MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

CONTRATO

CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE, ENTRE SI, CELEBRAM O MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA E A EMPRESA TLD TELEDATA COMERCIO E SERVICOS LTDA, NA FORMA ABAIXO:

CONTRATO Nº 190/2023 – SGA

O **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, pessoa jurídica de direito público, com sede na 5ª Avenida, 750, Centro Administrativo da Bahia, inscrita no CNPJ sob o Nº 04.142.491/0001-66, doravante denominado **CONTRATANTE,** neste ato representado, mediante Ato de Delegação nº 70/2014, pelo seu Superintendente de Gestão Administrativa, **André Luis Sant´Ana Ribeiro**, e a **TLD TELEDATA COMERCIO E SERVICOS LTDA** , CNPJ nº **33.927.849/0001-64**, doravante denominada **CONTRATADA**, estabelecida à Rua Sd. Luiz Gonzaga das Virgens, 111 – Edf. Liz Corporate, 4º andar, sala 402 – Caminho das Árvores, Cep: 41.820-560, Salvador – BA, representada por seu sócio, Sr. **Ricardo Luiz de Oliveira**, CPF/MF nº. 68******00, **CELEBRAM** o presente Contrato, com supedâneo no quanto disposto na Lei Estadual-BA nº 9.433/2005, e, ainda, observado o constante no Edital de Licitação do tipo menor preço, modalidade **Pregão Eletrônico nº 048/2023**, protocolado sob o nº 19.09.00843.0007700/2023-04, o qual integra este instrumento independentemente de transcrição, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 Constitui objeto do presente contrato de prestação de serviços de locação de equipamentos de Segurança da Informação, sob demanda, englobando o fornecimento de todo o hardware, software, subscrições, instalação, configuração, suporte técnico, treinamento, reposição de peças conforme especificações constantes no Termo de Referência e neste instrumento contratual.

1.2 Incluem-se no objeto contratado todos os custos com necessários à plena execução dos serviços contratados, tais como, todos os custos relativos a remunerações, encargos sociais, previdenciários e trabalhistas de todo o pessoal designado pela **CONTRATADA** para a execução do objeto, transportes de qualquer natureza, deslocamento, depreciação, aluguéis, administração, tributos e emolumentos.

CLÁUSULA SEGUNDA – DA FORMA DE FORNECIMENTO, DA ENTREGA E DO RECEBIMENTO

2.1 O Regime de execução do presente contrato é de Execução Indireta na modalidade empreitada por preço unitário.

2.2 A **CONTRATADA** deverá retirar a nota de empenho no prazo de 05 (cinco) dias, contados da data da convocação do **CONTRATANTE**;

2.2.1 As comprovações da convocação e da entrega/retirada da nota de empenho poderão ocorrer por quaisquer dos seguintes meios: por meio eletrônico (através de confirmação de recebimento de e-mail), aposição de assinatura (para retirada presencial) ou por Aviso de Recebimento dos correios (quando a entrega for via postal).

2.2.2 O Fornecedor poderá solicitar a prorrogação do prazo para retirada/recebimento da nota de empenho, por igual período ao original, por motivo justo e aceito pela Administração, nos termos do art. 124, § 4º, da Lei Estadual – BA nº 9433/2005.

2.3 As entregas, serviços de instalação, suporte técnico e manutenção serão executados em qualquer uma das unidades do Ministério Público do Estado da Bahia já existentes, conforme relacionadas no **Apenso I deste instrumento**, bem como em qualquer outra nova a ser criada futuramente dentro dos limites do Estado da Bahia e os eventuais limites de acréscimos e supressões contratuais.

2.3.1 A execução do serviço deverá ser agendada previamente junto à **Diretoria de Tecnologia da Informação** do **CONTRATANTE**, por meio da sua Coordenação de Assessoramento em Segurança da Informação - CASI, por meio do telefone 071-3103-0214 e/ou do e-mail casi@mpba.mp.br, e deverá ocorrer em dias úteis entre as 09:00h e as 17:00h;

2.4 A **CONTRATADA** deve realizar a entrega, instalação e todas as configurações dos equipamentos em até 90 (noventa) dias, contados da data de publicação do Contrato, iniciando neste momento a prestação dos serviços objetos desta contratação;

2.5 A **CONTRATADA** deverá realizar a instalação e configuração das Soluções de Segurança da Informação com subscrições do fabricante pelo período de 60 (sessenta) meses e prestação dos serviços, incluindo manutenção corretiva, preventiva, atendimento on-site de acordo com os demais itens deste Termo de Referência, uma equipe com perfil técnico adequado às atividades previstas, com técnicos treinados pelo fabricante para a operação e configuração de todos os componentes ofertados;

2.6 A execução do serviço será realizada sob demanda da **CONTRATANTE** de acordo com a necessidade institucional. Sempre que houver necessidade, a **CONTRATANTE** encaminhará à **CONTRATADA** um empenho estimativo acompanhado de uma ordem de serviço contendo a relação de localidades que deverão ser atendidas nos prazos de 90 (noventa) dias, podendo contemplar a quantidade de uma ou mais das localidades previstas para cada lote.

2.6.1 As comunicações formais entre a **CONTRATADA** e o **CONTRATANTE** deverão ocorrer através de e-mail, cujos endereços devem ser previamente informados pelas partes.

2.7 A execução dos serviços deverá observar, ainda:

2.7.1 A **CONTRATADA** deverá cumprir com todas as exigências técnicas e funcionais relacionadas com a solução ofertada, que devem ser implantadas durante o período contratado, sem ônus para o **CONTRATANTE**;

2.7.2 O serviço de instalação consiste na acomodação física, incluindo *patch cord* e configuração lógica dos equipamentos que compõe a solução;

2.7.3 Caberá à **CONTRATADA** a disponibilização de todos os recursos necessários, como hardware, software e recursos humanos necessários à execução dessa atividade;

2.7.4 O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção individual, bem como materiais complementares estritamente necessários à instalação ou à assistência técnica é de inteira responsabilidade da **CONTRATADA** e não deverá gerar ônus ao **CONTRATANTE**;

2.7.5 No tocante a equipamentos, periféricos, acessórios, técnicos de instalação, técnicos de manutenção, translado, transporte, estada, embalagens, necessários à execução da instalação e assistência técnica deverão ser de responsabilidade da **CONTRATADA** e não deverão gerar qualquer ônus ao **CONTRATANTE**;

2.7.6 No processo de instalação o Responsável Técnico deverá tomar todas as medidas necessárias visando garantir a perfeita execução do serviço (instalação e configuração).

2.7.7 A solução de segurança distribuída das unidades remotas, devem ser registradas na solução de Gerenciamento de Dispositivos que será instalado no Data Center do **CONTRATANTE**, sendo essa configuração inicial realizada pela **CONTRATADA** com base nas informações fornecidas pelo MPBA.

2.7.8 Homologação da instalação:

2.7.8.1 No prazo de até 10 (dez) dias uteis após a conclusão de instalação da solução ofertada, a **CONTRATADA** deverá fornecer documentação final contendo as configurações e topologias de como foram instalados os equipamentos;

2.7.8.2 A documentação deverá ser aprovada pelo **CONTRATANTE** através do seu fiscal técnico, caracterizando a homologação da solução;

2.7.9 Serviço de Manutenção: A manutenção visa manter em perfeito estado de operação os serviços e equipamentos fornecidos em atendimento ao objeto, deste modo a **CONTRATADA** deve cumprir os seguintes procedimentos:

2.7.9.1 Do *hardware*: desinstalação, reconfiguração ou reinstalação decorrentes de falhas no *hardware*, fornecimento de peças de reposição, substituição de *hardware*, atualização da versão de drivers, *firmwares* e *software* básico, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas especificas para os recursos utilizados;

2.7.9.2 Do *software* (aplicativos e sistema operacional): desinstalação, reconfiguração ou reinstalação decorrentes de falhas no *software*, atualização da versão de *software*, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas especificas para os recursos utilizados;

2.7.9.3 Quanto as atualizações pertinentes aos *softwares*, entende-se como "atualização" o provimento de toda e qualquer evolução de *software*, incluindo correções, "*patches*", "*fixes*", "*updates*", "*service packs*", novas "*releases*", "versões", "*builds*", englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de vigência contratual;

2.7.9.4 Os chamados de suporte deverão ser abertos diretamente na **CONTRATADA**, gerenciados pelo mesmo, através de número telefônico 0800 ou equivalente a ligação local e também por ambiente *WEB*, fornecendo, neste momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos prazos estabelecidos;
2.7.9.5 A **CONTRATADA** deve disponibilizar acesso ao ambiente *WEB* do fabricante para *download* de arquivos e *drivers*;

2.7.9.6 Todo serviço de suporte deve ser realizado por profissional certificado pelo fabricante;

2.7.9.7 O serviço de suporte deve proporcionar a interação com a equipe técnica do **CONTRATANTE**, fornecendo apoio na resolução de incidentes que envolvam os componentes da oferta, garantindo seu pronto reestabelecimento.

2.7.10 Operação da solução: A operação e administração dos equipamentos serão realizadas pela equipe de técnica do **CONTRATANTE**, quando necessário será solicitado a **CONTRATADA** suporte durante toda vigência contratual;

2.7.11 Exigências técnicas e operacionais:

2.7.11.1 A **CONTRATADA** deve prever os seguintes Níveis de Serviços para garantia e suporte:

NÍVEL	DESCRIÇÃO
1	Serviços indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação dos serviços.
3	Serviços disponíveis com ocorrência de falhas ou alertas. Dúvidas geral sobre equipamentos
4	Requisições de Serviços

2.7.11.2 Nível de Serviço Capital para item Solução De Segurança Cibernética – NGFW TIPO "A" e "B".

SLA CAPITAL					
Tipo	Prazo	Nível de severidade			
		1	2	3	4
On-site	Tempo de Solução	2 horas	4 horas	x	8 horas
Remoto	Tempo de Solução	1 hora	2 horas	8 horas	6 horas
Troca de Hardware	Tempo de Solução	24 horas	24 horas	X	X

2.7.11.3 Nível de Serviço Regionais para item Solução De Segurança Cibernética – NGFW TIPO “C” e “D”:

SLA REGIONAIS					
Tipo	**Prazo**	**Nível de severidade**			
		1	2	3	4
On-site	Tempo de Solução	4 horas	6 horas	x	12 horas
Remoto	Tempo de Solução	2 horas	4 horas	12 horas	8 horas
Troca de Hardware	Tempo de Solução	24 horas	48 horas	X	X

2.7.11.4 A **CONTRATADA** deve disponibilizar ao **CONTRATANTE** o serviço de um fiscal responsável pelo Contrato de Garantia e Suporte. Este deve ser o ponto focal de todas as necessidades de suporte do **CONTRATANTE** para casos de escalonamentos ou problemas de atendimento do Suporte Técnico;

2.7.11.5 A **CONTRATADA** deve fornecer documentação comprobatória das características solicitadas, conforme especificação técnica detalhada, independente da sua descrição, através de documentos cuja origem seja exclusivamente do fabricante dos produtos, como catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante através da internet, indicando as respectivas URL's (*Uniform Resource Locator*).

