805
Polícia Científica	1117
SSP	447
PROCON	87
TOTAL	26.072

2.9.3.Considerando a natureza dinâmica de criação de caixas postais para atendimento de novas demandas, será feito a contratação para 27.000 caixas postais, tal quantidade representa um acréscimo de em torno de 5% no quantitativo total listado acima.

2.9.4 O quantidade de 05 (cinco) unidades para o item de treinamento, corresponde ao quantitativo corpo técnico da GETEL que administram as soluções de e-mail em utilização na SSPGO.

3. QUANTITATIVO E VALOR ESTIMADO

3.1. QUANTITATIVO E VALOR ESTIMADO:

LOTE	ITEM	CÓDIGO	DESCRIÇÃO	MÉTRICA	QTD	VALOR UNITÁRIO 12 MESES	VALOR TOTAL 12 MESES
1	1.1	80497	Serviços de solução integrada Anti-Spam e Antivírus de e-mail, contemplando atualização de base de assinaturas, atualização de software e	Caixas Postais	27.000	R$ 21,32	R$ 575.640,00

			suporte técnico do fabricante, pelo período de 12 (doze) meses.				
	1.2	69299	Serviço de implantação em alta disponibilidade de solução de gateway de segurança de e-mail	Serviço de implantação	01	R$ 10.280,00	R$ 10.280,00
	1.3	43497	Treinamento em solução de gateway de segurança de e-mail.	Aluno	05	R$ 1.570,67	R$ 7.853,35
Valor total da Contratação							R$ 593.773,35

3.1.1. O valor total geral estimado para a presente contratação é de R$ 593.773,35 (quinhentos e noventa e três mil setecentos e setenta e três reais e trinta e cinco centavos).

3.1.2. Considerando a natureza dos serviços a licitação será realizada na modalidade Pregão Eletrônico do tipo Menor Preço observando, como critério de julgamento, o valor GLOBAL.

4. CLASSIFICAÇÃO DOS SERVIÇOS, PARCELAMENTO E ADJUDICAÇÃO DO OBJETO

4.1. Os serviços que constituem objeto desta contratação são caracterizados como serviços comuns, com conformidade com a Lei nº 10.520/2002 e o Decreto nº 7.174/2010, por possuir especificações usuais de mercado, nos termos dos referidos diplomas legais.

4.2. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto nº 9.507/2018, constituindo-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal do órgão licitante, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

4.3. PARCELAMENTO E ADJUDICAÇÃO DO OBJETO

4.3.1. No contexto desta contratação e de acordo com os requisitos levantados, verifica-se que o objeto poderá ser dividido em itens, tendo em vista que a divisão não traz prejuízo para o objetivo final almejado. Portanto o objeto será dividido em 03 (três) itens, porém deverá ser adquirido em lote único.

4.3.2. A contratação da solução de antispam com o fornecimento de software e serviços técnicos deverá ser em lote único, com a adjudicação de forma global a um único fornecedor.

4.3.3. A composição do lote ÚNICO neste Termo de Referência considera que os itens possuem a mesma natureza e apresentam relação de dependência física ou lógica entre si para garantir funcionamento adequado do conjunto. Afasta-se assim a figura da impossibilidade de competição visto que as empresas que atuam no ramo de mercado dos produtos podem ofertá-los agrupados. E garante segurança à CONTRATANTE no sentido de que o conjunto funcione em sintonia garantindo o correto funcionamento da solução.

4.3.4. Para melhor entender o agrupamento de itens em lote único vamos enfatizar abaixo a similaridade dos bens/serviços e o fato de que os mesmos funcionam em conjunto para prover as funcionalidades deles exigidas, a saber:

4.3.4.1. Item 1.1: composto pelas licenças do software pretendido contemplando atualização de base de assinaturas, atualização de software e suporte técnico do fabricante;

4.3.4.2. Item 1.2: composto pelo Serviço de implantação da solução em ambiente de produção utilizando as licenças fornecidas no item 1.1;

4.3.4.3. Item 1.3: composto pela transferência de conhecimento da solução ofertada no item 1.1, pelo processo de implantação do item 1.2 e capacitação oficial do fabricante;

4.3.5. Acredita-se que a promoção de fracionamentos no objeto, além destes que já foram elaborados, poderia incorrer em impossibilidade de implantação da solução e poderá causar sérios transtornos operacionais para a CONTRATANTE.

5. SUBCONTRATAÇÃO

5.1. Não será admitida a subcontratação do objeto da presente licitação.

6. ALTERAÇÃO SUBJETIVA

6.1. É admissível a fusão, cisão ou incorporação da contratada com/por outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

7. DOS REQUISITOS TÉCNICOS

7.1. DA PLATAFORMA

7.1.1. A solução integrada deve possuir controle de caixas postais e fluxo de análise de mensagens/dia ilimitadas, de acordo com os recursos de hardware disponíveis;

7.1.2. Deve ser uma solução MTA (Mail Transfer Agent) completa com suporte ao protocolo SMTP, que controla o envio e o recebimento de todas as mensagens da empresa, com registro de logs das atividades do MTA;

7.1.3. A licença de uso deve atingir ao número de caixas postais contratadas e o consumo da licença somente pode ocorrer para uma caixa postal que efetivamente realizou envio / recebimento de mensagens;

7.1.4. Deve ser capaz de filtrar o tráfego de correio, bloqueando a entrada de vírus, spyware, worms, trojans, SPAM, phishing, e-mail marketing, e-mail adulto ou qualquer outra forma de ameaça virtual;

7.1.5. Deve permitir alta disponibilidade das funções de filtragem, de maneira assegurar que o serviço de correio nunca pare por falha da solução;

7.1.6. A solução deve suportar o processamento de no mínimo 20.000 (dez mil) conexões simultâneas e 160.000 (cento e sessenta mil) mensagens por hora;

7.1.7. Deve ser capaz de efetuar implementação em virtual appliance, compatível com os principais sistemas de virtualização do mercado, entre eles:

a. VMWare;

b. Citrix;

c. Microsoft Hyper-V.

7.2 DAS CERTIFICAÇÕES DE COMPATIBILIDADES E PARCERIAS

7.2.1. O antivírus utilizado na solução, deverá participar do programa “Microsoft Active Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;

7.3 CARACTERÍSTICAS GERAIS

7.3.1 A licença de uso do software base deve possuir 12(doze) meses de atualização do fabricante compreendendo os seguintes módulos:

7.3.1.1. Atualização das assinaturas de segurança disponibilizadas automaticamente como por exemplo: assinaturas de vírus, malwares e outras ameaças, serviços de reputação de websites, IPs e assinaturas de Websites e aplicativos web;

7.3.1.2. Direito de uso da versão mais atual do produto licenciado caso esta esteja disponível pelo fabricante bom como atualizações de recursos melhorias dentro da mesma versão;

7.3.1.3. Acesso a base de inteligência global do fabricante para análise online de ameaças;

7.3.1.4. Deve possuir compatibilidade nativa com as principais soluções de mensageiria do mercado,tendo seu uso homologado e todas suas funcionalidades mantidas para integração ao microsoft exchange e zimbra;

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

7.3.2. Analisar mensagens, no mínimo, por meio dos seguintes métodos:

7.3.2.1. Proteção dinâmica por reputação;

7.3.2.2. Assinaturas de spam;

7.3.2.3. Filtros de Vírus;

7.3.2.3.1. A verificação de vírus, além da técnica tradicional (por assinatura), também deve ser feito através de BigData do fabricante, bem como utilização de método Fuzzy Hash para detecção de similaridades e detecção de possível variante de malware;

7.3.2.3.2. Possuir dois módulos de antivírus, sendo um do próprio fabricante, já devidamente licenciado para uso simultâneo;

7.3.2.4. Filtros de anexos;

7.3.2.5. Filtros de phishing;

7.3.2.6. Análise heurística;

7.3.2.7. Análise do cabeçalho, corpo e anexo das mensagens;

7.3.2.8. E-mail bounce;

7.3.2.9. Dicionários pré-definidos e customizados com palavras e expressões regulares;

7.3.2.9.1. Já deve vir com dicionários pré-estabelecidos, para posterior utilização, tais como:

7.3.2.9.1.1. Número de cartão de crédito;

7.3.2.9.1.2. CNPJ;

7.3.2.9.1.3. RG e CPF;

7.3.3. Deve possuir mecanismo de backup e recuperação da configuração da solução;

7.3.4. Deve possuir capacidade de envio de backup via FTP e SFTP, sendo configurado diretamente na interface gráfica da solução (sem necessidade de qualquer configuração em linha de comando);

7.3.5. Os manuais necessários à instalação e administração da solução, devem constar no seguinte idioma: Português do Brasil;

7.3.6. A interface de administração do sistema deve ser permitida a instalação, para uso no mínimo nos seguintes idiomas:

7.3.6.1. Português do Brasil;

7.3.6.2. Inglês;

7.3.7. Deve haver a possibilidade de usar o idioma Português do Brasil para administração, manutenção e geração de relatórios;

7.3.8. Deve possuir banco de dados relacional para armazenamento dos registros de acesso, logs de sistema e configurações. Caso a solução necessite de banco de dados específico e proprietário, as licenças deste deverão ser fornecidas pela contratada junto com a solução ofertada sem ônus para o contratante. Não serão aceitas soluções baseadas em armazenamento de Logs em formato Texto;

7.3.9. Deve possuir capacidade de configuração de roteamento de mensagens para múltiplos domínios de origem e destino;

7.3.10. Deve permitir a configuração de múltiplos domínios, com aplicação de regras de forma independente para cada um dos domínios;

7.3.11. Ter a capacidade de processar o tráfego de entrada e de saída de mensagens no mesmo appliance, com base no IP e domínio de origem da mensagem, permitindo criar filtros e ações diferenciadas para cada sentido;

7.3.12. A solução deve ser capaz de efetuar a saída de e-mails indicando um IP específico para a saída de mensagens, isto é, possuir a capacidade de redirecionar as mensagens de saída por IP's diferentes para cada domínio cadastrado no appliance se o administrador assim desejar;

7.3.13 .A solução deve permitir criação de regras por:

7.3.13.1. Grupos de usuários;

7.3.13.2. Domínios;

7.3.13.3. Range de IP;

7.3.13.4. IP/Rede;

7.3.13.5. Remetentes específicos;

7.3.13.6. Destinatários específicos;

7.3.13.7. Grupos de LDAP;

7.3.14. Tratar e analisar mensagens originadas e recebidas possibilitando a aplicação de regras e políticas customizáveis, além de diferenciadas por sentido de tráfego;

7.3.15. Possibilidade de permitir relay autenticado para clientes externos da corporação;

7.3.16. Deve possuir ferramenta de auditoria de email, com facilidade de pesquisa por origem, destino, assunto e conteúdo da mensagem permitindo a concatenação dos filtros através dos operadores lógicos "e" e "ou";

7.3.17. A console de gerenciamento deve permitir a transferência de arquivos (SCP/FTP) e ser acessada através de protocolo seguro (HTTPS – HyperText Transfer Protocol Secure) com no mínimo as seguintes funcionalidades:

7.3.17.1. Administração centralizada de todas as regras e filtros integrantes da solução;

7.3.17.2. Status da versão das assinaturas do antivírus em uso;

7.3.17.3. Controle de acesso de usuários, com diferentes privilégios de configuração;

7.3.17.4. Criação de relatórios, gráficos e estatísticas, com suporte a múltiplos domínios;

7.3.17.5. Retenção de mensagens com base nas regras em área de quarentena e gerência das áreas de quarentena pelo administrador e possibilidade do usuário gerenciar sua área

de quarentena.

7.3.18. Deve possuir administração via shell, através de SSH para CLI (command line interface), para execução de comandos de administração e suporte;

7.3.19. Suporte à assinatura e validação de autenticidade de mensagens através de Domains Keys, DKIM e SPF;

7.3.20. Permitir efetuar controle profundo dos anexos das mensagens, podendo tomar ações diferenciadas para:

7.3.20.1. Conteúdo do anexo;

7.3.20.2. Mime-Type do anexo;

7.3.20.3. Extensão do anexo;

7.3.20.4. Nome completo do anexo;

7.3.20.5. Nome parcial do anexo;

7.3.20.6. Expressão regular;

7.3.20.7. Tamanho do anexo;

7.3.20.8. Figerprint do anexo (permitir efetuar upload de um exemplo de arquivo para que o sistema crie uma assinatura de identificação);

7.3.20.9. Anexos compactados com senha;

7.3.20.10. Quantidade de níveis de compactação no mesmo anexo;

7.3.21. Possuir “Zimlet” de integração com o sistema de correio eletrônico Zimbra, permitindo que através da interface Web do Zimbra seja possível marcar uma mensagem como “Spam” ou “Não Spam”, atualizando o sistema de filtragem e gerando uma nova regra para autoaprendizagem do sistema;

7.3.22. Deve possuir um sistema de Disaster e Recover, ao qual com um só botão é efetuado o upload de um arquivo de backup e restauração do mesmo automaticamente.

