



UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

Pró-Reitoria de Gestão e Governança
Gabinete da Superintendência-Geral de Gestão
Coordenação Geral de Contratos

CONTRATO Nº 28/2024

Processo nº 23079.239092/2024-93

PARA AQUISIÇÃO, EM CARÁTER EMERGENCIAL, DE EQUIPAMENTOS DE REDE, QUE FAZEM ENTRE SI A UNIVERSIDADE FEDERAL DO RIO DE JANEIRO E A EMPRESA ZIVA TECNOLOGIA E SOLUÇÕES LTDA.

A **UNIVERSIDADE FEDERAL DO RIO DE JANEIRO**, com sede na Rua Antônio Barros de Castro, 119, Parque Tecnológico, Cidade Universitária, CEP 21.941-853, na Cidade do Rio de Janeiro/RJ, inscrita no CNPJ sob o nº 33.663.683/0001-16, neste ato sendo representada pela Pró-Reitora de Gestão e Governança, Senhora Claudia Ferreira da Cruz, conforme delegação de competência determinada pela Portaria nº 578 de 12 de julho de 2023, do Senhor Reitor, doravante denominada **CONTRATANTE**, e a empresa **ZIVA TECNOLOGIA E SOLUÇÕES LTDA**, inscrita no CNPJ: 05.816.526/0004-00, sediada na Rodovia Governador Mario Covas, nº 0, Sala 56, KM 290, Serra do Anil, Cariacica/ES - CEP 29147-030, doravante designado **CONTRATADO**, neste ato representada pela Senhora Patrícia Angelina da Conceição, conforme atos constitutivos da empresa OU procuração apresentada nos autos, tendo em vista o que consta no Processo nº 23079.239092/2024-93 e seus relacionados, e em observância às disposições da [Lei nº 14.133, de 1º de abril de 2021](#), e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Ato de Contratação Direta nº 106/2024 (ID PNCP 000752/2024), mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO ([ART. 92, I E II](#))

- 1.1. O objeto do presente instrumento é a aquisição de equipamentos de rede, em caráter emergencial, conforme condições, quantidades e exigências estabelecidas no anexo e no Termo de Referência.
- 1.2. Objeto da contratação: conforme anexo.
- 1.3. Vinculam esta contratação, independentemente de transcrição:
 - 1.3.1. O Termo de Referência;
 - 1.3.2. A Autorização de Contratação Direta e/ou o Aviso de Dispensa Eletrônica, caso existentes;
 - 1.3.3. A Proposta do contratado;
 - 1.3.4. Eventuais anexos dos documentos supracitados.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência deste Termo de Contrato é de até 01(um) ano, com início em 26 de agosto de 2024, início da execução em 27 de agosto de 2024 e encerramento em 26 de agosto de 2025, improrrogável, na forma do art. 75, VIII da Lei nº 14.133/2021.

2.1.1. A vigência poderá ultrapassar o exercício financeiro, desde que as despesas referentes à contratação sejam integralmente empenhadas até 31 de dezembro, para fins de inscrição em restos a pagar, conforme Orientação Normativa AGU nº 39, de 13 de dezembro de 2011.

2.2. O fornecimento da solução será iniciado a partir de 27 de agosto de 2024, e suas etapas observarão o cronograma fixado no Termo de Referência.

Período para entrega: 27/08/2024 a 10/09/2024;

Aceite provisório: no ato da entrega;

Período para aceite definitivo: 11/09/2024 a 20/09/2024;

2.3. A Contratada se responsabilizará pela garantia de que tratam os subitens 1.3.1 e 4.15 a 4.25 do Termo de Referência da contratação, pelo período de 60(sessenta) meses, a partir do recebimento definitivo do objeto, independentemente da vigência contratual.

Período de Garantia do equipamento, dentro da vigência contratual: De 21/09/2024 a 26/08/2025;

Período de Garantia do equipamento, após encerramento da vigência contratual: de 27/08/2025 a 20/09/2029;

2.4. Após o recebimento do objeto, deverá ser formalizado Termo Aditivo ao presente contrato, com adequação do registro do período de 60(sessenta) meses da garantia do equipamento, caso seja necessário, já que os períodos indicados na Subcláusula 2.2 podem ser antecipados, ou atrasados.

