

UNIVERSIDADE FEDERAL DA BAHIA

Processo Administrativo nº 23066.017887/2023-19

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de ativos de segurança de rede do tipo Next Generation Firewall (NGFW), com SD-WAN integrada, instalação e suporte técnico, com garantia de 60 (sessenta meses), para o Datacenter da UFBA, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	CATMAT	UNIDADE DE MEDIDA	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de Segurança – Firewall - Suporte/Garantia e licenciamento por 60 (Sessenta) meses, conforme ADENDO 01, constante no Termo de Referência.	481647	Unidade	02	R\$ 1.281.879,67	R\$ 2.563.759,34
VALOR TOTAL						R\$ 2.563.759,34

1.2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.3. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

1.4. O prazo de vigência da contratação é de 60 meses, contados do(a) data de assinatura dos referidos contratos, na forma do artigo 105 da Lei nº 14.133, de 2021.

1.5. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2023/2024, conforme detalhamento a seguir:

ALINHAMENTO AO PCA	
DFD	Classe/Grupo
249	EQUIPAMENTOS DE REDE DE TIC - LOCAL E REMOTA

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

4. DO PARCELAMENTO DA SOLUÇÃO DE TIC

4.1. A solução de TIC a ser contratada trata-se de soluções de segurança da informação que atenderão à UFBA. Em regra, conforme Inciso II do art. 47 da Lei nº 14.133/21, as compras deverão ser parceladas, quando for tecnicamente e economicamente vantajosas, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala. Desta forma, a adjudicação será realizada por item.

5. REQUISITOS DA CONTRATAÇÃO

5.1. Sustentabilidade:

ID	Requisitos de Sustentabilidade
1.	No que couber, visando a atender ao disposto na legislação aplicável – em destaque às Instruções Normativas 05/2017/SEGES e 01/2019/SGD – a CONTRATADA deverá priorizar, para a execução dos serviços, a utilização de bens que sejam no todo ou em partes compostos por materiais recicláveis, atóxicos e biodegradáveis.
2.	Usar equipamentos homologados pela Anatel e/ou ABNT, no que diz respeito a normas ambientais.
3.	Fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução dos serviços de instalação da Solução.

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

4.	Respeitar as Normas Brasileiras - NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos, incluindo práticas de logística reversa, conforme o caso.
5.	Dar preferência ao uso de bens constituídos por material reciclado, atóxico, biodegradável, conforme ABNT NBR - 15448-1 e 15448-2.
6.	Acondicionar os bens preferencialmente em embalagem individual adequada, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.
7.	Que os bens não contenham substâncias perigosas em concentração acima das recomendadas pelas normas técnicas.
8.	Todos os documentos ou artefatos gerados pela contratada, salvo manifestação explícita deverão ser entregues em formato digital.

5.2. Requisitos de Negócio

ID	Requisitos de Negócio
1.	A solução deverá permitir a segurança dos dados pessoais e institucionais por ela utilizado.
2.	A contratada deverá garantir a disponibilidade, integridade e confidencialidade da solução.
3.	A solução deverá possuir suporte técnico especializado.
4.	A solução deverá estar sempre atualizada, em sua última versão disponível, durante a vigência do contrato.
5.	A prestação dos serviços não gerará vínculo empregatício entre os empregados da Contratada e a Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.
6.	Todos os dados e ativos processuais produzidos em decorrência do uso da solução serão de inteira propriedade da UFBA.

5.3. Requisitos de Capacitação

ID	Requisitos de Capacitação
1.	Deve ser fornecido treinamento que ofereça os conhecimentos necessários e suficientes para a instalação, administração, configuração, otimização, resolução de problemas e utilização do equipamento, com carga horária mínima de 20 horas, para a equipe de 6 pessoas responsáveis pela operação do serviço, além da possibilidade de participação de ouvintes.

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

2.	<p>O treinamento deverá contemplar, no mínimo, os seguintes tópicos:</p> <ol style="list-style-type: none"> 1. Funcionalidades básicas do equipamento: senha de administração, hora e data, schedules e etc.; 3. Procedimento de registro e ativação de licenças; 4. Procedimento de atualização de software; 5. Zonas de segurança e objetos; 6. Interfaces físicas, interfaces virtuais (VLANs) e roteamento interno; 7. NAT; 8. Serviços de segurança como IPS e Anti-Malware; 9. Regras de firewall; 10. VPN; 11. Regras de aplicação, incluindo visibilidade das mesmas; 12. Geração de relatórios diversos da plataforma; 13. Monitoramento da plataforma; e 14. Demais funcionalidades existentes no firewall que não estão contempladas acima.
3.	<p>O Treinamento poderá ser realizado através de ferramentas de videoconferência ou presencialmente. Para melhor didática, a empresa fornecedora deverá disponibilizar um ambiente online (laboratório) para simular o uso dos equipamentos de firewall.</p>
4.	<p>O ambiente tecnológico a ser utilizado durante a capacitação fica sob responsabilidade da contratada, podendo a UFBA auxiliar no que for possível.</p>
5.	<p>A carga horária 20h poderá ser estendida conforme o necessário para que os capacitados recebam todo o treinamento necessário e suficiente para operar a solução.</p>
6.	<p>Os materiais didáticos (apostila, slides, livros, etc...), sejam eles impressos ou digitais, deverão ser providos pela empresa fornecedora e disponibilizados para consulta posterior.</p>
7.	<p>Para consulta posterior, deverá ser fornecido no mínimo 3 tipos de materiais (Ex: apostila + slide ou slide + livro ou apostila + slide + livro).</p>
8.	<p>Exige-se que o instrutor tenha domínio técnico pleno da solução e possuir certificado fornecido por centro de treinamento oficial do Fabricante que o credencie a ministrar treinamentos na solução.</p>
9.	<p>A contratada deverá emitir certificado ao final da capacitação indicando a carga horária, nome do participante, tópicos abordados no curso, bem como outras informações apropriadas.</p>

5.4. Requisitos Legais

ID	Requisitos Legais
-----------	--------------------------

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

1.	A contratada deverá observar e cumprir a Lei nº 14.133, de 1º de abril de 2021, que institui normas para licitações e contratos da Administração Pública.
2.	A contratada deverá observar e cumprir a Política de Segurança da Informação da UFBA.
3.	A contratada deverá observar e cumprir o Decreto Nº 9.637, de 26 de dezembro de 2018, da Presidência da República, que institui a Política Nacional de Segurança da Informação.
4.	A contratada deverá observar e cumprir a Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
5.	A contratada deverá observar e cumprir a Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, que dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP).

