

Diretoria de Operações, Engenharia e Tecnologia
Gerência Executiva de Tecnologia da Informação
Gerência de Infraestrutura, Suporte e Atendimento - DF/MA

Projeto Básico nº 0342858/2026/GISDF/GXTIN/DOTEC-EBC

PROJETO BÁSICO

UNIDADE DEMANDANTE: Gerência Executiva de Tecnologia da Informação

DIRETORIA RESPONSÁVEL: Diretoria de Operações, Engenharia e Tecnologia - DOTEC

A CONDIÇÕES GERAIS DA CONTRATAÇÃO

A.1. O objeto desta contratação consiste na **continuidade** da prestação de Serviço de Solução de Segurança da Informação do tipo Next Generation Firewall (NGFW), que contempla a manutenção da Solução de Firewall existente e do Serviço de SOC (Security Operations Center - Centro de Operação de Segurança), por um período de 180 (cento e oitenta) dias, garantidas as atualizações de versões, *patches* de segurança e *updates* de assinaturas contra ameaças por todo o período contratado.

A.2. A contratação abrange à manutenção das funcionalidades já contratadas e em operação da solução da marca Forcepoint, sem ampliação de escopo, sem incorporação de novas funcionalidades e sem aquisição de novos equipamentos, de modo a atender ao requisito legal de limitação da contratação aos bens e serviços necessários ao atendimento da situação emergencial. As especificações técnicas, os requisitos da contratação e os quantitativos estão detalhadamente descritos no **Encarte A** deste Projeto Básico.

A.3. Atualmente, a EBC possui contrato vigente para a prestação destes serviços (**Contrato EBC/DOTEC nº 051/2021**), cujo término está previsto, de forma improrrogável, para 04 de outubro de 2026. A presente contratação emergencial justifica-se pela impossibilidade material de conclusão tempestiva do certame licitatório definitivo e implantação da nova solução (**Processo SEI nº 53400-004736/2026-58**), associada à inviabilidade técnica de realização de uma migração complexa de infraestrutura de perímetro em curto prazo. A interrupção abrupta dos serviços de NGFW e SOC acarretaria vulnerabilidade crítica à rede corporativa e risco iminente de paralisação das atividades-fim de radiodifusão e jornalismo da Empresa Brasil de Comunicação SA.

A.4. O prazo de vigência da presente contratação será de **180 (cento e oitenta) dias** contados do início do prazo de execução dos serviços emergenciais, sendo expressamente **vedada a sua prorrogação**.

B DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

B.1. A solução deverá contemplar plataforma integrada de segurança cibernética composta pelos seguintes itens:

Item	Descrição	CATSER/CATMAT	Unidade	Quantidade
01	Serviço de Solução de Firewall da EBC (solução em cluster em: Brasília - DF, Rio de Janeiro - RJ, São Paulo SP, São Luis - MA e Tabatinga - AM	27014	subscrição	1 (serviço), com suporte e garantia por 180 (cento e oitenta) dias, que serão pagos de forma mensal
02	Serviço de SOC (Security Operations Center - Centro de Operação de Segurança). Serviço especializado na solução de Firewall	27014	subscrição	Por 180 (cento e oitenta) dias, que serão pagos de forma mensal.

B.2. As especificações técnicas detalhadas e os quantitativos por localidade estão descritos no **Encarte A** deste Projeto Básico.

C FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

C.1.1. A continuidade dos serviços de segurança de rede é o principal objetivo a ser alcançado, tendo em vista que a falta de uma Solução de Segurança da Informação do tipo Next Generation Firewall causaria transtornos de alto impacto aos negócios da EBC, como invasões de sistemas e mau funcionamento decorrente de ameaças cibernéticas. Atualmente, a Empresa Brasil de Comunicação possui uma Solução de Firewall do fabricante Forcepoint, com performance satisfatória dos hardwares e softwares, instalada em Brasília/DF, Rio de Janeiro/RJ, São Paulo/SP, Maranhão/MA e Tabatinga/AM, operando de forma redundante, com 02 (dois) equipamentos por praça e software de gerenciamento centralizado de toda a solução.

C.1.2. Toda informação gerada, armazenada, processada, transmitida e descartada por qualquer agente público é considerada um bem valioso. As informações podem ser geradas e manipuladas de diversas formas: mensagens e arquivos eletrônicos, internet, meio impresso, verbal, entre outros. Independente da forma, quatro aspectos da informação norteiam a sua segurança:

- a) Confidencialidade: a informação só deve ser acessível a quem tem a devida autorização;
- b) Integridade: a informação deve manter-se inalterada desde a sua geração ou alteração autorizada;
- c) Disponibilidade: a informação deve estar sempre disponível às pessoas autorizadas;
- d) Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

C.1.3. O Stateful Firewall tem por objetivo a criação de uma barreira entre diversos pontos da rede de dados, criando uma solução tolerante a falhas em alta disponibilidade e que atenda às necessidades de segurança da informação da EBC. Ele implementa a filtragem dos pacotes que trafegam pela rede, bloqueando o tráfego de pacotes não autorizados. É considerado mecanismo básico e obrigatório em qualquer ambiente de rede corporativo. O controle de aplicações permite a definição de políticas de acesso a determinados serviços na rede mundial de computadores, diminuindo a possibilidade de ameaças existentes nesses sítios. Já o IPS possibilita decisões de acesso baseadas no conteúdo da aplicação. Havendo a interação com o firewall dentro do NGFW, as inspeções de segurança se tornam mais profundas e correlacionadas. A análise de malware "zero-day", baseada em nuvem, busca ter acesso a uma base de dados constantemente atualizada, que identifica quais arquivos estão sendo tratados como maliciosos, bloqueando-os em caso de tentativa de entrada na rede interna. Por fim, a identificação de usuários com controle granular de permissões permite que acessos sejam customizados para diferentes grupos de usuários, de acordo com a necessidade da organização.

C.1.4. O Next Generation Firewall (NGFW) permite a interação das seguintes funções em um mesmo equipamento:

- a) Firewall Corporativo (Stateful Firewall);
- b) Controle de aplicações (AVC-Application Visibility Control);
- c) Prevenção de ameaças (IPS-Intrusion Prevention System);
- d) Análises de malware "zero-day" baseada em nuvem (Cloud-Based Sandboxing);
- e) Filtro de URL (URL Filtering); e Identificação de usuários com controle granular de permissões.

C.1.5. Assim, será necessária a contratação como serviços de uma a Solução de Firewall, para continuar provendo acesso à internet de forma segura, bem como as transmissões de dados entre as praças da EBC, com logs de acesso e controle de banda, entre outras funcionalidades NGFW (Next Generation Firewall).

C.1.6. Os benefícios s serem obtidos compreendem:

- Evitar a descontinuidade dos serviços de segurança de perímetro da rede corporativa da EBC, garantindo a proteção ininterrupta nas cinco praças (Brasília/DF, Rio de Janeiro/RJ, São Paulo/SP, Maranhão/MA e Tabatinga/AM);
- Promover uma transição contratual segura diante das necessidades atuais da empresa, considerando que todos os empregados da regional de São Paulo estão operando via cliente VPN em razão da mudança da sede, cujo cronograma físico foi alterado por meio da decisão aprovada na 9ª Reunião Ordinária da Diretoria Executiva, realizada em 22/07/2026, o que torna a disponibilidade e a segurança do acesso remoto ainda mais crítica nesse período;
- Proteger e controlar o tráfego de dados corporativos entre as praças interligadas e destas com a internet, da manutenção dos serviços de tieline, mochilink, além do tráfego intensificado de VPN decorrente da operação remota da regional de São Paulo;
- Garantir a confidencialidade, integridade e disponibilidade de informações da EBC;
- Assegurar prazo hábil e seguro para a conclusão do processo licitatório definitivo (**Processo SEI nº 53400-004736/2026-58**) e implantação da solução, sem comprometer, nesse ínterim, a proteção cibernética da Empresa, além do o acesso dos usuários a VPN cliente;
- Preservar a continuidade das atividades da EBC, produção e distribuição de conteúdo de comunicação pública, evitando prejuízos institucionais decorrentes de eventual incidente cibernético ou indisponibilidade de rede.

C.1.7. Considerando a iminência do encerramento do amparo contratual vigente e o risco inaceitável de interrupção dos serviços, a equipe de planejamento da contratação optou por requerer a contratação emergencial de continuidade da Solução de Segurança da Informação do tipo Next Generation Firewall e do Serviço de SOC (Security Operation Center).

C.1.8. A contratação dos serviços objeto deste Projeto Básico contempla a continuidade da utilização de todos os recursos da solução atual em alta disponibilidade com duplicidade de equipamentos (cluster) e o Serviço de SOC, operando nas unidades de Brasília/DF, Rio de Janeiro/RJ, São Paulo/SP, Maranhão/MA e Tabatinga/AM. Esta contratação terá prazo improrrogável de **180 (cento e oitenta) dias**, contemplando a manutenção estrita do ambiente já em produção, sem a aquisição de novos equipamentos, sem o acréscimo de novas funcionalidades e sem a inclusão de serviços de treinamento (escopos estes reservados ao processo licitatório regular e definitivo).

C.1.9. Considerando tratar-se de um serviço essencial pelo fato de que sua descontinuidade poderia implicar numa eventual paralisação das atividades fim ou meio da Empresa, implicando em sérios prejuízos e no impedimento de a EBC cumprir sua missão (Lei nº 11.652/2008), optou-se pela contratação emergencial e pelo período estritamente necessário para continuidade dos serviços de segurança de perímetro da rede corporativa da EBC, nos termos da Lei nº 13.303/2016 e Regulamento Interno de Licitações e Contratos - RILC.

C.1.10. Diferentemente da estratégia adotada para o certame regular definitivo (Processo SEI nº 53400-004736/2026-58) – o qual prevê renovação tecnológica com novos hardwares –, a presente contratação emergencial exige a manutenção dos hardwares Forcepoint já instalados. Essa medida decorre da impossibilidade material de concluir um processo de transição técnica e migração complexa para uma nova plataforma antes do término do contrato atual, configurando a contratação temporária do suporte e licenciamento da solução existente como a única alternativa técnica viável para evitar o colapso dos serviços em curto prazo.

C.1.11. Registre-se, ainda, que foram preservadas todas as especificações técnicas do Termo de Referência da contratação anterior (Processo SEI nº 00000.001173/2020-00), adaptadas para os atuais modelos de artefato, mantidos somente os serviços necessários e compatíveis com a continuidade da solução.

C.1.12. A iniciativa está alinhada ao Planejamento Estratégico da EBC, N1 -Garantir Solução de Proteção e Segurança de Perímetro e Segurança Horizontal, M1 - Manter Segurança Ativa A01 - Manter Contrato de Segurança de Perímetro Ativo, contratar segurança de perímetro horizontal , sob o PI de custeio 7SII563C005 .

D REQUISITOS LEGAIS DA CONTRATAÇÃO

D.1. A presente contratação observará os seguintes normativos:

D.1.1. Lei nº 13.303, de 2016: Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios e dá outras providências, **especificamente o art. 29, inc. XV.**

D.1.1.1. Registra-se a observância ao art. 40 da Lei nº 13.303/16 que trata da determinação de que as empresas públicas e as sociedades de economia mista deverão publicar e manter atualizado regulamento interno de licitações e contratos, compatível com o disposto nesta Lei.

D.1.2. Regulamento Interno de Licitações e Contratos da Empresa Brasil de Comunicação S/A – RILC/EBC, atualizado pela Deliberação CONSAD nº 28/2026: Disciplina os procedimentos de licitação e contratação no âmbito da EBC, **especificamente o art. 13, inc. XIV.**

D.1.3. Lei nº 13.709, de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD).

D.1.4. Decreto nº 9.507, de 2018: Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União.

D.1.5. Instrução Normativa SLTI/MP nº 05, de 2017, ratificada pela Instrução Normativa SEGES/MP nº 98, de 2022: Dispõe sobre regras e diretrizes para a contratação de serviços continuados ou não.

D.1.6. Instrução Normativa SLTI/MP nº 65, de 2021: Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral.

D.1.7. Instrução Normativa SGD/ME nº 94, de 2022: 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.

D.1.8. Portaria SGD/MGI nº 5.950, de 2023: Estabelece modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

D.2. Além dos normativos indicados, a presente contratação será regida pelas demais disposições legais constantes deste Termo de Projeto Básico e seus Encartes.

E1 REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio

E1.1. Trata-se da necessidade imediata de provimento de continuidade dos serviços de segurança de rede, que é o principal objetivo a ser alcançado. Tendo em vista que a falta da Solução de Segurança da Informação do tipo Next Generation Firewall (NGFW) e do monitoramento contínuo via SOC (Security Operations Center) causaria transtornos de alto impacto aos negócios da EBC, a interrupção acarretaria a paralisação das atividades da Empresa, inclusive produção e distribuição de conteúdos de comunicação pública, além de invasões de sistemas e mau funcionamento decorrente de pragas cibernéticas.

Requisitos de Manutenção

E1.2. Os requisitos de manutenção refletem a necessidade estrita de continuidade ininterrupta no fornecimento do suporte e das licenças da Solução de TIC em caso de falhas durante o período emergencial. Tais requisitos

estão discriminados no **ENCARTE A** deste Projeto Básico

Requisitos Temporais

E1.3. A Solução de Segurança da Informação do tipo Next Generation Firewall deverá ser executada da seguinte forma:

E1.3.1. A prestação dos serviços deverá ocorrer de forma contínua a partir do início do prazo de execução dos serviços emergenciais, pelo prazo improrrogável de 180 (cento e oitenta) dias.

E1.3.2. Por se tratar de manutenção de uma solução já em produção no ambiente da EBC, não haverá prazo para entrega de novos equipamentos ou de instalação. A transição para o contrato emergencial deverá ocorrer sem qualquer interrupção dos serviços de segurança e rede.

E1.3.3. O recebimento provisório e definitivo não se dará por entrega de equipamentos, mas sim de forma mensal, condicionado à comprovação da prestação regular dos serviços de suporte, licenciamento e monitoramento (SOC), mediante aceite e ateste da Equipe de Fiscalização da EBC.

Requisitos de Capacitação

E1.4. Referente ao serviço de treinamento da Solução de Firewall, considerando tratar-se de contratação temporária para a continuidade de solução já operada pela equipe técnica da EBC, a exigência de capacitação e treinamentos oficiais **não se aplica**.

Requisitos de Segurança e Privacidade

E1.5. Os recursos de TI da EBC não poderão ser utilizados pela Contratada, seus empregados ou prepostos para realização de atividades alheias aos serviços previstos ou englobados nesta contratação.

E1.6. A Contratada deverá manter sob sigilo as informações de que vier a tomar conhecimento por força da contratação, abstendo-se de divulgá-las.

E1.7. A Contratada deverá respeitar as normas de segurança estabelecidas pela EBC durante a realização de atividades relacionadas ao contrato.

Requisitos Sociais, Ambientais e Culturais

E1.8. Não permitir a utilização de qualquer trabalho de menor de dezesesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho de menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

E1.9. Para esta contratação, por se tratar de continuidade de soluções de segurança, foram consideradas as mesmas condições e ambientes já adotados pela EBC, garantindo a preservação dos investimentos já feitos, de modo a gerar o menor impacto ambiental e social possível.

E1.10. A solução já instalada/configurada para uso no idioma Português Brasileiro deve seguir as normas da ABNT, conforme definido nos requisitos de negócio.

Requisitos da Arquitetura Tecnológica

E1.11. As especificações de requisitos de arquitetura tecnológica e do projeto limitam-se à conservação da arquitetura redundante (02 equipamentos por praça) já instalada nas localidades de Brasília/DF, Rio de Janeiro/RJ, São Paulo/SP, Maranhão/MA e Tabatinga/AM. Os detalhamentos estão inseridos no **Encarte A** deste Projeto Básico.

Requisitos de Projeto e de Implementação

E1.12. As descrições das Soluções estão contidas no **Encarte A**

Requisitos de Implantação

E1.13. Não se aplica. A solução já se encontra totalmente implantada, homologada e em produção na infraestrutura da EBC

Requisitos de Garantia e Manutenção da Solução

E1.14. A prestação do serviço de Solução de Segurança da Informação do tipo Next Generation Firewall, que contempla a continuidade da Solução de Firewall, atualizações de licenças, assinaturas de ameaças e o Serviço de SOC (Security Operations Center), bem como a disponibilidade do equipamento, deve ser integralmente garantida pela Contratada pelo prazo estipulado no contrato, que é de **180 (cento e oitenta) dias**

Requisito de Capacitação

E1.15. Para garantir a segurança cibernética e a continuidade dos serviços durante o período emergencial, a Contratada deverá alocar equipe técnica especializada que atenda aos seguintes requisitos mínimos:

- **Administração da Solução de Firewall:** Os profissionais responsáveis pela configuração e sustentação do *Next Generation Firewall* (NGFW) deverão possuir certificação técnica emitida pelo fabricante da solução ofertada, em nível de administrador ou superior
- **Serviço de SOC:** Os profissionais alocados no *Security Operations Center* deverão possuir experiência comprovada na operação de ferramentas de monitoramento de segurança e resposta a incidentes cibernéticos.

Requisitos de Experiência Profissional e Formação da Equipe

E1.16. Os requisitos de qualificação profissional mínima exigidos e formação da equipe estão previstos no item 5.16 do Encarte A.

Requisitos de Metodologia de Trabalho

E1.17. Não serão exigidos requisitos de metodologia de trabalho para a presente contratação.

Requisitos de Segurança da Informação e Privacidade

E1.18. A Contratada, quando da assinatura do contrato, por meio de seu representante, assinará Termo de Ciência e Manutenção de Sigilo (**Encarte E**) em que se responsabilizará pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação. O termo visa assegurar que a Contratada manterá sigilo, sob pena de responsabilidade cível, penal e administrativa:

E1.18.1. Sobre todo e qualquer assunto de interesse da EBC ou de terceiros de que tomar conhecimento em razão da execução do objeto do Contrato, devendo orientar os seus empregados nesse sentido.

E1.18.2. Sobre todas as informações relativas à prestação dos serviços, incluindo documentação, procedimentos, configurações de equipamentos, software, políticas e quaisquer informações obtidas pela Contratada em função da prestação dos serviços, mesmo após o término do prazo de vigência ou rescisão do contrato.

E1.18.3. Sobre a política de segurança adotada pela EBC e as configurações de hardware e de softwares decorrentes.

E1.18.4. Sobre eventual processo configuração e customizações de equipamentos.

E1.18.5. A Contratada não poderá efetuar, sob qualquer pretexto, a transferência de qualquer responsabilidade que lhe compete para outras entidades, sejam fabricantes, técnicos, subempreiteiros etc., sem anuência expressa da EBC.