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS ([ART. 92, IV, VII E XVIII](#))

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

5. CLÁUSULA QUINTA - PREÇO

5.1. O valor total da contratação é de R\$ 547.000,00 (quinhentos e quarenta e sete mil reais).

5.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

5.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado

dependerão dos quantitativos efetivamente fornecidos.

6. CLÁUSULA SEXTA - PAGAMENTO ([ART. 92, V E VI](#))

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

7. CLÁUSULA SÉTIMA - REAJUSTE ([ART. 92, V](#))

7.1. Os preços inicialmente contratados são fixos e irredutíveis no prazo de um ano contado da data do orçamento estimado.

7.2. Após o interregno de um ano, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

7.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

7.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

7.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

7.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.8. O reajuste será realizado por apostilamento.

8. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE ([ART. 92, X, XI E XIV](#))

8.1. São obrigações do Contratante:

8.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

8.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

8.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.1.5. Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no

prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência.

8.1.6. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.1.7. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

8.1.8. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

8.1.9. Administração terá o prazo de 1 (um) mês, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.1.10. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 90 (noventa) dias.

8.1.11. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.2. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

9. CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO ([ART. 92, XIV, XVI E XVII](#))

9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.1.1. Entregar o objeto acompanhado do manual do usuário, com uma versão em português, e da relação da rede de assistência técnica autorizada;

9.1.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor ([Lei nº 8.078, de 1990](#));

9.1.3. Comunicar ao contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

9.1.4. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior ([art. 137, II, da Lei n.º 14.133, de 2021](#)) e prestar todo esclarecimento ou informação por eles solicitados;

9.1.5. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.1.6. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

9.1.7. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos: 1) prova de

regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

9.1.8. Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato;

9.1.9. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual.

9.1.10. Paralisar, por determinação do contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

9.1.11. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para qualificação na contratação direta;

9.1.12. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação ([art. 116, da Lei n.º 14.133, de 2021](#));

9.1.13. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas ([art. 116, parágrafo único, da Lei n.º 14.133, de 2021](#));

9.1.14. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

9.1.15. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no [art. 124, II, d, da Lei nº 14.133, de 2021](#).

9.1.16. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do contratante;

9.1.17. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

9.1.18. Orientar e treinar seus empregados sobre os deveres previstos na Lei nº 13.709, de 14 de agosto de 2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste contrato;

9.1.19. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina.

9.1.20. Submeter previamente, por escrito, ao contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

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

10. CLÁUSULA DÉCIMA – OBRIGAÇÕES PERTINENTES À LGPD

10.1. As partes deverão cumprir a [Lei nº 13.709, de 14 de agosto de 2018 \(LGPD\)](#), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

10.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do [art. 6º da LGPD](#).

10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

10.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

10.5. terminado o tratamento dos dados nos termos do [art. 15 da LGPD](#), é dever do contratado eliminá-los, com exceção das hipóteses do [art. 16 da LGPD](#), incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

10.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados ([LGPD, art. 37](#)), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

11. CLÁUSULA DÉCIMA PRIMEIRA– GARANTIA DE EXECUÇÃO ([ART. 92, XII](#))

11.1. A contratação conta com garantia de execução, nos moldes do [art. 96 da Lei nº 14.133](#), de 2021, na modalidade seguro garantia, em valor correspondente a 5% (cinco por cento) do valor inicial/total/anual do contrato.

11.2. Caso utilizada a modalidade de seguro-garantia, a apólice deverá ter validade durante a vigência do contrato e por mais 90 (noventa) dias após término deste prazo de vigência, permanecendo em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.

11.3. A apólice do seguro garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

11.4. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no item 11.10 deste contrato.

11.5. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

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

11.6.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

11.6.2. multas moratórias e punitivas aplicadas pela Administração à contratada; e

11.6.3. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

11.7. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 11.11, observada a legislação que rege a matéria.

11.8. A garantia em dinheiro deverá ser efetuada em favor do contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

11.9. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério competente.

11.10. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do [artigo 827 do Código Civil](#).

11.11. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

11.12. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

11.13. O Contratante executará a garantia na forma prevista na legislação que rege a matéria.

11.13.1. O emitente da garantia ofertada pelo contratado deverá ser notificado pelo contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais ([art. 137, § 4º, da Lei n.º 14.133, de 2021](#)).

