MINISTÉRIO DAS COMUNICAÇÕES

PROJETO BÁSICO

Segurança em Nuvem para Tratamento e Proteção de Sítios Web
(GovShield)

Referência: Arts. 12 a 24 IN SGD/ME Nº 1/2019

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação de serviços continuados de segurança em nuvem para tratamento e proteção de sítios Web, na modalidade Plataforma como Serviço (PaaS), denominada **GovShield**, a serem executados conforme condições, quantidades e exigências estabelecidas neste Projeto Básico.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. Bens e Serviços que compõem a solução

Grupo	Item	Descrição Serviço	M
1	1	GovShield - Plataforma de proteção básica e distribuição de conteúdo para proteção de sítios Web HTTP e HTTPS vinculadas a domínio DNS e seus respetivos subdomínios.	
	2	Adicional de 1 TB referente ao tráfego de acesso externo aos sítios Web.	

2.1.1. O GovShield é uma plataforma de segurança em nuvem para tratamento e proteção de sítios Web com CDN (*Content Delivery Network*), que conta com um conjunto de ferramentas de proteção contra ataques, interrompendo o tráfego malicioso antes que ele atinja o sítio do MCOM.

2.1.2. A modalidade bronze possui as funcionalidades listadas abaixo, onde o SERPRO faz toda a gestão e entrega os relatórios de segurança ao final do mês ou sob demanda.

a) Volume de 1 TB de tráfego de acesso externo aos sítios Web;

b) Administração do ambiente realizada pelo SERPRO;

c) Política de segurança padrão do SERPRO;

d) *Web Application Firewall;*

e) Proteção contra DDoS;

f) CDN (*Content Delivery Network*);

g) Aceleração e Disponibilidade de DNS;

h) Proteção contra ataques ao Servidor DNS;

i) Aceleração na resolução de nomes no DNS;

j) Base dinâmica de reputação de IPs;

k) Atendimento de Solicitação de Serviço 8x5;

l) Suporte 24/7;

m) SLA da plataforma de 99,70%;

n) Tratamento de incidente de segurança.

2.1.3. Os serviços são vinculados mensalmente a um domínio DNS e seus respectivos subdomínios.

2.1.4. A modalidade bronze possui 1 TB disponível mensalmente para proteção de sítios web. O adicional de Terabytes que exceder o disponível pela modalidade será cobrado a partir do 3º (terceiro) mês de consumo.

2.1.5. O serviço adicional descrito no item 2 da tabela acima se trata de item a ser executado sob demanda, **sem garantia de consumo**, excepcionalmente se ultrapassado o volume mensal previsto para o item 1.

3 – JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

3.1.1 O Ministério das Comunicações, diante da necessidade de manutenção e disponibilidade adequadas de suas infraestruturas de TI, para a necessária proteção de seu sítio e atualização contínua e transparente do conjunto de regras de segurança contra os mais recentes ataques cibernéticos, busca, por meio dessa contratação, disponibilizar uma plataforma de segurança em nuvem composta por um conjunto de ferramentas e recursos de proteção com análise de tráfego, contra ataques, interrompendo qualquer tráfego malicioso antes de atingir o sítio do MCOM.

3.1.2 A contratação de serviços em nuvem objetiva benefícios que são consequentes da abstração, da complexa e onerosa gestão dos recursos computacionais necessários para que as soluções de segurança sejam implantadas e se mantenham em funcionamento com a qualidade e segurança devidas. Essa abstração inclui a despreocupação com aquisição ou contratação de licenças de *softwares*, *hardwares*, manutenção da infraestrutura e logística dos recursos tecnológicos, *upgrade* das soluções contratadas, garantias de continuidade e segurança.

3.1.3 O fornecimento de serviços *online* com escalabilidade de acordo com a sazonalidade de tráfego e a extensão do serviço proporcionará a gestão de produtos de segurança, com soluções inovadoras e de baixo custo para o MCOM. Assim, com a pretensa contratação busca-se aumentar a eficácia operacional e a melhoria na oferta de serviços à sociedade.

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

3.2.1. Objetivos Estratégicos

OBJETIVO ESTRATÉGICO	REFERÊNCIA
Garantir recursos materiais e infraestrutura de TIC necessários ao desempenho das atribuições institucionais.	Mapa Estratégico MCOM 2021-2023

3.2.2. Alinhamento ao PDTIC MCOM (2023)

Tendo em vista que o PDTIC 2023 está em fase de elaboração, foi solicitada a inclusão da contratação no PDTIC 2023, conforme formulário SEI 10261093, item "Solução de Gestão de Vulnerabilidades".

3.2.3. Alinhamento ao PAC MCOM (2023)

ITEM	DESCRIÇÃO	REFERÊNCIA
CGTI - 16	Solução de Gestão de Vulnerabilidades	https://www.gov.br/mcom/pt-br/acesso-a-informacao/transparencia-e-prestacao-de-contas/licitacoes-e-contratos-1/PCA2023VERSAOFINAL.pdf

3.2.4. Registra-se que contratação está em consonância com os documentos estratégicos elencados no art. 6º da IN SGD/ME nº 1/2019, citados acima. Os alinhamentos à Estratégia de Governo Digital - EGD 2023 serão observados em momento oportuno, pois ainda não foi divulgada a EGD para o ano de 2023.

3.2.5. Ressalta-se que a contratação não tem por objetivo a oferta digital de serviços públicos.

3.3. Estimativa da demanda

3.3.1. Considerando a quantidade de serviços disponibilizados externamente pelo MCOM, em levantamento realizado pela equipe técnica da CGTI, a estimativa da demanda é de fornecer proteção para aproximadamente 50 (cinquenta) sítios do domínio *mcom.gov.br.