E1.18.6. A Contratada deverá, ainda, submeter seus profissionais aos regulamentos de segurança e disciplina instituídos pela EBC, durante o tempo de permanência nas suas dependências.

E1.19. Política de Segurança

E1.19.1. O fornecedor não poderá armazenar consigo qualquer documento técnico que contemple configurações e regras de segurança aplicadas nos equipamentos implantados na rede da EBC.

- E1.19.2.** Todos os perfis de acesso e caixas postais eventualmente concedidos ao fornecedor deverão ser imediatamente excluídos após o término do contrato.
- E1.19.3.** A EBC terá propriedade sobre todos os dados, documentos e procedimentos operacionais produzidos no escopo da presente contratação.
- E1.19.4.** O fornecedor deverá respeitar as normas de segurança estabelecidas pela EBC durante a realização de atividades nas dependências da EBC.
- E1.19.5.** Não será permitida intervenção nas bases de dados, a menos que haja autorização expressa e formal da área gestora dos sistemas.
- E1.19.6.** A inclusão de componentes de software proprietários sem prévia e expressa autorização da EBC é vedada em qualquer das etapas de execução dos serviços.
- E1.19.7.** Possibilitem a rastreabilidade de forma a manter trilha de auditoria de segurança da informação;
- E1.19.8.** Assegure a continuidade do negócio implementado pela solução;
- E1.19.9.** Realizem o tratamento de dados pessoais (Lei 13709/2018) e informações classificadas, conforme legislação vigente;
- E1.20.** Prevejam a realização de auditoria de SIC (Segurança da Informação e Comunicação) de conformidade dos requisitos de segurança da informação previstos pela contratação;
- E1.20.1.** Assegurem a gestão e tratamento de incidentes de forma sistematizada;
- E1.20.2.** Indiquem diretrizes para o desenvolvimento e obtenção de software seguro.

E2

OUTROS REQUISITOS APLICÁVEIS À CONTRATAÇÃO

Participação na licitação

E2.1. Por se tratar de contratação direta, não se aplicam requisitos de participação em licitação.

E2.1.1. Também não se aplica a contratação de empresas reunidas em consórcio, por tratar-se de contratação direta da atual responsável pela solução, cuja escolha decorre da necessidade de continuidade imediata do ambiente instalado.

Formalização da contratação

E2.2. De acordo com o Regulamento Interno de Licitações e Contratos/RILC, a relação a ser estabelecida entre a EBC e a Contratada será formalizada por meio de instrumento de contrato, conforme artigo 84 do RILC/EBC.

E2.2.1. Será admitida a subcontratação exclusivamente para a central de atendimento (registro de chamados), sendo vedada a subcontratação do gerenciamento, do monitoramento (SOC) e do suporte técnico especializado, permanecendo a Contratada integralmente responsável perante a EBC pela execução do objeto, nos termos do subitem E1.18.5.

Indicação de marcas ou modelos

E2.3. A referência à marca **Forcepoint**, correspondente à solução de *Next Generation Firewall* (NGFW), decorre exclusivamente da necessidade de continuidade temporária do ambiente já instalado e em produção, não envolvendo aquisição de novos equipamentos ambiente tecnológico da EBC. A exigência específica desta marca e de seus respectivos modelos justifica-se, de forma excepcional, pela natureza estritamente emergencial e transitória desta contratação (180 dias), cujo escopo é garantir a continuidade ininterrupta dos serviços vigentes.

Da exigência de carta de solidariedade

E2.9. Não se aplica

Da verificação de amostra do objeto

E2.10. Não se aplica

Vistoria

E2.11. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

Sustentabilidade

E2.12. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto e no decorrer deste Projeto Básico, devem ser atendidos os requisitos cabíveis que se baseiam no Guia Nacional de Contratações Sustentáveis da AGU e aplicado, no que couber, o disposto no Decreto nº 7.746/2012, a Política de Sustentabilidade Socioambiental - PO 900/03 e o Plano Diretor de Logística Sustentável da EBC.

E2.12.1. Especificamente em relação ao Plano Diretor de Logística Sustentável - PLS, aprovada pela Deliberação CONSAD nº 02/2026, considerando que a solução é do tipo de prestação de serviço com appliance serão observadas, caso seja compatíveis, a exigência de requisitos do PLS.

E2.13. Serão exigidos da Contratada:

E2.13.1. Declaração de que nem ela nem seus dirigentes foram condenados por infringir as leis de combate à discriminação, em todas as suas formas, por motivos de raça, gênero e outros, conforme dispõe a Constituição Federal de 1988 em seu inciso IV do art. 3º, inciso I do art. 5º, e os arts. 38 e 39 do Estatuto da Igualdade Racial, Lei nº 12.288, de 20 de julho de 2010.

E2.13.2. Declaração de que não pratica, de nenhuma forma, ações que lesionem a Dignidade da Pessoa Humana e a Valorização do Trabalho Humano, protegidas nos arts. 1º e 170 da Constituição Federal, e que possam ser enquadradas nos arts. 149, 203 e 207 do Código Penal.

E2.13.3. Declaração negativa de inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituída por meio da Portaria Interministerial MTPS – MHD nº 04/2016.

E2.13.4. Declaração de que não possui inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituída por meio da Portaria Interministerial MTPS – MHD nº 15 de 26/07/2024.

E2.14. A Contratada deverá se comprometer a não explorar o trabalho infantojuvenil, em atenção ao que dispõe:

- a) o inciso XXXIII do art. 7º da Constituição Federal de 1988;
- b) o Título III, Capítulo IV, do Decreto-Lei nº 5.452, de 1 de maio de 1943 (CLT);
- c) os arts. 60 a 69 da Lei nº 8.069, de 19 de julho de 1990 (ECA);
- d) o Decreto nº 6.841, de 12 de junho de 2008, o qual trata da proibição das piores formas de trabalho infantil e ação imediata para sua eliminação.

Garantia da Contratação

E2.15. Para segurança do integral cumprimento do Contrato, inclusive multa eventualmente aplicada, será exigido da Contratada garantia, a seu critério, em qualquer das modalidades previstas no § 1º, art. 70, da Lei nº 13.303/2016, observando no que couber os dispositivos da Instrução Normativa nº 05/2017 e o Decreto nº 9.507/2018, nas seguintes modalidades:

- a) caução em dinheiro;
- b) seguro-garantia;
- c) fiança bancária.

E2.16. A garantia deverá assegurar, qualquer que seja a modalidade escolhida, o pagamento de:

- a) prejuízos advindos do não cumprimento do contrato;
- b) multas moratórias e punitivas aplicadas pela EBC a Contratada;
- c) prejuízos diretos causados à EBC decorrentes de culpa ou dolo durante a execução do contrato;
- d) obrigações previdenciárias, trabalhistas e de FGTS, de qualquer natureza, não honradas pela Contratada.

E2.17. A garantia deverá ser apresentada no prazo de até 10 (dez) dias úteis a contar da data de assinatura do Contrato, no valor de 5% (cinco por cento) sobre o valor total do Contrato.

E2.18. A garantia ficará sob a responsabilidade e à ordem da Gerência Executiva de Orçamento, Finanças e Contabilidade da EBC.

E2.19. No caso de a Contratada optar pelo seguro-garantia, este deverá dar cobertura aos riscos elencados no E2.16, correspondente a 5% (cinco por cento) do valor total do contrato, na modalidade "Seguro-garantia do Construtor, do Fornecedor e do Prestador de Serviço", com cláusula específica indicando a cobertura adicional de obrigações previdenciárias, trabalhistas e de FGTS não honradas pela Contratada, observado o limite de 02 (dois) meses do custo da folha de pagamento dos empregados que venham a participar da execução dos serviços contratados.

E2.20. A garantia em dinheiro deverá ser efetuada na Caixa Econômica Federal, em conta específica, com correção monetária, em favor da EBC.

E2.21. A garantia na modalidade fiança bancária deverá ser apresentada.

E2.22. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, inclusive indenização a terceiros, a Contratada deverá proceder à respectiva reposição no prazo de 05 (cinco) dias úteis, contados da data em que for notificado pela EBC mediante ofício entregue contrarrecibo.

E2.23. A garantia deverá ter validade de 90 (noventa) dias após a data de término do prazo de vigência a que se referir, nos moldes do art. 70 da Lei nº 13.303/2016.

E2.23.1. A garantia somente será restituída após o término da vigência contratual, ante a comprovação de que a Contratada pagou todas as verbas rescisórias trabalhistas decorrentes da contratação; caso esse pagamento não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas diretamente pela EBC.

E2.24. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 1% (um por cento) do preço total do contrato por dia de atraso, até o máximo de 10% (dez por cento).

E2.25. O atraso superior a 25 (vinte e cinco) dias corridos autoriza a EBC a promover a retenção dos pagamentos devidos a Contratada, até o limite de 5% do valor total do contrato, a serem depositados junto à Caixa Econômica Federal, com correção monetária, em favor da EBC.

E2.25.1. O bloqueio efetuado com base no E2.26 não gera direito a nenhum tipo de compensação financeira a Contratada.

E2.25.2. A Contratada, a qualquer tempo, poderá substituir o bloqueio por quaisquer das modalidades de garantia previstas no E2.15.

E2.25.3. O valor da multa moratória decorrente do atraso da entrega da garantia poderá ser glosado de pagamentos devidos a Contratada.

E2.26. O número do contrato garantido deverá constar dos instrumentos de garantia ou seguro a serem apresentados pelo garantidor e/ou segurador.

E2.27. Quando da abertura de processos para eventual aplicação de penalidade, o Gestor ou Fiscal Técnico do Contrato deverá comunicar o fato à seguradora e/ou fiadora paralelamente às comunicações de solicitação de defesa prévia a Contratada, bem como as decisões finais de primeira e última instância administrativa.

E2.28. O garantidor não é parte interessada para figurar em processo administrativo instaurado pela EBC com o objetivo de apurar prejuízos e/ou aplicar sanções a Contratada.

E2.29. Será considerada extinta a garantia: (a) com a devolução da apólice, carta fiança ou autorização para levantamento de importâncias depositadas em dinheiro, acompanhada de declaração da EBC de que a Contratada cumpriu todas as cláusulas do contrato; (b) após o término da vigência do Contrato, nos termos do E2.24, podendo, independentemente de sua natureza, ser estendida em caso de ocorrência de sinistro.

E2.30. A EBC não executará a garantia na ocorrência de uma ou mais das seguintes hipóteses: (a) caso fortuito ou força maior; (b) alteração, sem prévio conhecimento da seguradora ou do fiador, das obrigações contratuais; (c) descumprimento das obrigações pela Contratada decorrente de atos ou fatos praticados pela EBC; (d) atos ilícitos dolosos praticados por empregados da EBC.

E2.31. Para efeitos da execução da garantia, os inadimplementos contratuais deverão ser comunicados pela EBC a Contratada e/ou à Instituição Garantidora no prazo de até 90 (noventa) dias após o término de vigência do contrato.

E2.32. A Contratada deverá, durante toda a vigência do instrumento contratual, manter atualizada a vigência da garantia contratual.

Condições de execução do objeto

F.1. A execução dos serviços observará as disposições a seguir, sem prejuízo do disposto no **Encarte A** deste Projeto Básico.

F.2. A execução dos serviços emergenciais terá início em 05/10/2026, imediatamente após o encerramento do contrato vigente, sem solução de continuidade, observando-se o prazo máximo aplicável à contratação emergencial. Considerando que a solução já está plenamente implantada e em produção, **não haverá prazo de entrega, instalação, migração ou implantação de licenças/hardwares.**

F.2.1. A Contratada deverá garantir a continuidade ininterrupta do funcionamento dos equipamentos, das licenças, do suporte técnico especializado, da atualização de assinaturas e do monitoramento (SOC) a partir da data de assinatura do instrumento contratual emergencial, mantendo os mesmos padrões de configuração já existentes no ambiente da EBC.

F.2.2. Considerando que o amparo contratual anterior se encerra em 04/10/2026, a empresa Contratada tem a obrigação de garantir a revalidação sistêmica das licenças junto ao fabricante exatamente para o dia **05/10/2026**, assegurando que não ocorra nenhum hiato de cobertura ou interrupção dos serviços de proteção de perímetro na transição contratual.

F.2.3. Caso haja qualquer impedimento técnico, comercial ou administrativo junto ao fabricante que inviabilize a revalidação das licenças para o dia **05/10/2026**, a Contratada deverá **formalizar essa situação à EBC, por escrito, impreterivelmente antes da assinatura do instrumento contratual emergencial**, sob pena de responsabilização administrativa, civil e penal por eventuais indisponibilidades da rede da EBC.

Rotina de execução:

F.3. A rotina para a execução e pagamento dos serviços de continuidade seguirá o rito de faturamento mensal:

Nº	Evento	Prazo
1	Continuidade da operação (licenças revalidadas em 05/10/2026 - suporte e SOC)	Imediatamente e ininterruptamente a partir da assinatura do instrumento contratual.
2	Emissão do Termo de Recebimento Provisório	Em até 5 (cinco) dias corridos após a ativação das novas licenças
3	Emissão do Termo de Recebimento Definitivo ou de Rejeição	Em até 15 (quinze) dias corridos após o Termo de Recebimento Provisório.
4	Emissão da Nota Fiscal/Fatura	Em até 15 (quinze) dias corridos após o Termo de Recebimento Definitivo.
5	Liquidação e Pagamento	Em até 40 (quarenta) dias corridos após o recebimento da Nota Fiscal/Fatura devidamente atestada pelo Fiscal do Contrato.

F.4. O aceite definitivo estará condicionado à comprovação de:

- Conformidade das licenças com as especificações técnicas do **Encarte A** deste Projeto Básico;
- Funcionamento pleno de todas as funcionalidades contratadas da solução;
- Funcionamento do gerenciamento centralizado;
- Inexistência de impacto relevante na operação dos serviços institucionais.

Local de instalação da subscrição das licenças

F.5. A Contratada deverá efetuar a prestação do suporte técnico, monitoramento e atualização sistêmica, de forma remota, abrangendo os equipamentos Forcepoint que já se encontram instalados nas seguintes localidades:

- **Brasília-DF (Sede):** Setor Comercial Sul – SCS, Quadra 08, Blocos B 50/60, 1º subsolo, Asa Sul – Edifício Super Center Venâncio 2000 – CEP:70333-900.
- **Rio de Janeiro-RJ:** Rua da Relação, nº 18 – Centro.
- **São Paulo-SP:** Avenida Mofarrej, nº1.200 – Vila Leopoldina - CEP: 05311-000
- **São Luís-MA:** Rua Armando Vieira da Silva, nº126 – Bairro de Fátima – CEP: 650.030-
- **Tabatinga-AM:** Rua Rui Barbosa - Centro – CEP: 69640-000

F.6. Caso seja necessária alguma intervenção presencial extrema, a Contratada deverá agendar com antecedência, preferencialmente fora do horário comercial, visando minimizar impactos.

Materiais a serem disponibilizados

F.7. Não se aplica a essa contratação.

Especificação da Garantia e Manutenção do Serviço

F.8. A Contratada será responsável pelo suporte técnico especializado e pela manutenção da solução (hardware e software) durante todo o período emergencial e improrrogável de **180 (cento e oitenta) dias**.

F.8.1. A Contratada deverá assegurar assistência técnica, suporte e manutenção (corretiva e preventiva) de todos os componentes físicos, plataforma de gerenciamento e licenças associadas. O atendimento compreende a atualização de firmware, aplicação de patches de segurança, renovação e atualização ininterrupta de assinaturas de ameaças e o serviço contínuo de SOC (Security Operations Center).

F.8.2. O suporte técnico especializado de segundo nível deverá estar disponível 24x7x365 para incidentes de Severidade 1 (Crítica), e em dias úteis no horário comercial para as demais severidades, obedecendo aos SLAs vigentes.

F.9. A Contratada compromete-se a manter equipe técnica qualificada e certificada pelo fabricante para prestação do suporte durante a vigência contratual.

Mecanismos Formais de Comunicação

F.10. Para fins de acionamento do suporte técnico e do SOC, a Contratada deverá manter permanentemente disponíveis os seguintes meios:

- Número telefônico (0800 ou equivalente nacional);
- E-mail corporativo de suporte;
- Portal web (sistema de tickets) para registro de incidentes;
- *(Opcional/Complementar)* Aplicativo de mensagens ou chatbot.

F.11. As comunicações oficiais e aprovações de manutenções entre a EBC e a Contratada devem ser formalizadas por escrito via e-mail corporativo institucional.

Formas de transferência de conhecimento (Capacitação/Treinamento)

F.12. A presente contratação emergencial restringe-se à manutenção operacional e de licenciamento. A equipe interna da EBC já detém o conhecimento prévio necessário para atuar no primeiro nível da solução atual.

Procedimentos de transição e finalização do contrato

F.13. Durante a fase de transição para a solução definitiva, quando demandada pela EBC, a Contratada deverá colaborar com o repasse técnico e disponibilizar, de forma segura, as configurações, inventários e informações necessárias à transição, sem retenção posterior de cópias ou credenciais, garantindo uma transição íntegra para a futura solução

G **MODELO DE GESTÃO DO CONTRATO**

G.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 13.303, de 2016 e RILC/EBC, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

G.2. A EBC poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

G.3. A Contratada deverá assegurar, durante a vigência do contrato, assistência técnica, corretiva, incluindo-se todas as ações, sejam de manutenção, ativação, configuração, e outras necessárias, com vistas a garantir o correto funcionamento da solução, assim como o atendimento às necessidades da EBC, de acordo com os requisitos da contratação e os seguintes Níveis Mínimos de Serviços Exigidos e além do previsto **no Encarte A** deste Projeto Básico.

Preposto

G.4. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

G.5. A EBC poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade.

G.6. Após a assinatura do instrumento contratual e a nomeação do Gestor e Fiscais do Contrato, será realizada Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Projeto Básico e seus Encartes, e esclarecer possíveis dúvidas acerca da execução dos serviços.

Fiscalização

G.7. A fiscalização e gestão do contrato observarão as disposições específicas da NOR 218 - Norma de Gestão de Contratos e Parcerias da EBC.

G.8. Caberá ao Gestor, Fiscais Técnicos e Monitor do Contrato observar as ações dos artigos 10 e 11 do Decreto nº 9.507/2018, para supervisionar a execução dos serviços, verificando se todas as obrigações foram cumpridas.

G.9. Os serviços realizados somente serão pagos após o atesto do Fiscal Técnico na Nota Fiscal/Fatura.

