

Termo de Referência 16/2023

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
16/2023	153038-UNIVERSIDADE FEDERAL DA BAHIA-UF/BA	GERALDO EDMUNDO BARBOSA NETO	27/10/2023 16:49 (v 8.0)
Status	CONCLUIDO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação.		23066.040281/2023-79

1. Definição do objeto

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição eventual de Licenças de Softwares para atender às necessidades das diferentes unidades da Universidade Federal da Bahia, tanto para a área administrativa, quanto para a área acadêmica e de pesquisa, conforme condições, quantidades, exigências e estimativas, estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	LICENÇA DE PONTO DE ACESSO PARA A CONTROLADORA VIRTUAL SMART ZONE ESSENTIALS. Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador - Licença de ponto de acesso para a controladora virtual Smart zone Essentials. (Part number L09-0001-SG00)	27472	Und.	500	R\$ 508,91	R\$ 254.455,00
	LICENÇA DO PACOTE DE SOFTWARES ADOBE CREATIVE CLOUD VIP, Versão: Última versão disponível, Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software					

2	Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software, Última versão disponível - Licença de uso educacional da Suíte Adobe Creative Cloud for Teams Device Multiplataforma /Subscrição por 36 (trinta e seis) meses. Catser 27502	27502	Und.	69	R\$ 5.789,10	R\$ 399.447,90
3	LICENÇA DO SOFTWARE AUTODESK AUTOCAD REVIT LT, Última versão disponível, Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software Cessão temporária de direitos sobre programas de computador locação de software, Subscrição por 36 (trinta e seis) meses. Catser 27502	27502	Und.	5	R\$ 7.008,50	R\$ 35.042,50
4	LICENÇA DO SOFTWARE DE SOLUÇÃO DE ANTIVÍRUS CORPORATIVO, Última versão disponível, Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software, Última versão disponível - Subscrição por 36 (trinta e seis) meses. Catser 27502	27502	Und.	1000	R\$ 161,49	R\$ 161.490,00
5	LICENÇA DO SOFTWARE PARA SOLUÇÃO DE BACKUP PARA SERVIDORES, Versão: Última versão disponível. Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software. Cessão Temporária de Direitos Sobre Programas de	27502	Und.	1	R\$ 29.747,50	R\$ 29.747,50

	Computador Locação de Software, pelo período de 36 meses. Catser 27502					
6	<p>LICENÇA DO SOFTWARE SKETCHUP LAB EDUCACIONAL, VERSÃO: Versão: Última versão disponível. Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software</p> <p>Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software, Última versão disponível - Subscrição por 36 (trinta e seis) meses. Catser 27502</p>	27502	Und.	30	R\$ 306,25	R\$ 9.187,50
7	<p>LICENÇA PERPÉTUA DO SOFTWARE EDUCACIONAL CORELDRAW GRAPHICS SUITE, Versão: Última versão disponível, com atualizações por 02 anos. Licenciamento de direitos permanentes de uso de software para estação de trabalho.</p> <p>Aquisição de licença de uso do software coreldraw graphics suíte, versão: última versão disponível, período de 02 anos, inclusa a garantia, suporte e atualizações. Catser 27456</p>	27456	Und.	13	R\$ 1.155,78	R\$ 15.025,14
8	<p>LICENÇA PERPÉTUA DO SOFTWARE EDUCACIONAL DO SOFTWARE RHINO-EDIÇÃO BRASIL - Versão: Última versão disponível.</p> <p>Licenciamento de direitos permanentes de uso de software para estação de trabalho.</p> <p>Licenciamento de direitos permanentes de uso de software para estação de trabalho.</p> <p>Licença educacional Edição Brasil - Versão: Última versão disponível. LAB KIT</p>	27456	Und.	3	R\$ 1.025,00	R\$ 3.075,00

	– 30 usuários para usar o Rhino nos computadores em uma única sala de aula ou laboratório. Catser 27456					
9	<p>LICENÇA PERPÉTUA DO SOFTWARE MICROSOFT OFFICE PROFESSIONAL PLUS EDUCACIONAL - VERSÃO: ÚLTIMA VERSÃO DISPONÍVEL,</p> <p>Licenciamento de direitos permanentes de uso de software para estação de trabalho.</p> <p>Microsoft Office Professional Plus Educacional Versão: Última versão disponível para PC – O pacote deve incluir versões completas do Word, Excel, PowerPoint, OneNote, Access e Publisher – Versão 32/64 bits. Catser 27456</p>	27456	Und.	648	R\$ 141,16	R\$ 91.471,68
10	<p>LICENÇA PERPÉTUA DO SOFTWARE MICROSOFT SQL SERVER, Versão: Última versão disponível.</p> <p>Licenciamento de direitos permanentes de uso de software para servidor.</p> <p>Licenciamento de direitos permanentes de uso de software para servidor. Catser 27464</p>	27464	Und.	01	R\$ 18.000,00	R\$ 18.000,00
11	<p>LICENÇA PERPÉTUA DO SOFTWARE MICROSOFT WINDOWS SERVER 2022 REMOTE DESKTOP SERVICES - 1 USER CAL - VERSÃO: ÚLTIMA VERSÃO DISPONÍVEL,</p> <p>Licenciamento de Direitos Permanentes de Uso de Software para Estação de Trabalho. Catser 27456</p>	27456	Und.	150	R\$ 234,36	R\$ 35.154,00

12	<p>LICENÇA PERPÉTUA DO SOFTWARE MICROSOFT WINDOWS SERVER DATACENTER PER CORE, Licenciamento de Direitos Permanentes de Uso de Software para Servidor.</p> <p>Licença Perpétua Do Software Microsoft Windows Server Datacenter Per Core 2 Licences - Versão: Última Versão Disponível. Catmat: 27464</p>	27464	Und.	30	R\$ 7.667,65	R\$ 230.029,50
13	<p>LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA SERVIDOR - CONTROLADORA VIRTUAL SMART ZONE ESSENTIALS.</p> <p>Licenciamento de direitos permanentes de uso de software para servidor - Controladora Virtual Smartzone Essentials. (Part number L09-VSCG-WW00)</p>	27464	Und.	01	R\$ 7.914,14	R\$ 7.914,14
14	<p>SISTEMA DE GESTÃO LGPD PROTEGON, VERSÃO: Última versão disponível, Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software</p> <p>Cessão temporária de direitos sobre programas de computador locação de software. Subscrição por 12 (doze) meses. Catser 27502</p>	27502	Und.	1	R\$ 9.000,00	R\$ 9.000,00
15	<p>SOFTWARE AUTODESK ARCHITECTURE ENGINEERING & CONSTRUCTION COLLECTION, Última versão disponível, Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software</p> <p>Cessão temporária de direitos</p>	27502	Und.	2	R\$ 33.673,00	R\$ 67.346,00

sobre programas de computador locação de software, Subscrição por 36 (trinta e seis) meses. Catser 27502					
----------------------------------------------------------------------------------------------------------	--	--	--	--	--

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 12 (doze meses), podendo ser prorrogado por interesse das partes até o limite de 36 (trinta e seis) meses, na forma dos artigos 106 e 107 da Lei nº 14.133, de 1º de abril de 2021.

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

2. Fundamentação 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.

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

I) ID PCA no PNCP: 15180714000104-0-000001/2024

II) Data de publicação no PNCP: 19/05/2023

III) Id do item no PCA: 144

IV) Classe/Grupo: 182 - SERVIÇOS DE LICENCIAMENTO E CONTRATOS DE TRANSFERÊNCIA DE TECNOLOGIA

V) Identificador da Futura Contratação: 153038-212/2023

3. Descrição da solução

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

3.1. Aquisição eventual de Licenças de Softwares para atender às necessidades das diferentes unidades da Universidade Federal da Bahia, tanto para a área administrativa, quanto para a área acadêmica e de pesquisa, conforme condições, quantidades, exigências e estimativas, estabelecidas neste instrumento.

4. Requisitos da contratação

4. REQUISITOS DA CONTRATAÇÃO

Sustentabilidade:

4.1. A contratação deverá atender a critérios de sustentabilidade ambiental que a legislação determinar, a exemplo da IN nº 01, de 19 de janeiro de 2010, da SLTI/MPOG, no que couber, ou prover alternativas para verificação de sua aplicabilidade.

4.2 Todos os documentos ou artefatos gerados pela contratada, salvo manifestação explícita deverão ser entregues em formato digital.

Subcontratação, Consórcio e Cooperativas

4.3 Não será admitida a subcontratação do objeto licitatório.

4.4 Não poderão participar desta licitação entidades empresariais que estejam reunidas em consórcio e sociedades cooperativas.

Garantia da contratação

4.5. Não haverá exigência da garantia da contratação dos artigos 96 e seguintes da Lei nº 14.133, de 2021.

Requisitos de Capacitação

4.6 Não se aplica para o objeto da presente contratação.

Requisitos de Projeto e de Implementação

4.7 Não se aplica para o objeto da presente contratação.

Requisitos Legais

- Lei nº 14.133, de 1 de abril de 2021, que institui normas para licitações e contratos da Administração Pública;
 - Lei nº 8.248, de 23 de outubro de 1991, que dispõe sobre a capacitação e competitividade do setor de informática e automação;
 - Decreto nº 7.010, de 16 de novembro de 2009, dispõe sobre capacitação e competitividade do setor de tecnologia da informação;
 - Decreto nº 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública Federal;
 - 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;
 - Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
- Instrução Normativa Nº 65, de 07 de Julho de 2021, do Ministério da Economia, dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.
- Instrução Normativa SGD/MGI nº 6, de 29 de março de 2023, que regulamenta os requisitos e procedimentos para aprovação de contratações ou de formação de atas de registro de preços, a serem efetuados por órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo federal, relativos a bens e serviços de tecnologia da informação e comunicação - TIC.

Requisitos de Implantação

4.8 Não se aplica para o objeto da presente contratação.

Requisitos de Garantia

4.9 A CONTRATADA deverá prestar assistência técnica durante todo o **período de garantia do software**;

5.0 A abertura de chamados de suporte não poderá ser limitada.

Requisitos de Experiência Profissional

5.1 Não se aplica para o objeto da presente contratação.

Requisitos de Formação da Equipe

5.2 Não se aplica para o objeto da presente contratação.

Requisitos de Metodologia de Trabalho

5.3 Não se aplica para o objeto da presente contratação.

Requisitos de Segurança da Informação

5.4 A CONTRATADA deverá manter o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que venham a ser fornecidos ou que venha a ter acesso em razão da execução dos serviços, não podendo, sob qualquer pretexto, revelá-los, divulgá-los, reproduzi-los ou deles dar conhecimento a quaisquer terceiros.

