TERMO DE REFERÊNCIA PARA CONTRATAÇÃO DE SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Termo de Referência nº 009/2021 - SGI/ANEEL

Brasília, 07 de julho de 2021

1. IDENTIFICAÇÃO

1.1 Processo: 48500.000827/2021-41
1.2 Objetivo estratégico: OE15 - Modernizar a infraestrutura e soluções de tecnologia da informação
1.3 Item do PDTIC: OETI10 – Avançar na modernização da infraestrutura de TI
1.4 Item do PAC/ME: 317 - Solução de antispam para 4100 caixas postais com suporte e garantia por 12 meses.
1.5 Item do SIGANEEL: 26.9 - Adquirir Solução de Antispam / N.D. 3.3.90.40.0
1.6 Programa: Gestão e Manutenção do Ministério de Minas e Energia
1.7 Ação: Administração da Unidade
1.8 Atividade: Contratação de solução de antispam para a proteção do serviço de correio eletrônico da Agência.
1.9 Responsável: SGI/ANEEL

2. OBJETO

2.1 Objeto: Contratação de solução de antispam contemplando licenças de subscrição de software, instalação, repasse de conhecimento e garantia de atualizações com suporte técnico por 12 (doze) meses, prorrogáveis anualmente até o limite de 60 (sessenta) meses.

- Regime de execução Indireta (Lei nº8666/93, art.6º, VIII): Empreitada por Preço Global

2.2 O objeto enquadra-se como (Lei nº 10.520/2002, Decreto nº 3.555/2000, Decreto nº 5.450/2005, Instrução Normativa SEGES/MP nº 5/2017):

2.2.1 ☐ **Bem e/ou Serviço comum**, cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo ato convocatório, por meio de especificações usuais do mercado**.**

2.2.2 ☐ **Serviço não continuado ou contratado por escopo,** referente à execução de um objeto específico em um período pré-determinado.

2.2.3 ☒ **Serviço continuado**, essencial, que visa atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público ou o funcionamento das atividades finalísticas da ANEEL, de modo que sua interrupção poderá comprometer a prestação de um serviço público ou o cumprimento de sua missão institucional.

2.2.4 Não se aplica.

2.3 O objeto enquadra-se como contratação por meio do Sistema de Registro de Preços (Decreto nº 7892/2013) Não se aplica.

2.3.1 Anuência de participação à ata de RP: Não se aplica.

2.4 Forma de seleção do fornecedor:

2.4.1 ☒ **Licitação.** A contratação enquadra-se nos limites estabelecidos no Art. 23 da Lei n. 8666/93 e está em conformidade com a Lei nº 10.520/2002.

2.4.2 ☐ **Dispensa ou inexigibilidade de licitação:** Justificar a contratação direta do objeto, enfocando suas características peculiares e a legislação cabível (lei nº 8.666/93, efetuar o enquadramento nos incisos dos arts. 24-dispensa ou 25-inexigibilidade).. 24-dispensa ou 25-inexigibilidade).

2.4.3 ☐ **Adesão à ata de registro de preços de outro órgão.** Justificar a adesão, enfocando suas vantagens e indicando a legislação cabível (Decreto nº 7892/2013).

2.4.4 ☐ **Participação em ata de registro de preços de outro órgão:** Justificar a participação, enfocando suas vantagens e indicando a legislação cabível (Decreto nº 7892/2013).

2.5 Será admitida a subcontratação parcial do objeto (Lei nº 8666/1993, art. 72)*:* Não se aplica.

2.6 A execução do objeto poderá ser por empresas reunidas em consórcio (Lei nº 8666/1993, art.33, *caput*)*:* Não se aplica.

2.7 A adjudicação do OBJETO será por:

2.7.1 ☒ Por **ITEM.**

2.7.2 ☐ Por **ITENS** formando **GRUPO (S):** Não se aplica.

2.7.2.1 Quando a adjudicação for por preço global de um GRUPO de itens, a aquisição pela ANEEL somente será admitida nas seguintes hipóteses:

2.7.2.1.1 Aquisição de todos os itens do GRUPO, respeitadas as proporções de quantitativos definidos no certame; OU

2.7.2.1.2 Aquisição de um item isolado somente se seu preço unitário tenha sido o menor preço válido ofertado para o item na fase de lances.

2.7.2.1.3 Constitui irregularidade a aquisição (emissão de empenho) de um item isolado do GRUPO, quando o preço unitário adjudicado ao item não tenha sido o menor lance válido ofertado na disputa, salvo quando, justificadamente, ficar demonstrado que é inexequível ou inviável, dentro do modelo de execução do contrato, a demanda proporcional ou total de todos os itens do respectivo GRUPO.

3. JUSTIFICATIVA

Justificativa:

3.1 A ANEEL utiliza massivamente uma solução de correio eletrônico para envio e recebimento de e-mails de diversos agentes do setor elétrico localizados em redes privadas, governamentais e na Internet, contribuindo significativamente para a agilidade das comunicações e na eficácia de suas operações.

3.2 Entretanto, inerente à efetividade do uso dessa comunicação eletrônica, os emails recebidos pela Agência são constantemente alvo de propagandas eletrônicas indesejadas (spams) que afetam a produtividade de seus colaboradores e tentativas de ataques de phishings e de infecções de computadores por softwares maliciosos (malwares) e ocultos em links e arquivos em anexo, tais como: vírus, worms, cavalos-de tróia (trojans), spywares, rootkits, backdoors, ransomwares, entre outras ameaças.

3.3 No caso específico do recebimento de e-mails maliciosos, estes são utilizados por agentes mal-intencionados para causar graves danos às pessoas e organizações. Os malwares listados anteriormente visam realizar, por exemplo, a captura de dados pessoais, captura de logins de acesso a redes e sistemas corporativos, acesso indevido à infraestrutura de TI comprometida, criptografia de dados, vazamentos de dados sensíveis, perda definitiva de dados, extorsões, golpes bancários e destruição eletrônica de componentes de infraestrutura de TI.

3.4 Nesse contexto, a ANEEL, como uma importante organização federal pertencente ao Setor Elétrico e visando garantir a confidencialidade, integridade e disponibilidade de suas informações e comunicações eletrônicas, vem continuamente adquirindo ou renovando ao longo dos anos suas soluções de segurança cibernética para manutenção de uma estratégia de proteção em camadas do seu ambiente computacional em níveis adequados.

3.5 Nesse sentido, a solução de TI objeto específico dessa demanda é a empregada para combater a entrada dos e-mails indesejados e maliciosos supracitados diretamente nas caixas postais institucionais e dos colaboradores da Agência.

3.6 A última solução CONTRATADA para esse fim, composta por um cluster de 2 (dois) equipamentos do tipo appliance, está em uso na Agência desde 2018 e terá a sua licença de funcionamento expirada no segundo semestre de 2021, que resultará na parada de importantes funcionalidades de gerenciamento e de mecanismos fundamentais de atualização (vacinas e assinaturas contra malwares, novos patches e firmwares) e caso não seja substituída elevará a níveis preocupantes a probabilidade de concretização dos incidentes de segurança cibernética mencionados anteriormente.

3.7 Dessa forma, considerando-se que atualmente a principal ameaça cibernética às segurança das informações das organizações são iniciadas por meio do recebimento de e-mails maliciosos e tendo em vista os riscos decorrentes da descontinuidade dessa proteção à execução das operações da ANEEL e, no limite, do próprio

cumprimento de sua missão institucional, justifica-se a necessidade da realização de nova contratação visando manter a continuidade da segurança cibernética do correio eletrônico da Agência e, sobretudo da infraestrutura de TI e informações da ANEEL como um todo, contra ameaças que utilizam o e-mail como vetor de entrada de ataques cibernéticos.

3.8 Ressalta-se que estratégia da contratação em tela foi resultado de um estudo realizado pela equipe de contratação da ANEEL onde foram analisadas as alternativas de soluções disponíveis considerando-se as demandas de negócio, necessidades tecnológicas e recursos orçamentários, cujo conteúdo foi consubstanciado no documento Estudo Técnico Preliminar (SICNET2 48540.000827/2021-41).

3.9 Por fim, as justificativas para a realização dessa contratação foram então sintetizadas a seguir:

3.9.1 Mitigar os riscos de segurança cibernética do ambiente computacional da Agência associados à vulnerabilidades e ameaças provenientes de e-mails, por meio da contribuição específica que a solução de antispam realiza ao efetuar a inspeção e bloqueio de ameaças virtuais associadas ao recebimento de e-mails indesejados e maliciosos, que podem causar: (i) diminuição da produtividade do quadro de pessoal e (ii) danos à infraestrutura computacional, à segurança dos dados e informações críticas nela armazenadas e, em consequência, prejuízos à continuidade do negócio e ao cumprimento da Missão da Agência;

3.9.2 Modernizar a infraestrutura tecnológica de ativos de TI que promovem a segurança da informação da Agência por meio da adoção de solução que utilizem padrões tecnológicos mais avançados no que diz respeito à filtragem de e-mails (antispam);

3.9.3 Garantir a conformidade às instruções normativas e normas complementares expedidas pelo Gabinete de Segurança Institucional/PR que tratam da segurança da informação e comunicação na Administração Pública Federal, em especial a Norma Complementar nº 04/IN01/DSCI/GSIPR que dispõe sobre as diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações na APF, aos guias técnicos de segurança da informação expedidos por órgãos de controle externo (TCU/CGU), às normas de segurança da informação da ANEEL (Política de Segurança da Informação da ANEEL – NOA 12 e Instruções

Fundamento legal: A contratação tem amparo legal na Instrução Normativa SGD/ME nº 1 de 4 de abril de 2019, na Lei nº 10.520, de 17 de julho de 2002, no Decreto nº 10.024, de 20 de setembro de 2019, no Decreto nº 7.892, de 23 de janeiro de 2013, e, subsidiariamente, nas normas da Lei nº 8.666, de 21 de junho de 1993, e suas alterações.

4. RESULTADOS

Resultados a serem alcançados:

4.1 Prover a continuidade da segurança cibernética aplicada diretamente à solução de correio eletrônico da ANEEL e, indiretamente, ao restante da infraestrutura computacional disposta em rede da Agência (desktops, servidores físicos e virtuais e sistemas de storages);

4.2 Modernizar os mecanismos tecnológicos de proteção cibernética aplicados ao recebimento de mensagens eletrônicas indesejadas e/ou maliciosas de correio eletrônico (e-mails de marketing, spams, ataques de phishing, vírus, worms, ransomwares, entre outros malwares);

4.3 Contribuir para a redução dos riscos cibernéticos decorrentes de ataques virtuais à segurança das informações da Agência que empregam técnicas, táticas e procedimentos que fazem uso de mensagens de correio eletrônico;

4.4 Economicidade na contratação tendo em vista o atual cenário de restrições orçamentárias na APF;

5. PRAZOS:

5.1 Vigência do instrumento contratual: 12 (doze) meses, prorrogáveis anualmente até o limite de 60 (sessenta) meses.

5.2 Período de execução do objeto: 12 (doze) meses prorrogáveis anualmente até o limite de 60 (sessenta) meses

5.3 Meta de início de execução do objeto: 01/10/2021

5.4 Contratação atual para o mesmo objeto: Sim

5.4.1 Atual Contratado: Global TTI Soluções em Tecnologia da Informação CNPJ - 21823206000191

5.4.2 Fim da vigência: 26/03/2019 (fim da vigência contratual) e 24/10/2021 (fim da vigência da garantia de suporte técnico e atualização da ferramenta atual – 36 meses)

5.4.3 Valor: R$ 243.000,00

6. BENS E/OU SERVIÇOS QUE COMPÕEM A SOLUÇÃO DE TI E VALORES ESTIMADOS

6.1 Valor total: R$ 566.046,00 (quinhentos e sessenta e seis mil e quarenta e seis reais), estimado conforme o Anexo A – Orçamento deste TR, e assim composto:

Item	Descrição	Catser	Unidade	Valor Unitário (R$)	Valor Total (R$)
1	Contratação de solução de antispam contemplando fornecimento de licenças de subscrição de software para 4.100	27502	Caixa postal	138,06	566.046,00

	caixas postais, instalação, garantia, repasse de conhecimento e suporte técnico por 12 (doze) meses, prorrogáveis anualmente, até o limite de 60 (sessenta) meses.				
Valor Global da Contratação (R$)					**566.046,00**

6.2 Valor no exercício: R$ 566.046,00 (quinhentos e sessenta e seis mil e quarenta e seis reais)

6.3 Valor no próximo exercício: Não se aplica

6.4 O valor total estimado: R$ 566.046,00 (quinhentos e sessenta e seis mil e quarenta e seis reais)

7. DETALHAMENTO DO OBJETO:

7.1 ITEM 1 - SERVIÇO: Subscrição de licença de software de antispam para 4.100 (quatro mil e cem) caixas postais com instalação, garantia, repasse de conhecimento e suporte técnico

7.1.1 Classificação da Despesa

Tipo: Locação de software pronto ("de prateleira"), com direito de uso por prazo definido, expirando ao final deste: licença por subscrição.

7.1.1.1 **Natureza:**

7.1.1.1.1 ☒ **Despesa de custeio**. 33904006
7.1.1.1.2 ☐ **Despesa de investimento**.

7.1.2 Código CATSER/ MP: 27502

7.1.3 Natureza do serviço:

7.1.3.1 ☐ **Serviço não continuado ou contratado por escopo,** referente à execução de um objeto específico em um período pré-determinado.

7.1.3.2 ☒ **Serviço continuado**, essencial, que visa atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público ou o funcionamento das atividades finalísticas da ANEEL, de modo que sua interrupção poderá comprometer a prestação de um serviço público ou o cumprimento de sua missão institucional.

- **Observações:** Não se aplica.

7.1.4 REQUISITOS:

7.1.4.1 **Requisitos de negócio:**

7.1.4.1.1 Prover uma solução de filtragem de entrada de e-mails externos e envio de e-mails internos ao público externo contra ameaças do tipo *phishing* (engenharia social), *malwares* (*virus, worms, adwares, keyloggers, trojans*, entre outras), ataques dirigidos e persistentes, comprometimento de email corporativo e *ransomwares*;

7.1.4.1.2 A solução deverá ser provida em alta disponibilidade para continuidade do serviço de e-mails da ANEEL em caso de interrupção do servidor de e-mail interno;

7.1.4.1.3 A solução CONTRATADA deverá ser acompanhada da garantia com o próprio fabricante, contemplando atualizações de versões e serviço de suporte técnico durante toda o período da contratação;

7.1.4.2 **Requisitos de arquitetura tecnológica**

7.1.4.2.1 **Da Plataforma**

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

7.1.4.2.1.2 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;

7.1.4.2.1.3 A solução deve ser proprietária e a subscrição licenciada para utilização de todos os módulos que compõe a solução para 4.100 (quatro mil e cem) caixas postais;

7.1.4.2.1.4 Deve ser capaz de filtrar o tráfego de correio, bloqueando a entrada de vírus, spyware, worms, trojans, spam, phishing, e-mail marketing e conteúdos indesejados;

7.1.4.2.1.5 Deve possuir módulos de DLP, Criptografia, APT e Archiving compondo a solução;

7.1.4.2.1.6 Deve permitir alta disponibilidade das funções de filtragem, garantindo que o serviço de correio nunca pare por falha da solução;

7.1.4.2.1.7 A solução deve suportar o processamento de, no mínimo, 100.000 (cem mil) mensagens por hora;

7.1.4.2.1.8 A solução deverá ser entregue em appliance virtual e permitir a expansão da solução de hardware da ANEEL, a qualquer tempo, sem cobrança adicional de licença ou limitação de appliance virtual, sendo compatível com os principais sistemas de virtualização do mercado, entre eles:

7.1.4.2.1.8.1 VMWare;

7.1.4.2.1.8.2 Microsoft Hyper-V;

7.1.4.3 **Requisitos Gerais**

7.1.4.3.1 A licença de uso por subscrição do software deve possuir 12 (doze) meses de atualização do fabricante, compreendendo os seguintes módulos:

7.1.4.3.1.1 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;

7.1.4.3.1.2 Direito de uso da versão mais atual do produto licenciado caso esta esteja disponível pelo fabricante, bem como atualizações de recursos e melhorias dentro da mesma versão;

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

7.1.4.3.2 Deve analisar as mensagens, no mínimo, por meio dos seguintes métodos:

7.1.4.3.2.1 Proteção dinâmica por reputação;

7.1.4.3.2.2 Assinaturas de spam;

7.1.4.3.2.3 Filtros de Vírus;

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

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

7.1.4.3.2.4 Filtros de anexos;

7.1.4.3.2.5 Filtros de phishing;

7.1.4.3.2.6 Análise heurística;

7.1.4.3.2.7 Análise do cabeçalho, corpo e anexo das mensagens;

7.1.4.3.2.8 E-mail bounce;

7.1.4.3.2.9 Dicionários pré-definidos e customizados com palavras e expressões regulares;

7.1.4.3.2.10 Deve conter os seguintes dicionários pré-estabelecidos, para posterior utilização, tais como:

7.1.4.3.2.10.1 Número de cartão de crédito;

7.1.4.3.2.10.2 CNPJ;

7.1.4.3.2.10.3 RG e CPF.

7.1.4.3.2.11 Deve possuir mecanismo de backup e recuperação da configuração da solução;

7.1.4.3.2.12 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).

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

7.1.4.3.2.14 A interface de administração do sistema deve ter suporte a no mínimo um dos seguintes idiomas:

7.1.4.3.2.14.1 Português do Brasil;

7.1.4.3.2.14.2 Inglês.

7.1.4.3.2.15 A interface de quarentena do usuário deve suportar o idioma Português do Brasil;

7.1.4.3.2.16 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;

7.1.4.3.2.17 Deve possuir capacidade de configuração de roteamento de mensagens para múltiplos domínios de destino;

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

7.1.4.3.2.19 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;

7.1.4.3.2.20 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;

7.1.4.3.2.21 A solução deve permitir criação de regras por:

7.1.4.3.2.21.1 Grupos de usuários;

7.1.4.3.2.21.2 Domínios;

7.1.4.3.2.21.3 Range de IP;

7.1.4.3.2.21.4 IP/Rede;

7.1.4.3.2.21.5 Remetentes específicos;

7.1.4.3.2.21.6 Destinatários específicos;

7.1.4.3.2.21.7 Grupos de LDAP.

7.1.4.3.2.22 Tratar e analisar mensagens originadas e recebidas possibilitando a aplicação de regras e políticas customizáveis, além de diferenciadas por sendo de tráfego;

7.1.4.3.2.23 Possibilidade de permitir relay autenticado para clientes externos da corporação;

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

7.1.4.3.2.25 A console de gerenciamento deve acessada através de protocolo seguro (HTTPS – HyperText Transfer Protocol Secure) com no mínimo as seguintes funcionalidades:

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

7.1.4.3.2.25.2 Status da versão das assinaturas do antivírus em uso;

7.1.4.3.2.25.3 Controle de acesso de usuários, com diferentes privilégios de configuração;

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

7.1.4.3.2.25.5 Gerência das áreas de quarentena pelo administrador e possibilidade do usuário gerenciar sua área de quarentena.

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

7.1.4.3.2.25.7 Deve ser capaz de utilizar os protocolos de transferência de arquivos SCP e FTP;

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

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

7.1.4.3.2.26.1 Conteúdo do anexo;

7.1.4.3.2.26.2 Mime-Type do anexo;

7.1.4.3.2.26.3 Extensão do anexo;

7.1.4.3.2.26.4 Nome completo do anexo;

7.1.4.3.2.26.5 Nome parcial do anexo;

7.1.4.3.2.26.6 Expressão regular;

7.1.4.3.2.26.7 Tamanho do anexo;

7.1.4.3.2.26.8 Anexos compactados com senha;

7.1.4.3.2.26.9 Quantidade de níveis de compactação no mesmo anexo.

7.1.4.3.2.27 Deve possuir um sistema de Disaster e Recover ao qual é efetuado o upload de um arquivo de backup e restauração dele automaticamente;

7.1.4.3.2.28 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.

7.1.4.3.2.29 Deve possuir sistema de diagnóstico via interface WEB, com no mínimo a execução dos seguintes testes:

7.1.4.3.2.29.1 Teste de Conectividade TCP – Informando o Host e a Porta a serem testados;

7.1.4.3.2.29.2 Teste de Conectividade ICMP – Informando o Host a ser testado;

7.1.4.3.2.29.3 Teste de DNS – Informando o Host ou o Domínio a serem testados;

7.1.4.3.2.29.4 Teste de Envio de E-mail;

7.1.4.3.2.29.5 Teste de Lookup de E-mail via LDAP;

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

7.1.4.3.2.29.7 Teste de TRACEROUTE;

7.1.4.3.2.29.8 Teste de DNS Reverso;

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

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

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

7.1.4.3.2.29.12 Teste de portas de Saída utilizadas pelo sistema.

7.1.4.3.2.30 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:

7.1.4.3.2.30.1 Serviço de antivírus;

7.1.4.3.2.30.2 Serviço de MTA;

7.1.4.3.2.30.3 Serviço de Banco de Dados;

7.1.4.3.2.30.4 Serviço de SMNP.

7.1.4.3.2.31 Deve permitir a instalação de agentes/plug-ins (tanto no software de gerenciamento, quanto nos agentes que fazem a filtragem) para monitoramento com sistemas de terceiros, com no mínimo:

7.1.4.3.2.31.1 Zabbix;

7.1.4.3.2.31.2 Nagios.

7.1.4.4 **Da Alta Disponibilidade**

7.1.4.4.1 Suportar Cluster de Alta Disponibilidade na forma de Cluster Alvo-Alvo ou 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;

7.1.4.4.2 Deve permitir a configuração em Cluster com appliances virtualizados em Data Centers distintos;

7.1.4.4.3 O cluster deve poder ser formado por appliaces virtuais de forma mista;

7.1.4.4.4 Administração centralizada de múltiplos nós de filtragem 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;

7.1.4.4.5 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;

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

7.1.4.5 **Do Gerenciamento**

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

7.1.4.5.2 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;

7.1.4.5.3 O sistema deve possuir ainda, no mínimo, os perfis pré-definidos:

7.1.4.5.3.1 Administrador: Com acesso total às configurações da solução;

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

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

7.1.4.5.3.4 Operador: Com acesso à administração da quarentena e gerenciamento da "Blacklist e Whitelist";

7.1.4.5.3.5 Usuário: Possui a capacidade de administrar sua "Blacklist e Whitelist", individualmente, bem como sua área de quarentena individual.