3.3.2. Para escolha da modalidade a ser contratada, o MCOM identificou durante o periodo de degustação da ferramenta, que tanto as funcionalidades quanto o volume disponibilizados na modalidade bronze são suficientes para atender às necessidades do órgão.

3.4. Parcelamento da Solução de TIC

3.4.1. Não se aplica o parcelamento da solução por se tratar de produto/serviço único.

3.5. Resultados e Benefícios a Serem Alcançados

3.5.1. Manter o nível de proteção das informações armazenadas e do investimento em tecnologia da informação;

3.5.2. Garantir robustez na proteção de sítios contra roubos de dados e ataques DDoS;

3.5.3. Garantir um serviço de qualidade, com alta escalabilidade a partir de soluções tecnológicas modernas de segurança em nuvem;

3.5.4. Prover controles automatizados e integrados que responderão aos ataques com rapidez;

3.5.5. Atualização contínua e sem intervenção humana das regras de segurança através de um portal web de gerência.

4 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. Proteção de sítios web do domínio *mcom.gov.br com CDN contra ataques, interrompendo o tráfego malicioso antes que atinja o sítio do MCOM;

4.1.2. Interface de atendimento amigável;

4.1.3. Análise de ameaças em potencial nas solicitações de visitantes com base em várias características, dentre elas: endereço IP do visitante, recursos solicitados e regras de segurança definidas pelo MCOM;

4.1.4. Proteção DoS e DDoS: proteção para ataques de negação de serviço e negação de serviço distribuído;

4.1.5. WAF: proteção contra ataques como pichação de sites, SQL *Injection* e de demais tipos de ciberataques conhecidos e customizáveis. O *Web Application Firewall* visa proteger um aplicativo da Web específico ou conjunto de aplicativos da Web contra ataques cibernéticos;

4.1.6. Proteção contra ataques DNS: proteção para o serviço de resolução de nomes de internet contra ataques de indisponibilidade e ataques específicos ao serviço;

4.1.7. CDN e Cache: recursos de CDN (*Content Delivery Network*) provendo a possibilidade de armazenagem de réplicas de conteúdo para acesso geográfico disperso com o objetivo de redução do tempo de acesso ao conteúdo e latência;

4.1.8. Proteção domínio SSL: proteção para tráfego criptografado por meio da tecnologia SSL;

4.1.9. Bloqueio por geolocalização: bloqueio de ataques com base em sua localização geográfica;

4.1.10. Bloqueio por IP: mecanismos para bloqueio de ataques com base no endereço IP;

4.1.11. Suporte IPv6;

4.1.12. Regras de *Rate Controls*: controles baseados em regras de controle de tráfego, sendo possível o controle e limitação de requisições;

4.1.13. *Site Failover*: mecanismo para manutenção da disponibilidade do sítio/aplicação em caso de indisponibilidade do principal, possibilitando o redirecionamento de solicitações para um sítio secundário;

4.1.14. Otimização de rotas na internet: mecanismos para cálculo e otimização de rotas de acessos ao sítio na internet;

4.1.15. Interface de administração Via Web: interface que possibilita a mobilidade e controle na gestão da solução;

4.1.16. Aceleração para resolução DNS: mecanismos para a aceleração de resolução de nomes DNS;

4.1.17. Analisador de desempenho de sítio: mecanismos para a análise de desempenho do sítio/aplicação;

4.1.18. Proteção para API: mecanismos para a inspeção automatizada de solicitações a APIs;

4.1.19. Alta disponibilidade para DNS: mecanismos que possibilitem a alta disponibilidade do serviço DNS;

4.1.20. Integração com SIEM;

4.1.21. Anti Robô: detecção, tratamento e prevenção ao uso de bots; e

4.1.22. Base de reputação por IPs por geolocalização, por indústria, dinâmica ou IPs reconhecidos como nocivos.

4.2. Requisitos de Capacitação

4.2.1. Não se aplica, visto que o objeto da contratação envolve apenas o fornecimento de serviços de TIC.

4.3. Requisitos Legais

4.3.1. A presente contratação será realizada pela modalidade Dispensa da Licitação, em conformidade com o inciso XVI do Art. 24 da Lei nº 8.666, de 21 de junho de 1993.

4.3.2. A legislação adicional aplicável à contratação do objeto deste Projeto Básico encontra amparo na Instrução Normativa nº 01/SGD/ME, de 04 de abril de 2019 e legislação correlata.

4.4. Requisitos de Manutenção

4.4.1. A Plataforma deve implementar estratégias e mecanismos que garantam a manutenção da disponibilidade da solução e a proteção dos domínios, conforme níveis mínimos de serviço definidos neste Projeto Básico.

4.5. Requisitos Temporais

4.5.1. O serviço deverá ser disponibilizado no prazo de 10 (dez) dias úteis a contar da assinatura da Ordem de Serviço.

4.6. Requisitos de Segurança e Privacidade

4.6.1. A Plataforma deve possuir estrutura física e lógica que garanta um ambiente seguro e controlado, atendendo, ainda, aos requisitos de segurança física e lógica necessários à garantia da disponibilidade, integridade e confidencialidade das informações do MCOM.

4.6.2. Deverão ser observadas as disposições da Instrução Normativa GSI/PR nº 01, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, a qual disciplina a gestão de segurança da Informação e Comunicações na Administração Pública Federal, bem como ao Decreto nº 3505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

4.6.3. Deverão ser observadas as disposições do Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade, no que couber, conforme Seção 7 do Anexo da IN SGD/ME nº 1/2019.

4.6.4. Outros requisitos de segurança e privacidade encontram-se definidos nos Requisitos Mínimos da Contratação, Anexo A deste Projeto Básico.

4.7. Requisitos Sociais, Ambientais e Culturais

4.7.1. Durante o fornecimento dos serviços, deverão ser observados pelo SERPRO e pelo MCOM práticas que tenham menor impacto ambiental.