Outros Requisitos Aplicáveis

5.5 A presente seção destaca aqueles requisitos que devem ser considerados ao longo do planejamento da contratação, para se assegurar o alcance dos objetivos pretendidos com a aquisição, conforme a seguir:

- a) Aderência às políticas de segurança da UFBA;
- b) Garantia de atualização das versões e corretivos, tendo como finalidade a padronização, garantindo a continuidade dos serviços finalísticos da UFBA;
- c) A solução deverá ser compatível com as demandas previstas no PAC e PDTI;
- d) A solução deverá estar alinhada, na medida do possível, com a Lei Geral de Proteção de Dados Pessoais (Lei N° 13.709, de 14 de agosto de 2018). Em especial, aos princípios de segurança (Art. 6º, inciso VII) e prevenção (Art. 6º, inciso VIII).

5. Modelo de execução do objeto

5. MODELO DE EXECUÇÃO DO OBJETO

Condições de Entrega

5.1. As licenças do software contratado, bem como suas chaves de ativação, devem ser disponibilizadas em até 15 dias corridos após a emissão da Ordem de Serviço, podendo ser prorrogado por igual período desde que justificado pela CONTRATADA e autorizado pela CONTRATANTE;

5.2. Os itens deverão ser entregues via download, devendo o link e demais instruções ser enviadas para o e-mail licencas.softwares@ufba.br;

5.3. Para fins do período de licenciamento, a contagem do prazo iniciará a partir da aplicação do código de ATIVAÇÃO do software, portanto, não se confunde com a data de fornecimento do software; e

5.4. A contratada deve, também, informar o canal oficial para suporte.

Garantia, manutenção e assistência técnica

5.5. O período de licenciamento da subscrição e garantia para as licenças perpétuas deverão corresponder à tabela abaixo, contados a partir da data de aplicação do código de ativação do software. Essa aplicação deve ocorrer num prazo máximo 30 dias da data de fornecimento do software e do seu código de ativação.

Id.	Serviço	Licença	Período/Garantia
4005000000040	LICENÇA DE PONTO DE ACESSO PARA A CONTROLADORA VIRTUAL SMARTZONE ESSENTIALS	Subscrição	60 meses
4006000000013	LICENÇA DO PACOTE DE SOFTWARES ADOBE CREATIVE CLOUD VIP	Subscrição	36 meses
4006000000034	LICENÇA DO SOFTWARE AUTODESK AUTOCAD REVIT LT	Subscrição	36 meses
4006000000009	LICENÇA DO SOFTWARE DE SOLUÇÃO DE ANTIVÍRUS CORPORATIVO	Subscrição	36 meses

4006000000053	LICENÇA DO SOFTWARE PARA SOLUÇÃO DE BACKUP PARA SERVIDORES	Subscrição	36 meses
4006000000014	LICENÇA DO SOFTWARE SKETCHUP LAB EDUCACIONAL,	Subscrição	36 meses
4005000000039	LICENÇA PERPÉTUA DO SOFTWARE EDUCACIONAL CORELDRAW GRAPHICS SUITE	Perpétua	24 meses
4005000000030	LICENÇA PERPÉTUA DO SOFTWARE EDUCACIONAL DO SOFTWARE RHINO-EDIÇÃO BRASIL	Perpétua	-
4005000000003	LICENÇA PERPÉTUA DO SOFTWARE MICROSOFT OFFICE PROFESSIONAL PLUS EDUCACIONAL - VERSÃO: ÚLTIMA VERSÃO DISPONÍVEL	Perpétua	-
4006000000052	LICENÇA PERPÉTUA DO SOFTWARE MICROSOFT SQL SERVER	Perpétua	-
4005000000031	LICENÇA PERPÉTUA DO SOFTWARE MICROSOFT WINDOWS SERVER 2022 REMOTE DESKTOP SERVICES - 1 USER CAL - VERSÃO: ÚLTIMA VERSÃO DISPONÍVEL	Perpétua	-
4005000000036	LICENÇA PERPÉTUA DO SOFTWARE MICROSOFT WINDOWS SERVER DATACENTER PER CORE	Perpétua	-
4005000000041	LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA SERVIDOR - CONTROLADORA VIRTUAL SMARTZONE ESSENTIALS. (Part number L09-VSCG-WW00)	Subscrição	60 meses
4006000000054	SISTEMA DE GESTÃO LGPD PROTEGON, VERSÃO	Subscrição	12 meses
4006000000035	SOFTWARE AUTODESK ARCHITECTURE ENGINEERING & CONSTRUCTION COLLECTION	Subscrição	36 meses

6. Modelo de gestão do contrato

6. MODELO DE GESTÃO DO CONTRATO

6.1. O contrato ou instrumento equivalente 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.

6.2. 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.

6.3. 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.

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

6.5. 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.

6.6. 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](#)).

6.7. 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](#));

6.7.1. 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](#));

6.7.2. Identificada qualquer inexistência 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](#));

6.7.3. 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](#)).

6.7.4. 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](#)).

6.7.5. 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](#)).

6.8. 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](#)).

6.8.1. 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](#)).

6.9. 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](#)).

6.9.1. 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](#)).

6.9.2. 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](#)).

6.9.3. 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](#)).

6.9.4. 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](#)).

6.10. 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](#)).

6.11. 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](#)).

7. Critérios de medição e pagamento

7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do Objeto

7.1. 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.

7.2. 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 05 (cinco) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.3. O recebimento definitivo ocorrerá no prazo de 15 (quinze) dias, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

7.4. 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 15 (quinze) dias.

7.5. 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.

7.6. 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.

7.7. 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.

7.8. 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

7.9. 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](#).

7.9.1. 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](#).

7.10. 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;

- 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.

7.11. 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;

7.12. 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](#).

7.13. 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.

7.14. 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.

7.15. 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.

7.16. 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.

7.17. 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

7.18. 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](#).

7.19. 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 de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, de correção monetária.

Forma de pagamento

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

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

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

7.22.1. 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.

7.23. 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

7.33. 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.

7.33.1. As cessões de crédito não fiduciárias dependerão de prévia aprovação do contratante.

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

7.35. 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 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](#).

7.36. 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.

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

8. Critérios de seleção do fornecedor

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

Forma de seleção e critério de julgamento da proposta

8.1. 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.

Exigências de habilitação

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

Habilitação jurídica

8.3. **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;

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

8.5. **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> ;

8.6. **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;

8.7. **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](#).

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

8.9. **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

8.10. **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.

8.11. **Agricultor familiar:** Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pela Secretaria Especial de Agricultura Familiar e do Desenvolvimento Agrário, nos termos do [art. 4º, §2º do Decreto nº 10.880, de 2 de dezembro de 2021](#).

8.12. **Produtor Rural:** matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da [Instrução Normativa RFB n. 971, de 13 de novembro de 2009](#) (arts. 17 a 19 e 165).

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

Habilitação fiscal, social e trabalhista

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

8.16. 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.

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

8.18. 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;

8.19. Prova de inscrição no cadastro de contribuintes [Estadual/Distrital] relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

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

8.21. Caso o fornecedor seja considerado isento dos tributos [Estadual/Distrital] 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.

8.22. 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

8.23. 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;

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

8.25. 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).

8.26. 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 exigido para fins de habilitação capital mínimo OU patrimônio líquido mínimo de 10% do valor total estimado da contratação

8.27. 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).

8.28. 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

8.29. As empresas deverão comprovar a aptidão para a prestação dos serviços em características e prazos compatíveis com o objeto desta licitação, mediante a apresentação de atestado(s)/certidão(ões)/declaração(ões) fornecidos por pessoas jurídicas de direito público ou privado, em nome da licitante, comprovando a execução satisfatória do fornecimento de licenças iguais às previstas na descrição de cada item em disputa em quantitativo não inferior a 20% (vinte por cento) do quantitativo previsto para os referidos itens.

8.30. Será permitido o somatório de atestados para comprovar os quantitativos mínimos relativos ao mesmo quesito de capacidade técnica de cada item.

8.31. A licitante deve apresentar declaração que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública, conforme o disposto no art. 5º da Lei nº 14.133, de 2021.

8.32. A licitante deve disponibilizar, quando solicitado, todas as informações necessárias à comprovação de legitimidade do(s) atestado(s) apresentado(s) fornecendo, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da CONTRATANTE e local em que foram prestados os serviços.

8.32. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

9. Estimativas do Valor da Contratação

Valor (R\$): 1.366.385,86

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

Análise de custos				
Item	Descrição do Software	Qtde	Valor Unitário	Valor Total
1	LICENÇA DE PONTO DE ACESSO PARA CONTROLADORA	500	R\$508,91	R\$254.455,00
2	LICENÇA DO PACOTE DE SOFTWARES ADOBE CREATIVE CLOUD VIP	69	R\$5.789,10	R\$399.447,90
3	AUTODESK AUTOCAD REVIT LT	5	R\$7.008,50	R\$35.042,50
4	SOLUÇÃO DE ANTIVÍRUS CORPORATIVO	1000	R\$161,49	R\$161.490,00
5	SOFTWARE VEEAM BACKUP	1	R\$29.747,50	R\$29.747,50
6	SKETCHUP LAB EDUCACIONAL	30	R\$306,25	R\$9.187,50
7	CORELDRAW GRAPHICS SUITE	13	R\$1.155,78	R\$15.025,14
8	LICENÇA PERPÉTUA DO SOFTWARE EDUCACIONAL DO SOFTWARE RHINO	3	R\$1.025,00	R\$3.075,00
9	MICROSOFT OFFICE PROFESSIONAL PLUS	648	R\$141,16	R\$91.471,68
10	MICROSOFT SQL SERVER	1	R\$18.000,00	R\$18.000,00
11	WINDOWS SERVER 2022 REMOTE DESKTOP SERVICES	150	R\$234,36	R\$35.154,00
12	MICROSOFT WINDOWS SERVER DATACENTER PER CORE	30	R\$7.667,65	R\$230.029,50
13	LICENCIAMENTO PARA SERVIDOR CONTROLADORA VIRTUAL SMARTZONE	1	R\$7.914,14	R\$7.914,14
14	GESTÃO TOTAL DA LGPD	1	R\$9.000,00	R\$9.000,00
15	AUTODESK ARCHITECTURE ENGINEERING & CONSTRUCTION COLLECTION	2	R\$33.673,00	R\$67.346,00
Total				R\$1.366.385,86

9.1. O custo estimado total da contratação é de R\$ 1.366.385,86 (Um milhão, trezentos e sessenta e seis mil reais e trezentos e oitenta e cinco reais e oitenta e seis centavos), conforme custos unitários apostos na tabela acima.