G.10. O descumprimento total ou parcial das responsabilidades assumidas pela Contratada ensejará a aplicação de sanções administrativas, previstas neste instrumento e na legislação vigente, podendo culminar em rescisão contratual.

H **OBRIGAÇÕES DA EBC**

H.1. Além de outras obrigações previstas neste Projeto Básico, a EBC compromete-se a:

H.1.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta.

H.1.2. Exercer o acompanhamento e a fiscalização dos serviços, por servidor ou comissão especialmente designados, anotando em registro próprio as falhas detectadas e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

H.1.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção.

H.1.4. Pagar à Contratada o valor resultante da prestação dos serviços, no prazo e condições estabelecidos neste Projeto Básico.

H.1.5. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da Contratada, no que couber, em conformidade com a legislação aplicável.

H.1.6. Não praticar atos de ingerência na administração da Contratada, tais como: exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados.

H.1.7. Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato.

H.1.8. Proporcionar todas as facilidades para que a Contratada possa desempenhar suas obrigações, permitindo acesso às suas dependências mediante o devido controle.

H.1.9. Assegurar que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto dessa relação contratual pertençam à EBC, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados.

H.1.10. Disponibilizar à Contratada, mediante formalização adequada, as informações atualizadas sobre as políticas de segurança, topologia de rede, configurações e demais dados necessários para a execução da contratação.

I OBRIGAÇÕES DA CONTRATADA

I.1. Além de outras obrigações previstas neste Projeto Básico, a Contratada compromete-se a:

I.1.1. Prestar os serviços nos prazos e condições estabelecidos neste Projeto Básico.

I.1.2. Manter, durante toda a execução do contrato, devidamente atualizadas e em compatibilidade com as obrigações assumidas, todas as condições de regularidade jurídico-fiscal exigidas para a contratação.

I.1.3. Fornecer à EBC, no prazo de 02 (dois) dias úteis do recebimento da Nota de Empenho e/ou assinatura do instrumento de contrato, a lista nominal de seus empregados vinculados à prestação dos serviços.

I.1.4. Caso, pela natureza do serviço, não seja possível a entrega da lista mencionada no subitem anterior ou de alguns de seus itens, a Contratada poderá apresentar declaração informando os motivos que impedem a entrega da documentação solicitada, assumindo responsabilidade exclusiva por todos os encargos trabalhistas e eximindo a EBC de qualquer obrigação.

I.1.5. Responsabilizar-se por quaisquer ônus ou despesas referentes a obrigações trabalhistas, previdenciárias, fiscais e para com FGTS, bem como encargos de possíveis demandas trabalhistas, cível ou penal, relacionados aos serviços, bem como as despesas com transportes, local e interestadual, e a alimentação de seus empregados, decorrentes da execução do objeto contratado.

I.1.6. Ser responsável por obrigações estabelecidas em acordo, convenção, dissídio coletivo de trabalho ou equivalentes das categorias abrangidas na prestação dos serviços.

I.1.6.1. A EBC não se vincula às disposições estabelecidas em acordos, dissídios ou convenções coletivas de trabalho que tratem de:

- Pagamento de participação dos trabalhadores nos lucros ou nos resultados da Contratada;
- Matéria não trabalhista, ou que estabeleçam direitos não previstos em lei, tais como valores ou índices obrigatórios de encargos sociais ou previdenciários;

- Preços para os insumos relacionados ao exercício da atividade.

I.1.7. Indicar preposto para ser o interlocutor entre a Contratada e a EBC, que será o responsável pela fiscalização e acompanhamento da execução dos serviços e que assuma perante o Gestor e o Fiscal Técnico do Contrato designados pela EBC a responsabilidade de deliberar sobre qualquer determinação de urgência que se torne necessária.

I.1.8. Responsabilizar-se pela defesa contra todas as reclamações judiciais ou extrajudiciais e arcar com os ônus decorrentes dos prejuízos que possam ocorrer em consequência da prestação dos serviços por sua culpa ou de seus profissionais, e que venham a ser arguidos por terceiros contra a EBC.

I.1.9. Assumir a responsabilidade por quaisquer danos causados diretamente à EBC ou a terceiros, independentemente da comprovação de culpa ou dolo quando da prestação dos serviços, não excluindo ou reduzindo essa responsabilidade à fiscalização ou ao acompanhamento pela EBC.

I.1.10. Responsabilizar-se por todas as despesas utilizadas na execução dos serviços que incidam direta ou indiretamente sobre os serviços contratados, isentando a EBC de qualquer responsabilidade jurídica ou financeira em quaisquer ocorrências.

I.1.11. Prestar os esclarecimentos que forem solicitados pela EBC, cujas reclamações se obriga a atender prontamente, bem como dar ciência imediata aos Fiscais Técnicos de qualquer anormalidade que verificar quando da execução do Contrato.

I.1.12. Comunicar à EBC, de imediato, qualquer alteração ocorrida no endereço, conta bancária ou outros dados julgados necessários.

I.1.13. Manter sob as penas da Lei o mais completo e absoluto sigilo sobre quaisquer dados, informações, documentos, especificações técnicas e comerciais, topologias, firmwares e demais informações que venha a tomar conhecimento em razão da execução contratual.

I.1.13.1. Assinar o Termo de Sigilo e Privacidade – **Encarte D** deste Projeto Básico, na ocasião da celebração do instrumento contratual ou emissão de Nota de Empenho em seu favor, com vistas a atender a regulamentação relativa à proteção de dados pessoais prevista na Lei nº 13.709/2018 – LGPD.

I.1.14. 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, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação.

I.1.15. Prestar os serviços com as qualidades e especificações descritas neste Projeto Básico, sem imperfeições.

I.1.16. Responsabilizar-se por todos os custos relativos à contratação, inclusive obtendo todas as licenças e autorizações necessárias à prestação dos serviços, arcando com quaisquer despesas e responsabilizando-se pelo cumprimento de eventuais exigências formuladas pelos órgãos competentes.

I.1.17. Facilitar os trabalhos da fiscalização, acatando imediatamente as instruções, sugestões, observações e decisões que emanem da fiscalização, corrigindo as falhas e superando as dificuldades apontadas quanto ao cumprimento das cláusulas contratuais.

I.1.18. Refazer, às suas custas, os serviços reprovados pela Fiscalização da EBC, quer seja pela baixa qualidade, quanto pela imperícia, imprudência e/ou incompetência de seus empregados, arcando com o custo de todos os materiais necessários.

I.1.19. Atender às normas de segurança e demais regulamentos em vigor nas dependências da EBC.

I.1.20. Acatar todas as orientações dos Fiscais Técnicos, sujeitando-se à mais ampla e irrestrita fiscalização, prestando de imediato e com solicitude os esclarecimentos solicitados e atendendo às reclamações formuladas.

I.1.21. Garantir a disponibilização de firmwares, licenças e atualizações de segurança durante toda a vigência contratual.

I.1.22. Acompanhar a execução das políticas de segurança existentes, assegurando a continuidade dos serviços institucionais durante todo o período da contratação.

I.1.23. Cumprir rigorosamente os Acordos de Nível de Serviço (SLA) definidos no **Encarte A** deste Projeto Básico, sob pena de aplicação das glosas e sanções previstas.

I.1.24. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos gerados em decorrência dessa relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à EBC.

I.1.25. A Contratada garante à EBC o uso, o gozo e a disposição dos produtos fornecidos, respondendo, ainda, pelos vícios e defeitos que porventura apresentarem durante o período de garantia.

I.1.26. A Contratada arcará com todas as perdas e danos, incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais que a EBC for compelida a responder, caso os produtos fornecidos em decorrência deste contrato violem direitos de terceiros.

J

CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

J.1. A mensuração dos resultados ocorrerá por intermédio da análise dos níveis de serviços estabelecidos no **Encarte A** deste Projeto Básico, sendo rejeitado e solicitados os ajustes devidos para posterior atesto na Nota Fiscal/Fatura.

J.1.1. Para o serviço de suporte técnico mensal, serão aplicados os seguintes indicadores previstos no **Encarte A** deste Projeto Básico.

J.1.2. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis.

Recebimento do objeto

J.2. Os serviços serão recebidos nos termos do RILC/EBC e normativo interno próprio (NOR 218), bem como das disposições previstas no Tópico F deste Projeto Básico.

J.3. Para efeito de recebimento provisório, ao final de cada período de faturamento, o Fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos no **Encarte A** deste Projeto Básico, que poderá resultar no redimensionamento de valores a serem pagos à Contratada, registrando em relatório a ser encaminhado ao gestor documental do contrato.

J.3.1. A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no recebimento.

J.4. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Projeto Básico e na proposta, sem prejuízo da aplicação de penalidades.

J.5. Ocorrerá o recebimento definitivo pela observância da NOR 218 e após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

J.5.1. Emitir documento comprobatório da avaliação realizada pelos Fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pela Contratada, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

J.5.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções.

J.5.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas.

J.5.4. Comunicar à Contratada para que emita a Nota Fiscal/Fatura, com o valor exato dimensionado pela fiscalização.

J.5.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

J.6. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela Contratada, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

J.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Liquidação

J.8. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de até 30 (trinta) dias corridos para fins de liquidação, na forma desta seção, prorrogáveis por igual período.

J.8.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do artigo 13 do RILC/EBC.

J.9. Para execução do pagamento, a Contratada deverá fazer constar da Nota Fiscal/Fatura correspondente, emitida sem rasura, em nome da Empresa Brasil de Comunicação S/A – EBC, com CNPJ do local onde ocorreu a prestação dos serviços, o número de sua conta bancária, o nome do Banco e a respectiva Agência.

J.10. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal/Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

J.10.1. o prazo de vencimento;

J.10.2. a data da emissão;

J.10.3. os dados do contrato e do órgão contratante;

J.10.4. o período respectivo de execução do contrato;

J.10.5. o valor a pagar; e

J.10.6. eventual destaque do valor de retenções tributárias cabíveis.

J.11. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que a Contratada providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à EBC.

J.12. A Nota Fiscal/Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais.

J.13. Constatando-se, junto ao SICAF, a situação de irregularidade da Contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da EBC.

J.14. Não havendo regularização ou sendo a defesa considerada improcedente, a EBC deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da Contratada, 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.

J.15. Persistindo a irregularidade, a EBC deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

J.16. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a Contratada não regularize sua situação junto ao SICAF.

Pagamento

J.17. O pagamento será efetuado por meio de Ordem Bancária até o 10º (décimo) dia útil a contar da finalização da liquidação da despesa.

J.18. Caso a Contratada seja optante do Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, deverá apresentar, com a Nota Fiscal/Fatura, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor, se aplicável.

J.19. Nos preços deverão estar incluídos todos os ônus tributários, fiscais, parafiscais, trabalhistas e sociais e demais despesas de qualquer natureza que incidam direta ou indiretamente sobre o objeto contratado.

J.20. O número de inscrição no CNPJ indicado nos faturamentos da Contratada deverá ser o mesmo indicado em sua proposta. Quando se tratar de matriz e filial, comprovando as centralizações de recolhimentos tributários, poderá ser aceito o faturamento em CNPJ da matriz.

J.20.1. Se a Contratada for a matriz, todos os documentos deverão estar em nome da matriz, e se for a filial,

todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, sejam emitidos somente em nome da matriz.

J.20.2. Serão aceitos registros de CNPJ de Contratada matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

J.21. Os pagamentos a serem efetuados em favor da Contratada estarão sujeitos, no que couber, às retenções na fonte nos seguintes termos:

J.21.1. do Imposto de Renda da Pessoa Jurídica – IRPJ, da Contribuição Social sobre o Lucro Líquido – CSLL, da contribuição para seguridade social – COFINS e da contribuição para o PIS/PASEP, na forma da Instrução Normativa RFB nº 1.234, de 11 de janeiro de 2012, conforme determina o art. 64 da Lei nº 9.430, de 27/12/1996 e alterações;

J.21.2. da contribuição previdenciária ao Instituto Nacional do Seguro Social – INSS, conforme determina a Lei nº 8.212, de 24/07/1991, e alterações, bem como Instruções Normativas que regem a matéria;

J.21.3. do Imposto Sobre Serviços de Qualquer Natureza – ISSQN, na forma da Lei Complementar nº 116, de 31/07/2003, c/c a legislação Distrital ou municipal em vigor.

K

REAJUSTAMENTO DE PREÇOS

K.1. Considerando que se trata de contratação por prazo determinado e inferior a 1 (um) ano, não será admitido o reajuste dos preços dos serviços contratados.

L

FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

L.1. Considerando que se trata de contratação direta com fundamento no art. 13, inc. XIV do RILC, não se aplica critério de julgamento.

Regime de execução

L.2. O regime de execução será de contratação por preço global.

Da Aplicação da Margem de Preferência

L.3. Não será aplicada margem de preferência na presente contratação, observado o disposto na legislação vigente.

Exigências de Habilitação

Habilitação jurídica

L.4. A Contratada deverá apresentar os documentos de habilitação jurídica exigidos pela legislação vigente, aptos a comprovar sua capacidade para adquirir direitos e assumir obrigações, bem como sua regular constituição e representação legal.

Regularidade fiscal, social e trabalhista

L.5. A Contratada deverá apresentar Certidão de regularidade fiscal quanto aos débitos inscritos ou não em Dívida Ativa da União, inclusive em relação às contribuições previdenciárias e ao Fundo de Garantia por Tempo de Serviço (FGTS);

L.6. A Contratada deverá apresentar também Certidões Negativas:

- Condenação Cíveis por Ato de Improbidade Administrativa e Inelegibilidade;
- Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS);
- Débitos Trabalhistas - CNDT;
- Cadastro Informativo de Créditos não Quitados do Setor Público Federal (Cadin).

L.7. A Contratada deverá apresentar, ainda, Declaração de que não se enquadra nas hipóteses de impedimento do art. 26 do Regulamento Interno de Licitações e Contratos da EBC, conforme **Encarte C** deste Projeto Básico.

L.8. Caso o prestador de serviços seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da Lei.

Qualificação Econômico-Financeira

L.9. A Contratada deverá apresentar Certidão negativa de insolvência civil expedida pelo distribuidor do seu domicílio ou sede, caso se trate de pessoa física, desde que admitida a sua participação na licitação, ou de sociedade simples;

L.10. A Contratada deverá apresentar Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

Qualificação Técnica

L.11. Não será exigida comprovação da qualificação técnica, considerando que a solução já está implantada e que tal comprovação ocorreu anteriormente no âmbito do Pregão Eletrônico nº 015/2021 (SEI nº 00000.001173/2020-00).

M.1. A aplicação de penalidades à Contratada reger-se-á conforme o estabelecido no Capítulo V, Seção I, do RILC, bem como no Título II, Capítulo II, Seção III – Das Sanções Administrativas, da Lei nº 13.303/2016.

M.2. A Contratada que deixar de cumprir as obrigações dispostas neste Projeto Básico ficará sujeita, nos termos do art. 83 da Lei nº 13.303/2016, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

- Advertência;
- Multa, na forma disciplinada neste Tópico;
- Suspensão temporária de participação em licitação e impedimento de contratação com a EBC pelo período de até 02 (dois) anos.

M.3. Em caso de descumprimento do prazo estabelecido para execução dos serviços na forma estabelecida no **item F.2.1.**, sem que haja justificativa aceita pelo Fiscal Técnico da contratação, a Contratada ficará sujeita à multa moratória equivalente a 2% (dois por cento) do valor total da contratação, por dia corrido de atraso, até o limite de 10% (dez por cento) do valor total global da contratação.

M.4. Em caso de interrupção ou suspensão, salvo motivo de força maior ou caso fortuito, dos serviços solicitados, por até 15 (quinze) dias, sem comunicação formal ao Fiscal do Contrato, a Contratada estará sujeita à aplicação de multa compensatória de até 10% (dez por cento) do valor total global da contratação.

M.4.1. Em caso de interrupção ou suspensão, salvo motivo de força maior ou caso fortuito, dos serviços solicitados, por mais de 15 (quinze) dias, sem comunicação formal ao Fiscal do Contrato, a Contratada restará configurada inexecução total do Contrato, o que poderá acarretar a rescisão contratual.

M.5. Caso a Contratada provoque a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas, etc), estará sujeita à aplicação de multa compensatória de até 15% (quinze por cento) do valor total global da contratação, sem prejuízo da suspensão temporária e impedimento de contratar com a EBC, bem como às demais penalidades previstas neste tópico, o que poderá acarretar a rescisão contratual.

M.6. Caso a Contratada permita o funcionamento dos sistemas de modo adverso ao especificado nos requisitos da solução e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços, estará sujeita à aplicação de multa compensatória de até 10% (dez por cento) do valor total global da contratação, sem prejuízo da suspensão temporária e impedimento de contratar com a EBC, bem como das demais penalidades previstas neste tópico, o que poderá acarretar a rescisão contratual.

M.7. Caso a Contratada comprometa o sigilo das informações armazenadas nos sistemas da EBC, estará sujeita à aplicação de multa compensatória de até 20% (vinte por cento) do valor total global da contratação, sem prejuízo da suspensão temporária e impedimento de contratar com a EBC, bem como das demais penalidades previstas neste tópico, o que poderá acarretar a rescisão contratual.

M.8. Caso a Contratada comprometa a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas da EBC, estará sujeita à aplicação de multa compensatória de até 20% (vinte por cento) do valor total global da contratação, sem prejuízo da suspensão temporária e impedimento de contratar com a EBC, bem como das demais penalidades previstas neste tópico, o que poderá acarretar a rescisão contratual.

M.9. No caso de outras ações que impliquem em inexecução parcial do objeto, a Contratada estará sujeita à aplicação de multa compensatória de até 15% (quinze por cento) do valor total global da contratação.

M.10 No caso de inexecução total do objeto, a Contratada estará sujeita à aplicação de multa compensatória de até 20% (vinte por cento) do valor total global da contratação.

M.11 A critério da EBC, a aplicação das penalidades não ensejará, obrigatoriamente, a rescisão do Contrato, servindo como punição pecuniária contra a reincidência no descumprimento das obrigações.

M.12. As penalidades descritas neste tópico podem ser aplicadas isoladas ou cumulativamente, a critério da EBC, após análise das circunstâncias que ensejarem sua aplicação, e serão obrigatoriamente registradas no SICAF.

M.13. As importâncias decorrentes das multas não recolhidas nos prazos determinados poderão ser descontadas dos pagamentos eventualmente devidos à Contratada ou, quando for o caso, cobradas judicialmente.

M.14. Nenhuma penalidade será aplicada sem o devido processo administrativo, sendo facultada a apresentação de defesa prévia pela Contratada, no prazo de até **10 (dez) dias úteis**, a contar da data em que for comunicada pela EBC.