11.13.2. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do [art. 20 da Circular Susep nº 662, de 11 de abril de 2022](#).

11.14. Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do contratante, mediante termo circunstanciado, de que o contratado cumpriu todas as cláusulas do contrato;

11.15. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

11.16. O garantidor não é parte para figurar em processo administrativo instaurado pelo contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

11.17. O contratado autoriza o contratante a reter, a qualquer tempo, a garantia, na forma prevista no Edital e neste Contrato.

11.17.1. A garantia de execução é independente de eventual garantia do produto ou serviço prevista especificamente no Termo de Referência.

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS ([ART. 92, XIV](#))

12.1. Comete infração administrativa, nos termos da [Lei nº 14.133, de 2021](#), o contratado que:

- a) der causa à inexecução parcial do contrato;
- b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no [art. 5º da Lei nº 12.846, de 1º de agosto de 2013](#).

12.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

- i. Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave ([art. 156, §2º, da Lei nº 14.133, de 2021](#));
- ii. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave ([art. 156, § 4º, da Lei nº 14.133, de 2021](#));
- iii. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave ([art. 156, §5º, da Lei nº 14.133, de 2021](#)).
- iv. Multa:
 - 1. Moratória de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 15 (quinze) dias;
 - 2. Moratória de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso injustificado, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.
 - i. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.
 - 3. Compensatória, para as infrações descritas nas alíneas “e” a “h” do subitem 11.1, de 10% (dez por cento) a 30% (trinta por cento) do valor do Contrato.
 - 4. Compensatória, para a inexecução total do contrato prevista na alínea “c” do subitem 11.1, de 10% (dez por cento) a 30% (trinta por cento) do valor do Contrato.

5. Para infração descrita na alínea “b” do subitem 11.1, a multa será 10% (dez por cento) a 30% (trinta por cento) do valor do Contrato.

6. Para infrações descritas na alínea “d” do subitem 11.1, a multa será de 2% (dois por cento) a 15% (quinze por cento) do valor do Contrato.

7. Para a infração descrita na alínea “a” do subitem 11.1 a multa será de 10% (dez por cento) a 30% (trinta por cento) do valor do Contrato.

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante ([art. 156, §9º, da Lei nº 14.133, de 2021](#))

12.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa ([art. 156, §7º, da Lei nº 14.133, de 2021](#)).

12.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação ([art. 157, da Lei nº 14.133, de 2021](#))

12.4.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente ([art. 156, §8º, da Lei nº 14.133, de 2021](#)).

12.4.3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do [art. 158 da Lei nº 14.133, de 2021](#), para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

12.6. Na aplicação das sanções serão considerados ([art. 156, §1º, da Lei nº 14.133, de 2021](#)):

- a) a natureza e a gravidade da infração cometida;
- b) as peculiaridades do caso concreto;
- c) as circunstâncias agravantes ou atenuantes;
- d) os danos que dela provierem para o Contratante;
- e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.7. Os atos previstos como infrações administrativas na [Lei nº 14.133, de 2021](#), ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na [Lei nº 12.846, de 2013](#), serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei ([art. 159](#)).

12.8. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia ([art. 160, da Lei nº 14.133, de 2021](#)).

12.9. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da

sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. ([Art. 161, da Lei nº 14.133, de 2021](#)).

12.10. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do [art. 163 da Lei nº 14.133/21](#).

12.11. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

13. CLÁUSULA DÉCIMA TERCEIRA– DA EXTINÇÃO CONTRATUAL ([ART. 92, XIX](#))

13.1. O contrato será extinto quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.

13.2. Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato.

13.2.1. Quando a não conclusão do contrato referida no item anterior decorrer de culpa do contratado:

- a) ficará ele constituído em mora, sendo-lhe aplicáveis as respectivas sanções administrativas; e
- b) poderá a Administração optar pela extinção do contrato e, nesse caso, adotar as medidas admitidas em lei para a continuidade da execução contratual.

13.3. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no [artigo 137 da Lei nº 14.133/21](#), bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.3.1. Nesta hipótese, aplicam-se também os [artigos 138 e 139 da mesma Lei](#).