2.7.11.6 Todos os componentes e acessórios deverão ser entregues instalados e funcionando perfeitamente;

2.7.11.7 Os serviços de instalação e manutenção não deverão obstruir o andamento das rotinas de trabalho dos ambientes objetos de intervenção. Quando da intervenção nestes ambientes, será de responsabilidade da **CONTRATADA**, a recomposição total dos mesmos, deixando os locais totalmente limpos e arrumados, inclusive com relação a algum dano a eles causado quando da execução dos serviços;

2.7.11.8 Quando da execução dos serviços, os locais de trabalho deverão ser mantidos desobstruídos e bemsinalizados, quando for o caso, de maneira a não comprometer a segurança daqueles que ali trafegam;

2.7.11.9 Após a execução dos serviços, as áreas deverão ser mantidas limpas, retirando-se toda e qualquer impureza e sobras de materiais;

2.7.11.10 Para facilitar os procedimentos do **CONTRATANTE**, a **CONTRATADA** deve apresentar planilhas específicas, para cada local que foi objeto de intervenção, constando relação detalhada dos produtos efetivamente instalados, dos desempenhos esperados e especificação dos procedimentos técnicos e, se couber, dos instrumentos usualmente adotados para se efetuar os testes.

2.7.12 Treinamento:

2.7.12.1 Caberá à **CONTRATADA** prover todos os recursos didáticos necessários à realização do treinamento em modelo *HANDS-ON*;

2.7.12.2 Deverá ser fornecido treinamento na solução adquirida de no mínimo 20 horas, para até 04 (quatro) pessoas, designadas pela **CONTRATANTE**, em até 10 (dez) dias após o término da instalação, a fim de repassar as informações necessárias dos produtos adquiridos, incluindo detalhamento do produto e seus aspectos gerais de configuração e operação com instrutor certificado pela fabricante dos produtos para realizar os treinamentos, comprovando mediante apresentação de certificado expedito pela **CONTRATADA** da solução;

2.7.12.3 O treinamento deverá cobrir conhecimentos necessários para administração, configuração, gerência, otimização, resolução de problemas e utilização da solução;

2.8 As Soluções de Segurança da Informação do presente instrumento devem possuir total compatibilidade entre si, objetivando garantir a completa conectividade e interoperabilidade resultando no perfeito funcionamento do conjunto, com níveis de desempenho adequados aos fins a que se destinam no contexto de melhorias nos Serviços de TIC do **CONTRATANTE**;

2.9 Correrá por conta exclusiva da **CONTRATADA** a responsabilidade por todas as despesas de instalação, suporte técnico remoto e local bem como deslocamento dos seus técnicos ao local da instalação e manutenção dos equipamentos, seja para retirada e/ou entrega, incluindo todas as despesas de transporte, frete e seguro correspondentes;

2.10 Caso a **CONTRATADA** necessite fornecer *hardwares* e/ou *softwares* adicionais não especificados nominalmente neste Termo de Referência, mas necessários para atender as funcionalidades exigidas, o custo desses deverão estar inseridos no preço total ofertado;

2.11 Todos os componentes e subcomponentes objetos deste instrumento deverão ser novos, de primeiro uso, sem previsão de descontinuidade anunciada, com tecnologia atualizada e avançada, em linha de produção atendendo às características técnicas presentes nos anexos deste instrumento e do Edital do certame que lhe dá fundamento.

2.12 O recebimento do objeto contratual ficará sob a responsabilidade do(a) fiscal do contrato (responsável pela habilitação para pagamentos) e observará o seguinte:

2.12.1 O recebimento provisório ocorrerá no prazo de até 05 (cinco) dias;

2.12.2 Para fins de recebimento provisório/definitivo, não se reputará como válido o recebimento dado pelo **CONTRATANTE** em fatura (ou documento afim) apresentada por transportadora a serviço da **CONTRATADA**;

2.11 O **CONTRATANTE** rejeitará, no todo ou em parte, o objeto contratual em desacordo com as condições pactuadas (tais como bens ou serviços em dissonância com as especificações e exigências contratuais/editalícias, com vícios ou defeitos de fabricação, com prejuízo ao perfeito funcionamento ou com danos nas embalagens que possam comprometer a qualidade do conteúdo), podendo, entretanto, se lhe convier, decidir pelo recebimento, neste caso com as deduções cabíveis;

2.12 O recebimento definitivo do objeto deste contrato se dará no prazo de 10 (dez) dias, e só será concretizado depois de adotados, pelo **CONTRATANTE**, todos os procedimentos contidos no Ato Normativo nº 007/2005 e na Instrução Normativa nº 006/2012, respeitadas as exigências contidas do art. 161 da Lei Estadual- BA nº 9.433/2005;

2.12.1 O recebimento ocorrerá também em conjunto com a Comissão de Recebimento de Obras, Bens, Materiais e Serviços do **CONTRATANTE**, designada pela Portaria nº 047/2021-SGA – ou por instrumento que eventualmente a substitua, caso o valor do objeto contratual seja superior ao limite estabelecido para a modalidade de convite, nos termos do art. 161, §4º, da Lei Estadual/BA nº 9.433/2005;

2.13 O aceite ou aprovação do objeto pelo **CONTRATANTE** não exclui a responsabilidade da **CONTRATADA** por vícios, defeitos ou disparidades com as especificações estabelecidas neste Contrato e no processo de Licitação que o originou, verificadas posteriormente, garantindo-se ao **CONTRATANTE**, inclusive, as faculdades previstas na Lei Federal n.º 8.078/90 – Código de Defesa do Consumidor.

CLÁUSULA TERCEIRA - DA DOTAÇÃO ORÇAMENTÁRIA

As despesas para o pagamento deste contrato correrão por conta dos recursos da Dotação Orçamentária a seguir especificada:

Cód. Unidade Orçamentária/Gestora	Destinação de Recursos (Fonte)	Ação (P/A/OE)	Região	Natureza da Despesa
40.101.0021	100	2002	9900	33.90.40

CLÁUSULA QUARTA - DO PREÇO

4.1 Os preços unitários definidos para a prestação de serviços é o seguinte:

ITEM	DESCRIÇÃO	QUANTIDADE ESTIMADA	Valor unitário R$	Valor Mensal estimado	Valor Global estimado meses)
1	Solução de segurança cibernética – NGFW **TIPO A**	1	R$ 72.201,11	R$ 72.201,11	R$ 4.332.066,60
2	Solução de segurança cibernética – NGFW **TIPO B**	5	R$ 3.497,33	R$ 17.486,65	R$ 1.049.199,00
3	Solução De Segurança Cibernética – NGFW **TIPO C**	36	R$ 992,79	R$ 35.740,44	R$ 2.144.426,40
4	Solução De Segurança Cibernética – NGFW **TIPO D**	55	R$ 992,79	R$ 54.603,45	R$ 3.276.207,00
5	Unidade Centralizada de Armazenamento de Logs e Relatórios	01	R$ 26.866,70	R$ 26.866,70	R$ 1.612.002,00
6	Unidade Centralizada de Gerenciamento de Dispositivos	01	R$ 13.834,98	R$ 13.834,98	R$ 830.098,80

4.2 Dá-se ao presente contrato o valor anual estimado de **R$ 2.648.799,96 (dois milhões, seiscentos e quarenta e oito mil, setecentos e noventa e nove reais e noventa e oito centavos)**, e total (considerada a vigência total consignada na cláusula oitava) de **R$ 13.243.999,80 (treze milhões, duzentos e quarenta e três mil, novecentos e noventa e nove reais e oitenta centavos).**

4.2.1 O valor global estabelecido é meramente estimativo, não cabendo à **CONTRATADA**, portanto, quaisquer direitos de cobrança caso o montante estipulado no item anterior não seja atingido durante a vigência deste instrumento, porquanto o pagamento relativo ao fornecimento dos itens somente ocorrerá em razão da quantidade efetivamente instalada e aceita;

4.3 Nos preços computados neste Contrato estão inclusos todos e quaisquer custos necessários ao fiel cumprimento deste instrumento, inclusive todos aqueles relativos a remunerações, encargos sociais, previdenciários e trabalhistas de todo o pessoal disponibilizado pela **CONTRATADA** para a execução do objeto, entregas e transportes de qualquer natureza, alimentação, hospedagem, materiais empregados, inclusive ferramentas e fardamentos, depreciação, aluguéis, administração, tributos e emolumentos.

CLÁUSULA QUINTA – DOS ACRÉSCIMOS E SUPRESSÕES

5.1 A **CONTRATADA** se obriga a aceitar, quando solicitado e devidamente motivado pela Administração, nas mesmas condições estabelecidas neste instrumento, os acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, na forma do § 1º do art. 143 da Lei Estadual-BA nº 9.433/2005;

5.2 As supressões poderão ser superiores a 25% (vinte e cinco por cento), desde que haja resultado de acordo entre os contratantes.

CLÁUSULA SEXTA - DAS CONDIÇÕES DE PAGAMENTO E DA RETENÇÃO DE TRIBUTOS

6.1 O faturamento referente ao objeto deste contrato será efetuado **mensalmente, conforme quantitativo efetivamente demandados e aceitos pelo CONTRATANTE,** e os pagamentos serão processados mediante apresentação, pela **CONTRATADA**, de fatura, nota fiscal e certidões cabíveis, documentação que deverá estar devidamente acompanhada do **ACEITE** pelo **CONTRATANTE**, e se concluirá no prazo de 08 (oito) dias úteis a contar da data de apresentação da documentação, desde que não haja pendência a ser regularizada;

6.1.1 O faturamento será realizado conforme a quantidade de instalações efetivadas e postas em atividade, devidamente atestadas pela equipe técnica do **CONTRATANTE**.

6.1.2 Verificando-se qualquer pendência impeditiva do pagamento, será considerada data da apresentação da documentação aquela na qual foi realizada a respectiva regularização;

6.1.2.1 Eventuais erros na apresentação da nota fiscal/fatura, ou nos documentos pertinentes à contratação, ou, ainda, de circunstância que impeça a liquidação de despesa, como obrigações financeiras pendentes, decorrentes de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a **CONTRATADA** providencie as medidas saneadoras.

6.2 As faturas/notas fiscais far-se-ão acompanhar da documentação probatória relativa ao recolhimento dos tributos que tenham como fato gerador o objeto consignado na **CLÁUSULA PRIMEIRA**;

6.2.1 Na hipótese de subcontratação, não serão aceitas notas fiscais emitidas pelas empresas subcontratadas, devendo todo o faturamento ser realizado em nome da empresa **CONTRATADA**;

6.3 O **CONTRATANTE** realizará a retenção de impostos ou outras obrigações de natureza tributária, de acordo com a legislação vigente;

6.4 Os pagamentos serão efetuados através de ordem bancária, para crédito em conta corrente e agência indicadas pela empresa contratada, preferencialmente em banco de movimentação oficial de recursos do Estado da Bahia;

6.5 A atualização monetária dos pagamentos devidos pelo **CONTRATANTE**, em caso de mora, será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE *pro rata tempore,* observado, sempre, o disposto no item **6.1.2**.

6.5.1 Para efeito de caracterização de mora imputável **ao CONTRATANTE**, não serão considerados eventuais atrasos de pagamento no período de fechamento do exercício financeiro do Estado da Bahia, compreendido entre o final do mês de dezembro e o mês de janeiro do exercício subsequente, decorrentes de circunstâncias alheias à vontade das partes, isto é, por força de bloqueio de rotinas no sistema estadual obrigatoriamente utilizado para a execução dos pagamentos devidos **pelo CONTRATANTE**.