7.3.23. Possuir a função de abertura de relay automático para empresas que usam Microsoft Office 365, sem necessidade de cadastro de IP´s ou DNS da Microsoft para abertura de relay.

7.3.24. Deve possuir sistema de diagnóstico, com no mínimo de execução nos seguintes testes:

7.3.24.1. Teste de Conectividade TCP – Bastando informar o Host e Porta a ser testado;

7.3.24.2. Teste de Conectividade ICMP – Bastando Informar o Host a ser testado;

7.3.24.3. Teste de DNS – Bastando informar Host ou Domínio a ser testado;

7.3.24.4. Teste de Envio de E-mail;

7.3.24.5. Teste de Lookup de E-mail via LDAP;

7.3.24.6. Teste de Conectividade com o fabricante (para isso, testa-se as portas necessárias de comunicação junto ao fabricante);

7.3.24.7. Teste de TRACEROUTE;

7.3.24.8. Teste de DNS Reverso;

7.3.24.9. Teste de SPF, para checar se tem registro para um determinado domínio;

7.3.24.10. Teste de DKIM, para checar se tem registro para um domínio;

7.3.24.11. Teste de DMARC, para checar se tem registro para um domínio;

7.3.24.12. Teste de portas de Saída utilizadas pelo sistema.

7.3.25. Deve ter a capacidade de controle sobre os serviços executados no sistema, com a ação de: parar, inicializar ou reinicializar. O controle dos serviços devem ser sobre no mínimo os seguintes itens:

7.3.25.1. Serviço de antivírus;

7.3.25.2. Serviço de Controle de bounce;

7.3.25.3. Serviço de Cache do Banco de Dados;

7.3.25.4. Serviço de DKIM;

7.3.25.5. Serviço de DMARC;

7.3.25.6. Serviço de DLP;

7.3.25.7. Serviço de Mailsplit;

7.3.25.8. Serviço do Reputação das Mensagens;

7.3.25.9. Serviço de SMNP.

7.3.26. Deve permitir a instalação de agentes/plug-ins (tanto no appliance de gerenciamento, quanto nos agentes que fazem a filtragem) para monitoramento com sistemas de terceiros, tais como:

7.3.26.1. Zabbix;

7.3.26.2. Cacti;

7.3.26.3. Nagios;

7.4. DA ALTA DISPONIBILIDADE

7.4.1. Suportar Cluster de Alta Disponibilidade na forma de Cluster Ativo-Ativo e Ativo-Passivo e Load Balance através do registro MX e/ou sistemas de balanceamento proprietário, assegurando as funções de filtragem que o serviço de recebimento, processamento e entrega das mensagens não pare por falha na solução;

7.4.2. Deve permitir a configuração em Cluster com appliances virtualizados em DataCenters distintos;

7.4.3. Suportar replicação completa dos registros de e-mails e quarentena, para caso seja apresentado algum problema em um dos nodes do cluster, o outro assumir todo o processamento;

7.4.4. O cluster deve poder ser formado por appliances físicos e/ou appliances virtuais, de forma mista.

7.4.5. Administração centralizada de múltiplos pontos de acesso em uma única interface web, independente se estiver em modo cluster de alta disponibilidade ou load balance de forma que o gerenciamento e a replicação de políticas do cluster também seja feita de forma centralizada;

7.4.6. A administração de todo cluster deve ser feita através de um único IP de destino, não sendo permitido a gestão de regras de forma descentralizada.

7.4.7. Possuir capacidade de replicação automática das configurações e balanceamento de carga através um único Virtual IP.

7.5. DO GERENCIAMENTO

7.5.1. O acesso à interface de administração deve possuir diferentes níveis de acesso de forma granular, permitindo que sejam configurados perfis diferentes de administradores, por endereços de e-mail e domínio permitidos;

7.5.2. O sistema deve permitir criar usuário do tipo Auditor que tenha permissão de visualizar através da interface web os e-mails que forem colocados para auditoria, sendo possível definir

quais endereços de e-mails ou domínios ele poderá auditar;

7.5.3. O sistema deve possuir ainda no mínimo quatro perfis de administrador pré-definidos:

7.5.3.1. Administrador: Com acesso total às configurações da solução;

7.5.3.2. Administrador: Com acesso total às configurações da solução sem acesso à leitura dos e-mails armazenados tanto na quarentena como mensagens auditadas;

7.5.3.3. Auditor: Com acesso a visualização dos e-mails armazenados para auditoria;

7.5.3.4. Operador: Com acesso à administração da quarentena e gerenciamento da “Black e White List”;

7.5.3.5. Usuário: Possui a capacidade de administrar sua “Black e White List”, individualmente, bem como sua área de quarentena individual;

7.5.4. Permitir a criação de grupos, para posterior aplicação de regras. Os grupos poderão ser criados através das seguintes métricas:

7.5.4.1. Emails;

7.5.4.2. Domínios;

7.5.4.3. IP’s;

7.5.4.4. Range de IP;

7.5.4.5. Expressão Regular;

7.5.4.6. Usuários;

7.5.4.7. Listas de distribuição;

7.5.4.8. Grupos de LDAP.

7.5.4.9. Possibilidade de utilizar todos os anteriores como exceção.

7.6. DOS ALERTAS E LOGS

7.6.1. Deve enviar notificações por e-mail ao administrador, caso as atualizações não tenham sido realizadas com sucesso;

7.6.2. A solução deve ser capaz de gerar notificações a remetente e/ou destinatário com mensagem de alerta customizável;

7.6.3. 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 do mesmo, não sendo necessário acionamento da fabricante da solução;

7.6.4. Possuir mecanismo de feedback por email ao administrador sobre recursos e atualizações do sistema;

7.6.5. Deve possuir capacidade de envio dos logs de um ponto de acesso específico ou de todo o cluster para um servidor de syslog. Também deve ser possível selecionar os logs a serem enviados, bastando selecionar conforme opções indicados:

7.6.5.1. Emergency;

7.6.5.2. Alert;

7.6.5.3. Critical;

7.6.5.4. Error;

7.6.5.5. Warning;

7.6.5.6. Notice;

7.6.5.7. Informational;

7.6.5.8. Debug;

7.6.6. Deve ser possível enviar email caso ocorra consumo excessivo de algum recurso do sistema. Os sistemas monitorados para envio do email podem ser:

7.6.6.1. Espeço em disco;

7.6.6.2. Filas de email;

7.6.6.3. Memória;

7.6.6.4. Processador;

7.6.6.5. Serviço de Filtragem;

7.6.6.6. Atualização do sistema de segurança;

7.6.6.7. Antivirus e Antispam;

7.6.6.8. Ponto de acesso indisponível.

7.7. DAS FUNCIONALIDADES PARA O USUÁRIO FINAL

7.7.1. Possuir interface web de administração segura HTTPS para que o usuário final possa administrar suas opções pessoais, sem que estas opções interfiram na filtragem dos demais usuários;

7.7.2. A interface do usuário final deve estar no idioma configurado pelo administrador, sendo no mínimo os seguintes idiomas:

7.7.2.1. Português do Brasil;

7.7.2.2. Inglês;

7.7.3. O usuário final deve poder incluir e remover endereços em sua lista pessoal de bloqueio ou de liberação de e-mails;

7.7.4. O usuário final deve poder visualizar as mensagens bloqueadas e liberá-las, a seu critério, desde que as mesmas sejam consideradas somente como “possível spam” ou “spam;

7.7.5. O usuário final deve poder solicitar liberação de uma mensagem ao administrador, caso a mensagem contenha conteúdo considerado malicioso ou bloqueado por outro critério qualquer ao qual não permita que o usuário final a libere;

7.7.6. O usuário deverá poder selecionar qual o idioma utilizado sua interface, sendo no mínimo os seguintes idiomas:

7.7.6.1. Português do Brasil;

7.7.6.2. Inglês;

7.8. DA QUARENTENA

7.8.1. Permitir ao administrador da solução executar pesquisa nas áreas de quarentena de todos os usuários através de interface web segura (HTTPS), acessando o próprio appliance, sem necessidade de nenhum hardware adicional;

7.8.2. Deve possibilitar a gestão de quarentena pelos administrados de forma que o mesmo possa visualizar a razão de um determinado bloqueio, remetente, destinatário, data, assunto, IP do host destinatário, a mensagem original, tamanho da mensagem original e permitindo no mínimo as ações liberar e/ou excluir;

7.8.3. Caso uma mensagem seja bloqueada ou rejeitada, a solução deverá informar também a razão do bloqueio e quais regra foram ativadas;

7.8.4. A interface deve permitir identificar quais Regras do Modulo de AntiSpam foram ativadas e qual sua pontuação, afim de permitir ao administrador a elaboração de regras granulares;

7.8.5. A solução deve suportar a criação de áreas de quarentena personalizadas para usuários específicos;

7.8.6. Deve permitir também que todas as áreas de quarentenas sejam armazenadas de forma criptografadas no próprio appliance, seja ele virtual ou físico.

7.8.7. Deve permitir que o tempo de armazenamento da quarentena seja individual por cada área de quarentena;

7.8.8. Deve permitir a visualização do resumo de todas as áreas de quarentena e volume de mensagens;

7.8.9. O sistema de quarentena de e-mails deve criptografar automaticamente as mensagens armazenadas, evitando o acesso não autorizado aos arquivos e ao conteúdo dos e-mails armazenados em quarentena, assim aumentando a confiabilidade e segurança da solução;

7.8.10. Possibilitar ao administrador selecionar o período de expiração das mensagens na quarentena, por exemplo: manter as mensagens das últimas 72 horas, dessa forma ao ultrapassar esse limite, o sistema automaticamente começará a apagar os e-mails quarentenados mais antigos;

7.8.11. O tempo de armazenamento da quarentena deve ser individual por área de quarentena, devendo também permitir armazenamento por tempo “indeterminado”;

7.8.12. Possibilitar ao administrador selecionar o roteamento das mensagens em quarentena por tamanho da quarentena, por exemplo limitar uma quarentena a 100GB, sendo que ao ultrapassar o limite deste tamanho, o sistema automaticamente começará a apagar os e-mails quarentenados mais antigos;

7.8.13. O administrador ao criar uma quarentena customizada, deverá ter a capacidade de selecionar quais usuários poderão ter acesso a ela;

7.8.14. Pelo sigilo da informação, permitir que seja selecionada quais quarentenas customizadas somente sejam acessíveis a determinados administradores, permitindo a granularidade de acesso destas quarentenas.

7.9. DOS USUÁRIOS E GRUPOS

7.9.1. Possuir integração com serviço de diretórios LDAP, Microsoft Active Directory e Zimbra para obtenção de informações de usuários cadastrados para validação de destinatário e configuração de políticas, bem como impedir ataques de dicionário (“Directory Harvest Attack”) sem que haja necessidade de modificar os parâmetros “default” do serviço de diretórios;

7.9.2. Permitir criação de conectores para múltiplos serviços de diretório, por exemplo conector para servidor LDAP e outro conector para Microsoft Active Directory;

7.9.3. Possuir a funcionalidade de filtrar individualmente, baseado em políticas definidas por domínio, subdomínio, grupo de usuários e usuário individual, de forma integrada com ferramentas de LDAP, mesmo que a mensagem seja destinada a múltiplos destinatários, em categorias distintas;

7.9.4. Permitir a utilização de mais de um servidor de LDAP, para autenticação dos usuários em outro servidor LDAP, caso ocorra indisponibilidade do servidor primário de LDAP;

7.9.5. Integração nativa com os principais sistemas de colaboração do mercado, entre eles:

7.9.5.1. Microsoft Exchange®;

7.9.5.2. Zimbra Collaboration Suite®;

7.9.5.3. IBM Lotus Domino®;

7.9.6. Possibilitar a customização de regras e políticas por usuários ou grupos;

7.9.7. A solução deverá permitir a configuração do intervalo de sincronismo entre a solução anti-spam e o serviço de diretório;

7.9.8. Permitir atrelar grupos a regras específicas de rotas, por exemplo: Não aplicar determinada regra do módulo de anti-vírus para os e-mails que vierem de um determinado domínio, sendo que esta regra somente será aplicada a um grupo específico de usuários.