N	ORÇAMENTO ESTIMADO
---	--------------------

N.1. O valor total estimado da contratação é de **R\$ 198.178,08** (cento e noventa e oito mil cento e setenta e oito reais e oito centavos), para o período de **180 (cento e oitenta) dias**, conforme tabela descritiva a seguir:

Item	Descrição	Valor Mensal	Valor Total (180 dias)
01	Serviço de Solução de Firewall da EBC (solução em cluster em: Brasília - DF, Rio de Janeiro - RJ, São Paulo SP, São Luis - MA e Tabatinga AM	R\$ 27.584,95	R\$ 165.509,70
02	Serviço de SOC (Security Operations Center - Centro de Operação de Segurança). Serviço especializado na solução de Firewall	R\$ 5.444,73	R\$ 32.668,38
Valor total global			R\$ 198.178,08

N.2. No valor estimado total da contratação estão inseridos todos os custos diretos e indiretos que incidem sobre a prestação dos serviços de licenciamento, suporte técnico, manutenção e serviço de SOC referentes à solução.

N.3. Em conformidade com o disposto no art. 7º do Decreto nº 9.507/2018, são vedadas nesta contratação: a indexação de preços por índices gerais, a caracterização do objeto como fornecimento de mão de obra, a previsão de reembolso de salários pela EBC e a pessoalidade e a subordinação direta dos empregados da Contratada aos gestores da EBC.

O	CONSIDERAÇÕES GERAIS
---	----------------------

- O.1.** A EBC poderá, nas mesmas condições contratuais e por acordo com a Contratada, proceder a acréscimos ou supressões, até o limite de 25% (vinte e cinco por cento) do preço inicial atualizado, de acordo com a necessidade da EBC, conforme disposto no art. 95 do RILC da EBC.
- O.2.** É vedada a contratação de empregado pertencente ao quadro de pessoal da EBC.
- O.3.** É vedada a veiculação de publicidade acerca da contratação, salvo se houver prévia e expressa autorização da EBC.
- O.4.** Fica vedada a utilização, durante a execução dos serviços, de empregado da Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança da EBC, nos termos do artigo 7º do Decreto nº 7.203/2010.
- O.5.** Para fins de atendimento às disposições previstas na Lei nº 13.709/2018 – LGPD, a Contratada assinará o Termo de Sigilo e Privacidade – **Encarte D** deste Projeto Básico, na ocasião da celebração do instrumento de contratação.
- O.6.** Todos os custos necessários ao perfeito fornecimento da solução deverão estar contemplados na proposta comercial, não sendo admitidos acréscimos posteriores decorrentes de omissões da Contratada.
- O.7.** Toda a solução fornecida deverá permanecer plenamente licenciada, suportada e atualizada durante toda a vigência contratual.
- O.8.** A Contratada responderá integralmente pelos danos causados à EBC ou a terceiros em decorrência de ação ou omissão de seus empregados, representantes ou prepostos.
- O.9.** Quaisquer alterações técnicas necessárias durante a execução contratual deverão ser previamente submetidas à aprovação da fiscalização da EBC.
- O.10.** A solução deverá manter compatibilidade com as evoluções tecnológicas disponibilizadas pelo fabricante durante toda a vigência do contrato, sempre que abrangidas pelo licenciamento contratado.
- O.11.** Os direitos de uso das licenças deverão permanecer válidos durante todo o período contratado, incluindo acesso às funcionalidades originalmente ofertadas e às atualizações disponibilizadas pelo fabricante sem custos adicionais.
- O.12.** Constitui obrigação permanente da Contratada atuar em conformidade com as melhores práticas de mercado em Segurança da Informação, Cibersegurança, Governança de TIC e Gestão de Incidentes, preservando a disponibilidade, integridade, confidencialidade e rastreabilidade das informações tratadas no âmbito da presente contratação.
- O.13.** As dúvidas pertinentes a este Projeto Básico poderão ser sanadas com o Sr. Rodrigo Barreto ou Danilo Costa, por meio dos telefones (61) 3799-5267 e (61) 3799-5821, ou nos e-mails: rodrigo.barreto@ebc.com.br e danilo.costa@ebc.com.br.

DADOS DOS RESPONSÁVEIS PELA ELABORAÇÃO DO PROJETO BÁSICO:

INTEGRANTE REQUISITANTE		INTEGRANTE TÉCNICO	
DANILO LIMA COSTA Coordenador de Suporte de Infraestrutura II - DF/MA		ANTÔNIO VALTER MARTINS coordenador de Atendimento - DF/MA	
INTEGRANTE ADMINISTRATIVO			
CÍNTIA DE MORAES Coordenadora de Análise e Conformidade Processual			

De acordo: HAILTON LOPES DA SILVA Gerente Executivo de Tecnologia da Informação
Responsável pela aprovação: BRÁULIO COSTA RIBEIRO Diretor de Operações, Engenharia e Tecnologia

RELAÇÃO DOS ENCARTES QUE ACOMPANHAM O PRESENTE PROJETO BÁSICO:

ENCARTE A	Descrição Detalhada do Objeto, Especificações Técnicas e Acordo de Nível de Serviço (SLA)
ENCARTE B	Modelo de Proposta de Preços
ENCARTE C	Declaração para Participação e Contratação – Impedimentos do RILC da EBC
ENCARTE D	Termo de Sigilo e Privacidade
ENCARTE E	Termo de Ciência e Declaração de Manutenção de Sigilo
ENCARTE F	Modelo de Termo de Garantia do Objeto
ENCARTE G	Modelo de Carta de Fiança Bancária para Garantia de Execução Contratual

ENCARTE A

Descrição Detalhada do Objeto, Especificações Técnicas e SLA

DO OBJETO

- 1.1. O objeto desta contratação consiste na **continuidade** da prestação de Serviço de Solução de Segurança da Informação do tipo Next Generation Firewall (NGFW), que contempla a manutenção da Solução de Firewall existente e do **Serviço de SOC (Security Operations Center - Centro de Operação de Segurança)** por um período de 180 (cento e oitenta) dias, garantidas as atualizações de versões, *patches* de segurança e *updates* de assinaturas contra ameaças por todo o período contratado.
- 1.2. A Solução de Segurança da Informação do tipo Next Generation Firewall (NGFW) tem por objetivo a proteção de informação perimetral e de rede interna que inclui firewall, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares “Zero Day e APTs”, Filtro de URL, compondo uma plataforma de segurança integrada e robusta;
- 1.3. O Serviço de SOC (Security Operations Center - Centro de Operação de Segurança) deverá contemplar as unidades da EBC em Brasília/DF, Rio de Janeiro/RJ, São Paulo/SP, São Luís/MA e Tabatinga/AM, seguindo as especificações deste Encarte.
- 1.4. O serviço será contratado por 180 (cento e oitenta) dias, com execução de pagamento mensal, conforme rotina de execução estipulado **no item F.3;**

2. SOLUÇÃO DE FIREWALL

2.1. Solução de Segurança da Informação do tipo Next Generation Firewall e Serviço de SOC (Security Operations Center - Centro de Operação de Segurança) para gerência e monitoramento da Solução, por 180 (cento e oitenta) dias

2.1.1. A Solução deverá seguir todos os requisitos estipulados neste **Encarte A**, além de possuir garantia de hardware e software por 180 (cento e oitenta) dias.

3. SOLUÇÃO DE PROTEÇÃO E SEGURANÇA DE REDES DA EBC

3.1. A Solução de proteção e segurança de Firewall da EBC deverá contemplar TODAS as funcionalidades de NGFW disponíveis pelo fabricante, respeitando a disponibilidade do serviço, por modelos de cada praça (DF, RJ, SP, MA e AM)

3.2. O licenciamento deverá contemplar o direito de manter o software em sua versão mais atualizada e estável, além de executar as atualizações de todos os patches de correção (melhoria ou vulnerabilidade), caso existam.

3.3. Todos os profissionais da CONTRATADA deverão respeitar o sigilo das informações fornecidas pela EBC e deverão assinar o termo de confidencialidade (Pessoa Física e Jurídica) das informações, conforme termo apresentando no **Encarte E**.

4. REQUISITOS DA SOLUÇÃO DE FIREWALL

Os requisitos técnicos serão separados por TIPO (Tipo 1, 2 e 3), conforme necessidade de performance, separadas por localidade da EBC.

4.1. DAS ESPECIFICAÇÕES TÉCNICAS - TIPO 1 (Praças DF), totalizando 2 (dois) appliances.

4.1.1. Deverá possuir, throughput igual ou superior a 13 Gbps com a funcionalidade de firewall, controle de aplicação e IPS habilitados.

4.1.2. Deverá possuir, throughput igual ou superior a 5 Gbps para as funcionalidades de Threat Protection habilitadas simultaneamente (Firewall + IPS + Aplicação Control + Antivirus e Antispyware). Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades separadas ou em conjunto, somente o de menor valor será aceito;

4.1.3. Os throughputs deverão ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de solicitar a contratada a aferição da performance dos equipamentos em bancada.

4.1.4. O Throughput é a quantidade de tráfego de saída que um único equipamento é capaz de encaminhar, não havendo soma entre os membros do cluster;

4.1.5. Deverá suportar, uma taxa igual ou superior a 8.000.000 conexões simultâneas;

4.1.6. Deverá suportar, uma taxa igual ou superior a 150.000 novas conexões por segundo;

4.1.7. Deverá possuir fonte 120/240 AC ou DC, redundante;

4.1.8. Deverá possuir Disco Solid State Drive (SSD) ou nvme ou Cfast;

4.1.9. Deverá possuir, no mínimo, 04 (quatro) interfaces de rede 10/100/1000 base-TX;

4.1.10. Deverá possuir, no mínimo, 04 (quatro) interfaces de rede 10 Gbps SFP+;

4.1.11. Deverá possuir 1 (uma) interface de rede 1 Gbps para gerenciamento;

4.1.12. Deverá possuir 1 (uma) interface do tipo console ou similar;

4.1.13. Deverá possuir suporte a, no mínimo, 30 (trinta) zonas de segurança;

4.1.14. Deverá estar licenciada para suportar, 1500 (Mil e quinhentos) clientes de VPN SSL simultâneos;

- 4.1.15. Deverá estar licenciada para suportar, 200 (duzentos) túneis de VPN IPSEC simultâneos;
- 4.1.16. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- 4.1.17. A plataforma da Solução deve ser otimizada para análise de conteúdo de aplicações em camada7;
- 4.1.18. O hardware e software que executem as funcionalidades de proteção de rede, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- 4.1.19. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
- 4.1.20. O software deverá ser fornecido em sua versão mais atualizada;
- 4.1.21. Deverá possuir a funcionalidade para criação de 1024 VLAN Tags 802.1q;
- 4.1.22. Deverá possuir a funcionalidade para criação de agregação de links 802.3ad e LACP;
- 4.1.23. A solução deve suportar Jumbo frames;
- 4.1.24. Deverá possuir a funcionalidade para criação de policy based routing ou policy based forwarding;
- 4.1.25. Deverá possuir a funcionalidade para criação de roteamento multicast (PIM-SM);
- 4.1.26. Deverá possuir a funcionalidade para criação de DHCP Relay e DHCP Server;
- 4.1.27. Deverá suportar a criação de objetos de rede que possam ser reutilizados;
- 4.1.28. Deverá suportar sub-interfaces ethernet lógicas;
- 4.1.29. Deverá suportar, no mínimo, 4 (quatro) roteadores virtuais na mesma instância de firewall ou através de instâncias distintas;
- 4.1.30. O appliance de firewall deve ter a capacidade de testar o funcionamento de rotas default com a definição de um endereço IP de destino, que deve estar comunicável através de uma rota. Caso haja falha na comunicação, o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;
- 4.1.31. Deverá suportar Nat dinâmico (Many-to-1), Nat dinâmico (Many-to-Many), Nat estático (1-to-1), NAT estático (Many-to-Many), Tradução de porta (PAT), NAT de Origem, NAT de Destino, Suportar NAT de Origem e NAT de Destino simultaneamente;
- 4.1.32. Deverá implementar balanceamento de link do IP de origem;
- 4.1.33. Deverá implementar balanceamento de link do IP de origem e destino;
- 4.1.34. Deverá implementar balanceamento de link através do método round-robin ou número de sessões ou volume de dados;
- 4.1.35. Deverá implementar balanceamento de link por peso. Nesta opção deverá ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deverá suportar o balanceamento de, no mínimo, dois links;
- 4.1.36. Deverá implementar balanceamento de link através de políticas por usuário e grupos de usuários do AD;
- 4.1.37. Deverá implementar balanceamento de link através de políticas por aplicação e porta de destino;
- 4.1.38. Deverá enviar log para sistemas de monitoração externos, simultaneamente;

- 4.1.39. Deverá haver a opção de enviar logs para os sistemas de monitoração externos via protocolo seguro TLS ou SSL;
- 4.1.40. Deverá possuir proteção contra anti-spoofing;
- 4.1.41. Deverá permitir bloquear sessões TCP que usem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma, possíveis tráfegos maliciosos;
- 4.1.42. Deverá exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de tráfego;
- 4.1.43. Para IPv4, deverá suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 4.1.44. Para IPv6, deverá suportar roteamento estático.
- 4.1.45. Deverá suportar, as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), Identificação de usuários a partir do AD, Captive Portal, IPv6 over IPv4 IPsec, Regras de proteção contra DoS (Denial of Service), PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPsec, VPN SSL, Ativo/Passivo, SNMP, NTP, DNS, e controle de aplicação;
- 4.1.46. Deverá possuir modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 4.1.47. Deverá possuir modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 4.1.48. Deverá possuir modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 4.1.49. Deverá possuir modo misto de trabalho Sniffer e L3 em diferentes interfaces físicas;
- 4.1.50. Deverá suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Modo transparente e em layer 3;
- 4.1.51. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede, certificados de-criptografados.
- 4.1.52. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
- 4.1.53. As funcionalidades de firewall, VPN IPsec e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.
- 4.1.54. Deverá suportar controles por zona de segurança.
- 4.1.55. Deverá possuir controles de políticas por porta e protocolo.
- 4.1.56. Deverá ter o controle de políticas por aplicações, como por exemplo categoria de aplicações, risco e características.
- 4.1.57. Deverá possuir controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 4.1.58. Deverá suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;
- 4.1.59. Deverá controlar políticas por código de País (Por exemplo: BR, USA, UK, RUS);
- 4.1.60. Deverá controlar, inspecionar e de-criptografar SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

- 4.1.61. Deverá de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
- 4.1.62. Deverá de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
- 4.1.63. Deverá bloquear os seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg
- 4.1.64. Deverá possuir Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
- 4.1.65. Deverá possuir QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
- 4.1.66. Suportar objetos e regras IPV6.
- 4.1.67. Suportar roteamento multicast.
- 4.1.68. Deverá suportar, no mínimo, três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
- 4.1.69. Suportar a atribuição de agendamento as políticas, com o objetivo de habilitar e desabilitar políticas em horários pré-definidos, de forma automática.

4.2. DAS ESPECIFICAÇÕES TÉCNICAS - TIPO 2 (Praças RJ e SP), totalizando 4 (quatro) appliances. (Sendo 2 (dois) para a praça RJ e 2 (dois) para a praça SP)

- 4.2.1. Deverá possuir throughput igual ou superior a 3,5 Gbps com a funcionalidade de firewall controle de aplicação e IPS habilitados;
- 4.2.2. Deverá possuir throughput igual ou superior a 1,8 Gbps para as funcionalidades de Threat Protection habilitadas simultaneamente (Firewall + IPS + Aplicação Control + Antivirus e Antispyware). Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades separadas ou em conjunto, somente o de menor valor será aceito;
- 4.2.3. Os throughputs deverão ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de solicitar a contratada a aferição da performance dos equipamentos em bancada.
- 4.2.4. O Throughput é a quantidade de tráfego de saída que um único equipamento é capaz de encaminhar, não havendo soma entre os membros do cluster;
- 4.2.5. Deverá suportar, uma taxa igual ou superior a, 8.000.000 conexões simultâneas;
- 4.2.6. Deverá suportar, uma taxa igual ou superior a, 65.000 novas conexões por segundo;
- 4.2.7. Deverá possuir fonte 120/240 AC ou DC;
- 4.2.8. Deverá possuir Disco Solid State Drive (SSD) ou nvme ou Cfast;
- 4.2.9. Deverá possuir, no mínimo, 04 (quatro) interfaces de rede 10/100/1000 base-TX;
- 4.2.10. Deverá possuir, no mínimo, 04 (quatro) interfaces de rede 10 Gbps SFP+;
- 4.2.11. Deverá possuir 1 (uma) interface de rede 1 Gbps para gerenciamento;
- 4.2.12. Deverá possuir 1 (uma) interface do tipo console ou similar;
- 4.2.13. Deverá possuir suporte a, no mínimo, 20 (vinte) zonas de segurança;
- 4.2.14. Deverá estar licenciada para suportar, 200 (duzentos) clientes de VPN SSL simultâneos;
- 4.2.15. Deverá estar licenciada para suportar, 200 (duzentos) túneis de VPN IPSEC simultâneos;

- 4.2.16. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- 4.2.17. A plataforma da Solução deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 4.2.18. O hardware e software que executem as funcionalidades de proteção de rede, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- 4.2.19. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
- 4.2.20. O software deverá ser fornecido em sua versão mais atualizada;
- 4.2.21. Deverá possuir a funcionalidade para criação de 1024 VLAN Tags 802.1q;
- 4.2.22. Deverá possuir a funcionalidade para criação de agregação de links 802.3ad e LACP;
- 4.2.23. A solução deve suportar Jumbo frames;
- 4.2.24. Deverá possuir a funcionalidade para criação de policy based routing ou policy based forwarding;
- 4.2.25. Deverá possuir a funcionalidade para criação de roteamento multicast (PIM-SM);
- 4.2.26. Deverá possuir a funcionalidade para criação de DHCP Relay e DHCP Server;
- 4.2.27. Deverá suportar a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
- 4.2.28. Deverá suportar sub-interfaces ethernet lógicas;
- 4.2.29. O appliance de firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino, que deve estar comunicável através de uma rota. Caso haja falha na comunicação, o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;
- 4.2.30. Deverá suportar Nat dinâmico (Many-to-1), Nat dinâmico (Many-to-Many), Nat estático (1-to-1), NAT estático (Many-to-Many), Tradução de porta (PAT), NAT de Origem, NAT de Destino, Suportar NAT de Origem e NAT de Destino simultaneamente;
- 4.2.31. Deverá implementar Network Prefix Translation (NPTv6), ou outro mecanismo prevenindo problemas de roteamento assimétrico;
- 4.2.32. Deverá implementar balanceamento de link por IP de origem;
- 4.2.33. Deverá implementar balanceamento de link por IP de origem e destino;
- 4.2.34. Deverá implementar balanceamento de link através do método round-robin ou número de sessões ou volume de dados.;
- 4.2.35. Deverá implementar balanceamento de link por peso. Nesta opção deverá ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deverá suportar o balanceamento de, no mínimo, dois links;
- 4.2.36. Deverá implementar balanceamento de link através de políticas por usuário e grupos de usuários do AD;
- 4.2.37. Deverá implementar balanceamento de link através de políticas por aplicação e porta de destino;
- 4.2.38. Deverá enviar log para sistemas de monitoração externos, simultaneamente;