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

7.1.4.5.4.1 E-mails;

7.1.4.5.4.2 Domínios;

7.1.4.5.4.3 IP's;

7.1.4.5.4.4 Range de IP;

7.1.4.5.4.5 Expressão Regular;

7.1.4.5.4.6 Usuários;

7.1.4.5.4.7 Listas de distribuição;

7.1.4.5.4.8 Grupos de LDAP.

7.1.4.6 **Dos Alertas e Logs da Solução**

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

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

7.1.4.6.3 Possuir registro de log de TODAS as ações executadas na interface de administração para fins de auditoria. Esse log deve ser de fácil acesso para obtenção dele, não sendo necessário acionamento da fabricante da solução;

7.1.4.6.4 Possuir mecanismo de alerta por e-mail quando houver nova atualização do sistema e sobre o status do processo de atualizações;

7.1.4.6.5 Deve possuir capacidade de envio dos logs de um nó específico ou de todo o cluster para um servidor de syslog ou de SIEM. Também deve ser possível selecionar os logs a serem enviados, no mínimo, para as opções abaixo:

7.1.4.6.5.1 Emergency;

7.1.4.6.5.2 Alert;

7.1.4.6.5.3 Critical;

7.1.4.6.5.4 Error;

7.1.4.6.5.5 Warning;

7.1.4.6.5.6 Notice;

7.1.4.6.5.7 Informational;

7.1.4.6.5.8 Debug.

7.1.4.6.6 Deve ser possível enviar alertas por e-mail e por SNMP caso ocorra consumo excessivo de algum recurso do sistema. Os sistemas monitorados para envio dos alertas devem ser, no mínimo:

7.1.4.6.6.1 Espaço em disco;

7.1.4.6.6.2 Filas de e-mail;
7.1.4.6.6.3 Memória;
7.1.4.6.6.4 Processador;
7.1.4.6.6.5 Serviço de Filtragem;
7.1.4.6.6.6 Atualização do sistema de segurança;
7.1.4.6.6.7 Antivirus e Antispam;
7.1.4.6.6.8 Ponto de acesso indisponível.

7.1.4.7 **Das Funcionalidades para o usuário final**

7.1.4.7.1 Possuir interface web de administração segura HTTPS para que cada usuário final possa administrar suas opções pessoais e sua quarentena, sem que estas opções interfiram na filtragem dos demais usuários;
7.1.4.7.2 A interface do usuário final deve estar no idioma configurado pelo administrador, sendo no mínimo o seguinte idioma:
7.1.4.7.2.1 Português do Brasil.
7.1.4.7.3 O usuário final deve ser capaz de incluir e remover endereços em sua lista pessoal de bloqueio ou de liberação de e-mails;
7.1.4.7.4 O usuário final deve ser capaz de visualizar as mensagens bloqueadas e liberá-las, a seu critério, desde que elas sejam consideradas somente como “possível spam” ou “spam”;
7.1.4.7.5 O usuário final deve ser capaz de solicitar liberação de uma mensagem ao administrador, caso a mensagem contenha conteúdo considerado malicioso ou bloqueado por outro critério qualquer, o qual não permita que o usuário final a libere;
7.1.4.7.6 O usuário deverá ser capaz de selecionar qual o idioma utilizado sua interface, sendo no mínimo o seguinte idioma:
7.1.4.7.6.1 Português do Brasil.

7.1.4.8 **Da Quarentena**

7.1.4.8.1 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;
7.1.4.8.2 Deve possibilitar a gestão de quarentena pelos administradores de forma que eles possam 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;
7.1.4.8.3 Caso uma mensagem seja bloqueada ou rejeitada, a solução deverá informar também a razão do bloqueio e quais regra foram ativadas;
7.1.4.8.4 A interface deve permitir identificar quais Regras do Modulo de AntiSpam foram ativadas e qual sua pontuação, a fim de permitir ao administrador a elaboração de regras granulares;

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

7.1.4.8.6 Deve permitir também que todas as áreas de quarentenas sejam armazenadas de forma criptografadas na solução;

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

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

7.1.4.8.9 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;

7.1.4.8.10 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;

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

7.1.4.8.12 Possibilitar ao administrador selecionar o rotacionamento 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;

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

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

7.1.4.9 **Dos Usuários e Grupos**

7.1.4.9.1 Possuir integração com serviço de diretórios LDAP, Microsoft Active Directory para obtenção de informações de usuários cadastrados para validação de destinatário e configuração de políticas, bem como impedir ataques de dicionário (“Directory Harvest Attack");

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

7.1.4.9.3 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;

7.1.4.9.4 Permitir a utilização de mais de um servidor de LDAP ou Microsoft Active Directory ao mesmo tempo. Caso ocorra indisponibilidade do servidor primário a autenticação dos usuários deverá ocorrer normalmente no outro servidor configurado;

7.1.4.9.5 Integração nativa com o Microsoft Exchange;
7.1.4.9.6 Possibilitar a customização de regras e políticas por usuários ou grupos;
7.1.4.9.7 A solução deverá permitir a configuração do intervalo de sincronismo com o serviço de diretório;
7.1.4.9.8 Permitir atrelar grupos a regras específicas de rotas, por exemplo: Não aplicar determinada regra do módulo de antivírus para os e-mails que vierem de um determinado domínio, sendo que esta regra somente será aplicada a um grupo específico de usuários.

7.1.4.10 **Dos Relatórios**

7.1.4.10.1 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;
7.1.4.10.2 Deve ser capaz de gerar relatórios gráficos e agendar o envio dos mesmos a usuários específicos via e-mail;
7.1.4.10.3 Deve ser capaz de gerar relatórios por data ou por um intervalo de tempo específico;
7.1.4.10.4 Deve ser possível configurar um período para a retenção dos dados utilizados para geração dos relatórios;
7.1.4.10.5 Capacidade de criar relatórios contendo no mínimo as seguintes informações:
7.1.4.10.5.1 Sumário de mensagens;
7.1.4.10.5.2 Quantidade de mensagens processadas;
7.1.4.10.5.3 Relatório de Volume de Mensagens por Data;
7.1.4.10.5.4 Principais origens de spam por domínio, endereço de e-mail;
7.1.4.10.5.5 Principais destinos de spam por domínio, endereço de e-mail;
7.1.4.10.5.6 Principais origens de vírus;
7.1.4.10.5.7 Principais fontes de ataque;
7.1.4.10.5.8 Relatório de Top E-mail Relays;
7.1.4.10.5.9 Relatório de Top Remetentes por Quantidade;
7.1.4.10.5.10 Relatório de Top Remetentes por Volume;
7.1.4.10.5.11 Relatório de Top Destinatário por Quantidade;
7.1.4.10.5.12 Relatório de Top Destinatário por Volume;
7.1.4.10.5.13 Estatísticas da quarentena;
7.1.4.10.5.14 Conexões completadas X bloqueadas;
7.1.4.10.5.15 Relatório de tráfego;
7.1.4.10.5.16 Principais destinatários de Spam;
7.1.4.10.5.17 Principais destinatários de e-mail;
7.1.4.10.5.18 Top Ataques por fraude de e-mail / tentativa de spoof.
7.1.4.10.5.19 Permitir filtros de relatórios com definição de origem e destinos específico;
7.1.4.10.5.20 Possuir relatórios estatísticos de conexões, ameaças, quarentena e SPAM;
7.1.4.10.5.21 Deve apresentar estatísticas e monitoramento em tempo real (online) de e-mails com base em gráficos;
7.1.4.10.6 Os relatórios, no mínimo, devem poder ser filtrados por:

7.1.4.10.6.1 Período de tempo;
7.1.4.10.6.2 Ponto de Filtragem que o e-mail passou;
7.1.4.10.6.3 De;
7.1.4.10.6.4 Para;

7.1.4.10.7 Qual a classificação que a mensagem atingiu, dentre eles no mínimo:
7.1.4.10.7.1 DLP;
7.1.4.10.7.2 Provável SPAM;
7.1.4.10.7.3 SPAM;
7.1.4.10.7.4 Vírus;
7.1.4.10.7.5 Conteúdo Bloqueado;
7.1.4.10.7.6 Whitelist;
7.1.4.10.7.7 Blacklist;
7.1.4.10.7.8 Tamanho Excedido;
7.1.4.10.7.9 Phishing.
7.1.4.10.7.10 Relatório para um único usuário ou Domínio.

7.1.4.11 **Do Rastreamento das Mensagens**

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

7.1.4.11.2 O rastreamento deve ser possível através de qualquer um dos seguintes campos:
7.1.4.11.2.1 ID da mensagem;
7.1.4.11.2.2 E-mail do Remente;
7.1.4.11.2.3 E-mail do Destinatário;
7.1.4.11.2.4 Domínio do Remetente;
7.1.4.11.2.5 Domínio do Destinatário;
7.1.4.11.2.6 Assunto da mensagem;
7.1.4.11.2.7 Nome do anexo;
7.1.4.11.2.8 Palavra contida no conteúdo do corpo da mensagem;
7.1.4.11.2.9 IP de Origem da mensagem;
7.1.4.11.2.10 Tamanho da mensagem;
7.1.4.11.2.11 Regra de SPAM;
7.1.4.11.2.12 Regra de DLP;
7.1.4.11.2.13 Se a mensagem foi entregue ou não;
7.1.4.11.2.14 Regras personalizadas aplicadas na mensagem;
7.1.4.11.2.15 Nome da ameaça encontrada.

7.1.4.11.3 A console deve apresentar ainda as seguintes características de rastreamento de mensagens:
7.1.4.11.3.1 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”;

7.1.4.11.3.2 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;

7.1.4.11.3.3 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;

7.1.4.11.4 Deve apresentar como resultado as seguintes informações:

7.1.4.11.4.1 Remetente da mensagem;

7.1.4.11.4.2 Destinatários da mensagem;

7.1.4.11.4.3 Servidor de origem;

7.1.4.11.4.4 Se foi armazenada em quarentena;

7.1.4.11.4.5 Se contenha vírus;

7.1.4.11.4.6 A regra que atuou;

7.1.4.11.4.7 O servidor de origem;

7.1.4.11.4.8 O tamanho da mensagem;

7.1.4.11.4.9 Se foi entregue ou não;

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

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

7.1.4.11.6 Se o e-mail estiver sido bloqueado por ser considerado spam ou possível spam, o log 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);

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

7.1.4.11.8 Rastrear e-mails a partir de uma determinada ameaça;

7.1.4.11.9 Apresentar na interface gráfica as fontes de ataque e, através delas, apresentar quais e-mails foram recebidos, originários dessa fonte de ataque.

7.1.4.12 **Da Proteção Contra Ataques**

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

7.1.4.12.2 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;

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

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

7.1.4.12.3.2 Rejeitar a conexão SMTP que se caracterize como "flooding".

7.1.4.12.3.3 Deve ser capaz de efetuar a filtragem do tráfego de correio eletrônico bloqueando a entrada e saída de:

7.1.4.12.3.4 Vírus;
7.1.4.12.3.5 Spyware;
7.1.4.12.3.6 Worms;
7.1.4.12.3.7 Trojans;
7.1.4.12.3.8 Spam;
7.1.4.12.3.9 Phishing;
7.1.4.12.3.10 E-mail Marketing, ou qualquer outra forma de ameaça virtual.

7.1.4.12.4 Deve possuir controle total da comunicação permitindo restringir:
7.1.4.12.4.1 IP reverso mal configurado;
7.1.4.12.4.2 Domínios inexistentes;
7.1.4.12.4.3 Permitir identificar e bloquear e-mails vindos de domínios recentemente cadastrados.

7.1.4.12.5 Deve permitir ao administrador criar filtros e assinaturas, bem como realizar atualização automática delas, em frequência de consulta configurada pelo administrador.

7.1.4.12.6 Permitir criação de políticas customizadas para tratamento de spam, vírus e filtragem de conteúdo, de acordo com o destinatário da mensagem;

7.1.4.12.7 Permitir configurar ações diferenciadas sobre as mensagens suspeitas, incluindo:
7.1.4.12.7.1 Aceitar;
7.1.4.12.7.2 Colocar em quarentena;
7.1.4.12.7.3 Inserir tag personalizada no assunto;
7.1.4.12.7.4 Marcar o cabeçalho.

7.1.4.12.8 A solução deve ser capaz de tomar as seguintes ações sobre as mensagens:
7.1.4.12.8.1 Alterar o assunto da mensagem;
7.1.4.12.8.2 Adicionar cabeçalhos para rastreamento;
7.1.4.12.8.3 Descartar a mensagem;
7.1.4.12.8.4 Colocar em uma determinada área de quarentena definida pelo administrador.

7.1.4.12.9 Deve permitir a criação de regras baseadas no idioma que as mensagens foram escritas, com capacidade de identificar no mínimo, português, inglês e espanhol;

7.1.4.12.10 Deve permitir a criação de regras baseadas por país;

7.1.4.12.11 Possuir a capacidade de criar filtros personalizados usando expressões regulares;

7.1.4.12.12 Permitir criação de blacklists e whitelists, com opção por domínio, subdomínio, endereço de e-mail e endereço IP;

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

7.1.4.12.14 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;

7.1.4.12.15 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”;

7.1.4.12.16 O fabricante da solução deve possuir consulta de reputação de IP de remetentes de e-mail. Esta consulta deve retornar os dados do remetente, com informações referentes à:

7.1.4.12.16.1 IP reverso e localização;

7.1.4.12.16.2 Registro em blacklists mundiais;

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

7.1.4.12.17 Capacidade de efetuar consultas externas ou internas na própria console da solução, para análise de endereço IP do remetente quantoa sua reputação, bem como verificação de spams e phishings recebidos e outros tipos de ameaças;

7.1.4.12.18 Deve ser capaz de realizar “Reverse DNS Lookup” (rDNS), para validação de fontes de e-mail;

7.1.4.12.19 Deve possuir suporte ao bloqueio de conexões de e-mails nocivos durante o diálogo SMTP, permitindo a economia de banda, armazenamento e otimização de processamento do appliance virtual, em especial baseado em lista local de bloqueio de conexão por: IP, e-mail, domínio, RBL’s e SPF;

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

7.1.4.12.21 Deve ter capacidade de proteção a spoofing de e-mail (tanto Spoofing de e-mails na entrada – quando o hacker utiliza o domínio da organização como remetente, como Spoofing de e-mails na saída – quando tem algum e-mail de saída que não esteja com o domínio da organização como remetente);

7.1.4.12.22 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;

7.1.4.12.23 Possuir mecanismo de "Spam Throttling" permitindo ao administrador limitar o fluxo de mensagens recebidas de origens com baixa reputação;

7.1.4.12.24 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;

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

7.1.4.12.26 Possuir controle de “Outbreak”, penalizando o remetente por um tempo configurável pelo administrador ao detectar:

7.1.4.12.26.1 Número excessivo de spams (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;

7.1.4.12.26.2 Número excessivo de vírus (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;

7.1.4.12.26.3 Número excessivo de ataques de dicionário (configurado pelo administrador) oriundos de uma mesma fonte de e-mail;

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

7.1.4.12.27.1 Fontes de ataques;
7.1.4.12.27.2 Ameaças encontradas.

7.1.4.13 **Da Proteção Contra Spam e Phishing**

7.1.4.13.1 Possuir filtro de antispam para detecção de spams usando no mínimo as seguintes tecnologias:
7.1.4.13.1.1 FingerPrint: Filtro por assinatura de spam;
7.1.4.13.1.2 Análise Heurística: Análise completa de toda mensagem contra spam, de acordo com as características da mensagem;
7.1.4.13.1.3 Análise de Documentos: Análise de documentos anexados na mensagem (PDF, DOC, DOCX e TXT);
7.1.4.13.1.4 Análise de Imagens: Filtragem de spam em imagens;
7.1.4.13.1.5 Filtro de URL: Filtragem por URL mal-intencionada contidas no corpo da mensagem, dessa forma combatendo possível e-mail Phishing;
7.1.4.13.2 Permitir ao administrador definir filtros por URL através de categorias, divididas por assunto, sendo possível definir uma pontuação. As seguintes categorias mínimas deverão estar contidas na solução:
7.1.4.13.2.1 Conteúdo pornográfico;
7.1.4.13.2.2 Abuso infantil;
7.1.4.13.2.3 Redes sociais;
7.1.4.13.2.4 Racismo e ódio;
7.1.4.13.2.5 Pesquisa de empregos;
7.1.4.13.2.6 Streaming de áudio;
7.1.4.13.2.7 Streaming de vídeo;
7.1.4.13.2.8 Esportes;
7.1.4.13.2.9 Notícias;
7.1.4.13.2.10 Compras Online.
7.1.4.13.3 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;
7.1.4.13.4 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;
7.1.4.13.5 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;

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

7.1.4.13.6.1 Recurso de Grey List;

7.1.4.13.6.2 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”;

7.1.4.13.6.3 Recurso de checagem por DMARC;

7.1.4.13.6.4 Recurso de checagem por assinatura DKIM;

7.1.4.13.6.5 Recurso de checagem de DNS Reverso;

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

7.1.4.13.6.7 Análise de reputação de IP;

7.1.4.13.6.8 Reputação de Mensagens;

7.1.4.13.6.9 Filtros de URL;

7.1.4.13.6.10 Filtro de anti-phishing;

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

7.1.4.13.6.12 Machine Learning.

7.1.4.13.7 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;

7.1.4.13.8 Possuir a possibilidade de criação de regras personalizadas de filtragem baseadas em:

7.1.4.13.8.1 Origens das mensagens;

7.1.4.13.8.2 Destino das mensagens;

7.1.4.13.8.3 Domínios;

7.1.4.13.8.4 Endereços de e-mails;

7.1.4.13.8.5 Expressões regulares (dicionário de palavras);

7.1.4.13.8.6 Fluxo;

7.1.4.13.8.7 Quantidade de mensagens;

7.1.4.13.8.8 Tamanho de anexo;

7.1.4.13.8.9 Número máximo de destinatários em uma única mensagem;

7.1.4.13.8.10 Tipo de arquivos em anexo;

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

7.1.4.13.8.12 Anexos criptografados;

7.1.4.13.8.13 Anexos compactados;

7.1.4.13.8.14 Níveis de compactação dos arquivos anexos;

7.1.4.13.8.15 Quantidade de anexos na mensagem;

7.1.4.13.8.16 Conteúdo HTML no corpo da mensagem.

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

7.1.4.13.9.1 “<form>”;

7.1.4.13.9.2 “<script>”;

7.1.4.13.9.3 “<iframe>”.