4.7.2. A presente contratação deverá prezar, sempre que possível, por documentos em meios digitais em detrimento ao uso de papel impresso.

4.7.3. O acesso aos serviços deverá estar disponível no idioma Português do Brasil.

4.8. Requisitos de Arquitetura Tecnológica

4.8.1. A plataforma deve entregar o conjunto de solução numa arquitetura baseada em nuvem.

4.9. Requisitos de Projeto e de Implementação

4.9.1. A Plataforma deve fornecer um conjunto de soluções em um ambiente próprio do SERPRO, integradora e provedor ou provedor, com controle e monitoramento de acesso ao ambiente implantado da solução, configurando um modelo de utilização de recursos computacionais dedicados e públicos, permitindo ao MCOM abstrair-se da aquisição e gestão dos recursos computacionais utilizados na Plataforma.

4.10. Requisitos de Implantação

4.10.1. Para habilitação do domínio no Govshield, a CONTRATADA deverá repassar todas as orientações para que a equipe técnica do MCOM faça as modificações necessárias no DNS.

4.10.2. O MCOM deverá informar à CONTRATADA a lista de domínios, subdomínios e endereços IPs, dentre outras informações necessárias à implementação dos serviços.

4.10.3. O MCOM indicará técnico com conhecimento de cada aplicação afetada, bem como dos dados trafegados, para análise dos logs gerados e personalização das funcionalidades da ferramenta de acordo com as necessidades de cada aplicação.

4.11. Requisitos de Garantia e Suporte Técnico

4.11.1. A solicitação de atendimento ou suporte técnico poderá ser realizada durante a vigência do contrato, 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, nos canais de atendimento disponibilizados pela CONTRATADA.

4.11.2. O suporte técnico compreende os atendimentos relacionados ao produto contratado, como relatos de indisponibilidade, falhas ou esclarecimentos de dúvidas sobre a solução.

4.12. Requisitos de Experiência Profissional

4.12.1. Não se aplica, visto que não há necessidade de exigências relativas à equipe da CONTRATADA para o tipo de serviço prestado, o qual será avaliado unicamente em função dos resultados e níveis mínimos de serviço predefinidos.

4.13. Requisitos de Formação da Equipe

4.13.1. Não se aplica, visto que não há necessidade de exigências relativas à equipe da CONTRATADA para o tipo de serviço prestado, o qual será avaliado unicamente em função dos resultados e níveis mínimos de serviço predefinidos.

4.14. Requisitos de Metodologia de Trabalho

4.14.1. A gestão das funcionalidades da plataforma será realizada pela CONTRATADA, de acordo com a modalidade contratada e com os pré-requisitos definidos pelo MCOM, devendo ser entregues relatórios de segurança mensalmente ou sempre que demandado pelo MCOM.

4.14.2. Os relatórios de segurança deverão apresentar indicadores de tráfego, segurança e performance, bem como eventos de segurança detectados e analisados no período.

4.15. Requisitos de Segurança da Informação e Privacidade

4.15.1. A CONTRATADA deverá assinar o Termo de Confidencialidade, Anexo B deste Projeto Básico, garantindo a manutenção do sigilo de informações do CONTRATANTE necessárias à prestação dos serviços.

4.15.2. Deverão ser observadas, durante toda execução contratual, as diretrizes da Política de Segurança da Informação e Comunicações (POSIC) do Ministério das Comunicações.

4.15.3. Deverão ser observadas as disposições da Lei Geral de Proteção de Dados – LGPD.

5 – RESPONSABILIDADES

5.1. Deveres e responsabilidades da CONTRATANTE

5.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço, de acordo com os critérios estabelecidos no Projeto Básico;

5.1.3. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis;

5.1.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7. Prever que os direitos de propriedade intelectual e direitos autorais sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração.

> 5.1.7.1. A propriedade intelectual da tecnologia e modelos desenvolvidos direta ou indiretamente para a prestação dos serviços definidos neste Projeto Básico será exclusiva da CONTRATADA e/ou de seus parceiros no desenvolvimento dos serviços objeto do contrato.

5.1.8. Verificar, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações do Projeto Básico, para fins de aceitação e, posterior, recebimento definitivo;

5.1.9. Conferir todos os relatórios técnicos gerados e apresentados durante a execução contratual, efetuando o seu recebimento e atesto quando os mesmos estiverem em conformidade com os padrões de informação e qualidade exigidos;

5.1.10. Assegurar as condições necessárias para a execução dos serviços contratados;

5.1.11. Efetuar o correto pagamento, dentro dos prazos especificados neste Projeto Básico.

5.2. Deveres e responsabilidades da CONTRATADA

5.2.1. Indicar formalmente e por escrito, no prazo máximo de 5 (cinco) dias úteis após a assinatura do contrato, junto à CONTRATANTE, um preposto idôneo com poderes de decisão para representar a CONTRATADA, principalmente no tocante à eficiência e agilidade da execução do objeto deste Projeto Básico, e que deverá responder pela fiel execução do contrato;

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

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

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

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

5.2.6. Ceder à Administração os direitos de propriedade intelectual e direitos autorais sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, salvo quanto à propriedade intelectual da tecnologia e modelos desenvolvidos direta ou indiretamente para a prestação dos serviços definidos neste Projeto Básico, que será exclusiva da CONTRATADA e/ou de seus parceiros no desenvolvimento dos serviços objeto do contrato.

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

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

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

5.2.10. Executar os serviços contratados de acordo com o Projeto Básico, desde que o CONTRATANTE tenha assegurado as condições necessárias para a utilização dos serviços contratados, tais como canais de comunicação e infraestrutura de processamento.

5.2.11. Disponibilizar, em meio eletrônico, relatório de prestação de contas discriminando os serviços, Notas Fiscais e Guias de pagamento correspondentes ao serviço prestado.