- 4.2.39. Deverá haver a opção de enviar logs para os sistemas de monitoração externos via protocolo seguro TLS ou SSL;
- 4.2.40. Deverá possuir proteção contra anti-spoofing;
- 4.2.41. Deverá permitir bloquear sessões TCP que usem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma, possíveis tráfegos maliciosos;
- 4.2.42. Deverá exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de tráfego;
- 4.2.43. Para IPv4, deverá suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 4.2.44. Para IPv6, deverá suportar roteamento estático;
- 4.2.45. Deverá suportar as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), Identificação de usuários a partir do AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEC, VPN SSL, Ativo/Passivo, SNMP, NTP, DNS e controle de aplicação;
- 4.2.46. Deverá possuir modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 4.2.47. Deverá possuir modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 4.2.48. Deverá possuir modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 4.2.49. Deverá possuir modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 4.2.50. Deverá suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Modo transparente e em layer 3
- 4.2.51. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede, certificados de-criptografados, associações de Segurança das VPNs e Tabelas FIB;
- 4.2.52. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
- 4.2.53. As funcionalidades de firewall, VPN IPSec e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.
- 4.2.54. Deverá suportar controles por zona de segurança.
- 4.2.55. Deverá possuir controles de políticas por porta e protocolo.
- 4.2.56. Deverá ter o controle de políticas por aplicações, como por exemplo categoria de aplicações, risco e características.
- 4.2.57. Deverá possuir controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 4.2.58. Deverá suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;
- 4.2.59. Deverá controlar políticas por código de País (Por exemplo: BR, USA, UK, RUS);
- 4.2.60. Deverá controlar, inspecionar e de-criptografar SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

- 4.2.61. Deverá de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
- 4.2.62. Deverá de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
- 4.2.63. Deverá bloquear os seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg
- 4.2.64. Deverá possuir Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
- 4.2.65. Deverá possuir QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
- 4.2.66. Suportar objetos e regras IPV6.
- 4.2.67. Suportar roteamento multicast.
- 4.2.68. Deverá suportar, no mínimo, três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
- 4.2.69. Suportar a atribuição de agendamento as políticas, com o objetivo de habilitar e desabilitar políticas em horários pré-definidos, de forma automática.

4.3. DAS ESPECIFICAÇÕES TÉCNICAS - TIPO 3 (Praças MA e AM), totalizando 4 (quatro) appliances. (Sendo 2 (dois) para a praça MA e 2 (dois) para a praça AM)

- 4.3.1. Deverá possuir, throughput igual ou superior a 1.5 Gbps com a funcionalidade de controle de aplicação;
- 4.3.2. Deverá possuir throughput igual ou superior a 780 Mbps para as funcionalidades de Threat Protection habilitadas simultaneamente (Firewall + IPS + Application Control + Antivirus e Antispyware). Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades separadas ou em conjunto, somente o de menor valor será aceito;
- 4.3.3. Os throughputs deverão ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de solicitar a aferição da performance dos equipamentos em bancada.
- 4.3.4. O Throughput é a quantidade de tráfego de saída que um único equipamento é capaz de encaminhar, não havendo soma entre os membros do cluster;
- 4.3.5. Deverá suportar uma taxa igual ou superior a 2.000.000 conexões simultâneas;
- 4.3.6. Deverá suportar, uma taxa igual ou superior a, 30.000 novas conexões por segundo;
- 4.3.7. Deverá possuir fonte 120/240 AC ou DC
- 4.3.8. Deverá possuir Disco Solid State Drive (SSD) ou nvme ou Cfast;
- 4.3.9. Deverá possuir, no mínimo, 06 (seis) interfaces de rede 10/100/1000 base-TX;
- 4.3.10. Deverá possuir 1 (uma) interface de rede 1 Gbps para gerenciamento;
- 4.3.11. Deverá possuir 1 (uma) interface do tipo console ou similar;
- 4.3.12. Deverá possuir suporte a, no mínimo, 10 (trinta) zonas de segurança;
- 4.3.13. Deverá estar licenciada para suportar, 200 (duzentos) clientes de VPN SSL simultâneos;

- 4.3.14. Deverá estar licenciada para suportar, 200 (duzentos) túneis de VPN IPSEC simultâneos;
- 4.3.15. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- 4.3.16. A plataforma da Solução deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 4.3.17. O hardware e software que executem as funcionalidades de proteção de rede, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- 4.3.18. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
- 4.3.19. O software deverá ser fornecido em sua versão mais atualizada;
- 4.3.20. Deverá possuir a funcionalidade para criação de 1024 VLAN Tags 802.1q;
- 4.3.21. Deverá possuir a funcionalidade para criação de agregação de links 802.3ad e LACP;
- 4.3.22. A solução deve suportar Jumbo frames;
- 4.3.23. Deverá possuir a funcionalidade para criação de policy based routing ou policy based forwarding;
- 4.3.24. Deverá possuir a funcionalidade para criação de roteamento multicast (PIM-SM);
- 4.3.25. Deverá possuir a funcionalidade para criação de DHCP Relay e DHCP Server;
- 4.3.26. Deverá suportar a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
- 4.3.27. Deverá suportar sub-interfaces ethernet lógicas;
- 4.3.28. Os appliances de firewall deverão ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino, que deve estar comunicável através de uma rota. Caso haja falha na comunicação, o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;
- 4.3.29. Deverá suportar Nat dinâmico (Many-to-1), Nat dinâmico (Many-to-Many), Nat estático (1-to-1), NAT estático (Many-to-Many), Tradução de porta (PAT), NAT de Origem, NAT de Destino, Suportar NAT de Origem e NAT de Destino simultaneamente;
- 4.3.30. Deverá implementar Network Prefix Translation (NPTv6) ou outro mecanismo prevenindo problemas de roteamento assimétrico;
- 4.3.31. Deverá implementar balanceamento de link por hash do IP de origem;
- 4.3.32. Deverá implementar balanceamento de link por hash do IP de origem e destino;
- 4.3.33. Deverá implementar balanceamento de link através do método round-robin ou número de sessões ou volume de dados;
- 4.3.34. Deverá implementar balanceamento de link por peso. Nesta opção deverá ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deverá suportar o balanceamento de, no mínimo, dois links;
- 4.3.35. Deverá implementar balanceamento de link através de políticas por usuário e grupos de usuários do AD;
- 4.3.36. Deverá implementar balanceamento de link através de políticas por aplicação e porta de destino;

- 4.3.37. Deverá enviar log para sistemas de monitoração externos, simultaneamente;
- 4.3.38. Deverá haver a opção de enviar logs para os sistemas de monitoração externos via protocolo seguro TLS ou SSL;
- 4.3.39. Deverá possuir proteção contra anti-spoofing;
- 4.3.40. Deverá permitir bloquear sessões TCP que usem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma, possíveis tráfegos maliciosos;
- 4.3.41. Deverá exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de tráfego;
- 4.3.42. Para IPv4, deverá suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 4.3.43. Para IPv6, deverá suportar roteamento estático;
- 4.3.44. Deverá suportar as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), Identificação de usuários a partir do AD, Captive Portal, IPv6 over IPv4 IPsec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPsec, VPN SSL, Ativo/Passivo, SNMP, NTP, DNS, e controle de aplicação;
- 4.3.45. Deverá possuir modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede
- 4.3.46. Deverá possuir modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 4.3.47. Deverá possuir modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 4.3.48. Deverá possuir modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 4.3.49. Deverá suportar a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Modo transparente e em layer 3
- 4.3.50. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede, certificados de-criptografados, associações de Segurança das VPNs e Tabelas FIB;
- 4.3.51. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
- 4.3.52. As funcionalidades de firewall, VPN IPsec e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.
- 4.3.53. Deverá suportar controles por zona de segurança.
- 4.3.54. Deverá possuir controles de políticas por porta e protocolo.
- 4.3.55. Deverá possuir o controle de políticas por aplicações, como por exemplo, categoria de aplicações, risco e características.
- 4.3.56. Deverá possuir controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 4.3.57. Deverá suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;
- 4.3.58. Deverá controlar políticas por código de País (Por exemplo: BR, USA, UK, RUS);

- 4.3.59. Deverá controlar, inspecionar e de-criptografar SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);
- 4.3.60. Deverá de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
- 4.3.61. Deverá de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
- 4.3.62. Deverá bloquear os seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg
- 4.3.63. Deverá possuir Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
- 4.3.64. Deverá possuir QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
- 4.3.65. Suportar objetos e regras IPV6.
- 4.3.66. Suportar roteamento multicast.
- 4.3.67. Deverá suportar, no mínimo, três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
- 4.3.68. Suportar a atribuição de agendamento as políticas, com o objetivo de habilitar e desabilitar políticas em horários pré-definidos, de forma automática.

5. CARACTERÍSTICAS GERAIS DOS TIPOS 1,2 E 3 DO ITEM 1 (SOLUÇÃO DE FIREWALL)

5.1. CONTROLE DE POLÍTICA DE FIREWALL

- 5.1.1. Deverá suportar controles por zona de segurança.
- 5.1.2. Deverá controlar as políticas por porta e protocolo.
- 5.1.3. Deverá ter o controle de políticas por aplicações, como por exemplo categoria de aplicações, risco e características.
- 5.1.4. Deverá ter o controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 5.1.5. Deverá suportar consultas a fontes externas de endereços IP, domínios e URLs, podendo ser adicionados nas políticas de firewall, para bloqueio ou permissão do tráfego;
- 5.1.6. Deverá permitir autenticação segura, através de certificado nas fontes externas de endereços IP, domínios e URLs;
- 5.1.7. Deverá permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;
- 5.1.8. Deverá controlar as políticas por código de País (Por exemplo: BR, USA, UK, RUS).
- 5.1.9. Deverá controlar, inspecionar e de-criptografar SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
- 5.1.10. Deverá de-criptografar tráfego Inbound e Outbound, em conexões negociadas com TLS 1.2;
- 5.1.11. Deverá de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);

- 5.1.12. Deverá possibilitar o bloqueio dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg
- 5.1.13. Deverá possibilitar o Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
- 5.1.14. Deverá possibilitar o QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
- 5.1.15. Deverá suportar objetos e regras IPV6.
- 5.1.16. Deverá suportar roteamento multicast.
- 5.1.17. Deverá suportar, no mínimo, três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP Reset para o server ou para os dois lados da conexão;
- 5.1.18. Deverá suportar a atribuição de agendamento de políticas, com objetivo de habilitar e desabilitar políticas em horários pré-definidos, de forma automática.

5.2. CONTROLE DE APLICAÇÕES

- 5.2.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
- 5.2.2. Deverá possibilitar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- 5.2.3. Reconhecer aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- 5.2.4. Reconhecer, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;
- 5.2.5. Para tráfego criptografado SSL, deverá de-criptografar pacotes a fim de possibilitar a leitura de payload, para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 5.2.6. Deverá permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção, concedendo o acesso a aplicativos como Skype apenas para alguns usuários;
- 5.2.7. Deverá permitir a habilitação de aplicações SAAS, apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: Office 365, Skype, aplicativos google, gmail, etc;
- 5.2.8. Identificar o uso de táticas evasivas via comunicações criptografadas;
- 5.2.9. Atualizar a base de assinaturas de aplicações automaticamente;
- 5.2.10. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do AD;

- 5.2.11. Os dispositivos de proteção de rede deverão possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
- 5.2.12. Deverá ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 5.2.13. Deverá suportar múltiplos métodos de identificação e classificação das aplicações, no mínimo a checando as assinaturas, decodificando os protocolos e utilizando análise heurística;
- 5.2.14. Para manter a segurança da rede eficiente, deverá suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- 5.2.15. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.
- 5.2.16. O appliance deverá permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 5.2.17. Deverá alertar o usuário quando uma aplicação for bloqueada;
- 5.2.18. Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 5.2.19. Deverá possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 5.2.20. Deverá possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;
- 5.2.21. Deverá possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 5.2.22. Deverá possibilitar a criação de grupos estáticos de aplicações com características das aplicações como:
- 5.2.23. Tecnologia utilizada na aplicação (Client-Server, Browser Based, Network Protocol, etc).
- 5.2.24. Nível de risco da aplicação.
- 5.2.25. Categoria e subcategoria de aplicações.
- 5.2.26. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

5.3. PREVENÇÃO DE AMEAÇAS

- 5.3.1. Para proteção do ambiente, contra-ataques, os dispositivos de proteção deverão possuir módulo de IPS, Antivírus e Anti-Spyware, integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante.
- 5.3.2. Deverá incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 5.3.3. As funcionalidades de IPS, Antivírus e Anti-Spyware deverão operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

- 5.3.4. Deverá sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 5.3.5. Deverá implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e Antispyware: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset
- 5.3.6. As assinaturas deverão poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- 5.3.7. Exceções por IP de origem ou de destino deverão ser possíveis nas regras, de forma geral e assinatura a assinatura;
- 5.3.8. Deverá suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
- 5.3.9. Deverá permitir o bloqueio de vulnerabilidades.
- 5.3.10. Deverá permitir o bloqueio de exploits conhecidos.
- 5.3.11. Deverá incluir proteção contra ataques de negação de serviços.
- 5.3.12. Deverá suportar a inspeção e criação de regras de proteção de DOS e QOS;
- 5.3.13. Deverá possuir os seguintes mecanismos de inspeção de IPS:
- 5.3.14. Deverá analisar padrões de estado de conexões;
- 5.3.15. Deverá analisar decodificação de protocolo;
- 5.3.16. Deverá analisar detecção de anomalias de protocolo;
- 5.3.17. Deverá utilizar análise heurística;
- 5.3.18. Deverá utilizar IP Defragmentation;
- 5.3.19. Deverá possibilitar a remontagem de pacotes de TCP;
- 5.3.20. Deverá bloquear pacotes malformados.
- 5.3.21. Deverá ser imune e capaz de impedir ataques básicos como: Syn Flood, ICMP flood, UDP flood, etc;
- 5.3.22. Deverá detectar e bloquear a origem de port scans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;
- 5.3.23. Deverá bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 5.3.24. Deverá suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
- 5.3.25. Deverá possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- 5.3.26. Deverá possuir assinaturas para bloqueio de ataques de buffer overflow;
- 5.3.27. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 5.3.28. Deverá permitir o uso de operadores de negação, na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- 5.3.29. Deverá permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

- 5.3.30. Será permitido, caso o appliance de firewall não suporte, o uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares, em protocolo SMB, de forma a conter malwares a se espalhar de forma horizontal pela rede;
- 5.3.31. Deverá suportar bloqueio de arquivos por tipo;
- 5.3.32. Deverá Identificar e bloquear comunicação com botnets;
- 5.3.33. Deverá suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);
- 5.3.34. Deverá suportar referência cruzada com CVE;
- 5.3.35. Deverá registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
- 5.3.36. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 5.3.37. Deverá permitir captura de pacotes por assinaturas de IPS e Antispyware;
- 5.3.38. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 5.3.39. Os eventos deverão identificar o país de onde partiu a ameaça;
- 5.3.40. Deverá incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
- 5.3.41. Deverá proteger contra downloads involuntários usando HTTP de arquivos executáveis. Maliciosos.
- 5.3.42. Deverá rastrear vírus em pdf.
- 5.3.43. Deverá permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)
- 5.3.44. Deverá ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall, considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração distinta de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

5.4. ANÁLISE DE MALWARES MODERNOS

- 5.4.1. Devido a nova geração de Malwares ser muito dinâmica e um antivírus comum, reativo, não ser capaz de detectá-los, com a mesma velocidade que suas variações são criadas, a solução ofertada deverá possuir funcionalidades para análise de Malwares não conhecidos, incluídas na própria ferramenta ou entregue com composição com outro fabricante;
- 5.4.2. O dispositivo de proteção deverá ser capaz de enviar arquivos trafegados, de forma automática, para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
- 5.4.3. Deverá selecionar através de políticas granulares, quais tipos de arquivos sofrerão esta análise, incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
- 5.4.4. Deverá possuir a capacidade de diferenciar arquivos analisados em, pelo menos, três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;

- 5.4.5. Deverá suportar a análise de comportamentos maliciosos, para a análise da ameaça não conhecida;
- 5.4.6. Deverá suportar a análise de arquivos maliciosos, em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);
- 5.4.7. Deverá suportar a monitoração de arquivos trafegados na internet (HTTPs, HTTP, SMTP);
- 5.4.8. A solução deverá possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deverá ser gerado um relatório, caso a abertura do link pela sandbox o identifique como site hospedeiro de exploits;
- 5.4.9. A análise de links em sandbox, deverá ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;
- 5.4.10. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deverá ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails, permitindo identificação ágil do usuário, vítima do ataque;
- 5.4.11. O sistema de análise “In Cloud” ou local deverá prover informações sobre as ações do Malware, na máquina infectada, como informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis, utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);
- 5.4.12. Deverá permitir exportar o resultado das análises de malwares de dia Zero em PDF ou CSV a partir da própria interface de gerência;
- 5.4.13. Deverá suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
- 5.4.14. Deverá suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar ou class), MacOS (mach-O, DMG ou PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

5.5. FILTRO DE URL

- 5.5.1. Deverá permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 5.5.2. Deverá ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.
- 5.5.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, e base de dados local.
- 5.5.4. Deverá permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
- 5.5.5. Deverá suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
- 5.5.6. Deverá suportar a base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
- 5.5.7. Deverá suportar a exclusão de URLs do bloqueio, por categoria;
- 5.5.8. Deverá permitir a customização de página de bloqueio;

5.5.9. Deverá suportar a inclusão nos logs do produto de informações das atividades dos usuários;

5.5.10. Deverá salvar nos logs das informações dos seguintes campos do cabeçalho HTTP, nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

5.6. IDENTIFICAÇÃO DE USUÁRIOS

5.6.1. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory e base de dados local;

5.6.2. Deverá possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

5.6.3. Deverá possuir integração com Radius para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

5.6.4. Deverá suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC, via syslog ou RADIUS, para a identificação de endereços IP e usuários;