13.3.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

13.3.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.4. O termo de extinção, sempre que possível, será precedido:

13.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.4.2. Relação dos pagamentos já efetuados e ainda devidos;

13.4.3. Indenizações e multas.

13.5. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório ([art. 131, caput, da Lei n.º 14.133, de 2021](#)).

13.6. O contrato poderá ser extinto:

13.6.1. caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica,

financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função ~~na licitação~~ no processo de contratação direta ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021);

14. CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA ([ART. 92, VIII](#))

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, nas dotações abaixo discriminadas:

I. Gestão/Unidade: 15236/153115

II. Fonte de Recursos:1000

III. Programa de Trabalho:230296

IV. Elemento de Despesa:449052

V. Plano Interno:V0000G01CIN

VI. Nota de Empenho: 2024NE596

I. Gestão/Unidade: 15236/153115

II. Fonte de Recursos:1000

III. Programa de Trabalho:230300

IV. Elemento de Despesa:339040

V. Plano Interno:V0000G01CIN

VI. Nota de Empenho: 2024NE000592

14.2. As dotações relativas aos exercícios financeiros subsequentes serão indicadas após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

15. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS ([ART. 92, III](#))

15.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na [Lei nº 14.133, de 2021](#), e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na [Lei nº 8.078, de 1990 – Código de Defesa do Consumidor](#) – e normas e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos [arts. 124 e seguintes da Lei nº 14.133, de 2021](#).

16.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

16.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do [art. 136 da Lei nº 14.133, de 2021](#).

17. CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no [art. 94 da Lei 14.133, de 2021](#), bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei n.º 14.133, de 2021, e ao [art. 8º, §2º, da Lei n. 12.527, de 2011](#), c/c [art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012](#).

18. CLÁUSULA DÉCIMA OITAVA– FORO ([ART. 92, §1º](#))

18.1. Fica eleito o Foro da Justiça Federal da Cidade do Rio de Janeiro para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme [art. 92, §1º, da Lei nº 14.133/21](#).

Claudia Ferreira da Cruz
Universidade Federal do Rio de Janeiro
CONTRATANTE

Patrícia Angelina da Conceição
Ziva Tecnologia e Soluções Ltda
CONTRATADO

TESTEMUNHAS:

1-

2-

ANEXO I AO TERMO DE CONTRATO Nº 28/2024

ITEM	ESPECIFICAÇÃO	CÓDIGO	UND	QUANT	PREÇO UNITARIO	PREÇO TOTAL
1		609340	und	01	R\$489.755,00	R\$489.755,00

SOLUÇÃO DE SEGURANÇA DE REDES NGFW

- Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux;
- Deverá ser entregue em equipamento único, para atender as funcionalidades exigidas;
- Deverá possuir e estar licenciado pelo período de 60 (sessenta) meses para suporte, garantia, atualização de firmware e atualização automática de bases de dados, incluindo as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Otimização WAN, DLP – Data Leak Prevention.
- Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários;
- Deverá incluir licença para a funcionalidade de VPN SSL;
- Deverá incluir licença para atualização de vacina de antivírus/anti-spyware.

- Deverá incluir licença de atualização para filtro de conteúdo Web;
- Deverá incluir licença de atualização do IPS e da lista de aplicações detectadas;
- Deverá possuir licença para número ilimitado de usuários e endereços IP;
- Deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de proteção avançada durante a vigência contratual;
- Deverá possuir um relatório de uso de mídia social;
- Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

FUNCIONALIDADES DE FIREWALL

- Deverá possuir controle de acesso à internet por endereço IP de origem e destino;
- Deverá possuir controle de acesso à internet por subrede;
- Deverá suportar tags de VLAN (802.1q);
- Deverá possuir ferramenta de diagnóstico do tipo tcpdump;
- Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
- Deverá possuir integração com tokens para autenticação de 02

- (dois) fatores;
- Deverá suportar single-sign-on para Active Directory, Citrix e RADIUS;
 - Deverá possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP);
 - Deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;
 - Deverá permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
 - Deverá permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;
 - Deverá possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;
 - Deverá suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;
 - 3.1.2.14. Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;
 - Deverá suportar aplicações multimídia, como: H.323 e SIP;
 - Deverá possuir tecnologia de firewall do tipo Statefull;
 - Deverá possuir alta