10. Adequação orçamentária

10. ADEQUAÇÃO ORÇAMENTÁRIA

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

10.2. A contratação será atendida pela seguinte dotação:

I) Gestão/Unidade: 15223/153038;

II) Fonte de Recursos: 1000 - Recursos Livres da União;

III) Programa de Trabalho: 169554 - Funcionamento de Instituições Federais de Ensino Superior e/ou 169556 - Reestruturação e Modernização das Instituições;

IV) Elemento de Despesa: 33.90.40.xx SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ e/ou 44.90.40.xx - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ;

V) Plano Interno: M20RKG01GRN e/ou V20RKG01GRN.

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

11. ADENDO 01

CONDIÇÕES GERAIS

1. Da proposta

1.1. Após a solicitação do Pregoeiro, e após tempo por ele estipulado, a licitante deverá entregar os seguintes documentos, sob pena de desclassificação:

1.1.1. Proposta de preço, com valor e descrição detalhada de cada item;

1.1.2. Na proposta de cada licitante deverão ser listados todos os componentes da solução proposta com seus respectivos Part Numbers, além de descrição e quantidades;

1.1.3. A não entrega da proposta conforme solicitado implica na desclassificação da empresa licitante.

2. Condições de Fornecimento

2.1. Todos os softwares deverão ser do fabricante especificado, para garantir total integração com o ambiente já existente na UFBA;

2.2. Os itens 02, 03, 05, 06 e 15 devem ser fornecidos com suporte técnico e atualização do próprio fabricante pelo período mínimo de 36 (trinta e seis) meses;

2.3. O item 14 deve ser fornecido com suporte técnico e atualização do próprio fabricante pelo período mínimo de 12(doze) meses

2.4. O item 07 deve ser fornecido com suporte técnico e atualização do próprio fabricante pelo período mínimo de 24(vinte e quatro) meses.

2.6 O item 9 deverá possuir licenciamento de direitos permanentes de uso de software na versão 2019 ou superior disponível.

A Licença deverá possuir as seguintes características:

- SQL Server 2019 Standard Core - 24 Core
- Licença, SQL Server 2019 Standard 64-bits Licenciamento por core não tem limite de usuários. Não há necessidade de adquirir chaves de acesso nesta versão, licenciamento por servidor.
- Um único SQL Server deverá possuir 1 instância padrão e até 15 instâncias nomeadas do mecanismo relacional.
- Tipo de Licenciamento: Full “Sem Restrições” Licença Perpétua.

2.7 Os itens 07, 08, 10, 11 e 12 deverão ter licenciamento de direitos permanentes de uso de software na última versão disponível.

3. Suporte Telefônico e Garantia

3.1. Prestar os serviços a partir da data de emissão do “Termo de Recebimento Definitivo”, garantindo o acesso ao suporte do software fornecido, através de telefone 0800 ou de ligação com custo equivalente ao de chamada local ou outros recursos de comunicação disponíveis para resolução de problemas, esclarecimento de dúvidas e orientação com relação aos softwares.

3.2. Garantir, no caso de fornecimento de mídias de instalação, que se encontrem livres de erros, realizando sua substituição por novas mídias originais em caso de falha ou erro de leitura que impossibilite a instalação do produto.

4. Relação detalhada dos itens:

Descrição da Solução de TIC a ser contratada					
Item	Código	Qtde	Descrição do Software	Licença	Período
1	4005000000040	500	LICENÇA DE PONTO DE ACESSO PARA CONTROLADORA	Subscrição	60 meses
2	4006000000013	69	LICENÇA DO PACOTE DE SOFTWARES ADOBE CREATIVE CLOUD VIP	Subscrição	36 meses
3	4006000000034	5	AUTODESK AUTOCAD REVIT LT	Subscrição	36 meses
4	4006000000009	1000	SOLUÇÃO DE ANTIVÍRUS CORPORATIVO	Subscrição	36 meses
5	4006000000053	1	SOFTWARE VEEAM BACKUP	Subscrição	36 meses
6	4006000000014	30	SKETCHUP LAB EDUCACIONAL	Subscrição	36 meses
7	4005000000039	13	CORELDRAW GRAPHICS SUITE	Subscrição	24 meses
8	4005000000030	3	LICENÇA PERPÉTUA DO SOFTWARE EDUCACIONAL DO SOFTWARE RHINO	Perpétua	Permanente
9	4005000000003	648	MICROSOFT OFFICE PROFESSIONAL PLUS	Perpétua	Permanente
10	4006000000052	1	MICROSOFT SQL SERVER	Perpétua	Permanente
11	4005000000031	150	WINDOWS SERVER 2022 REMOTE DESKTOP SERVICES	Perpétua	Permanente
12	4005000000036	30	MICROSOFT WINDOWS SERVER DATACENTER PER CORE	Perpétua	Permanente
13	4005000000041	1	LICENCIAMENTO PARA SERVIDOR CONTROLADORA VIRTUAL SMARTZONE	Subscrição	60 meses
14	4006000000054	1	GESTÃO TOTAL DA LGPD	Subscrição	12 meses
15	4006000000035	2	AUTODESK ARCHITECTURE ENGINEERING & CONSTRUCTION COLLECTION	Subscrição	36 meses

12. ADENDO 02

Os requisitos descritos em seguida são exigidos para o item 04 – Solução de Antivírus Kaspersky Endpoint Security

CONDIÇÕES GERAIS

1. Da proposta

1.1. Após solicitação do Pregoeiro, e após tempo por ele estipulado, a licitante deverá entregar os seguintes documentos sob pena de desclassificação:

1.1.1. Proposta de preço, com valor e descrição detalhada de cada item;

1.1.2. Na proposta de cada licitante deverão ser listados todos os componentes da solução proposta com seus respectivos Part Numbers, além de descrição e quantidades;

1.1.3. A não entrega da proposta conforme solicitado implica na desclassificação da empresa licitante.

2. Condições de Fornecimento

2.1. Todas as licenças, referentes aos softwares e/ou drivers componentes da solução adquirida, devem estar em nome da CONTRATANTE, em modo definitivo válidas por 36 meses, legalizadas, não sendo admitidas versões “shareware” ou “trial”;

- 2.2. O período de validade das licenças é iniciado na data de aceite da implantação da solução;
- 2.3. O item 04 deve ser fornecido com suporte técnico pelo período mínimo de 36 (trinta e seis) meses.

3. Instalação

- 3.1. A CONTRATADA deverá realizar a instalação da solução ofertada, em estações de trabalho e servidores, a serem definidos pela CONTRATANTE de acordo com o número de licenças adquiridas, contemplando criação de novas regras, migração de regras e políticas atualmente em utilização, em até 60 (sessenta) dias após assinatura do contrato;
- 3.2. Todo serviço de suporte e configuração deve ser realizado por profissional certificado pelo fabricante;
- 3.3. Deverá ser apresentado projeto técnico para aprovação pela CONTRATANTE antes do início das atividades, no prazo máximo de 15 (quinze) dias úteis após a assinatura do contrato;
- 3.4. Fica a cargo da CONTRATADA fornecer os documentos (Descritivo do serviço, arquitetura do serviço e instruções de trabalho) que instruem a aprovação no Comitê de Gestão de Mudanças de liberação do serviço para a produção;
- 3.5. As atividades que possam causar impacto no ambiente de produção deverão ser realizadas fora do horário de expediente.

4. Garantia

- 4.1. O item 04 deverá ter garantia total de 36 (trinta e seis) meses contados a partir da data de aceite da implantação do(s) software(s);
- 4.2. Sem apresentar qualquer ônus à CONTRATANTE, a garantia deverá ser fornecida diretamente pelo fabricante da solução, e deverá abranger a manutenção corretiva com a cobertura de todo e qualquer defeito apresentado;
- 4.3. A CONTRATADA deverá ser o único responsável por todo e qualquer ato de seus empregados, credenciados e representantes, inclusive sobre danos causados à CONTRATANTE ou a terceiros, por negligência, imperícia, imprudência e/ou dolo, durante toda a vigência do contrato;
- 4.4. A CONTRATADA é a única responsável pelos softwares fornecidos à CONTRATANTE, mesmo que tenham sido adquiridos de terceiros.

5. Suporte / Assistência Técnica

- 5.1. Os chamados de assistência técnica, durante o período de garantia de 36 (trinta e seis) meses, deverão ser abertos pela CONTRATANTE, junto à CONTRATADA, através de serviço telefônico 0800 ou de ligação com custo equivalente ao de chamada local;
- 5.2. Os serviços de abertura de chamados deverão estar disponíveis em regime 24x7;
- 5.3. Os serviços de garantia englobam todos os elementos de software da solução, incluindo a prestação de serviços de manutenção e assistência técnica da solução, obrigando-se a CONTRATADA a manter todo o ambiente de antivírus corporativo permanentemente em perfeitas condições de funcionamento para a finalidade a que se destina, na forma estabelecida neste Termo;
- 5.4. Todos os chamados, inclusive os que podem resultar em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, deverão ser documentados. Esta documentação, bem como outras geradas em processos de atendimento, auditorias, manutenção ou configurações, deverá ser entregue à CONTRATANTE através de relatórios (impressos e/ou em mídia digital) mediante solicitação;
- 5.5. A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução de problemas encontrados, quando for o caso;
- 5.6. A manutenção corretiva, que se fará mediante chamado da CONTRATANTE, compreende quaisquer serviços que se fizerem necessários para manter a solução adquirida em perfeito estado de funcionamento, devendo a CONTRATADA atender, nas condições dos níveis de serviços estabelecidos neste Termo, a todo e qualquer chamado que venha a receber da CONTRATANTE;
- 5.7. Após a realização de manutenções corretivas, caberá ao técnico da CONTRATADA verificar a sua eficácia por meio de testes, em conjunto com o operador/usuário da CONTRATANTE, havendo a obrigatoriedade da assinatura de ambos no relatório ao final dos trabalhos;
- 5.8. Na manutenção corretiva a que se refere o item anterior, além dos testes a serem realizados, o técnico da CONTRATADA deverá acompanhar o funcionamento de todo o ambiente de antivírus, certificando-se de que o problema foi solucionado;
- 5.9. Os chamados para manutenção corretiva somente serão considerados atendidos após a conclusão dos reparos nos prazos estabelecidos neste Termo, sendo necessária a emissão de relatório após cada intervenção;
- 5.10. Deverão ser prestadas, sempre que solicitado, orientações à equipe técnica da CONTRATANTE, ou seus usuários, pertinentes às funções da solução adquirida;
- 5.11. A CONTRATADA deverá fornecer atualizações automáticas das versões de software e manter a homogeneidade da última versão em todo o ambiente da solução fornecida;
- 5.12. Toda intervenção no ambiente da solução adquirida deverá ser comunicada e negociada previamente, para que sejam definidas a data e hora da sua realização;
- 5.13. A CONTRATADA deverá disponibilizar à CONTRATANTE o serviço de atendimento através de um gestor de contrato de suporte, que deverá ser o ponto focal de todas as necessidades de suporte da CONTRATANTE para casos de escalções ou problemas de atendimento do suporte técnico. Caso a CONTRATADA não possua laboratórios em território nacional, o referido gestor deverá ter fluência na língua portuguesa, a fim de facilitar a comunicação entre as partes;

5.14. A CONTRATANTE permitirá o acesso dos técnicos credenciados pela CONTRATADA às instalações onde se encontrarem instalados os softwares e/ou equipamentos, para a prestação dos serviços de manutenção. No entanto, todo o pessoal da CONTRATADA ficará sujeito às normas internas de segurança da CONTRATANTE, notadamente àquelas atinentes à identificação, trânsito e permanência nas suas dependências;

5.15. Os acessos remotos à solução necessários para a realização de atualização, manutenção preventiva e corretiva devem ser previamente solicitados e acompanhados pela CONTRATANTE;

5.16. Caso seja necessária a permanência do técnico da CONTRATADA nas instalações da CONTRATANTE além do tempo previsto para resolução do problema, tal fato não deverá representar qualquer ônus adicional à última.