CLÁUSULA SÉTIMA – DA MANUTENÇÃO DAS CONDIÇÕES DA PROPOSTA, DO REAJUSTAMENTO E DA REVISÃO DE PREÇOS

7.1 A eventual concessão de reajustamento, nos termos do inc. XXV do art. 8º c/c artigo 144 e seguintes da Lei Estadual – BA nº 9.433/2005, fica condicionada à apresentação de requerimento formal pela **CONTRATADA**, após o transcurso do prazo de 12 (doze) meses, contados da data da apresentação da proposta;

7.1.1 Adotar-se-á o INPC/IBGE como índice oficial para o cálculo da variação de preços, tendo como referencial o acumulado de 12 (doze) meses, sendo o termo inicial o mês de apresentação da proposta e termo final o mês que antecede a data de aniversário, a saber:

7.1.1.1 Mês 1: dezembro/2023;

7.1.1.2 Mês 12: novembro/2024;

7.2 Serão objeto de reajuste apenas os valores relativos a parcelas de serviços empenhadas após o decurso do prazo de 12 (doze) meses, contados da apresentação da proposta, observando-se ainda que:

7.2.1 Reajustamentos subsequentes deverão observar o interregno mínimo de 12 (doze) meses, contados da data-base de aplicabilidade da concessão do último reajuste;

7.2.2 A variação do valor contratual para fazer face ao reajuste de preços não caracteriza alteração do mesmo, podendo ser registrada por simples apostila, dispensando a celebração de aditamento;

7.2.3 Quando, antes da data do reajustamento, tiver ocorrido revisão do contrato para manutenção do seu equilíbrio econômico-financeiro, exceto nas hipóteses de força maior, caso fortuito, agravação imprevista, fato da administração ou fato do príncipe, será a revisão considerada à ocasião do reajuste, para evitar acumulação injustificada;

7.3 A revisão de preços nos termos do inc. XXVI do art. 8º da Lei Estadual nº. 9.433/2005, por interesse da **CONTRATADA**, dependerá de requerimento formal, instruído com a documentação que comprove o desequilíbrio econômico-financeiro do Contrato. Deverá ser instaurada pelo **CONTRATANTE**, entretanto, quando este pretender recompor o preço que se tornou excessivo;

7.3.1 A revisão de preços, se ocorrer, deverá ser formalizada através de celebração de Aditivo Contratual.

CLÁUSULA OITAVA - DA VIGÊNCIA

A vigência do presente contrato será de 60 (sessenta) meses, contados a partir da data da publicação do seu resumo no Diário Eletrônico do Poder Judiciário do Estado da Bahia.

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA

9.1 Além das determinações contidas na **CLÁUSULA SEGUNDA** deste contrato e no processo de Licitação que o originou – que aqui se consideram literalmente transcritas, bem como daquelas decorrentes de lei, a **CONTRATADA**, obriga-se a:

9.2 Executar o objeto contratual de acordo com os prazos e as especificações técnicas constantes no instrumento convocatório e seus anexos, no local determinado, nos dias e nos turnos e horários de expediente do **CONTRATANTE**, não podendo eximirse da obrigação, ainda que parcialmente, sob a alegação de falhas, defeitos ou falta de pessoal, materiais e/ou peças;

9.3 Prestar diretamente o objeto contratado, não o transferindo a outrem, no todo ou em parte, ressalvando-se apenas os casos de cisão, fusão ou incorporação da empresa contratada, desde que não impeçam os compromissos assumidos para com o **CONTRATANTE**, admitindo-se a subcontratação, nos seguintes termos:

9.3.1 A **CONTRATADA** somente poderá subcontratar parte dos serviços objeto deste instrumento, **referentes aos serviços de instalação dos equipamentos e suporte técnico in loco dos mesmos**, hipótese em que será necessária a prévia e expressa aprovação pelo **CONTRATANTE**;

9.3.2 A subcontratação não exime a responsabilidade da **CONTRATADA**, observada a qualidade, a fidelidade ao objeto e a garantia sobre a totalidade dos serviços prestados, cabendo-lhe também a devida supervisão e coordenação dessas atividades. A empresa subcontratada deverá estar credenciada pelo fabricante da solução que irá compor a oferta, possuir sede ou filial no estado da Bahia e possuir equipe técnica própria certificada e credenciada. Nestes casos, a SUBCONTRATADA deverá comprovar capacidade técnica para executar a parcela do objeto que lhe será imputada, bem como comprovar o vínculo com o fabricante da solução;

9.4 Manter durante toda a execução da contratação, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no procedimento de licitação;

9.5 Providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes que, porventura, sejam necessários à execução da contratação;

9.6 Responsabilizar-se pelo cumprimento das exigências previstas na legislação profissional específica e pelos encargos fiscais e comerciais resultantes da execução da contratação;

9.6.1 A eventual retenção de tributos pelo **CONTRATANTE** não implicará na responsabilização deste, em hipótese alguma, por quaisquer penalidades ou gravames futuros, decorrentes de inadimplemento(s) de tributos pela empresa contratada;

9.7 Emitir notas fiscais/faturas de acordo com a legislação e com este documento, contendo descrição dos bens e serviços (quando couber), indicação de quantidades, preços unitários e valor total;

9.8 Arcar, quando da execução do objeto contratado, com todo e qualquer dano ou prejuízo, independentemente da natureza, causado ao **CONTRATANTE** e/ou a terceiros, ainda que por sua culpa, em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir ao **CONTRATANTE** todos os custos decorrentes de indevida paralisação ou interrupção dos serviços contratados;

9.9 Não introduzir, seja a que título for, nenhuma modificação na especificação do objeto contratado ou das eventuais normas técnicas a serem seguidas, sem o consentimento prévio, e por escrito, do **CONTRATANTE**;

9.10 Atender, nos prazos consignados neste instrumento e/ou pelo **CONTRATANTE**, às recusas ou determinações de desfazimento/refazimento fornecimentos e/ou serviços acessórios que não estejam sendo ou não tenham sido executados de acordo com as Normas Técnicas e/ou em conformidade com as condições do Edital (e anexos) constante no processo licitatório que o originou, providenciando sua imediata correção ou realização, sem ônus para o **CONTRATANTE**;

9.11 Zelar pela boa e completa execução contratual, permitindo e oferecendo condições para a mais ampla e completa fiscalização durante a vigência deste contrato, fornecendo informações, propiciando o acesso à documentação pertinente e à execução contratual, e atendendo às observações e exigências apresentadas pela fiscalização;

9.12 Manter sob sua exclusiva responsabilidade toda a supervisão e direção da eventual mão de obra necessária à execução completa e eficiente da contratação;

9.13 Comunicar formalmente ao **CONTRATANTE** qualquer anormalidade que interfira no bom andamento da execução da contratação;

9.14 Prestar todos os esclarecimentos que forem solicitados pelo **CONTRATANTE**.

9.15 Assegurar a correta integração e funcionalidade dos serviços, em função do projeto e das especificações técnicas constantes neste instrumento e no Edital de licitação que lhe deu fundamento;

9.16 Efetuar inspeção/vistoria do local onde ocorrerá a instalação dos equipamentos, conforme indicação do **CONTRATANTE**, para verificar os detalhes técnicos de execução;

9.17 Apresentar, ao final do serviço de instalação, o relatório de conclusão do projeto, contendo os seguintes documentos:

9.17.1 Memorial descritivo de todo o serviço e produtos utilizados;

9.17.2 Relação de garantias dos equipamentos e serviços;

9.18 Manter toda estrutura de pessoal e ferramental necessários para execução do contrato, incluindo, fornecimento e serviços, independentemente da demanda definida pela **CONTRATANTE**;

9.19 Responsabilizar-se por toda a logística (transporte e comunicação) necessária à execução do fornecimento e dos serviços propostos, em todo o Município de Salvador, para atendimento imediato às solicitações do **CONTRATANTE**, conforme a demanda;

9.20 Arcar com todas as despesas provenientes da limpeza dos locais de instalações e adequações necessárias;

9.21 Manter preposto para representá-la durante a execução dos serviços ora tratados, desde que aceito pelo **CONTRATANTE**;

9.22 Disponibilizar um profissional que acompanhará as ações junto ao **CONTRATANTE** para recebimento de Ordens de Serviço, informações, contato com os técnicos responsáveis pelos serviços, coordenação, administração e supervisão do seu pessoal, bem como de qualquer comunicação junto ao **CONTRATANTE**;

9.22.1 Cada prestador de serviços da **CONTRATADA** deverá se apresentar uniformizado, com fardamento padrão fornecido pela **CONTRATADA**, e portando crachá de identificação;

9.23 Não efetuar despesa, celebrar acordos, fazer declarações ou prestar informações em nome do **CONTRATANTE**;

9.24 Fazer a alusão ao termo de sigilo e confidencialidade, que todos os envolvidos precisam ter ciência e responder por.

9.25 A **CONTRATADA** se compromete em atender as disposições do temo de sigilo e confidencialidade, **Apenso II** deste instrumento, bem como garantir o seu entendimento a todos os envolvidos nesta contratação.

CLÁUSULA DÉCIMA - DAS OBRIGAÇÕES DO CONTRATANTE

10.1 **CONTRATANTE,** além das obrigações contidas neste contrato por determinação legal, obriga-se a:

10.2 Fornecer, no prazo de 10 (dez) dias a contar da data da assinatura do contrato, as informações necessárias para que a **CONTRATADA** possa executar plenamente o objeto contratado;

10.3 Realizar os pagamentos devidos pela execução do contrato, nos termos e condições previstos nas **CLÁUSULAS QUARTA E SEXTA**;

10.4 Permitir o acesso dos empregados autorizados da **CONTRATADA** às instalações físicas do **CONTRATANTE**, nos locais e na forma que se façam necessários para a execução do contrato;

10.5 Acompanhar e fiscalizar o fiel cumprimento dos prazos e das condições de realização do presente contrato, notificando a **CONTRATADA**, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução do objeto, para que sejam adotadas as medidas corretivas necessárias;

10.6 Fornecer à **CONTRATADA,** mediante solicitação, atestado de capacidade técnica, quando o fornecimento do objeto atender satisfatoriamente os prazos de entrega, qualidade e demais condições previstas neste Contrato.

CLÁUSULA DÉCIMA PRIMEIRA – DA FISCALIZAÇÃO CONTRATUAL

11.1 Na forma das disposições estabelecidas na Lei Estadual-BA nº 9.433/2005, o **CONTRATANTE** designará servidor(es), **por meio de Portaria específica para tal fim**, para a fiscalização deste contrato, tendo poderes, entre outros, para notificar a **CONTRATADA** sobre as irregularidades ou falhas que porventura venham a ser encontradas na execução deste instrumento;

11.2 Incumbe à fiscalização acompanhar e verificar a perfeita execução do contrato, em todas as suas fases, competindo-lhe, inclusive:

11.2.1 Acompanhar o cumprimento dos prazos de execução – a incluir tanto a entrega quanto a prestação de assistência técnica, e determinar as providências necessárias à correção de falhas, irregularidades e/ou defeitos, podendo ainda suspender a execução contratual, sem prejuízo das sanções contratuais legais;

11.2.2 Transmitir à **CONTRATADA** instruções, e comunicar alterações de prazos, cronogramas de execução e especificações do projeto, quando for o caso;

11.2.3 Promover a verificação da execução do objeto contratual, emitindo a competente habilitação para o recebimento de pagamentos;

11.2.4 Esclarecer prontamente as dúvidas da **CONTRATADA**, solicitando ao setor competente do **CONTRATANTE**, se necessário, parecer de especialistas;

11.3 A fiscalização, pelo **CONTRATANTE**, não desobriga a **CONTRATADA** de sua responsabilidade quanto à perfeita execução do objeto contratual;

11.3.1 A ausência de comunicação, por parte do **CONTRATANTE**, sobre irregularidades ou falhas, não exime a **CONTRATADA** das responsabilidades determinadas neste contrato.