5.5. Requisitos de Manutenção

ID	Requisitos de Manutenção
1.	Todos os equipamentos que compõe a solução devem acompanhar extensão de garantia de suporte e manutenção de software e hardware, com substituição de peças e/ou equipamentos, por um período de 60 meses.
2.	O modelo dos equipamentos não pode estar prestes a ser descontinuados para o serviço de suporte pelo fabricante, ou seja, não pode estar no final de seu “ciclo de vida”, durante a vigência do contrato.
3.	A empresa fornecedora deverá fornecer os softwares e suas atualizações, firmwares, sistema operacional, durante toda a vigência da garantia, através de meio eletrônico ou magnético sem ônus adicionais.
4.	A contratada deverá disponibilizar canal de comunicação (telefone, e-mail ou sistema de chamados), para abertura e gerenciamento de chamados técnicos 24x7.
5.	Dada a necessidade de reposição de peça/equipamento, a CONTRATADA deverá preparar ou realizar a substituição, reconfiguração (importação de arquivos de backup), no datacenter da STI/UFBA, em até 1 (um) dia útil.
6.	Os chamados técnicos serão classificados de acordo com a severidade devendo atender aos respectivos prazos de solução definidos abaixo: <ul style="list-style-type: none"> SEVERIDADE BAIXA – prazo máximo de 48 horas para solução: correção de falha que não impede a continuidade da maior parte dos negócios e solicitações de informações sobre os produtos, incluindo configuração e instalação; SEVERIDADE MÉDIA – prazo máximo de 24 horas para solução: problemas que causem impactos significativos nos negócios, incluindo degradação de desempenho; SEVERIDADE ALTA – prazo máximo de 04 horas para solução: problemas que causem a interrupção parcial ou total dos serviços.
7.	Quaisquer peças, componentes ou outros materiais que substituírem os defeituosos deverão ser originais do fabricante e de qualidade e características técnicas iguais ou superiores aos existentes no equipamento, sem ônus para a UFBA.

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

8.	Em caso da impossibilidade em solucionar o problema nos prazos estipulados, a CONTRATADA compromete-se a substituir urgentemente o equipamento defeituoso, até o término do reparo do mesmo, por outro equivalente ou superior, de sua propriedade, a fim de proporcionar a operacionalização do equipamento e a continuidade da rotina de trabalho dos usuários.
9.	Todas as despesas relacionadas com a eventual substituição dos equipamentos, no local de instalação (STI/UFBA), ocorrerão por conta da contratada e/ou do fabricante.
10.	A CONTRATADA não poderá cobrar valores adicionais, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho em sábados, domingos e feriados ou em horário noturno, bem como qualquer outro valor adicional.
11.	A CONTRATADA e/ou fabricante deverá providenciar o deslocamento do equipamento, quando necessário, bem como seu retorno ao local de origem, sendo considerado, para todos os efeitos, durante este período, como fiel depositário do mesmo.

5.6. Requisitos Temporais

ID	Requisitos Temporais
1.	A resolução de problemas deverá ser atendida conforme estabelecido neste Termo de Referência.
2.	As datas de realização do treinamento serão acordadas através de reunião do gestor do contrato com o preposto da CONTRATADA, após a assinatura do contrato e mediante a abertura de ordem de serviço pela contratante.

5.7. Requisitos de Segurança e Privacidade

ID	Requisitos de Segurança e Privacidade
1.	A contratada deverá observar e cumprir a Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018)
2.	A contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos
3.	A contratada deverá coibir o vazamento de dados e fraudes digitais
4.	Em conformidade com o disposto na NC 14/IN01/DSIC/GSIPR, os dados e informações do contratante devem residir exclusivamente em território nacional, incluindo replicação e cópias de segurança (<i>backups</i>), de modo que a Contratante disponha de todas as garantias da legislação brasileira enquanto tomador do serviço e responsável pela guarda das informações armazenadas em nuvem.

5.8. Requisitos Sociais, Ambientais e Culturais

ID	Requisitos Sociais, Ambientais e Culturais
1.	Os serviços prestados pela Contratada deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e materiais consumidos bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pela contratante.

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

5.9. Requisitos de Arquitetura Tecnológica

ID	Requisitos de Arquitetura Tecnológica
1.	A alta disponibilidade informada acima deverá suportar os modos ativo-ativo e ativo-passivo, com sincronização, em tempo real, de configuração e de estados das sessões. No caso de falha de um dos equipamentos do cluster, não deverá haver perda das configurações e nem das sessões já estabelecidas e a transição entre os equipamentos deverá acontecer de forma transparente para o usuário.
2.	A solução deverá incluir as funcionalidades mínimas de um Firewall de nova geração: 1. Funcionalidades de um firewall tradicional; 2. IPS integrado; 3. Controle de aplicação; e 4. Outras características elencadas no ADENDO 01 - Especificações Técnicas da Solução de TIC.

5.10. Requisitos de Projeto e de Implementação

ID	Requisitos de Projeto e de Implementação
1.	A contratada deverá realizar o planejamento das atividades a serem executadas, através da elaboração de um cronograma e um plano de projeto e implementação, em consonância com as disposições constantes neste Termo de Referência.
2.	Reunião para detalhamento de todos os parâmetros de configuração da solução de segurança da informação.
3.	Definição do plano de testes, em conjunto com o corpo responsável da UFBA, de cada etapa para migração dos serviços.
4.	Definição de cronograma de implementação do projeto com o planejamento de migração para não afetar a operação da rede atual.
5.	Deverá ser executado por profissionais devidamente capacitados, com certificação do fabricante.

5.11. Requisitos de Implantação

ID	Requisitos de Implantação
1.	A contratada deverá realizar o planejamento das atividades a serem executadas, bem como cronograma detalhado, devendo ser entregue em um Plano de Projeto, elaborado em consonância com as disposições constantes neste Termo de Referência.
2.	O Plano de Projeto deverá ser entregue antes da execução das atividades, validado e aprovado previamente pelo Gestor do Contrato.
3.	A implantação da solução no ambiente da UFBA deve obedecer a gestão de mudança e liberação que são realizadas na STI.

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

4.	Os serviços serão executados conforme o acordado no Plano de Projeto, que deverão conter as atividades necessárias para entrega e perfeito funcionamento do objeto contratado.
5.	Deverá ocorrer uma reunião de início de Projeto para alinhamento dos serviços a serem executados, agendada previamente entre as partes, através de e-mail ou telefone, em até 15 (quinze) dias após a assinatura do contrato.
6.	Deverá ocorrer uma reunião para apresentação e validação do Plano de Projeto.
7.	Em caráter excepcional e a critério da UFBA, as atividades poderão ser realizadas em dias e horários distintos do estabelecido, definidos em comum acordo com a contratada.

5.12. Requisitos de Garantia e Manutenção

ID	Requisitos de Garantia e Manutenção
1.	A contratada deverá disponibilizar canal de comunicação (telefone, e-mail ou sistema de chamados), para abertura e gerenciamento de chamados técnicos 24x7.
2.	A contratada deverá possibilitar que as novas atualizações da solução sejam utilizadas pela UFBA durante o período de vigência do contrato.

5.13. Requisitos de Experiência Profissional

ID	Requisitos de Experiência Profissional
1.	Apresentar uma lista com o nome de cada profissional que será utilizado na execução dos serviços, ficando a critério da UFBA a aprovação dos profissionais listados, bem como solicitar a substituição de qualquer profissional que julgar não possuir a capacitação necessária para execução dos serviços.
2.	Os profissionais deverão possuir certificado fornecido por centro de treinamento oficial do Fabricante que o credencie na implantação da solução contratada.