7.10. DOS RELATÓRIOS

7.10.1. Deve permitir a geração de relatórios de todos os appliances de um cluster de forma centralizada através de uma única interface web no console de gerenciamento;

7.10.2. Deve ser capaz de gerar relatórios gráficos e agendar o envio dos mesmos a usuários específicos via e-mail;

7.10.3. Permitir a seleção de dados para a formulação de relatórios por data ou por um intervalo de tempo específico;

7.10.4. Deve permitir a configuração de um período para a retenção de dados para a formulação de relatórios;

7.10.5. Capacidade de criar relatórios globais e por domínio contendo no mínimo as seguintes informações:

7.10.5.1. Sumário de mensagens;

7.10.5.2. Quantidade de mensagens processadas;

7.10.5.3. Principais origens de spam por domínio, endereço de e-mail;

7.10.5.4. Principais destinos de spam por domínio, endereço de e-mail;

7.10.5.5. Principais origens de vírus;

7.10.5.6. Principais fontes de ataque;

7.10.5.7. Estatísticas da quarentena;

7.10.5.8. Conexões completadas X bloqueadas;

7.10.5.9. Relatório de tráfego;

7.10.5.10. Principais destinatários de Spam

7.10.5.11. Principais destinatários de e-mail;

7.10.5.12. TOP Attachments;

7.10.5.13. TOP SPF Violations;

7.10.5.14. TOP Ataques por fraude de email / tentativa de spoof;

7.10.6. Permitir filtros de relatórios com definição de origem e destinos específico;

7.10.7. Possuir relatórios estatísticos de conexões, ameaças, quarentena, SPAM;

7.10.8. Deve apresentar estatísticas e monitoramento em tempo real (online) de e-mails com base em gráficos;

7.10.9. Capacidade de remoção automática das mensagens em quarentena de acordo com as configurações definidas pelo administrador do sistema;

7.10.10. Os relatórios no mínimo devem poder ser filtrados por:

7.10.10.1. Período de tempo;

7.10.10.2. Ponto de Filtragem que o email passou;

7.10.10.3. De;

7.10.10.4. Para;

7.10.10.5. Qual a classificação que a mensagem atingiu, dentre eles no mínimo:

7.10.10.5.1. DLP;

7.10.10.5.2. Provável SPAM;

7.10.10.5.3. SPAM;

7.10.10.5.4. Vírus;

7.10.10.5.5. Conteúdo Bloqueado;

7.10.10.5.6. Whitelist;

7.10.10.5.7. Blacklist;

7.10.10.5.8. Tamanho Excedido;

7.10.10.5.9. Phishing.

7.10.10.6. Relatório para um único usuário ou Domínio.

7.10.11. Para evitar agendamento de múltiplos relatórios, dessa forma consumindo recursos desnecessários do sistema, o appliance deve possuir um sistema de relatório integrado e com isso, em um único relatório agendado agrupa-se no mínimo os seguintes os relatórios:

7.10.11.1. Relatório de Volume de Mensagens por Data;

7.10.11.2. Relatório dos Principais Destinatários de SPAM;

7.10.11.3. Relatório dos Principais Remetentes de SPAM;

7.10.11.4. Relatório de Top E-mail Relays;

7.10.11.5. Relatório de Top Remetentes por Quantidade;

7.10.11.6 .Relatório de Top Remetentes por Volume;

7.10.11.7. Relatório de Top Destinatário por Quantidade;

7.10.11.8. Relatório de Top Destinatário por Volume;

7.10.11.9. Relatório de Vírus;

7.10.11.10. Relatório de Estatísticas da Quarentena.

7.11. DO RASTREAMENTO DAS MENSAGENS

7.11.1 Permitir o rastreamento de mensagens, independente de qual equipamento do cluster processou, de forma centralizada e por meio da interface de gerenciamento HTTPS (não será aceito pesquisa via linha de comando);

7.11.2 O rastreamento deve ser possível através de qualquer um dos seguintes campos:

7.11.2.1 ID da mensagem;

7.11.2.2 Email do Remente;

7.11.2.3 Email do Destinatário;

7.11.2.4 Domínio do Remetente;

7.11.2.5 Domínio do Destinatário;

7.11.2.6 Assunto da mensagem;

7.11.2.7 Nome do anexo;

7.11.2.8 Palavra contida no conteúdo do corpo da mensagem;

7.11.2.9 IP de Origem da mensagem;

7.11.2.10 Tamanho da mensagem;

7.11.2.11 Regra de SPAM;

7.11.2.12 Regra de DLP;

7.11.2.13 Se a mensagem foi entregue ou não;

7.11.2.14 Regras personalizadas aplicadas na mensagem;

7.11.2.15 Nome da ameaça encontrada.

7.11.3. A console deve apresentar ainda as seguintes características de rastreamento de mensagens:

7.11.3.1. Rastreamento completo de mensagens aceitas, retidas e rejeitadas, desde o recebimento da mensagem pelo IP cliente até a entrega para o IP destino, usando como filtro o assunto, o remetente, o destinatário, regra de bloqueio, conteúdo do corpo da mensagem, data, status, hora de entrega da mensagem permitindo a concatenação dos filtros através dos operadores lógicos “e” e “ou”;

7.11.3.2. O rastreamento deve ser a partir de uma única interface de gerenciamento independente de qual appliance filtrou a mensagem, não sendo aceito pesquisa via linha de comando;

7.11.3.3. O rastreamento deverá ter a opção de ser efetuado de todos os pontos de filtragem, sem a obrigatoriedade de separação de um único ponto de filtragem por vez;

7.11.3.4. Deve apresentar como resultado as seguintes informações:

7.11.3.4.1. Remetente da mensagem;

7.11.3.4.2. Destinatários da mensagem;

7.11.3.4.3. Servidor de origem;

7.11.3.4.4. Se foi armazenada em quarentena;

7.11.3.4.5. Se continha vírus

7.11.3.4.6. A regra que atuou;

7.11.3.4.7. O servidor de origem;

7.11.3.4.8. O tamanho da mensagem;

7.11.3.4.9. Se foi entregue ou não;

7.11.3.4.10. Qual ponto de filtragem utilizado (qual appliance processou a mensagem);

7.11.3.5. No caso de a mensagem ter sido entregue, deve ser possível a apresentação do log de entrega da mesma e para qual IP entregue;

7.11.3.6. Se o email tiver sido bloqueado por ser considerado spam ou possível spam, deve apresentar os filtros aplicados, bem como a pontuação apresentada por cada filtro e explicação do que representa o filtro aplicado (para facilidade do entendimento do administrador);

7.11.3.7. Deve ser capaz de visualizar a fila de e-mails em tempo real, bem como o sentido do email na fila (se é fila de entrada de email ou saída de email), indicando total de emails na fila de saída, total de emails na fila de entrada e total de emails com erros na entrega;

7.11.3.8. Rastrear emails à partir de uma determinada ameaça.

7.11.3.9. Apresentar na interface gráfica as fontes de ataque e através delas, apresentar quais emails recebidos, originários dessa fonte de ataque;

7.11.3.10. Apresentar em mapa geográfico da localização das fontes de ataque.

7.12. DA PROTEÇÃO CONTRA ATAQUES

7.12.1. A solução deve ser capaz de bloquear ataques de negação de serviço (Denial of Service);

7.12.2. Ser uma solução MTA (Mail Transfer Agent) completa suportando o protocolo SMTP, e com Suporte a envio e recebimento de e-mails criptografados utilizando o protocolo TLS/ SSL, permitindo configurar domínios onde o TLS é mandatório;

7.12.3. A solução deverá possuir a capacidade de executar as seguintes ações:

7.12.3.1. Limitar o número de conexões TCP permitidas através de um valor configurável;

7.12.3.2. Rejeitar a conexão SMTP que se caracterize como "flooding";

7.12.4. Deve ser capaz de efetuar a filtragem do trafego de correio eletrônico bloqueando a entrada de:

7.12.4.1. Vírus;

7.12.4.2. Spyware;

7.12.4.3. Worms;

7.12.4.4. Trojans;

7.12.4.5. Spam;

7.12.4.6. Phishing;

7.12.4.7. e-mail Marketing, ou qualquer outra forma de ameaça virtual;

7.12.5. Deve possuir controle total da comunicação permitindo restringir:

7.12.5.1. IP reverso mal configurado;

7.12.5.2. Domínios inexistentes;

7.12.5.3. Permitir identificar e bloquear e-mails vindos de domínios recentemente cadastrados;

7.12.5.4. Enforce RFC821;

7.12.6. Deve permitir ao administrador criar filtros e assinaturas, bem como realizar atualização automática das mesmas, em frequência de consulta configurada pelo administrador. A frequência de atualização desta consulta deve ser de no mínimo 15 minutos, sem necessidade de interrupção do serviço;

7.12.7. A solução deve ser capaz de filtrar contra vírus as mensagens tanto de entrada quanto de saída de e-mails;

7.12.8. Permitir criação de políticas diferenciadas para tratamento de spam, vírus e filtragem de conteúdo, de acordo com o destinatário da mensagem;

7.12.9. Permitir configurar ações diferenciadas sobre as mensagens suspeitas, incluindo:

7.12.9.1. Aceitar;

7.12.9.2. Colocar em quarentena;

7.12.9.3. Inserir tag personalizada no assunto;

7.12.9.4. Marcar o cabeçalho;

7.12.10. A solução deve ser capaz de tomar as seguintes ações sobre as mensagens:

7.12.10.1. Alterar o assunto da mensagem;

7.12.10.2. Adicionar cabeçalhos para rastreamento;

7.12.10.3. Descartar a mensagem;

7.12.10.4. Colocar em uma determinada área de quarentena definida pelo administrador;

7.12.11. Deve permitir também a criação de regras baseadas no idioma que as mensagens foram escritas, com capacidade de identificar no mínimo, português, e Inglês , ou a aplicação de regras por país;

7.12.12. Possuir a capacidade de criar filtros personalizados usando expressões regulares;

7.12.13. Permitir criação de listas negras e listas brancas, com opção por domínio, subdomínio, endereço de e-mail e endereço IP;

7.12.14. Deve prover um mecanismo que impeça a sua utilização como retransmissor de mensagens originadas externamente (relay);

7.12.15. Capacidade de limitar o número máximo de mensagens enviadas por remetente a cada hora, com opção de bloqueio automático do remetente, caso esse limite seja excedido.

7.12.16. Permite criar regras customizáveis contra spammers, possibilitando um controle avançado em todo conteúdo do e-mail efetuando buscas por Expressões Regulares presentes em todo conteúdo do e-mail (SMTP HEADER, BODY, URL, ANEXOS), sendo possível criar regras compostas utilizando os operadores lógicos “E” e “OU”;

7.12.17. O fabricante da solução deve possuir seu próprio sistema de reputação (RBL), integrado à solução, com a possibilidade do administrador reportar um possível spammer. Esta consulta deve retornar os dados do remetente, com informações referentes à:

7.12.17.1. Infraestrutura de rede;

7.12.17.2. Registro em blacklists mundiais;

7.12.17.3. Configuração de serviço de notificação de envio e autenticidade de mensagens de mensagens como SPF e DKIM.

7.12.18. Capacidade de efetuar consultas externas para análise de endereço IP do remetente quanto a sua reputação, bem como verificação de Spams e phishings recebidos e outros tipos de ameaças;

7.12.19. Deve ser capaz de realizar Reverse DNS LookUp (rDNS), para validação de fontes de email;

7.12.20. Deve possuir suporte ao bloqueio de conexões de e-mails nocivos antes do diálogo SMTP, permitindo a economia de banda, armazenamento e otimização de processamento do appliance, em especial baseado em lista local de bloqueio, RBLs e SPF;

7.12.21. Deve permitir que o administrador do sistema cadastre novas RBL’s para serem utilizadas a nível de conexão SMTP;

7.12.22. Possibilidade de restringir o processamento de mensagens (relay) endereço IP;

7.12.23. Deve ter capacidade de proteção a spoofing de email (tanto Spoofing de emails na entrada – quando o hacker utiliza o domínio do órgão como remetente, como Spoofing de emails na saída – quando tem algum email de saída que não esteja com o domínio do órgão como remetente), já incrementado na solução, bastando o administrador ativar a regra, sem necessidade de customizar uma regra para isso;

7.12.24. Possuir capacidade de criar cotas de envio e recebimento de e-mails em um prazo determinado de tempo, limitando o fluxo e prevenindo ataque do tipo DOS ou distribuição de spam através de um computador infectado na rede interna;

7.12.25. Possuir mecanismo de “Engargalamento de Email” (Spam Throttling) permitindo ao administrador limitar o fluxo de mensagens recebidas de origens com baixa reputação;

7.12.26. Deve ser capaz de limitar o fluxo de mensagens automaticamente, de acordo com o volume de mensagens indevidas recebidas de um determinado IP de origem;