11.4 O **CONTRATANTE** poderá recusar, sustar e/ou determinar a substituição de bens ou refazimento de serviços que não estejam sendo ou não tenham sido fornecidos ou executados de acordo com as Normas Técnicas e/ou em conformidade com as condições deste contrato ou do procedimento licitatório que o originou, ou ainda que atentem contra a segurança de terceiros ou de bens;

11.4.1 Qualquer bem ou serviço considerado não aceitável, no todo ou em parte, deverá ser refeito, reparado ou substituído pela **CONTRATADA**, às suas expensas;

11.4.2 A não aceitação de algum bem ou serviço, no todo ou em parte, não implicará na dilação do prazo de execução, salvo expressa concordância do **CONTRATANTE**.

11.5 O **CONTRATANTE** poderá determinar o afastamento momentâneo, de suas dependências ou do local da execução do contrato, de empregados ou prepostos da **CONTRATADA**, cuja permanência venha embaraçar ou dificultar a ação fiscalizadora;

11.6 Para fins de fiscalização, o **CONTRATANTE** poderá solicitar à **CONTRATADA**, a qualquer tempo, os documentos relacionados com a execução do presente contrato.

CLÁUSULA DÉCIMA SEGUNDA - DAS PENALIDADES

12.1 A **CONTRATADA** sujeitar-se-á às sanções administrativas previstas na Lei Estadual-BA nº. 9.433/2005, as quais poderão vir a ser aplicadas após o prévio e devido processo administrativo, assegurando-lhe, sempre, o contraditório e a ampla defesa.

12.2 Em caso de inadimplemento parcial ou total de obrigações pela **CONTRATADA**, e não sendo suas justificativas aceitas pelo **CONTRATANTE,** àquela poderão ser aplicadas, observado o disposto no item anterior, as seguintes penalidades: 12.2.1 Multa;

12.2.2 Suspensão temporária de participação em licitação e impedimento de contratar com a Administração pelo prazo de até 05 (cinco) anos;

12.2.3 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes desta punição e até que seja promovida sua reabilitação perante a Administração Pública Estadual;

12.2.4 Descredenciamento do sistema de registro cadastral.

12.3 Nas hipóteses de aplicação das sanções previstas nos **subitens 12.2.2 a 12.2.4**, estas serão impostas à **CONTRATADA** cumulativamente com multa.

12.4 A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará o **CONTRATADA** à multa de mora, que será graduada por infração e de acordo com a gravidade da infração, obedecidos os seguintes limites máximos:

12.4.1 Para hipótese de inexecução relacionada ao cumprimento de obrigação **principal**:

12.4.1.1 - 10% (dez por cento) sobre o valor da nota de empenho ou do Contrato, em caso de descumprimento total da obrigação;

12.4.1.2 - 0,3% (três décimos por cento) ao dia, até o 30º (trigésimo) dia de atraso, sobre o valor total da parte do serviço não realizado;

12.4.1.3 - 0,7% (sete décimos por cento) por cada dia de atraso subsequente ao 30º (trigésimo), sobre o valor da parte do serviço não realizado;

12.4.2 Para hipótese de inexecução relacionada ao cumprimento de obrigação **acessória**, assim consideradas aquelas que coadjuvam com a principal:

12.4.2.1 - 0,2% (dois décimos por cento) ao dia, até o 30º (trigésimo) dia de atraso, sobre o valor global do contrato;

12.4.2.2 - 0,6% (seis décimos por cento) por cada dia de atraso subsequente ao 30º (trigésimo), sobre o valor global do contrato;

12.4.2.3 - Para cada obrigação acessória descumprida, a aplicação dos percentuais definidos nos **subitens 12.4.2.1 e**

12.4.2.2, estará limitada ao montante global de 10% (dez por cento) do valor global do contrato;

12.5 A aplicação de multa à **CONTRATADA** não impede que a Administração rescinda unilateralmente o contrato e aplique as demais sanções previstas na Lei Estadual-BA nº 9.433/2005;

12.6 Quando aplicadas, as multas deverão ser pagas espontaneamente no prazo máximo de 05 (cinco) dias úteis, ou serem deduzidas do pagamento a ser efetuado pelo **CONTRATANTE**, caso este deva ocorrer dentro daquele prazo.

12.6.1 Na hipótese de ausência de adimplemento voluntário e impossibilidade de dedução, as multas poderão ser cobradas judicialmente, a critério do **CONTRATANTE**.

12.7 A aplicação de multas não tem caráter compensatório, e o seu pagamento não eximirá a **CONTRATADA** da responsabilidade por perdas e/ou danos decorrentes das infrações cometidas.

12.8 Os custos correspondentes a danos e/ou prejuízos causados por culpa ou dolo da **CONTRATADA** deverão ser ressarcidos ao **CONTRATANTE** no prazo máximo de 05 (cinco) dias úteis, contados da notificação administrativa, sob pena de, sem prejuízo do ressarcimento, serem considerados como hipótese de inadimplemento contratual, sujeita, portanto, à aplicação das sanções administrativas previstas nesta Cláusula.

CLÁUSULA DÉCIMA TERCEIRA – DA GARANTIA CONTRATUAL

13.1 A **CONTRATADA** deverá apresentar ao **CONTRATANTE**, no prazo máximo de 05 (cinco) dias contados da assinatura do contrato, garantia de 5% (cinco por cento) do valor do contrato, podendo optar por uma das modalidades previstas no parágrafo 1º do art. 136 da Lei Estadual nº 9.433/2005.

13.1.2 A ausência de apresentação da garantia e respectivo comprovante de quitação (conforme o caso) pela **CONTRATADA**, no prazo estipulado nesta cláusula, se configura como hipótese de pendência impeditiva do pagamento, nos termos da **CLÁUSULA SEXTA** deste instrumento, sem prejuízos das sanções contratuais e legais aplicáveis à matéria, em especial o artigo 167, incisos III e X da Lei Estadual/BA nº 9.433/2005;

13.2 A garantia, em qualquer das modalidades, responderá pelo inadimplemento das obrigações contratuais e pelas multas impostas, independentemente de outras cominações legais;

13.2.1 A **CONTRATADA** fica obrigada a, durante toda a vigência do contrato, reforçar o valor vigente da garantia sempre que esta for utilizada para o adimplemento de obrigações e/ou multas;

13.3 Caso haja a celebração de aditivo/apostilamento contratual que enseje acréscimo ao valor contratado, a **CONTRATADA** fica obrigada a complementar a garantia, em igual proporção, antes da consagração do aditamento/apostila;

13.3.1 Nos termos do art. 20 do Decreto Estadual nº 13.967/2012, na hipótese de a **CONTRATADA** se negar a efetuar o reforço da garantia, dentro de 10 (dez) dias contados da data de sua convocação, será aplicada multa no percentual de 2,5% (dois e meio por cento) incidente sobre o valor global do contrato;

13.4 A garantia, quando prestada nas modalidades seguro-garantia ou fiança bancária, deverá ser emitida por instituição devidamente habilitada/credenciada pelo Banco Central para tal mister, e contemplar todo o período de execução do contrato, desde o início de sua vigência até o exaurimento completo do período de 24 (vinte e quatro) meses de licenciamento/atualização contratado;

13.4.1 A garantia prestada em quaisquer das modalidades descritas neste item somente será aceita se contemplar todos os eventos indicados no item 13.6;

13.5 A garantia, quando prestada na modalidade caução, somente será restituída à **CONTRATADA**, no montante a que esta fizer jus, após a finalização total da execução do contrato, observadas as regras impeditivas de pagamento constantes na **CLÁUSULA OITAVA**;

13.5.1 A garantia, quando prestada em dinheiro, será atualizada monetariamente na oportunidade de sua devolução pelo **CONTRATANTE**, segundo critérios da instituição bancária onde se procedeu ao depósito;

13.6 A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

13.6.1 Prejuízos advindos do não cumprimento do objeto do contrato;

13.6.2 Prejuízos diretos causados ao **CONTRATANTE** decorrentes de culpa ou dolo durante a execução do contrato;

13.6.3 Multas moratórias e punitivas aplicadas pelo **CONTRATANTE** à **CONTRATADA**;

13.6.4 Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela **CONTRATADA**, quando couber;

CLÁUSULA DÉCIMA QUARTA - CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS - LEI N. 13.709/2018

14.1 É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, mantendo-se sigilo e confidencialidade, sob pena de responsabilização administrativa, civil e criminal;

14.2 A **CONTRATADA** declara que tem ciência da existência da Lei Geral de Proteção de Dados e se compromete a adequar todos os procedimentos internos ao disposto na legislação com o intuito de proteger os dados pessoais repassados pelo **CONTRATANTE**;

14.3 A **CONTRATADA** fica obrigada a comunicar ao Ministério Público do Estado da Bahia, em até 24 (vinte e quatro) horas do conhecimento, qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da LGPD;

14.4 A **CONTRATADA** cooperará com a **CONTRATANTE** no cumprimento das obrigações referentes ao exercício dos direitos dos titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e também no atendimento de requisições e determinações do Poder Judiciário, Ministério Público, ANPD e Órgãos de controle administrativo em geral;

14.5 Eventuais responsabilidades das partes serão apuradas conforme estabelecido neste contrato e também de acordo com o que dispõe a Seção III, Capítulo VI da LGPD.

CLÁUSULA DÉCIMA QUINTA- DA VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO

Integram o presente contrato, como se nele estivessem transcritas, as cláusulas e condições estabelecidas no edital constante no processo licitatório que o originou, referido no preâmbulo deste instrumento, bem como na proposta da **CONTRATADA** apresentada na referida licitação, naquilo em que não divirja deste instrumento.

CLÁUSULA DÉCIMA SEXTA – DA PUBLICIDADE

O **CONTRATANTE** será responsável pela publicação do resumo deste instrumento no Diário da Justiça Eletrônico (DJ-e), do Poder Judiciário do Estado da Bahia, no prazo de 10 (dez) dias corridos, contados a partir da sua assinatura.

CLÁUSULA DÉCIMA SÉTIMA - DO FORO

Fica eleito o Foro da Cidade do Salvador-Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas oriundas do presente Contrato.

CLÁUSULA DÉCIMA OITAVA- DAS DISPOSIÇÕES GERAIS

18.1 O **CONTRATANTE** não responderá por quaisquer compromissos assumidos perante terceiros pela **CONTRATADA,** ou seus prepostos, ainda que vinculados à execução do presente contrato;
18.2 A inadimplência da **CONTRATADA**, com relação a quaisquer custos, despesas, tributos, exigências ou encargos previstos neste contrato, não transfere ao **CONTRATANTE** a responsabilidade pelo seu pagamento, nem poderá onerar o objeto do contrato.

18.3 Aplicar-se-á a Lei Estadual nº 9.433/2005 para dirimir toda e qualquer questão legal relativa à execução deste contrato, em especial os casos omissos.

18.4 Fica assegurado ao **CONTRATANTE** o direito de alterar unilateralmente o contrato, mediante justificação expressa, nas hipóteses previstas no inciso I do art. 143 da Lei Estadual nº 9.433/2005, para melhor adequação às finalidades de interesse público, desde que mantido o equilíbrio econômico-financeiro original do contrato e respeitados os demais direitos da **CONTRATADA**.

18.5 Não caracterizam novação eventuais variações do valor contratual resultantes de reajustamento e/ou revisão de preços, de compensações financeiras decorrentes das condições de pagamento nele previstas ou, ainda, de alterações de valor em razão da aplicação de penalidades.