5.14. Requisitos de Formação da Equipe

ID	Requisitos de Formação da Equipe
1.	Não se aplica.

5.15. Requisitos de Metodologia de Trabalho

ID	Requisitos de Metodologia de Trabalho
1.	A UFBA encaminhará Ordem de Serviço/Fornecimento solicitando implantação da solução adquirida.
2.	A solução deverá ser implantada no prazo estabelecido neste Termo de Referência.
3.	A CONTRATADA, com apoio da UFBA, no que couber, realizará a implantação e a configuração dos equipamentos.

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

4.	Sendo atendido pela contratada o demandado na Ordem de Serviço/Fornecimento, a UFBA procederá com o recebimento provisório e em seguida após análise dos serviços e bens fornecidos será elaborado o termo de recebimento definitivo e o processo de pagamento.
5.	A implantação da solução poderá ser realizada em fases e de acordo com a necessidade da UFBA.
6.	O pagamento será efetuado conforme a implantação da solução contratada e entrega dos equipamentos.

5.16. Requisitos de Segurança da Informação e Privacidade

ID	Requisitos de Segurança da Informação e Privacidade
1.	A contratada deverá observar a Lei Geral de Proteção de Dados Pessoais -LGPD (Lei nº 13.709/2018)
2.	A contratada deverá observar a ABNT NBR ISO/IEC 27001:2013. Tecnologia da Informação - Técnicas de Segurança
3.	A contratada deverá observar a ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação
4.	A contratada deverá observar a ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 2700
5.	A contratada deverá observar Guia de Boas Práticas da LGPD – CCGD (Comitê Central de Governança de Dados).

5.16.1 Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

5.16.1.1 Instrução Normativa SLTI/MPOG nº 1, de 19 de janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.

5.16.1.2 Decreto nº 9.373, de 11 de maio de 2018, dispõe sobre a alienação, a cessão, a transferência, a destinação e a disposição final ambientalmente adequadas de bens móveis no âmbito da administração pública federal direta, autárquica e fundacional.

5.16.1.3 Resolução Conama nº 401, de 4 de novembro de 2008, que estabelece os limites máximos de chumbo, cádmio e mercúrio para pilhas e baterias comercializadas no território nacional e os critérios padrões para o seu gerenciamento ambientalmente adequado, e dá outras providências.

5.16.1.4 Art. 33, inciso VI, da Lei Federal nº 12.305/2010, que dispõe sobre a Política Nacional de Resíduos Sólidos, de abrangência nacional, determina que os fabricantes, importadores, distribuidores e comerciantes de produtos eletro-eletrônicos e seus componentes são obrigados a estruturar e implementar sistemas de logística reversa, mediante retorno dos produtos e embalagens após o uso pelo consumidor, de forma independente do serviço público de limpeza urbana e de manejo dos resíduos sólidos.

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

5.16.1.5 Guia Nacional de Licitações Sustentáveis– DECOR/CGU/AGU, quando da aquisição de bens, serão exigidos os seguintes critérios de sustentabilidade:

5.16.1.6 Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação.

Subcontratação

5.17. *Não é admitida a subcontratação do objeto contratual.*

Garantia da contratação

5.18. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% do valor contratual, conforme regras previstas no contrato.

5.19. A garantia nas modalidades caução e fiança bancária deverá ser prestada em até 15 dias após assinatura do contrato.

5.20. No caso de seguro-garantia sua apresentação deverá ocorrer, no máximo, até a data de assinatura do contrato.

5.21. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

6. RESPONSABILIDADES

6.1. Deveres e responsabilidades da CONTRATANTE

6.1.1. Nomear servidores que integrarão a Equipe de Gestão do Contrato nos termos do art. 29 da Instrução Normativa SGD/ME Nº 94/2022, composta por Gestor do Contrato, Fiscal Técnico, Fiscal Requisitante e Fiscal Administrativo para acompanhar e fiscalizar a execução dos contratos.

6.1.2. Encaminhar formalmente a demanda, preferencialmente por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos neste Termo de Referência ou Projeto Básico, observando-se o disposto no art. 18 a 32 da Instrução Normativa ME Nº 94/2022.

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

- 6.1.3. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas.
- 6.1.4. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato.
- 6.1.5. Comunicar à contratada todas e quaisquer ocorrências relacionadas ao fornecimento da solução de TIC.
- 6.1.6. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável.
- 6.1.7. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos, cuja criação ou alteração seja, objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.
- 6.1.8. Comunicar a CONTRATADA toda e quaisquer ocorrências relacionadas com o produto.
- 6.1.9. Fiscalizar a entrega dos serviços/bens, podendo sustar, recusar, solicitar fazer ou desfazer qualquer entrega ou serviços, no todo ou em parte, que não esteja de acordo com as condições e exigências estabelecidas em cada ordem de serviço ou no Termo de Referência.
- 6.1.10. Analisar os relatórios de desempenho e os resultados entregues verificando se as exigências, procedimentos e processos definidos e aprovados nas ordens de serviço foram atendidos, assim como se os índices foram alcançados, propondo as glosas e multas cabíveis para cada caso.
- 6.1.11. Emitir relatórios sobre os atos relativos à execução do Contrato que vier a ser firmado, em especial, quanto ao acompanhamento e fiscalização da execução dos serviços, à exigência de condições estabelecidas e proposta de aplicação de sanções;
- 6.1.12. Notificar à CONTRATADA eventual irregularidade no cumprimento das obrigações contratuais.
- 6.1.13. Impor sanções contratuais caso suas demandas de correção de irregularidades, notificadas à CONTRATADA, não sejam corrigidas dentro do prazo estabelecido.
- 6.1.14. Exigir o cumprimento de todos os compromissos assumidos pela CONTRATADA, de acordo com as especificações do objeto, constantes deste Termo de Referência.
- 6.1.15. Fiscalizar a execução do objeto, tanto sob o aspecto quantitativo como qualitativo.

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

6.1.16. Analisar e verificar se os Acordos de Níveis de Serviços contratados foram alcançados e propor as glosas estipuladas para cada caso.

6.2. Deveres e responsabilidades da CONTRATADA

6.2.1. Indicar formalmente e por escrito, no prazo máximo de 5 dias úteis após a assinatura do contrato, junto à contratante, um preposto idôneo com poderes de decisão para representar a contratada, principalmente no tocante à eficiência e agilidade da execução do objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato.

6.2.2. Atender prontamente quaisquer orientações e exigências da Equipe de Gestão e Fiscalização do Contrato, inerentes à execução do objeto contratual.

6.2.3. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante.

6.2.4. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

6.2.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação.

6.2.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC.

6.2.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato.

6.2.8. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados à Administração.

6.2.9. Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

6.2.10. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da contratante.

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

6.2.11. Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão.

6.2.12. Cumprir, às suas próprias expensas, todas as cláusulas contratuais que definam suas obrigações.

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

6.2.14. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados durante a execução deste contrato, ainda que acontecido em dependência da CONTRATANTE.