5.6.5. Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

5.6.6. Deverá suporte a autenticação Kerberos, caso não suporte autenticação direta por AD ou Openldap

5.6.7. Deverá suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL, caso não suporte autenticação direta por AD ou Openldap

5.6.8. Deverá possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

5.6.9. Deverá identificar usuários através de leitura do campo x-forwarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

5.6.10. Deverá permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos, através de leitura do campo x-forwarded-for;

5.6.11. Deverá implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do AD;

5.6.12. Deverá possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente.

QoS

5.6.13. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deverá ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

5.6.14. Deverá suportar a criação de políticas de QoS por:

- 5.6.15. Endereço de origem
- 5.6.16. Endereço de destino
- 5.6.17. Por usuário e grupo do LDAP/AD.
- 5.6.18. Por porta;
- 5.6.19. O QoS deverá possibilitar a definição de classes por:
- 5.6.20. Banda Garantida
- 5.6.21. Banda Máxima
- 5.6.22. Fila de Prioridade.
- 5.6.23. Deverá suportar a marcação de pacotes Diffserv, inclusive por aplicação;
- 5.6.24. Deverá disponibilizar estatísticas RealTime para classes de QoS.
- 5.6.25. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

5.7. **FILTRO DE DADOS**

- 5.7.1. Deverá permitir a criação de filtros para arquivos e dados pré-definidos;
- 5.7.2. Deverá permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, Instant Messaging, SMB, etc);
- 5.7.3. Deverá suportar a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 5.7.4. Deverá permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
- 5.7.5. Deverá permitir listar o número de aplicações suportadas para controle de dados;

5.8. **GEOLOCALIZAÇÃO**

- 5.8.1. Deverá suportar a criação de políticas por Geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 5.8.2. Deverá possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- 5.8.3. Deverá possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

5.9. **VPN**

- 5.9.1. Deverá suportar VPN Site-to-Site e Client-To-Site;
- 5.9.2. Deverá suportar IPSec VPN;
- 5.9.3. Deverá suportar SSL VPN;
- 5.9.4. A VPN IPSEC deverá suportar:
- 5.9.5. DES e 3DES;

- 5.9.6. Autenticação MD5 e SHA-1;
- 5.9.7. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 5.9.8. Algoritmo Internet Key Exchange (IKEv1 e v2);
- 5.9.9. AES 128 e 256 (Advanced Encryption Standard)
- 5.9.10. Autenticação via certificado IKE PKI.
- 5.9.11. Deverá possuir interoperabilidade com os seguintes fabricantes:
- 5.9.12. Cisco;
- 5.9.13. Checkpoint;
- 5.9.14. Juniper;
- 5.9.15. Palo Alto Networks;
- 5.9.16. Fortinet;
- 5.9.17. Sonic Wall;
- 5.9.18. A VPN SSL deve suportar:
- 5.9.19. O usuário deverá realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
- 5.9.20. As funcionalidades de VPN SSL deverão ser atendidas com ou sem o uso de agente;
- 5.9.21. Deverá atribuir endereço IP nos clientes remotos de VPN SSL;
- 5.9.22. Deverá permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
- 5.9.23. Deverá permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD e grupo de usuário AD;
- 5.9.24. Deverá permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 5.9.25. Deverá atribuir DNS nos clientes remotos de VPN;
- 5.9.26. Deverá permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 5.9.27. Deverá suportar autenticação via AD/LDAP e base de usuários local;
- 5.9.28. Deverá permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
- 5.9.29. Deverá permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-login;
- 5.9.30. Deverá permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- 5.9.31. O agente de VPN a ser instalado nos equipamentos desktop e laptops, deverá ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
- 5.9.32. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,
- 5.9.33. Deverá permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

- 5.9.34. Antes ou Após autenticação do usuário na estação;
- 5.9.35. Sob demanda do usuário;
- 5.9.36. Deverá manter uma conexão segura com o portal durante a sessão.
- 5.9.37. O agente de VPN SSL client-to-site deverá ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OS, Windows 10;
- 5.9.38. Deverá haver a opção de o cliente remoto escolher manualmente o gateway de VPN;
- 5.9.39. Deverá possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;

5.10. **CONSOLE DE GERÊNCIA**

- 5.10.1. Deverá centralizar a administração de regras e políticas do cluster usando uma única interface de gerenciamento.
- 5.10.2. Deverá centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;
- 5.10.3. O gerenciamento da solução deverá suportar acesso via SSH, cliente ou WEB (HTTPS) ou API aberta;
- 5.10.4. Deverá permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;
- 5.10.5. Caso haja a necessidade de instalação de cliente para administração da solução, o mesmo deverá ser compatível com sistemas operacionais Windows ou Linux ou Mac;
- 5.10.6. O gerenciamento deve permitir/possuir:
- 5.10.7. Criação e administração de políticas de firewall e controle de aplicação;
- 5.10.8. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- 5.10.9. Criação e administração de políticas de Filtro de URL;
- 5.10.10. Monitoração de logs;
- 5.10.11. Ferramentas de investigação de logs;
- 5.10.12. Debugging;
- 5.10.13. Captura de pacotes.
- 5.10.14. Acesso concorrente de administradores;
- 5.10.15. Deverá permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;
- 5.10.16. Deverá mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.
- 5.10.17. Deverá possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmos na configuração do dispositivo;
- 5.10.18. Deverá permitir usar palavras chaves e cores para facilitar identificação de regras;

- 5.10.19. Deverá permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN client-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;
- 5.10.20. Deverá suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;
- 5.10.21. Deverá bloquear as alterações, no caso acesso simultâneo de dois ou mais administradores;
- 5.10.22. Deverá possibilitar definir perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 5.10.23. Deverá haver autenticação integrada ao Microsoft Active Directory e servidor Radius;
- 5.10.24. Deverá conter a localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
- 5.10.25. Deverá atribuir sequencialmente um número a cada regra de firewall, NAT;
- 5.10.26. Deverá possibilitar a criação de regras que fiquem ativas em horário definido;
- 5.10.27. Deverá possibilitar a criação de regras com data de expiração;
- 5.10.28. Deverá possibilitar a habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
- 5.10.29. Deverá possibilitar a validação de regras antes da aplicação;
- 5.10.30. Deverá implementar mecanismo de validação de configurações antes da aplicação das mesmas, permitindo identificar erros, tais como: regras em shadowing etc.
- 5.10.31. Será aceito o uso de appliance externo para permitir a validação de regras antes da aplicação.
- 5.10.32. Deverá possibilitar a validação da(s) política(s), avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- 5.10.33. Será aceito o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- 5.10.34. Deverá possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.
- 5.10.35. Deverá possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)
- 5.10.36. Deverá possibilitar a geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
- 5.10.37. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
- 5.10.38. Deverá possibilitar a geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
- 5.10.39. Deverá prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Antispyware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

- 5.10.40. Deverá permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day" detectados em sandbox e tráfego bloqueado;
- 5.10.41. O gerenciamento da solução deverá possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
- 5.10.42. Deverá permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, antispayware, Filtro de URL e filtro de arquivos em uma única tela;
- 5.10.43. Deverá possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Antispayware), etc;
- 5.10.44. Deverá prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Antispayware), e URLs que passaram pela solução;
- 5.10.45. Deverá possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;
- 5.10.46. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
- 5.10.47. Deverá possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;
- 5.10.48. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) deverão poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;
- 5.10.49. Deverá ser possível exportar os logs em CSV;
- 5.10.50. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.
- 5.10.51. Deverá possuir rotação do log;
- 5.10.52. Deverá permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;
- 5.10.53. Deverá permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
- 5.10.54. Deverá executar a exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
- 5.10.55. Situação do dispositivo e do cluster;
- 5.10.56. Principais aplicações;
- 5.10.57. Principais aplicações por risco;
- 5.10.58. Administradores autenticados na gerência da plataforma de segurança;
- 5.10.59. Número de sessões simultâneas;
- 5.10.60. Status das interfaces;
- 5.10.61. Uso de CPU;
- 5.10.62. Deverá na geração de relatórios, no mínimo, os seguintes relatórios devem ser gerados:

- 5.10.63. Resumo gráfico de aplicações utilizadas;
- 5.10.64. Principais aplicações por utilização de largura de banda de entrada e saída;
- 5.10.65. Principais aplicações por taxa de transferência de bytes;
- 5.10.66. Principais hosts por número de ameaças identificadas;
- 5.10.67. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Antispyware), de rede vinculadas a este tráfego;
- 5.10.68. Deverá permitir a criação de relatórios personalizados;
- 5.10.69. Em cada critério de pesquisa do log deverá ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;
- 5.10.70. Gerar alertas automáticos via:
 - 5.10.71. Email;
 - 5.10.72. SNMP;
 - 5.10.73. Syslog;

5.11. GERENCIAMENTO CENTRALIZADO

- 5.11.1. O gerenciamento centralizado, deverá ser do mesmo fabricante dos equipamentos (appliance) de Tipo 1, 2 e 3.
- 5.11.2. Deverá possibilitar o gerenciamento de no mínimo 10 (dez) equipamentos (appliance).
- 5.11.3. O gerenciamento da Solução de Firewall deverá possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.
- 5.11.4. Deverá possuir o controle sobre os equipamentos da Solução de Firewall (itens 1, 2 e 3), em uma única console, com administração de privilégios e funções.
- 5.11.5. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico, deverá ser compatível com rack 19 polegadas e possui todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual, deverá ser compatível com VMware ESXi e/ou RHEV;
- 5.11.6. Deverá permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;
- 5.11.7. Deverá suportar organizar os dispositivos administrados em grupos: os sistemas virtuais deverão ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;
- 5.11.8. Deverá implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;
- 5.11.9. Deverá implementar a criação de perfis de usuários com acesso à plataforma de gerenciamento, com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;
- 5.11.10. Deverá permitir a criação de objetos e políticas compartilhadas;
- 5.11.11. Deverá consolidar logs e relatórios de todos os dispositivos administrados;
- 5.11.12. Deverá permitir a exportação de backup de configuração automaticamente via agendamento;

5.11.13. Deverá permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e/ou grupos de firewalls;

5.11.14. Deverá mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

5.12. SERVIÇO DE SUPORTE TÉCNICO E GARANTIA DOS EQUIPAMENTOS DA SOLUÇÃO DE FIREWALL

5.12.1. Todas as atividades deverão ser executadas segundo as melhores práticas do fabricante em termos de desempenho, disponibilidade e segurança, por técnico certificado por este, de modo a garantir total interoperabilidade do ambiente computacional.

5.12.2. A CONTRATADA deverá apresentar comprovação de que é uma parceira credenciada da fabricante da solução de Next Generation Firewall ofertada.

5.12.3. A CONTRATADA assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio da EBC ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando da execução demandada pela EBC.

5.12.4. Suporte on-site e remoto por período de 180 (cento e oitenta) dias, contemplando as seguintes atividades e características:

5.12.5. Todo suporte técnico dos itens expostos neste Projeto Básico é de responsabilidade exclusiva da CONTRATADA;

5.12.6. Serviços de suporte técnico compreendem o atendimento para identificação e correção de falhas ou inconsistências detectadas nos produtos, inclusive nas suas configurações e parametrizações, também se aplicando na prestação de informações necessárias ao esclarecimento de dúvidas, de forma a garantir o perfeito funcionamento e utilização da solução, de acordo com o estabelecido nos manuais que acompanham o produto;

5.12.7. Suporte técnico e atendimento ininterruptos e prestados no regime de 24 horas por dia, 7 dias por semana, incluindo fim de semana e feriados;

5.12.8. A CONTRATADA deverá disponibilizar uma central de atendimento, com números de telefone 0800, e-mail de correio eletrônico e endereço web para abertura de chamados online;

5.12.9. Toda e qualquer solicitação feita pela CONTRATANTE (EBC) deverá ser registrada pela CONTRATADA, em sistema informatizado para acompanhamento e controle da execução dos serviços;

5.12.10. A CONTRATADA deverá comunicar a CONTRATANTE (EBC) sobre a descoberta de erros (bugs) na solução durante toda a vigência do contrato. A descrição destes erros e seus possíveis impactos deverão ser divulgados para a CONTRATANTE (EBC), tão logo sejam identificados;

5.12.11. Suporte na modalidade remota e presencial, de acordo com a demanda da CONTRATANTE (EBC);

5.12.12. Resolução de dúvidas e esclarecimentos relativos à utilização e configuração das funcionalidades do ambiente da solução;

5.12.13. Resolução de dúvidas relativas ao licenciamento da solução e validação da conformidade do ambiente da EBC em relação às regras de licenciamento do fabricante;

5.12.14. Resolução de problemas de desempenho do ambiente da solução;

5.12.15. Resolução de problemas da solução que limitem ou impeçam o desenvolvimento e/ou execução das aplicações da EBC que façam uso efetivo das suas funcionalidades;

- 5.12.16. O serviço de suporte deverá ser prestado em idioma português do Brasil;
- 5.12.17. A EBC poderá efetuar um número ilimitado de chamados de suporte durante a vigência da garantia para suprir suas necessidades de utilização da solução;
- 5.12.18. Os prazos máximos para a resolução dos chamados obedecerão ao disposto na tabela constante no item 5.21 – ACORDO DE NÍVEL DE SERVIÇO
- 5.12.19. A CONTRATADA deverá fornecer relatório de atendimento técnico, referente a cada chamado, contendo no mínimo as seguintes informações:
- 5.12.20. Data e hora da abertura do chamado;
- 5.12.21. Data e hora do início do atendimento;
- 5.12.22. Responsável pelo atendimento da solicitação;
- 5.12.23. Motivo da ocorrência (indicação do defeito);
- 5.12.24. Status do chamado (aberto, em tratamento, fechado, etc.);
- 5.12.25. Data e hora do fechamento do chamado;
- 5.12.26. Solução adotada (resolução);
- 5.12.27. A CONTRATADA deverá indicar na Proposta apresentada o número de telefone, e-mail e endereço de site na internet da central de atendimento para abertura de chamados.
- 5.12.28. A CONTRATADA deverá oferecer garantia mínima de 180 (cento e oitenta) dias para os itens da Solução de Firewall, contados a partir da data da emissão da nota fiscal.
- 5.12.29. A garantia ofertada deverá ser da CONTRATADA ou diretamente pelo fabricante, mas com o intermédio da CONTRATADA em todas as ações necessárias.
- 5.12.30. Em caso de substituição de equipamento, este deverá ser realizado por idêntico modelo ou superior, devidamente justificado;
- 5.12.31. Como são equipamentos redundantes em cluster, com alta disponibilidade, os níveis de serviço se referem a indisponibilidade do serviço provido pelo cluster. Caso um dos equipamentos do cluster apresente falhas que não prejudique o serviço provido, o chamado deverá ser classificado como uma solicitação que não envolve paralisação ou severa perda de desempenho.

5.13. **SERVIÇO DE SOC (SECURITY OPERATION CENTER – CENTRO DE OPERAÇÃO DE SEGURANÇA) (ITEM 3)**

5.13.1. **REQUISITOS DO SERVIÇO DE SOC**

- 5.13.2. Serviços da central operacional de segurança
- 5.13.3. O serviço de SOC consiste na sustentação, gerência, monitoramento e correções da solução de Next Generation Firewall atualmente em operação na EBC, disposto nos itens que compõem este Projeto Básico.
- 5.13.4. Toda e qualquer atividade referente a configurações, ajustes e outras parametrizações, que ocorrerem durante a vigência contratual, será precedida da abertura de um chamado técnico.
- 5.13.5. Caso a atividade ocorra de modo proativo, a CONTRATADA informará a EBC o motivo da execução tempestiva das ações através de um canal de comunicação, como e-mail ou telefone.
- 5.13.6. A EBC poderá solicitar a execução de serviços específicos através de canais de comunicação, como:
- 5.13.7. E-mail;

- 5.13.8. Contato Telefônico via 0800;
- 5.13.9. Sistema de Chamados Web;
- 5.13.10. A CONTRATADA deverá possuir sistema de abertura de chamados para que a EBC possa receber um identificador único para cada solicitação de atendimento. A CONTRATADA deverá possuir recursos, como central de e-mail, página web, central telefônica e etc., para manter a equipe técnica do CONTRATANTE (EBC) informada sobre o andamento de cada solicitação de serviço, esteja ele em execução ou encerrado.
- 5.13.11. As solicitações serão classificadas e atendidas segundo prioridade definida pela equipe técnica da CONTRATADA, mediante informação de urgência e impacto da EBC.
- 5.13.12. A EBC considerará efetivamente realizado o serviço quando houver confirmação por sua área técnica da conclusão satisfatória do atendimento;
- 5.13.13. Todas as solicitações técnicas somente poderão ser encerradas com a anuência da EBC.
- 5.13.14. A CONTRATADA manterá cadastro das pessoas indicadas pela EBC, que poderão efetuar a abertura e fechamento das solicitações de serviço.
- 5.13.15. A CONTRATADA deverá emitir relatórios mensais, e sempre que solicitado pela EBC, em arquivo eletrônico, preferencialmente nos formatos .DOC, .DOCX ou .PDF, com informações analíticas dos serviços prestados no período, incluindo:
- 5.13.16. Quantidade de chamados registrados no período;
- 5.13.17. Número do chamado registrado e nível de severidade, inclusive aqueles com reabertura;
- 5.13.18. Data e hora de abertura (horário de Brasília/DF);
- 5.13.19. Data e hora de início e conclusão do atendimento (horário de Brasília/DF);
- 5.13.20. Consumo total de horas dos chamados no mês;
- 5.13.21. Identificação do técnico do CONTRATANTE (EBC) que registrou o chamado;
- 5.13.22. Identificação do técnico da CONTRATADA(EBC) que prestou o suporte técnico;
- 5.13.23. Descrição do problema;
- 5.13.24. Descrição da solução;
- 5.13.25. Informações sobre eventuais escalações;
- 5.13.26. Total de chamados no mês e o total acumulado até a apresentação do relatório.
- 5.13.27. Nos casos em que alguma atividade do serviço necessite da parada da solução, a EBC deverá ser imediatamente notificada para que se proceda com a autorização, ou para que seja agendada nova data, a ser definida pela EBC.
- 5.13.28. O serviço de SOC deverá operar todos os dias do ano, no idioma português, devendo a empresa possuir uma central de atendimento sem custos adicionais para a EBC.
- 5.13.29. A central de atendimento poderá ser subcontratada, mas todas as tratativas deverão ser feitas entre a CONTRATADA e a EBC.
- 5.13.30. O serviço de SOC deverá atender a solução que compõem o item 1 (da Solução de Firewall);
- 5.13.31. O Serviço de SOC deverá ser prestado seguindo as devidas recomendações abaixo:
- 5.13.32. A CONTRATADA deverá ter profissionais empregados e qualificados de acordo com as certificações da solução de Next Generation Firewall ofertada;
- 5.13.33. Não serão aceitas certificações de nível sales, foundation ou accreditation;