5.3. Deveres e responsabilidades do órgão gerenciador da ata de registro de preços

5.3.1. Não se aplica, pois o processo de contratação será realizado por meio de dispensa de licitação.

6 – MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

6.1.1. Após a assinatura do contrato, será realizada a reunião inicial nos termos do art. 31 da IN 01/2019 - SGD/ME.

6.2.2. O MCOM providenciará a abertura da Ordem de Serviço para demandar a execução dos serviços pela CONTRATADA.

6.2.3. O serviço deverá ser disponibilizado no prazo de 10 (dez) dias úteis a contar da assinatura da Ordem de Serviço.

6.2.4. O Termo de Recebimento Provisório será emitido no prazo de 3 (três) dias corridos a contar da entrega do relatório mensal pela CONTRATADA, e consistira na declaração formal de que os serviços foram prestados, para posterior análise das conformidades e qualidades baseadas nos requisitos e nos critérios de aceitação.

6.2.5. O Termo de Recebimento Definitivo será emitido no prazo de 3 (três) dias corridos após o recebimento provisório e consistirá na declaração formal de que os serviços prestados atendem aos requisitos estabelecidos e aos critérios de aceitação.

6.2.6. A CONTRATADA deverá disponibilizar mensalmente, em meio eletrônico, relatório de prestação de contas discriminando os serviços, Notas Fiscais e Guias de pagamento correspondentes ao serviço prestado.

6.2. Quantidade mínima de bens ou serviços para comparação e controle

6.2.1. Segue abaixo a estimativa de volume de serviços a serem demandados:

Grupo	Item	Descrição Serviço	M
1	1	GovShield - Plataforma de proteção básica e distribuição de conteúdo para proteção de sítios Web HTTP e HTTPS vinculadas a domínio DNS e seus respetivos subdomínios.	
	2	Adicional de 1 TB referente ao tráfego de acesso externo aos sítios Web.	

6.2.2. O serviço adicional descrito no item 2 da tabela acima se trata de item a ser executado sob demanda, **sem garantia de consumo**, excepcionalmente se ultrapassado o volume mensal previsto para o item 1 e será cobrado a partir do 3º (terceiro) mês de consumo.

6.3. Mecanismos formais de comunicação

6.3.1. Estabelecem-se como mecanismos formais de comunicação:

6.3.1.1. Ordem de Serviço;

6.3.1.2. E-mail, Ofício, cartas ou documentos gerados por meio do Sistema Eletrônico de Informações (SEI);

6.3.1.3. Canais de atendimento disponibilizados pela CONTRATADA.

6.4. Manutenção de Sigilo e Normas de Segurança

6.4.1. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais documentos.

6.4.2. Após a assinatura do contrato, a CONTRATADA deverá assinar o Termo de Confidencialidade, Anexo B deste Projeto Básico, em que se responsabilizará pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação.

6.4.3. A CONTRATADA deverá assegurar integral conformidade dos serviços objetos do contrato às disposições condas na Lei nº 13.709 de 2018 - Lei Geral de Proteção de Dados Pessoais - a partir do início de sua vigência, bem como com todas e quaisquer alterações que venham a ser aplicadas ao referido diploma legal, observados os prazos legalmente estipulados.

7. MODELO DE GESTÃO DO CONTRATO

7.1 Para cumprir as atividades de gestão e fiscalização do CONTRATO, o CONTRATANTE designará servidores (titulares e substitutos) para executar os seguintes papéis:

a) Gestor do Contrato: servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;

b) Fiscal Técnico: servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato;

c) Fiscal Requisitante: servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação; e

d) Fiscal administrativo: servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos.

7.2 Critérios de Aceitação

7.1.1. O aceite dos serviços fica condicionado à apresentação dos relatórios de segurança contendo todas as informações exigidas neste Projeto Básico.

7.1.2. Deverão ser aferidos os níveis de disponibilidade do serviço, conforme Níveis Mínimos definidos neste Projeto Básico.

7.2. Procedimentos de Teste e Inspeção

7.2.1. A CONTRATANTE poderá realizar testes de segurança nos sítios do MCOM para se certificar de que os serviços estão sendo fornecidos conforme os parâmetros de proteção exigidos.

7.3. Níveis Mínimos de Serviço Exigidos

7.3.1. Todos os recursos necessários ao funcionamento pleno e integral do objeto contratado são de inteira responsabilidade da CONTRATADA, que deverá realizar, de forma continuada, tarefas e rotinas que garantam o pleno funcionamento de toda a infraestrutura, de forma ininterrupta, mantendo em pleno funcionamento todo objeto da contratação.

7.3.2. A disponibilidade da solução deve ser de, no mínimo, 99,70%, conforme indicador IDS detalhado a seguir:

IDS – INDICADOR DE DISPONIBILIDADE DA SOLUÇÃO		
Tópico	**Descrição**	
Finalidade	Medir o percentual de disponibilidade da solução.	
Meta a cumprir	**IDS > = 99,70%**	A meta visa garantir disponibilidade mensal do serviço de, no mínimo, 99,70%.
Instrumento de medição	Registros de incidentes de alta severidade na Central de Serviços da Contratada.	
Forma de acompanhamento	Relatório de disponibilidade da solução.	
Periodicidade	Mensal	
Mecanismo de Cálculo (métrica)	D = ((Tm – Ti)/Tm)*100 onde: D = Percentual de tempo de disponibilidade. Ti = Somatório dos minutos de interrupção observados durante o período de prestação de serviço. Tm = Somatório de minutos do período previsto para a prestação do serviço.	
Observações	A disponibilidade de acesso será considerada no horário de funcionamento do serviço, desconsiderando-se as paradas previamente comunicadas, bem como aquelas programadas nos sistemas estruturantes fontes da informação.	
Início de Vigência	A partir do recebimento definitivo da solução.	
Faixas de ajuste no pagamento e Sanções	Quando o nível de serviço não for atingido, será calculado o desconto por intermédio da seguinte fórmula: **Desc = [1 - (Ia / Ic)] * Vs** onde: Desc= Valor do desconto Ia = Indicador aferido Ic= Indicador contratado Vs = Valor do serviço	

7.3.3. Não será considerado descumprimento de nível de serviço em caso de interrupção ou degradação do serviço, programada ou não, ocorrer por motivo de caso fortuito ou de força maior, ou por fatos atribuídos ao próprio CONTRATANTE ou terceiros, por erros de operação do CONTRATANTE.