7.1.4.13.10 Possibilidade de criar regras para ações a serem tomadas pela ferramenta, quando as mensagens forem consideradas confiáveis e/ou Spams, permitindo ao administrador configurar nesses casos as seguintes ações:

7.1.4.13.10.1 Entregar direto o e-mail;

7.1.4.13.10.2 Colocar em quarentena;

7.1.4.13.10.3 Remover mensagem;

7.1.4.13.10.4 Auditar mensagem;

7.1.4.13.10.5 Encaminhar a mensagem;

7.1.4.13.10.6 Notificar o destinatário;

7.1.4.13.10.7 Adicionar header na mensagem;

7.1.4.13.10.8 Transformar HTML em texto simples.

7.1.4.13.11 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 certo período de tempo, mensagens a usuários inválidos/inexistentes no domínio;

7.1.4.13.12 Deve permitir a criação de regras 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, IP do remetente; campo header da mensagem, conteúdo no corpo da mensagem e url contidas no e-mail;

7.1.4.13.13 A solução deve permitir a utilização de quarentena por usuário, possibilitando que cada usuário cadastrado em um controlador de diretório LDAP ou Microsoft Active Directory, que esteja integrado com a solução, administre suas próprias mensagens categorizadas como spam;

7.1.4.13.14 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;

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

7.1.4.13.16 Possuir proteção contra bounce e-mail attack através “Bounce Address Tag Verification”;

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

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

7.1.4.13.19 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 como, no mínimo:

7.1.4.13.19.1 Microsoft Exchange.

7.1.4.14 **Da Proteção Contra Vírus**

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

7.1.4.14.2 Deverá ser capaz de filtrar vírus nos dois sentidos de tráfego (entrada e saída de e-mail);

7.1.4.14.3 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;

7.1.4.14.4 A solução deve possuir, no mínimo, duas engines de antivírus e antimalware já integrados na solução sem custo adicional;

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

7.1.4.14.5.1 Dia-zero (zero-day);

7.1.4.14.5.2 Vírus outbreak;

7.1.4.14.5.3 Hora-zero (Zero-hour);

7.1.4.14.5.4 Targeted Attack Protection

7.1.4.14.5.5 APT - advanced persistent threat.

7.1.4.14.5.6 Tomar no mínimo as seguintes ações:

7.1.4.14.5.7 Descartar a mensagem;

7.1.4.14.5.8 Colocar em uma determinada área da quarentena definida pelo administrador.

7.1.4.15 **Das Notificações de Quarentena Individual do Usuário**

7.1.4.15.1 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;

7.1.4.15.2 Grupos diferentes de usuários devem poder receber a notificação em horários diferentes;

7.1.4.15.3 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, das seguintes informações:

7.1.4.15.3.1 E-mail de origem;

7.1.4.15.3.2 Título/Assunto do e-mail;

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

7.1.4.15.3.4 Logomarca do digest;

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

7.1.4.15.4.1 Liberar uma mensagem bloqueada;

7.1.4.15.4.2 Bloquear o remetente da mensagem (blacklist), para que as futuras mensagens dele já sejam barradas;

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

7.1.4.15.4.4 Reportar o bloqueio indevido;

7.1.4.15.4.5 Solicitar envio de novo resumo;

7.1.4.15.4.6 Acessar sua área de quarentena.

7.1.4.15.5 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);

7.1.4.15.6 A solução deverá permitir ao administrador selecionar quais ações serão liberadas para o usuário final selecionar, no mínimo:

7.1.4.15.6.1 Liberar e-mail;

7.1.4.15.6.2 Reportar Falso Positivo;

7.1.4.15.6.3 Incluir o remetente do e-mail em blacklist individual (do próprio usuário);

7.1.4.15.6.4 Incluir o remetente do e-mail em whitelist individual (do próprio usuário);

7.1.4.15.6.5 Visualizar o e-mail.

7.1.4.16 **Do Disclaimer**

7.1.4.16.1 Deve possuir a capacidade de incluir “disclaimers” nas mensagens enviadas;

7.1.4.16.2 A solução deverá suportar aplicação de “disclaimers” diferenciados para usuários e grupos diferentes através da integração com o serviço de diretório LDAP ou Microsoft Active Directoy;

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

7.1.4.17 **Da Prevenção Contra Roubo de Informações (DLP – Data Loss Prevention) e Conformidade**

7.1.4.17.1 Deve possuir módulo DLP (Data Loss Prevention) do próprio fabricante, já integrado na solução, sem a necessidade de licenciamento adicional, ou seja, já licenciado com a mesma quantidade de caixas postais da solução de proteção de e-mail;

7.1.4.17.2 O módulo de DLP deve analisar todo conteúdo da mensagem a fim de 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;

7.1.4.17.3 Deve permitir criar regras de conformidade “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:

7.1.4.17.3.1 Identificação de CPF;

7.1.4.17.3.2 Número de cartão de crédito;

7.1.4.17.3.3 CNPJ.

7.1.4.17.3.4 As regras de conformidade podem ser criadas utilizando os termos dos dicionários definidos e que estejam nos seguintes campos da mensagem, podendo ser definido o número de ocorrências mínimas para execução da regra:

7.1.4.17.3.5 Cabeçalho;

7.1.4.17.3.6 URL (contidas no e-mail);

7.1.4.17.3.7 Corpo do e-mail;

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

7.1.4.17.4 Permitir ao administrador criar regras de conformidade 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;

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

7.1.4.17.4.2 Entregar a mensagem;

7.1.4.17.4.3 Não entregar a mensagem;

7.1.4.17.4.4 Armazenar a mensagem para auditoria;

7.1.4.17.4.5 Notificar remetente e destinatário da mensagem;

7.1.4.17.4.6 Encaminhar a mensagem para outro destinatário.

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

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

7.1.4.18 **Da Criptografia de E-mail**

7.1.4.18.1 Deve possuir módulo de criptografia do próprio fabricante, já integrado na solução, sem a necessidade de licenciamento adicional, ou seja, já licenciado com a mesma quantidade de caixas postais da solução de proteção de e-mail;

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

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

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

7.1.4.18.4.1 Assunto;

7.1.4.18.4.2 Destinatário;

7.1.4.18.4.3 E-mail do Remetente;

7.1.4.18.4.4 Nome do Anexo.

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

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

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

7.1.4.18.8 Deve possibilitar ao administrador indicar se o destinatário poderá responder o e-mail;

7.1.4.18.9 Deve possibilitar ao administrador indicar se o destinatário poderá encaminhar o e-mail.

7.1.4.19 **Da Proteção Contra Ataques Dirigidos (TAP – Targeted Attack Protection)**

7.1.4.19.1 Deverá prover proteção contra ataques dirigidos tais como:

7.1.4.19.1.1 Spear-phishing;

7.1.4.19.1.2 Ataques Zero-Day;

7.1.4.19.1.3 Ameaças avançadas persistentes (APTs).

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

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

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

7.1.4.19.5 Análise Estática (Análise de código): Verificação de comportamento suspeito, scripts escondidos, partes de códigos maliciosos e redirecionamento a outros sites maliciosos;

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

7.1.4.19.7 Possuir, dentro da solução, um dashboard do módulo de Segurança contra-ataques dirigidos;

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

7.1.4.19.8.1 Detecção - A análise de e-mail 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;

7.1.4.19.8.2 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;

7.1.4.19.8.3 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 possam sofrer, passando para usuários específicos, dispondo de ferramentas para ajudar a remediar danos, tudo baseado em um painel de controle online.

7.1.4.19.9 Não será aceita solução baseada apenas em reputação de URL;

7.1.4.19.10 A solução deve conter engine para detecção de Anomalias, não podendo se limitar a análise com definições baseadas em ataques já conhecidos;

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

7.1.4.19.11.1 E-mail do Destinatário;

7.1.4.19.11.2 E-mail do Remetente;

7.1.4.19.11.3 Domínio de Origem;
7.1.4.19.11.4 Domínio de Destino;
7.1.4.19.11.5 IP/Rede;
7.1.4.19.11.6 Range de IP;
7.1.4.19.11.7 Expressão Regular;
7.1.4.19.11.8 Usuários;
7.1.4.19.11.9 Listas de distribuição;
7.1.4.19.11.10 Grupo de LDAP.

7.1.4.19.12 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 deverá ser bloqueado para acesso;

7.1.4.19.13 O sistema deverá ser capaz de varrer anexos, com no mínimo, tipos PDF, arquivos em Flash para payloads maliciosos e microsoft office;

7.1.4.19.14 Ao detectar arquivos maliciosos, deverá ser capaz de configurar regras para descartar e salvar uma cópia na quarentena;

7.1.4.19.15 Deve possuir tecnologia SandBox local do mesmo fabricante ou em nuvem do próprio fabricante no Brasil, desde que esteja em conformidade com todas as regras da legislação vigente brasileira (Lei Geral de Proteção de Dados Pessoais);

7.1.4.19.16 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, caso o administrador opte por este serviço. Este sistema de SandBox deve conter tecnologia de detecção usando “Análise Comportamental” do arquivo identificando assim malwares e variantes sem a necessidade de assinaturas;

7.1.4.19.17 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;

7.1.4.19.18 A proteção URL deverá reescrever links para os protocolos HTTP, HTTPS, FTP e URL's que comecem com “www” independente do protocolo;

7.1.4.19.19 A solução deverá permitir que o administrador configure o sistema de proteção URL para que reescreva todas as mensagens que contiverem URL e envie ao sandbox para testes garantindo um alto nível de segurança;

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

7.1.4.19.21 No Dashboard da solução deve ser possível:

7.1.4.19.21.1 Exibir o número de cliques em cada ameaça;
7.1.4.19.21.2 Exibir qual usuário clicou na URL detectada como ameaça;
7.1.4.19.21.3 Exibir informações atualizadas sobre as ameaças detectadas;
7.1.4.19.21.4 Exibir a classificação da mensagem

7.1.4.19.21.5 Exibir status atualizado e detalhado sobre as ameaça com no mínimo com as seguintes informações:

7.1.4.19.21.6 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;

7.1.4.19.21.7 Bloqueado - Número de vezes que o modulo de Proteção URL impediu o usuário de acessar o site malicioso;

7.1.4.19.21.8 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.

7.1.4.19.22 Exibir timeline das ameaças, exibindo quando foi recebida, identificada e quando foi clicada ou liberada;

7.1.4.19.23 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;

7.1.4.19.24 Possuir ferramenta para bloqueio ou liberação de URL pelo administrador da ferramenta;

7.1.4.19.25 Possuir ferramenta para bloqueio ou liberação do IP pelo administrador da ferramenta;

7.1.4.19.26 Possuir ferramenta para bloqueio ou liberação do arquivo pelo administrador da ferramenta;

7.1.4.19.27 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;

7.1.4.19.28 Disponibilizar sistema de coleta (report) de amostra do IP para análise da engenharia do fabricante;

7.1.4.19.29 Ao administrador enviar uma amostra de um arquivo para análise e visualizar o retorno de todas as ocorrências encontradas para esse arquivo.

7.1.4.19.30 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 reports enviados pelos usuários, ficando a cargo do administrador decidir pelo bloqueio ou a liberação de tal URL e/ou Arquivo;

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

7.1.4.19.31.1 JavaScript;

7.1.4.19.31.2 Links;

7.1.4.19.31.3 Executáveis;

7.1.4.19.31.4 VB Script.

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

7.1.4.19.32.1 pdf;

7.1.4.19.32.2 doc;

7.1.4.19.32.3 docx;

7.1.4.19.32.4 ppt;

7.1.4.19.32.5 pptx;
7.1.4.19.32.6 xls;
7.1.4.19.32.7 xlsx.

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

7.1.4.19.34 O SandBox do fabricante deve ter a capacidade de analisar arquivos, mesmo que estejam inseridos em arquivos compactados, do tipo:

7.1.4.19.34.1 .swf;
7.1.4.19.34.2 .pdf;
7.1.4.19.34.3 .doc;
7.1.4.19.34.4 .xls;
7.1.4.19.34.5 .xlsx;
7.1.4.19.34.6 .ppt;
7.1.4.19.34.7 .ppt;
7.1.4.19.34.8 .pptx;
7.1.4.19.34.9 .rtf.

7.1.4.19.35 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 e Belize;

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

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

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

7.1.4.20 **Do Sistema de Proteção a Fraude de E-mail**

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

7.1.4.20.1.1 Pontuar;
7.1.4.20.1.2 Ignorar;
7.1.4.20.1.3 Bloquear.

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

7.1.4.20.2.1 Pontuar;
7.1.4.20.2.2 Ignorar;
7.1.4.20.2.3 Bloquear.

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

7.1.4.20.4 Deve possuir sistema de detecção de e-mails oriundos de servidores de e-mails gratuitos tais como Google, Yahoo, Hotmail, etc, para serem usados em regras personalizadas de filtragem;

7.1.4.20.5 Nativamente deve possuir sistema de detecção de e-mails externos (e-mails de entrada) que tentem utilizar o domínio da própria organização como remetente, sem necessidade de criação de regra específica para este tipo de fraude.

7.1.4.21 **Do Archiving e Auditoria de E-mail**

7.1.4.21.1 O sistema deve permitir o armazenamento de cópia da mensagem original;

7.1.4.21.2 O sistema deverá possuir uma interface de gerenciamento web via HTTPS, onde será possível administrar toda solução;

7.1.4.21.3 Será permitido soluções de gerenciamento unificadas com a "Solução de Segurança para Serviço de E-mail" ou soluções de terceiros desde que devidamente licenciadas e passíveis de integração com a "Solução de Segurança para Serviço de E-mail" e com o sistema de correio Eletrônico Microsoft Exchange;

7.1.4.21.4 O sistema deve permitir o armazenamento de todas as mensagens de entrada e de saída da rede de dados da contratante, bem como ter a capacidade de armazenar os e-mails internos trafegados dentro da empresa;

7.1.4.21.5 Deve permitir a integração com sistema de correio Microsoft Exchange para o armazenamento dos e-mails trafegados no domínio interno da empresa. Esta integração pode ser feita através de uma conta especifica no Exchange usando o protocolo POP3 ou através do uso de conectores para o envio e recebimento das mensagens utilizando protocolo SMTP/TLS;

7.1.4.21.6 A solução deve permitir integração com a "Solução de Segurança para Serviço de E-mail" através do protocolo SMTP/TLS para armazenamento das mensagens ou caso a solução seja do mesmo fabricante será permitido integração através de protocolo proprietário da solução;

7.1.4.21.7 O sistema deve permitir que o administrador configure o tempo de armazenamento e o "rotacionamento" automático das mensagens utilizando pelo menos os seguintes critérios:

- 7.1.4.21.7.1 Por número de dias;
- 7.1.4.21.7.2 Por número de meses;
- 7.1.4.21.7.3 Por número de anos;
- 7.1.4.21.7.4 Por volume de armazenamento de dados em MB/GB.

7.1.4.21.8 A solução deve permitir a realização de backup dos dados para um sistema de backup externo. Serão aceitas soluções que permitam exportar os dados para um compartilhamento externo ou que permitam a instalação de agente de backup;

7.1.4.21.9 O sistema deve possuir console de administração possibilitando a consulta das mensagens armazenadas, efetuando busca por pelo menos os seguintes campos:

- 7.1.4.21.9.1 ID da mensagem;
- 7.1.4.21.9.2 IP de Origem da mensagem;

7.1.4.21.9.3 Assunto do e-mail;
7.1.4.21.9.4 De;
7.1.4.21.9.5 Para;
7.1.4.21.9.6 Palavras contidas no corpo da mensagem;
7.1.4.21.9.7 Nome de anexo;
7.1.4.21.9.8 Data;
7.1.4.21.9.9 Tamanho da mensagem;
7.1.4.21.9.10 Cabeçalhos da mensagem.

7.1.4.21.10 O sistema deve permitir auditoria completa das mensagens incluindo a possibilidade do Download da mensagem original e/ou seus anexos;

7.1.4.21.11 Deve ser possível criar usuários com permissões distintas a fim de limitar o acesso às informações, desta forma a solução deverá possuir no mínimo os seguintes perfis de acesso:

7.1.4.21.12 Permitir definir o domínio/e-mail que um usuário pode ter acesso;

7.1.4.21.13 Definir se o usuário deverá ou não ter acesso ao conteúdo da mensagem/anexos;

7.1.4.21.14 Permitir a criação de usuários para administração da ferramenta de forma granular, ou seja, definir quais áreas do sistema o usuário poderá ter acesso.

7.1.4.21.15 Deve ser compatível com as principais normas de segurança da informação tais como: LGPD;

7.1.4.21.16 Permitir auditoria completa das ações realizadas pelos administradores na interface Web com no mínimo o registro das seguintes ações: Login, Acesso a mensagem, Visualização e Download da Mensagem e Modificações de configurações de parâmetros da solução;

7.1.4.21.17 Possibilitar o encaminhamento (envio) da Mensagem armazenada;

7.1.4.21.18 Permitir integração com os Serviços de Diretórios para acesso a solução: Microsoft AD, LDAP;

7.1.4.21.19 Possibilidade de gerar relatórios dos e-mails armazenados com as seguintes opções:

7.1.4.21.19.1 Data;
7.1.4.21.19.2 Origem/Destino;
7.1.4.21.19.3 Domínio.

7.1.4.21.20 Qual a categoria a mensagem recebeu, dentre elas no mínimo:

7.1.4.21.20.1 DLP;
7.1.4.21.20.2 Provável SPAM;
7.1.4.21.20.3 SPAM;
7.1.4.21.20.4 Vírus;
7.1.4.21.20.5 Conteúdo Bloqueado;
7.1.4.21.20.6 Whitelist;
7.1.4.21.20.7 Blacklist;
7.1.4.21.20.8 Tamanho Excedido;
7.1.4.21.20.9 Phishing.

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

7.1.5 Requisitos de projeto e implementação:

7.1.5.1 A instalação terá um prazo máximo de 30 (trinta) dias úteis após a data de assinatura do contrato;

7.1.5.2 A empresa vencedora procederá com a instalação na supervisão de técnicos da SGI (Superintendência de Gestão Técnica da Informação – ANEEL) e, sendo posteriormente aferido e testado o seu perfeito funcionamento;

7.1.5.3 Compreende-se, nesta etapa, a instalação de sistemas, softwares e aplicativos dos PRODUTOS fornecidos pela CONTRATADA, bem como a migração das configurações existentes na ANEEL para os novos PRODUTOS;

7.1.5.4 A CONTRATADA deve elaborar um documento de planejamento de instalação para aprovação da ANEEL antes da execução da instalação;

7.1.6 Requisitos de metodologia de trabalho:

7.1.6.1 Realização de Reunião Inicial previamente à entrega da solução e execução dos serviços de instalação;

7.1.6.2 Reuniões entre a ANEEL e CONTRATADA para discussão de assuntos referentes às instalações em execução e acompanhamento do cronograma;

7.1.6.3 Execução das etapas demandadas e posterior aceite/rejeição pela equipe de fiscalização da contratação e o Gestor do Contrato;

7.1.6.4 Profissional qualificado da CONTRATADA deverá realizar o repasse de conhecimento para operacionalização e administração diária da solução fornecida, direcionada à equipe técnica da ANEEL, logo após a homologação da solução por parte da ANEEL e em data a ser combinada, com duração mínima de 4 (quatro) horas, contemplando no mínimo os seguintes aspectos:

7.1.6.4.1 Administração diária da solução;
7.1.6.4.2 Configurações de MTA;
7.1.6.4.3 Configurações de políticas e regras de spam, phishing, DLP, criptografia, anti-APT, fraude de email, antivirus;
7.1.6.4.4 Configuração de quarentena de usuário e da solução;
7.1.6.4.5 Pesquisa de e-mails e logs da solução;
7.1.6.4.6 Monitoramento de estatísticas da solução;
7.1.6.4.7 Geração de relatórios;
7.1.6.4.8 Backup de configurações;
7.1.6.4.9 Procedimentos de atualização de firmware;
7.1.6.4.10 Teste de comunicações com a infraestrutura do fabricante;
7.1.6.4.11 Submissão de spams ao fabricante;

7.1.6.5 Prestar o serviço objeto desta contratação nos horários estipulados pelo órgão, ou em outro horário, mediante negociação com a ANEEL, inclusive feriados e nos finais de semana;

7.1.6.6 Fornecer número telefônico para contato e registro de ocorrências sobre o acompanhamento do serviço contratado;

7.1.6.7 Emitir e entregar os certificados de garantia dos softwares e serviços.

7.1.7 Requisitos legais:

7.1.7.1 Lei Federal nº 8.666/1993: Institui normas para licitações e contratos da Administração Pública e dá outras providências;

7.1.7.2 Lei Federal nº 10.520/2002: Institui no âmbito da União, Estados, Distrito Federal e Municípios, a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;

7.1.7.3 Decreto nº 7.746/2012: Regulamenta o art. 3º da Lei no 8.666, de 21 de junho de 1993, para estabelecer critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável nas contratações realizadas pela administração pública federal, e institui a Comissão Interministerial de Sustentabilidade na Administração Pública - CISAP;

7.1.7.4 Decreto nº 7.174/2010: Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal;

7.1.7.5 Decreto nº 10.024/2019: Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal;

7.1.7.6 Instrução Normativa SLTI-MPOG nº 01/2019: Dispõe sobre Plano Anual de Contratações de bens, serviços, obras e soluções de tecnologia da informação e comunicações no âmbito da Administração Pública federal direta, autárquica e fundacional e sobre o Sistema de Planejamento e Gerenciamento de Contratações.

7.1.7.7 Instrução Normativa SGD/ME nº 31/2019: Altera a Instrução Normativa nº 1, de 4 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

7.1.8 Requisitos sociais e culturais: Não se aplica

7.1.9 Requisitos de capacitação da equipe de fiscalização e gestão do contrato, representante de TIC na UORG e/ou usuário da solução: Não se aplica

7.1.10 Requisitos de capacitação dos profissionais da CONTRATADA associados à execução do objeto:

7.1.10.1 A CONTRATADA deverá possuir, durante a vigência do contrato, profissionais certificados na administração e suporte pelo fabricante da solução.

7.1.10.2 **Requisitos de Garantia**

7.1.10.2.1 A CONTRATADA deverá oferecer garantia por 12 (doze) meses para a solução CONTRATADA, estando disponível para acionamento 24 horas por dia, 7 dias por semana (24x7);

7.1.10.2.2 A subscrição deve ser fornecida com licenciamento e garantia de atualização de softwares para o período da contratação;

7.1.11 Requisitos temporais:

7.1.11.1 A CONTRATADA deverá fornecer os produtos instalados e em produção no ambiente computacional da ANEEL em no máximo 30 (trinta) dias úteis após a assinatura do contrato;

7.1.11.2 A CONTRATADA deverá realizar o repasse de conhecimento em até 10 (dez) dias úteis após a data do recebimento definitiva da solução pela ANEEL;

7.1.11.3 A CONTRATADA deverá iniciar o serviço de garantia e suporte técnico da solução a contar da data de emissão do Termo de Recebimento Definitivo em conformidade com o estabelecido neste Termo de Referência, devendo ser prestados durante a vigência de 12 (doze) meses.