6. Níveis de serviço e tempos esperados

6.1. Plantão telefônico através de número 0800, ou serviço equivalente ao custo de chamada local, como serviço de uso ilimitado, no período de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

6.2. Para efeito dos atendimentos técnicos, a CONTRATADA deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

NÍVEIS DE SEVERIDADE DOS CHAMADOS	
Nível	Descrição
1	Serviços totalmente indisponíveis.
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos.
3	Serviços disponíveis com ocorrência de alarmes de avisos, consultas sobre problemas, dúvidas gerais sobre o equipamento fornecido.

Tabela de Prazos de Atendimento ao Software			
Prazos	Níveis de Severidade		
	1	2	3
Início atendimento	1 horas	4 horas	24 horas
Término atendimento	4 horas	12 horas	72 horas

Observações:

6.2.1.1. Todo o chamado somente será caracterizado como “encerrado” mediante concordância da CONTRATANTE;

6.2.1.2. Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, esta deverá ser programada e planejada com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da CONTRATANTE.

7.0 Especificações Técnicas

7.1. Requisitos gerais obrigatórios para a solução de Antivírus Kaspersky Endpoint Security

7.1.1. A plataforma deve se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução de acordo com as permissões definidas na solução;

7.1.2. A plataforma deve se integrar com o Vcenter da VMware, Prism da Nutanix ou Active Directory, para a visualização e gerência dos servidores contidos nesse ambiente;

7.1.3. A solução deve permitir a criação de perfis diferenciados de gerência que permita pelo menos:

- Criar perfis de operação que possam apenas visualizar relatórios e iniciar escaneamento por vírus no endpoints;
- Criar perfis de administração que permitam o controle total sobre a solução.

7.1.4. A plataforma deve se integrar com o Active Directory para que possa ser efetuado o controle entre as máquinas no Active Directory e as máquinas que possuem os agentes instalados;

7.1.5. A comunicação entre o console de gerenciamento e os agentes deverá ser criptografada;

7.1.6. A plataforma de gerenciamento deverá possuir dashboards para facilidade de monitoração. O dashboard deverá ser configurável pelo administrador;

7.1.7. Deverá possuir a capacidade de classificar eventos de modo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas;

7.1.8. Deverá possuir a capacidade de atualizar os componentes como vacinas, engines, assinaturas de forma agendada e automática diretamente do repositório do fabricante da solução;

7.1.9. Gerenciar a atualização dos componentes nos endpoints automaticamente permitindo que ela ocorra mesmo que o módulo servidor não esteja disponível. Nesse caso, o cliente deverá buscar a atualização no repositório do fabricante;

7.1.10. A solução deverá possuir a capacidade de se criar políticas de configuração para cada recurso;

7.1.11. A solução deverá possuir a capacidade de se criar políticas de configuração global para todos os endpoints, por grupo de endpoints ou individualmente para cada endpoint;

7.1.12. A solução deverá manter as políticas de configuração no cliente de forma que o comportamento seja mantido inalterado mesmo que o servidor de gerência esteja indisponível;

7.1.13. A solução deverá vir com políticas-padrão pré-definidas e aptas a funcionarem para todos os módulos, cabendo ao administrador realizar ajustes específicos para o seu ambiente;

7.1.14. A solução deverá permitir a criação de grupos de endpoints dinâmicos com base no IP do endpoint;

7.1.15. A solução deverá permitir a criação de grupos de endpoints estáticos;

7.1.16. A hierarquia de prevalectimento das políticas de configurações deverá ser a seguinte: Global > Grupos de Endpoints > Endpoint;

7.1.17. No gerenciamento de licenças deve ser informada a quantidade em utilização de licenças;

7.1.18. Para efeito de administração a solução deverá avisar quando um agente encontra-se conectado e não conectado a sua console de gerenciamento;

7.1.19. A solução deverá coletar informações pelo menos sobre identificação de vírus, ataques, bloqueio de aplicativos, bloqueio de tráfego nos endpoints e armazenar em um banco de dados centralizado de forma que por meio da console de gerência seja possível consultar, gerar relatórios, gerar dados estatísticos, independente do estado do endpoint;

7.1.20. A solução deverá permitir a customização alertas visuais para os usuários quando:

- For identificado vírus ou qualquer malware em sua estação;
- Aplicativos forem bloqueados;
- Dispositivos forem bloqueados;
- Tráfego de rede for bloqueado;

7.1.21. A solução deverá possibilitar a remoção de qualquer tipo de alerta para o usuário final mantendo apenas os logs centralizados para uso do administrador;

7.2 Logs e relatórios:

7.2.1. A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo:

- Data e Hora;
- Tipo de evento como: Vírus Encontrado, Tentativa de Intrusão, Vulnerabilidade, entre outras;
- Endpoint de Origem e Destino sendo este último se for o caso devido à natureza do evento.

- Detalhes do evento de acordo com o tipo como, nome do vírus, software invasor, regra aplicada, resultado obtido no tratamento.
- 7.2.2. Apresentar relatórios customizados de todas as suas funcionalidades e devem apresentar dados de: usuário, alerta, ataque, firewall, informações forenses, sistema, logs e recomendações;
- 7.2.3. Os relatórios deverão ser exportados no formato PDF, CSV, HTML;
- 7.2.4. Ter a capacidade de gerar registros/logs para auditoria;
- 7.2.5. Customização dos relatórios gráficos gerados;
- 7.2.6. A solução deverá possuir pelo menos os seguintes tipos de relatórios, via gerenciamento centralizado:

- Tabelas e/ou gráficos de máquinas verificadas;
- Tabelas e/ou gráficos de realização de tarefas agendadas;
- Erros de sistema;
- Scans em andamento;
- Máquinas com a lista de definições de vírus desatualizada;
- Qual a versão do software instalado em cada máquina;
- Os vírus que mais foram detectados;
- As máquinas que mais sofreram infecções em um determinado período de tempo;
- Os usuários que mais sofreram infecções em um determinado período de tempo;
- Sumário de eventos de IPS por assinatura, por alvo, por endereço IP origem;
- Os 10 principais ativos atacados;
- As 10 principais assinaturas;
- Sumário das aplicações bloqueadas e update de quarentena;

7.3 Controle de aplicativos e dispositivos:

7.3.1. A solução deverá permitir bloquear, registrar ou ignorar a execução de aplicações:

- Pelo nome do executável;
- Pela extensão do executável;
- Pelo seu identificador único gerado por algoritmos de hash ou fingerprint;
- Local de armazenamento. Ex: Dispositivos USB, CD/DVD Rom.

7.3.2. O bloqueio de aplicações deverá funcionar independentemente do local onde esta estiver instalada ou armazenada;

7.3.3. Deverá ser possível gerenciar o uso de dispositivos USB, CD/DVD e Bluetooth através de controles de leitura/escrita /execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido.

7.4 Características gerais da solução anti-malware

7.4.1. Deverá rastrear por malwares diversos, incluindo Vírus, Worm, Trojan, Keylogger, Screenlogger, Spyware, Adware, Backdoor, Exploits, Sniffers, Port Scanners, Bot, Rootkit;

7.4.2. Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva;

7.4.3. Capacidade de retomar atualizações de DAT's e de software do ponto onde foram interrompidas em caso de perda de conexão, sem necessidade de reinício de todo o processo;

7.4.4. O sistema de antispayware deve estar totalmente integrado ao software antivírus utilizando a mesma biblioteca DAT de definições de vírus e demais ameaças;

7.4.5. Possuir tecnologia de detecção baseada em hash ou fingerprint de arquivos armazenados em repositório centralizado para consulta;

7.4.6. A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura;

7.4.7. Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site da Internet, com determinação de frequência e horários;

7.4.8. Permitir o rastreamento manual por meio de interface gráfica, sem uso de linhas de comando, com fornecimento de opção de rastreamento;

7.4.9. Realizar o rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados;

7.4.10. Rastrear, em tempo real, arquivos durante os processos de gravação e leitura;

7.4.11. Rastrear vírus em mensagens eletrônicas recebidas no cliente de correio eletrônico, a exemplo do Microsoft Outlook;

7.4.12. Uma vez verificada a ameaça, a solução deverá permitir as seguintes ações:

- Negar acesso ao arquivo infectado e prosseguir;
- Limpar o arquivo;
- Apagar o arquivo infectado;
- Mover o arquivo infectado para área de segurança (quarentena);
- Permitir a determinação de ações primárias e secundárias. Ex: Limpar arquivo, caso não consiga, mover para quarentena.

- 7.4.13. Deverá possibilitar a criação de exceções de rastreamento para pastas, arquivos específicos, tipos de arquivos e processos em execução;
- 7.4.14. Reparar o registro do sistema após eliminação de epidemia;
- 7.4.15. Possuir proteção contra estouro de buffer;
- 7.4.16. Permitir o bloqueio de compartilhamentos da máquina em caso de epidemia;
- 7.4.17. Deverá rastrear por arquivos comprimidos (compactados), com os seguintes formatos: ZIP, ZIP2EXE, LZEXE, ARJ, LZH, PKLITE, LHA, RAR, TAR, GZIP e Microsoft Compress, no mínimo em 5 níveis de compactação;
- 7.4.18. Deverá possuir base de reputação de arquivos que permitam o bloqueio de malwares para os quais não existam ainda vacinas disponíveis. Recurso comumente chamado de proteção dia-zero;
- 7.4.19. Deverá permitir a definição do uso máximo de CPU para o processo de rastreamento;
- 7.4.20. Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local;
- 7.4.21. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede;
- 7.4.22. Instalação sem reinicialização da estação de trabalho;
- 7.4.23. Proteção contra desinstalação não autorizada do produto e proteção contra remoção do módulo residente em memória através de senhas distintas.