- 5.13.34. A CONTRATADA deverá monitorar e gerenciar toda a solução de Next Generation Firewall durante o período de vigência contratual;
- 5.13.35. O serviço de SOC será realizado por uma equipe de trabalho que será responsável pela prestação dos seguintes tipos de serviços:
- 5.13.36. Gerenciamento;
- 5.13.37. Monitoramento;
- 5.13.38. As rotinas básicas de trabalho, apresentadas no item “Descrição das Rotinas Básicas de Trabalho” poderão ser alteradas a qualquer momento pela EBC, por iniciativa própria ou a partir de sugestões da CONTRATADA, como objetivo de melhorar o serviço prestado.
- 5.13.39. Equipe prevista para a prestação dos serviços de SOC:

Qualificação Profissional	Equipe Inicial
Perfil Coordenador	1
Perfil Analista Sênior	2
Perfil Analista Pleno	2

- 5.13.40. A Qualificação profissional mínima exigida para cada tipo de serviço e para cada nível de empregado da CONTRATADA está discriminado no item “Qualificação Profissional Mínima Exigida”.
- 5.13.41. O serviço de SOC será prestado com atendimento 24x7x365 para as chamados críticos. E os atendimentos ocorreram de acordo com o SLA definido na tabela abaixo **item 5.18**. Quanto ao atendimento sobreaviso: Fora do horário comercial, equipe da CONTRATADA deverá estar disponível para, eventualmente, fazer parte de um serviço de sobreaviso, disponível para acesso remoto ao ambiente da EBC, de forma a fazer cobertura 24x7 do ambiente, para suporte técnico a solução de Next Generation Firewall. Caso necessário, ou solicitado, o atendimento deverá ser realizado nas dependências da EBC.
- 5.13.42. A CONTRATADA terá acesso via VPN a console de gerenciamento centralizado para as atividades solicitadas e toda a parte de gerência e monitoramento da solução;

5.14. **GERENCIAMENTO**

- 5.14.1. Será de responsabilidade da CONTRATADA o gerenciamento completo da solução de Next Generation firewall.
- 5.14.2. O gerenciamento dos parâmetros da solução de Next Generation Firewall, em fase posterior a implantação dos mesmos, estará limitado as seguintes atividades:
- 5.14.3. A CONTRATADA ficará responsável por:
- 5.14.4. Criação de regras de firewall;
- 5.14.5. A CONTRATADA poderá identificar regras duplicadas ou que podem ser otimizadas para aumentar a performance dos equipamentos;
- 5.14.6. A CONTRATADA poderá sugerir melhorias nas regras para melhor organização;
- 5.14.7. Caso a CONTRATADA identifique regras com risco elevado ao negócio, a mesma orientará a EBC sobre os riscos de execução da regra;
- 5.14.8. Criação de objetos;
- 5.14.9. Criação de regras de NAT;
- 5.14.10. Criação de rotas;
- 5.14.11. Controle de acesso a VPN;

- 5.14.12. Criação de túnel IPSEC;
- 5.14.13. Configuração de túnel IPSEC;
- 5.14.14. Configuração de novas interfaces;
- 5.14.15. Revisão de regras;
- 5.14.16. Backup de configurações;
- 5.14.17. Atividades não relacionadas ao serviço prestado;
- 5.14.18. Mitigação de malwares em endpoints infectados;
- 5.14.19. Identificação de movimentação lateral de tráfego, onde o fluxo de dados não é controlado pela solução de Next Generation Firewall;
- 5.14.20. Identificação e bloqueio de arquivos com conteúdo sensível a organização;
- 5.14.21. Para o gerenciamento dos ativos, deverão ser aplicadas todas as recomendações da fabricante;
- 5.14.22. A contratada, deverá ser realizar a atualização do sistema operacional dos equipamentos para a última versão estável informada pela fabricante, sempre que solicitada pela CONTRATANTE (EBC);
- 5.14.23. Todas as atualizações que envolvam indisponibilidade do ambiente, devem ser agendadas com a equipe técnica da CONTRATANTE (EBC).
- 5.14.24. A CONTRATADA deverá gerar relatórios mensais (enviados por e-mail a todas as pessoas pré-definidas pela equipe da EBC), e quando solicitados pela CONTRATANTE (EBC), extraídos da solução de Next Generation Firewall, contendo atividades detectadas conforme os itens abaixo:
- 5.14.25. Ameaças;
- 5.14.26. Filtro de Conteúdo Bloqueado;
- 5.14.27. Análises do Sandbox;
- 5.14.28. Acesso a VPN;
- 5.14.29. Falhas detectadas na solução;
- 5.14.30. Arquivos que foram analisados pela solução de Next Generation Firewall;
- 5.14.31. Disponibilização de painéis na Solução Integrada de SOC;
- 5.14.32. A CONTRATADA deverá realizar a configuração de painéis e relatórios de monitoramento na Solução Integrada de SOC fornecida, de modo a permitir o acompanhamento do status diário da solução pela EBC.
- 5.14.33. A CONTRATADA deverá configurar um conjunto básico de painéis, contendo indicadores definidos de acordo as bases específicas para monitoramento, podendo as mesmas serem customizadas para o ambiente da EBC.
- 5.14.34. Toda a atividade de gerenciamento desejada pela CONTRATANTE (EBC) deverá ser aberta através de portal de chamados, telefone ou e-mail.
- 5.14.35. O portal de chamados deverá ser fornecido via acesso web.
- 5.14.36. Toda e qualquer atividade referente ao gerenciamento, que pode ocorrer durante a fase de gerenciamento da solução, serão precedidas da abertura de um chamado técnico.
- 5.14.37. A CONTRATADA deverá fornecer contato telefônico via 0800 com atendimento 24x7.

5.15. MONITORAMENTO

- 5.15.1. O monitoramento da solução deverá ser realizado em regime contínuo, 24x7.
- 5.15.2. O monitoramento da solução deverá ser realizado nas dependências da CONTRATADA.
- 5.15.3. A CONTRATADA deverá monitorar alertas gerados pela solução ofertada, envolvendo atividades como:
- 5.15.4. Alta disponibilidade;
- 5.15.5. Atividades de Rede;
- 5.15.6. Atividades de Ameaças;
- 5.15.7. Atividades do Túnel Ipsec;
- 5.15.8. Falhas de interfaces dos equipamentos;
- 5.15.9. Consumo de link de internet;
- 5.15.10. Controle de Aplicações;
- 5.15.11. Detecções de Botnet;
- 5.15.12. Detecção de Hosts com acessos a domínios maliciosos;
- 5.15.13. Em eventos de monitoramento de alertas de segurança, onde o analista identificar certos indicadores de comportamento, que serão detalhados pela solução de Next Generation Firewall, a CONTRATADA emitirá um relatório informativo de modo a dar visibilidade a CONTRATANTE (EBC) de possíveis riscos associados ao evento.
- 5.15.14. Em casos de incidentes ocorridos, detectados em soluções terceiras, a CONTRATADA poderá ser acionada a fim de identificar algum registro do incidente da solução de Next Generation Firewall.

5.16. **Requisitos de Formação da Equipe**

5.16.1. A qualificação profissional mínima exigida, com relação à certificação, compreende:

Perfil do Coordenador		
Formação	Nível Superior completo, com carga horária mínima de 360 horas, em uma das seguintes áreas: Segurança da Informação, Rede de Computadores, Análise de Sistemas, Ciência da Computação, Processamento de Dados, Sistemas de Informação, Engenharia da Computação, Engenharia de Redes ou áreas afins.	
	Curso de pós-graduação ou especialização em gestão.	
Experiência	Mínimo de 5 (cinco) anos de experiência em tecnologia da informação, comprovados através de registro em CTPS por empresa onde a atividade principal está ligada a área.	

Perfil do Profissional Analista Sênior	
--	--

Formação	Nível Superior completo, com carga horária mínima de 360 horas, em uma das seguintes áreas: Segurança da Informação, Rede de Computadores, Análise de Sistemas, Ciência da Computação, Processamento de Dados, Sistemas de Informação, Engenharia da Computação, Engenharia de Redes ou Curso de pós-graduação em segurança da informação.	
Experiência	Mínimo de 3 (três) anos de experiência em tecnologia da informação, comprovados através de registro em CTPS por empresa onde a atividade principal está ligada a área.	

Perfil do Profissional Analista Pleno		
Formação	Nível Superior completo, com carga horária mínima de 360 horas, em uma das seguintes áreas: Segurança da Informação, Rede de Computadores, Análise de Sistemas, Ciência da Computação, Processamento de Dados, Sistemas de Informação, Engenharia da Computação, Engenharia de Redes ou áreas afim.	
Experiência	Mínimo de 1 (um) anos de experiência em tecnologia da informação, comprovados através de registro em CTPS por empresa onde a atividade principal está ligada a área.	

5.17. CENTRO DE OPERAÇÃO DE SEGURANÇA DA INFORMAÇÃO

5.17.1. O Centro de Operação de Segurança da CONTRATADA deverá estar fisicamente estabelecido fora da EBC;

5.17.2. Deverá possuir estrutura física que garanta um ambiente seguro e controlado.

5.17.3. Deverá utilizar sistema de gerenciamento de CFTV.

5.17.4. Deverá filmar toda a área do Datacenter, mantendo as imagens armazenadas por no mínimo 60 (sessenta) dias.

5.17.5. Deverá ter o controle de acesso ao Datacenter com biometria.

5.17.6. Deverá efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao Centro de Operação de Segurança da Informação.

5.17.7. Caso algum dos serviços de gerenciamento e monitoramento não seja realizado no mesmo espaço físico que o de Centro de Operação de Segurança da Informação, todos os requisitos devem ser atendidos.

- 5.17.8. Deverá possuir sistema de climatização de modo a garantir as corretas condições térmicas para os equipamentos no ambiente da infraestrutura física;
- 5.17.9. Deverá possuir solução de no-break de modo a garantir o funcionamento mesmo em caso de falha elétrica no ambiente da infraestrutura física do Datacenter do Centro de Operação de Segurança da Informação.
- 5.17.10. A CONTRATADA deverá possuir solução de segurança, interna, composta de pelo menos:
- 5.17.11. Detecção de intrusão para o acesso à internet;
- 5.17.12. Solução de Firewall;
- 5.17.13. Solução de antivírus;
- 5.17.14. Solução de prevenção de ameaças;
- 5.17.15. Solução de Sandboxing;
- 5.17.16. Solução de Filtro de Conteúdo Web;
- 5.17.17. Solução de Gerenciamento de Vulnerabilidades;
- 5.17.18. A EBC realizará vistoria e auditoria no ambiente da CONTRATADA para averiguar os quesitos técnicos solicitados, em até 90 dias, após assinatura de contrato. Novas vistorias poderão ser realizadas a critério exclusivo da EBC, sem aviso prévio.

5.18. **ACORDO DE NÍVEL DE SERVIÇO**

Localidade	Tipo do Chamado	Tempo para atendimento inicial	Prazo para Solução
Brasília/Rio de Janeiro/São Paulo	Solicitações e chamados que não envolvam paralisações ou severa perda de desempenho nos serviços	2 horas	24 horas
São Luis/MA e Tabatinga/AM	Solicitações e chamados que não envolvam paralisações ou severa perda de desempenho nos serviços	2 horas	48 horas
Brasília/Rio de Janeiro/São Paulo	Solicitações e chamados que envolvam paralisações ou severa perda de desempenho nos serviços	2 horas	4 horas
São Luis/MA e Tabatinga/AM	Solicitações e chamados que envolvam paralisações ou severa perda de desempenho nos serviços	2 horas	8 horas

5.19 **Mecanismo de Glosa por Descumprimento de SLA**

Tópico	Descrição
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes no chamado técnico.

Meta a cumprir	TC	Diferenciação do tipo de chamado nas solicitações que envolvam ou não paralisação ou severa perda de desempenho nos serviços.
	TA	Tempo para atendimento inicial do chamado (em horas), a partir da abertura do chamado técnico, junto à CONTRATADA.
	TS	Tempo para solução dos chamados (em horas), a partir da abertura do chamado técnico, junto à CONTRATADA.
Instrumento de medição	Através dos chamados técnicos abertos junto à CONTRATADA, avaliando as metas a cumprir. Será utilizado o Instrumento de Medição de Resultados que trata a IN 05/2017-SEGES/ME, aplicada de forma subsidiária.	
Forma de acompanhamento	A avaliação será feita pelo fiscal técnico, que utilizará a linha de base do cronograma registrada na abertura do chamado, levando em conta o tempo de atendimento inicial, tempo para solução dos chamados e o tipo de chamado (Severidade).	
Periodicidade	A cada abertura de chamado técnico junto à CONTRATADA, respeitando o período mensal de avaliação.	

	Localidade	Tipo de chamado	Tempo para atendimento inicial (TA) dos chamados (em horas)	Tempo para solução (TS) dos chamados (em horas)	Classificação do atendimento / Sanção
	Brasília, São Paulo e Rio de Janeiro	Solicitações e chamados que não envolvam paralisações ou severa perda de desempenho nos serviços	TA > 2 = Glosa de 0,1% do valor mensal do Item Contratado	TS ≤ 24	Aceito
				TS > 24	Glosa de 1% do valor mensal do Item Contratado
				TS > 72	Glosa de 3% do valor mensal do Item Contratado
				TS > 120	Glosa de 6% do valor mensal do Item Contratado
		Solicitações e chamados que envolvam paralisações ou severa perda de desempenho nos serviços	TA > 2 = Glosa de 0,1% do valor mensal do Item Contratado	TS ≤ 4	Aceito
				TS > 4	Glosa de 1% do valor mensal do Item Contratado
				TS > 12	Glosa de 3% do valor mensal do Item Contratado

Mecanismo de Cálculo (métrica)				TS > 24	Glosa de 1% por hora de atraso até a entrega da solução e até o limite de 30% do valor mensal do Item Contratado.
	Tabatinga e São Luís	Solicitações e chamados que não envolvam paralisações ou severa perda de desempenho nos serviços	TA > 2 = Glosa de 0,1% do valor mensal do Item Contratado	TS ≤ 48	Aceito
				TS > 48	Glosa de 1% do valor mensal do Item Contratado
				TS > 96	Glosa de 3% do valor mensal do Item Contratado
				TS > 144	Glosa de 7% do valor mensal do Item Contratado
		Solicitações e chamados que envolvam paralisações ou severa perda de desempenho nos serviços	TA > 2 = Glosa de 0,1% do valor mensal do Item Contratado	TS ≤ 8	Aceito
				TS > 8	Glosa de 1% do valor mensal do Item Contratado
				TS > 16	Glosa de 3% do valor mensal do Item Contratado
				TS > 48	Glosa de 0,5% por hora de atraso até a entrega da solução e até o limite de 30% do valor mensal do Item Contratado
	TC = TA + TS				
Onde:					
TC – Tipo de chamado (Severidade);					
TA – Tempo de atendimento inicial do chamado – Corresponde ao tempo de recebimento do chamado e início das tratativas com a equipe técnica da EBC.					
TS – Tempo de solução dos chamados – Corresponde ao período inicial da prestação do serviço até a sua resolução final.					
A data de início será aquela constante na abertura do chamado;					
A data de fechamento do chamado deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução do chamado continua a correr, findando-se apenas quanto a Contratada executa a resolução do chamado técnico e haja aceitação por parte do fiscal técnico.					
Início de Vigência		A partir da emissão do chamado técnico.			

ENCARTE B

Modelo de Proposta de Preços

1. IDENTIFICAÇÃO DA CONTRATADA

Razão Social: _____

CNPJ: _____

Endereço: _____

Cidade: _____ UF: _____ CEP: _____

Telefone: _____

E-mail: _____

Representante Legal: _____

Cargo: _____

2. OBJETO DA PROPOSTA

Prestação de Serviço de Solução de Segurança da Informação do tipo Next Generation Firewall (NGFW), que contempla a manutenção da Solução de Firewall existente e do Serviço de SOC (Security Operations Center - Centro de Operação de Segurança) por um período de 180 (cento e oitenta) dias, garantidas as atualizações de versões, *patches* de segurança e *updates* de assinaturas contra ameaças por todo o período contratado.

3. PLANILHA DE PREÇOS

Item	Descrição	Unidade	Valor Mensal (R\$)	Valor Total (R\$)
01	Serviço de Solução de Firewall da EBC (solução em cluster em: Brasília - DF, Rio de Janeiro - RJ, São Paulo SP, São Luis - MA e Tabatinga - AM	Subscrição		
02	Serviço de SOC (Security Operations Center - Centro de Operação de Segurança). Serviço especializado na solução de Firewall	Subscrição		
Valor total global por 180 (cento e oitenta) dias				

4. RESUMO FINANCEIRO

Descrição	Valor (R\$)
Valor Global da Proposta	_____
Valor por extenso	_____

A proposta possui validade mínima de 90 (noventa) dias, contados da data de sua apresentação.