7.4. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

7.4.1. Os ônus decorrentes do descumprimento de quaisquer obrigações estabelecidas neste instrumento contratual serão de responsabilidade da parte que lhes der causa, sem prejuízo de eventual responsabilização daquele que der causa ao inadimplemento por perdas e danos perante a parte prejudicada.

7.4.2. Eventual aplicação de sanção administrativa deve ser formalmente motivada, sendo assegurado o prévio contraditório e a ampla defesa.

7.4.3. Na aplicação das sanções a autoridade competente levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena e o dano causado à parte prejudicada, observado o princípio da proporcionalidade.

7.4.4. Constituirá:

a) Advertência – Sanção aplicável à ocorrência de inexecução parcial não reiterada ou quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado.

b) Mora – O recebimento total em atraso dos serviços contratados ou atraso na execução das disposições contratuais.

c) Inexecução parcial – O recebimento parcial, ainda que em atraso, dos serviços contratados para o período de referência.

d) Inexecução total – O não recebimento de todas as parcelas dos serviços contratados.

7.4.5. Por inexecução parcial ou total do contrato, a CONTRATADA estará sujeito à aplicação das sanções descritas no art. 87 da Lei 8.666/93, de forma gradativa e proporcional à gravidade da falta cometida e de eventual dano causado, assegurados o contraditório e a ampla defesa de forma prévia.

7.4.5.1. Em caso de descumprimento total ou parcial das obrigações, o valor da multa não excederá a 10% (dez por cento) do valor do contrato.

7.4.5.2. Fica estipulado o percentual de 0,5% (zero vírgula cinco por cento) ao mês pro rata die sobre o valor do item inadimplido para os casos de mora (atraso).

7.4.6. Ficam estipulados a título de multa compensatória os percentuais de:

7.4.6.1. 2% (dois por cento) sobre o valor do item inadimplido para os casos de inexecução parcial reiterada.

7.4.6.2. 10% (dez por cento) sobre o valor do contrato para os casos de inexecução total.

7.4.7. Dentro do mesmo período de referência, para o mesmo item inadimplido, a multa por inexecução total substitui a multa por inexecução parcial e a multa por mora; da mesma forma, a multa por inexecução parcial substitui a multa por mora.

7.4.8. Os valores devidos pela CONTRATADA serão pagos preferencialmente por meio de redução do valor cobrado na fatura do mês seguinte à respectiva aplicação. Na ausência de saldo contratual em serviços a serem prestados, a CONTRATADA pagará ao CONTRATANTE eventual diferença, preferencialmente, por meio de cobrança administrativa.

7.5. Do Pagamento

7.5.1. Será realizado pagamento mensal dos serviços, contabilizado, para efeitos de cobrança, do dia 21 (vinte e um) ao dia 20 (vinte) do mês especificado no relatório.

7.5.2. Caberá ao MCOM indicar todas as informações necessárias para envio eletrônico (e-mail) da nota fiscal e das guias de pagamento correspondentes aos serviços prestados.

7.5.3 Desde o primeiro faturamento, o relatório de prestação dos serviços será encaminhado automaticamente pela CONTRATADA para o e-mail informado pelo MCOM.

7.5.4 O prazo para pagamento das faturas/guias de recolhimento compreende até 20 (vinte) dias corridos a partir da data de emissão da nota fiscal e o prazo para emissão dar-se-á até o último dia útil do mês de referência.

7.5.5 O valor da primeira fatura poderá ser cobrado proporcionalmente *(pro rata die)* a partir da instalação/habilitação do serviço contratado.

7.5.6 O valor mensal será atestado definitivamente em até 3 (três) dias corridos do recebimento provisório ou da disponibilização da documentação correspondente à prestação do serviço.

7.5.7 Decorrido o prazo para recebimento definitivo, sem que haja manifestação formal do CONTRATANTE, a CONTRATADA emitirá automaticamente as notas fiscais referentes aos serviços prestados.

7.5.8 Caso ocorra rejeição parcial ou total dos serviços, após a emissão das notas fiscais, os referidos acertos serão compensados na fatura do mês subsequente. Na ausência de saldo contratual em serviços a serem prestados, o os valores serão pagos ao CONTRATANTE por meio de cobrança administrativa.

8. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1 A prestação de serviços de segurança em nuvem para tratamento e proteção de sítios web com CDN (*Content Delivery Network*), denominada **GovShield**, é precificada pelo SERPRO conforme valores disponíveis em https://www.loja.serpro.gov.br/govshield.

8.2 Abaixo, segue estimativa de custo da contratação para um periodo de 12 (doze) meses:

Grupo	Item	Descrição Serviço	Modalic
1	1	GovShield - Plataforma de proteção básica e distribuição de conteúdo para proteção de sítios Web HTTP e HTTPS vinculadas a domínio DNS e seus respetivos subdomínios.	Bronz
	2	Adicional de 1 TB referente ao tráfego de acesso externo aos sítios Web.	Bronz
Valor Global			

8.3. A modalidade bronze possui 1 TB disponível mensalmente para proteção de sítios web. O adicional de Terabytes que exceder o disponível pela modalidade, será cobrado a partir do 3º (terceiro) mês de consumo.