18.6 Inexistindo disposição específica, as obrigações contratuais devem ser praticadas no prazo de 05 (cinco) dias.

E, por assim estarem justos e contratados, firmam o presente Contrato para que produza seus efeitos legais, após a publicação na Imprensa Oficial.

Salvador, datado e assinado digitalmente/eletronicamente.

TLD TELEDATA COMERCIO E SERVICOS LTDA
Ricardo Luiz de Oliveira
Sócio-administrador

Ministério Público do Estado da Bahia
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

Documento assinado eletronicamente por **Ricardo Luiz de Oliveira** em 27/12/2023, às 15:06, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.

Documento assinado eletronicamente por **André Luis Sant Ana Ribeiro** em 12/01/2024, às 15:08, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0910687** e o código CRC **7DAD5844**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

CONTRATO

APENSO I

Especificações Técnicas Detalhadas

1. SOLUÇÃO DE SEGURANÇA CIBERNÉTICA – NGFW – TIPO A

1.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

1.2. A solução deverá ser composta por dois equipamentos independentes que deverão estar licenciados e funcionar em cluster de alta disponibilidade no modo ATIVO-ATIVO.

1.3. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 4U, no máximo.

1.4. Deverá possuir e estar licenciado durante a vigência contratual, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention, e Virtualização.

1.5. Deverá possuir fonte de alimentação com chaveamento automático 110/220V redundante Hot Swappable. A fonte fornecida deverá suportar sozinha a operação da unidade com todos os módulos de interface ativos.

1.6. Firewall com capacidade mínima de processamento de 45 (quarenta e cinco) Gbps.

1.7. IPS com capacidade mínima de processamento de 11,5 (onze e meio) Gbps.

1.8. Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 7 (sete) Gbps.

1.9. Inspeção SSL Throughput com capacidade mínima de processamento de 10 Gbps.

1.10. Deverá suportar, pelo menos, 9.500 (nove mil e quinhentos) usuários ativos na rede com todas as funcionalidades solicitadas neste Termo de Referência, habilitadas e funcionais.

1.11. VPN com capacidade de, pelo menos, 40 (quarenta) Gbps de tráfego IPSec.

1.12. VPN SSL com capacidade de, pelo menos, 8 (oito) Gbps de tráfego.

1.13. Deverá suportar 7.000.000 (sete milhões) conexões simultâneas.

1.14. Deverão ser licenciados para suportar, pelo menos, 9.000 (nove mil) usuários de VPN SSL.

1.15. Deverá suportar, pelo menos, 400.000 (quatrocentas mil) novas conexões por segundo.

1.16. Deverá suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Site-Site.

1.17. Deverá suportar, pelo menos, 60.000 (sessenta mil) túneis de VPN Client-Site.

1.18. Deverá possuir, pelo menos, 2 (duas) interfaces QSFP+ 40GE.

1.19. Deverá possuir, pelo menos, 2 (duas) interfaces SFP28 25GE.

1.20. Deverá possuir, pelo menos, 2 (duas) interfaces SFP+ 10GE.

1.21. Deverá possuir, pelo menos, 8 (oito) interfaces SFP 01GE.

1.22. Deverá possuir, pelo menos, 15 (quinze) interfaces RJ 45.

1.23. Deverá possuir porta USB 3.0 para conexão de modem 3G/4G.

1.24. Todos os equipamentos que acompanharem a solução deverão operar em modo de alta disponibilidade (cluster) e estar licenciados para operar desta forma.

1.25. Deverá possuir licença para número ilimitado de usuários e endereços IP.

1.26. Deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de UTP durante a vigência contratual.

1.27. Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários.

1.28. Deverá incluir licença para a funcionalidade de VPN SSL.

1.29. Deverá incluir licença para atualização de vacina de antivírus/anti-spyware.

1.30. Deverá incluir licença de atualização para filtro de conteúdo Web.

1.31. Deverá incluir licença de atualização do IPS e da lista de aplicações detectadas.

1.32. Deverá ser fornecida toda documentação técnica em formato digital, através de aceso a URL do fabricante, em português do Brasil ou em inglês.

2. SOLUÇÃO DE SEGURANÇA CIBERNÉTICA – NGFW – TIPO B

2.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

2.2. A solução deverá ser composta por dois equipamentos independentes que deverão estar licenciados e funcionar em cluster de alta disponibilidade no modo ATIVO-ATIVO.

2.3. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 4U, no máximo.

2.4. Deverá possuir e estar licenciado durante a vigência contratual, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL,
Controle de Aplicações, DLP – Data Leak Prevention, e Virtualização;

2.5. Deverá possuir fonte de alimentação com chaveamento automático 110/220V redundante. A fonte fornecida deverá suportar sozinha a operação da unidade com todos os módulos de interface ativos.

2.6. Deverá possuir firewall com capacidade mínima de processamento de 10 (dez) Gbps.

2.7. Deverá possuir IPS com capacidade mínima de processamento de 2 (dois) Gbps.

2.8. Deverá possuir Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1 (um) Gbps.

2.9. Deverá possuir Inspeção SSL Throughput com capacidade mínima de processamento de 1 (um) Gbps.

2.10. Deverá possuir VPN com capacidade de, pelo menos, 10 (dez) Gbps de tráfego IPSec.

2.11. Deverá suportar 1.300.000 (um milhão e trezentas mil) conexões simultâneas.

2.12. Deverão ser licenciados para suportar, pelo menos, 400 (quatrocentos) usuários de VPN SSL.

2.13. Deverá suportar, pelo menos, 50.000 (cinquenta mil) novas conexões por segundo.

2.14. Deverá suportar, pelo menos, 1.000 (um mil) túneis de VPN Site-Site.

2.15. Deverá suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Client-Site.

2.16. Deverá possuir, pelo menos, 2 (duas) interfaces SFP+ 10GE.

2.17. Deverá possuir, pelo menos, 6 (seis) interfaces SFP 01GE.

2.18. Deverá possuir, pelo menos, 14 (quatorze) interfaces RJ 45.

2.19. Todos os equipamentos que acompanharem a solução devem suportar operar em modo de alta disponibilidade e estar licenciados para operar desta forma.

2.20. Deverá possuir licença para número ilimitado de usuários e endereços IP.

2.21. Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários.
2.22. Deverá incluir licença para a funcionalidade de VPN SSL.

2.23. Deverá ser compatível e Gerenciado pelo item “Unidade Centralizada de Gerenciamento de Dispositivos”.

2.24. Deverá ser compatível com o item “Unidade Centralizada de Armazenamento de Logs e Relatórios”.

2.25. Deverá ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

3. SOLUÇÃO DE SEGURANÇA CIBERNÉTICA – NGFW – TIPO C

3.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

3.2. A solução deverá ser composta por dois equipamentos independentes que deverão estar licenciados e funcionar em cluster de alta disponibilidade no modo ATIVO-ATIVO.

3.3. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 4U, no máximo. 3.4. Deverá possuir e estar licenciado durante a vigência contratual, minimamente com as seguintes funcionalidades: Firewall,
Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention, e Virtualização;

3.5. Deverá possuir firewall com capacidade mínima de processamento de 5 (cinco) Gbps.

3.6 Deverá possuir IPS com capacidade mínima de processamento de 1 (um) Gbps.

3.7. Deverá possuir Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 650 (seiscentos e cinquenta) Mbps.

3.8. Deverá possuir Inspeção SSL Throughput com capacidade mínima de processamento de 600(seiscentos) Mbps.

3.9. Deverá possuir VPN com capacidade de, pelo menos, 6 (seis) Gbps de tráfego IPSec.

3.10. Deverá possuir VPN SSL com capacidade de, pelo menos, 800 (oitocentos) Mbps de tráfego.

3.11. Deverá suportar 600.000 (seiscentos mil) conexões simultâneas.

3.12. Deverão ser licenciados para suportar, pelo menos, 200 (duzentos) usuários de VPN SSL.

3.13. Deverá suportar, pelo menos, 30.000 (trinta mil) novas conexões por segundo.

3.14. Deverá suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.

3.15. Deverá suportar, pelo menos, 400 (quatrocentos) túneis de VPN Client-Site.

3.16. Deverá possuir, pelo menos, 10 (dez) interfaces RJ 45.

3.17. Deverá possuir porta USB para conexão de modem 3G/4G.

3.18. Todos os equipamentos que acompanharem a solução deverão suportar operação em modo de alta disponibilidade e estar licenciados para operar desta forma.

3.19. Deverá possuir licença para número ilimitado de usuários e endereços IP.

3.20. Deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de UTP durante a vigência contratual.

3.21. Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários.

3.22. Deverá incluir licença para a funcionalidade de VPN SSL;

3.23. Deverá incluir licença para atualização de vacina de antivírus/anti-spyware.

3.24. Deverá incluir licença de atualização para filtro de conteúdo Web.

3.25. Deverá incluir licença de atualização do IPS e da lista de aplicações detectadas.

3.26. Deverá ser compatível e Gerenciado pelo item “Unidade Centralizada de Gerenciamento de Dispositivos”.

3.27. Deverá ser compatível com o item “Unidade Centralizada de Armazenamento de Logs e Relatórios”.

3.28. Deverá ser fornecida toda documentação técnica em formato digital, através de aceso a URL oficial do fabricante, bem como manual de utilização, em português do Brasil ou em inglês.

4. SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA - NGFW – TIPO D

4.1. Solução baseada em *appliance*. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

4.2. Deverá possuir e estar licenciado durante a vigência contratual, minimamente com as seguintes funcionalidades: Firewall,
Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention, e Virtualização;

4.3. Deverá possuir firewall com capacidade mínima de processamento de 5 (cinco) Gbps.

4.4. Deverá possuir IPS com capacidade mínima de processamento de 1 (um) Gbps.
4.5. Deverá possuir Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 650 (seiscentos e cinquenta) Mbps.

4.6. Deverá possuir Inspeção SSL Throughput com capacidade mínima de processamento de 600(seiscentos) Mbps.

4.7. Deverá possuir VPN com capacidade de, pelo menos, 6 (seis) Gbps de tráfego IPSec.

4.8. Deverá possuir VPN SSL com capacidade de, pelo menos, 800 (oitocentos) Mbps de tráfego.

4.4. Deverá suportar 600.000 (seiscentos mil) conexões simultâneas.

4.10. Deverão ser licenciados para suportar, pelo menos, 200 (duzentos) usuários de VPN SSL.

4.11. Deverá suportar, pelo menos, 30.000 (trinta mil) novas conexões por segundo.

4.12. Deverá suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.

4.13. Deverá suportar, pelo menos, 400 (quatrocentos) túneis de VPN Client-Site.

4.14. Deverá possuir, pelo menos, 10 (dez) interfaces RJ 45.

4.15. Deverá possuir porta USB para conexão de modem 3G/4G.

4.16. Todos os equipamentos que acompanharem a solução deverão suportar operação em modo de alta disponibilidade e estar licenciados para operar desta forma.

4.17. Deverá possuir licença para número ilimitado de usuários e endereços IP.

4.18. Deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de UTP durante a vigência contratual.

4.19. Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários.

4.20. Deverá incluir licença para a funcionalidade de VPN SSL;

4.21. Deverá incluir licença para atualização de vacina de antivírus/anti-spyware;

4.22. Deverá incluir licença de atualização para filtro de conteúdo Web.

4.23. Deverá incluir licença de atualização do IPS e da lista de aplicações detectadas.

4.24. Deverá ser compatível e Gerenciado pelo item “Unidade Centralizada de Gerenciamento de Dispositivos”.

4.25. Deverá ser compatível com o item “Unidade Centralizada de Armazenamento de Logs e Relatórios”.

4.26. Deverá ser fornecida toda documentação técnica em formato digital, através de acesso a URL do fabricante, bem como manual de utilização, em português do Brasil ou em inglês.