7.12.27. Possuir funcionalidade de verificação de DMARC (Domain-based Message Authentication Reporting & Conformance);

7.12.28. Possuir controle de surtos, penalizando o remetente por um tempo configurável pelo administrador ao detectar:

7.12.28.1. Número excessivo de spams (configurado pelo administrador) oriundos de uma mesma fonte de email;

7.12.28.2. Número excessivo de vírus (configurado pelo administrador) oriundos de uma mesma fonte de email;

7.12.28.3. Número excessivo de ataques de dicionário (configurado pelo administrador) oriundos de uma mesma fonte de email;

7.12.29. Deve possuir apresentação de ameaças detectadas em tempo real. Nesse sistema de detecção de ameaças em tempo real, deve ser possível identificar:

7.12.29.1. Fontes de ataque;

7.12.29.2. Ameaças encontradas;

7.12.29.3. Ameaças Identificadas.

7.13. DA PROTEÇÃO CONTRA SPAM E PHISHING

7.13.1. Possuir filtro de anti-spam para detecção de spams usando no mínimo as seguintes tecnologias:

7.13.1.1. FingerPrint: Filtro por assinatura de spam;

7.13.1.2. Análise Heurística: Análise completa de toda mensagem contra spam, de acordo com as características da mensagem;

7.13.1.3. Análise de Documentos: Análise de documentos anexados na mensagem (PDF, DOC, DOCX e TXT);

7.13.1.4. Análise de Imagens: Filtragem de spam em imagens;

7.13.1.5. Filtro de URL: Filtragem por URL mal-intencionada contidas na no corpo da mensagem, dessa forma combatendo possível e-mail Phishing;

7.13.2. Filtro de URL com Categorização – Permitir ao administrador definir através de categorias, com no mínimo 10 categorias, divididas por assunto, possibilitando ao administrador definir uma pontuação. Categorias mínimas contidas na solução:

7.13.2.1. Conteúdo pornográfico;

7.13.2.2. Abuso infantil;

7.13.2.3. Redes sociais;

7.13.2.4. Racismo e ódio;

7.13.2.5. Pesquisa de empregos;

7.13.2.6. Streaming de áudio;

7.13.2.7. Streaming de vídeo;

7.13.2.8. Esportes;

7.13.2.9. Notícias;

7.13.2.10. Compras On Line;

7.13.3. Deve possuir tecnologia capaz de avaliar um link recebido em um e-mail, mesmo que escondido em um e-mail HTML e assim verificar o caminho para o qual este link está apontando, efetuando a verificação se nesta página apontada pelo link há algum formulário de solicitação de senha, usuário e outras ameaças, efetuando o bloqueio da mensagem sem a necessidade de assinatura, tornando assim a proteção mais proativa no combate a phishing;

7.13.4. Deve possuir tecnologia capaz de avaliar um link "URL" recebido em um e-mail, mesmo que escondido em um e-mail HTML e assim verificar o caminho para o qual este link está apontando, efetuando a verificação se este link encaminha para um sistema que efetua um redirecionamento automático para download de um arquivos (Tipo Zip, EXE, RAR, etc), na tentativa de enganar o usuário , efetuando o bloqueio da mensagem sem a necessidade de assinatura, tornando assim a proteção mais proativa no combate a phishing;

7.13.5. Deve permitir que o administrador cadastre novas RBL's a serem utilizadas a nível de cálculo de SPAM. O administrador deverá ter a autonomia para selecionar quais RBL's serão utilizadas a nível de conexão SMTP e quais serão utilizadas a nível de cálculo de SPAM;

7.13.6. Possuir no mínimo as seguintes tecnologias para prevenção e bloqueio de spam:

7.13.6.1. Recurso de Grey List;

7.13.6.2. Recurso de checagem por SPF (Sender Policy Framework) permitindo a criação de regras individuais e customizadas para usuários ou grupos, permitindo criar ações específicas para "fail" e "soft fail", conforme descrito pelo Comitê Gestor da Internet no Brasil em seu website oficial (HTTP://www.antispam.br/admin/spf);

7.13.6.3. Recurso de checagem por Sender ID;

7.13.6.4. Recurso de checagem por assinatura DKIM;

7.13.6.5. Recurso de checagem de DNS Reverso;

7.13.6.6. Checagem de validade de domínio através de verificação da configuração da zona do DNS do remetente;

7.13.6.7. Análise de reputação de IP;

7.13.6.8. Filtros de URL;

7.13.6.9. Filtro de anti-phishing;

7.13.6.10. Consulta de RBL´s (real-time blackhole list);

7.13.6.11. Filtro bayesiano utilizando tecnologia Bayes Databases;

7.13.7. Classificar a reputação de novas origens de spam com tecnologia de classificação dinâmica. O sistema de reputação deve utilizar dados de redes globais de monitoramento de tráfego web e de e-mail, não restringindo ao fluxo de mensagens do ambiente instalado;

7.13.8. Possuir a possibilidade de criação de regras personalizadas de filtragem baseadas em:

7.13.8.1. Origens das mensagens;

7.13.8.2. Destino das mensagens;

7.13.8.3. Domínios;

7.13.8.4. Endereços de e-mails;

7.13.8.5. Expressões regulares (dicionário de palavras);

7.13.8.6. Fluxo;

7.13.8.7. Quantidade de mensagens;

7.13.8.8. Tamanho de anexo;

7.13.8.9. Número máximo de destinatários em uma única mensagem;

7.13.8.10. Tipo de arquivos em anexo;

7.13.8.11. Extensões de arquivos em anexo, identificados por Mime-Type;

7.13.8.12. Anexos criptografados;

7.13.8.13. Anexos compactados;

7.13.8.14. Níveis de compactação dos arquivos anexos;

7.13.8.15. Quantidade de anexos na mensagem;

7.13.8.16. Conteúdo HTML no corpo da mensagem;

7.13.9. Possuir mecanismo de análise de conteúdo HTML no corpo da mensagem mensagens, permitindo ao administrador desarmar as tags HTML e bloquear as mensagens, possuindo no mínimo a identificação das seguintes Tags:

7.13.9.1. “<form>”;

7.13.9.2. “<script>”;

7.13.9.3. “<iframe>”;

7.13.10. Possibilidade de criar regras para ações a serem tomadas pela ferramenta, quando as mensagens forem consideradas Confiáveis e Spams permitindo ao administrador configurar nesses casos as seguintes ações:

7.13.10.1. Entregar direto o e-mail;

7.13.10.2. Colocar em quarentena;

7.13.10.3. Remover mensagem;

7.13.10.4. Auditar mensagem;

7.13.10.5. Encaminhar a mensagem;

7.13.10.6. Notificar o destinatário;

7.13.10.7. Adicionar header na mensagem;

7.13.10.8. Transformar HTML em texto simples;

7.13.11. Possuir sistema de detecção de ataque de diretórios (DHA – Directory Harvest Attack), capaz de recusar novas conexões SMTP de uma fonte emissora, caso ela tenha enviado, em um período de tempo, mensagens a usuários inválidos/inexistentes no domínio;

7.13.12. Deve permitir regras internas para aumentar ou diminuir a probabilidade de ser SPAM com base em critérios internos da contratante, permitindo definir no mínimo: país de origem, endereço de domínio e IP do remetente;

7.13.13. A solução deve permitir a utilização de quarentena por usuário, possibilitando que cada usuário cadastrado em um controlador de diretório:

7.13.13.1. Microsoft Active Directory;

7.13.13.2. LDAP;

Esteja integrado com a solução e administre suas próprias mensagens categorizadas como spam;

7.13.14. Deve permitir a aplicação de políticas de SPAM diferentes por nome de domínio, destinatário, grupo de destinatários e por destinatário específico, integrado aos sistemas de diretório LDAP e MS Active Directory;

7.13.15. Deve ter a capacidade de rejeitar mensagens para destinatários inválidos durante o dialogo SMTP (tratar Non-Delivery Report Attack);

7.13.16. Possuir proteção contra bounce email attack através “Bounce Address Tag Verification”;

7.13.17. Deve permitir a inclusão de múltiplas listas de remetentes bloqueados, permitindo regras de bloqueio se o IP estiver presente nestas listas;

7.13.18. Deve permitir que mensagens de Falso Negativo sejam reportadas através da interface gráfica para o laboratório do fabricante ou oferecer um caminho para que mensagens de falso negativo sejam reportadas diretamente ao laboratório do fabricante;

7.13.19. Deve possuir mecanismo que permita a adição de Cabeçalho de identificação da classificação das mensagens como SPAM, a fim de integrar com sistemas de correio eletrônicos tais como:

7.13.19.1. Microsoft Exchange;

7.13.19.2. Zimbra Collaboration Suite;

7.13.19.3. Lotus Domino e outros;

7.13.20. Deve possuir mecanismo de análise e detecção de imagens pornográficas e/ou nudez, permitindo ao administrador definir a sensibilidade da detecção e a criação de regras por usuários e/ou grupos de usuários e permitindo a tomada de ações de bloquear ou liberar a mensagem.

7.14. DA PROTEÇÃO CONTRA VÍRUS

7.14.1. Possuir módulo de verificação com suporte a dois ou mais mecanismos diferentes de antivírus, executando simultaneamente;

7.14.2. Deverá ser capaz de filtrar vírus nos dois sentidos de tráfego (entrada e saída de email);

7.14.3. Possuir módulo de detecção “Hora Zero” para a identificação de novas ameaças desconhecidas pelo antivírus, colocando em determinada área da quarentena por período de tempo, até nova verificação pelo antivírus.

7.14.4. Scan de arquivos compactados recursivamente, no mínimo, 5 (cinco) camadas, contemplando no mínimo, os seguintes compactadores: .rar, .zip, .tar, .arj, .cab, .lha, .exe, .lzh, .tgz e .gzip;

7.14.5. A solução deve possuir um motor antivírus e Antimalware do próprio fabricante da solução, ou um motor Antivírus e AntiMalware de terceiro já integrado a solução sem custo adicional;

7.14.6. Proteção contra Vírus, no mínimo com as tecnologias já licenciadas sem a necessidade de módulo adicional:

7.14.6.1. Dia-zero (zero-day);

7.14.6.2. Vírus outbreak;

7.14.6.3. Hora-zero (Zero-hour);

7.14.6.4. Targeted Attack protection;

7.14.7. Tomar no mínimo as seguintes ações:

7.14.7.1. Alterar o assunto da mensagem;

7.14.7.2. Adicionar cabeçalhos para rastreamento;

7.14.7.3. Descartar a mensagem;

7.14.7.4. Colocar em uma determinada área da quarentena definida pelo administrador;

7.14.7.5. Notificar o remetente e/ou destinatário com uma mensagem customizável, informando o nome do vírus;

7.14.8. Permitir quarentena automática de anexos criptografados;

7.14.9. Permitir criação de rota customizada para permitir entrada de anexos criptografados para entrega a determinados grupos de e-mails.

7.15. DAS NOTIFICAÇÕES DE QUARENTENA INDIVIDUAL DO USUÁRIO

7.15.1. A solução deverá permitir ao administrador agendar o envio do resumo das mensagens na quarentena individual do usuário (Digest) em períodos de tempo pré-configuráveis por horário e dia, possibilitando ações do usuário diretamente através dos comandos definidos neste Digest, dispensando a instalação de agentes e acesso a quarentena individual do usuário.

7.15.2. Grupos diferentes de usuários devem poder receber a notificação em horários diferentes.

7.15.3. O digest deve ser enviado em Língua portuguesa do Brasil, mas com a possibilidade de customização do texto, para todos os usuários ou para um determinado grupo de usuários;

7.15.4. Deve ser possível a customização do digest com as seguintes características alteráveis:

7.15.4.1. Email de origem;

7.15.4.2. Título/Assunto do email;

7.15.4.3. Mensagem do digest, com possibilidade de inclusão de imagens e links, bem como mudança de fonte, alinhamento e cor;

7.15.4.4. Logomarca do digest;

7.15.5. O digest deve permitir ao usuário final tomar no mínimo as ações de:

7.15.5.1. Liberar uma mensagem bloqueada;

7.15.5.2. Bloquear o remetente da mensagem (blacklist), para que as futuras mensagens do mesmo já sejam barradas;

7.15.5.3. Marcar o remetente como confiável (whitelist), para que as futuras mensagens do mesmo não sejam pontuadas como spam;

7.15.5.4. Reportar o bloqueio indevido;

7.15.5.5. Solicitar envio de novo resumo;

7.15.5.6. Acessar sua área de quarentena;

7.15.6. Deve permitir que o administrador escolha qual quarentena a ser incluída no Digest do usuário final, por exemplo incluir no Digest os e-mails quarentenados que foram considerados conteúdos maliciosos (VÍRUS).