8.4. O adicional descrito no item 2 da tabela acima se trata de item a ser executado sob demanda, **sem garantia de consumo**, excepcionalmente se ultrapassado o volume mensal previsto para o item 1.

9. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1. As fontes de recurso serão indicadas posteriormente, quando for realizada a inclusão do Plano de Contratações Anual - PAC, conforme indicado nos autos.

9.2. Segue cronograma de execução físico-financeira da solução a ser contratada:

Item	Descrição Serviço	Previsão Desembolso
		1º ano
1	GovShield - Plataforma de proteção básica e distribuição de conteúdo para proteção de sítios Web HTTP e HTTPS vinculadas a domínio DNS e seus respetivos subdomínios.	R$ 73.724,40
2	Adicional de 1 TB referente ao tráfego de acesso externo aos sítios Web.	R$ 13.406,20
Valor Global		**R$ 87.130,60**

10. DA VIGÊNCIA DO CONTRATO

10.1. O contrato vigorará por 12 (doze) meses, contados a partir da data da sua assinatura, podendo ser prorrogado por períodos iguais e sucessivos, limitado a 60 (sessenta) meses, nos termos do Inciso II, Art. 57, da Lei nº 8.666, de 1993.

10.1.1 Caso a assinatura seja efetivada por meio de certificação digital ou eletrônica, considerar-se-á como início da vigência a data em que o último signatário assinar.

10.2. A prorrogação do contrato dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada de comprovação da vantajosidade para a Administração.

11. DO REAJUSTE DE PREÇOS

11.1. O reajuste dar-se-á por meio da aplicação do Índice de Custo de Tecnologia da Informação (ICTI), apurado pelo Instituto de Pesquisa Econômica Aplicada (IPEA), acumulado nos últimos doze meses contados a partir da data de assinatura do contrato.

11.2. A data base para cálculo do índice da primeira correção monetária será o mês de assinatura do contrato, considerando-se esta data a do orçamento do contrato e tomando-se como base a seguinte fórmula:

$Ir = (I1 – Io) / Io$

$R = Vo \times Ir$

$V1 = Vo + R$

Onde:

Ir - índice de reajustamento

I1 - índice correspondente à data para qual se deseja reajustar o valor (aniversário de 12 (doze) meses a partir da assinatura do Contrato)

Io - índice correspondente à data base do contrato (mês de assinatura do Contrato)

R - valor do reajustamento procurado

V1 - preço final já reajustado

Vo - preço original do Contrato, na data base (valor a ser reajustado)

11.3. Os valores de "Io" e de "I1" podem ser consultados no sítio eletrônico do IPEA, localizado no seguinte endereço: http://www.ipea.gov.br.

11.4. Seguindo o disposto no art. 65, §8º da Lei 8.666/93, os reajustes poderão ocorrer por simples apostilamento, devendo ser efetivados de forma automática e de ofício, não sendo exigível prévio requerimento ou solicitação por parte da proponente.

11.5. De acordo com o art. 2º da lei 10.192/2001, os efeitos do reajuste serão considerados a partir do dia subsequente ao aniversário de vigência do contrato e a aplicação dos demais reajustes respeitarão o intervalo mínimo de 12 (doze) meses entre suas aplicações (art. 2º da lei 10.192/2001).

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

11.7. 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.

12. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. Regime, Tipo e Modalidade da Licitação

12.1.1. O regime de execução do contrato será caracterizado como empreitada por preço global, pois é possível precisar de antemão o quantitativo do objeto a ser contratado.

12.1.2. A contratação dos serviços será por meio da modalidade de dispensa de licitação, com base no inciso XVI do artigo 24 da Lei nº 8.666 de 1993.

12.1.2 O serviço é classificado como de natureza de prestação continuada.

12.2 Adoção do Sistema de Registro de Preços (se aplicável)

12.2.1 Não se aplica, pois trata-se de contratação por dispensa de licitação.

12.3 Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência

12.3.1. Não se aplica, pois trata-se de contratação por dispensa de licitação.

12.3 Critérios de Qualificação Técnica para a Habilitação

12.3.1. Não se aplica, pois trata-se de contratação por dispensa de licitação.

12.4 Participação de consórcios

12.4.1. Não se aplica, pois trata-se de contratação por dispensa de licitação.

12.5 Permissão de subcontratação

12.5.1. Não será admitida a subcontratação do objeto licitatório, por se tratar de produto/serviço único contratado por meio de dispensa de licitação.

13. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

13.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 6388/2022/SEI-MCOM, de 10 de agosto 2022 (SEI nº 10296236), publicada no Boletim de Serviços nº 61, de 16 de agosto de 2022 (SEI nº 10318719).

13.2. Foram observados, neste Projeto Básico, os guias, manuais e modelos publicados pelo Órgão Central do SISP (art. 8º, §2, da IN SGD/ME nº 1/2019).

13.3. Conforme o §6º do art. 12 da IN SGD/ME nº 01, de 2019, o Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

13.4. São partes integrantes deste Projeto Básico os seguintes anexos:

- Anexo A - Especificações Técnicas;
- Anexo B - Termo de Confidencialidade;
- Anexo C - Modelo de Ordem de Serviço;
- Anexo D - Modelo de Termo de Recebimento Provisório;
- Anexo E - Modelo de Termo de Recebimento Definitivo;
- Anexo F - Estudo Técnico Preliminar da Contratação SEI (10412326)

Integrante Requisitante	**Integrante Técnico**	
(Assinado eletronicamente) **Filipe Carneiro Guimarães** Analista de Sistemas Matrícula/SIAPE: 01443304	*(Assinado eletronicamente)* **Victor Hugo de Souza Peçanha** Assistente de Tecnologia da Informação Matrícula/SIAPE: 2420446	Cl

Autoridade Máxima da Área de TIC
(Assinado eletronicamente) **WANESSA QUEIROZ DE SOUZA OLIVEIRA** Subsecretária de Planejamento e Tecnologia da Informação