5. CERTIFICAÇÕES NECESSÁRIAS PARA OS NGFW´S:

5.1. Certificação ICSA e/ou Common Criteria para Firewall;

5.2. Certificação ICSA e/ou Common Criteria para Anti-Malware;

5.3. Certificação ICSA e/ou Common Criteria para VPN SSL;

5.4. Certificação ICSA e/ou Common Criteria para VPN IPSec;

5.5. Certificação ICSA e/ou Common Criteria para IPS;

5.6. O equipamento de firewall e/ou IPS deverá ter sido aprovado nos testes da NSS Labs e deverá estar na lista de recomendados.

6. FUNCIONALIDADE DE FIREWALL

6.1. Deverá possuir controle de acesso à internet por endereço IP de origem e destino;

6.2. Deverá possuir controle de acesso à internet por sub rede;

6.3. Deverá suportar tags de VLAN (802.1q);

6.4. Deverá possuir ferramenta de diagnóstico do tipo tcpdump;

6.5. Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

6.6. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

6.7. Deverá suportar single-sign-on para Active Directory, RADIUS;

6.8. Deverá possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

6.9. Deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

6.10. Deverá permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

6.11. Deverá permitir controle de acesso à Internet por domínio, por exemplo: gov.br, org.br, edu.br;

6.12. Deverá possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

6.13. Deverá suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

6.14. Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;

6.15. Deverá suportar aplicações multimídia, como: H.323 e SIP;

6.16. Deverá possuir tecnologia de firewall do tipo Statefull;

6.17. Deverá suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

6.18. Deverá permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;

6.19. Deverá suportar PBR – Policy Based Routing;

6.20.Deverá permitir a criação de VLANS no padrão IEEE 802.1q;

6. 21.Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

6.22. Deverá permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;

6.23. Deverá permitir forwarding de camada 2 para protocolos não IP;

6.24. Deverá suportar forwarding multicast;

6.25. Deverá suportar roteamento multicast PIM Sparse Mode ou Dense Mode;

6.26. Deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

6.27. Deverá permitir o agrupamento de serviços;

6.28. Deverá permitir o filtro de pacotes sem a utilização de NAT;

6.29. Deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

6.30. Deverá possuir mecanismo de anti-spoofing;

6.31. Deverá permitir criação de regras definidas pelo usuário;

6.32. Deverá permitir o serviço de autenticação para tráfego HTTP e FTP;

6.33. Deverá permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

6.34. Deverá possuir a funcionalidade de balanceamento e contingência de links;

6.35. Deverá suportar sFlow;

6.36. O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas";

6.37. Deverá ter a capacidade de permitir a criação de regras de firewall específicas para tipos de dispositivos identificados automaticamente (funcionalidade está conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows;

6.38. Deverá ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

6.39. Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

6.40. Deverá permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

6.41. Deverá suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;

6.42. Deverá permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;

6.43. Deverá possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

6.44. Deverá suportar SIP, H.323 e SCCP NAT Traversal;

6.45. Deverá permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;

6.46. Deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

7. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

7.1. Deverá permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

7.2. Deverá permitir modificação de valores DSCP para o DiffServ;

7.3. Deverá permitir priorização de tráfego e suportar ToS;

7.4. Deverá limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

7.5. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

7.6. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

7.7. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

7.8. Deverá permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

7.9. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

7.10. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

7.11. Deverá ter a capacidade de permitir a criação de perfis de controle de banda específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Linux e Windows.

8. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

8.1. Deverá possuir solução de filtro de conteúdo Web integrado à solução de segurança;

8.2. Deverá possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

8.3. Deverá possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;

8.4. Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;

8.5. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

8.5.1 Proxy anônimo;
8.5.2 Webmail;
8.5.3 Instituições de saúde;
8.5.4 Notícias;
8.5.5 Phishing;
8.5.6 Hackers;
8.5.7 Pornografia;
8.5.8 Racismo;
8.5.9 Websites pessoais;
8.5.10 Compras;

8.6. Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

8.7. Deverá permitir a criação de, pelo menos, 07 (sete) categorias personalizadas;

8.8. Deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

8.9. Deverá prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado quando houver tentativa de acesso a determinado serviço permitido ou bloqueado;

8.10. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
8.11. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

8.12. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

8.13. Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

8.14. Deverá permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;

8.15. Deverá permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

8.16. Deverá permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

8.17. Deverá permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

8.18. Deverá filtrar o conteúdo baseado em categorias em tempo real;

8.19. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

8.20. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

8.21. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

8.22. Deverá permitir a criação de regras para acesso/bloqueio por sub rede de origem;

8.23. Deverá ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;

8.24. Deverá permitir o bloqueio de redirecionamento HTTP;

8.25. Deverá permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

8.26. Deverá possuir Proxy Explícito e Transparente;

8.27. Deverá implementar roteamento WCCP e ICAP;

9. FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

9.1. Deverá permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

9.2. Deverá possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;

9.3. Deverá estar orientado à proteção de redes;

9.4. Deverá permitir funcionar em modo transparente, sniffer e router;

9.5. Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

9.6. Deverá permitir a criação de padrões de ataque manualmente;

9.7. Deverá possuir integração à plataforma de segurança;

9.8. Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;

9.9. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;

9.10. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

9.11. Deverá possuir mecanismos de detecção/proteção de ataques;
9.12. Deverá possuir reconhecimento de padrões;

9.13. Deverá possuir análise de protocolos;

9.14. Deverá possuir detecção de anomalias;

9.15. Deverá possuir detecção de ataques de RPC (Remote Procedure Call);

9.16. Deverá possuir proteção contra-ataques de Windows ou NetBios;

9.17. Deverá possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

9.18. Deverá possuir proteção contra-ataques DNS (Domain Name System);

9.19. Deverá possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;

9.20. Deverá possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);

9.21. Deverá possuir métodos de notificação de detecção de ataques;

9.22. Deverá possuir alarmes na console de administração;

9.23. Deverá possuir alertas via correio eletrônico;

9.24. Deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

9.25. Deverá ter a capacidade de resposta/logs ativa a ataques;

9.26. Deverá prover a terminação de sessões via TCP resets;

9.27. Deverá armazenar os logs de sessões;

9.28. Deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

9.29. Deverá mitigar os efeitos dos ataques de negação de serviços;

9.30. Deverá permitir a criação de assinaturas personalizadas;

9.31. Deverá possuir filtros de ataques por anomalias;

9.32. Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

9.33. Deverá permitir filtros de anomalias de protocolos;

9.34. Deverá suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

9.35. Deverá suportar verificação de ataque na camada de aplicação;

9.36. Deverá suportar verificação de tráfego em tempo real, via aceleração de hardware;

9.37. Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset.

10. FUNCIONALIDADE DE VPN

10.1. Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

10.2. Deverá possuir suporte a certificados PKI X.509 para construção de VPNs;

10.3. Deverá possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;

10.4. Deverá possuir suporte a VPN SSL;

10.5. Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

10.6. A VPN SSL deverá possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plugin ActiveX e/ou Java;

10.7. Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

10.8. A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS X;

10.9. Deverá permitir a arquitetura de VPN hub and spoke;

10.10. Deverá possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

11. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

11.1. Deverá reconhecer, no mínimo, 2.000 (duas mil) aplicações;

11.2. Deverá possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;

11.3. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:

11.3.1. P2P
11.3.2. Instant Messaging;
11.3.3. Web;
11.3.4. Transferência de arquivos;
11.3.5. VoIP;

11.4. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

11.5. Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

11.6. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

11.7. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

11.8. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

11.9. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

11.10. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

11.11. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

11.12. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

11.13. Deverá permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;

11.14. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

11.15. Deverá permitir criação de padrões de aplicação manualmente;

12. FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION)

12.1. O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de Informações) de gateway deverá funcionar de maneira que se consiga que os dados sensíveis não saiam da rede e também deverá funcionar de modo que se previna que dados não requisitados entrem na sua rede;

12.2. Deverá inspecionar, no mínimo, os tráfegos de e-mail, HTTP, NNTP e de mensageiros instantâneos;

12.3. Sobre o tráfego de e-mail, deverá inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;

12.4. Deverá realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS-Word;

12.5. Deverá fazer a varredura no conteúdo de um cookie HTTP buscando por determinado texto;

12.6. Deverá aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;

12.7. Deverá verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saintes possui um tamanho máximo especificado pelo administrador;

12.8. Deverá utilizar expressões regulares para composição das regras de verificação dos tráfegos;

12.9. Deverá tomar minimamente as ações de bloquear, banir usuário e colocar em quarentena a interface sobre as regras que coincidirem com o tráfego esperado pela regra;

12.10. Deverá permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail, HTTP e mensageiros instantâneos;

12.11. Deverá permitir a composição de múltiplas regras de DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

13. FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

13.1. Deverá permitir a criação de endereços IPs virtuais;

13.2. Deverá permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

13.3. Deverá suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

13.4. Deverá permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;

13.5. Deverá permitir persistência de sessão por cookie HTTP ou SSL session ID;

13.6. Deverá permitir que seja mantido o IP de origem;

13.7. Deverá suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

13.8. Deverá ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

13.9. Deverá permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável **E HTTP EM URL CONFIGURÁVEL.**

14. FUNCIONALIDADE DE VIRTUALIZAÇÃO

14.1. Deverá suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

14.2. Deverá permitir a criação de administradores independentes para cada uma das instâncias virtuais;

14.3. Deverá permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

15. FUNCIONALIDADE DE SD-WAN

15.1. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

15.2. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

15.3. A solução SD-WAN deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

15.4. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto:
bloqueio de malwares e reconhecimento em camada 7 de aplicações.

15.5. Solução deve ser capaz de prover Zero Touch provisioning.

15.6. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

15.7. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

15.8. A solução deve ser capaz de criar VPN "Full-Mesh" em interface Gráfica ou CLI, de forma automática, e sem que o administrador precise configurar site por site.

15.9. A configuração VPN IPSEC deverá oferecer suporte para DH Group: 14 e 15.

15.10. Reconhecimento em camada 7 totalmente segregado da camada 4.

15.11. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.

15.12. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

15.13. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc);

15.14. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6;

15.15. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.

15.16. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

15.17. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de saúde melhor que o link atual.

15.18. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.

15.19. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

16. UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATÓRIOS

16.1 CARACTERISTICAS DO EQUIPAMENTO:

16.1.1. Solução poderá ser entregue em applaiance ou em formato de solução virtual(VM) compativel com as plataformas VmWARE ou Microsoft Hyper-V;

16.1.2. Em caso de solução virtualizada, a contratada deverá fornecer os hardware e software necessários para hospedagem da solução, sendo de sua exclusiva responsabilidade todo e qualquer custo de aquisição, implantação, suporte e garantia desses itens durante a vigência do contrato.