7.16. DO DISCLAIMER

7.16.1. Capacidade de incluir “disclaimers” nas mensagens enviadas;

7.16.2. A solução deverá suportar aplicação de “disclaimers” diferenciados para usuários e grupos diferentes através da integração com o serviço de diretório LDAP;

7.16.3. A solução deverá suportar a configuração dos “disclaimers” em formato html e texto.

7.17. DA PREVENÇÃO A ROUBO DE INFORMAÇÕES (DLP) E COMPLIANCE

7.17.1. Deve possuir módulo DLP (Data Loss Prevention), já integrado na solução sem a necessidade de licenciamento adicional ou outro appliance;

7.17.2. O módulo de DLP deve analisar todo conteúdo da mensagem a fim garantir a confiabilidade das mensagens que saem da empresa, permitindo ao administrador configurar diversas

ações a fim de restringir, controlar ou auditar as mensagens e informações sensíveis da empresa;

7.17.3. Deve permitir criar regras de compliance “Auditoria/Aderência” através de filtros avançados de análise da mensagem, permitindo identificar através de Dicionários (Conjunto de Palavras e Expressões Regulares) personalizados pelo administrador ou já existentes na ferramenta, dentre eles:

7.17.3.1. Identificação de CPF;

7.17.3.2. Número de cartão de crédito;

7.17.3.3. CNPJ;

7.17.4. Deve permitir a busca a partir dos dicionários de palavras dentro dos arquivos em anexo nos e-mails com suporte a no mínimo aos formatos .doc, .xls, .ppt, .pdf;

7.17.5. As regras de compliance podem ser criadas utilizando os Dicionários definidos nos seguintes campos da mensagem, podendo ser definido o número de ocorrências mínimas para execução da regra:

7.17.5.1. Cabeçalho;

7.17.5.2. URL (contidas no e-mail);

7.17.5.3. Corpo do email;

7.17.5.4. Anexos e documentos no mínimo: .DOC, .DOCX, .XLS, .XLSX, .PDF, .PPT, .PPTX e .TXT;

7.17.6. Permitir ao administrador criar regras de compliance para arquivos criptografados, possibilitando ao administrador configurar a ação a ser tomada quando um anexo criptografado é identificado. A ferramenta deve ter no mínimo três algoritmos de detecção: Mecanismo Heurístico, Myme-Type e Extensão;

7.17.7. Todos os itens do DLP devem permitir configurações através de regras que permitam ao administrador definir, no mínimo, as seguintes ações:

7.17.7.1. Entregar a mensagem;

7.17.7.2. Não entregar a mensagem;

7.17.7.3. Armazenar a mensagem para auditoria;

7.17.7.4. Notificar remetente e destinatário da mensagem;

7.17.7.5. Encaminhar a mensagem para outro destinatário;

7.17.8. Todos os itens do DLP devem permitir configurações que permitam ao administrador criar regras complexas através de operadores lógicos “E” e “OU”;

7.17.9. Deve permitir ao administrador gerar notificação (se assim desejar) ao remetente do email, indicando que o email enviado não condiz com as normas da empresa. Essa notificação poderá ser customizada de acordo com a necessidade do administrador.

7.18. DA CRIPTOGRAFIA DE E-MAIL

7.18.1. Deve possuir módulo de criptografia do próprio fabricante, já integrado na solução sem a necessidade de licenciamento adicional ou outro appliance.

7.18.2. A criptografia deve atuar na saída de e-mails que trabalhe de maneira transparente ao usuário final, sem a necessidade de plugins, agentes ou outro tipo de software e com uma interface para o destinatário das mensagens, customizável pelo administrador;

7.18.3. A console de gerenciamento do módulo de criptografia deve ser a mesma para toda a solução, não exigindo console de administração adicional;

7.18.4. Deve possibilitar ao administrador, definir quais mensagens serão criptografadas com base em no mínimo:

7.18.4.1. Assunto;

7.18.4.2. Destinatário;

7.18.4.3. Email do Remetente;

7.18.4.4. Nome do Anexo;

7.18.5. A criptografia das mensagens deve utilizar sistema de chaves gerada de forma independente;

7.18.6. Deve impossibilitar o uso de Cache de Browser para acesso as mensagens criptografadas;

7.18.7. Deve possibilitar ao administrador a indicação do tempo de expiração da mensagem criptografada;

7.18.8. Deve possibilitar ao administrador indicar se o destinatário poderá responder o email;

7.18.9. Deve possibilitar ao administrador indicar se o destinatário poderá encaminhar o email.

7.19 DO SISTEMA DE PROTEÇÃO CONTRA ATAQUES DIRIGIDOS (TARGETED ATTACK PROTECTION – TAP)

7.19.1. Deverá prover proteção contra ataques dirigidos tais como:

7.19.1.1. Spear-phishing;

7.19.1.2. Ataques Zero-Day;

7.19.1.3. Ameaças avançadas persistentes (APTs);

7.19.2. Deve possuir técnica para construção de modelos estatísticos com Big Data;

7.19.3. Deve possuir no mínimo 3 (três) camadas de proteção sendo elas:

7.19.3.1. Verificação da lista de códigos maliciosos: Verificação de campanhas de e-mails emergentes e conhecimento de novos sites maliciosos;

7.19.3.2. Análise de código: Verificação de comportamento suspeito, scripts escondidos, partes de códigos maliciosos e redirecionamento a outros sites maliciosos;

7.19.3.3. Análise Dinâmica: Utilização de “Sandbox” para simular a máquina de um usuário real e observar as alterações efetuadas no sistema;

7.19.4. Possuir acesso ao Dashboard do módulo de Segurança contra-ataques dirigidos;

7.19.5. O sistema de proteção contra-ataques dirigidos deve executar no mínimo 3 (três) etapas:

7.19.5.1. Detecção - A análise de email deve verificar variáveis em tempo real incluindo as propriedades da mensagem, bem como, o histórico de e-mail do destinatário para identificar anomalias que indiquem uma ameaça potencial;

7.19.5.2. Proteção - Deve assegurar que links para URLs suspeitas são dinamicamente reescritas antes que o e-mail seja entregue ao destinatário. Cada vez que um usuário clica em um destes links esteja ele na empresa ou em um local remoto o serviço verifica se o destino é seguro;

7.19.5.3. Ação - Deve demonstrar aos administradores e gestores de segurança em tempo real e de forma interativa uma visão dos ataques sofridos e das ameaças que posam

sofrer, passando para usuários específicos, dispondo de ferramentas para ajudar a remediar danos, tudo baseado em um painel de controle on-line;

7.19.6. Não será aceita solução baseada apenas em reputação de URL.

7.19.7. A solução deve conter engine para detecção de Anomalias, não podendo se limitar a analise com definições baseadas em ataques já conhecidos.

7.19.8. A solução deve ser proativa e ter capacidade de detecção por heurística, utilizando técnicas de análise de grande volume de dados, desta forma definindo um modelo de padrão de mensagens da corporação, levando em conta remetentes, destinatários, volume de mensagens e vários outros fatores, dessa forma modelando os e-mails “Normais” da corporação e barrando “Anomalias”, fazendo essa análise e definição de padrão por caixa postal.

7.19.9. Deve ser possível habilitar ou desabilitar a proteção URL baseada em rotas especificas configuradas no mínimo pelas seguintes condições:

7.19.9.1 Email do Destinatário;

7.19.9.2. Email do Remetente;

7.19.9.3. Domínio de Origem;

7.19.9.4. Domínio de Destino;

7.19.9.5. IP/Rede;

7.19.9.6. Range de IP;

7.19.9.7. Expressão Regular;

7.19.9.8. Usuários;

7.19.9.9. Listas de distribuição;

7.19.9.10. Grupo de LDAP;

7.19.10. A proteção de URL deverá reescrever os links do e-mail e a cada clique o sistema deverá analisar a URL e somente depois de passar por todos os testes, sendo constatado que não é malicioso, deve redirecionar para a URL original. Se após a análise for constatado site malicioso, o sistema deverá exibir mensagem de alerta e o site será bloqueado no navegador;

7.19.11. O sistema deverá ser capaz varrer anexos no mínimo nas extensões PDF, Microsoft Office, arquivos em Flash para payloads maliciosos, Microsoft Office com as seguintes extensões a serem verificadas:

7.19.11.1. .swf;

7.19.11.2. .pdf;

7.19.11.3. .doc;

7.19.11.4. .xls;

7.19.11.5. .xlsx;

7.19.11.6. .ppt;

7.19.11.7. .ppt;

7.19.11.8. .pptx;

7.19.11.9. .rtf;

7.19.12. A solução deverá dispor de Dashboard alertando aos administradores de ataques por e-mail e deverá fornecer detalhes sobre o ataque direcionado, fará triagem para reduzir potenciais danos, reportando ao fabricante criando relatórios detalhados para o departamento de segurança e executivo;

7.19.13. Deverá ser capaz de efetuar a verificação da reputação de anexos e caso a reputação do anexo não conste no banco de dados, a solução deverá ter a opção de enviar automaticamente o anexo para a nuvem do fabricante para análise em tempo real em sistema de Sandbox do próprio fabricante. Este sistema de Sandbox deve conter tecnologia de detecção usando "Analise Comportamental" do arquivo identificando assim malwares e variantes sem a necessidade de assinaturas;

7.19.14. Deve possuir tecnologia SandBox local, isto é, efetuar o SandBox sem enviar o arquivo ao fabricante ou a terceiros, efetuando toda a análise de anexos dos emails localmente, atendendo dessa forma a legislação vigente brasileira (Lei Geral de Proteção de Dados Pessoais).

7.19.15. 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 e os usuários que ignoraram através do Dashboard;

7.19.16. A proteção URL deverá reescrever links para os protocolos HTTP, HTTPS e FPT, URL's que comecem com "www" independente do protocolo;

7.19.17. A solução deverá permitir que o administrador configure o sistema de proteção URL reescrevendo todas as mensagens que contiverem URL e enviado ao sandbox para testes garantindo um alto nível de segurança;

7.19.18. A solução deverá prover lista de exceções de URL para que não sejam reescritas;

7.19.19. O Dashboard deverá exibir o número de cliques em cada ameaça;

7.19.20. O Dashboard deverá exibir qual usuário clicou na URL detectada como ameaça;

7.19.21. O Dashboard deverá exibir informações atualizadas sobre as ameaças detectadas, deverá exibir a classificação da mensagem e deverá exibir status atualizado e detalhado sobre as ameaça no mínimo com as seguintes informações:

7.19.21.1. Clicado – Número de vezes que uma URL reescrita foi clicada por um usuário, inclusive se a mensagem for encaminhada para outro usuário e também for clicada.

7.19.21.2. Bloqueado - Número de vezes que o modulo de Proteção URL impediu o usuário de acessar o site malicioso.

7.19.21.3. Permitida – Número de vezes que o modulo de proteção URL permitiu ao usuário acessar o site original da URL reescrita e que não foi detectada como maliciosa.

7.19.22. O Dashboard deverá exibir timeline das ameaças, exibindo quando foi recebida, identificada e quando foi clicada ou liberada;

7.19.23. No Dashboard deverá ser possível filtrar uma URL em um campo de busca para analisar todas as ocorrências com aquela URL, bem como verificar o status atual dela e preview da página web;

7.19.24. O Dashboard deverá possuir ferramenta para bloqueio ou liberação de URL pelo administrador da ferramenta;

7.19.25. No Dashboard deverá ser possível filtrar um IP em um campo de busca para analisar todas as ocorrências com aquele IP, bem como verificar o status atual dele e preview da página web;

7.19.26. O Dashboard deverá disponibilizar sistema de coleta (report) de amostra do IP para a engenharia do fabricante analisar;

7.19.27. O Dashboard deverá possuir ferramenta para bloqueio ou liberação do IP pelo administrador da ferramenta;

7.19.28. No Dashboard deverá ser possível analisar um arquivo, sendo enviado pelo administrador como amostra e retornar todas as ocorrências do arquivo enviado;

7.19.29. O Dashboard deverá possuir ferramenta para bloqueio ou liberação do arquivo pelo administrador da ferramenta;

7.19.30. A ferramenta de segurança contra ataques dirigidos, deve possuir o sistema colaborativo, ao qual o administrador poderá configurar que o usuário final possa indicar liberação e bloqueio de URL's, mesmo analisados pelo sistema e dessa forma reportando falsos positivos e falsos negativos. Deve prover também um Dashboard onde o Administrador poderá verificar todos reportes enviados pelos usuários, ficando a cargo do administrador decidir pelo bloqueio ou a liberação de tal URL e/ou Arquivo.