7.5 Características específicas da solução de firewall de desktop:

- 7.5.1. O modo de filtragem do firewall deverá ser stateful bidirecional;
- 7.5.2. Deverá permitir a criação de regras de firewall tendo como critério pelo menos:

- O endereço ip local ou remoto;
- Range de endereços ip local e remoto;
- Grupos de endereços ip local e remoto;
- Hostname do dispositivo local e remoto;
- Adaptador (Wireless, Ethernet, Dial-up);
- Portas locais e remotas;
- Direção do tráfego de rede (inbound e outbound);
- Aplicação e Processos locais.

7.5.3. O firewall deverá possuir, no mínimo, as seguintes ações:

- Monitorar e, a critério do administrador, registrar no log;
- Bloquear e, a critério do administrador, registrar no log;
- Permitir e, a critério do administrador, registrar no log;
- Deverá vir com regras padrões de proteção contra Port Scan, Denial Of Service, AntiMac Spoofing;
- Bloquear por tempo determinado do tráfego de rede das origens de ataques com opção de ativar, desativar e definir o tempo;
- Permitir a desativação do Firewall nativo do Windows.

7.6 Características específicas da solução de monitoramento de integridade dos servidores físicos e virtuais:

- 7.6.1. A solução deverá rastrear e indicar ao administrador quais os softwares e arquivos que existem no endpoint de modo a ser monitorado pela integridade;
- 7.6.2. Deverá ser capaz de criar regras customizadas para monitoramento de integridade de pastas ou arquivos de sistemas;
- 7.6.3. Deverá monitorar por modificações os seguintes elementos do sistema:

- Arquivos;
- Pastas;
- Chaves de Registros;
- Processos;
- Serviços;
- Portas Ativas.

7.6.4. Deverá rastrear a integridade dos arquivos por:

- Data de Criação;
- Última Modificação;
- Permissões;
- Dono;

- Grupo;
- Tamanho;
- Fingerprint ou hash.

7.6.5. Deverá registrar em log e colocar em relatório todas as modificações que ocorrerem;

7.6.6. O monitoramento deverá ocorrer em tempo real ou sob demanda;

7.6.7. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

7.6.8. Deverá possibilitar escolher o diretório onde o arquivo será monitorado.

7.7 Proteção para endpoints virtuais:

7.7.1. A solução deverá possuir versão compatível com endpoints virtuais atendendo aos requisitos abaixo, além dos requisitos já descritos nesta especificação:

- A solução deverá ser suportada e otimizada para uso em ambiente virtual VMware 6.0 ou superior, permitindo o rastreamento por malwares em servidores virtuais;
- A solução deverá ter a capacidade de realizar o rastreamento realtime, por demanda e agendado;
- A solução deverá ter a capacidade de impedir em tempo real (realtime) a gravação de malwares;
- A solução deverá permitir varredura por vírus, em endpoints virtuais que estejam desligados, por meio da console de gerência ou ferramenta autônoma da mesma solução e do mesmo fabricante;
- A solução deverá ser capaz de realizar a varredura por vírus em arquivos VMDK (discos virtuais) usado em endpoints virtuais do ambiente VMWARE;
- Deverá ser possível a instalação e remoção remota do agente de administração nos sistemas virtuais, sem a necessidade de intervenção no sistema virtual.

7.7.2. Características gerais do agente da solução:

Para situações onde o administrador entenda necessária a proteção de um endpoint utilizando agente, deverá ser provido agente que atenda aos requisitos abaixo, além dos requisitos já descritos nesta especificação:

- A solução deverá ser capaz de gerenciar e ter os clientes para instalação em ambientes operacionais Windows Vista, Windows 7, Windows 10, Windows Server 2003, 2008, 2008R2, 2012, de 32bits e 64bits e Distribuições Linux de 32bits e 64bits, ou versões mais recentes destes sistemas operacionais, em ambientes baseados nas plataformas de virtualização Microsoft Hyper-V, VMWare ou Nutanix;

- Os agentes deverão oferecer a possibilidade de instalação por meio de pacote MSI para ambiente Windows;
- Os agentes deverão oferecer a possibilidade de serem instalados, mas não ativados, sendo ativado posteriormente pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;
- A ativação do agente deverá ser possível por meio da console de gerenciamento;
- A Solução deverá realizar análise de vulnerabilidades dos seguintes ativos: desktops, notebooks e servidores;
- A análise deve considerar vulnerabilidades tanto dos produtos quanto das suas configurações;
- O funcionamento da Solução deve prescindir da instalação de agentes nos ativos;
- Caso a Solução necessite de softwares extras para executar suas funcionalidades, como gerenciador de bancos de dados, gerador de relatórios, etc., as licenças deverão ser fornecidas no bojo da Solução, sem ônus para a Contratante.

7.7.3. A Solução deve ser capaz de identificar e analisar ao menos os seguintes sistemas operacionais: Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2016, Windows XP, Windows Vista, Windows 7, Windows 10, Linux, IBM AIX, Apple MacOS e VMWare ESX, ou versões mais recentes destes sistemas operacionais;

7.7.4. A Solução deve ser capaz de identificar e analisar versões atuais e anteriores das seguintes aplicações de servidores: Microsoft Hyper-V, VMWare, KVM, Microsoft IIS, Apache, IBM WebSphere, Microsoft Exchange, Postfix, Microsoft SQL Server, Microsoft DNS, ISC BIND, Oracle, MySQL, PostgreSQL, IBM DB2, Microsoft Terminal Server e SSHd;

7.7.5. A Solução deve ser capaz de identificar e analisar versões atuais e anteriores das seguintes aplicações clientes: suíte Microsoft Office, OpenOffice.Org, Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, Adobe Flash Player, Adobe Reader, Java, Skype, Apple iTunes, Microsoft Media Player e Apple Quicktime.

7.8 Base de vulnerabilidades:

7.8.1. A base de dados de vulnerabilidades deve ser atualizada automaticamente pela Solução, via internet, através de downloads incrementais diretamente do site do fabricante;

7.8.2. A periodicidade de atualização deve ser configurável;

7.8.3. A solução deve permitir alteração dos níveis de severidade das vulnerabilidades na base de dados da ferramenta;

7.8.4. Cada vulnerabilidade deve conter uma descrição com no mínimo as seguintes informações:

- Nome;

- Nível de risco;
- Descrição;
- Recomendações/Solução;
- Referências.

7.8.5. No campo "Recomendações/Solução" da vulnerabilidade, deve constar o link para download do patch de correção (se existente) e outras possíveis ações de remediação para a brecha encontrada.

7.8.6. O campo "Referências" deve conter informações como o número CVE, Bugtraq ID, ID do fabricante ou outras informações aplicáveis à vulnerabilidade.

7.8.7. O fabricante da ferramenta deve possuir um time de pesquisas de vulnerabilidades com funcionamento em 24X7 (vinte e quatro horas, sete dias na semana).

7.9 Varredura de ativos

7.9.1. A Solução deve ser fornecida em arquitetura distribuída, com motores de varredura espalhados por diversas localidades.

7.9.2. A Solução deve possibilitar a realização de busca de ativos na rede e classificar esses ativos ao menos pelas seguintes propriedades:

- Nome DNS;
- Nome NetBIOS;
- Endereço IP.

7.9.3. A Solução deve permitir o agrupamento dos ativos encontrados em grupos departamentais ou por range de IP. Deve ser possível atribuir diferentes níveis de criticidade aos grupos criados.

7.9.4. A Solução deve prover cálculo de risco, levando em consideração a criticidade definida para cada ativo analisado pela ferramenta e também o nível de severidade das vulnerabilidades encontradas.

7.9.5. A Solução deve permitir ao administrador que pare ou reinicie uma varredura a qualquer momento da operação.

7.9.6. A Solução deve possuir opções de varreduras agendadas ou executadas sob demanda.

7.9.7. Deve ser possível criar exclusões dentro de um range de varreduras.

7.9.8. Deve ser possível habilitar ou desabilitar a realização de testes intrusivos.

7.9.9. Deve ser possível definir opções de performance da varredura (exemplo: número de conexões simultâneas e uso de banda) para evitar problemas de rede decorrentes do tráfego da análise.

7.9.10. A Solução deve possuir módulo de remediação embutido, para criar tickets e fazer a distribuição dos mesmos aos usuários da ferramenta. Os tickets devem ser encerrados automaticamente quando da correção da vulnerabilidade detectada.

7.9.11. Varredura para Análise de Segurança de Configurações dos Ativos;

7.9.12. A Solução deve ser capaz de detectar o uso de senhas padrão ou de senhas fracas, com o uso de dicionários, no Sistema Operacional analisado e em serviços, como por exemplo: SSH, FTP, TELNET, Microsoft SQL Server e interfaces de gerenciamento de equipamentos de TI.

7.10 Console de administração e configuração

7.10.1. A administração da Solução deve ser possível via interface Web;

7.10.2. O acesso à console deve ser de forma criptografada, protegida por autenticação com usuário/senha;

7.10.3. A ferramenta deve possuir painel executivo com o resultado das últimas varreduras realizadas, mostrando o nível de risco encontrado;

7.10.4. Deve ser possível exportar e importar as configurações para backup/restore;

7.10.5. Geração de Logs e Relatórios.

7.10.6. A Solução deve oferecer os seguintes tipos de relatórios:

- Relatório executivo com o resumo gerencial das vulnerabilidades encontradas;
- Relatório detalhado, com informações detalhadas sobre as vulnerabilidades encontradas, inclusive sua descrição, referências e recomendações;

7.10.7. Relatório de tendências, mostrando a evolução das vulnerabilidades e riscos encontrados em análises sucessivas de um mesmo ativo ou grupo de ativos;

7.10.8. A Solução deve gerar log para toda e qualquer varredura, onde conste: data, hora da varredura, endereço IP do ativo e resultado de cada teste;

7.10.9. A Solução deve permitir a personalização do formato e das informações incluídas nos relatórios das análises;

7.10.10. A Solução deve possibilitar ao usuário a definição de vulnerabilidades como falso-positivos ou riscos aceitos, excluindo essas vulnerabilidades dos relatórios;

7.10.11. Deve ser possível exportar os ativos encontrados para o formato CSV;

7.10.12. Os relatórios das análises devem poder ser gerados nos formatos HTML, PDF e CSV;

7.10.13. Deve ser possível enviar automaticamente os relatórios das análises por e-mail.

8. Detalhes do item:

Item	Sipac	Qtde	Descrição do Software	Licença	Período
04	4006000000009	1000	Kaspersky Endpoint Security	Subscrição	36 meses

13. ADENDO 03

Os requisitos descritos em seguida são exigidos para os itens 01 e 13.