6.2.15. É de responsabilidade da contratada fornecer a seus técnicos todas as ferramentas, softwares e instrumentos necessários e suficientes para a execução dos serviços, bem como prover e se responsabilizar pela locomoção dos mesmos até a UFBA.

6.2.16. A empresa a ser contratada deverá garantir que os produtos licenciados para uso não infringem quaisquer patentes, direitos autorais ou trade-secrets, devendo a empresa a ser contratada se responsabilizar por quaisquer despesas relacionadas que ocorram.

6.2.17. O contrato possuirá um gestor e uma equipe de fiscalização (fiscal requisitante, fiscal técnico e fiscal administrativo) formalmente designados, os quais atuarão de acordo com as competências estabelecidas neste Termo de Referência e nos normativos vigentes, de forma não taxativa.

7. MODELO DE EXECUÇÃO DO OBJETO

7.1. Rotina de Execução

7.1.1. Após a assinatura do Contrato, o Gestor do contrato deverá convocar a reunião inicial com todos os envolvidos na contratação. A reunião inicial poderá ser realizada de forma presencial ou remota. Na reunião inicial será disponibilizado:

a) A Carta de apresentação do Preposto, que deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE;

b) Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência;

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

c) O representante legal da contratada deverá entregar o Termo de Compromisso (ADENDO 02) e o Termo de Ciência (ADENDO 03), contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes da instituição;

d) O representante legal da contratada deverá apresentar o cronograma de execução do projeto;

e) Serão feitos esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.

7.1.2. Prazos, horários de fornecimento de bens ou prestação dos serviços:

a) O prazo de entrega dos bens é de 45 dias, contados a partir do envio da nota de empenho, em remessa única;

b) A instalação da solução demandada deverá estar implantada em até 60 dias, após o a data de recebimento dos equipamentos.

c) O(s) equipamento(s) deverão ser entregues e instalados no seguinte endereço: Superintendência de Tecnologia da Informação - STI da UFBA - Campus Universitário de Ondina, Av. Milton Santos - Ondina, Salvador – BA;

c.1) Os bens deverão ser entregues de segunda-feira a sexta-feira no horário das 08:30h às 12:00h e das 13:00h às 16:30h.

d) A entrega deverá ser agendada com antecedência mínima de 24 horas.

7.1.3. Referente à documentação mínima exigida, a Contratada deverá fornecer:

a) Manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração;

b) Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações executadas; e

c) Relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.

7.1.4. Formas de transferência de conhecimento:

a) A fim de promover a transferência de conhecimento, a implantação da solução deverá ocorrer com participação, sempre que possível, dos técnicos da UFBA que atuarão na solução. Durante a implantação da solução a equipe da CONTRATADA deverá repassar as informações para a equipe da UFBA, apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados.

Garantia, manutenção e assistência técnica

- 7.3. Os equipamentos deverão possuir garantia do fabricante por um período de 60 (sessenta) meses, com disponibilidade para chamada de manutenção no regime 24x7 (24 horas por dia, 7 dias por semana).
- 7.4. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.
- 7.5. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.
- 7.6. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.
- 7.7. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.
- 7.8. Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 1 (Um) dia útil, contados a partir da data de notificação.
- 7.9. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.
- 7.10. Na hipótese do subitem acima, o Contratado deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.
- 7.11. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.
- 7.12. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.

7.13. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

7.14. O atendimento inicial deve ser realizado no prazo máximo de 01 (uma) hora para chamados críticos e demais chamados no prazo máximo de 08 (oito) horas, observando as prioridades de atendimento, durante o período de vigência da garantia.

7.15. Entende-se por chamados críticos aqueles derivados de problemas graves, quando o ambiente estiver parado ou quando o seu desempenho impedir a execução das atividades de negócio.

8. MODELO DE GESTÃO DO CONTRATO

8.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

8.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

8.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

8.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

8.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

8.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

8.7. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

8.7.1. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

8.7.2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

8.7.3. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

8.7.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

8.7.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

8.8. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

8.8.1. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

8.9. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

8.9.1. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

8.9.2. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

8.9.3. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

8.9.4. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

8.10. O fiscal administrativo do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual. (Decreto nº 11.246, de 2022, art. 22, VII).

8.11. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do Objeto

9.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

9.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 01 (Um) dia, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

9.3. O recebimento definitivo ocorrerá no prazo de 05 (Cinco) dias, após a data de implantação da solução, sendo o ateste emitido por servidores designados pelo CONTRATANTE, que elaborarão relatório para fins de liberação do pagamento das Notas Fiscais/Faturas;

9.4. Durante a vigência deste contrato, a execução do objeto será acompanhada e fiscalizada pela Equipe de Gestão e Fiscalização Contratual, devidamente designada para esse fim, permitida a assistência de terceiros.

9.5. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até 05 (Cinco) dias.

9.6. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

9.7. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

9.8. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

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

Liquidação

9.10. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

9.10.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

9.11. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

- a) o prazo de validade;

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

- b) a data da emissão;
- c) os dados do contrato e do órgão contratante;
- d) o período respectivo de execução do contrato;
- e) o valor a pagar; e
- f) eventual destaque do valor de retenções tributárias cabíveis.

9.12. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

9.13. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta *on-line* ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

9.14. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

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

9.16. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

9.17. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

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

Prazo de pagamento

9.19. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

9.20. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice correspondente de correção monetária.

Forma de pagamento

9.21. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

9.22. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

9.23. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

9.23.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

9.24. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Cessão de crédito

9.25. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.

9.26. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

9.27. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, tudo nos termos do Parecer JL-01, de 18 de maio de 2020.

9.28. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

9.29. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do contratado.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

Forma de seleção e critério de julgamento da proposta

10.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo Menor Preço por item.

Exigências de habilitação

10.2. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Habilitação jurídica

10.3. **Pessoa física:** cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

10.4. **Empresário individual:** inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.5. **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

10.6. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI:** inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

10.7. **Sociedade empresária estrangeira:** portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

10.8. **Sociedade simples:** inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.9. **Filial, sucursal ou agência de sociedade simples ou empresária:** inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

10.10. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

10.11. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

10.12. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

10.13. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

10.14. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

10.15. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

10.16. Prova de inscrição no cadastro de contribuintes Estadual ou Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.17. Prova de regularidade com a Fazenda Estadual ou Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

10.18. Caso o fornecedor seja considerado isento dos tributos Estadual ou Municipal relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.19. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

10.20. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

10.21. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

10.22. Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

I - Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante);

II - Solvência Geral (SG) = (Ativo Total) / (Passivo Circulante + Passivo não Circulante); e

III - Liquidez Corrente (LC) = (Ativo Circulante) / (Passivo Circulante).

10.23. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

exigido para fins de habilitação capital mínimo OU patrimônio líquido mínimo de 5% do valor total estimado da contratação OU valor total estimado do item pertinente.