7.1.11.4 A subscrição do licenciamento e garantia da solução terão vigência de 12 (doze) meses e ANEEL terá direito a toda e qualquer nova atualização do software, sejam versões, patches, hotfixes ou assinaturas e subscrições de segurança que fizerem parte da solução durante esse período.

7.1.12 Requisitos de segurança da informação e privacidade:

7.1.12.1 A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da ANEEL e aos padrões estabelecidos pela ISO 17799;

7.1.12.2 A solução deve ser mantida atualizada para assegurar sua disponibilidade e integridade continuadas;

7.1.12.3 O serviço deve passar por manutenção de acordo com os intervalos e especificações de serviço recomendados pelo fornecedor e acordados com a CONTRATADA;

7.1.12.4 Devem ser mantidos registros sobre todas as falhas ocorridas ou suspeitadas e sobre todas as manutenções preventivas e corretivas;

7.1.12.5 Controles apropriados devem ser realizados quando se enviar informações (logs/mensagens), isto é, devem ser verificadas as identidades de emissor e destinatário (sejam eles pessoas ou máquinas), assim como deve ser certificado se o conteúdo destas informações deve realmente ser compartilhado entre tais entes.

7.1.12.6 Os produtos deverão apresentar política de privacidade oferecida pelo fabricante a fim de garantir o sigilo dos dados consultados através dos softwares licenciados.

7.1.12.7 A CONTRATADA se compromete a manter sigilo absoluto em relação a todos os dados gerados no processo de prestação dos serviços.

7.1.12.8 A solução deverá prever a geração de trilhas de auditoria para todas as operações de inclusão, exclusão, alteração de dados, desligamento do ambiente e alteração de configuração do sistema.

7.1.12.9 A CONTRATADA deverá realizar quando solicitado e em conjunto com a ANEEL uma análise de impacto na privacidade dos dados pessoais relacionada ao objeto da contratação, considerando o descrito pelo relatório de impacto à proteção de dados pessoais, conforme previsto na Lei 13.709/2018, quando da concepção de qualquer novo projeto, produto ou serviço.

7.1.12.10 A CONTRATADA deverá realizar e apresentar à ANEEL, quando solicitado, uma análise/avaliação de riscos dos recursos de processamento da informação, sistemas de segurança da informação e quaisquer outros ativos relacionados ao objeto do contrato, indicando o nível de risco ao qual o objeto do contrato e a Contratante está exposta, baseada em análise de vulnerabilidades, resguardando os segredos de negócio, direitos autorais e direitos de propriedade intelectual aplicáveis, conforme metodologia indicada pela Contratante.

7.1.12.11 A CONTRATADA deverá apresentar em tempo determinado pela ANEEL:

7.1.12.11.1 Documentação que descreve a arquitetura física e lógica do objeto;

7.1.12.11.2 Uma descrição dos controles de segurança cibernética implementados em cada componente descrito na arquitetura física e lógica;

7.1.12.11.3 Matriz de responsabilidades descrevendo os papéis e suas respectivas responsabilidades pela segurança cibernética relacionada ao objeto da contratação e com relação aos itens aqui descritos.

7.1.12.12 A CONTRATADA deverá utilizar recursos de segurança cibernética e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e, sempre que possível, em versões comprovadamente seguras e atualizadas, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a ANEEL está exposta, considerando os critérios de aceitabilidade de riscos definidos pela ANEEL.

7.1.12.13 A CONTRATADA deverá assegurar que os ambientes tecnológicos de desenvolvimento, teste, homologação e produção estejam segregados e possuam controles de segurança cibernética adequados a cada ambiente, de forma a para reduzir o nível de riscos de acessos ou modificações não autorizadas.

7.1.12.14 A CONTRATADA deverá possuir e implementar processo de gestão de mudanças adequado para que mudanças na organização, nos processos de negócio e nos recursos de processamento da informação sejam controlados e não afetem a segurança cibernética, reduzindo o nível de risco ao qual o objeto do contrato e/ou a ANEEL está exposta, considerando os critérios de aceitabilidade de riscos definidos pela ANEEL.

7.1.12.15 A CONTRATADA deve possuir um processo de Gestão de Incidentes que registre os incidentes de segurança cibernética ocorridos e que guarde informações como: a descrição dos incidentes ou eventos, as informações e sistemas envolvidos, as medidas técnicas e de segurança utilizadas para a proteção das informações, os riscos relacionados ao incidente e as medidas tomadas para mitigá-los e evitar reincidências; além de implementar e manter controles e procedimentos específicos para detecção, tratamento e resposta a incidentes de segurança cibernética, de forma a reduzir o nível de risco ao qual o objeto do contrato e/ou a ANEEL está exposto, considerando os critérios de aceitabilidade de riscos definidos pela ANEEL.

7.1.12.16 A CONTRATADA deve implementar os controles necessários para o registro de eventos e incidentes de segurança cibernética.

7.1.12.17 A CONTRATADA deve reportar de imediato à ANEEL incidentes que envolvam vazamento de dados, fraude ou comprometimento da informação relacionados ao objeto do contrato.

7.1.12.18 A CONTRATADA deve implementar os controles necessários para coleta e preservação de evidências de incidentes de segurança.

7.1.12.19 A CONTRATADA deverá implementar controles de acesso baseado em uma política de controle de acesso para o objeto contratado, elaborada pela Contratante em conjunto com a CONTRATADA, tendo em vista o princípio do menor privilégio e a proteção adequada aos dados pessoais, de forma a reduzir o nível de risco ao qual o objeto e a Contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela Contratante.

7.1.12.20 A política deve estabelecer, dentre outros critérios, que se deve conceder autorizações de acesso apenas quando realmente sejam necessárias para o desempenho de uma atividade específica, definindo também protocolos para cadastramento, mecanismo de controle de acesso (como, por exemplo, validação de formulário), habilitação, inabilitação, atualização de direitos de acesso e exclusão de usuário, além de revisões periódicas da política. A política também deve definir situações e protocolos para acesso a informações sensíveis, necessidades de não repúdio, situações que requerem autenticação via duplo fator e acesso via certificado digital, nos casos e que a Contratante julgar necessário.

7.1.12.21 A CONTRATADA deverá apresentar à ANEEL, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados, de forma a assegurar a auditabilidade do objeto contratado, bem como demais dispositivos legais aplicáveis.

7.1.12.22 A CONTRATADA deverá disponibilizar todos os recursos necessários para que a ANEEL, ou outra entidade por ela indicada, realize atividade continuada de auditoria de segurança cibernética relacionadas ao objeto do contrato.

7.1.12.23 A CONTRATADA deve implementar e manter controles específicos para registro de eventos e rastreabilidade de forma a manter trilha de auditoria de segurança cibernética, aderente a disposto em dispositivo legal correlato publicado pelo GSI/PR, de forma a assegurar a rastreabilidade das ações de usuário por meio de logs de transações e de acesso aos sistemas, conforme especificação de requisitos, e gerá-los e disponibilizá-los à Contratante para fins de auditorias e inspeções.

7.1.12.24 A CONTRATADA deve implementar medidas de salvaguarda para os logs descritos no item anterior, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas relacionados ao objeto do contrato, de forma que esses não tenham permissão de exclusão ou desativação dos registros (logs) de suas próprias atividades.

7.1.12.25 A CONTRATADA deve implementar e manter controles e procedimentos específicos para assegurar o completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da CONTRATADA venham tomar conhecimento em razão da execução do contrato, de forma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da solução objeto do contrato, cumprindo e fazendo cumprir o disposto nos acordos de confidencialidade firmados, partes integrantes deste documento.

7.1.12.26 A CONTRATADA deverá comunicar à ANEEL, de imediato, a ocorrência de transferência, remanejamento ou demissão de funcionário, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da ANEEL, porventura colocados à disposição para realização dos serviços contratados.

7.1.13 Requisitos socioambientais:

7.1.13.1 A CONTRATADA deverá atender, no que couber, os critérios de sustentabilidade ambiental;

7.1.13.2 Os serviços deverão ser prestados de acordo com os critérios de sustentabilidade ambiental contidos na Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MPOG e no Decreto nº 7.746/2012, no que couber, observando os itens que fazem parte dos programas da ANEEL.

7.1.13.3 A CONTRATADA deverá cumprir, no que couber, as exigências do inciso XI, art. 7° da Lei 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos – PNRS.

7.1.14 MODELO DE EXECUÇÃO E GESTÃO

7.1.14.1 **Forma de execução:** Parcela única

7.1.14.2 **O início da execução do objeto ocorrerá logo após:**

7.1.14.2.1 ☐ O aceite ou retirada da Nota de empenho pela CONTRATADA.

7.1.14.2.2 ☒ A assinatura do Contrato pelas partes.

7.1.14.2.3 ☐ O aceite ou retirada da Ordem de Serviço – OS pela CONTRATADA.

7.1.14.2.4 ☐ O recebimento do Ofício, e-mail ou fax pela CONTRATADA.

7.1.14.3 **Produto(s)**:

7.1.14.3.1 A CONTRATADA deverá fornecer o(s) software(s) que compõe(em) a solução de filtragem de antispam devidamente instalado(os) e operacional(nais) conforme as especificações técnicas deste Termo de Referência;

7.1.14.3.2 A CONTRATADA deverá fornecer um documento constando o PLANO DE INSTALAÇÃO dos softwares da solução para atender as necessidades da ANEEL antes do início da instalação da solução.

7.1.14.3.3 A CONTRATADA deverá fornecer ao final da instalação a documentação AS-BUILT, contendo o detalhamento da instalação e configurações realizadas na solução, inclusive o checklist completo dos softwares entregues, instalados e configurados na ANEEL;

7.1.14.3.4 A CONTRATADA deverá fornecer um TERMO DE GARANTIA comprovando que o(os) software(s) que compõe(em) a solução está (ão) coberto(s) pela garantia do fabricante, pelo prazo mínimo de 12 (doze) meses, contados a partir da emissão do Termo de Recebimento Definitivo emitido pela ANEEL.

7.1.14.4 **Metodologia para estimativa de demandas**: O fornecimento da solução deverá atender ao quantitativo de 4.100 (quatro mil e cem) caixas postais, que corresponde à atual quantidade de caixas postais eletrônicas institucionais e de usuários do serviço de correio eletrônico da Agência.

7.1.14.5 **Local, dias e horários para a prestação:** Os serviços deverão ser prestados fisicamente na ANEEL, de Segunda a Sexta, 8h00/17h00.

7.1.14.6 **O objeto compreenderá:**

7.1.14.6.1 **Entrega:**

7.1.14.6.1.1 A entrega da solução instalada, configurada e em produção na ANEEL deverá ser realizada em até 30 (trinta) dias úteis após a data de assinatura do contrato. Os serviços de garantia e suporte técnico se iniciarão logo após a data do recebimento definitivo da solução pela ANEEL e terão a vigência de 12 (doze) meses.

7.1.14.6.2 **Instalação:**

7.1.14.6.2.1 A instalação da solução deverá ser realizada fisicamente na ANEEL, de segunda-feira a sexta-feira, das 08hs às 17hs.

7.1.14.6.3 **Implantação:**

7.1.14.6.3.1 Caberá à CONTRATADA a disponibilização de todos os recursos necessários, tais como softwares e recursos humanos necessários à instalação e implantação dos PRODUTOS;

7.1.14.6.3.2 A CONTRATADA realizará adequação/configuração dos PRODUTOS fornecidos ao longo da etapa de migração e realização de novas configurações;

7.1.14.6.3.3 A CONTRATADA deverá fornecer todas as licenças necessárias dos PRODUTOS ofertados e dos elementos adicionais que se fizerem necessários à instalação/migração e ao pleno funcionamento do ambiente de produção.

7.1.14.6.3.4 A etapa de implantação e migração deve acontecer de forma gradual e transparente, de acordo com a conveniência da ANEEL;

7.1.14.6.3.5 Durante a implantação e migração, a CONTRATADA deverá realizar, entre outras atividades:

7.1.14.6.3.6 Atualização inicial de firmware, software e/ou patches, caso necessário, para que a versão de instalação corresponda com a última versão válida disponibilizada pelo fabricante;

7.1.14.6.3.6.1 Configurações básicas;
7.1.14.6.3.6.2 Acompanhamento de migrações de regras e políticas;
7.1.14.6.3.6.3 Elaboração e execução de scripts;
7.1.14.6.3.6.4 Análise de performance;
7.1.14.6.3.6.5 Resolução de problemas.

7.1.14.6.3.7 Durante a etapa de implantação e migração, os PRODUTOS fornecidos pela CONTRATADA serão colocados em plena operação, em condições reais de produção;

7.1.14.6.3.8 Durante esta etapa, a equipe da CONTRATADA deverá estar presente, nos horários de implantação e migração definidos pela ANEEL;

7.1.14.6.3.9 Caberá a ANEEL o acompanhamento da migração, fornecimento de informações sobre os aplicativos e ferramentas existentes no ambiente, bem como a definição e concessão de janelas de intervenção;

7.1.14.6.3.10 As atividades de implantação e migração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou final de semana;

7.1.14.6.3.11 A CONTRATADA deve garantir que a migração não irá alterar as versões ou o funcionamento dos serviços instalados na unidade objeto da migração, sem a prévia autorização da ANEEL;

7.1.14.6.3.12 A CONTRATADA deverá, com a supervisão da ANEEL, planejar e realizar a instalação dos softwares com total interoperabilidade operacional com ambiente atual da ANEEL, sem impacto no ambiente de produção;

7.1.14.6.4 **Manutenção e Suporte Técnico**

7.1.14.6.4.1 **Do serviço de suporte técnico**

7.1.14.6.4.1.1 O serviço de suporte técnico consiste na realização de manutenção preventiva e corretiva de todos os itens da especificação técnica do objeto;

7.1.14.6.4.1.2 A execução do serviço de suporte técnico deverá ser realizada pela CONTRATADA por meio de profissional certificado nos conhecimentos de administração e suporte técnico pelo fabricante da solução sem custos adicionais para o CONTRATANTE, durante o

período de licenciamento, suporte técnico e garantia, sendo indispensável a apresentação de documentação original do fabricante que comprove a validade da certificação enquanto durar o vínculo contratual, podendo ser solicitada a qualquer momento;

7.1.14.6.4.1.3 O serviço de suporte técnico deverá ser realizado em regime de 24 (vinte e quatro) horas por 7 (sete) dias por semana, todos os dias do ano, no idioma português, devendo a empresa possuir uma central de atendimento sem custos para o CONTRATANTE.

7.1.14.6.4.1.4 O atendimento deverá ser categorizado em quatro níveis. A CONTRATADA deverá garantir tempo máximo de atendimento e restauração de serviço, conforme a tabela acima.

7.1.14.6.4.1.5 O CONTRATANTE fará a "abertura de chamados" técnicos através de ligação telefônica ou via web, em período integral 24 (vinte e quatro) horas por dia 07 (sete) dias por semana. A CONTRATADA deverá informar o número do telefone em sua proposta. Se a Central de Suporte estiver localizada fora de Brasília, a CONTRATADA deverá informar o DDG (discagem direta gratuita 0800). O acesso à área restrita de suporte em endereço eletrônico (web site) deverá estar disponível, também, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

7.1.14.6.4.1.6 A CONTRATADA deverá disponibilizar suporte técnico de toda a solução, através da forma de atendimento remoto, em período integral – 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, pelo período de garantia da solução.

7.1.14.6.4.1.7 A CONTRATADA deverá disponibilizar acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (web site) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, com pesquisa efetuada através de ferramentas de busca) e atualizações.

7.1.14.6.4.1.8 A CONTRATADA deverá prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da ANEEL, em relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações.

7.1.14.6.4.1.9 No caso de chamados com nível de severidade 4 (ordens de serviço), o chamado deverá conter a descrição dos serviços a serem executados de forma a facilitar elaboração da OS. Caberá à

CONTRATADA, com apoio do CONTRATANTE, o detalhamento do serviço a ser executado, incluindo requisitos funcionais e não funcionais, premissas, restrições, riscos e demais informações necessárias à correta execução dos serviços.

7.1.14.6.4.1.10 Durante o período de vigência do suporte técnico e garantia, quando for o caso, todos os firmwares e softwares deverão ser atualizados a cada nova versão ou correção, sem nenhum custo adicional para a ANEEL;

7.1.14.6.4.1.11 O serviço de suporte técnico poderá ser atendido através de contato telefônico, por e-mail, remoto supervisionado (quando acordado) ou nas dependências do ANEEL, sendo este critério decidido pela equipe técnica do ANEEL;

7.1.14.6.4.1.12 A CONTRATADA deverá possuir sistema de abertura de chamados para que o ANEEL possa receber um identificador único para cada solicitação de atendimento e que tenha recurso(s) (e-mail, página web, central telefônica) que possa manter a equipe técnica da ANEEL informada sobre o andamento de cada chamado, esteja ele aberto, em andamento ou fechado.

7.1.14.6.4.2 **Da Manutenção Preventiva**

7.1.14.6.4.2.1 A manutenção preventiva será destinada a atualizar os componentes do software e a realizar quaisquer operações que evitem uma parada parcial ou total da solução;

7.1.14.6.4.2.2 Durante a manutenção preventiva a CONTRATADA deverá analisar a solução, sua condição atual de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta segundo as recomendações do fabricante. A equipe técnica do ANEEL decidirá sobre a aplicação ou não das recomendações;

7.1.14.6.4.2.3 A manutenção preventiva deverá ser executada mensalmente conforme cronograma a ser definido em conjunto com o gestor do contrato e equipe técnica da ANEEL;

7.1.14.6.4.2.4 O cronograma anual poderá sofrer adequações durante o ano vigente, desde que a CONTRATADA e a ANEEL estejam de acordoe que não seja descumprido o atendimento mensal;

7.1.14.6.4.2.5 Deverá ser gerado um relatório técnico mensal em 2 (duas) vias a cada manutenção preventiva, que deverá ser entregue até 5 (cinco) dias após a visita da CONTRATADA, para a equipe técnica da ANEEL,

que dará ciência no documento e arquivará internamente uma das vias após análise e aceitação do seu conteúdo;

7.1.14.6.4.3 **Da Manutenção Corretiva**

7.1.14.6.4.3.1 A manutenção corretiva será destinada a remover os defeitos apresentados pelos componentes de software de toda solução objeto do contrato, compreendendo também a atualização de versões da solução que se fizerem necessários;

7.1.14.6.4.3.2 A manutenção corretiva será realizada sempre que a solução apresentar falha que impeça o seu funcionamento regular e requeira uma intervenção técnica especializada;

7.1.14.6.4.3.3 A manutenção corretiva pode ser solicitada a qualquer momento em que o sistema apresente pane, deficiência ou dificuldade de operação;

7.1.14.6.4.3.4 As visitas para prestação do serviço de manutenção preventiva e corretiva, independentemente da quantidade necessária, não implicarão em custos adicionais para a ANEEL e deverão estar inclusas no custo mensal proposto do suporte técnico especializado.

7.1.14.6.5 **Garantia Técnica:**

7.1.14.6.5.1 A garantia será de 12 (doze) meses, a partir da emissão do Termo de Recebimento Definitivo (TRD) da solução pela ANEEL;

7.1.14.6.5.2 A garantia técnica deve cobrir defeitos em quaisquer dos componentes de software da solução, sem ônus adicional para o ANEEL;

7.1.14.6.5.3 A garantia técnica também deverá prover o direito da ANEEL ao recebimento de todas as novas versões ou releases dos softwares adquiridos, bem como de produtos que eventualmente venham a ser substituídos.

7.1.14.6.5.4 A garantia e assistência técnica devem englobar todos os seus componentes e/ou softwares da solução;

7.1.14.6.5.5 Os serviços referentes à garantia técnica e respectivos serviços de suporte técnico, devem ser prestados na modalidade on-site (presencial) ou remoto (quando acordado com a ANEEL) em regime de 24x7 (24 horas por dia, 7 dias da semana);

7.1.14.6.5.6 As manutenções que exijam paralisação do ambiente, ou que coloquem em risco sua disponibilidade, devem ser executados fora do

horário de expediente da Contratante (antes das 6:00h ou após as 22:00h em dias úteis, ou em finais de semana e feriados);

7.1.14.6.5.7 A solução ofertada deve ter prazo de garantia de funcionamento e de direito a atualização contados a partir da data da emissão do Termo de Recebimento Definitivo pela ANEEL.

7.1.14.6.5.8 Os custos relativos ao fornecimento da garantia devem ser computados no preço dos próprios itens referentes ao software.

7.1.14.6.5.9 Durante o prazo de garantia, a CONTRATADA deverá providenciar, sem ônus adicional para a ANEEL, o fornecimento de atualização de versão e/ou release, bem como patches de todos os softwares que integram a solução, incluindo drivers e todos os demais elementos integrantes da solução fornecida.

7.1.14.6.5.10 A garantia consiste, entre outros, em:

7.1.14.6.5.10.1 Reparar eventuais falhas de funcionamento, mediante a aplicação de atualização e/ou correção dos componentes de software, de acordo com os manuais e normas técnicas específicas.

7.1.14.6.5.10.2 Responsabilizar-se pelas ações executadas ou recomendadas por analistas e consultores do quadro da empresa, assim como pelos efeitos delas advindos na execução das atividades previstas neste Termo de Referência ou no uso dos acessos, privilégios ou informações obtidas em função das atividades por estes executadas;

7.1.14.6.5.10.3 Comunicar, por escrito, à ANEEL, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos o objeto deste Termo de Referência, fazendo constar a causa de inadequação e a ação devida para a correção;

7.1.14.6.5.11 A CONTRATADA deverá disponibilizar a atualização dos produtos licenciados assim que houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos.