CONDIÇÕES GERAIS

1. Da proposta

1.1. Após solicitação do Pregoeiro, e após tempo por ele estipulado, a licitante deverá entregar os seguintes documentos sob pena de desclassificação:

- 1.1.1. Proposta de preço, com valor e descrição detalhada de cada item;
- 1.1.2. Na proposta de cada licitante deverão ser listados todos os componentes da solução proposta com seus respectivos Part Numbers, além de descrição e quantidades;
- 1.1.3. A não entrega da proposta conforme solicitado implica na desclassificação da empresa licitante.

2. Do Projeto

O Projeto de Modernização da rede wifi visa o licenciamento da migração da controladora física SN 321308000133 para a controladora virtual smartzone Ruckus na UFBA. O escopo contempla o fornecimento de uma controladora, incluindo 500 licenças de ponto de acesso.

3. Condições de Fornecimento

- 3.1. Todas as licenças, referentes aos softwares e/ou drivers componentes da solução adquirida, devem estar em nome da CONTRATANTE, em modo definitivo e com garantia e suporte por 60 meses, legalizadas, não sendo admitidas versões “shareware” ou “trial”;
- 3.2. O período de validade das licenças é iniciado na data de aceite da implantação da solução;
- 3.3. O item 01 e 13 devem ser fornecidos com suporte técnico pelo período mínimo de 60 (sessenta) meses;

4. Instalação

- 4.1. A CONTRATADA deverá realizar a instalação da solução ofertada, em até 30 (trinta) dias após assinatura do contrato;
- 4.2. Todo serviço de suporte e configuração deve ser realizado por profissional certificado pelo fabricante;
- 4.3. Deverá ser apresentado projeto técnico para aprovação pela CONTRATANTE antes do início das atividades, no prazo máximo de 15 (quinze) dias após a assinatura do contrato;
- 4.4. Fica a cargo da CONTRATADA fornecer os documentos (Descritivo do serviço, arquitetura do serviço e instruções de trabalho) que instruem a aprovação no Comitê de Gestão de Mudanças de liberação do serviço para a produção;
- 4.5. As atividades que possam causar impacto no ambiente de produção deverão ser realizadas fora do horário de expediente a serem definidas pela CONTRATANTE.

5. Garantia

- 5.1. Os itens 01 e 13 deverão ter garantia total de 60 (sessenta) meses contados a partir da data de aceite da implantação do(s) software(s);
- 5.2. Sem apresentar qualquer ônus à CONTRATANTE, a garantia deverá ser fornecida diretamente pelo fabricante da solução,

e deverá abranger a manutenção corretiva com a cobertura de todo e qualquer defeito apresentado;

5.3. A CONTRATADA deverá ser o único responsável por todo e qualquer ato de seus empregados, credenciados e representantes, inclusive sobre danos causados à CONTRATANTE ou a terceiros, por negligência, imperícia, imprudência e/ou dolo, durante toda a vigência do contrato;

5.4. A CONTRATADA é a única responsável pelos softwares fornecidos à CONTRATANTE, mesmo que tenham sido adquiridos de terceiros.

6. Suporte / Assistência Técnica

6.1. Os chamados de assistência técnica, durante o período de garantia de 60 (sessenta) meses, deverão ser abertos pela CONTRATANTE, junto à CONTRATADA, através de serviço telefônico 0800 ou de ligação com custo equivalente ao de chamada local;

6.2. Os serviços de abertura de chamados deverão estar disponíveis em regime 24x7;

6.3. Os serviços de garantia englobam todos os elementos de software da solução, incluindo a prestação de serviços de manutenção e assistência técnica da solução, obrigando-se a CONTRATADA a manter todo o ambiente corporativo permanentemente em perfeitas condições de funcionamento para a finalidade a que se destina, na forma estabelecida neste Termo;

6.4. Todos os chamados, inclusive os que podem resultar em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, deverão ser documentados. Esta documentação, bem como outras geradas em processos de atendimento, auditorias, manutenção ou configurações, deverá ser entregue à CONTRATANTE através de relatórios (impressos e/ou em mídia digital) mediante solicitação;

6.5. A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução de problemas encontrados, quando for o caso;

6.6. A manutenção corretiva, que se fará mediante chamado da CONTRATANTE, compreende quaisquer serviços que se fizerem necessários para manter a solução adquirida em perfeito estado de funcionamento, devendo a CONTRATADA atender, nas condições dos níveis de serviços estabelecidos neste Termo, a todo e qualquer chamado que venha a receber da CONTRATANTE;

6.7. Após a realização de manutenções corretivas, caberá ao técnico da CONTRATADA verificar a sua eficácia por meio de testes, em conjunto com o operador/usuário da CONTRATANTE, havendo a obrigatoriedade da assinatura de ambos no relatório ao final dos trabalhos;

6.8. Na manutenção corretiva a que se refere o item anterior, além dos testes a serem realizados, o técnico da CONTRATADA deverá acompanhar o funcionamento de todo o ambiente, certificando-se de que o problema foi solucionado;

6.9. Os chamados para manutenção corretiva somente serão considerados atendidos após a conclusão dos reparos nos prazos estabelecidos neste Termo, sendo necessária a emissão de relatório após cada intervenção;

6.10. Deverão ser prestadas, sempre que solicitado, orientações à equipe técnica da CONTRATANTE, ou seus usuários, pertinentes às funções da solução adquirida;

6.11. A CONTRATADA deverá fornecer atualizações automáticas das versões de software e manter a homogeneidade da última versão em todo o ambiente da solução fornecida;

6.12. Toda intervenção no ambiente da solução adquirida deverá ser comunicada e negociada previamente, para que sejam definidas a data e hora da sua realização;

6.13. A CONTRATADA deverá disponibilizar à CONTRATANTE o serviço de atendimento através de um gestor de contrato de suporte, que deverá ser o ponto focal de todas as necessidades de suporte da CONTRATANTE para casos de escalões ou problemas de atendimento do suporte técnico. Caso a CONTRATADA não possua laboratórios em território nacional, o referido gestor deverá ter fluência na língua portuguesa, a fim de facilitar a comunicação entre as partes;

6.14. A CONTRATANTE permitirá o acesso dos técnicos credenciados pela CONTRATADA às instalações onde se encontrarem instalados os softwares e/ou equipamentos, para a prestação dos serviços de manutenção. No entanto, todo o pessoal da CONTRATADA ficará sujeito às normas internas de segurança da CONTRATANTE, notadamente àquelas atinentes à identificação, trânsito e permanência nas suas dependências;

6.15. Os acessos remotos à solução necessários para a realização de atualização, manutenção preventiva e corretiva devem ser previamente solicitados e acompanhados pela CONTRATANTE;

6.16. Caso seja necessária a permanência do técnico da CONTRATADA nas instalações da CONTRATANTE além do tempo previsto para resolução do problema, tal fato não deverá representar qualquer ônus adicional à última.

7. Níveis de serviço e tempos esperados

7.1. Plantão telefônico através de número 0800, ou serviço equivalente ao custo de chamada local, como serviço de uso ilimitado, no período de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

7.2. Para efeito dos atendimentos técnicos, a CONTRATADA deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

NÍVEIS DE SEVERIDADE DOS CHAMADOS

Nível	Descrição
1	Serviços totalmente indisponíveis.
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso.
3	Serviços disponíveis com ocorrência de alarmes de avisos, consultas sobre problemas, dúvidas gerais sobre a solução fornecida.

Tabela de Prazos de Atendimento ao Software			
Prazos	Níveis de Severidade		
	1	2	3
Início atendimento	1 hora	4 horas	2 4 horas
Término atendimento	4 horas	12 horas	7 2 horas

Observações:

7.2.1.1. Todo o chamado somente será caracterizado como “encerrado” mediante concordância da CONTRATANTE;

7.2.1.2. Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, esta deverá ser programada e planejada com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da CONTRATANTE.

8.0 Especificações Técnicas

ITEM 01 - LICENÇA DE AP PARA CONTROLADORA WIRELESS – Part Number L09-0001-SG00

1. Licença para expansão da capacidade de gerenciamento dos Pontos de Acesso de sua capacidade atual para adicionar de forma unitária os pontos de acesso;
2. Deve ser compatível com os pontos de acesso em uso na Universidade (Ruckus);
3. Deve ter suporte de 60 (sessenta) meses na modalidade 24x7 NBD.

ITEM 13 - CONTROLADORA WIRELESS VIRTUAL CARACTERÍSTICAS TÉCNICAS MÍNIMAS DO GERENCIAMENTO DOS PONTOS DE ACESSO (WLAN) – Part Number: L09-VSCG-WW00

1. A solução de gerência de rede deve ser fornecida em Virtual Appliance;
2. Deve ser obrigatoriamente do mesmo fabricante dos AP's (Access Point) em uso na Universidade (Ruckus);
3. Deve ser compatível com VMware ESXi (vSphere) e KVM (Kernel Virtual Machine);

4. Deve permitir a configuração e gerenciamento através de browser padrão (HTTP, HTTPS);
5. Deve suportar os padrões 802.11ax e 802.11ac wave I e wave II;
6. Deverá suportar operação como um cluster (N+1) para prover resiliência e desempenho, podendo o mesmo ser composto por, no mínimo, 2 (dois) controladores e expansível até 4 (quatro) controladores;
7. Deve vir acompanhado de todos os acessórios necessários para operacionalização da solução, tais como softwares, documentações técnicas e manuais que contenham informações suficientes, que possibilitem a instalação, configuração e operacionalização da solução;
8. Deve possuir uma arquitetura modular do tipo multi-tenant, permitindo gestão centralizada, mas com acesso independente e isolado para cada domínio;
9. Deverá suportar pontos de acesso internos e externos nos padrões 802.11a/b/g/n/ac/ax;
10. Deverá possuir suporte a RESTful API compatível com JSON e disponibilizar suporte às funções GET, POST, DELETE, PUT e PATCH;
11. Capacidade para gerenciar, no mínimo, 1024 (um mil e vinte e quatro) Pontos de Acesso, podendo chegar através de atualização de licenças de software a até 5000 (cinco mil) Pontos de Acesso simultâneos por controlador;
12. Suportar, no mínimo, 25.000 (trinta e cinco mil) dispositivos simultâneos por controlador;
13. Prover o gerenciamento centralizado dos Pontos de Acesso, suportando versões de firmware diferentes;
14. Deverá permitir gerenciamento através de Endereço IP, Range de IPs e Sub-Redes pré-configuradas;
15. Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF);
16. O controlador WLAN poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso por ele gerenciados, inclusive via roteamento em camada 3 do modelo OSI;
17. Possibilitar a configuração de envio dos eventos do Controlador WLAN para um servidor de Syslog remoto;
18. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps SNMP;
19. Permitir a visualização de alertas da rede em tempo real;
20. Implementar, no mínimo, 3 (três) níveis de acesso administrativo ao equipamento (apenas leitura, leitura/escrita e administrador da senha de visitante) protegidos por senhas independentes;
21. Permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador;
22. Permitir a configuração e gerenciamento através de navegador padrão por meio de HTTPS;
23. Gerenciar de forma centralizada a autenticação de usuários;
24. Permitir o envio de alertas ou alarmes através do protocolo SMTP, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS);
25. Permitir que o processo de atualização de versão seja realizado através de navegador padrão (HTTPS) ou SSH;
26. Deverá possuir a capacidade de importação de certificados digitais emitidos por uma autoridade certificadora externa;
27. A disponibilidade da rede sem fio deve ser passível de agendamento para, no mínimo, as opções a seguir:
 - a. 27.1. 24 horas por dia, 7 dias na semana;
 - b. 27.2. Agendamento customizado permitindo escolher os dias da semana e horários;
 - c. 27.3. Os horários definidos não precisam ser sequenciais, ou seja, a solução deve suportar que o administrador defina o horário de funcionamento das 08:00 às 12:00 e 14:00 às 18:00.
28. Possuir ferramentas de diagnóstico e log de eventos para depuração e gerenciamento em primeiro nível;
29. Possuir ferramenta que permite o monitoramento em tempo real de informações de utilização de CPU, memória e estatísticas de rede;
30. Possibilitar cópia "backup" da configuração, bem como a funcionalidade de restauração da configuração através de navegador padrão (HTTPS) ou FTP ou TFTP;