5. DADOS BANCÁRIOS

Banco: _____

Agência: _____

Conta Corrente: _____

PIX: _____

5. ASSINATURA

Local: _____

Data: // _____

Representante Legal:

Nome:

Cargo:

ENCARTE C

DECLARAÇÃO PARA PARTICIPAÇÃO E CONTRATAÇÃO

IMPEDIMENTOS DO RILC DA EBC

.....(Razão Social), inscrita no CNPJ sob o nº (MATRIZ), por intermédio de seu representante legal o(a) Sr(a)..... portador(a) da Carteira de Identidade - RG nº..... e do CPF nº.....DECLARA, sob pena de responder civil e penalmente no caso de informações inverídicas, que:

I. Não está impedida de participar de licitações e de ser contratada pela EBC;

II. Não possui administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social que seja diretor ou empregado da EBC;

III. Não está suspensa de participar em licitação e nem de contratar com a EBC;

IV. Não está declarada inidônea pela União;

V. Não é constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea;

VI. Não possui administrador na condição de sócio de empresa suspensa, impedida ou declarada inidônea;

VII. Não é constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida, ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

VIII. Não possui administrador que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

IX. Não possui no quadro de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea;

X. Não possui relação de parentesco, até o terceiro grau civil, com dirigente da EBC, empregado da EBC cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação e/ou autoridade do ente público a que a EBC esteja vinculada;

XI. Não é sócio de empresa que tenha terminado seu prazo de gestão ou rompido seu vínculo com a EBC há menos de 06 (seis) meses;

XII. Nos preços propostos estão incluídos todos os custos e despesas, taxas e impostos, de qualquer natureza que possam incidir, direta ou indiretamente, sobre o objeto a ser contratado, tais como: salário, ônus tributários, fiscais, parafiscais, trabalhistas e sociais, auxílio-alimentação, vale-transporte, uniforme, frete, todos os materiais, utensílios, equipamentos, dentre outros;

XIII. Possui responsabilidade exclusiva sobre a quitação de encargos previdenciários, fiscais, trabalhistas e comerciais decorrentes da execução do contrato;

XIV. Garante a qualidade dos serviços prestados durante a vigência do Contrato;

XV. Conhece a legislação de regência do objeto a ser licitado e que esse será executado e fornecido de acordo com as condições estabelecidas;

XVI. Assumem o compromisso de não realizar atos de discriminação, em todas as suas formas, por motivos de raça, gênero e outros, conforme dispõe a Constituição Federal de 1988 em seu inciso IV do art. 3º, inciso I do art. 5º e os arts. 38 e 39 do Estatuto da Igualdade Racial, Lei nº 12.288, de 20 de julho de 2010;

XVII. Se compromete a não praticar, de nenhuma forma, ações que lesionem a Dignidade da Pessoa Humana e a Valorização do Trabalho Humano protegidos nos arts. 1º e 170 da Constituição Federal, e que possam ser enquadradas nos arts. 149, 203 e 207 do Código Penal (dispositivos que tratam do trabalho análogo ao de escravo e tráfico de pessoas para esse fim), Decreto nº 5.017/2004, que promulga o Protocolo de Palermo e as Convenções da OIT nos 29 e 105;

XVIII. Concorde, expressa e integralmente, com os termos e condições de contratação do Regulamento Interno de Licitações e Contratos da Empresa Brasil de Comunicação SA – EBC e da Lei nº 13.303/2016, disponível no seguinte endereço eletrônico: <https://acessoainformacao.ebc.com.br/institucional/atos-normativos/regulamento-interno-de-licitacoes-e-contratos>;

XIX. Não explora o trabalho infantojuvenil, em atenção ao que dispõe o inciso XXXIII do art. 7º da Constituição Federal de 1988, o Título III, Capítulo IV, do Decreto-Lei nº 5.452, de 1 de maio de 1943 (CLT), os arts. 60 a 69 da Lei nº 8.069, de 19 de julho de 1990 (ECA), e o Decreto nº 6.841, de 12 de junho de 2008, o qual trata da proibição das piores formas de trabalho infantil e ação imediata para sua eliminação;

XX. Não possui inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pelo Ministério do Trabalho e Emprego, por meio da Portaria Interministerial MTE/MDHC/MIR nº 18, de 13 de setembro de 2024.

XXI. Declaro observar e atender as disposições contidas no Projeto Básico, especialmente no que tange aos requisitos de sustentabilidade afetos ao objeto da contratação.

_____, de _____ de 20____.

(Local e Data)

(Nome e Assinatura do Representante Legal)

(Identificação Completa)

(Nº do RG do declarante)

ENCARTE D

Termo de Sigilo e Privacidade

CONTRATANTE: EMPRESA BRASIL DE COMUNICAÇÃO S.A. - EBC

CNPJ: 09.168.704/0001-42

CONTRATADA:

CNPJ:

CLÁUSULA PRIMEIRA – DO OBJETO

Constitui objeto deste Termo esclarecer e identificar as condições específicas para regulamentar as obrigações relativas à proteção de dados pessoais, previstos na Lei nº 13.709/2018 e na regulamentação pertinente, a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações e dados, disponibilizados pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do Contrato Original celebrado entre as partes.

CLÁUSULA SEGUNDA – CONCEITOS E DEFINIÇÕES

2.1. Para os efeitos deste TERMO aplicam-se os seguintes conceitos e definições:

2.1.1. Confidencialidade ou Sigilo:

Propriedade de que a informação não seja revelada a pessoa física, sistema, órgão ou entidade não autorizados e credenciados, sem a prévia e expressa autorização da EBC.

2.1.2. Contrato de trabalho ou Contrato principal:

Contrato celebrado entre as partes, ao qual este Termo de Sigilo se vincula.

2.1.3. Dado pessoal:

Informação relacionada a pessoa natural identificada ou identificável (Lei nº 13.709/2018).

2.1.4. Dado pessoal sensível:

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

2.1.5. Informação:

Conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

2.1.6. Informação de acesso restrito:

Aquelas que estão submetidas temporariamente à restrição de acesso público.

2.1.7. Informação sigilosa:

Aquelas que estão submetidas à restrição de acesso público, cujo conhecimento e divulgação estão regidos por esse instrumento.

2.1.8. Informações de acesso restrito, sigilosas por legislação específica (não exaustivas):

I. Hipóteses de sigilo aplicáveis a informações de natureza patrimonial:

- a) Segredo industrial (Lei nº 9.279/1996);
- b) Direito autoral (Lei nº 9.610/1998); e
- c) Propriedade intelectual de Software (Lei nº 9.609/1998).

II. Hipóteses de sigilo decorrentes de direitos de personalidade:

- a) Sigilo Fiscal (Art. 198 da Lei nº 5.172/1966);
- b) Sigilo bancário (Art. 1º da LC nº 105/2001);
- c) Sigilo Comercial (§ 2º do art. 155 da Lei nº 6.404/1976);
- d) Sigilo Empresarial (Art. 169 da Lei nº 11.101/2005); e
- e) Sigilo Contábil (Art. 1.190 e 1.191 da Lei nº 13.105/2015).

III. Hipóteses de sigilo decorrentes de processos e procedimentos:

- a) Sigilo de inquérito policial (Art. 20 da Decreto-Lei nº 3.689/1941);
- b) Segredo de justiça no processo civil (Art. 189 da Lei nº 13.105/2015); e
- c) Segredo de justiça no processo penal (§ 6º do art. 201 da Decreto-Lei nº 3.689/1941).

IV. Hipóteses de sigilo empresarial/estratégico:

Sigilo de informações aplicáveis às atividades concorrenciais, e/ou relativas aos negócios estratégicos da EBC.

2.1.9. Necessidade de conhecer:

Condição pessoal inerente à função ou atividade, indispensável para que o colaborador tenha acesso a dados ou informações classificadas. De acordo com este princípio, os colaboradores só devem ter acesso às informações necessárias para o desenvolvimento de suas atividades relacionadas com a execução do objeto contratual.

2.1.10. Tratamento ou processamento de dados pessoais:

Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

CLÁUSULA TERCEIRA – INFORMAÇÕES SIGILOSAS

3.1. Serão consideradas como informações sigilosas, toda e qualquer informação, revelada à outra parte por razão da execução do contrato, contendo ou não marcação ou rótulo de grau de sigilo. O termo "informação" 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 Original celebrado entre as partes.

3.2. A CONTRATADA compromete-se a não revelar, copiar, transmitir, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do Contrato Original, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do Contrato Original.

CLÁUSULA QUARTA – EXTENSÃO DA RESPONSABILIDADE

4.1. A CONTRATADA se obriga a:

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 sigilosas por seus agentes, representantes ou por terceiros, obtidas em virtude do Contrato Original; e

b) Comunicar à CONTRATANTE de forma prévia e expressa, antes de qualquer divulgação, caso haja solicitação de revelar qualquer das informações relativas ao Contrato Original, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão ou autoridade pública competente.

CLÁUSULA QUINTA – DIREITOS E OBRIGAÇÕES

5.1. A CONTRATADA se compromete e se obriga a utilizar a informação sigilosa revelada pela CONTRATANTE exclusivamente para os propósitos da execução do Contrato Principal, em conformidade com o disposto neste Termo e no Contrato Original.

5.2. A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação que tiver acesso em virtude do Contrato Original, sem o consentimento expresso e prévio da CONTRATANTE.

5.3. A CONTRATADA se compromete a obter o aceite formal dos funcionários/colaboradores que atuarão direta ou indiretamente na execução do Contrato Principal sobre a existência deste Termo, bem como da natureza sigilosa das informações, a instruir sobre as formas de tratamento das informações a que terão acesso, e dar ciência à CONTRATANTE dos documentos comprobatórios, quando solicitado.

5.4. A CONTRATADA obriga-se a tomar todas as medidas necessárias a proteção da informação sigilosa, bem como para evitar e prevenir a revelação a terceiros.

5.5. A CONTRATADA deve adotar Política de Segurança de Informação que comprove o atendimento dos requisitos de sigilo e segurança definidos no âmbito do Contrato Original, observando a LGPD e a regulamentação pertinente.

5.1. A CONTRATADA deverá, quando requerido pela CONTRATANTE, proceder com o imediato descarte de forma irreversível, incluindo todas e quaisquer cópias eventualmente existentes em qualquer suporte de todas as informações sigilosas sob sua custódia referentes ao Contrato Original.

CLÁUSULA SEXTA – DA PROTEÇÃO DE DADOS PESSOAIS

6.1. Ambas as partes se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, em qualquer formato ou suporte, cooperando mutuamente para observar a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), em especial perante a Autoridade Nacional de Proteção de Dados (ANPD), sem prejuízo dos demais órgãos ou autoridades públicas competentes.

6.2. São escopo de tratamento somente os dados pessoais indispensáveis para a execução do objetivo contratual, e conforme bases legais pré-estabelecidas e acordadas, e finalidades específicas, cabendo à CONTRATADA observar estritamente a finalidade a que se destinam os dados pessoais a que venha a ter conhecimento.

6.3. Necessidades de coleta de consentimento para outras finalidades deverão ser identificadas e correr sob responsabilidade da CONTRATANTE, ouvido previamente o Encarregado pelo Tratamento de Dados na EBC.

6.4. À CONTRATADA é vedada qualquer forma de compartilhamento de dados pessoais com terceiros no âmbito do contrato, sem prévia e expressa autorização da CONTRATANTE, ouvido previamente o Encarregado pelo Tratamento de Dados na EBC.

6.5. Ao término do Contrato Original, a CONTRATADA deverá comprovar a cessação de acessos, uso e o descarte definitivo dos dados pessoais, no que couber, conforme procedimentos a serem determinados, ouvido previamente o Encarregado pelo Tratamento de Dados na EBC.

6.6. A CONTRATADA adotará todas as medidas de segurança necessárias para impedir a divulgação, alteração ou destruição não autorizados dos dados pessoais, bem como acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, conforme a previsão do art. 46 da Lei nº 13.709/2018 (LGPD).

CLÁUSULA SÉTIMA – DISPOSIÇÕES ESPECIAIS

7.1. Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

7.2. O não exercício, por qualquer uma das Partes, de direitos assegurados neste instrumento não importará em renúncia aos mesmos, sendo considerado como mera tolerância para todos os efeitos de direito;

7.3. Todas as condições, termos e obrigações ora pactuadas serão regidas pela legislação e regulamentação brasileiras pertinentes, inclusive as Normas Internas da EBC;

7.4. O presente Termo somente poderá ser alterado mediante termo aditivo ao Contrato Original firmado pelas partes;

7.5. Teve acesso e compromete-se a observar a Política de Segurança da Informação e da Comunicação - PO 900-01, disponível no Portal da EBC: https://www.ebc.com.br/sites/_institucional/files/atoms/files/politica-de-seguranca-da-informacao-e-comunicacao-po-900-01-aprovada.pdf

7.6. Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste Termo de Sigilo e Privacidade, que permanecerá válido e com todos

seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

7.7. O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados 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; e

7.8. Este Termo não deve ser interpretado como criação ou envolvimento das Partes, ou suas afiliadas, nem em obrigação de divulgar informações sigilosas para a outra Parte.

CLÁUSULA OITAVA – DA VIGÊNCIA

8.1. O presente Termo de Sigilo e Privacidade tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de início das atividades pertinentes ao Contrato Original, do qual será tido por Anexo, mantendo-se o dever de sigilo após o prazo final do Contrato Original por 5 (cinco) anos ou, se a informação for estratégica para os negócios da EBC ou aplicáveis às atividades concorrenciais, não poderá ser divulgada.

_____, de _____ de 20____.

(Local e Data)

(Nome e Assinatura do Representante Legal)

(Identificação Completa)

(Nº do RG do declarante)

ENCARTE E

Termo de Ciência e Declaração de Manutenção de Sigilo

Contrato n °:		
Objeto:		
Contratante:		
Gestor do Contrato:		Matrícula:
Contratada:		CNPJ:
Preposto da Contratada:		CPF:

Por este instrumento, os empregados da empresa contratada declaram ter ciência do Termo de Sigilo e Privacidade (**Encarte D**) e das normas de segurança vigentes na Contratante.

_____, de _____ de 20____.

(Local e Data)

CIÊNCIA.

CONTRATADA:

Funcionário:

Matrícula:

Funcionário:

Matrícula:

Funcionário:

Matrícula:

Funcionário:

Matrícula:

ENCARTE F

MODELO DE TERMO DE GARANTIA DO OBJETO

A empresa < inserir a razão social da empresa >, CNPJ nº. < inserir o nº do CNPJ da empresa >, DECLARA que cumprirá fielmente, desde a data da celebração do instrumento, todas as exigências contidas no Projeto Básico para a continuidade da prestação de Serviço de _____, relativas às obrigações decorrentes da garantia a ser prestada nos locais onde os mesmos forem instalados, que se encontram discriminados na Nota Fiscal nº. < inserir o número da NF >, e abaixo relacionados: < descrição básica dos equipamentos, com respectivos números de série>.

Nome do Representante Legal: _____

Cargo do Representante Legal: _____

Identificação do Representante Legal:

RG nº. _____,

CPF nº. _____.

Local e Data: _____, _____ de _____ de _____.

(Nome e Assinatura do Representante Legal)

(Identificação Completa)

(Nº do RG do declarante)

Observações: O prazo de garantia previsto no Projeto Básico é de 180 (cento e oitenta) dias para todos os equipamentos.

ENCARTE G

MODELO DE CARTA DE FIANÇA BANCÁRIA PARA GARANTIA DE EXECUÇÃO CONTRATUAL

1 - Pela presente, o (a) (nome da instituição fiadora) com sede em (endereço completo), por seus representantes legais infra-assinados, declara que se responsabiliza como FIADOR e principal pagador, com expressa renúncia dos benefícios estatuídos no artigo 827, do Código Civil Brasileiro, da empresa (nome da empresa), com sede em (endereço completo), até o limite de R\$ (valor da garantia) (valor por escrito) para efeito de garantia à execução do Contrato nº (número do contrato, formato xx/ano), decorrente do processo licitatório (modalidade e número do instrumento convocatório da licitação – ex.: Pregão Eletrônico nº xx/ano), firmado entre a AFIANÇADA e a Empresa Brasil de Comunicação S/A - EBC para (objeto da licitação).

2 - A fiança ora concedida visa garantir o cumprimento, por parte de nossa AFIANÇADA, de todas as obrigações estipuladas no contrato retromencionado, abrangendo o pagamento de:

- a) prejuízos advindos do não cumprimento do contrato;
- b) multas punitivas aplicadas pela EBC a Contratada;
- c) prejuízos diretos causados à EBC pela Contratada decorrentes de culpa ou dolo durante a execução do contrato; e
- d) obrigações previdenciárias e/ou trabalhistas e FGTS não honradas pela Contratada.

3 - Esta fiança é válida por (prazo, contado em dias, correspondente à vigência do contrato) (valor por escrito) dias, contados a partir de (data de início da vigência do contrato), vencendo-se, portanto, em (data).

4 - Na hipótese de inadimplemento de qualquer das obrigações assumidas pela AFIANÇADA, o (a) (nome da instituição fiadora) efetuará o pagamento das importâncias que forem devidas, no âmbito e por efeito da presente fiança, até o limite acima estipulado, no prazo de 48 (quarenta e oito) horas, contado do recebimento de comunicação escrita da EBC.

5 - A comunicação de inadimplemento deverá ocorrer até o prazo máximo de 90 (noventa) dias após o vencimento desta fiança.

6 - Nenhuma objeção ou oposição da nossa AFIANÇADA será admitida ou invocada por este FIADOR com o fim de escusar-se do cumprimento da obrigação assumida neste ato e por este instrumento perante a EBC.

7 - Obriga-se este FIADOR, outrossim, pelo pagamento de quaisquer despesas judiciais e/ou extrajudiciais, bem assim por honorários advocatícios, na hipótese de a EBC se ver compelida a ingressar em juízo para demandar o cumprimento da obrigação a que se refere a presente fiança.

8 - Se, no prazo máximo de 90 (noventa) dias após a data de vencimento desta fiança, o (a) (nome da instituição fiadora) não tiver recebido da EBC qualquer comunicação relativa a inadimplemento da AFIANÇADA, ou termo circunstanciado de que a AFIANÇADA cumpriu todas as cláusulas do contrato, acompanhado do original desta Carta de Fiança, esta fiança será automaticamente extinta, independentemente de qualquer formalidade, aviso, notificação judicial ou extrajudicial, deixando, em consequência, de produzir qualquer efeito e ficando o FIADOR exonerado da obrigação assumida por força deste documento.

9 - Declara, ainda, este FIADOR, que a presente fiança está devidamente contabilizada e que satisfaz às determinações do Banco Central do Brasil e aos preceitos da legislação bancária aplicáveis e, que, os signatários deste Instrumento estão autorizados a prestar a presente fiança.

10 - Declara, finalmente, que está autorizado pelo Banco Central do Brasil a expedir Carta de Fiança e que o valor da presente se contém dentro dos limites que lhe são autorizados pela referida entidade federal.

(Local e data)

(Instituição garantidora)

(Assinaturas autorizadas)



Documento assinado eletronicamente por **Hailton Lopes da Silva, Gerente-Executivo**, em 29/09/2026, às 17:57, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Antonio Valter Martins, Coordenador(a) III**, em 29/09/2026, às 18:06, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Danilo Lima Costa, Coordenador II**, em 29/09/2026, às 18:07, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Cintia De Moraes, Coordenador(a) III**, em 29/09/2026, às 20:04, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Braulio Costa Ribeiro, Diretor(a) de Operações, Engenharia e Tecnologia**, em 29/09/2026, às 21:01, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.ebc.com.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0342858** e o código CRC **89F4C038**.

Setor Comercial Sul - SCS Quadra 08, Bloco B-50/60, 1º Subsolo, Edifício Venâncio 2000 - Bairro Asa Sul, Brasília/DF - CEP 70333-900 - www.ebc.com.br

Processo nº 53400-011111/2026-42

SEI nº 0342858