7.1.14.6.5.12 O direito de atualização de versão de cada programa deverá abranger:

7.1.14.6.5.12.1 Downloads de drivers, firmwares, patches, atualizações dos softwares e manuais técnicos, a partir do sítio internet do fabricante do produto.

7.1.14.6.5.12.2 Todas as atualizações, novas versões e releases dos softwares que fizerem parte da solução CONTRATADA.

7.1.14.6.5.12.3 Direito de acesso pelos técnicos da ANEEL à base de conhecimento e a fóruns da solução no sítio do fabricante.

7.1.14.6.5.12.4 Notificar a ANEEL em prazo não superior a dez dias sobre a disponibilidade de novas versões e releases dos softwares que fizerem parte da solução fornecida.

7.1.14.6.5.12.5 Juntamente com a documentação de instalação e configuração da solução, como requisito para emissão do Termo de Recebimento Definitivo, a CONTRATADA deverá entregar a seguinte documentação:

7.1.14.6.5.12.5.1 Termo (s) de Garantia comprovando que os softwares que compõem a solução estão cobertos pela garantia do fabricante, pelo prazo mínimo de 12 (doze) meses, contados a partir da emissão do Termo de Recebimento Definitivo emitido pela ANEEL.

7.1.14.6.5.13 A CONTRATADA deverá orientar a CONTRATANTE para, quando for conveniente à CONTRATANTE, proceder à aplicação de pacotes de correção e implantação de versões do produto, cabendo à CONTRATADA orientar e disponibilizar um técnico para contato, em caso de dúvidas ou falhas, por meio telefônico ou correio eletrônico.

7.1.14.6.5.14 A CONTRATADA deverá promover o isolamento, identificação e caracterização de falhas de laboratório (bugs), encaminhamento da falha ao laboratório do fabricante e acompanhamento de sua solução.

7.1.14.6.5.15 Serão consideradas falhas de laboratórios o comportamento ou características dos softwares que se mostrem diferentes daqueles previstos na documentação do produto e sejam considerados pela CONTRATANTE como prejudiciais ao seu uso.

7.1.14.7 A CONTRATADA deverá realizar o repasse de conhecimento para operacionalização e administração diária da solução fornecida, direcionada à equipe técnica da ANEEL, logo após a homologação da solução por parte da ANEEL em até 10 dias úteis após a data do recebimento definitivo da solução, com duração mínima de 4 (quatro) horas, contemplando no mínimo os seguintes aspectos:

7.1.14.7.1 Administração diária da solução;
7.1.14.7.2 Configurações de MTA;

7.1.14.7.3 Configurações de políticas e regras de spam,phishing, DLP, criptografia, anti-APT, fraude de email, antivirus;
7.1.14.7.4 Configuração de quarentena de usuário e da solução;
7.1.14.7.5 Pesquisa de e-mails e logs da solução;
7.1.14.7.6 Monitoramento de estatísticas da solução;
7.1.14.7.7 Geração de relatórios;
7.1.14.7.8 Backup de configurações;
7.1.14.7.9 Procedimentos de atualização de firmware;
7.1.14.7.10 Teste de comunicações com a infraestrutura do fabricante;
7.1.14.7.11 Submissão de spams ao fabricante;

7.1.14.8 **Cronograma:**

Cronograma de execução do serviço de implementação da solução			
Evento	**Descrição**	**Prazo**	**Responsável**
1	Início do Contrato	-	ANEEL e CONTRATADA
2	Reunião inicial	Em até 5 (cinco) dias corridos, contados a partir do evento 01	ANEEL e CONTRATADA
3	Entrega do Plano de Instalação da solução	Em até 15 (quinze) dias corridos, contados a partir do evento 02.	CONTRATADA
4	Entrega dos softwares da solução	Em até 20 (dias) corridos após o evento 01	CONTRATADA
5	Instalação, configuração, operacionalização em produção e entrega do "As built" da solução	Em até 30 (trinta) dias úteis, contados a partir do evento 01	CONTRATADA
6	Repasse de conhecimento da solução	Em até 10 (dez) dias úteis após o evento 05	CONTRATADA

7.1.14.9 **Unidade de medida para pagamento com base no resultado:** Serviço prestado.

7.1.14.10 **Listas de verificação**: A CONTRATADA deverá fornecer o checklist contendo todos os itens entregues, instalados e configurados à CONTRATANTE par fins de conferência.

7.1.14.11 **Critérios de aceitação:** A CONTRATANTE conferirá todos os itens entregues, instalados e configurados no ambiente da ANEEL conforme os requisitos deste TR.

7.1.14.12 **Acordo de Nível de Serviços (ANS):**

7.1.14.12.1 A CONTRATADA deverá realizar atendimentos "on-site" (Severidade 1 e 2) e remotos (Severidade 3 e 4, 5) do serviço de suporte técnico conforme categorização dos chamados definida abaixo:

SEVERIDADE	DESCRIÇÃO	TEMPO TOTAL DE SOLUÇÃO (DEFINITIVA/CONTORNO)
1 – Urgente (alta)	Indisponibilidade total do serviço	04 (quatro) horas / 01 (uma) hora
2 - Muito importante (Média/alta)	Erros ou problemas que impactem o ambiente de produção.	06 (seis) horas / 02 (duas) horas
3 – Importante (baixa)	Problemas contornáveis que não degradam o ambiente de produção.	24 (vinte) horas / 12 (doze) horas
4 – Informação (Atendidos por meio de Ordens de Serviço)	Consulta técnica, dúvidas em geral, monitoramento, atualizações de software – patches e fixes)	48 (quarenta e oito) horas / 36 (trinta e seis) horas
5 – Implementação de novos serviços e features de software remotamente	OBS: Fora da janela de manutenção advinda de chamados urgentes, muito importantes e importantes	72 (setenta e duas) horas/ 48 (quarenta e oito)

7.1.14.13 **Equipe Técnica:** Não se aplica.

7.1.14.14 **Fornecimento de insumos:** Não se aplica.

7.1.14.15 **Outras observações:** Não se aplica.

7.1.14.16 **Forma de Aceite: Parcela única**

7.1.14.17 **Recebimento**

7.1.14.17.1 **Recebimento Provisório**

7.1.14.17.1.1 **Prazo, contado da apresentação do serviço:** No ato de entrega no AS-BUILT (documento contendo todos os detalhes da instalação e configurações realizadas na solução para funcionamento no ambiente computacional da ANEEL).

7.1.14.17.1.2 **Responsável:** Fiscal Técnico**.**

7.1.14.17.1.3 **Requisitos/Procedimentos:** O recebimento do AS-BUILT, pelo Fiscal Técnico, será considerado o Termo de Recebimento Provisório, não havendo documento específico para o TRP.

7.1.14.17.2 **Recebimento Definitivo**

7.1.14.17.2.1 **Prazo, contado do Recebimento Provisório:** Até 15 (quinze) dias úteis a partir da entrega do AS-BUILT.

7.1.14.17.2.2 **Responsável:** Fiscal Técnico, Fiscal Requisitante e Gestor do Contrato.

7.1.14.17.2.3 **Requisitos/Procedimentos:** Conferência e aprovação do conteúdo do documento AS-BUILT quanto às ações e configurações efetuadas pelo Fiscal Técnico.

7.1.14.17.3 **Forma de pagamento:** Parcela única

7.1.14.17.3.1 Os pagamentos serão efetuados após o RECEBIMENTO DEFINITIVO dos serviços prestados, obedecendo aos seguintes eventos:

7.1.14.17.3.2 Apresentação da nota fiscal/fatura pelo CONTRATADO à área técnica responsável;

7.1.14.17.3.3 Atesto da nota fiscal pela SGI/ANEEL (Gestor do Contrato) em até 5 (cinco) dias úteis, contados do recebimento desta;

7.1.14.17.3.4 Pagamento pela SAF/ANEEL em até 10 (dez) dias úteis, contados do atesto da nota fiscal/fatura.

7.1.14.17.3.5 A Nota Fiscal deverá ser apresentada no valor exato autorizado pela CONTRATANTE, quando do RECEBIMENTO DEFINITIVO DOS SERVIÇOS.

7.1.14.17.3.6 Antes de cada pagamento ao CONTRATADO, será realizada consulta ao Sistema de Cadastramento Unificado de Fornecedores – SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

7.1.14.17.3.7 O CONTRATADO deverá manter registro atualizado no Sistema de Cadastramento Unificado de Fornecedores – SICAF, e para efeito de pagamento das notas fiscais, as Certidões Negativa de Débito junto ao INSS (CND) e de Débitos de Tributos e Contribuições Federais e o Certificado de Regularidade do FGTS (CRF) deverão estar válidos perante o SICAF, caso contrário, deverão ser apresentados tais documentos com prazos válidos.

7.1.14.17.3.8 Caso a ANEEL constate a irregularidade do CONTRATADO junto ao SICAF, o notificará, por escrito, para que no prazo de 5 (cinco) dias regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

7.1.14.17.3.9 Não havendo regularização ou sendo a defesa considerada improcedente, a ANEEL:

7.1.14.17.3.9.1 Oficiará os órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do CONTRATADO, bem como quanto à existência de pagamento a ser efetuado, para que

sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos; e

7.1.14.17.3.9.2 Persistindo a irregularidade, adotará as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada a ampla defesa e o contraditório.

7.1.14.17.3.10 Será rescindido o contrato em execução com o CONTRATADO irregular no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

7.1.14.17.3.11 Havendo a efetiva execução do objeto, os pagamentos da parte incontroversa serão realizados normalmente, até que se decida pela rescisão do contrato, caso o CONTRATADO não regularize sua situação junto ao SICAF.

7.1.14.17.3.12 Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

7.1.14.17.3.13 O ressarcimento financeiro decorrente de eventuais atrasos de pagamento será calculado do dia subsequente ao vencimento da fatura até a data do efetivo pagamento, mediante a aplicação de juros moratórios de 6% (seis por cento) ao ano sobre a parcela em atraso “pro rata die”.

7.1.14.17.3.14 Não haverá, sob hipótese alguma, pagamento antecipado ao CONTRATADO.

7.1.14.17.3.15 A ANEEL reserva-se o direito de suspender o pagamento se a prestação dos serviços não estiver de acordo com a especificação apresentada e aceita.

7.1.14.17.3.16 São hipóteses de glosa nos pagamentos as situações indicadas abaixo, caso não estejam previstas no IMR ou no instrumento equivalente:

7.1.14.17.3.16.1 Cotação de tributo em percentual maior que o adequado, segundo as regras do edital;

7.1.14.17.3.16.2 Inexecução parcial ou total das atividades contratadas;

7.1.14.17.3.16.3 Não produção dos resultados contratados;

7.1.14.17.3.16.4 Não execução do contrato com a qualidade mínima exigida;

7.1.14.17.3.16.5 Não utilização de materiais e recursos humanos exigidos para a execução do serviço ou a utilização deles com qualidade ou quantidade inferior à demandada;

7.1.14.17.3.16.6 Equívocos no dimensionamento dos quantitativos da proposta que se revelem superiores às necessidades da Administração, quando detectados em momento ulterior aos recebimentos provisório e definitivo da contratação;

7.1.14.17.3.16.7 Custos não renováveis já pagos ou amortizados que não foram eliminados quando da prorrogação contratual.

7.1.14.17.3.17 O processamento das glosas não impede a instauração concomitante de procedimento para apuração de responsabilidade administrativa visando a aplicação de sanção administrativa.

7.1.14.17.3.18 Obriga-se a CONTRATADA a apresentar documentos de cobrança claros, com critérios transparentes, de forma a facilitar o atesto inequívoco dos serviços.

7.1.14.17.3.19 A CONTRATANTE poderá interromper o prazo do processamento do pagamento sem que represente qualquer ônus, quando a nota fiscal/fatura estiver em desacordo com o estabelecido no contrato e/ou a contiver erros de preenchimento a cargo da CONTRATADA que comprometam a compreensão, intelecção e interpretação de toda a cobrança encaminhada.

7.1.14.17.3.20 Não havendo, porém, comprometimento, nos termos do item supracitado, de toda a nota fiscal/fatura encaminhada, a CONTRATANTE poderá efetuar o pagamento do valor correspondente à parcela incontroversa, permanecendo interrompido o prazo para a parte da cobrança que apresenta problemas, até que a CONTRATADA, em resposta, restabeleça as condições para o atesto.

7.1.14.17.3.21 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, quando couber.

7.1.14.17.3.22 As notas fiscais deverão ser emitidas pela CONTRATADA por meio eletrônico, visando a adequação aos procedimentos internos da ANEEL.

7.1.14.17.3.23 É vedado o pagamento, a qualquer título, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante, com fundamento na Lei de Diretrizes Orçamentárias vigente, devendo a Administração verificar se o SICAF acusa o referido vínculo.

7.1.14.17.3.24 Condições: Não se aplica.

7.1.14.17.3.25 Cronograma financeiro: Não se aplica.

8. GARANTIA

8.1. **Garantia de execução do contrato:** a CONTRATADA prestará garantia financeira nos termos previstos no instrumento convocatório ou no Contrato.

9. INSERÇÃO, TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

9.1. **Plano de inserção contratual**: Não se aplica.

9.2. **Transição e encerramento contratual:** Não se aplica.

9.3. No encerramento do contrato os responsáveis por sua gestão deverão elaborar e instruir o processo administrativo com um relatório final acerca das ocorrências da fase de execução contratual, a ser utilizado como fonte de informações para as futuras contratações, encaminhando-o à SLC para as devidas providências de encerramento de contrato.

10. MECANISMOS DE COMUNICAÇÃO FORMAL ENTRE AS PARTES

10.1. A comunicação entre a ANEEL e a CONTRATADA será efetuada por meio de:

10.1.1. ☒ Ofício.

10.1.2. ☒ E-mail.

10.1.3. ☒ Ordem de Serviço – OS.

10.1.4. ☒ Ferramenta de abertura de chamados.

10.1.5. ☒ Ata de reunião.

10.1.6. ☐ Outros: Escrever outros mecanismos

10.2. No caso de ata de registro de preços gerenciada pela ANEEL: Não se aplica.

11. GESTÃO DA SEGURANÇA DA INFORMAÇÃO, SIGILO E DIREITOS

11.1. **Segurança da Informação, confidencialidade e sigilo**: os serviços decorrentes da contratação são objeto de sigilo, não podendo a CONTRATADA, nem aos profissionais neles envolvidos, de qualquer modo tornar públicas ou conhecidas quaisquer informações relativas à infraestrutura, softwares e soluções utilizadas no ambiente computacional da ANEEL.

11.1.1. A CONTRATADA deverá firmar o Termo de Compromisso e Manutenção de Sigilo encaminhado pela ANEEL e fazer com que todos os seus funcionários diretamente envolvidos na contratação assinem o Termo de Ciência deste compromisso (conforme

Anexos C e D deste Termo de Referência), de maneira a se manter sigilo absoluto sobre todas as informações relativas à infraestrutura, softwares, dados e documentos integrantes dos serviços a serem executados, com total obediência às normas de segurança vigentes, ou que venham a ser implantadas, além de não ser divulgado qualquer assunto tratado nas dependências da ANEEL, ou a serviço desta, salvo se expressamente autorizado.

11.1.2. Para a execução do Contrato, a CONTRATADA deverá conhecer e a observar as normas internas da ANEEL referentes ao tema (Norma de Organização nº 01/2006-ANEEL/ANP/CPRM, e demais normativos vigentes).

11.1.3. No caso de substituição ou inclusão de empregados por parte da CONTRATADA, o preposto deverá entregar Termo de Ciência assinado pelos novos empregados envolvidos na execução contratual.

11.2. **Propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação**: Não se aplica.

11.3. **Transferência do conhecimento**: Não se aplica.

12. FUNÇÕES E RESPONSABILIDADES DO GESTOR E FISCAIS DO CONTRATO

12.1. A CONTRATANTE designará os seguintes servidores responsáveis pela gestão e fiscalização do contrato:

12.1.1. **GESTOR DO CONTRATO,** servidor com atribuições gerenciais, preferencialmente da área requisitante da solução de TIC, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, e responsável, em especial, pelas seguintes atividades:

12.1.1.1. Coordenar e comandar o processo de gestão e fiscalização do contrato;

12.1.1.2. Convocar e realizar reunião inicial para esclarecimentos relativos às questões operacionais, administrativas e de gestão do contrato, repasse de conhecimentos necessários à execução, e disponibilização da infraestrutura, quando couber, a ser realizada conjuntamente com os fiscais do contrato (FISCAL TÉCNICO, FISCAL REQUISITANTE e FISCAL ADMINISTRATIVO) e o CONTRATADO, quando este deverá apresentar o preposto designado para a contratação, e os termos de compromisso e de ciência assinados.

12.1.1.3. Autorizar a execução do Contrato mediante a emissão do documento indicado no Termo de Referência;

12.1.1.4. Notificar o CONTRATADO sempre que o mesmo descumprir qualquer condição pactuada, bem como diante de ocorrências ou de circunstâncias notadas durante a fiscalização que possam prejudicar a execução, solicitando as providências necessárias;

12.1.1.5. Receber a fatura correspondente, atestá-la se o objeto entregue e os valores cobrados estiverem de acordo com o contratado, e a mesma atender a forma

estabelecida pela legislação vigente, e providenciar o pagamento no prazo e condições estabelecidas, efetuando glosa de valores errôneos, quando necessário.

12.1.1.5.1. Encaminhar indicações de glosas nas notas fiscais ou faturas, quando o objeto entregue e os valores cobrados estiverem em desacordo com o contratado;

12.1.1.6. Rejeitar, no todo ou em parte, o objeto entregue em desacordo com o instrumento contratual, comunicar formalmente e exigir do CONTRATADO as providências necessárias para sua imediata regularização, sem prejuízo das sanções e glosas cabíveis;

12.1.1.7. Em conjunto com o FISCAL REQUISITANTE e o FISCAL TÉCNICO, confeccionar e assinar o Termo de Recebimento Definitivo – TRD com base na avaliação dos níveis de serviços prestados;

12.1.1.8. Após a emissão do TRD, emitir autorização ao Contratado para o faturamento dos serviços, encaminhando-a ao preposto da empresa;

12.1.1.9. Manter histórico de gestão do contrato, efetuando por despacho formal no processo administrativo da contratação, com apoio dos FISCAIS REQUISITANTE, TÉCNICO E ADMINISTRATIVO, registros formais de todas as ocorrências positivas e negativas da execução do contrato, por ordem histórica, indicando dia, mês, ano, empregados do CONTRATADO eventualmente envolvidos, ações necessárias para a regularização das faltas ou defeitos, e dar ciência a seu superior hierárquico;

12.1.1.10. Monitorar os prazos de execução e de vigência contratual, inclusive no tocante aos procedimentos administrativos internos exigidos para sua continuidade ou encerramento.

12.1.1.11. Monitorar a execução financeira do contrato, mediante o controle de pagamentos efetuados e do recurso orçamentário, visando dar cumprimento ao cronograma financeiro.

12.1.1.12. Com base no histórico de gestão do contrato e nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação, encaminhar nota técnica à SLC, acompanhada da documentação necessária para tal procedimento, sobre procedimentos relativos à execução do objeto contratual, em especial quanto à proposição de sanções devido a descumprimentos de obrigações, alterações, prorrogações e rescisões, repactuações e reajustes, motivando e fundamentando seu entendimento favorável ou desfavorável da questão.

12.1.1.13. Durante a execução contratual, coordenar a equipe de Fiscalização do contrato na atualização contínua do Mapa de Gerenciamento de Riscos, e realização das seguintes atividades:

12.1.1.13.1. Reavaliação dos riscos identificados nas fases anteriores e atualização de suas respectivas ações de tratamento; e

12.1.1.13.2. Identificação, análise, avaliação e tratamento de novos riscos.

12.1.1.13.2.1. O Mapa de Gerenciamento de Riscos deve ser juntado aos autos do processo administrativo, pelo menos:

12.1.1.13.2.2. Ao final da elaboração do Termo de Referência ou Projeto Básico;

12.1.1.13.2.3. Ao final da fase de Seleção do Fornecedor;

12.1.1.13.2.4. Uma vez ao ano, durante a gestão do contrato; e

12.1.1.13.2.5. Após eventos relevantes.

12.1.2. **FISCAL TÉCNICO DO CONTRATO,** servidor representante da área de TIC, indicado para fiscalizar tecnicamente o contrato, e responsável, em especial, pelas seguintes atividades:

12.1.2.1. Confeccionar e assinar o Termo de Recebimento Provisório, quando da entrega do objeto constante na Ordem de Serviço ou de Fornecimento de Bens;

12.1.2.2. Em conjunto com o GESTOR DO CONTRATO e o FISCAL REQUISITANTE, confeccionar e assinar o Termo de Recebimento Definitivo.

12.1.2.3. Em conjunto com o FISCAL REQUISITANTE, avaliar a qualidade dos serviços realizados ou dos bens entregues e justificativas, a partir das especificações e critérios de aceitação definidos para o objeto;

12.1.2.4. Em conjunto com o FISCAL REQUISITANTE, identificar não conformidades com os termos contratuais;

12.1.2.5. Em conjunto com o FISCAL ADMINISTRATIVO, verificar a manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica;

12.1.2.6. Apoiar, juntamente com o FISCAL ADMINISTRATIVO, a verificação da manutenção da necessidade, economicidade e oportunidade da contratação, pelo FISCAL REQUISITANTE;

12.1.2.7. Em conjunto com o FISCAL REQUISITANTE, verificar a manutenção das condições definidas nos Modelos de Execução e de Gestão do Contrato.