31. Possuir a capacidade de armazenar múltiplos arquivos de configuração do controlador pertencente à rede sem fio;
32. Monitorar o desempenho da rede sem fio, permitindo a visualização de informações de cada ponto de acesso;
33. Implementar cluster de controladores WLAN no modo ativo/ativo, com sincronismo automático das configurações entre controladores para suporte a redundância em alta disponibilidade (HA - high availability);
34. Deverá efetuar compartilhamento de recursos e licenças de pontos de acesso entre os controladores participantes do cluster;
35. Deverá em caso de falha realizar a redundância de forma automática e sem nenhuma necessidade de intervenção do administrador de rede;
36. Deverá possuir a capacidade de geração de informações ou relatórios de, no mínimo, os seguintes tipos: Listagem de clientes Wireless, Listagem de Pontos de Acesso, utilização da rede;
37. Deverá suportar, somente por meio do controlador e do ponto de acesso, a identificação de aplicações dos clientes conectados com base na camada 7 do modelo OSI, permitindo o controle de acesso, de banda (uplink e/ou downlink) e definição de regra de QoS para estas aplicações;
38. O pacote de assinaturas das aplicações com base na camada 7 do modelo OSI deve ser atualizado automaticamente, não sendo necessária intervenção manual por parte do administrador da solução;
39. Deve ser possível especificar regras de usuários baseadas em tempo, permitindo determinar em quais dias e horários a regra estará ativa, possibilitando ainda que os horários não sejam obrigatoriamente sequenciais, ou seja, deve ser possível escolher das 08:00 às 12:00 e das 14:00 às 18:00, por exemplo;
40. Permitir visualizar a localização dos pontos de acesso e através desta obter o status de funcionamento dos mesmos;
41. Deverá possibilitar a importação de plantas baixas nos formatos dwg ou jpg ou png, devendo permitir a visualização dos Pontos de Acesso instalados com seu estado de funcionamento, bem como disponibilizar uma visualização da cobertura do sinal em 2.4GHz ou 5GHz;
42. Deve ser possível localizar o dispositivo cliente na planta baixa;
43. Implementar funcionalidade de análise espectral, permitindo a detecção de interferências no ambiente de rede sem fio;
44. Implementar análise de tráfego por WLAN, Ponto de acesso e dispositivos cliente, apresentando os 10 itens mais usados;
45. Deve ser possível definir o nível de segurança administrativo da solução suportando, no mínimo:
 - a. 45.1. Habilitar Captcha para Acesso;
 - b. 45.2. Período em dias para alteração obrigatória da senha;
 - c. 45.3. Política para reutilização de senha;
 - d. 45.4. Comprimento mínimo da senha e complexidade;
 - e. 45.5. Segundo Fator de Autenticação via SMS;
 - f. 45.6. A solução deve suportar a adição de um serviço de SMS externo, tal como Twilio.
46. Deve suportar integração com tags da Ekahau e AeroScout/Stanley para Real-Time Location Service (RTLS);
47. Deverá implementar suporte aos protocolos IPv4 e IPv6;
48. Deverá suportar tagging de VLANs;
49. Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1X;
50. Suportar associação dinâmica de ACL e de QoS por usuário, com base nos parâmetros da etapa de autenticação;
51. Deverá suportar, no mínimo, 1030 (mil e trinta) SSIDs simultâneos;
52. Deverá possuir funcionalidade de balanceamento de carga entre VLANs e permitir que clientes sejam designados para diferentes VLANs dentro de um mesmo SSID, com suporte a até 50 VLANs por pool;

53. Em caso de falha de comunicação entre os pontos de acesso e a controladora, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Também deve permitir que novos usuários se associem à rede sem fio utilizando autenticação do tipo 802.1X mesmo que os pontos de acesso estejam sem comunicação com a controladora;
54. Deve ser possível evitar que dispositivos 802.11b se conectem à rede, visando melhorar o desempenho da rede sem fio;
55. Deve suportar 802.11d e 802.11k;
56. Deve suportar captura de pacotes por ponto de acesso para resolução de problemas, sendo possível definir a captura nos rádios de 2.4 GHz e 5 GHz, bem como na interface LAN. Ainda, a operação deve ser realizada via interface Web e deve ser possível exportar o arquivo de captura para análise local em software de análise de pacote, tal como Wireshark;
57. Deve ser possível rastrear a conexão de um cliente wireless em tempo real para analisar problemas de conectividade e identificar em qual estágio o problema aconteceu;
58. Deve ser possível estabelecer um limite para o nível de sinal visando permitir que o cliente se junte à rede sem fio, o qual deve ser estabelecido em dBm e variar entre -60dBm e -90dBm;
59. Deverá suportar de forma centralizada a configuração de agregação de portas (LACP) ethernet dos pontos de acesso que possuírem suporte a essa funcionalidade;

Deve suportar auto configuração e auto correção para rede Mesh;

1. Os itens a seguir devem estar integrados a solução ofertada, não serão aceitos equipamentos externos a solução. Caso sejam necessárias licenças ou softwares de controle os mesmos devem ser fornecidos de forma que a solução esteja operacional e sem nenhuma restrição no ato de sua implementação (hardware e softwares necessários para implementação);
2. Implementar, pelo menos, os seguintes padrões de segurança wireless:
 - a. 2.1. (WPA) Wi-Fi Protected Access;
 - b. 2.2. (WPA2) Wi-Fi Protected Access 2;
 - c. 2.3. (WPA3) Wi-Fi Protected Access 3;
 - d. 2.4. (TKIP) Temporal Key Integrity Protocol;
 - e. 2.5. (AES) Advanced Encryption Standard;
 - f. 2.6. Chave única por usuário em um mesmo SSID;
 - g. 2.7. IEEE 802.1X;
 - h. 2.8. IEEE 802.11i;
 - a. 2.9. IEEE 802.11w.
3. Implementar, pelo menos, os seguintes controles/filtros:
 - a. 3.1. Baseado em endereço MAC e isolamento de cliente na camada 2 do modelo OSI;
 - b. 3.2. Baseado em endereço IP;
 - c. 3.3. Baseado em protocolo, tais como TCP, UDP, ICMP e IGMP;
 - d. 3.4. Baseado em porta de origem e/ou destino;
 - e. 3.5. Baseado em tipo ou sistema operacional do dispositivo.
4. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:
 - a. 4.1. Endereço MAC;
 - b. 4.2. Autenticação Local;
 - c. 4.3. Captive Portal;
 - d. 4.4. Active Directory;
 - e. 4.5. RADIUS;
 - f. 4.6. IEEE 802.1X;
 - g. 4.7. LDAP.
5. Deverá permitir a seleção/uso de servidor RADIUS específico com base no SSID;
6. Deverá suportar servidor de autenticação RADIUS redundante. Isto é na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário;
7. A solução deverá suportar a criação de uma zona de visitantes, que terá seu acesso controlado através de senha cadastrada internamente, sendo que esta deverá possuir a configuração de tempo pré-determinado de acesso à rede sem fio;

8. O controlador deverá permitir a criação de múltiplos usuários visitantes (guests) de uma única vez (em lote);
9. Deve ser possível definir o período de validade da senha de visitantes em quantidade de horas, dias e semanas;
10. Deve permitir que após o processo de autenticação de usuários visitantes (guests) os mesmos sejam redirecionados para uma página de navegação específica e configurável;
11. Deve permitir que múltiplos usuários visitantes (guests) compartilhem a mesma senha de acesso à rede;
12. Deverá dispor de opção para enviar a senha de usuários visitantes (guests) por e-mail ou por SMS;
13. Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (guests) diretamente para a Internet, de forma totalmente separada do tráfego da rede corporativa;
14. Deve disponibilizar autenticação dos usuários por meio de Redes Sociais suportando, no mínimo, 4 (quatro) redes sociais diferentes dentro de uma mesma WLAN;
15. Deverá permitir o isolamento do tráfego unicast, multicast ou ambos entre usuários visitantes (guests) em uma mesma VLAN/Subrede, sendo possível adicionar exceções com base em endereços MAC e IP;
16. Deverá ser possível permitir que o ponto de acesso filtre todo o tráfego IPv4 e IPv6 dos tipos multicast e broadcast dos clientes sem fio associados, com exceção de alguns tráfegos pertencentes a uma lista de exclusões, tais como ARP, DHCPv4 e DHCPv6, MLD, IGMP, IPv6 NS, IPv6 NA, IPv6 RS e todos os pacotes do tipo unicast;
17. Deverá ser possível especificar o tipo de serviço Bonjour que será permitido entre VLANs;
18. Deve suportar mecanismo de acesso de acordo com o padrão Hotspot 2.0;
19. Deve implementar mecanismos de segurança e proteção da rede sem fio contemplando, no mínimo, os recursos abaixo:
 - a. 19.1. SSID Spoofing – Detectar APs não pertencentes ao controlador propagando o mesmo SSID;
 - b. 19.2. MAC Spoofing – Detectar APs não pertencentes ao controlador propagando o mesmo MAC de um AP válido;
 - c. 19.3. Rogue APs – Detectar APs não pertencentes ao controlador;
 - d. 19.4. Same Network – Detectar APs não pertencentes ao controlador exibindo qualquer SSID pertencentes ao mesmo segmento de rede LAN;
 - e. 19.5. Ad Hoc – Possibilidade de detectar rede Ad Hoc como rogue;
 - f. 19.6. Flood de Deauthentication – Detectar quando há um número excessivo de frames de desautenticação oriundos de um mesmo transmissor;
 - g. 19.7. Flood de Disassociation – Detectar quando há um número excessivo de frames de desassociação oriundos de um mesmo transmissor;
 - h. 19.8. Excesso de Clear to Send (CTS) – Detectar quando há um número excessivo de frames de CTS para um endereço MAC específico;
 - a. 19.9. Excesso de Request to Send (RTS) – Detectar quando há um número excessivo de frames de RTS para um endereço MAC específico;
 - j. 19.10. Excesso de Energia – Possibilidade de detectar tráfego com nível de potência de transmissão excessivo.
20. Deve implementar varredura de rádio frequência para identificação de ataques e Pontos de Acesso intrusos não autorizados (rogues);
21. Deve fazer a varredura no canal de operação do Ponto de Acesso sem impacto na performance da rede WLAN;
22. Deve utilizar os Pontos de Acesso para fazer a monitoração do ambiente Wireless procurando por pontos de acesso do tipo rogue de forma automática;
23. Deve ser possível especificar um ponto de acesso ou grupo de pontos de acesso para atuarem somente com a função de monitoramento visando detectar ataques e analisar o ambiente de rádio frequência;
24. Deverá ser capaz de localizar Pontos de Acesso do tipo rogue na planta baixa adicionada ao sistema com informações de, no mínimo:
 - a. 24.1. Pontos de Acesso que detectam;
 - b. 24.2. Tipo de Rogue;