16.1.3. As configurações mínimas para o equipamento a ser fornecido pela CONTRATADA para hospedar a solução virtual são:

16.1.3.1. Possuir a capacidade de receber pelo menos 600 GB de logs diários;
16.1.3.2. Possuir a capacidade analítica sustentada de 18 mil logs por segundo;
16.1.3.3. Possuir no mínimo 2 (duas) interfaces 10GE SFP+; 16.1.3.4. Possuir no mínimo 2 (duas) interfaces 10GE RJ45;
16.1.3.5. Possuir Possuir fonte de alimentação redundante Hot Swappable onde cada fonte fornecida deverá suportar sozinha a operação do equipamento;

16.1.4. A solução e seus equipamentos deverão ser instalados em rack do CONTRATANTE, ocupando no máximo 2U de altura;

16.1.5. Deverão ser fornecidos todos os acessórios e/ou itens necessários para instalação e pleno funcionamento da solução no ambiente da CONTRATADA, incluindo parafusos, cabos, transceivers, itens para instalação segura no rack, etc.

16.1.6. Deverá possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período da vigência contratual.

16.1.7. O suporte técnico deverá permitir a atualização de firmware dos equipamentos, da solução de virtualização e das bases de dados de todas as funcionalidades da solução de análise de logs;

16.2 REQUISITOS MINIMOS DE FUNCIONALIDADES:

16.2.1. Deve ser compatível com as Soluções “A”, “B”, “C” e “D” deste termo.

16.2.2. Deverá suportar o acesso via SSH ou WEB (HTTPS) para gerenciamento de soluções. Sendo que o gerenciamento administrativo da solução (configuração de Usuários / relatórios) deve ser realizado através de WEB ou GUI. O acesso SSH deve se dar mais para gerir problemas de hardwares e/ou alterações a nível CLI, para alterações no modo de processamento de pacotes e CPU´s e troubleshooting;

16.2.3. Deverá possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento.

16.2.4. Deverá permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento.

16.2.5. Deverá suportar SNMP versão 2 e 3;

16.2.6. Deverá permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados.

16.2.7. Deverá permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução.

16.2.8. Deverá permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH;

16.2.9. Deverá possuir autenticação de usuários para acesso à plataforma via LDAP;

16.2.10. Deverá possuir autenticação de usuários para acesso à plataforma via Radius;

16.2.11. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

16.2.12. Deverá possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas.

16.2.13. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de gráfico;

16.2.14. Deverá possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.

16.2.15. Deverá possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.

16.2.16. Deverá possuir visualização da quantidade de logs enviados de cada dispositivo monitorado;

16.2.17. Deverá possuir mecanismos de apagamento automático para logs antigos.

16.2.18. Deverá permitir importação e exportação de relatórios;

16.2.19. Deverá ter a capacidade de criar relatórios no formato HTML;

16.2.20. Deverá ter a capacidade de criar relatórios em formato PDF;

16.2.21. Deverá ter a capacidade de criar relatórios no formato XML;

16.2.22. Deverá permitir exportar os logs no formato CSV;

16.2.23. Deverá gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.

16.2.24. Deverá permitir que os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.

16.2.25. Deverá ter relatórios predefinidos.

16.2.26. Deverá poder enviar automaticamente os logs para um servidor FTP externo para a solução;

16.2.27. Deverá permitir a duplicação de relatórios existentes, deve ser possível para edição posterior.

16.2.28. Deverá ter a capacidade de personalizar a capa dos relatórios obtidos.

16.2.29. Deverá permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs.

16.2.30. Deverá ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

16.2.31. Deverá ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real.

16.2.32. Deverá permitir que os arquivos de log sejam baixados da plataforma para uso externo.

16.2.33. Deverá ter a capacidade de gerar e enviar relatórios periódicos automaticamente.

16.2.34. Deverá permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.

16.2.35. Deverá permitir o envio por e-mail relatórios automaticamente.

16.2.36. Deverá permitir que o relatório seja enviado por email ao destinatário específico.

16.2.37. Deverá permitir a programação da geração de relatórios, conforme calendário definido pelo administrador.

16.2.38. Deverá exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado.

16.2.39. Deverá permitir o uso de filtros nos relatórios.

16.2.40. Deverá permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros.

16.2.41. Deverá permitir especificar o idioma dos relatórios criados;

16.2.42. Deverá gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.

16.2.43. Deverá permitir o envio automático de relatórios para um servidor SFTP ou FTP externo.

16.2.44. Deverá ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios.

16.2.45. Deverá possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros.

16.2.46. Deverá ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles.

16.2.47. Deverá importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios.

16.2.48. Deverá ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log.

16.2.49. Deverá fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.

16.2.50. Deverá ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.

16.2.51. Deverá permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

16.2.52. Deverá permitir visualizar em tempo real os logs recebidos.

16.2.53. Deverá permitir o encaminhamento de log no formato syslog.

16.2.54. Deverá permitir o encaminhamento de log no formato CEF (Common Event Format).

16.2.55. Deverá gerar alertas de eventos a partir de logs recebidos;

16.2.56. Deverá permitir a criação de incidentes a partir de alertas de eventos para o terminal;

16.2.57. Suportar o padrão SAML ou LDAP ou RADIUS para autenticação do usuário administrador;

17 UNIDADE CENTRALIZADA DE GERENCIAMENTO DE DISPOSITIVOS

17.1 CARACTERISTICAS DO EQUIPAMENTO:

17.1.1. A solução poderá ser entregue em appliance ou no formato de solução virtual, compatível com as plataformas VMware, Microsoft Hyper-V, Citrix XenServer, KVM, no caso de solução virtualizada a responsabilidade pela implantação de servidor/hardware com licenciamento necessário será da CONTRATANTE.

17.1.2. Deverá possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período da vigência contratual.

17.1.3. Deve possuir licença para gerenciar de forma centralizada de no mínimo 200 dispositivos.

17.1.4. Deve garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;

17.1.5. Deve possuir definição de perfis de acesso ao console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

17.1.6. Deve gerar alertas automáticos via e-mail e snmp;

17.1.7. Deve monitorar a performance e Status dos links conectados a Solução de Segurança dos links de Internet;

17.1.8. Deve possibilitar a criação e administração de políticas de firewall, controle de aplicação, sistema prevenção a intrusão (IPS – intrusion prevention system), antivírus, pontos de acesso sem fio e de filtro de URL;

17.1.9. Deve permitir usar palavras chaves ou cores para facilitar identificação de regras;

17.1.10. Deve permitir localizar quais regras um objeto (ex. Computador, serviço, etc.) Está sendo utilizado;

17.1.11. Deve atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;

17.1.12. Deve permitir criação de regras que fiquem ativas em horário definido;

17.1.13. Deve permitir criação de regras com data de expiração;

17.1.14. Deve permitir realizar o backup das configurações para permitir o retorno (rollback) de uma configuração salva;

17.1.15. Deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing), ou garantir que esta exigência seja plenamente atendida por meio diverso.

17.1.16. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

17.1.17. Deve garantir que todos os componentes da Solução de Segurança dos Links de Internet sejam controlados de forma centralizada, utilizando apenas um servidor de gerência;

17.1.18. Deve garantir que os dispositivos de segurança sejam visualizados na operação integrada da rede através de geolocalização, e integrados com uma aplicação de mapas online (google maps, bing maps ou outra equivalente);

17.1.19. Deve possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;

17.1.20. Deve permitir ao administrador transferir os backups para um servidor SFTP;

17.1.21. Deve realizar a função de gerência em um equipamento exclusivo, não exercendo outras funções (como firewall);

17.1.22. Deve garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota, de maneira centralizada;

17.1.23. Deve permitir aos administradores se autenticarem nos servidores de gerência através de contas de usuários locais, de bases externas LDAP e RADIUS.

17.1.24. Deve suportar e realizar a sincronização do relógio interno dos equipamentos da solução via protocolo NTP;

17.1.25. Deve gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;

17.1.26. Deve permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como licenças, horário do sistema e firmware;

17.1.27. Deve permitir criar os objetos que serão utilizados nas políticas, de forma centralizada;

18 LISTA DE UNIDADES E TIPO DE SLA:

LOCALIDADE	NIVEL DE SLA
ALAGOINHAS	SLA REGIONAL
AMARGOSA	SLA REGIONAL
BARREIRAS	SLA REGIONAL
BARREIRAS CIRA	SLA REGIONAL
BOM JESUS DA LAPA	SLA REGIONAL
BRUMADO	SLA REGIONAL
CACHOEIRA	SLA REGIONAL

CAETITÉ	SLA REGIONAL
CAMACAN	SLA REGIONAL
CAMACARI	SLA REGIONAL
CANAVIEIRAS	SLA REGIONAL
CANDEIAS	SLA REGIONAL
CASA NOVA	SLA REGIONAL
CÍCERO DANTAS	SLA REGIONAL
CONCEICAO DO COITE	SLA REGIONAL
CRUZ DAS ALMAS	SLA REGIONAL
DIAS D'AVILA	SLA REGIONAL
ENTRE RIOS	SLA REGIONAL
EUCLIDES DA CUNHA	SLA REGIONAL
EUNAPOLIS	SLA REGIONAL
FEIRA DE SANTANA	SLA REGIONAL
GANDU	SLA REGIONAL
GUANAMBI	SLA REGIONAL
IBICARAÍ	SLA REGIONAL
IBOTIRAMA	SLA REGIONAL
ILHEUS	SLA REGIONAL
ILHÉUS AMBIENTAL	SLA REGIONAL
ILHÉUS SALOBRINHO – UESC	SLA REGIONAL
IPIAU	SLA REGIONAL
IRECE	SLA REGIONAL
ITABERABA	SLA REGIONAL
ITABUNA	SLA REGIONAL
ITACARE	SLA REGIONAL

ITAMARAJU	SLA REGIONAL
ITAPETINGA	SLA REGIONAL
ITUBERA	SLA REGIONAL
JACOBINA	SLA REGIONAL
JEQUIE	SLA REGIONAL
JEREMOABO	SLA REGIONAL
JUAZEIRO	SLA REGIONAL
LAPÃO	SLA REGIONAL
LAURO DE FREITAS	SLA REGIONAL
LENÇÓIS	SLA REGIONAL
LIVRAMENTO	SLA REGIONAL
LUIS EDUARDO MAGALHAES	SLA REGIONAL
MACAÚBAS	SLA REGIONAL
MATA DE SÃO JOÃO	SLA REGIONAL
MORRO DO CHAPÉU	SLA REGIONAL
MURITIBA	SLA REGIONAL
NAZARÉ DAS FARINHAS	SLA REGIONAL
PARIPIRANGA	SLA REGIONAL
PAULO AFONSO	SLA REGIONAL
PILÃO ARCADO	SLA REGIONAL
POÇÕES	SLA REGIONAL
PORTO SEGURO	SLA REGIONAL
PRAIA DO FORTE	SLA REGIONAL
REMANSO	SLA REGIONAL
RIACHÃO DO JACUÍPE	SLA REGIONAL
RIBEIRA DO POMBAL	SLA REGIONAL
RUY BARBOSA	SLA REGIONAL
SALVADOR – SEDE CAB	SLA CAPITAL
SALVADOR – SEDE CAB CORE DE REDE	SLA CAPITAL

SALVADOR – CEAF	SLA REGIONAL
SALVADOR – EDF. TEIX. DE FREITAS	SLA CAPITAL
SALVADOR – SEDE NAZARÉ	SLA CAPITAL
SALVADOR – FÓRUM SUSSUARANA	SLA CAPITAL
SANTA MARIA DA VITÓRIA	SLA REGIONAL
SANTO AMARO	SLA REGIONAL
SANTO ANTÔNIO DE JESUS	SLA REGIONAL
SÃO FELIX	SLA REGIONAL
SÃO FRANCISCO DO CONDE	SLA REGIONAL
SEABRA	SLA REGIONAL
SENHOR DO BONFIM	SLA REGIONAL
SERRINHA	SLA REGIONAL
SIMÕES FILHO	SLA REGIONAL
TEIXEIRA DE FREITAS	SLA REGIONAL
VALENÇA	SLA REGIONAL
VALENÇA AMBIENTAL	SLA REGIONAL
VITÓRIA DA CONQUISTA	SLA REGIONAL
XIQUE-XIQUE	SLA REGIONAL

APENSO II

TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Os abaixo-assinados, de um lado o **MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA**, CNPJ nº 04.142.491/0001-66, sediado na cidade de Salvador–BA, à 5ª Avenida, nº 750, do Centro Administrativo da Bahia, CEP 41.745-004, doravante denominado **CONTRATANTE**, e de outro lado a empresa **TLD TELEDATA COMERCIO E SERVICOS LTDA , CNPJ nº 33.927.849/0001-64, situada na cidade de Salvador, à Rua S. Luiz Gonzaga das Virgens, 111, Ed. Liz Corporate, 4º Andar, sala 402, Caminhos das Árvores,** doravante denominada **CONTRATADA**, tem entre si justa e acertada, a celebração do presente **TERMO DE COMPROMISSO DE SIGILO E CONFIDENCIALIDADE**, através do qual a **CONTRATADA** aceita não divulgar sem autorização previa e formal segredos e informações sensíveis de propriedade do **CONTRATANTE** e se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:

1.A **CONTRATADA** reconhece que em razão das suas atividades profissionais, estabelece contato com informações sigilosas, que devem ser entendidas como segredo. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, ai se incluindo os próprios colaboradores da **CONTRATADA**, sem a expressa e escrita autorização do **CONTRATANTE**.