7.19.31. Deve possuir módulo de CDR "Content Disarm and Reconstruction", que quando ativado irá remover conteúdos possivelmente perigoso, em no mínimo para os seguintes tipos:

7.19.31.1. JavaScript;

7.19.31.2. Links;

7.19.31.3. Executáveis;

7.19.31.4. VB Script;,

7.19.31.5. De dentro de documentos, em no mínimo para os seguintes tipos:

7.19.31.5.1. PDF;

7.19.31.5.2. DOC;

7.19.31.5.3. DOCX;

7.19.31.5.4. PPT;

7.19.31.5.5. PPTX;

7.19.31.5.6. XLS;

7.19.31.5.7. XLSX;

7.19.32. Deve possuir capacidade de ignorar reescrita de algumas URL's e não envio de arquivos para análise no SandBox do fabricante;

7.19.33. O SandBox do fabricante deve ter a capacidade de analisar arquivos do tipo:

7.19.33.1. .swf;

7.19.33.2. .pdf;

7.19.33.3. .doc;

7.19.33.4. .xls;

7.19.33.5. .xlsx;

7.19.33.6. .ppt;

7.19.33.7. .ppt;

7.19.33.8. .pptx;

7.19.33.9. .rtf;

7.19.34. Deve ter a opção de não fazer reescrita de URL's em casos de mensagens criptografadas, no mínimo com os sistemas de criptografia:

7.19.34.1. PGP;

7.19.34.2. S/MIME;

7.19.34.3. DKIM;

7.19.35. Deve ter a opção de não fazer reescrita de URL's em casos de mensagens oriundas de determinados países, por exemplo: Mensagens oriundas da China, Austrália e Belize;

7.19.36. Deve poder desativar a reescrita de URL's se a mensagem atingir uma pontuação de mínima de SPAM definida pelo administrador;

7.19.37. Possibilidade do administrador de incluir URL's, arquivos e IP's em uma lista de bloqueio (Blacklist) no sistema de TAP;

7.19.38. Possibilidade do administrador de incluir URL's, arquivos e IP's em uma lista segura (Whitelist) no sistema de TAP.

7.20. DO SISTEMA DE PROTEÇÃO A FRAUDES DE E-MAIL:

7.20.1. A solução deverá ter a capacidade de detectar domínios recém adquiridos (tempo de considerado como recém adquirido deverá ser configurável pelo administrador) e indicar o que deve ser feito neste caso:

7.20.1.1. Pontuar;

7.20.1.2. Ignorar;

7.20.1.3. Bloquear.

7.20.2. Deve possuir capacidade de detecção de Spoofing de emails externos, isto é, ter a capacidade de comparar o domínio do cabeçalho do email (Header do Email/Envelope SMTP), com o domínio apresentado como remetente para o usuário final (Cabeçalho From) e indicar o que deve ser feito se forem diferentes:

7.20.2.1. Pontuar;

7.20.2.2. Ignorar;

7.20.2.3. Bloquear.

7.20.3. O sistema deve possuir a opção de configurar regras para detectar emails que estejam utilizando ataques do tipo Look-A-Like Domain, isto é, detectar emails com domínios similares aos domínios utilizados pelo órgão.

7.20.4. Deve possuir sistema de detecção de emails oriundos de servidores de emails gratuitos (free emails), tais como Google, Yahoo, Hotmail, etc.

7.20.5. Nativamente deve possuir sistema de detecção de emails externos (emails de entrada) que tentem utilizar o(s) domínio(s) da própria empresa como remetente, sem necessidade de criação de regra específica para este tipo de fraude.

7.21 DO TREINAMENTO

7.21.1. A capacitação deverá ser fornecida em turma de no mínimo 05 (cinco) colaboradores da área de tecnologia da CONTRATANTE;

7.21.2. O treinamento deverá ser realizado presencialmente, em infraestrutura disponibilizada pela CONTRATANTE e deverá possuir carga horária mínima de 24 (vinte e quatro) horas;

7.21.3. A capacitação deverá consistir em treinamento oficial em acordo com as políticas do fabricante da solução fornecida;

7.21.4. Deverá ser ministrado por instrutor certificado na solução;

7.21.5. Os softwares, materiais, apostilas, profissionais, instrutores e todos os requisitos necessários à realização adequada do treinamento são de responsabilidade exclusiva da CONTRATADA.

7.21.5.1. Uma cópia do material do treinamento deverá ser enviada com antecedência mínima de 15 (quinze) dias da data de início do treinamento à CONTRATANTE, para análise e aprovação.

7.21.5.2. O material não aprovado pelo Contratante deverá ser refeito pela CONTRATADA e novamente aprovado.

7.21.6. O treinamento deverá ser ministrado em português e composto de aulas teóricas e práticas (Hands On).

7.21.7. O treinamento deverá abordar todas as funcionalidades da solução de gateway de segurança de e-mail ofertada, bem como a instalação, configuração, administração, operação, otimização, automatização de tarefas, metodologia de diagnóstico e resolução de problemas (troubleshooting), geração de relatórios, cópia de segurança (backup) e restauração, controle de acesso, auditoria e gerenciamento de logs;

7.21.8. Todas as despesas com passagens, hospedagens e alimentação dos seus instrutores no período do treinamento ficarão a cargo da CONTRATADA.

7.21.9. Após a realização da capacitação, a empresa deverá fornecer certificado de conclusão para cada participante;

7.21.10. O cronograma para realização dos eventos será definido pela CONTRATANTE em conjunto com a CONTRATADA;

7.21.10.1. O treinamento deverá ser realizado no prazo máximo até 30 (trinta) dias corridos, após a assinatura do contrato.

7.21.11. Ao final do treinamento, deverá ser realizada junto aos participantes uma avaliação do curso por meio de formulário da CONTRATADA;

7.21.11.1. Caso o curso seja avaliado como insatisfatório pelos participantes da turma, treinamento deverá ser refeito, sem ônus adicional à CONTRATANTE, respeitando as condições elencadas neste Termo de Referência.

7.21.11.2. O cálculo para avaliação insatisfatória dar-se-á da seguinte forma: A média da avaliação do curso entre os participantes for ruim ou regular.

7.21.11.3.Os critérios da avaliação são medidos como segue:Ruim(1); Regular(2);Bom(3);Ótimo(4 ou 5).

7.21.12. A CONTRATADA deverá assegurar-se que os participantes do treinamento assinem ou confirmem diariamente lista de presença. A lista deverá ser entregue à CONTRATANTE;

7.22. DA IMPLANTAÇÃO

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

7.22.2. A implantação consiste em entregar a solução em plenas condições de uso (configurada e integrada com a solução de correio eletrônico utilizada pela CONTRATANTE);

7.22.3. Todas as customizações presentes na solução atual da CONTRATANTE devem ser migradas para a nova solução;

7.22.4. Também devem ser migradas as regras presentes de forma nativa na solução atual que forem consideradas importantes pela CONTRATANTE.

7.22.5. A instalação em alta disponibilidade e testes dos produtos devem estar inclusos no custo do produto;

7.22.5.1 A alta disponibilidade é caracterizada pela instalação de 2 (dois) ou mais nós de processamento, configurados em cluster;

7.22.5.2. Caberá à contratada enviar de forma prévia documento completo informando as regras de firewall necessárias para a implantação da solução, bem como documentação clara e inequívoca acerca dos dados que serão trafegados por meio destas regras; Havendo liberações para rede externa da contratante que não do próprio fluxo de e-mails, deve ser

fornecido um documento onde a contratada detalha e responsabiliza-se unica e exclusivamente pela segurança dos dados trafegados.

7.22.6. 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;

7.22.7. A CONTRATADA deverá executar uma série de testes funcionais básicos para verificar o perfeito funcionamento do ambiente. Estes testes deverão ser realizados nos componentes de hardware e software envolvidos no projeto;

7.22.7.1. A CONTRATADA deverá realizar Testes de falhas, redundância, backup e restore;

7.22.8 A CONTRATADA deverá prestar apoio na parametrização das ferramentas de monitoramento do ambiente, tais como Nagios e Zabbix;

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

7.22.10. Ao final do processo de implantação deve ser gerado um documento detalhando os passos realizados para instalação e configuração da solução;

7.23 DO SUPORTE TÉCNICO

7.23.1. O prazo de suporte técnico da solução ofertada deverá ser de, no mínimo, 12(doze) meses, contados a partir da data do aceite definitivo;

7.23.2. A CONTRATADA deve garantir para a CONTRATANTE o fornecimento de acesso irrestrito (24 horas x 7 dias da semana) à área de suporte do fabricante, especialmente ao endereço eletrônico (web site), a toda a documentação técnica pertinente (guias de instalação/configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).

7.23.3. As respostas do suporte técnico contratado deverão ser efetuadas na língua portuguesa (português do Brasil), tanto por email, quanto por contato telefônico.

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

7.23.5. A abertura de chamados pelo CONTRATANTE será efetuada por correio eletrônico, por sistema de controle de chamados, com email de resposta do chamado aberto apresentando o número do ticket aberto, para acompanhamento.

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

7.23.6.1. Os chamados de severidade ALTA (Quando há indisponibilidade de uso da solução) deverão ser atendidos em até 1 (uma) hora após a abertura e deverão ser solucionados em até 24 (vinte e quatro) horas, contados a partir da abertura do chamado;

7.23.6.2. 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 ser atendidos em até 4 (quatro) horas após a abertura e deverão ser solucionados em até 48 (quarenta e oito) horas, contados a partir da abertura do chamado;

7.23.6.3. Os chamados de severidade BAIXA (Nível de severidade aplicado para instalação, configuração, atualização de versões e implementações de novas funcionalidades) deverão ser atendidos em até 8 (oito) horas após a abertura e deverão ser solucionados em até 72 (setenta e duas) horas, contados a partir da abertura do chamado;

7.23.6.4. Os chamados de severidade INFORMATIVO (Nível informacional ou dúvidas) deverão ser atendidos em até 16 (dezesseis) horas após a abertura;

7.23.7. A CONTRATADA deverá possuir técnico especializado na solução, com no mínimo 1 (um) técnico certificado pelo fabricante e com certificação dentro da validade.

7.24. DAS ATUALIZAÇÕES

7.24.1. Automaticamente e sem custos adicionais, deverá ser possível o acesso ao conteúdo mais recente dos produtos, funcionalidades adicionais e correções de produtos disponibilizadas pelo fabricante;

7.24.2. Deve ser possível submeter pedidos para atualização de produtos;

7.24.3. As atualizações de versões e o serviço de suporte técnico da solução deverão ser Garantidos pela Contratada, por um período de 12(doze) meses, após a emissão de Termo de Recebimento Definitivo;

7.24.3.1. Para que as atualizações de versões estejam disponíveis durante toda a vigência do contrato, a contratada deverá estar credenciada e autorizada pelo fabricante.

7.24.3.2. A Contratante reserva o direito de, a qualquer momento, solicitar tais comprovações que se fizerem necessárias.

7.24.4. A contratada deverá, sem ônus adicional para o Contratante, fornecer as atualizações (“patches”) de segurança e de versão para os appliances que compõem a solução.

7.24.5. A solução deverá continuar a filtragem das mensagens em ambos os sentidos (inbound e outbound) mesmo após o término do licenciamento ou suporte.

7.25. DOS TESTES E HOMOLOGAÇÃO

7.25.1. Além da análise das informações fornecidas em documentação técnica pertinente, poderá ser realizado teste de homologação (Prova de Conceito) da solução nas instalações do contratante a fim de validar o atendimento aos requisitos básicos.

7.25.2. O teste de homologação poderá ser solicitado à licitante classificada em primeiro lugar que tiver os documentos previstos no Termo de Referência do Edital aprovados pela área técnica, podendo também ser solicitada aos demais licitantes.

7.25.3. O teste de homologação será conduzido pela contratante no local de suas instalações e tem como objetivo aferir a adequação do objeto às especificações constantes no Item 7 do Termo de referência.

7.25.4. A CONTRATADA convocado a realizar o Teste de Homologação terá o prazo de até 10 (dez) dias úteis, contados da data da convocação, para entregar uma amostra completa da solução ofertada contendo equipamentos (quando couber) acompanhado dos softwares e licenças necessárias ao seu funcionamento pelo período de 30 (trinta) dias corridos.

7.25.5. O Teste de Homologação deverá ser realizado sem custo para a CONTRATANTE pelo período de 30 (trinta) dias corridos, contados da data da entrega.

7.25.6. Estão incluídos no prazo de 30 (trinta) dias corridos a instalação, a configuração e a demonstração de que os produtos atendem às especificações constantes no Item 7 do Termo de referência.