- c. 24.3. Nome da Rede;
 - d. 24.4. Nível de sinal de detecção.
25. Na ocorrência de inoperância de um Ponto de Acesso, o controlador sem fio deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida;
 26. Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede e mudar as condições de rádio frequência baseado em desempenho;
 27. Detectar interferência e ajustar parâmetros de rádio frequência, evitando problemas de cobertura de RF de forma automática;
 28. Implementar sistema automático de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos para otimizar o desempenho;
 29. Implementar funcionalidade de balanceamento de carga entre os rádios de um mesmo Ponto de Acesso;
 30. Permitir que o serviço wireless seja desabilitado de determinado ponto de acesso. Também deve ser possível selecionar o serviço de qual rádio (banda) de determinado ponto de acesso deve ser desabilitado;
 31. Deve suportar BSS Coloring visando melhorar a eficiência na utilização do espectro;
 32. Suportar 802.11e;
 33. Deverá possuir funcionalidade de configuração do limite de banda disponível por usuário ou através de SSID/BSSID;
 34. Deverá permitir a configuração de prioridade de um determinado SSID sobre outros SSIDs existentes na controladora;
 35. Deve suportar WiFi Calling.

GARANTIA E SUPORTE

1. Garantia e suporte 24x7 do fabricante para a solução de software ofertada pelo período mínimo de 60 (sessenta) meses, incluindo a evolução para novas versões.
2. A proponente deverá informar em sua proposta o código de serviço de garantia do fabricante ("part number"), incorporada à solução.

9. CONFIGURAÇÃO, INSTALAÇÃO E MIGRAÇÃO DE AMBIENTE LEGADO

1. Todas as fases de planejamento, instalação e configuração poderão ser realizadas remotamente ou com a presença de técnicos da Contratada, que deverão possuir capacidade técnica necessária à execução do serviço;
2. Os trabalhos deverão ser realizados dentro do horário de funcionamento da UFBA, salvo casos onde necessite parada no ambiente que demande janelas de manutenção. Neste último caso, deve ser negociado os horários com antecedência;
3. Deve ser realizado previamente ao início dos trabalhos uma análise da topologia e arquitetura da rede, considerando os roteadores, switches e demais equipamentos de infraestrutura já existentes;
4. Deve realizar as configurações de acordo com as melhores práticas do fabricante;
5. A instalação e configuração do serviço incluirá:
6. Configuração lógica dos Pontos de Acesso e Controladora;
7. Instalação da controladora adquirida no ambiente determinado pela CONTRATANTE;
8. Criação de Template de configuração;
9. Não deve ser considerado como escopo do serviço a instalação física dos pontos de acesso;
10. Deverá entregar documentação detalhada ao final da realização dos trabalhos contendo o passo-a-passo de toda instalação e configuração dos equipamentos envolvidos no projeto.

14. ADENDO 04

SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA BAHIA
COORDENAÇÃO DE MATERIAL E PATRIMÔNIO

MODELO DE PROPOSTA DE PREÇOS**RAZÃO SOCIAL DA PROPONENTE:****CNPJ:****ENDEREÇO:****PESSOA DE CONTATO:****TELEFONE/ FAX/ E-MAIL:****VALIDADE:**

ITEM	DESCRIÇÃO/ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE	VALOR ESTIMADO UNITÁRIO	VALOR ESTIMA TOTAL
1	<p>LICENÇA DE PONTO DE ACESSO PARA A CONTROLADORA VIRTUAL SMART ZONE ESSENTIALS.</p> <p>Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador - Licença de ponto de acesso para a controladora virtual Smart zone Essentials. (Part number L09-0001-SG00)</p>	27464	Und.	500		
	<p>LICENÇA DO PACOTE DE SOFTWARES ADOBE CREATIVE CLOUD VIP, Versão: Última versão disponível, Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software</p>					

2	Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software, Última versão disponível - Licença de uso educacional da Suíte Adobe Creative Cloud for Teams Device Multiplataforma/Subscrição por 36 (trinta e seis) meses. Catser 27502	27502	Und.	69	R\$	R\$
3	LICENÇA DO SOFTWARE AUTODESK AUTOCAD REVIT LT , Última versão disponível, Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software Cessão temporária de direitos sobre programas de computador locação de software, Subscrição por 36 (trinta e seis) meses. Catser 27502	27502	Und.	5	R\$	R\$
4	LICENÇA DO SOFTWARE DE SOLUÇÃO DE ANTIVÍRUS CORPORATIVO , Última versão disponível, Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software, Última versão disponível - Subscrição por 36 (trinta e seis) meses. Catser 27502	27505	Und.	1000	R\$	R\$
5	LICENÇA DO SOFTWARE PARA SOLUÇÃO DE BACKUP PARA SERVIDORES , Versão: Última versão disponível. Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software. Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software, pelo período de 36 meses. Catser 27502	27502	Und.	1	R\$	R\$
6	LICENÇA DO SOFTWARE SKETCHUP LAB EDUCACIONAL, VERSÃO: Versão: Última versão disponível. Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software, Última versão	27502	Und.	30	R\$	R\$

	disponível - Subscrição por 36 (trinta e seis) meses. Catser 27502					
7	<p>LICENÇA PERPÉTUA DO SOFTWARE EDUCACIONAL CORELDRAW GRAPHICS SUITE, Versão: Última versão disponível, com atualizações por 02 anos. Licenciamento de direitos permanentes de uso de software para estação de trabalho.</p> <p>Aquisição de licença de uso do software coreldraw graphics suíte, versão: última versão disponível, período de 02 anos, inclusa a garantia, suporte e atualizações. Catser 27456</p>	27456	Und.	13	R\$	R\$
8	<p>LICENÇA PERPÉTUA DO SOFTWARE EDUCACIONAL DO SOFTWARE RHINO-EDIÇÃO BRASIL - Versão: Última versão disponível.</p> <p>Licenciamento de direitos permanentes de uso de software para estação de trabalho.</p> <p>Licenciamento de direitos permanentes de uso de software para estação de trabalho.</p> <p>Licença educacional Edição Brasil - Versão: Última versão disponível. LAB KIT – 30 usuários para usar o Rhino nos computadores em uma única sala de aula ou laboratório. Catser 27456</p>	27456	Und.	3	R\$	R\$
9	<p>LICENÇA PERPÉTUA DO SOFTWARE MICROSOFT OFFICE PROFESSIONAL PLUS EDUCACIONAL - VERSÃO: ÚLTIMA VERSÃO DISPONÍVEL,</p> <p>Licenciamento de direitos permanentes de uso de software para estação de trabalho.</p> <p>Microsoft Office Professional Plus Educacional Versão: Última versão disponível para PC – O pacote deve incluir versões completas do Word, Excel, PowerPoint, OneNote, Access e Publisher – Versão 32/64 bits. Catser 27456</p>	27456	Und.	648	R\$	R\$

10	<p>LICENÇA PERPÉTUA DO SOFTWARE MICROSOFT SQL SERVER, Versão: Última versão disponível. Licenciamento de direitos permanentes de uso de software para servidor.</p> <p>Licenciamento de direitos permanentes de uso de software para servidor. Catser 27464</p>	27464	Und.	1	R\$	R\$
11	<p>LICENÇA PERPÉTUA DO SOFTWARE MICROSOFT WINDOWS SERVER 2022 REMOTE DESKTOP SERVICES - 1 USER CAL - VERSÃO: ÚLTIMA VERSÃO DISPONÍVEL,</p> <p>Licenciamento de Direitos Permanentes de Uso de Software para Estação de Trabalho. Catser 27456</p>	27456	Und.	150	R\$	R\$
12	<p>LICENÇA PERPÉTUA DO SOFTWARE MICROSOFT WINDOWS SERVER DATACENTER PER CORE, Licenciamento de Direitos Permanentes de Uso de Software para Servidor.</p> <p>Licença Perpétua Do Software Microsoft Windows Server Datacenter Per Core 2 Licences - Versão: Última Versão Disponível. Catmat: 27464</p>	27464	Und.	30	R\$	R\$
13	<p>LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA SERVIDOR - CONTROLADORA VIRTUAL SMART ZONE ESSENTIALS.</p> <p>Licenciamento de direitos permanentes de uso de software para servidor - Controladora Virtual Smartzone Essentials. (Part number L09-VSCG-WW00)</p>	27464	Und.	1		
	<p>SISTEMA DE GESTÃO LGPD PROTEGON, VERSÃO: Última versão disponível, Cessão</p>					

14	Temporária de Direitos Sobre Programas de Computador Locação de Software Cessão temporária de direitos sobre programas de computador locação de software. Subscrição por 12 (doze) meses. Catser 27502	27502	Und.	1	R\$	R\$
15	SOFTWARE AUTODESK ARCHITECTURE ENGINEERING & CONSTRUCTION COLLECTION , Última versão disponível, Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software Cessão temporária de direitos sobre programas de computador locação de software, Subscrição por 36 (trinta e seis) meses. Catser 27502	27502	Und.	2	R\$	R\$

15. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

Despacho: PORTARIA Nº 87 – PROAD, DE 04 DE JULHO DE 2023

LEONARDO JORDAO DE CARVALHO
TÉCNICO DE TECNOLOGIA DA INFORMAÇÃO