2.As informações, exemplificadas abaixo, devem receber o tratamento de confidencialidade adequado, de acordo com o seu nível de classificação.

2.1. Programas de computador, suas listagens, documentação, artefatos diversos, código fonte e código objeto;

2.2. Toda a informação relacionada a programas existentes ou em fase de desenvolvimento, inclusive fluxogramas, estatísticas, especificações, avaliações, resultados de testes, arquivos de dados, artefatos diversos e versões “beta” de quaisquer programas;

2.3. Documentos, informações e dados armazenados de atuação consultiva e contenciosa, de estratégias ou demais dados e/ou informações de caráter sigiloso ou restrito;

2.4. Metodologia, projetos e serviços utilizados;

2.5. Números e valores financeiros.

2.6 Demais informações trafegadas no ambiente de rede do **CONTRATANTE**, como arquivos e e-mails;

3. A **CONTRATADA** reconhece que a lista acima é meramente exemplificativa e ilustrativa e que outras hipóteses de confidencialidade que já existam ou que venham a surgir no futuro devem ser mantidas sob segredo. Em caso de dúvida acerca da confidencialidade de determinada informação a **CONTRATADA** deve tratar a mesma sob sigilo até que seja autorizado, formalmente, a tratá-la de forma diferente pelo **CONTRATANTE**.

4.A **CONTRATADA** reconhece que, no seu desligamento definitivo do contrato, deverá entregar ao **CONTRATANTE** todo e qualquer material de propriedade desta, inclusive notas pessoais envolvendo matérias sigilosas relacionadas com a atividade, registros de documentos de qualquer natureza que tenham sido usados, criados ou estado sob seu controle. A **CONTRATADA** também assume o compromisso de não utilizar qualquer informação adquirida quando de suas atividades para o **CONTRATANTE**.

5.A **CONTRATADA** deve assegurar que todos os seus colaboradores guardarão sigilo sobre as informações que porventura tiverem acesso, mediante o ciente de seus colaboradores em Termo próprio a ser firmado entre a **CONTRATADA** e seus colaboradores, e que os mesmos comprometer-se-ão a informar, imediatamente, ao seu superior hierárquico, qualquer violação das regras de sigilo, por parte dele ou de qualquer pessoa, inclusive nos casos de violação não intencional.

5.1.A coleta dos Termos de Sigilo de seus colaboradores não exime a **CONTRATADA** das penalidades por violação das regras por parte de seus contratados.

5.2.A **CONTRATADA** deverá fornecer cópia de todos os termos firmados com seus colaboradores quando do início dos trabalhos.

5.3. Sempre que um colaborador for admitido, a **CONTRATADA** deverá fornecer cópia do respectivo termo de sigilo por aquele firmado no prazo de 2 (dois) dias após a contratação.

6.A **CONTRATADA** deverá seguir a Política de Segurança da Informação definida pelo **CONTRATANTE**.

7.O não cumprimento de quaisquer das cláusulas deste Termo implicará em responsabilização civil e criminal, de acordo com a legislação vigente.

TLD TELEDATA COMERCIO E SERVICOS LTDA
Ricardo Luiz de Oliveira
Sócio

Ministério Público do Estado da Bahia
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

Documento assinado eletronicamente por **Ricardo Luiz de Oliveira** em 27/12/2023, às 15:05, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.

Documento assinado eletronicamente por **André Luis Sant Ana Ribeiro** em 09/01/2024, às 18:35, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0911650** e o código CRC **86216A2A**.

MINISTÉRIO PÚBLICO
DO ESTADO DA BAHIA

PORTARIA

PORTARIA SGA Nº 472/2023

O SUPERINTENDENTE DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA , no uso de suas atribuições, RESOLVE designar os servidores Iaçanã Lima de Jesus Carneiro, matrícula nº [redacted] e Plinio Andrade Passos, matrícula nº [redacted] para exercerem as atribuições de fiscal e suplente, respectivamente, do contrato nº 190/2023-SGA, relativo à prestação de serviços de locação de equipamentos de Segurança da Informação, sob demanda, englobando o fornecimento de todo o hardware, software, subscrições, instalação, configuração, suporte técnico, treinamento, reposição de peças.

Superintendência de Gestão Administrativa do Ministério Público do Estado da Bahia.

André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

(Datado e assinado eletronicamente)

Documento assinado eletronicamente por **André Luis Sant Ana Ribeiro** em 10/01/2024, às 20:40, conforme Ato Normativo n° 047, de 15 de Dezembro de 2020 - Ministério Público do Estado da Bahia.

A autenticidade do documento pode ser conferida no site https://sei.sistemas.mpba.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0910698** e o código CRC **C0A83038**.

PORTARIA SGA Nº 018/2024
O SUPERINTENDENTE DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, no uso de suas atribuições, RESOLVE designar os servidores Tiago Rios Rocha, matrícula nº [redacted] e Ana Paula Araujo Lino Mota, matrícula nº [redacted], para exercerem as atribuições de fiscal e suplente, respectivamente, do contrato nº 037/2023-SGA, relativo à prestação de serviços de engenharia de manutenção preventiva e corretiva em equipamentos de ar-condicionado, tipo SPLIT e ACJ, instalados nas sedes do Ministério Público do Estado da Bahia, situadas na cidade de Salvador/BA e Região Metropolitana Salvador – Bahia.
Ficam revogadas as designações anteriores relativas à Portaria nº 107/2023.
Superintendência de Gestão Administrativa do Ministério Público do Estado da Bahia, 11 de janeiro de 2024.
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

PORTARIA SGA Nº 019/2024
O SUPERINTENDENTE DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, no uso de suas atribuições, RESOLVE designar os servidores Maira de Almeida Soares, matrícula nº 355.390 e Ana Paula Araujo Lino Mota, matrícula nº 353.945, para exercerem as atribuições de fiscal e suplente, respectivamente, do contrato nº 091/2023-SGA, relativo à prestação de serviços de engenharia para manutenção preventiva e corretiva em sistema de combate a incêndio.
Ficam revogadas as designações anteriores relativas à Portaria nº 257/2023.
Superintendência de Gestão Administrativa do Ministério Público do Estado da Bahia, 11 de janeiro de 2024.
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

PORTARIA SGA Nº 020/2024
O SUPERINTENDENTE DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, no uso de suas atribuições, RESOLVE designar os servidores Tiago Rios Rocha, matrícula nº 355.383 e Ana Paula Araujo Lino Mota, matrícula nº 353.945, para exercerem as atribuições de fiscal e suplente, respectivamente, do contrato nº 097/2023-SGA, relativo à prestação de serviços de Engenharia de Manutenção Preventiva e Corretiva em Sistema de Climatização - sede Nazaré.
Ficam revogadas as designações anteriores relativas à Portaria nº 306/2023.
Superintendência de Gestão Administrativa do Ministério Público do Estado da Bahia, 11 de janeiro de 2024.
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

PORTARIA SGA Nº 021/2024
O SUPERINTENDENTE DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, no uso de suas atribuições, RESOLVE designar os servidores Tiago Rios Rocha, matrícula nº [redacted] e Ana Paula Araujo Lino Mota, matrícula nº [redacted], para exercerem as atribuições de fiscal e suplente, respectivamente, do contrato nº 125/2023-SGA, relativo à prestação de serviços de Manutenção preventiva e corretiva em 01 (um) nobreak, instalado na sede do Ministério Público do Estado da Bahia, situada no Centro Administrativo do Estado da Bahia.
Ficam revogadas as designações anteriores relativas à Portaria nº 320/2023.
Superintendência de Gestão Administrativa do Ministério Público do Estado da Bahia, 11 de janeiro de 2024.
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

O SUPERINTENDENTE DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, no uso de suas atribuições, RESOLVE tornar sem efeito a publicação relativa ao Contrato nº 190/2023 e Portaria 472/2023, constante da edição nº 3.491 do Diário da Justiça Eletrônico do dia 12/01/2024.
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa

RESUMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS – Nº 190/2023 - SGA. Processo SEI: 19.09.00843.0007700/2023-04 – PE 048/2023. Parecer jurídico: 910/2023. Partes: Ministério Público do Estado da Bahia e a empresa TLD Teledata Comercio e Serviço Ltda, CNPJ nº 33.927.849/0001-64. Objeto: prestação de serviços de locação de equipamentos de Segurança da Informação, sob demanda, englobando o fornecimento de todo o hardware, software, subscrições, instalação, configuração, suporte técnico, treinamento, reposição de peças. Regime de Execução: Empreitada por preço unitário. Valor Global estimado: R$ 13.243.999,80 (treze milhões, duzentos e quarenta e três mil, novecentos e noventa e nove reais e oitenta centavos). Dotação Orçamentária: Unidade Orçamentária/Gestora 40.101.0021. Ação (P/A/OE): 2002. Região: 9900. Destinação de Recursos: 100. Natureza de Despesa: 33.90.40. Forma de Pagamento: Ordem bancária para crédito em conta corrente do Contratado. Prazo de vigência: 60 (sessenta) meses, a contar da data da publicação do resumo no Diário da Justiça Eletrônico.

PORTARIA SGA Nº 472/2023
O SUPERINTENDENTE DE GESTÃO ADMINISTRATIVA DO MINISTÉRIO PÚBLICO DO ESTADO DA BAHIA, no uso de suas atribuições, RESOLVE designar os servidores Iaçanã Lima de Jesus Carneiro, matrícula nº [redacted] e Plinio Andrade Passos, matrícula nº [redacted], para exercerem as atribuições de fiscal e suplente, respectivamente, do contrato nº 190/2023-SGA, relativo à prestação de serviços de locação de equipamentos de Segurança da Informação, sob demanda, englobando o fornecimento de todo o hardware, software, subscrições, instalação, configuração, suporte técnico, treinamento, reposição de peças.
Superintendência de Gestão Administrativa do Ministério Público do Estado da Bahia, 11 de janeiro de 2024.
André Luis Sant´Ana Ribeiro
Superintendente de Gestão Administrativa