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

- Deverá permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;
- Deverá suportar PBR – Policy Based Routing;
- Deverá permitir a criação de VLANs no padrão IEEE 802.1q;
- 3.1.2.21. Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
- Deverá permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;
- Deverá permitir forwarding de camada 2 para protocolos não IP;
- Deverá suportar forwarding multicast;
- Deverá suportar roteamento multicast PIM Sparse Mode e Dense Mode;
- Deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos:
 - TCP, UDP, ICMP e IP;
- Deverá permitir o agrupamento de serviços;
- Deverá permitir o filtro

- | | | | | | | |
|---|--|--|--|--|--|--|
| de pacotes sem a utilização de NAT; | | | | | | |
| • Deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas; | | | | | | |
| • Deverá possuir mecanismo de anti-spoofing; | | | | | | |
| • Deverá permitir criação de regras definidas pelo usuário; | | | | | | |
| • Deverá permitir o serviço de autenticação para tráfego HTTP e FTP; | | | | | | |
| • Deverá permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing; | | | | | | |
| • Deverá possuir a funcionalidade de balanceamento e contingência de links; | | | | | | |
| • Deverá suportar sFlow; | | | | | | |
| • Solução deve ser capaz de prover Zero Touch provisioning. | | | | | | |
| • Deverá possuir Módulo de plataforma confiável (TPM). | | | | | | |
| • A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN. | | | | | | |
| • O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas. | | | | | | |
| • Deverá ter a capacidade de permitir | | | | | | |

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

- Deverá ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;
- Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
- Deverá permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;
- Deverá suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;
- Deverá permitir funcionamento em modo bridge, router,

proxy explícito, sniffer e/ou VLAN- tagged;

- Deverá possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 O, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;
- Deverá suportar SIP, H.323 e SCCP NAT Traversal;
- Deverá permitir a criação de objetos e
- agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;
- Deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

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

FUNCIONALIDADE DE ANTI-SPAM DE

GATEWAY

- Deverá permitir, na funcionalidade de AntiSpam, verificação do cabeçalho SMTP do tipo MIME;
- Deverá possuir filtragem de e-mail por palavras chaves;
- Deverá permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;
- Deverá possuir, para a funcionalidade de AntiSpam, o recurso de RBL;
- Deverá permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;
- Deverá ter a capacidade de permitir a criação de perfis de AntiSpam específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo:
 -
- Deverá permitir priorização de tráfego e suportar ToS;
- Deverá limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de

identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
- Deverá permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;
- Deverá ter a capacidade de permitir a criação de perfis de controle de banda específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.
- tablets, celulares e PCs.
- Deverá possuir solução de filtro de conteúdo Web integrado à solução de segurança;
- Deverá possuir, pelo menos, 70 (setenta) categorias para

classificação de sites Web;

- Deverá possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;
- Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;
- Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo; Webmail; Instituições de saúde; Notícias; Phishing; Hackers; Pornografia; Racismo; Websites pessoais; Compras;
- Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
- Deverá permitir a criação de, pelo menos, 05 (cinco) categorias personalizadas;
- Deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;
- Deverá prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
- Deverá prover funcionalidade de

identificação transparente de usuários cadastrados no Microsoft Active Directory;

- Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;
- Deverá permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;
- Deverá permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;
- Deverá permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);
- Deverá permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;
- Deverá filtrar o conteúdo baseado em categorias em tempo real;
- Deverá garantir que as atualizações regulares do produto sejam

realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

- Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem;
- Deverá ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;
- Deverá permitir o bloqueio de redirecionamento HTTP;
- Deverá permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;
- Deverá possuir Proxy Explícito e Transparente;
- Deverá implementar roteamento WCCP e ICAP;
- Deverá ter a capacidade de permitir a criação de perfis de filtragem Web específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais

Android, Apple,
Blackberry, Linux e
Windows.

FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

- Deverá permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
- Deverá possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;
- Deverá estar orientado à proteção de redes;
- Deverá permitir funcionar em modo transparente, sniffer e router;
- Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
- Deverá permitir a criação de padrões de ataque manualmente;
- Deverá possuir integração à plataforma de segurança;
- Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;
- Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;

- | | | | | | | |
|---|--|--|--|--|--|--|
| <ul style="list-style-type: none">• Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;• Deverá possuir mecanismos de detecção/proteção de ataques;• Deverá possuir reconhecimento de padrões;• Deverá possuir análise de protocolos;• Deverá possuir detecção de anomalias;• Deverá possuir detecção de ataques de RPC (Remote Procedure Call);• Deverá possuir proteção contra-ataques de Windows ou NetBios;• Deverá possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);• Deverá possuir proteção contra-ataques DNS (Domain Name System);•• Deverá possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;• Deverá possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);• Deverá possuir métodos de notificação de detecção de ataques;• Deverá possuir alarmes na console de | | | | | | |
|---|--|--|--|--|--|--|

- | | | | | | | |
|---|--|--|--|--|--|--|
| administração; | | | | | | |
| • Deverá possuir alertas via correio eletrônico; | | | | | | |
| • Deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede; | | | | | | |
| • Deverá ter a capacidade de resposta/logs ativa a ataques; | | | | | | |
| • Deverá prover a terminação de sessões via TCP resets; | | | | | | |
| • Deverá armazenar os logs de sessões; | | | | | | |
| • Deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos; | | | | | | |
| • Deverá mitigar os efeitos dos ataques de negação de serviços; | | | | | | |
| • Deverá permitir a criação de assinaturas personalizadas; | | | | | | |
| • Deverá possuir filtros de ataques por anomalias; | | | | | | |
| • Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination; session limit; | | | | | | |
| • Deverá permitir filtros de anomalias de protocolos; | | | | | | |
| • Deverá suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion; | | | | | | |
| • Deverá suportar verificação de ataque na camada de aplicação; | | | | | | |
| • Deverá suportar | | | | | | |

verificação de tráfego em tempo real, via aceleração de hardware;

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

FUNCIONALIDADE DE VPN

- Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- Deverá possuir suporte a certificados PKI X.509 para construção de VPNs;
- Deverá possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSeC Client-to-Site;
- Deverá possuir suporte a VPN SSL;
- Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- A VPN SSL deverá possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
- Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;
- A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS X; 3.1.7.9.
- Deverá permitir a arquitetura de VPN hub and spoke;
- Deverá possuir suporte a inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple

Certificate Enrollment Protocol) e mediante arquivos.

**FUNCIONALIDADE DE
CONTROLE DE
APLICAÇÕES**

- Deverá reconhecer, no mínimo, 2.000 (duas mil) aplicações;
- Deverá possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;
- Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P; Transferência de arquivos; VoIP;
- Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active

Directory;

- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;
- Deverá permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;
- Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;
- Deverá permitir criação de padrões de aplicação manualmente;

FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION)

- O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de Informações) de gateway deverá funcionar de maneira que se consiga que os dados confidenciais e ou de identificação pessoal não saiam da rede e também deverá

funcionar de modo que se previna que dados não requisitados entrem na sua rede;

- Deverá inspecionar, no mínimo, os tráfegos de e-mail, HTTP, NNTP e de mensageiros instantâneos;
- Sobre o tráfego de e-mail, deverá inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;
- Deverá realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS- Word;
- Deverá fazer a varredura no conteúdo de um cookie HTTP buscando por determinado texto;
- Deverá aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;
- Deverá verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saindes possui um tamanho máximo especificado pelo administrador;
- Deverá utilizar expressões regulares para composição das regras de verificação dos tráfegos;
- Deverá tomar minimamente as ações de bloquear, banir usuário e colocar em quarentena a interface sobre as regras que coincidirem com o tráfego esperado pela regra;
- Deverá permitir o armazenamento em solução específica de armazenamento de

logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail, HTTP e mensageiros instantâneos;

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

FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

- Deverá permitir a criação de endereços IPs virtuais;
- Deverá permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;
- Deverá suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;
- Deverá permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Round Robin, Weighted Round Robin, First Alive e HTTP host;
- Deverá permitir persistência de sessão por cookie HTTP ou SSL session ID;
- Deverá permitir que seja mantido o IP de origem;
- Deverá suportar SSL offloading nos equipamentos que suportem, pelo menos,

- | | | | | | | |
|--|--|--|--|--|--|--|
| 200 (duzentos) usuários; | | | | | | |
| <ul style="list-style-type: none">• Deverá ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;• Deverá permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável. | | | | | | |