12.1.3. **FISCAL REQUISITANTE DO CONTRATO,** servidor representante da área da solução de TIC, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista de negócio e funcional da solução de TIC, e responsável, em especial, pelas seguintes atividades:

12.1.3.1. Em conjunto com o GESTOR DO CONTRATO e o FISCAL TÉCNICO, confeccionar e assinar o Termo de Recebimento Definitivo.

12.1.3.2. Com apoio dos FISCAIS TÉCNICO e ADMINISTRATIVO verificar a manutenção da necessidade, economicidade e oportunidade da contratação,

12.1.3.3. Em conjunto com o FISCAL TÉCNICO, avaliar a qualidade dos serviços realizados ou dos bens entregues e justificativas, a partir das especificações e critérios de aceitação definidos para o objeto;

12.1.3.4. Em conjunto com o FISCAL TÉCNICO, identificar não conformidades com os termos contratuais;

12.1.3.5. Com apoio dos FISCAIS TÉCNICO E ADMINISTRATIVO, verificar a manutenção da necessidade, economicidade e oportunidade da contratação;

12.1.3.6. Em conjunto com o FISCAL TÉCNICO, verificar a manutenção das condições definidas nos Modelos de Execução e de Gestão do Contrato.

12.1.4. FISCAL ADMINISTRATIVO DO CONTRATO, servidor representante da área administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos, e responsável, em especial, pelas seguintes atividades:

12.1.4.1. Verificar a aderência aos termos contratuais;

12.1.4.2. Verificar as regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento;

12.1.4.3. Receber do preposto os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados, no caso de substituição ou inclusão de empregados pela CONTRATADA;

12.1.4.4. Em conjunto com o FISCAL TÉCNICO, verificar a manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica;

12.1.4.5. Apoiar, juntamente com o FISCAL TÉCNICO, a verificação da manutenção da necessidade, economicidade e oportunidade da contratação, pelo FISCAL REQUISITANTE.

12.2. Conforme a Instrução Normativa SGD/ME nº1/2019, art.29, IV, os papéis dos fiscais não poderão ser acumulados pelo mesmo servidor, salvo o de FISCAL REQUISITANTE e de FISCAL TÉCNICO.

12.3. O acompanhamento e fiscalização do contrato pelos servidores designados pela CONTRATANTE não exclui nem reduz a responsabilidade do CONTRATADO, até mesmo perante terceiros, por qualquer irregularidade, inclusive resultante de imperfeições técnicas, emprego de material inadequado ou de qualidade inferior, e nem implica corresponsabilidade da CONTRATANTE ou de seus agentes.

12.4. É vedado à Administração ou aos seus servidores praticar atos de ingerência na administração da CONTRATADA, a exemplo de:

12.4.1. Possibilitar ou dar causa a atos de subordinação, vinculação hierárquica, prestação de contas, aplicação de sanção e supervisão direta sobre os empregados da CONTRATADA;

12.4.2. Exercer o poder de mando sobre os empregados da CONTRATADA, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da

contratação previr a notificação direta para a execução das tarefas previamente descritas no contrato de prestação de serviços para a função específica, tais como nos serviços de recepção, apoio administrativo ou ao usuário;

12.4.3. Direcionar a contratação de pessoas para trabalhar nas empresas CONTRATADAs;

12.4.4. Promover ou aceitar o desvio de funções dos trabalhadores da CONTRATADA, mediante a utilização destes em atividades distintas daquelas previstas no objeto da contratação e em relação à função específica para a qual o trabalhador foi contratado;

12.4.5. Considerar os trabalhadores da CONTRATADA como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens;

12.4.6. Definir o valor da remuneração dos trabalhadores da empresa CONTRATADA para prestar os serviços, salvo nos casos específicos em que se necessitam de profissionais com habilitação/experiência superior a daqueles que, no mercado, são remunerados pelo piso salarial da categoria, desde que justificadamente; e

12.4.7. Conceder aos trabalhadores da CONTRATADA, direitos típicos de servidores públicos, tais como recesso, ponto facultativo, dentre outros.

13. OBRIGAÇÕES DA CONTRATADA

13.1 Manter-se durante a vigência do contrato, habilitado e apto a cumprir todas as obrigações pactuadas.

13.2 Entregar os produtos e serviços conforme Termos e Condições deste Termo de Referência.

13.3 Responsabilizar-se integralmente pela execução do objeto contratado, garantindo a qualidade da prestação e sua aderência às condições pactuadas e à legislação vigente.

13.4 Responsabilizar-se integralmente por todos os encargos e custos necessários à perfeita execução do objeto contratado, conforme as normas vigentes, sendo que a Administração não poderá ser responsabilizada por eventuais descumprimentos de encargos assumidos pela CONTRATADA.

13.5 Responsabilizar-se por quaisquer demandas trabalhistas, penais e civis, movidas por seus empregados ou terceiros contra a CONTRATANTE, relacionadas à execução do presente contrato.

13.6 Responsabilizar-se pelo cumprimento da legislação específica, em caso de acidente do trabalho ocorrido nas dependências da CONTRATANTE, com qualquer de seus empregados, vinculados à execução do objeto contratado.

13.7 Responsabilizar-se pela adequada utilização e restituição, nas mesmas condições que lhe foram entregues, de todas as dependências, materiais, instalações, ferramentas e utensílios, disponibilizados pela CONTRATANTE.

13.8 Responsabilizar-se, sem prejuízo da execução contratual, pela reparação, correção, remoção, reconstrução ou substituição, às suas expensas, dos danos (inclusive bens extraviados) causados por seus empregados, comprovadamente, à CONTRATANTE ou a terceiros, em razão de ação ou omissão dolosa ou culposa, sua ou de seus prepostos, independentemente de outras cominações contratuais ou legais, não excluindo ou reduzindo a responsabilidade da fiscalização ou acompanhamento da execução dos serviços pela Contratante.

13.9 Dar ciência sobre quaisquer operações societárias que resultem em fusão, cisão ou incorporação da CONTRATADA, bem como de alteração de seu objeto social, por escrito, à CONTRATANTE, para avaliação e anuência expressa desta quanto à continuidade da relação contratual, desde que sejam observados pela nova pessoa jurídica que eventualmente sucedê-la todos os requisitos de habilitação exigidos na licitação, e, mantidas as demais cláusulas e condições do contrato, não haja prejuízo à execução do objeto pactuado;

13.10 Não ceder direitos ou subcontratar o objeto do contrato.

13.11 Não caucionar ou utilizar o instrumento contratual para qualquer operação financeira, sob pena de rescisão contratual.

13.12 Não vincular o pagamento de salários e demais vantagens de seus empregados ao pagamento de faturas emitidas em nome da ANEEL.

13.13 Cumprir, por si e por seus empregados e prepostos, todas as disposições normativas aplicáveis, especialmente relacionadas:

13.13.1 Ao objeto do contrato;

13.13.2 Às normas de órgãos públicos responsáveis pela emissão de autorizações, alvarás e permissões, conselhos profissionais e de classe, órgãos oficiais de controle de qualidade e metrologia ou órgãos emissores de normas técnicas;

13.13.3 À segurança, sigilo e veiculação de informações;

13.13.4 Ao Código de Ética da ANEEL;

13.13.5 A demais diretrizes e normas organizacionais da ANEEL.

13.14 Atender orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual, nas condições pactuadas;

13.15 Providenciar a substituição ou a correção nos prazos pactuados, a partir da notificação pela ANEEL, de objeto recusado por estar em desacordo com às especificações;

13.16 Comunicar à ANEEL, por escrito, com a urgência adequada ao evento que o ensejar, quaisquer fatos ou circunstâncias detectadas que possam prejudicar a execução, ou comprometer a integridade de pessoas e do patrimônio público;

13.17 Não veicular publicidade ou divulgar qualquer outra informação acerca desta contratação, sem prévia autorização da CONTRATANTE;

13.18 Indicar e manter preposto apto a representá-lo junto à CONTRATANTE durante a execução contratual, de fácil acesso ao GESTOR DO CONTRATO, para tomada de providências visando a solução de problemas em tempo hábil, e, quando cabível, participar de reuniões, receber orientações e diligências, encaminhar, responder e decidir questões relacionadas às disposições contratuais, de modo a garantir a qualidade da execução e os resultados previstos para a prestação dos serviços;

13.19 Submeter-se à fiscalização, sobretudo permitindo o acesso da CONTRATANTE a elementos de informação:

13.19.1 Responder a questionamentos e apresentar documentos, no prazo determinado pela CONTRATANTE, quando acionada por meio de correspondência oficial, sob a pena da aplicação de sanções cabíveis.

13.19.2 Considerar prazo para resposta de 5 dias úteis, caso este não tenha sido estabelecido na correspondência recebida.

13.19.3 Realinhar a prestação do serviço conforme orientação.

13.20 Manter a produtividade ou a capacidade mínima de fornecimento da Solução de Tecnologia da Informação durante a execução do contrato, conforme estabelecido no Edital e seus anexos;

13.21 Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a CONTRATADA relatar à Contratante toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;

13.22 Vedar a utilização, na execução dos serviços, de empregado que seja familiar (cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau) de agente público ocupante de cargo em comissão ou função de confiança na CONTRATANTE, nos termos do artigo 7° do Decreto n° 7.203, de 2010;

13.23 Providenciar a retirada imediata, quando exigido pela CONTRATANTE, de empregado cuja idoneidade, capacidade, atuação, permanência, e/ou comportamento sejam julgados prejudiciais, inconvenientes ou insatisfatórios, ou entendidos como inadequados à prestação dos serviços, substituindo-o no prazo de até 24 horas;

13.24 Fornecer, sem nenhum ônus para seu funcionário, e fiscalizar sua utilização:

13.24.1 Equipamentos de segurança e outros necessários para a execução de serviços;

13.24.2 Crachá de identificação como empregado do Contratado, com foto;

13.24.3 Uniforme de primeiro uso e completo, no padrão fixado no Termo de Referência.

13.25 Manter a garantia técnica e/ou financeira nas condições pactuadas, visando o cumprimento de suas obrigações com relação a tais seguros.

13.26 Ceder à CONTRATANTE, nos termos estabelecidos no edital e seus anexos, os direitos de propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação e Comunicação - TIC sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação, os modelos de dados e as bases de dados.

13.27 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos;

13.27.1 Ocorrendo o desaparecimento de bens ou danos ao patrimônio da Contratante, evitáveis pelo cumprimento das rotinas contratuais, responderá a CONTRATADA pelo prejuízo, apurado em procedimento próprio, respeitado o contraditório e a ampla defesa, instruído, dentre outros elementos pertinentes, com o boletim de ocorrência, quando poderá escusar-se da responsabilidade caso demonstre o perfeito cumprimento de suas obrigações contratuais.

13.27.1.1 Não afastada a responsabilidade da CONTRATADA, a reparação do dano operar-se-á preferencialmente mediante a substituição do bem desaparecido ou danificado por outro idêntico ou de qualidade superior.

13.27.1.2 Não sendo possível a substituição prevista no item anterior, a Contratante poderá autorizar o ressarcimento em espécie, promovendo previamente, nesta hipótese, a apuração do valor atualizado de mercado do bem, para efeitos de pagamento.

13.27.1.3 Não havendo o pagamento por parte da CONTRATADA, no prazo de 5 (cinco) dias úteis, o valor apurado conforme a cláusula anterior será descontado da garantia oferecida ou da próxima fatura mensal. A reincidência no fato ensejará a rescisão unilateral, sem prejuízos das perdas e danos a serem cobrados da CONTRATADA.

13.28 Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los caso o previsto inicialmente não seja satisfatório para o atendimento ao objeto

da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993. Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da contratante, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento dos serviços demandados e executados, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário, com base na alínea "b" do inciso I do art. 65 da Lei nº 8.666, de 1993.

13.29 Comunicar formalmente à Receita Federal a ocorrência de situação de exclusão obrigatória do Simples Nacional, conforme previsão do art. 30, §1º, da LC 123, de 2006.

13.30 Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social, bem como as regras de acessibilidade previstas na legislação, quando houver se beneficiado da preferência estabelecida pela Lei nº 13.146, de 2015.

14. OBRIGAÇÕES DO CONTRATANTE

14.1 Exigir do contratado que permaneça habilitado e apto a cumprir todas as obrigações pactuadas durante a vigência do contrato.

14.2 Disponibilizar à CONTRATADA os elementos, informações e/ou esclarecimentos necessários à prestação do objeto nos termos estabelecidos no Edital e seus Anexos.

14.3 Realizar o pagamento no prazo e condições estabelecidas, após atesto das faturas pelo GESTOR DO CONTRATO.

14.4 Notificar a CONTRATADA por escrito da ocorrência de imperfeições na execução dos serviços, fixando prazo para a sua correção, sob pena de instauração de processo de responsabilidade administrativa.

14.5 Notificar a CONTRATADA a instauração de processos para apuração de responsabilidade administrativa, decidir e aplicar sobre ele as sanções administrativas previstas no Edital e seus anexos, garantidos o contraditório e a ampla defesa, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável.

14.6 Verificar e acionar a garantia técnica e/ou financeira, exigindo da CONTRATADA, nos termos pactuados, o cumprimento de suas obrigações com relação a tais seguros.

14.7 Informar à CONTRATADA quaisquer débitos de sua responsabilidade.

14.8 Deduzir e recolher os tributos devidos na fonte sobre os pagamentos efetuados, conforme legislação aplicável.

14.9 Designar servidor (agente da administração) como GESTOR DO CONTRATO e FISCAIS TÉCNICO, ADMINISTRATIVO E REQUISITANTE DO CONTRATO para auxiliá-lo, no

acompanhamento e fiscalização da execução do contrato, visando a verificação da conformidade da prestação e da alocação dos recursos, de forma a assegurar o perfeito cumprimento do ajuste, conforme o previsto na Lei nº 8666/93, arts. 67 e 73, Decreto nº 9.507/2018, art. 6º, Instrução Normativa SGD/ME nº 1/2019, e neste Termo de Referência.

14.10 Assegurar que o ambiente de trabalho, inclusive seus equipamentos e instalações, apresentem condições adequadas ao cumprimento pela CONTRATADA, das normas de segurança e saúde no trabalho, quando o serviço for executado em suas dependências, ou em local por ela designado.

14.11 Encaminhar formalmente a demanda nos termos pactuados;

14.12 Providenciar o recebimento provisório e definitivo do objeto contratual, nos termos da cláusula específica de recebimento, respeitada a Lei nº 8.666/93.

14.13 Observar e cumprir a legislação cabível sobre terceirização de serviços, notadamente, as disposições contidas no Decreto nº 9.507/2018 e as Instruções Normativas SEGES/MPDG nº 5/2017, e SGD/ME nº1/2019.

14.14 Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável;

15. SANÇÕES ADMINISTRATIVAS

15.1 O CONTRATADO ficará sujeito às sanções administrativas na forma prevista abaixo, garantida a ampla defesa e o contraditório e observada à legislação pertinente.

15.2 Comete infração administrativa nos termos dos artigos 86 e 87 da Lei nº 8.666, de 1993, o CONTRATADO que atrasar a execução, não executar ou executar parcialmente qualquer das obrigações assumidas em decorrência do contrato, ficando sujeito às seguintes sanções contratuais:

15.2.1 **Advertência,** nas situações que merecem reprovação branda por parte da Administração, como também alerta do rigor da fiscalização e da possibilidade de penalização mais gravosa, em caso de reincidência;

15.2.2 **Multas,** Moratória (de caráter sancionatório, que objetiva penalizar o atraso) e Compensatória (de caráter indenizatório, sendo uma prefixação de indenização por perdas e danos), na forma abaixo especificada:

15.2.2.1 Multa moratória diária de até 0,33% (trinta e três centésimos por cento) sobre o valor mensal do contrato, limitado ao valor equivalente a 20% (vinte por cento) desse montante;

15.2.2.2 Multa compensatória:

15.2.2.2.1 De 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

15.2.2.2.2 Até o limite de 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução parcial do objeto, com incidência sobre o valor contratual definido pela CONTRATANTE (valor total, valor mensal, valor do grupo, valor do item ou outro valor pertinente), e a gravidade do inadimplemento indicado na tabela abaixo:

GRAVIDADE DO INADIMPLEMENTO	PERCENTUAL DA MULTA COMPENSATÓRIA
MUITO LEVE	2 %
LEVE	5 %
MÉDIA	8 %
GRAVE	15 %
MUITO GRAVE	20 %

15.2.2.2.2.1 Com relação às ocorrências abaixo, fica prefixada a gravidade, em concordância com o percentual de multa compensatória apresentado na tabela anterior:

OCORRÊNCIA	GRAVIDADE	INCIDÊNCIA
Não entregar o(s) software (es) no prazo estabelecido	MÉDIA	Aplicável ao valor do Contrato
Não entregar o PLANO DE INSTALAÇÃO no prazo estabelecido	MÉDIA	Aplicável ao valor do Contrato
Não instalar o(s) software(es), configurá-lo(os) e torná-lo (os) operacional em produção no prazo estabelecido	GRAVE	Aplicável ao valor do Contrato
Não entregar o AS BUILT da solução instalada no prazo estabelecido	MÉDIA	Aplicável ao valor do Contrato
Não substituir o produto que não corresponda ao exigido nas especificações, no prazo máximo de 15 (trinta) dias corridos, após notificação.	GRAVE	Aplicável ao valor do Contrato
Não se manter ou não buscar a regularização das condições de regularidade fiscal, previdenciária e trabalhista, habilitação jurídica e qualificação técnica, durante a vigência do contrato.	LEVE	Aplicável ao valor do Contrato
Descumprir prazo estabelecido neste Termo de Referência para atendimento de chamados de suporte técnico e manutenção preventiva/corretiva	GRAVE	Aplicável ao valor do Contrato
Não utilizar mão-de-obra qualificada e tecnicamente habilitada conforme estabelecido no Termo de Referência da Contratação para prestação do serviço contratado	GRAVE	Aplicável ao valor do Contrato

Não se responsabilizar pela adequada utilização e restituição, nas mesmas condições que lhe foram entregues, de todas as dependências, materiais, instalações, equipamentos, ferramentas e utensílios, disponibilizados pela CONTRATANTE.	GRAVE	Aplicável ao valor do Contrato
Não se responsabilizar pela reparação, correção, remoção, reconstrução ou substituição, às suas expensas, dos danos (inclusive bens extraviados) causados por seus empregados, à CONTRATANTE ou a terceiros.	MÉDIA	Aplicável ao valor do Contrato
Não dar ciência sobre quaisquer operações societárias que resultem em sua fusão, cisão ou incorporação, bem como de alteração de seu objeto social, por escrito, à CONTRATANTE	MÉDIA	Aplicável ao valor do Contrato
Ceder direitos ou subcontratar o objeto do contrato.	MUITO GRAVE	Aplicável ao valor do Contrato
Caucionar ou utilizar o instrumento contratual para qualquer operação financeira	MUITO GRAVE	Aplicável ao valor do Contrato
Vincular o pagamento de salários e demais vantagens de seus empregados ao pagamento de faturas emitidas em nome da CONTRATANTE	MUITO GRAVE	Aplicável ao valor do Contrato
Não cumprir, por si e por seus empregados e prepostos, diretrizes, normas organizacionais e Código de Ética da ANEEL relacionadas ao objeto do contrato.	MUITO GRAVE	Aplicável ao valor do Contrato
Não cumprir, por si e por seus empregados e prepostos, todas as disposições normativas aplicáveis à segurança, sigilo e veiculação de informações	MUITO GRAVE	Aplicável ao valor do Contrato
Não comunicar à CONTRATANTE por escrito, quaisquer fatos ou circunstâncias detectadas que possam prejudicar a execução, ou comprometer a integridade de pessoas e do patrimônio público	GRAVE	Aplicável ao valor do Contrato
Veicular publicidade ou divulgar qualquer outra informação acerca da contratação, sem prévia autorização da CONTRATANTE	MUITO GRAVE	Aplicável ao valor do Contrato
Não indicar e manter preposto apto a representá-lo junto à CONTRATANTE	GRAVE	Aplicável ao valor do Contrato
Não se submeter à fiscalização e responder a questionamentos e/ou apresentar documento no prazo determinado.	MÉDIA	Aplicável ao valor do Contrato
Não ajustar a prestação do serviço conforme determinado nos itens do Termo de Referência, após aviso realizado pela ANEEL	MUITO GRAVE	Aplicável ao valor da Ordem de Serviços
Não vedar a utilização, na execução dos serviços, de empregado que seja familiar (cônjuge,	GRAVE	Aplicável ao valor do Contrato

companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau) de agente público ocupante de cargo em comissão ou função de confiança na CONTRATANTE, nos termos do artigo 7° do Decreto n° 7.203, de 2010.		
Não manter garantia técnica e/ou financeira nas condições pactuadas	GRAVE	Aplicável ao valor do Contrato
Não transmitir à CONTRATANTE o direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente	MUITO GRAVE	Aplicável ao valor do Contrato

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

15.2.2.4 Tendo a multa alcançado o limite de 20% do valor total contratado, a prestação se tornado inútil, ou antes que haja prejuízo à Administração na persistência da(s) conduta(s), a CONTRATANTE estará autorizada a:

15.2.2.4.1 Reclamar perdas e danos excedentes não compensados pela aplicação de multa correspondente;

15.2.2.4.2 Avaliar a possibilidade de rescisão do contrato.

15.2.2.5 Os valores das multas consistem em créditos a serem recolhidos no prazo e forma legal, resguardados atos de cobrança e execução, administrativa e judicial, na forma sequencial e prioritária de: retenção e dedução dos pagamentos devidos pela Administração; pagamento mediante Guia de Recolhimento da União – GRU; e desconto do valor da garantia prestada.