10.24. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

10.25. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º)

Qualificação Técnica

10.26. Efetuada a verificação referente ao cumprimento das condições de participação no certame, a habilitação das licitantes será realizada mediante a apresentação da seguinte documentação complementar:

- a) Atestado de Capacidade Técnica demonstrando que a proponente forneceu equipamentos, para pessoa física ou jurídica de direito público ou privado, e realizou a instalação, configuração e suporte técnico de solução de firewall de próxima geração compatível com o objeto deste termo de referência;
- b) Atestado de Capacidade Técnica demonstrando que a proponente realizou, para pessoa física ou jurídica de direito público ou privado, treinamento da solução de firewall de próxima geração compatível com o objeto deste termo de referência;
- c) Os atestados acima referidos deverão conter identificação do emitente, características e localização da prestação do serviço, local, data da expedição e declaração do emitente do atestado de que o serviço foi realizado a contento.
- d) O atestado deverá ser em nome da LICITANTE, e elaborados em papel timbrado da empresa emitente, contendo os seguintes dados mínimos e obrigatórios:
- e) Razão Social, CNPJ e endereço completo da empresa emitente;
- f) Razão Social da LICITANTE;
- g) Objeto do contrato;
- h) Descrição do objeto do contrato: (descrição detalhada dos serviços prestados);
- i) Local e Data de emissão do Atestado;
- j) Nome, assinatura do signatário, telefone e e-mail de contato da empresa emitente.

10.27. A empresa licitante deverá apresentar atestado(s) que comprove(m), no mínimo, atendimento a 50% dos quantitativos previstos para os itens do objeto;

10.28. Serão aceitos somatórios de atestados de capacidade técnica para comprovação, podendo os mesmos serem de fabricantes distintos.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

- 11.1. O custo estimado total da contratação é de R\$ 2.563.759,34 (Dois milhões e quinhentos e sessenta e três mil e setecentos e cinquenta e nove reais e trinta e quatro centavos), conforme custos unitários apostos no tópico 1 deste Termo de Referência.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

12.2. A contratação será atendida pela seguinte dotação:

- I) Gestão/Unidade: 15223/153038 – Universidade Federal da Bahia (UFBA)
- II) Fonte de Recursos: 1000000000 e/ou 1444000000
- III) Programa de Trabalho: 12.364.5013.8282.0029 - Reestruturação e Modernização das Instituições - No Estado Da Bahia
- IV) Elemento de Despesa: 4.4.90.52.00 - Equipamentos e Material Permanente
- V) Plano Interno: M8282G0100N - REUNI

12.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

13. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Salvador, 22 de março de 2023.

<hr/> <div>Edmilson Nascimento Integrante Requisitante</div> <div>SIAPE: 1950002</div>	<hr/> <div>Jean Mendes Integrante Técnico</div> <div>SIAPE: 3215040</div>
--	---

Autoridade Máxima da Área de TIC
<hr/> <div>Luiz Cláudio de Araújo Mendonça Superintendente SIAPE: 0285144</div>

Aprovo,

Autoridade Competente
<hr/> <div>Wagner Miranda Gomes <i>Pró-Reitor de Administração</i></div>

ADENDO 01 - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE TIC**1. DESCRITIVO TÉCNICO - INFORMAÇÕES GERAIS**

- 1.1 Abaixo serão detalhadas as especificações técnicas mínimas das soluções a serem implementadas;
- 1.2 O projeto deverá contemplar serviço de instalação, configuração e treinamento de toda a solução;
- 1.3 Os equipamentos deverão possuir garantia do fabricante por um período de 60 (sessenta) meses, com disponibilidade para chamada de manutenção no regime 24x7 (24 horas por dia, 7 dias por semana);
- 1.4 Todas as funcionalidades da solução adquirida deverão ser mantidas, mesmo após o vencimento do prazo de garantia dos equipamentos;
- 1.5 Os quantitativos gerais do projeto são:

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTD
01	Solução de Segurança – Firewall Garantia e licenciamento por 60 (sessenta) meses.	Unidade	2

1.6 ITEM 01 – FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA - FIREWALL

- 1.1.1.O Firewall deverá suportar e estar licenciado para o uso das diversas ferramentas de segurança incluídas em um Next Generation Firewall, como Antivírus, IPS, Filtragem Web, Controle de Aplicações, Proteção contra Botnets, Proteção contra Malwares Avançados e AntiSpam de Gateway.

O equipamento deverá ser fornecido com licenciamento 24x7, para habilitar todas as funcionalidades descritas neste Termo de Referência por 60 meses;

- 1.1.2.A solução a ser fornecida deverá ser preferencialmente compatível com a ferramenta FortiAnalyzer-2000E, atualmente em uso para análise de logs na STI/UFBA. Caso a contratada ofereça uma solução incompatível com a ferramenta citada, deverá fornecer outra ferramenta de análise de logs, podendo ser implementada pelo próprio firewall ou virtual, desde que seja semelhante ou superior.

1.1.3.CARACTERÍSTICAS DE HARDWARE:

- 1.1.3.1. Deve suportar, no mínimo, 190 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, considerando pacotes de 512 bytes
- 1.1.3.2. Deve suportar, no mínimo, 21 Gbps de throughput IPS
- 1.1.3.3. Deve suportar, no mínimo, 55 Gbps de throughput de VPN IPSec
- 1.1.3.4. Deve suportar, no mínimo, 10 Gbps de throughput de VPN SSL

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

- 1.1.3.5. Deve suportar, no mínimo, 11 Gbps de throughput de Inspeção SSL
- 1.1.3.6. Deve suportar, no mínimo, 33 Gbps de throughput de Controle de Aplicação
- 1.1.3.7. Deve suportar, no mínimo, 14.5 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware.
- 1.1.3.8. Suporte a, no mínimo, 11 milhões de conexões simultâneas;
- 1.1.3.9. Deve suportar o gerenciamento de no mínimo 190 Switches do mesmo fabricante por equipamento;
- 1.1.3.10. Suporte a, no mínimo, 700 mil novas conexões por segundo
- 1.1.3.11. Estar licenciado para, ou suportar sem o uso de licença, 15 mil túneis de VPN IPSEC Site-to-Site simultâneos
- 1.1.3.12. Estar licenciado para, ou suportar sem o uso de licença, 90 mil túneis de clientes VPN IPSEC simultâneos
- 1.1.3.13. Estar licenciado para, ou suportar sem o uso de licença, 5 mil clientes de VPN SSL simultâneos
- 1.1.3.14. Caso seja necessário fornecimento de licenças para prover o uso de VPN para a quantidade de usuários solicitada, a licença deverá operar em caráter perpétuo
- 1.1.3.15. Possuir ao menos 8 interfaces 1Gbps SFP
- 1.1.3.16. Possuir ao menos 14 interfaces 1Gbps RJ-45
- 1.1.3.17. Possuir ao menos 10 Interfaces SFP28 de até 25Gbps, permitindo também o uso de transceivers 10Gbps SFP+ e Gigabit SFP, com fornecimento de 2(dois) transceivers SFP + (SR 10GE);
- 1.1.3.18. Possuir ao menos 4 Interfaces 40Gbps compatível com transceivers QSFP+;
- 1.1.3.19. Deve possuir disco Onboard Storage do tipo Solid State Drive NVMe (SSD) de, no mínimo, 480 (quatrocentos e oitenta) GB de armazenamento do sistema operacional e registro de logs
- 1.1.3.20. Deverá possuir interface USB 3.0 para exportação de backups;
- 1.1.3.21. Deverá possuir interface do tipo console para utilização de CLI
- 1.1.3.22. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
- 1.1.3.23. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance
- 1.1.3.24. Possuir no máximo 2 RU de altura e acompanhar kit de instalação em rack
- 1.1.3.25. Deverá possuir fontes de alimentação internas redundantes, do tipo hot-swappable;
- 1.1.3.26. O fabricante ofertado deve estar posicionado no quadrante "Leader" do quadrante mágico do Gartner de 2022, na categoria Network Firewalls.