FUNCIONALIDADE DE SD-WAN

- | | | | | | | |
|--|--|--|--|--|--|--|
| <ul style="list-style-type: none">• A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.• A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.• A solução SD-WAN deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.• A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.• Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em | | | | | | |
|--|--|--|--|--|--|--|

que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

- A solução deve ser capaz de criar VPN "Full-Mesh" em interface Gráfica, de forma automática, e sem que o administrador precise configurar site por site.
- A configuração VPN IPSEC deverá oferecer suporte para DH Group: 14 e 15.
- Reconhecimento em camada 7 totalmente segregado da camada 4.
- Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.
- O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc)
- A solução de SD-WAN

deve suportar Roteamento dinâmico BGP com suporte a IPv6.

- A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.
- A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SDWAN.
- A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de Saúde melhor que o link atual.
- A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.
- A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

CARACTERISTICAS

ESPECÍFICAS

- Deverá possuir fonte de alimentação com chaveamento automático 110/220V redundante Hot Swappable.
- A fonte fornecida deverá suportar sozinha a operação da unidade com todos os módulos de interface ativos.
- IPS com capacidade mínima de processamento de 12 (doze) Gbps.
- Proteção a ameaças avançadas, isto é, com as funções de Firewall, IPS, controle de aplicação e proteção de Malware/Antivírus ativadas, com capacidade mínima de processamento de 10 (dez) Gbps.
- Caso o fabricante divulgue múltiplos valores para este requisito, somente o de menor valor será aceito;
- Inspeção SSL Throughput com capacidade mínima de processamento de 9 (nove) Gbps.
- VPN com capacidade de, pelo menos, 55 (cinquenta e cinco) Gbps de tráfego IPsec.
- VPN SSL com capacidade de, pelo menos, 4 (quatro) Gbps de tráfego.
- Suportar no mínimo throughput de 100 Mpps (milhões de pacotes por segundo)
- Deverá suportar 8.000.000 (oito milhões) de sessões concorrente.
- Deverão ser licenciados para

suportar, pelo menos, 8.000 (oito mil) usuários de VPN SSL. • Deverá suportar, pelo menos, 500.000 (quinhentas mil) novas conexões por segundo. • Deverá suportar, pelo menos, 2.000 (dois mil) túneis de VPN Site-Site. • Deverá suportar, pelo menos, 40.000 (quarenta mil) túneis de VPN Client-Site. • Deverá possuir, pelo menos, 04 (quatro) interfaces SFP28 25GE. • Deverá possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE. • Deverá possuir, pelo menos, 14 (quatorze) interfaces 1 GE RJ 45. • Deverá possuir porta USB 3.0 para conexão de modem 3G/4G. • Deverá acompanhar 2 SFP+ 10 Gbps multimodo para interligação aos equipamentos adjacentes. • Deverá possuir homologação junto a ANATEL; • Desejável que seja capaz de gerenciar equipamentos de pontos de acesso sem fio, via funcionalidade de Controladora Wireless. • Desejável que seja capaz de gerenciar switches, via funcionalidade de Controladora Switch. • Migração de configuração para o equipamento adquirido.					
---	--	--	--	--	--

2	Treinamento para equipe técnica sobre solução adquirida.	20052	und	01	R\$57.245,00	R\$57.245,00
TOTAL					VALOR	R\$547.000,00

PATRICIA
ANGELINA DA
CONCEICAO: [Redacted]
Assinado de forma digital
por PATRICIA ANGELINA
DA
CONCEICAO: [Redacted]
Dados: 2024.08.23
16:15:19 -03'00'

gov.br Documento assinado digitalmente
DANIELE MENDONCA DELGADO
Data: 23/08/2024 17:56:33-0300
Verifique em https://validar.itl.gov.br

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Atualização: maio/2023
Termo de contrato modelo para Pregão Eletrônico para contratação de compras/Solução de Tecnologia da Informação e Comunicação
Aprovado pela Secretaria de Governo Digital.
Identidade visual pela Secretaria de Gestão

gov.br Documento assinado digitalmente
RENATA RIFFAN PESSANHA MAIA BELMONT
Data: 27/08/2024 10:19:39 0300
Verifique em https://validar.itl.gov.br