15.2.2.6 É possível, ad cautelam, a retenção do valor da multa presumida antes da instauração do regular procedimento administrativo.

15.2.3 **Suspensão de licitar e impedimento de contratar com o órgão ou entidade CONTRATANTE, pelo prazo de até dois anos;**

15.2.3.1 Entende-se aplicável a sanção supra, quando apurada conduta capaz de deixar pendente, total ou parcialmente, a prestação acordada, com prejuízo ao interesse público e perda de confiança na relação contratual.

15.2.4 **Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;**

15.2.5 **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;**

15.2.5.1 A declaração de inidoneidade funda-se em situação ou fato delituoso e será aplicada nos casos em que a apuração de responsabilidade conclua ter havido dolo ou má-fé do CONTRATADO, em conduta lesiva, prejudicial à CONTRATANTE ou ilícita, que recomende o seu afastamento.

15.3 A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

15.4 Também fica sujeita às penalidades das cláusulas 15.2.3,15.2.4 e 15.2.5, o CONTRATADO que:

15.4.1 Tenha sofrido condenação definitiva por praticar, por meio doloso, fraude fiscal no recolhimento de quaisquer tributos;

15.4.2 Demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

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

15.6 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 CONTRATANTE, observado o princípio da proporcionalidade.

15.7 As penalidades previstas são independentes entre si, podendo ser aplicadas isoladas, ou cumulativamente, nos termos do §2º, do art. 87, da Lei nº 8.666/93, sem prejuízo de outras medidas cabíveis, no tocante à responsabilidade civil, penal e administrativa, tais quais:

15.7.1 Provocar a iniciativa do Ministério Público, nos termos do art. 101 da Lei nº 8.666 e art.27 do Código de Processo Penal,

15.7.2 Oficiar ao Tribunal de Contas da União, em face do artigo 46 da Lei nº 8.443/92.

15.7.3 Instaurar processos administrativos, em face da Lei nº 12.846/13.

15.7.3.1 Quando houver indícios de prática de infração administrativa tipificada pela Lei nº12.846/13, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da

empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

15.7.3.2 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

15.7.3.3 O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

15.8 As penalidades serão registradas no SICAF e, no caso de penalidades aplicadas a pessoas físicas ou jurídicas que impliquem restrição ao direito de contratar ou licitar com a Administração Pública, independentemente de seu fundamento legal, também serão registradas no Sistema de Gestão de Procedimentos de Responsabilização de Entes Privados – CGU-PJ.

16. CRITÉRIO DE REAJUSTAMENTO DE PREÇOS

16.1 Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

16.2 Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se, na forma definida no instrumento convocatório ou no contrato, o Índice de Custo de Tecnologia da Informação - ICTI/IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

17. RESCISÃO

17.1 O Contrato originado por este Termo de Referência poderá ser rescindido, por ato unilateral e escrito da Administração, sem prejuízo das demais sanções do contrato ou do instrumento convocatório, em caso de:

17.1.1 Hipóteses previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei;

17.1.2 Mora, sem prejuízo das multas aplicáveis, que evolui em intensidade e se resolve em inadimplemento total da obrigação;

17.1.3 Caracterização da insolvência do CONTRATADO com envolvimento comprovado em protesto de títulos e emissão de cheques sem a suficiente provisão de fundos ou outro fato semelhante que represente risco à sua saúde financeira.

17.1.4 Falta de manutenção das condições de habilitação e qualificação, exigidas no instrumento convocatório e/ou contrato.

17.2 O Contrato poderá ser rescindido amigavelmente, por acordo entre as partes, desde que haja conveniência para a Administração e não tenha ocorrido nenhuma das hipóteses previstas para a rescisão unilateral da avença, conforme os termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

17.3 Os casos de rescisão contratual serão formalmente motivados, assegurando-se ao CONTRATADO o direito à prévia e ampla defesa.

17.4 A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

17.5 O termo de rescisão será precedido no processo administrativo por nota técnica emitida pelo Gestor, com aprovação da autoridade superior, cujo conteúdo deverá apresentar:

17.5.1 Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

17.5.2 Relação dos pagamentos já efetuados e ainda devidos;

17.5.3 Relação dos processos de apuração de responsabilidade administrativa instaurados, e de indenizações e multas conferidas.

17.6 Não havendo culpa do CONTRATADO a rescisão poderá ser acompanhada, no que couber, do ressarcimento de prejuízos comprovadamente suportados pelo CONTRATADO, da devolução da garantia, do pagamento pela execução até a rescisão e cobertura do custo de desmobilização.

17.7 O contrato poderá ser rescindido no caso de se constatar a ocorrência da vedação estabelecida no art. 5º do Decreto nº 9.507, de 2018.

18. EXIGÊNCIAS PARA PARTICIPAÇÃO NA LICITAÇÃO E QUALIFICAÇÃO DO PRESTADOR DO SERVIÇO OU FORNECEDOR

18.1 **Vistoria obrigatória do local de execução dos serviços, pelo licitante, ou seu representante devidamente identificado, para que seja formulada a proposta licitatória:** Não se aplica.

18.2 **Solicitação de prova de conceito:** Não se aplica.

18.3 **Licenças, alvarás, autorizações, comprovações de propriedade e outros:** Não se aplica.

18.4 **Qualificação Econômico-Financeira**

18.4.1 Certidão negativa de falência, recuperação judicial, ou extrajudicial: expedida pelo cartório de distribuição da sede da licitante.

18.4.2 Balanço patrimonial e Demonstrações Contábeis do último exercício social: apresentados na forma da lei, com protocolo na respectiva junta comercial,

comprovando índices de Liquidez Geral, Solvência Geral e Liquidez Corrente superiores a 1 (um).

18.4.3 Comprovação de Patrimônio Líquido de no mínimo 10% (dez por cento) do valor estimado da contratação.

18.5 **Qualificação Técnica**

18.5.1 **Prova de atendimento a requisitos previstos em lei especial:** Não se aplica.

18.5.2 **Comprovação de aptidão para o desempenho de atividade pertinente e compatível** em características, quantidades e prazos com o objeto licitatório, por meio do:

18.5.3.1 Atestado (s) de Capacidade Técnica expedido(s) por pessoa jurídica de direito público ou privado em nome do licitante, comprovando o fornecimento de solução de antispam para no mínimo 1.000 (hum mil) caixas postais, compreendendo o serviço de instalação e o serviço suporte técnico, este último prestado por no mínimo 1 (hum) ano.

18.5.3.2 Os atestados apresentados deverão referir-se a serviços prestados no âmbito da atividade econômica principal ou secundária especificadas no contrato social vigente da licitante.

18.5.3.3 O licitante deverá disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, podendo ser solicitado a apresentar, dentre outros documentos a cópia do contrato que deu suporte à contratação ou a informar o endereço atual da contratante e local em que foram prestados os serviços.

18.5.3 **Declaração de que possui ou instalará escritório em Brasília-DF, a ser comprovado no prazo de até 60 (sessenta) dias contado a partir da vigência do contrato**: Não se aplica.

18.5.4 **Certificado de Entidade Certificadora:** Não se aplica.

18.5.5 **Registro ou inscrição na entidade profissional/ocupacional competente, demonstrando objeto social e formação de Responsável Técnico compatíveis com o objeto:** Não se aplica.

18.5.6 **Indicação de Responsável Técnico, detentor de atestado técnico e/ou de Certificado de Entidade Certificadora, registro na entidade profissional/ocupacional competente, com vínculo empregatício com a LICITANTE a ser comprovado no momento da assinatura do contrato:** Não se aplica.

18.5.7 **Indicação de Equipe Técnica, com a seguinte formação e experiência profissional:** Não se aplica.

18.5.8 **Outras observações:**

18.5.8.1 Declaração emitida pela licitante informando que possuirá na assinatura do contrato equipe técnica certificada pela fabricante da solução ofertada, qualificada para execução dos serviços de instalação e suporte técnico na solução de antispam ofertada.

18.6 A comprovação técnica de atendimento de todos os requisitos da especificação técnica deverá ser realizada por meio da apresentação de catálogos, manuais ou guias, todos oficiais do fabricante, em mídia digital ou através de links de internet para download, bem como pela apresentação de planilha ponto-a-ponto com a comprovação de atendimento de cada requisito, com a indicação do nome do documento e página.

19. ANEXOS DO TERMO DE REFERÊNCIA

19.1 Anexo A do Termo de Referência – Orçamento;

19.2 Anexo B do Termo de Referência – Termo de Compromisso de Manutenção de Sigilo;

19.3 Anexo C do Termo de Referência – Termo de Ciência de Manutenção de Sigilo para Colaboradores;

19.4 Anexo D do Termo de Referência – Atividades de Gestão e Fiscalização da Execução Contratual;

19.5 Anexo E do Termo de Referência - Modelo de Ordem de Fornecimento/Serviço;

RECOMENDAÇÃO

Visando resultados objetivos, a fim de atingir a eficiência e eficácia, com redução de esforços e economia de recursos financeiros, bem como maior celeridade ao processo, solicita-se a aprovação da autoridade competente.

INTEGRANTE REQUISITANTE	INTEGRANTE ADMINISTRATIVO	INTEGRANTE TÉCNICO
ANDRÉ GUSTAVO DE ANDRADE MOREIRA Analista Administrativo – SGI SIAPE nº: 1863983	ARNALDO JOSÉ FERNANDES JUNIOR Analista Administrativo – SLC SIAPE nº: 1522568	IGO RODRIGUES DE CASTRO Analista Administrativo – SGI SIAPE nº: 1912777

DE ACORDO E APROVAÇÃO DA AUTORIDADE COMPETENTE

De acordo.

Em atenção ao disposto no art. 50 da Lei nº9.784/1999, aprovo este Termo de Referência e acrescento que esta contratação é necessária para dar o apoio necessário às atividades a serem desempenhadas pela ANEEL.

Ressalto que as especificações técnicas do objeto estão limitadas às exigências da demanda, e não contém minúcias excessivas, irrelevantes ou desnecessárias, que limitem a competição.

Sendo assim, quanto à formalização, aprovo na íntegra sua estruturação, estando todos os elementos necessários à instrução processual devidamente demonstrados, e adequados aos termos da legislação concernente à contratação na Administração Pública.

Destaco ainda que a contratação, objeto deste Termo de Referência, não implica a criação, expansão ou aperfeiçoamento de ação governamental; e que os serviços a contratar podem ser objeto de execução indireta na Administração Pública federal direta, autárquica e fundacional, de acordo com as hipóteses estabelecidas pelo Decreto nº 9.507/2018 e pela Portaria nº 443/2018.

_____

ISSAO HIRATA
SUPERINTENDENTE DE GESTÃO TÉCNICA DA INFORMAÇÃO - SGI
SIAPE nº: 3352541

Anexo A do Termo de referência- Orçamento

1. Após definição da solução viável – Contratar solução de antispam – conforme detalhado no documento Estudo Técnico Preliminar da Contratação (SICNET2 48540.001282/2021-00) a SGI realizou uma pesquisa de preços conforme descrito na Instrução Normativa nº 73, de 5 de agosto de 2020, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

2. Para tanto, foi realizada inicialmente a pesquisa diretamente no painel de preços. Foram pesquisados no referido portal tanto em "material" como "serviço" as compras públicas ocorridas neste ano e no ano de 2020 que continham as seguintes expressões no campo "objeto da compra": antispam ou filtragem de e-mails.

3. A partir dos dados informados nos relatórios do painel de preços, os documentos das contratações foram então pesquisados e obtidos diretamente do portal Comprasnet, as contratações cujo objeto se mostraram similares ao objeto de contatação desse estudo (Anexo I deste estudo).

Tabela 1 - Pesquisa de Preços - FONTE: Painel de Preços								
Órgão ou entidade	**Descrição do objeto**	**Detalhamento do objeto**	**Empresa**	**Prazo**	**Qtd.**	**Valor Unitário**	**Valor Total**	**Marca**
Aquisições de Solução								
Arquivo Nacional (P.E. 10/2020)	Aquisição de Solução de Antivírus, Antispam, para todo ambiente de rede do Arquivo Nacional – Ministério da Justiça e Segurança Pública, nas condições, quantidades e exigências estabelecidas neste Instrumento...	Solução de segurança antispam e email gateway	HSC DESENVOLVIMENTO E SERVICOS EM TECNOLOGIA DA INFORMAÇÃO	12 meses	750	**89,84 (A)** por caixa postal/ano	67.380,00	HSC
INEP (P.E. 19/2020)	Contratação de subscrição de solução para filtragem e proteção das mensagens de correio eletrônico, contemplando todos os softwares e suas licenças de uso, incluindo serviços de implantação, suporte técnico especializado e fornecimento de hardware durante o período de garantia	Subscrição Solução de Segurança para Serviço de E-mail para 2500 caixas postais – por 48 meses.	BLUE EYE SOLUCOES EM TECNOLOGIA LTDA	48 meses	2.500	388,90 por caixa postal/ano	3.889.000,00	HSC
Ministério da Economia (P.E. 6/2020)	Objeto: Pregão Eletrônico - Contratação de serviços de solução de Antivírus e solução de Antispam para	Serviço de Licenciamento de uso da solução de Antispam com atualização continuada, conforme especificações contidas	HSC DESENVOLVIMENTO E SERVICOS EM TECNOLOGIA DA INFORMAÇÃO	12 meses	25.000	10,40 por caixa postal/ano	260.000,00	HSC

	execução em ambiente computacional do Ministério da Economia, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.	em Termo de Referência.						
		Serviço de suporte técnico (software/equipamento) on-site (Brasília -DF) ou remotamente 24x7, conforme termo de referência.			12	6.666,66 por mês	79.999,92	
TRE-PB (P.E. 38/2020)	Contratação de empresa especializada para prestação do serviço de fornecimento de uma solução de filtragem de e-mails para atender às necessidades do Tribunal Regional Eleitoral da Paraíba.	VIRTUAL APPLIANCE PARA FILTRAGEM DE E-MAIL COM SUPORTE PARA 36 (TRINTA E SEIS) MESES E COM SUBSCRIÇÃO PARA 2.000 CAIXAS DE E-MAIL.	FAST HELP INFORMATICA LTDA	36 meses	2.000	21,50 por caixa postal/ano	129.000,00	HSC
Renovações de solução								
CREA-PR P.E (P.E. 26/2020)	Prestação de serviços de renovação do licenciamento de uso de programas de computador do tipo antivírus e antispam do fabricante Trend Micro, e serviços de suporte.	-	PBI INFORMATICA LTDA	12 meses	1	179.799,00 por ano	179.799,00	Cisco
FURNAS (P.E 141/2020)	Aquisição de licenças de uso para o equipamento de segurança AntiSpam CISCO IronPort Série C e licença de centralizador de configuração e relatórios para o equipamento CISCO IronPort Série M, conforme edital. Apresentar preço global total para o fornecimento.	-	NTT BRASIL COMERCIO E SERVICOS DE TECNOLOGIA LTDA	12 meses	1	197.055,00 por ano	197.055,00	Cisco
Governo do Estado do Ceará (P.E. 1055/2020)	Licença Unified (UTM) Protection (FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud) válida por 36 (trinta e seis) meses com suporte técnico telefônico do fabricante em regime de atendimento 24x7 para equipamentos Fortigate 1000D.	-	MORPHUS TECNOLOGIA DA INFORMACAO LTDA	36 meses	2	89.333,33 por equipamento/ ano	536.000,00	Fortinet
INB (Indústrias Nucleares do Brasil) (1002/2021)	Fornecimento de solução VIRTUAL CISCO IRONPORT EMAIL SECURITY APPLIANCE, com 1.500 licenças de antispam, antivírus, VOF (Vírus Outbreak Filter) e do respectivo	Item 1 - Cessão temporária de direitos sobre solução VIRTUAL CISCO IRONPORT EMAIL SECURITY APPLIANCE, com 1.500 licenças de antispam, antivírus, VOF (Vírus Outbreak Filter).	YSSY SOLUCOES S.A.	36 meses	1.500	41,90 por caixa postal/ano	188.550,00	Cisco

	serviço de implantação/migração, posto CIF nas Indústrias Nucleares do Brasil S/A - INB	Item 2 - Serviços de Instalação, Transição e Configuração / Parametrização de Software		-	1	17.450,00 por ano	17.450,00	
INMETRO (P.E. 2/2020)	Aquisição de soluções de E-mail Gateway (AntiSpam) e de Endpoint Protection Platform (EPP), de forma integrada as suas unidades regionais do Rio de Janeiro, Porto Alegre, Goiânia e Brasília, incluindo suporte e direito de atualização por 36 (trinta e seis) meses, bem como serviçosde instalação e configuração	Licenças do E-mail Gateway (Antispam) com suporte e atualizações por 36 (trinta e seis) meses,	DMK3 TECNOLOGIA LTDA	36	3.050	34,10 por caixa postal/ano	311.984,50	Kaspersky
MS - Instituto Nacional de Traumato-Ortopedia - RJ (P.E. 9/2021)	Pregão Eletrônico - Aquisição de Ferramentas de Segurança de rede (antispam, antivírus e outros)..	Aquisição de Licença do APPLIANCE ANTISPAM	PTLS SERVICOS DE TECNOLOGIA E ASSESSORIA TECNICA LTDA	36 meses	1.500	33,11 por caixa postal/ano	148.995,00	Cisco

4. Os resultados das consultas foram então divididos na tabela acima em “aquisições de solução” - para pregões abertos em que foram adquiridas novas soluções pela organização - e “renovações de solução” - para pregões com indicação de marcas e inclusão de part numbers;

5. Após a análise do edital das aquisições verificou-se que apenas o pregão realizado no Arquivo Nacional (P.E. 006/2020) possui similaridade na especificação técnica do objeto e na quantidade demandada desta contratação em estudo. Observou-se também que no pregão do ME a quantidade contratada (25.000) está muito acima do perseguido pela ANEEL (4.100). No pregão do INEP, apesar também da similaridade da solução dos requisitos funcionais da solução com a deste estudo, a análise detalhada do termo de referência mostrou que a solução foi ofertada com inclusão de vários hardwares e que o preço de cada hardware não foi discriminado na proposta, não sendo considerada como uma boa referência para a estimação do preço em tela. Por fim, a análise detalhada do objeto do edital do pregão realizado no TRE-PB também mostrou que a solução especificada não possui todos os requisitos ou recursos técnicos que são demandados pela solução da ANEEL na contratação em tela, sendo dessa forma considerada inadequada para constar como estatística para o cálculo de preço estimado de referência.

6. Em seguida, na verificação das contratações cujo objeto eram renovações com uso dos termos supracitados na filtragem do painel observou-se que se tratava de renovações de soluções de marcas diversas (CISCO, KASPERSKY, FORTINET) da utilizada pela ANEEL (SYMANTEC) e que, com isso, também não foram consideradas adequadas para compor os preços estimados uma vez que a estratégia da contatação em análise nesse ponto é renovar a atual.

7. Sendo assim, foi necessário buscar pelo termo “Symantec” direto no campo “objeto de compra” na referida ferramenta, tendo em vista a necessidade de se pesquisar os preços da realização de uma possível renovação da solução instalada na ANEEL.

8. Pesquisando dessa forma, foram obtidas as seguintes contratações no painel: PE 36/2020 do CPRM, PE 26/0220 do CRF-SP (Conselho Regional de Farmácia do Estado de São Paulo), PE 23/2020 da Secretaria Executiva da Fazenda do Estado do Pará e PE 12/2020 do Conselho de Arquitetura e Urbanismo de São Paulo. Entretanto, a análise do edital e do objeto de cada uma delas também mostrou que faziam referência somente à renovação de produtos não-similares ao do objeto da contratação em questão, a saber: plataformas de proteção de endpoint (antivírus) e aplicativo de backup, não sendo, portanto, consideradas adequadas para compor a pesquisa de preço para contratação em questão.

9. Em suma, a pesquisa realizada no painel de preços resultou na obtenção de apenas uma contratação considerada adequada para compor os preços médios de referência: P.E. 10/2020 ocorrido no Arquivo Nacional. Nela, o valor unitário por ano por caixa postal resultante do pregão foi de R$ 89,84 e o fabricante da solução ofertada foi a HSC (High Security Center – Brasil).

10. Sendo assim, na inexistência de outros preços para compor um preço médio de referência com no mínimo 3 (três) contratações públicas, foi necessário complementar essa pesquisa com realização de consulta direta com fornecedores, uma vez que não há pesquisa publicada em mídia especializada, sítios eletrônicos especializados ou de domínio amplo, apresentando data e hora de acesso, e realizada dentro do período de até 6(seis) meses anteriores da publicação do instrumento convocatório e o objeto desta contratação também não consta no catálogo de soluções de TIC previsto na Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019.