1.1.4. CARACTERÍSTICAS GERAIS DE FUNCIONALIDADES

- 1.1.4.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
- 1.1.4.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 1.1.4.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- 1.1.4.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 1.1.4.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
- 1.1.4.6. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
- 1.1.4.7. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

- 1.1.4.8. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
- 1.1.4.9. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
- 1.1.4.10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 1.1.4.11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
- 1.1.4.12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
- 1.1.4.13. Os dispositivos de proteção de rede devem suportar sFlow;
- 1.1.4.14. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
- 1.1.4.15. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 1.1.4.16. Deve suportar NAT dinâmico (Many-to-1);
- 1.1.4.17. Deve suportar NAT dinâmico (Many-to-Many);
- 1.1.4.18. Deve suportar NAT estático (1-to-1);
- 1.1.4.19. Deve suportar NAT estático (Many-to-Many);
- 1.1.4.20. Deve suportar NAT estático bidirecional 1-to-1;
- 1.1.4.21. Deve suportar Tradução de porta (PAT);
- 1.1.4.22. Deve suportar NAT de Origem;
- 1.1.4.23. Deve suportar NAT de Destino;
- 1.1.4.24. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- 1.1.4.25. Deve poder combinar NAT de origem e NAT de destino na mesma política
- 1.1.4.26. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 1.1.4.27. Deve suportar NAT64 e NAT46;
- 1.1.4.28. Deve implementar o protocolo ECMP;
- 1.1.4.29. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 1.1.4.30. Enviar log para sistemas de monitoração externos, simultaneamente;
- 1.1.4.31. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- 1.1.4.32. Proteção anti-spoofing;
- 1.1.4.33. Suportar otimização do tráfego entre dois equipamentos;
- 1.1.4.34. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 1.1.4.35. Para IPv6, deve suportar roteamento estático e dinâmico (RIPng, OSPFv3, BGP4+);
- 1.1.4.36. Suportar OSPF graceful restart;
- 1.1.4.37. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 1.1.4.38. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- 1.1.4.39. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 1.1.4.40. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 1.1.4.41. Suporte a configuração de alta disponibilidade (HA) Ativo/Passivo e Ativo/Ativo: Em modo transparente;
- 1.1.4.42. Suporte a configuração de alta disponibilidade (HA) Ativo/Passivo e Ativo/Ativo: Em layer 3;
- 1.1.4.43. Suporte a configuração de alta disponibilidade (HA) Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;
- 1.1.4.44. A configuração em alta disponibilidade (HA) deve sincronizar: Sessões;
- 1.1.4.45. A configuração em alta disponibilidade (HA) deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
- 1.1.4.46. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

- 1.1.4.47. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
- 1.1.4.48. O HA deve possibilitar monitoração de falha de link;
- 1.1.4.49. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
- 1.1.4.50. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;
- 1.1.4.51. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
- 1.1.4.52. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado a exportar configuração dos sistemas virtuais (contextos) por ambas as interfaces;
- 1.1.4.53. Controle, inspeção e descryptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 1.1.4.54. O console de administração deve suportar pelo menos inglês, espanhol e português.
- 1.1.4.55. A solução deve oferecer suporte à integração nativa de equipamentos de proteção de e-mail, firewall de aplicativos, proxy, cache e ameaças avançadas.
- 1.1.4.56. Deverá ser comprovado que a solução ofertada foi aprovada no conjunto de critérios de avaliação contido nos testes da NSS Labs, da ICSA Labs, ou por meio de certificação similar, que cumpra a mesma finalidade ou que ateste as mesmas funcionalidades.

1.1.5.FUNCIONALIDADES DE CONTROLE POR POLÍTICAS

- 1.1.5.1. Deverá suportar controles por zona de segurança;
- 1.1.5.2. Controles de políticas por porta e protocolo;
- 1.1.5.3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 1.1.5.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 1.1.5.5. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;
- 1.1.5.6. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;
- 1.1.5.7. Ele deve suportar a automação de situações como detecção de equipamentos comprometidos, status do sistema, alterações de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um computador, execução de scripts ou funções em nuvem pública.
- 1.1.5.8. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);
- 1.1.5.9. Deve suportar o protocolo padrão da indústria VXLAN;
- 1.1.5.10. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall
- 1.1.5.11. Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução
- 1.1.5.12. A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteção de e-mail e firewall de aplicativos da Web.

1.1.6.FUNCIONALIDADES DE CONTROLE DE APLICAÇÃO

- 1.1.6.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- 1.1.6.2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

- 1.1.6.3. Reconhecer pelo menos as seguintes aplicações: BitTorrent, gnutella, Skype, facebook, LinkedIn, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
 - 1.1.6.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
 - 1.1.6.5. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
 - 1.1.6.6. Identificar o uso de táticas evasivas via comunicações criptografadas;
 - 1.1.6.7. Atualizar a base de assinaturas de aplicações automaticamente;
 - 1.1.6.8. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
 - 1.1.6.9. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
 - 1.1.6.10. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
 - 1.1.6.11. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
 - 1.1.6.12. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule etc.) possuindo granularidade de controle/políticas para eles;
 - 1.1.6.13. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat etc.) possuindo granularidade de controle/políticas para os mesmos;
 - 1.1.6.14. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
 - 1.1.6.15. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;
 - 1.1.6.16. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol etc.);
 - 1.1.6.17. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
 - 1.1.6.18. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
 - 1.1.6.19. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente
- 1.1.7.FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS
- 1.1.7.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
 - 1.1.7.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
 - 1.1.7.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
 - 1.1.7.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
 - 1.1.7.5. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
 - 1.1.7.6. Deve permitir o bloqueio de vulnerabilidades;