8. DEVERES E RESPONSABILIDADES DO CONTRATANTE

8.1. Nomear Gestor do Contrato e Fiscais Técnico do contrato para acompanhar e fiscalizar a execução dos contratos;

8.2. Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

8.3. Efetuar conferência minuciosa dos serviços entregues, aprovando-os se for o caso;

8.4. Rejeitar os serviços que não atendam aos requisitos constantes das especificações contidas no Termo de Referência;

8.5. Acompanhar e fiscalizar a execução do contrato por meio de servidores designados;

8.6. O Gestor do Contrato do CONTRATANTE atestará as notas fiscais para fins de pagamento, comprovada a prestação correta dos serviços, com base na informação prestada pelos Fiscais Técnicos;

8.7. Notificar a CONTRATADA, por meio de ofício, e-mail ou sistema de controle de ocorrências, sobre imperfeições, falhas ou irregularidades constatadas na execução do serviço, para que sejam adotadas as medidas corretivas cabíveis;

8.8. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento dos serviços contratados;

8.9. Definir produtividade ou capacidade mínima de fornecimento das Soluções de Tecnologia da Informação e Comunicação por parte da CONTRATADA, com base em informações de mercado, quando aplicável;

8.10. Prestar à CONTRATADA, em tempo hábil, as informações eventualmente necessárias à execução do serviço;

8.11. Emitir, por intermédio da solução computacional de apoio à execução dos serviços, as correspondentes Ordens de Serviço (OS), contendo todas as informações necessárias para a prestação do serviço, objeto do presente Termo de Referência;

8.12. Acompanhar, controlar e avaliar a prestação de serviço, por intermédio do gestor e fiscal do contrato, especialmente quanto aos aspectos quantitativos e qualitativos, de acordo com os padrões de qualidade definidos;

8.13. Permitir, sob supervisão, que os funcionários da empresa CONTRATADA, desde que devidamente identificados e incluídos na relação de técnicos autorizados, tenham acesso às dependências do CONTRATANTE, onde o serviço será prestado, respeitando as normas que disciplinam a segurança da informação e o patrimônio;

8.14. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis;

8.15. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em Contrato;

8.16. Efetuar o pagamento devido pela execução dos serviços, no prazo estabelecido no presente Termo de Referência, desde que cumpridas todas as formalidades e exigências previstas.

9. DEVERES E RESPONSABILIDADES DA CONTRATADA

9.1. Deverá nomear e apresentar preposto para representá-la durante o período de vigência do contrato;

9.2. Deverá executar fielmente o objeto contratado, de acordo com as normas legais;

9.3. Dar integral cumprimento a sua proposta, a qual passa a integrar este instrumento, independentemente de transcrição;

9.4. Disponibilizar solução computacional de apoio à execução dos serviços conforme requisitos estabelecidos neste Termo de Referência;

9.5. Cumprir o prazo máximo de entrega, contados a partir da assinatura do instrumento contratual;

9.6. Responder por qualquer prejuízo causado à Administração ou a terceiros por seus empregados ou prepostos, no cumprimento e execução dos serviços, reparando os danos eventualmente causados;

9.7. Assumir inteira responsabilidade pelo fornecimento e entrega dos serviços contratados, não podendo transferi-los a outrem, no todo ou em parte, sem prévia e expressa anuência da CONTRATANTE;

9.8. Atender prontamente quaisquer orientações e exigências do Gestor e Fiscais do Contrato, inerentes à execução do objeto contratual;

9.9. Executar fielmente os serviços contratados de acordo com as exigências do Contrato Administrativo, do Termo de Referência, do Edital e dos e seus Anexos;

9.10. Responsabilizar-se e reparar quaisquer danos diretamente causados ao CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pelo CONTRATANTE. O valor do dano, após processo apurativo de responsabilidade, no qual será garantido o contraditório e a ampla defesa, poderá ser descontado do primeiro pagamento subsequente à finalização do processo;

9.11. Propiciar todos os meios e facilidades necessárias à fiscalização pelo CONTRATANTE, cujo representante terá poderes para sustar os serviços, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;

9.12. Quando especificada, manter, durante a execução do Contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento dos serviços contratados;

9.13. Fornecer, sempre que solicitado, amostra para realização de Prova de Conceito para fins de comprovação de atendimento das especificações técnicas;

9.14. Acatar, no prazo estabelecido na notificação feita pelo Gestor do Contrato, as instruções, sugestões, observações e decisões que emanem do CONTRATANTE, corrigindo as deficiências apontadas quanto ao cumprimento das cláusulas contratuais, devendo, ainda, observar as normas de segurança estabelecidas pelo CONTRATANTE;

9.15. Manter, durante toda a execução do Contrato, as condições de habilitação e qualificação exigidas na licitação;

9.16. Obedecer a todas as normas, padrões, processos e procedimentos do CONTRATANTE definidos pela Gerência de Telecomunicações da SSPGO;

9.17. Prestar todos os esclarecimentos técnicos e administrativos que lhe forem solicitados pelo CONTRATANTE, relacionados à prestação dos serviços;

8.18. Não divulgar nem permitir a divulgação, sob qualquer hipótese, das informações a que venha a ter acesso em decorrência dos serviços realizados, sob pena de responsabilidade civil e/ou criminal;

9.19. Zelar pelo patrimônio do CONTRATANTE e usar de forma racional os materiais disponíveis para a execução do Contrato;

9.20. Responsabilizar-se pela solicitação de acesso aos funcionários aos sistemas e serviços do CONTRATANTE, necessários à prestação dos serviços, bem como pelos seus respectivos descredenciamentos quando necessários;

9.21. Assumir, plena e exclusivamente, todos os riscos provenientes da execução do objeto contratual, não assumindo o CONTRATANTE, em hipótese alguma, nenhuma responsabilidade subsidiariamente;

9.22. Propiciar a transferência de conhecimento aos servidores do CONTRATANTE durante toda a execução contratual;

9.23. Sempre que houver atualização tecnológica ou metodológica em que os técnicos envolvidos necessitem do novo conhecimento, o CONTRATANTE notificará a CONTRATADA da necessidade de capacitação de sua equipe ou de sua substituição por outra já capacitada;

9.24. Comunicar por escrito qualquer anormalidade, prestando ao CONTRATANTE os esclarecimentos julgados necessários;

9.25. Observar as obrigações elencadas e outras firmadas em Contrato ou existentes em normas internas do CONTRATANTE, caso contrário, ficará sujeita às penalidades e sanções administrativas descritas neste Termo de Referência;

9.26. Refazer os trabalhos impugnados pelo gestor do contrato, ficando por sua conta exclusiva as despesas decorrentes dessas providências.

9.27. Garantir que a execução dos serviços prestados ao CONTRATANTE não sejam interrompidos e não tenham redução de qualidade ou disponibilidade por falta de recursos materiais ou humanos.

9.28. Adotar todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando em ocorrência da espécie forem vítimas os seus técnicos e empregados no desempenho dos serviços ou em contato com eles, ainda que verificadas nas dependências da CONTRATANTE;

9.29. Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social trabalhista em vigor, obrigando-se a saldá-las na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com a CONTRATANTE;

9.30. A inadimplência da CONTRATADA, com referência aos encargos estabelecidos nas condições anteriores, não transfere a responsabilidade por seu pagamento à SSPGO, nem poderá onerar o objeto da licitação, razão pela qual a CONTRATADA renuncia desde já a qualquer vínculo de solidariedade, ativa ou passiva, para com a CONTRATANTE;

9.31. Aceitar, durante a vigência do Contrato, nas mesmas condições contratuais,os acréscimos ou supressão do objeto, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado, durante a sua vigência ;

9.32. Utilizar as melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações contidas no Contrato e seus anexos;

9.33. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas, caso os prazos e condições não sejam cumpridos;

9.34. Cumprir os Níveis de Serviço exigidos e demais condições estabelecidas no Contrato, Edital e seus Anexos;

9.35. Apresentar novas soluções dentro dos prazos e condições estabelecidas pela CONTRATADA, sem prejuízo de aplicação de penalidades previstas, caso sejam detectados erros ou impropriedades na solução apresentada;

10. RECEBIMENTO E ACEITAÇÃO DO OBJETO

10.1. O prazo de entrega, referente ao item 1.1, é de, no máximo, 10 (dez) dias corridos, contados a partir da assinatura do contrato, devendo as licenças fornecidas constar em site oficial do fabricante.

10.2. O prazo de implantação, referente ao item 1.2, é de 20 (vinte) dias úteis a partir da assinatura do contrato.

10.3. O prazo para a realização do treinamento, referente ao item 1.3, é de 60 (sessenta) dias a partir da assinatura do contrato.

10.4. Caso a solução ofertada seja composta por equipamentos, os mesmos deverão ser de primeira qualidade, de primeiro uso, transportados e acondicionados de maneira que garanta sua integridade, acompanhados de manual do usuário em português, na forma, quantidade e prazos previstos no Instrumento Contratual e no Termo de Referência, que integram o Edital;

10.5. Caso a solução ofertada seja composta por softwares, os mesmos deverão ser entregues em formato eletrônico (CD ou DVD) ou podem ser disponibilizados através de portal web do fabricante do software, desde que sejam providos mecanismos de controle de acesso e integridade apropriados;

10.5. Os bens e serviços deverão ser entregues no local indicado pela CONTRATANTE.

10.5.1. O horário de entrega de bens será das 08:00h às 12:00h e das 13:00h às 17:00h em dias úteis, conforme horário de Brasília. Não serão recebidos produtos fora deste horário, salvo prévio acordo;

10.6. Os pedidos de prorrogação de prazo de entrega só serão examinados quando formulados à CONTRATANTE até o prazo limite de entrega;

10.7. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo Fiscal do contrato, às custas da CONTRATADA, sem prejuízo da aplicação de penalidades.

10.8. O Termo de Recebimento Definitivo será emitido pela Fiscalização Contratual com o término da implementação da solução;

10.9. Para o recebimento definitivo é condição indispensável, mas não única, o devido reconhecimento e emissão da licença de uso em favor da CONTRATANTE pelo fabricante, de acordo com suas regras e práticas de licenciamento. A licença deverá estar registrada no site do fabricante em nome da CONTRATANTE

10.10. Caso a licença entregue não corresponda às especificações deste Termo de Referência, a Contratada deverá providenciar sua substituição, sem quaisquer ônus adicionais para o Contratante, no prazo máximo de 10 (dez) dias, contados a partir da respectiva notificação pela Fiscalização Contratual, sem prejuízo da incidência das sanções administrativas cabíveis.

10.11. Para o item 1.3, o Termo de Recebimento Definitivo será emitido pela Fiscalização Contratual após obtida avaliação satisfatória pelos participantes da turma e entrega do certificado de participação.

10.12. O recebimento definitivo do objeto não exclui a responsabilidade da contratada por vícios e desconformidades com as especificações técnicas exigidas no Edital de Licitação e Termo de Referência, ainda que verificados posteriormente.

11. FORMA DE PAGAMENTO

11.1. Os pagamentos serão realizados conforme abaixo:

11.1.1. Para o item 1.1, o pagamento será feito em única parcela, após a entrega e emissão do Termo de Recebimento Definitivo para o item;

11.1.2. Para o item 1.2, o pagamento será feito em única parcela, após a entrega e emissão do Termo de Recebimento Definitivo para o item;

11.1.3. Para o item 1.3, o pagamento será feito em única parcela, após a entrega e emissão do Termo de Recebimento Definitivo para o item;

11.2. Cada pagamento será efetuado em 30 (trinta) dias após a entrega da Nota Fiscal/Fatura correspondente

11.3. Na ocorrência de erros na(s) Nota(s) Fiscal(is) /Fatura(s) ou situação que impeça a liquidação da despesa, aquela(s) será(ão) devolvidas(s) e o pagamento ficará pendente até que as medidas saneadoras sejam providenciadas pela CONTRATADA.

11.4. Na hipótese acima mencionada, a contagem do prazo para pagamento será iniciada após a correção dos erros identificados e reapresentação da(s) Nota(s) /Fatura(s), não acarretando qualquer ônus para a CONTRATANTE.

11.5. O pagamento será efetuado em favor da CONTRATADA através de ordem bancária, devendo para isso ficar explicitado o nome da instituição financeira recebedora, agência, localidade, número da operação, quando for o caso, e número da conta corrente na qual
deverá ser depositado o crédito, que ocorrerá após a entrega dos equipamentos e mediante a aceitação e atesto na(s) Nota(s) Fiscal(is) /Fatura(s).