11. Informa-se que a solução será contratada por um curto período - 12 meses - tendo em vista a provável migração das caixas postais da Agência para o serviço de nuvem Exchange Online da Microsoft. Entretanto, na eventual ocorrência de caso fortuito ou de força maior ou mudança de orientação estratégica que impossibilite ou postergue a contratação do serviço do Exchange Online, se faz necessário prever a possibilidade de renovação da solução. Sendo assim, previu-se a realização de renovação da contratação anualmente, até o limite de cinco anos, caso permaneça as condições econômicas vantajosas para a ANEEL. O quantitativo de caixas postais da ANEEL (usuários e institucionais) foi dimensionada em 4.100 (quatro mil e cem), para um contingente de uso por 1.200 usuários (servidores e demais colaboradores).

12. Nesse sentido, foi obtida a lista de revendas nos sítios dos principais fabricantes de soluções de antispam disponíveis no mercado nacional, a saber: Symantec, Cisco, Trend Micro, Proofpoint e HSC e foram encaminhadas às empresas listadas na Tabela 2 abaixo, por email, as solicitações de cotações de preços, contendo valor unitário e valor total, para os seguintes objetos:

    a. Contratação de solução de antispam contemplando fornecimento de licenças de subscrição de software para 4.100 caixas postais, instalação, garantia, repasse de conhecimento e suporte técnico por 12 (doze) meses, prorrogáveis anualmente, até o limite de 60 (sessenta) meses, conforme especificação técnica enviada; e

    b. Renovação de garantia de atualizações de versões e suporte técnico da atual solução de antispam SMG (Symantec Message Gateway) para 4.100 caixas postais da ANEEL, por 12 (doze) meses, prorrogáveis anualmente, até o limite de 60 (sessenta) meses e Aquisição

de módulo de Sandbox da solução SMG para 4.100 caixas postais, contemplando instalação, garantia de atualizações e suporte técnico por 12 (doze) meses, prorrogáveis anualmente, até o limite de 60 (sessenta) meses.

Tabela 2 - Revendas consultadas	
Empresa	**Representante**
Blue Eye Soluções em Tecnologia	HSC, Symantec
Norden Tecnologia	HSC, Proofpoint, Symantec (Broadcom)
Fasthelp Segurança	HSC, Trend Micro, Symantec (Broadcom)
Alltech Soluções	Trend Micro
Aproach Tecnologia	Cisco
GlobalSec Tecnologia	Cisco

13. O conteúdo de cada uma das propostas comerciais recebidas foi sintetizado nas tabelas 3 e 4 a seguir (contratação versus renovação – com/sem módulo de sandbox) e estão detalhadas no Anexo II deste Estudo. Ressalta-se que algumas revendas interpretaram que o valor unitário a ser informado na pesquisa era para o quantitativo de 1 (uma) solução e não por caixa postal e que, com isso, informaram o valor unitário igual ao valor total da contratação.

14. Com isso, visando representar nas tabelas 3 e 4 o valor unitário por caixa postal de cada contratação, foi então realizada a operação de divisão do valor total informado em cada proposta por 4.100 (quatro mil e cem) resultando, em alguns casos, em valores com dízimas periódicas, que foram representados nas tabelas com apenas 2 (duas) casas decimais, sem aproximações. Dessa forma, nesses casos, se multiplicados tais valores unitários por 4.100 (quatro mil e cem) para obtenção dos valores totais das contratações, eles serão ligeiramente inferiores aos valores totais informados nas tabelas abaixo que foram transcritos diretamente das propostas enviadas pelas empresas.

Tabela 3 - Pesquisa de Preços - FONTE: Revendas Contratação de Solução de Antispam (alínea I do item 8.3.2.13 acima)			
Empresa	**Marca**	**Contratação aberta**	
		Valor Unitário (R$)	**Valor Total (R$)**
Alltech	Trend Micro	198,82	815.200,00
Aproachtech	Trend Micro	192,40	788.840,00
Blue Eye	Broadcom	240,89	987.649,00
FastHelp	HSC	163,41	670.000,00
Globalsec	Cisco	165,89	680.150,00
Norden	HSC	156,28	640.749,00
Valor Unitário Médio (R$)		186,28 (B)	-
Valor Total Médio (R$)			763.764,67

Tabela 4 - Pesquisa de Preços - FONTE: Revendas

Renovação de garantia de atualizações e suporte técnico da solução Symantec atual da ANEEL (alínea II do item 8.2.3.13 acima)				
Empresa	**Renovação sem módulo de Sandbox (situação atual da solução da ANEEL)**		**Renovação com módulo de Sandbox (para atendimento de novos requisitos técnicos demandados)**	
	Valor Unitário (R$)	**Valor Total (R$)**	**Valor Unitário (R$)**	**Valor Total (R$)**
Blue Eye	200,01	820.041,00	345,11	1.414.951,00
Fast Security	205,00	840.500,00	353,00	1.447.300,00
Norden	192,89	790.876,00	332,30	1.362.457,00
Valor Unitário Médio (R$)	199,30	-	343,47	-
Valor Total Médio (R$)		817.139,00	-	1.408.236,00

15. Da tabela 4 acima verifica-se inicialmente que o valor unitário médio por caixa postal da renovação da solução Symantec da ANEEL, sem adicionar novo módulo de segurança necessário para tornar a filtragem mais eficaz contra a entrada de spams modernos, foi de R$ 199,30. Esse valor é 6,98 % superior ao valor unitário médio obtido na realização de uma nova contratação de soluções concorrentes contidas na tabela 3 (R$ 186,28), que já incluem o módulo de sandbox.

16. Também foi estimado o preço da renovação da solução atual adicionando o módulo de sandbox, que traria maior segurança e tornaria a solução compatível com a especificação técnica utilizada para cotar preços das outras fabricantes da tabela 3. Nessa pesquisa, o valor unitário médio da renovação da solução obtido foi de R$ 343,47, mostrando-se superior em 84,36% ao valor unitário médio da realização de uma nova contratação de produto concorrente de fabricante que cotou preços à ANEEL (R$ 186,28).

17. Com isso, verifica-se que do ponto de vista econômico a opção mais adequada entre as duas avaliadas (contratação de nova solução versus renovação - com/sem sandbox) é a realização de uma nova contratação de solução de antispam devido ao menor valor estimado dessa estratégia. Dessa forma e para fins desse estudo, os valores estimados obtidos para a renovação da solução Symantec da ANEEL foram então desconsiderados para o cálculo dos valores finais de referência da contratação em tela.

18. Isto posto, o preço unitário final de referência para a contratação foi obtido por meio da média aritmética entre o valor unitário da contratação ocorrida no pregão do Arquivo Nacional (R$ 89,84), obtida por meio da pesquisa no painel de preços, e o valor unitário médio das propostas comerciais recebidas específicas para contratação de nova solução. O preço total de referência da contratação foi então obtido por meio do produto entre o preço unitário de referência e a quantidade de caixas postais demandada pela Agência (4.100):

Tabela 5 - Preços Finais de Referência para a Contratação		
Objeto da contratação	**Valor Unitário (R$) Fonte: Painel de Preços**	**Valor Unitário (R$) Fonte: Pesquisa com Fornecedores**
Contratação de solução de antispam contemplando fornecimento de licenças de subscrição de software para 4.100 caixas postais, instalação, garantia, repasse de conhecimento e suporte técnico por 12 (doze) meses, prorrogáveis anualmente, até o limite de 60 (sessenta) meses.	**89,84 (A)**	**186,28 (B)**
Valor Unitário de Referência (R$) C = (A+B)/2	**138,06** (C)	
Valor Global de Referência (R$) D = (C*4.100)	**566.046,00** (D)	

Anexo B do Termo de Referência - Termo de Compromisso de Manutenção de Sigilo

*A **AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA - ANEEL** sediada em Brasília – DF, SGAN 603, Módulo "j", CEP: 70.830-110, inscrita no CNPJ/MF sob o n° 02.270.669/0001-29, doravante denominada **CONTRATANTE**, e, de outro lado, a (NOME DA EMPRESA), sediada em (ENDEREÇO), CNPJ nº (CNPJ), doravante denominada **CONTRATADA**;*

*CONSIDERANDO que, em razão do CONTRATO nº **XX/20XX** doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a **informações sigilosas** do CONTRATANTE;*
*CONSIDERANDO a necessidade de ajustar as condições de revelação destas **informações sigilosas,** bem como definir as regras para o seu uso e proteção;*
CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE (Norma de Organização da ANEEL nº 012 disponível em: http://www2.aneel.gov.br/cedoc/prt20153522.pdf) ;
Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

CLÁUSULA SEGUNDA – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:
***INFORMAÇÃO:** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.*
***INFORMAÇÃO SIGILOSA:** aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.*
CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

CLÁUSULA TERCEIRA – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada

durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

CLÁUSULA QUARTA – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:
I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;
II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

CLÁUSULA QUINTA – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.
I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.
I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:
I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;
III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e
IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

CLÁUSULA SEXTA – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

CLÁUSULA SÉTIMA – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

CLÁUSULA OITAVA – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.
Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tais como aqui definidas.
Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:
I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.
III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;
IV – Todas as condições, TERMO e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;
V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;
VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;
VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, será incorporado a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;
VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

CLÁUSULA NONA – DO FORO

A CONTRATANTE elege o foro de Brasília onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 (duas) vias de igual teor e um só efeito.
_____, _____ de _____ de 20____
De Acordo

CONTRATANTE	***CONTRATADA***
_____	**_____**
Nome/Matrícula	***Nome/Matrícula***
TESTEMUNHA 1	***TESTEMUNHA 2***
Nome/Qualificação/Documentos	***Nome/Qualificação/Documentos***

Anexo C do Termo de Referência - Termo de Ciência de Manutenção de Sigilo para Colaboradores

Contrato nº:			
Objeto:			
Contratante:			
Gestor do Contrato:		***Matr.:***	
CONTRATADA:		***CNPJ:***	
Preposto da CONTRATADA:		***CPF:***	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as Normas de Segurança da Informação vigentes na Contratante (Norma de Organização da ANEEL nº 12 disponível em: http://www2.aneel.gov.br/cedoc/prt20153522.pdf).

_____,_____ de _____ de 20_____.

Ciência

CONTRATADA

Funcionários

_____	_____
Nome	***Nome***
CPF:	***CPF:***
_____	_____
Nome	***Nome***
CPF:	***CPF:***

Anexo D do Termo de Referência - Atividades de Gestão e Fiscalização da Execução Contratual

1. Conforme a Instrução Normativa SGD/ME nº1/2019, a Equipe de Fiscalização a ser designada após a celebração do contrato será composta pelo GESTOR DO CONTRATO, FISCAL TÉCNICO, FISCAL REQUISITANTE e FISCAL ADMINISTRATIVO.
   1.1. Ressalte-se que os papéis dos fiscais não poderão ser acumulados pelo mesmo servidor, salvo o de FISCAL REQUISITANTE e o de FISCAL TÉCNICO; o acompanhamento e fiscalização do contrato pelos servidores designados pela CONTRATANTE não exclui nem reduz a responsabilidade do CONTRATADO, até mesmo perante terceiros, por qualquer irregularidade, inclusive resultante de imperfeições técnicas, emprego de material inadequado ou de qualidade inferior, e nem implica corresponsabilidade da CONTRATANTE ou de seus agentes

2. O **GESTOR DO CONTRATO**, servidor com atribuições gerenciais, será preferencialmente da área requisitante da solução de TIC, sendo responsável, em especial, pelas seguintes atividades:
   2.1. Coordenar e comandar o processo de gestão e fiscalização do contrato;
   2.2. Convocar e realizar reunião inicial (dispensável para soluções compostas exclusivamente por fornecimento de bens de TIC) para esclarecimentos relativos às questões operacionais, administrativas e de gestão do contrato, repasse de conhecimentos necessários à execução, e disponibilização da infraestrutura, quando couber, a ser realizada conjuntamente com os fiscais do contrato (FISCAL TÉCNICO, FISCAL REQUISITANTE e FISCAL ADMINISTRATIVO) e o CONTRATADO, quando este deverá apresentar o preposto designado para a contratação, e os termos de compromisso e de ciência assinados.
   2.3. Autorizar a execução do Contrato mediante a emissão do documento indicado no Termo de Referência;
   2.4. Notificar o CONTRATADO sempre que o mesmo descumprir qualquer condição pactuada, bem como diante de ocorrências ou de circunstâncias notadas durante a fiscalização que possam prejudicar a execução, solicitando as providências necessárias;
   2.5. Receber a fatura correspondente, atestá-la se o objeto entregue e os valores cobrados estiverem de acordo com o contratado, e a mesma atender a forma estabelecida pela legislação vigente, e providenciar o pagamento no prazo e condições estabelecidas, efetuando glosa de valores errôneos, quando necessário.
   2.6. Encaminhar indicações de glosas nas notas fiscais ou faturas, quando o objeto entregue e os valores cobrados estiverem em desacordo com o contratado;
   2.7. Rejeitar, no todo ou em parte, o objeto entregue em desacordo com o instrumento contratual, comunicar formalmente e exigir do CONTRATADO as providências necessárias para sua imediata regularização, sem prejuízo das sanções e glosas cabíveis;
   2.8. Em conjunto com o FISCAL REQUISITANTE e o FISCAL TÉCNICO, confeccionar e assinar o Termo de Recebimento Definitivo – TRD com base na avaliação dos níveis de serviços prestados;
   2.9. Após a emissão do TRD, emitir autorização ao Contratado para o faturamento dos serviços, encaminhando-a ao preposto da empresa;
   2.10. Manter histórico de gestão do contrato, efetuando por despacho formal no processo administrativo da contratação, com apoio dos FISCAIS REQUISITANTE, TÉCNICO E ADMINISTRATIVO, registros formais de todas as ocorrências positivas e negativas da execução do contrato, por ordem histórica, indicando dia, mês, ano, empregados do CONTRATADO

eventualmente envolvidos, ações necessárias para a regularização das faltas ou defeitos, e dar ciência a seu superior hierárquico;

2.11. Monitorar os prazos de execução e de vigência contratual, inclusive no tocante aos procedimentos administrativos internos exigidos para sua continuidade ou encerramento.

2.12. Monitorar a execução financeira do contrato, mediante o controle de pagamentos efetuados e do recurso orçamentário, visando dar cumprimento ao cronograma financeiro.

2.13. Com base no histórico da contratação, e nos princípios da necessidade, economicidade e oportunidade, encaminhar o processo administrativo à SLC, no prazo cabível ao tipo de ajuste contratual demandado, devidamente instruído e motivado com entendimento favorável ou desfavorável à questão, sobre procedimentos referentes a:

2.13.1. Proposição de sanções;

2.13.2. Repactuações e reajustes;

2.13.3. Reequilíbrios;

2.13.4. Rescisões;

2.13.5. Prorrogações de prazos de vigência de serviços continuados (prorrogações), na forma prevista no art. 57, II, da Lei nº 8.666, de 1993;

2.13.5.1. O processo deverá estar instruído com: a) comprovação de que a forma de prestação dos serviços permanece de natureza continuada; b) comprovação de que os serviços tenham sido prestados regularmente; c) justificativa porque a ANEEL mantém interesse na realização do serviço; d) manifestação expressa da contratada concordando com a prorrogação; e) comprovação de que a contratada mantém as condições iniciais de habilitação; e f) comprovação de que o valor do contrato é mais vantajoso para a ANEEL do que a realização de nova contratação, sem prejuízo de eventual negociação com a contratada para adequação dos valores;

2.13.6. Alterações contratuais do objeto, desde que justificadas, na forma prevista no art. 65 da Lei nº 8.666, de 1993;

2.13.6.1. O processo deverá estar instruído com: a) a descrição do objeto do contrato com as suas especificações e do modo de execução; b) a descrição detalhada da proposta de alteração; c) a justificativa para a necessidade da alteração proposta e a referida hipótese legal; d) o detalhamento dos custos da alteração de forma a demonstrar que não extrapola os limites legais e que mantém a equação econômico-financeira do contrato; e) a ciência da contratada, por escrito, em relação às alterações propostas no caso de alteração unilateral ou a sua concordância para as situações de alteração por acordo das partes.

2.14. Durante a execução contratual, coordenar a equipe de Fiscalização do contrato na atualização contínua do Mapa de Gerenciamento de Riscos, e realização das seguintes atividades:

2.14.1. Reavaliação dos riscos identificados nas fases anteriores e atualização de suas respectivas ações de tratamento; e

2.14.2. Identificação, análise, avaliação e tratamento de novos riscos.

2.14.3. O Mapa de Gerenciamento de Riscos deve ser juntado aos autos do processo administrativo, pelo menos:

2.14.3.1. Ao final da elaboração do Termo de Referência ou Projeto Básico;

2.14.3.2. Ao final da fase de Seleção do Fornecedor;

2.14.3.3. Uma vez ao ano, durante a gestão do contrato; e

2.14.3.4. Após eventos relevantes.

3. O **FISCAL TÉCNICO DO CONTRATO**, servidor representante da área de TIC, será indicado para fiscalizar tecnicamente o contrato, sendo responsável, em especial, pelas seguintes atividades:
   3.1. Confeccionar e assinar o Termo de Recebimento Provisório, quando da entrega do objeto constante na Ordem de Serviço ou de Fornecimento de Bens;
   3.2. Em conjunto com o GESTOR DO CONTRATO e o FISCAL REQUISITANTE, confeccionar e assinar o Termo de Recebimento Definitivo.
   3.3. Em conjunto com o FISCAL REQUISITANTE, avaliar a qualidade dos serviços realizados ou dos bens entregues e justificativas, a partir das especificações e critérios de aceitação definidos para o objeto;
   3.4. Em conjunto com o FISCAL REQUISITANTE, identificar não conformidades com os termos contratuais;
   3.5. Em conjunto com o FISCAL ADMINISTRATIVO, verificar a manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica;
   3.6. Apoiar, juntamente com o FISCAL ADMINISTRATIVO, a verificação da manutenção da necessidade, economicidade e oportunidade da contratação, pelo FISCAL REQUISITANTE;
   3.7. Em conjunto com o FISCAL REQUISITANTE, verificar a manutenção das condições definidas nos Modelos de Execução e de Gestão do Contrato.

4. O **FISCAL REQUISITANTE DO CONTRATO**, servidor representante da área da solução de TIC, será indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista de negócio e funcional da solução de TIC, sendo responsável, em especial, pelas seguintes atividades:
   4.1. Em conjunto com o GESTOR DO CONTRATO e o FISCAL TÉCNICO, confeccionar e assinar o Termo de Recebimento Definitivo.
   4.2. Com apoio dos FISCAIS TÉCNICO e ADMINISTRATIVO verificar a manutenção da necessidade, economicidade e oportunidade da contratação,
   4.3. Em conjunto com o FISCAL TÉCNICO, avaliar a qualidade dos serviços realizados ou dos bens entregues e justificativas, a partir das especificações e critérios de aceitação definidos para o objeto;
   4.4. Em conjunto com o FISCAL TÉCNICO, identificar não conformidades com os termos contratuais;
   4.5. Com apoio dos FISCAIS TÉCNICO E ADMINISTRATIVO, verificar a manutenção da necessidade, economicidade e oportunidade da contratação;
   4.6. Em conjunto com o FISCAL TÉCNICO, verificar a manutenção das condições definidas nos Modelos de Execução e de Gestão do Contrato.

5. O **FISCAL ADMINISTRATIVO DO CONTRATO**, servidor representante da área administrativa, será indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos, sendo responsável, em especial, pelas seguintes atividades:
   5.1. Verificar a aderência aos termos contratuais;
   5.2. Verificar as regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento;
   5.3. Receber do preposto os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados, no caso de substituição ou inclusão de empregados pela contratada;
   5.4. Em conjunto com o FISCAL TÉCNICO, verificar a manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica;

5.5. Apoiar, juntamente com o FISCAL TÉCNICO, a verificação da manutenção da necessidade, economicidade e oportunidade da contratação, pelo FISCAL REQUISITANTE.

Anexo E do Termo de Referência - Modelo de Ordem de Fornecimento/Serviço

Ordem de Fornecimento/Serviço n° XXX/201X-SGI/ANEEL**.**

1 – IDENTIFICAÇÃO

Requisitante:	Superintendência de Gestão Técnica da Informação - SGI	**Data**:	XX/XX/201X
Contratada	xxxxxxxxxxxxxxxxxxxxxxxxxx		
Contrato:	000/201X- ANEEL	**Processo**: 48500.000000/201X	

2 – DESCRIÇÃO DO ESCOPO

Descrição do serviço.

3 – ESPECIFICAÇÃO DOS PRODUTOS / SERVIÇOS E VOLUMES

ID	PRODUTO / SERVIÇO
1	Exemplo: XXX

4 – CRONOGRAMA

	Tarefa	Início	Fim
	XXX	00/00/201X	00/00/210X

5 – INSTRUÇÕES COMPLEMENTARES

Termo de Concordância CONTRATADA	Termo de Autorização ANEEL
Concordamos com todas as informações e condições da presente Ordem de Serviço, comprometendo-nos a cumprir prazos, especificações e requisitos de qualidade. Brasília, 00/00/20xx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx Preposto Contratada	Autorizamos a execução dos serviços acima descritos, de acordo com as informações e condições da presente Ordem de Serviço. Brasília, 00/00/20xx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx Matrícula: 0000000 Gestor do Contrato