- 1.1.7.7. Deve incluir proteção contra-ataques de negação de serviços;
 - 1.1.7.8. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo;
 - 1.1.7.9. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo;
 - 1.1.7.10. Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;
 - 1.1.7.11. Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP;
 - 1.1.7.12. Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados;
 - 1.1.7.13. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood etc.;
 - 1.1.7.14. Detectar e bloquear a origem de portscans;
 - 1.1.7.15. Bloquear ataques efetuados por worms conhecidos;
 - 1.1.7.16. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
 - 1.1.7.17. Possuir assinaturas para bloqueio de ataques de buffer overflow;
 - 1.1.7.18. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
 - 1.1.7.19. Identificar e bloquear comunicação com botnets;
 - 1.1.7.20. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
 - 1.1.7.21. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
 - 1.1.7.22. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
 - 1.1.7.23. Os eventos devem identificar o país de onde partiu a ameaça;
 - 1.1.7.24. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
 - 1.1.7.25. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
 - 1.1.7.26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança etc., ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
 - 1.1.7.27. Suportar e estar licenciado com proteção contra-ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante;
- 1.1.8.FUNCIONALIDADES DE FILTRO DE URL
- 1.1.8.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
 - 1.1.8.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
 - 1.1.8.3. Suportar proxy Web transparente e Explicit Web Proxy;
 - 1.1.8.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
 - 1.1.8.5. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
 - 1.1.8.6. Possuir pelo menos 60 categorias de URLs;
 - 1.1.8.7. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
 - 1.1.8.8. Permitir a customização de página de bloqueio;
 - 1.1.8.9. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site).

1.1.9.FUNCIONALIDADES DE IDENTIFICAÇÃO DE USUÁRIOS

- 1.1.9.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
- 1.1.9.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.1.9.3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede etc.;
- 1.1.9.4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.1.9.5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 1.1.9.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- 1.1.9.7. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 1.1.9.8. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- 1.1.9.9. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução;
- 1.1.9.10. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

1.1.10. FUNCIONALIDADES DE QOS E TRAFFIC SHAPING

- 1.1.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
- 1.1.10.2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
- 1.1.10.3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
- 1.1.10.4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
- 1.1.10.5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- 1.1.10.6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
- 1.1.10.7. O QoS deve possibilitar a definição de tráfego com banda garantida;
- 1.1.10.8. O QoS deve possibilitar a definição de tráfego com banda máxima;
- 1.1.10.9. O QoS deve possibilitar a definição de fila de prioridade;
- 1.1.10.10. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
- 1.1.10.11. Suportar modificação de valores DSCP para o Diffserv;
- 1.1.10.12. Suportar priorização de tráfego usando informação de Type of Service;
- 1.1.10.13. Deve suportar QOS (traffic-shaping), em interface agregadas ou redundantes.

1.1.11. FUNCIONALIDADES DE FILTRO DE DADOS

- 1.1.11.1. Permitir a criação de filtros para arquivos e dados pré-definidos;
- 1.1.11.2. Os arquivos devem ser identificados por extensão e tipo;

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

- 1.1.11.3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF etc.) identificados sobre aplicações (HTTP, FTP, SMTP etc.);
- 1.1.11.4. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 1.1.11.5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 1.1.11.6. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

1.1.12. FUNCIONALIDADES DE ZTNA (ZERO TRUST NETWORK ACCESS)

- 1.1.12.1. A solução deverá permitir a implementação futura de ZTNA através do licenciamento dos Endpoints, permitindo a ativação das seguintes funcionalidades:
 - 1.1.12.1.1. Deverá permitir ao administrador a solicitação enforcement de identificação do usuário no login, de modo que o usuário necessite realizar uma confirmação de identidade através de no mínimo:
 - 1.1.12.1.1.1. Informação pessoal do sistema operacional;
 - 1.1.12.1.1.2. LinkedIn;
 - 1.1.12.1.1.3. Google;
 - 1.1.12.1.1.4. Salesforce;
 - 1.1.12.1.2. Deverá permitir aplicar perfis de segurança baseado em status de serviços do endpoint, permitindo que seja atribuído um perfil de acesso para os endpoints baseado em no mínimo:
 - 1.1.12.1.2.1. DHCP Server: Atribui um perfil de segurança se o endpoint estiver conectado a um servidor DHCP específico
 - 1.1.12.1.2.2. DNS Server: Atribui um perfil de segurança se o endpoint estiver conectado a um servidor DNS específico
 - 1.1.12.1.2.3. Conexão ao Servidor: Atribui um perfil de segurança se o endpoint estiver online e com sua versão atualizada de acordo com o servidor de gerenciamento
 - 1.1.12.1.2.4. Local IP/Subnet: Atribui um perfil de segurança se o endpoint estiver em um range de IPs específico
 - 1.1.12.1.2.5. Default Gateway: Atribui um perfil de segurança se o endpoint estiver enviando informações para um gateway de internet específico, permitindo também a configuração de endereço MAC do Gateway.
 - 1.1.12.1.2.6. Ping Server: Atribui um perfil de segurança se o endpoint conseguir enviar um ping para um servidor específico de rede
 - 1.1.12.1.2.7. VPN Tunel: Atribui um perfil de segurança se o endpoint estiver acessando a rede através de um Túnel de VPN, deve ser permitida a escolha de túnel de VPN para cada perfil
 - 1.1.12.1.3. Deve permitir a atribuição de usuários ou grupos de usuários a políticas de acesso.

1.1.13. GEOLOCALIZAÇÃO

- 1.1.13.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 1.1.13.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- 1.1.13.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

1.1.14. FUNCIONALIDADES DE VPN

- 1.1.14.1. Suportar VPN Site-to-Site e Cliente-To-Site;
- 1.1.14.2. Suportar IPSec VPN;
- 1.1.14.3. Suportar SSL VPN;
- 1.1.14.4. A VPN IPSec deve suportar Autenticação MD5 e SHA-1;
- 1.1.14.5. A VPN IPsec deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.
- 1.1.14.6. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

- 1.1.14.7. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 1.1.14.8. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 1.1.14.9. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSEC IPv6;
- 1.1.14.10. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 1.1.14.11. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 1.1.14.12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 1.1.14.13. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
- 1.1.14.14. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- 1.1.14.15. Deverá manter uma conexão segura com o portal durante a sessão;
- 1.1.14.16. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior);
- 1.1.14.17. Deve suportar Auto Discovery Virtual Private Network (ADVPN);
- 1.1.14.18. Deve suportar agregação de túneis IPSEC;
- 1.1.14.19. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSEC;
- 1.1.14.20. A VPN IPSEC deve suportar Forward Error Correction (FEC);
- 1.1.14.21. Deve suportar TLS 1.3 em VPN SSL.

1.1.15. FUNCIONALIDADES DE SD-WAN

- 1.1.15.1. Deve implementar balanceamento de link por hash do IP de origem;
- 1.1.15.2. Deve implementar balanceamento de link por hash do IP de origem e destino;
- 1.1.15.3. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.
- 1.1.15.4. Deve implementar balanceamento de link por custo configurado do link.
- 1.1.15.5. Deve suportar o balanceamento de, no mínimo, 256 links;
- 1.1.15.6. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSEC;
- 1.1.15.7. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- 1.1.15.8. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde;
- 1.1.15.9. Deve suportar Zero-Touch Provisioning;
- 1.1.15.10. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes;
- 1.1.15.11. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
- 1.1.15.12. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;
- 1.1.15.13. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS
- 1.1.15.14. Suportar UDP Hole Punching em arquitetura ADVPN;
- 1.1.15.15. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado;
- 1.1.15.16. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo;
- 1.1.15.17. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN;

1.1.15.18. Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link.