11.5.1. Os pagamentos somente serão efetivados por meio de crédito em conta corrente da CONTRATADA, preferencialmente na Caixa Econômica Federal - CEF, que é a Instituição Bancária contratada pelo Estado de Goiás para centralizar sua movimentação financeira, nos termos do art. 4º da Lei Estadual nº 18.364, de 10 de janeiro de 2014.

11.6. A CONTRATANTE reserva-se o direito de suspender o pagamento caso os serviços sejam entregues em desacordo com o Termo de Referência.

12. VIGÊNCIA, PRAZO E LOCAL DE ENTREGA/EXECUÇÃO DO OBJETO

12.1. O período de vigência do contrato será de 12 (doze) meses a partir da data de sua assinatura, eficácia a partir da publicação no Diário Oficial do Estado de Goiás,

12.2. O Contrato poderá ser prorrogado por igual e sucessivo período mediante termo aditivo, nos termos da Lei nº 8.666/93.

12.3. A CONTRATADA deverá sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do Art. 65 da Lei n. 8.666/93.

12.4. Os serviços e/ou equipamentos deverão ser entregues na Gerência de Telecomunicação da Secretaria da Segurança Pública do Estado de Goiás (Endereço: Avenida Anhanguera nº 7.364 – Setor Aeroviário – CEP: 74.435-300 – Goiânia - Goiás).

13. REAJUSTE DO CONTRATO

13.1. Será concedido reajuste dos preços dos serviços continuados com prazo de vigência igual ou superior a 12 (doze) meses, nos termos do Art. 40, inciso XI, da Lei Federal nº 8.666/1993, mediante requisição da CONTRATADA e desde que observado o interregno mínimo de 01 (um) ano. O interregno mínimo de 01 (um) ano será contato:

13.1.1. Para o primeiro reajuste: a partir da data da apresentação das propostas constante do instrumento convocatório.

13.1.2. Para os reajustes subsequentes ao primeiro: a partir da data dos efeitos financeiros do último reajuste.

13.2. O reajuste dos preços será feito pela aplicação do IPCA (Índice Nacional de Preços ao Consumidor Amplo), ou outro índice que venha a substituí-lo, observado os preços praticados no mercado.

13.3. Os novos valores contratuais decorrentes do reajuste terão suas vigências iniciadas após a assinatura do Termo de Apostilamento, respeitado o interregno mínimo estabelecido no item 13.1.

14. DOS CRITÉRIOS DE HABILITAÇÃO E QUALIFICAÇÃO TÉCNICA-OPERACIONAL DE FORNECEDORES

14.1. Será requerida das empresas LICITANTES, para fins de habilitação técnica, a comprovação de aptidão para a prestação dos serviços em características e quantidades compatíveis com o objeto desta licitação, mediante a apresentação de documentação que comprove o atendimento aos critérios listados a seguir:

i. Apresentação de Atestados de Capacidade Técnica, nos termos do item 14.4;
ii. Apresentação de Proposta de Preços, nos termos do item 14.5;

14.2. Os requisitos estabelecidos pela CONTRATANTE para comprovação de capacidade técnica foram fixados à luz da aplicação dos princípios da razoabilidade e da proporcionalidade e de forma adequada aos itens, etapas ou parcelas de maior relevância para a contratação.

14.3. É facultado à CONTRATANTE a instauração de diligência destinada a esclarecer ou a confirmar a veracidade das informações prestadas pela CONTRATADA constantes de sua Comprovação de Capacidade Técnica, Proposta de Preços e de eventuais documentos anexados.

14.4. COMPROVAÇÃO DA CAPACIDADE TÉCNICA

14.4.1. A fim de comprovar a capacitação técnica e experiência na execução de serviços correlatos aos do objeto deste Termo de Referência, o LICITANTE, nos termos do art. 30, §1º, da Lei n.º 8.666/1993, deverá, juntamente com a documentação de habilitação necessária, demonstrar aptidão e capacidade técnico-operacional para a execução do objeto mediante comprovação de prestação bem-sucedida de serviços em características e quantidades compatíveis com a presente licitação, por meio da apresentação de ATESTADO DE CAPACIDADE TÉCNICA, em nome do LICITANTE, em documento timbrado, emitido por entidade da administração federal, estadual ou municipal, direta ou indireta e/ou empresa privada, que deverá comprovar o atendimento aos seguintes requisitos:

14.4.1.1. Prestação de serviços de fornecimento de solução Anti-Spam / Antivírus de e-mail, contemplando atualização de base de assinaturas, atualização de software e suporte técnico, podendo considerar contratos já executados e/ou em execução, em atividades pertinentes e compatíveis em características técnicas deste Termo de Referência*;*

14.4.2. Os ATESTADOS DE CAPACIDADE TÉCNICA devem atender, também, ao seguinte:

14.4.2.1. Nos ATESTADOS devem estar explícitos a identificação e a localização do órgão/entidade/empresa que está fornecendo o ATESTADO, o responsável pelo setor encarregado do objeto em questão, os contatos para realização de diligências e a especificação pormenorizada dos serviços executados ou em execução.

14.4.2.2. No caso de ATESTADOS emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

14.4.2.3. Os ATESTADOS deverão ser válidos e conter a descrição das atividades pertinentes e compatíveis em características técnicas com o(s) Item(s) de interesse, bem como informações sobre o número do contrato vinculado e sua vigência, a data de início dos serviços prestados e dos produtos atestados. Portanto, os ATESTADOS deverão contemplar, no mínimo, as seguintes informações:

i. Nome do cliente;

ii. Endereço completo do cliente;

iii. Identificação do contrato;

iv. Descrição dos serviços prestados;

v. Vigência do contrato;

vi. Assinatura e identificação do signatário, contendo: nome, cargo ou função que exerce junto ao emitente e que o habilite a expedir o referido atestado; e

vii. Telefone ou e-mail de contato.

14.4.3. A critério da CONTRATANTE, poderá ser necessário diligenciar a pessoa jurídica indicada no ATESTADO DE CAPACIDADE TÉCNICA - nos termos do §3°do art. 43 da Lei n° 8.666/1993 - visando obter informações objetivas sobre o serviço prestado. Se for encontrada divergência entre o especificado nos ATESTADOS DE CAPACIDADE TÉCNICA e o apurado em eventual diligência, além da desclassificação no presente processo licitatório, fica sujeita o LICITANTE às penalidades legais cabíveis, garantidos o contraditório e a ampla defesa.

14.5. PROPOSTA DE PREÇOS

14.5.1. A PROPOSTA DE PREÇOS deverá ser apresentada de acordo com a descrição dos itens e os quantitativos listados no item 3 deste Termo de Referência, de forma a garantir a sua exequibilidade e permitir seu julgamento. A PROPOSTA TÉCNICA E DE PREÇOS deverá ter prazo de validade não inferior a 90 (noventa) dias corridos, a partir da data da sessão pública.

14.5.2. O LICITANTE deverá declarar, no momento de sua PROPOSTA, que possui capacidade técnica adequada para executar o objeto da licitação atendendo aos critérios de qualidade e aos níveis de serviço exigidos, cumprindo os requisitos especificados para a presente contratação.

14.5.3. Nos preços cotados deverão estar incluídas todas as despesas direta e indiretamente envolvidas na execução dos serviços, tais como transporte, seguros, salários, encargos sociais, encargos fiscais e taxas comerciais, impostos, taxas de contribuição, tarifas públicas e quaisquer outros custos, quando aplicáveis, necessários ao integral cumprimento do objeto contratado. Deverão estar contidos ainda todos os custos marginais referentes aos profissionais designados para a prestação dos serviços, tais como deslocamentos, hospedagens, treinamentos e etc.

14.5.4. A PROPOSTA deverá ser redigida em Língua Portuguesa (pt-BR), salvo quanto às expressões técnicas de uso corrente, sem emendas, rasuras ou entrelinhas, devidamente datada, sendo clara e precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado, com todos os preços expressos em REAIS (R$) e declaração expressa de que os serviços ofertados atendem aos requisitos técnicos especificados neste Termo de Referência.

14.6. MODELO DE PLANILHA DE ATENDIMENTO A REQUISITOS

14.6.1. O atendimento a todos os itens deve ser comprovado através de documentação oficial do fabricante da solução, que deverá ser anexada à proposta comercial ajustada. A instituição poderá realizar diligência junto ao fabricante para comprovar a autenticidade da documentação. A localização da comprovação na(s) página(s) deverá ser clara e precisa conforme modelo abaixo. O não atendimento destes requisitos implicará na desclassificação da proposta.

Item	Documento	Página	Localização

15. CRITÉRIOS DE JULGAMENTO

15.1. O LICITANTE será considerado tecnicamente habilitado se restar inequivocamente comprovado atender integralmente ao disposto nos critérios técnicos de habilitação, dessa forma:

i. Tenha comprovado sua capacidade técnico-operacional através da apresentação de ATESTADO(S) DE CAPACIDADE TÉCNICA que atendam aos requisitos estabelecidos no item 14.4;
ii. Tenha apresentado sua PROPOSTA DE PREÇOS em conformidade com o atendimento dos requisitos estabelecidos no item 14.5;

15.2. O LICITANTE será considerado inabilitado caso não comprove inequívoco atendimento aos critérios técnicos de habilitação e/ou deixe de apresentar quaisquer dos documentos exigidos para a habilitação e/ou apresente documentos em desacordo com o estabelecido, não se admitindo complementação posterior (exceto àquelas requisitadas em procedimento de diligência). Durante a avaliação documental poderá a CONTRATANTE solicitar prazo adicional com o objetivo de promover análise minuciosa dos documentos apresentados.

16. SANÇÕES APLICÁVEIS

16.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a CONTRATADA que:

16.1.1. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

16.1.2. Ensejar o retardamento da execução do objeto;

16.1.3. Falhar ou fraudar na execução do contrato;

16.1.4. Comportar-se de modo inidôneo;

16.1.5. Cometer fraude fiscal.

16.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

16.2.1. Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado.

16.2.2. Multa de:

16.2.2.1. 0,1% (um décimo por cento) até 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do serviço não realizado;

16.2.2.2. 0,1% (um décimo por cento) até 0,7% (sete décimos por cento) sobre o valor da parte do serviço não realizado, por dia subsequente ao trigésimo;

16.2.2.3. 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor da nota de empenho ou do contrato, em caso de inexecução total da obrigação;

16.2.2.4. 0,2% a 3,2% por dia sobre o valor mensal do contrato, conforme detalhamento constante das tabelas abaixo; e

16.2.2.5. 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato.

16.2.2.6 .As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

16.2.3. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até 2 (dois) anos.

16.2.4. Sanção de impedimento de licitar e contratar com órgãos e entidades do Estado de Goiás, com o consequente descredenciamento no CADFOR pelo prazo de até 5 (cinco) anos.

16.2.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir o CONTRATANTE pelos prejuízos causados.

16.3. As sanções previstas nos subitens 16.2.1, 16.2.3, 16.2.4 e 16.2.5 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados

16.4. Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas abaixo:

GRAU	CORRESPONDÊNCIA
1	0,2% ao dia sobre o valor mensal do contrato
2	0,4% ao dia sobre o valor mensal do contrato
3	0,8% ao dia sobre o valor mensal do contrato
4	1,6% ao dia sobre o valor mensal do contrato
5	3,2% ao dia sobre o valor mensal do contrato

INFRAÇÃO		
ITEM	**DESCRIÇÃO**	**GRAU**
1	Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais, por ocorrência.	05
2	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento.	04
3	Manter prestador de serviço sem qualificação para executar os serviços contratados, por empregado e por dia.	03
4	Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia.	02
Para os itens a seguir, deixar de:		
5	Cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência.	02
6	Substituir empregado que se conduza de modo inconveniente ou não atenda às necessidades do serviço,	01

	por funcionário e por dia.	
7	Cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência.	03
8	Indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato.	01

16.5. Também ficam sujeitas às penalidades do Art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

16.5.1. Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

16.5.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

16.5.3. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

16.6. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

16.7. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

16.8. As penalidades serão obrigatoriamente registradas no CADFOR.

17. RESPONSÁVEL PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA

17.1. Este termo foi elaborado por Jánison Calixto dos Santos.

17.2. Dúvidas deverão ser tratadas pelo e-mail janison.calixto@ssp.go.gov.br

Documento assinado eletronicamente por **JANISON CALIXTO DOS SANTOS**, **Gerente**, em 25/06/2021, às 15:49, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

A autenticidade do documento pode ser conferida no site **http://sei.go.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=1** informando o código verificador **000021474903** e o código CRC **BF76D22B**.

Referência: Processo nº 202100016009849 SEI 000021474903

Criado por JANISON CALIXTO DOS SANTOS, versão 5 por JANISON CALIXTO DOS SANTOS em 25/06/2021 15:36:28.