1.1.16. FUNCIONALIDADES DE WIRELESS CONTROLLER

- 1.1.16.1. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
- 1.1.16.2. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;
- 1.1.16.3. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
- 1.1.16.4. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
- 1.1.16.5. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
- 1.1.16.6. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
- 1.1.16.7. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes devem ser tunelados até o controlador wireless;
- 1.1.16.8. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
- 1.1.16.9. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
- 1.1.16.10. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;
- 1.1.16.11. A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;
- 1.1.16.12. A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das subredes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados localmente na interface do ponto de acesso;
- 1.1.16.13. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
- 1.1.16.14. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado dBm;
- 1.1.16.15. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
- 1.1.16.16. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
- 1.1.16.17. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

- 1.1.16.18. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de off-channel/Background scanning. Quando realizada através de off-channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
- 1.1.16.19. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
- 1.1.16.20. A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
- 1.1.16.21. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
- 1.1.16.22. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
- 1.1.16.23. A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
- 1.1.16.24. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
- 1.1.16.25. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 1.1.16.26. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
- 1.1.16.27. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
- 1.1.16.28. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
- 1.1.16.29. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
- 1.1.16.30. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
- 1.1.16.31. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
- 1.1.16.32. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
- 1.1.16.33. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;
- 1.1.16.34. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

- 1.1.16.35. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
- 1.1.16.36. A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;
- 1.1.16.37. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;
- 1.1.16.38. A solução deve implementar regras de firewall (stateful) para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que deve usar como critério endereços de origem e destino (IPv4 e IPv6), portas e protocolos;
- 1.1.16.39. A solução deve implementar recurso de web filtering para controle de websites acessados na rede wireless. Deve possuir uma base de conhecimento para categorização dos sites e permitir configurar quais categorias de sites serão permitidos e bloqueados para cada perfil de usuário e SSID;
- 1.1.16.40. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de Inspeção SSL que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle. Deve permitir o funcionamento deste recurso e a atualização periódica da base de aplicações durante todo o período de garantia da solução;
- 1.1.16.41. A base de reconhecimento de aplicações através de Inspeção SSL deve identificar com, no mínimo, 1500 (mil e quinhentas) aplicações;
- 1.1.16.42. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de Inspeção SSL;
- 1.1.16.43. A solução deve ainda, através da técnica de Inspeção SSL, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;
- 1.1.16.44. "A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:
- 1.1.16.45. - Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);
- 1.1.16.46. - Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
- 1.1.16.47. - ASLEAP;
- 1.1.16.48. - Null Probe Response / Null SSID Probe Response;
- 1.1.16.49. - Long Duration;
- 1.1.16.50. - Ataques contra Wireless Bridges;
- 1.1.16.51. - Weak WEP;
- 1.1.16.52. - Invalid MAC OUI;
- 1.1.16.53. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;
- 1.1.16.54. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
- 1.1.16.55. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
- 1.1.16.56. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
- 1.1.16.57. Deve implementar autenticação administrativa através do protocolo RADIUS;
- 1.1.16.58. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 1.1.16.59. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
- 1.1.16.60. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
- 1.1.16.61. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

- 1.1.16.62. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
- 1.1.16.63. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
- 1.1.16.64. A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
- 1.1.16.65. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
- 1.1.16.66. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
- 1.1.16.67. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
- 1.1.16.68. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
- 1.1.16.69. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
- 1.1.16.70. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
- 1.1.16.71. A solução deve garantir que usuários se autenticuem em captive portal que faça uso de endereço IPv6;
- 1.1.16.72. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
- 1.1.16.73. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
- 1.1.16.74. A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;
- 1.1.16.75. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
- 1.1.16.76. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
- 1.1.16.77. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
- 1.1.16.78. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
- 1.1.16.79. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
- 1.1.16.80. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
- 1.1.16.81. A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;
- 1.1.16.82. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
- 1.1.16.83. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
- 1.1.16.84. A solução deve permitir a captura de pacotes na rede wireless e exportá-los em arquivos no formato .pcap;
- 1.1.16.85. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela

TERMO DE REFERÊNCIA - AQUISIÇÕES - LICITAÇÃO

gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

- 1.1.16.86. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
- 1.1.16.87. A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
- 1.1.16.88. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
- 1.1.16.89. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;
- 1.1.16.90. A solução deve possuir ferramentas de diagnósticos e debug;
- 1.1.16.91. A solução deve suportar comunicação com elementos externos através de APIs;
- 1.1.16.92. A solução deverá ser compatível e gerenciar pontos de acesso do mesmo fabricante;
- 1.1.16.93. O fabricante ofertado deve estar posicionado no quadrante “Leader” do quadrante mágico do Gartner de 2021, na categoria WAN Edge Infrastructure.



SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA BAHIA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

ADENDO 02
TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO

O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não.

Referência: Art. 18, Inciso V, alínea “a” da IN SGD/ME Nº 94/2022.

Universidade Federal da Bahia, sediada na Av. Milton Santos, s/nº - Ondina, Salvador - BA, CEP 40170-110, CNPJ n.º 15.180.714/0001-04, doravante **denominado CONTRATANTE**, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n.º <CNPJ>, doravante denominada **CONTRATADA**;

CONSIDERANDO que, em razão do **CONTRATO N.º <nº do contrato>** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;

Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO**, doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.



SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA BAHIA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3 – DA INFORMAÇÃO SIGILOSA

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

4 – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer



SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA BAHIA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5 – DIREITOS E OBRIGAÇÕES

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

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

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

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

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

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

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física



SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA BAHIA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6 – VIGÊNCIA

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

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

8 – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios



SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA BAHIA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9 – FORO

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



SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA BAHIA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

10 – ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA	CONTRATANTE
<hr/> <div><Nome> <Qualificação></div>	<hr/> <div><Nome> Matrícula: xxxxxxxx</div>
TESTEMUNHAS	
<hr/> <div><Nome> <Qualificação></div>	<hr/> <div><Nome> <Qualificação></div>

Salvador, BA, <dia> de <mês> de <ano>.

ADENDO 03

Termo de Ciência e Manutenção de Sigilo

Contrato N°:			
Objeto:			
Contratante:			
Gestor do Contrato:		Matr.:	
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Ciência e Manutenção de Sigilo, e as normas de segurança vigentes na CONTRATANTE.

Salvador, _____ de _____ de 20_____.

CONTRATADA
Funcionários

<Nome>
Matrícula: <Matr.>

<Nome>
Matrícula: <Matr.>

<Nome>
Matrícula: <Matr.>

<Nome>
Matrícula: <Matr.>

<Nome>
Matrícula: <Matr.>

<Nome>
Matrícula: <Matr.>

<Nome>
Matrícula: <Matr.>

<Nome>
Matrícula: <Matr.>

<Nome>
Matrícula: <Matr.>

<Nome>
Matrícula: <Matr.>