Aprovo,

Autoridade Administrativa Competente
Assinado eletronicamente) **IVANCIR GONÇALVES DA ROCHA CASTRO FILHO** Coordenador Geral de Recursos Logísticos

ANEXO A - ESPECIFICAÇÕES TÉCNICAS

1 . CARACTERÍSTICAS GERAIS

1.1. WAF (Web Application Firewall);

1.2 A Solução de Firewall de Aplicação deve proteger contra as 10 (dez) principais vulnerabilidades OWASP (Open Web Application Security Project) em segurança de aplicações Web (Web Application Security);

1.3 A Solução de Firewall de Aplicação deve proteger, no mínimo, contra os ataques listados abaixo descritos:

1.3.1. SQL injection;

1.3.2. Cross-site scripting (XSS);

1.3.3 Adulteração de Parâmetros (Parameter tampering);

1.3.4 Manipulação de sessões (Session manipulation);

1.3.5 Cookie poisoning;

1.3.6 Ataques de buffer overflow em aplicações e banco de dados;

1.3.7. Ataques de força bruta;

1.3.8 Reconhecimento de Web server;

1.3.9 Cookie injection;

1.3.10 DoS;

1.3.11 Ataques a Web Services;

1.3.12 XML External Entities;

1.3.13 Information Leakage;

1.3.14 Insufficient Authentication;

1.3.15 Directory Indexing;

1.3.16 Session Fixation;

1.3.17 OS Commanding;

1.3.18 Format String;

1.3.19 LDAP Injection;

1.3.20 Remote File Inclusion;

1.3.21 Null Byte Injection;

1.3.22 SSI Injection;

1.3.23 HTTP Response Splitting;

1.3.24 SYN flood.

1.4 A Solução deve permitir aplicação de políticas em tempo real, sem a necessidade de interrupção do tráfego, independentemente da codificação de caracteres, implementando um controle do tráfego normalizado e sanitização de dados por meio da análise dos campos dos cabeçalhos HTTP e TAGs HTML, a fim de combater a técnicas de evasão.

1.5 A Solução deve utilizar expressões regulares e comparação de padrões de endereços IP e de rede, a fim de inspecionar e validar os campos dos cabeçalhos HTTP;

1.6. A Solução deve utilizar expressões regulares, a fim de inspecionar e validar tag HTML.

1.7. Deve permitir forçar com que as requisições feitas (request flows) por um usuário através da aplicação, entre uma página Web e outra, sejam consistentes ao comportamento esperado pela aplicação;

1.7.1.Deve trabalhar com métodos de detecção de ataques por assinatura, fazendo com que, mesmo sem assinaturas atualizadas, consiga efetuar bloqueios de ataques;

1.7.2 Deve permitir que o administrador bloqueie tráfego por geolocalização, permitindo que o tráfego de determinado país seja bloqueado;

1.7.3 Deve permitir a inspeção HTTPS

1.7.4 Deve ser capaz de receber informações de listas de endereços maliciosos e de botnets;

1.7.5 A inspeção do tráfego criptografado pode ser realizada da seguinte forma:

1.7.5.1 Inspeção transparente de tráfego utilizando interceptação (man in the middle);

1.7.5.2 Deve oferecer recurso de bloqueio baseado na reputação do endereço IP de origem, protegendo as aplicações de serem acessadas pelas seguintes origens: Rede TOR, proxies anônimos e endereços IP de baixa reputação;

1.7.5.3 Deve prover métodos para identificar e bloquear ataques de clientes automatizados de logins e acessos, ou seja, as tentativas de logins e acessos simultâneos em um curto intervalo de tempo entre os acessos;

1.7.5.4 Deve permitir modos de implementação utilizando técnicas de finalização e restabelecimento de conexões (proxy reverso) e análise do fluxo de dados sem interferência na conexão fim a fim (proxy transparente);

1.8. Deve suportar, no mínimo, os modos operacionais abaixo:

1.8.1. Passivo: Detecção completa de intrusão, sem bloqueio;

1.8.2. Ativo: Detecção completa de intrusão, interceptação e bloqueio;

1.9. Capacidade de definição de escopo de inspeção por:

1.9.1 Endereço IP da aplicação;

1.9.2 URL;

1.9.3 URIs.

1.10. A solução deve ser capaz de inspecionar e bloquear as solicitações HTTP, SOAP e XML, conforme definições abaixo:

1.10.1. Solicitações em não conformidade com o protocolo;

1.10.2. Proteção as versões HTTP 1.0, 1.1 e 2.0;

1.10.3. Deve trabalhar com filtros de segurança:

1.10.3.1 De proteção dos parâmetros globais dos servidores Web;

1.10.4. De definição de escopo dos métodos HTTP e HTTPS permitidos e bloqueados (HTTP methods);

1.10.5. De controle dos parâmetros das aplicações;

1.10.6 De proteção a sessão;

1.10.7 De bloqueio de vulnerabilidades;

1.10.8 De proteção a XML;

1.10.9 Possibilitar atualização de novas assinaturas para ataques conhecidos;

1.10.10 Permitir configurações por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;

1.10.11 A criação das políticas deve possuir as formas:

1.10.11.1 Por meio da observação do tráfego para a aplicação;

1.10.11.2 Por meio da observação do tráfego de teste e manual.

1.10.12 Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente, dentre os abaixo:

1.10.12.1 Assinatura de ataque;

1.10.12.2. Código de response;

1.10.12.3. Conteúdo da cookie;

1.10.12.4. Conteúdo do cabeçalho;

1.10.12.5. Conteúdo do payload;

1.10.12.6. Hostname;

1.10.12.7. IP de origem;

1.10.12.8. Método HTTP;

1.10.12.9. Número de ocorrências em determinado intervalo de tempo;

1.10.12.10. Parâmetro

1.10.12.11. Tipo de protocolo (HTTP ou HTTPS);

1.10.12.12. User-agent (navegador);

1.10.12.13. Permitir a criação de assinaturas de ataques;

1.10.13 Reconhecer assinaturas seletivas, e filtros de ataque que devem proteger contra:

1.10.13.1 Ataques de negação de serviços automatizados;

1.10.13.2. Requests em objetos restritos;

1.10.14 A solução oferecida deve possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos. Deve ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção à regra geral e possuir método de mitigação de DoS L7 baseado em:

1.10.14.1. Descarte de todas as requisições de um determinado IP e/ou país suspeito;

1.10.14.2. Geolocalização;

1.10.14.3. Possuir a lista de delegação de IPs públicos, identificando país de origem da requisição;

1.10.15 Aprender o comportamento da aplicação;

1.10.16 É vedado a aplicação automática de políticas sugeridas, exceto com autorização da CONTRATANTE;

1.10.17 Realizar as checagens em todos os tipos de entrada de dados, como URLs, formulários, cookies, campos ocultos e parâmetros, consultas (query), métodos HTTP, elementos XML e ações SOAP;

1.10.18 Proteger contra mensagens XML e SOAP malformadas;

1.10.19 Utilizar o campo HTTP X-Forwarded-For sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com NAT;

1.10.20 Remover as mensagens de erro do conteúdo que será enviado aos usuários;

1.10.21 Emitir os seguintes relatórios:

1.10.21.1 Gráfico indicando tipo de ataque;

1.10.21.2 Gráfico indicando quais URLs foram atacadas;

1.10.21.3 Gráfico indicando os endereços IPs de origem;

1.10.21.4 Gráfico indicando a localização geográfica dos endereços IPs de origem;

1.10.21.5 Permitir a seleção de período para emissão dos relatórios;

1.10.21.6 Deve permitir que um perfil aprendido de forma automatizada possa ser ajustado pelo administrador ou bloqueado, para que não sofra alterações;

1.10.21.7 Deve reconhecer alterações legítimas realizadas nas aplicações protegidas;

1.10.21.8 Para o tratamento de tráfego de API, deve suportar o modelo de segurança positivo, devendo ser capaz de aprender qual perfil de tráfego é legítimo e bloquear ataques ou atividades não autorizadas;

1.10.21.9 Ao detectar um ataque ou qualquer atividade não autorizada, deve ser possível bloquear:

1.10.21.9.1 Requisições e respostas HTTP;

1.10.21.9.2 Métodos HTTP;

1.10.21.9.3 Endereço IPv4 e Ipv6;

1.10.21.9.4 Endereço IP durante um intervalo de tempo específico.

1.10.21.10 Deve permitir a visualização da política que está instalada e ativa na Solução de Firewall de Aplicação;

1.10.21.11 Deve possuir funcionalidade que identifique continuamente vulnerabilidades para detecção de ataques existentes na base de assinaturas da solução;

1.10.21.12 Deve possuir interface intuitiva, com a capacidade de trabalhar com políticas distintas para diferentes aplicações;

1.10.21.13 Deve prover funções administrativas simples e comuns, como a atualização das políticas, políticas de personalização e de relaxamento para reduzir falsos positivos;

1.10.21.14 Deve permitir, através de um processo simples e manual, a aceitação de falsos positivos;

1.10.21.15 Deve suportar a configuração de hosts confiáveis para permitir a execução de operações não permitidas pela política adotada para uso em eventos de testes de penetração, solução de problemas (troubleshooting) e análise de performance;

1.10.21.16 Deve implementar listas brancas (white list) e lista negra (black list) para bloqueios ou liberação de acesso, sem que seja necessário realizar a consulta nos filtros e políticas de acesso;

1.10.21.17 Deve possuir API para administração das listas de forma automatizada;

1.10.21.18 Deve identificar e criar um perfil de utilização das aplicações, mesmo que as páginas Web e conteúdos sejam dinâmicos, como os desenvolvidos em JavaScript, CGI, ASP, PHP e Java.

1.10.22 A Plataforma deve prover solução de WAF Avançado (Web Application Firewall) para USN3 com todos os requisitos exigidos para WAF (Web Application Firewall) para USN1;

1.10.23 A plataforma deve prover solução de WAF Avançado com recursos avançados de proteção conforme descrito:

1.10.23.1 Configuração de regras de forma agrupada ou individual;

1.10.23.2 Prover a separação lógica das regras, gerenciando de uma forma granular.

1.10.24 Prover controles para evitar solicitações/requisições excessivas, por meio da utilização dos seguintes limitadores abaixo, visando alertar ou negar:

1.10.24.1 Por meio de identificador:

1.10.24.1.1 Client IP;

1.10.24.1.2 Client IP e User Agent;

1.10.24.1.3 Client Session ID Cookie Name.

1.10.24.2. Por meio de critérios, utilizando:

1.10.24.2.1 AS Number;

1.10.24.2.2 Hostname;

1.10.24.2.3 IP/CIDR;

1.10.24.2.4 Network List;

1.10.24.2.5 Path;

1.10.24.2.6 Extension;

1.10.24.2.7 Query String;

1.10.24.2.8 Request Header;

1.10.24.2.9 User-Agent;

1.10.24.2.10 Request Method.

1.10.24.3 Deve permitir a criação de regras customizadas para os seguintes critérios, possibilitando altertas ou negação:

1.10.24.3.1 Request Method;

1.10.24.3.2 Path;

1.10.24.3.3 Extension;

1.10.24.3.4 Filename;

1.10.24.3.5 Procotol Version;

1.10.24.3.6 Request Header;

1.10.24.3.7 Request Header Order;

1.10.24.3.8 Cookie;

1.10.24.3.9 Query String;

1.10.24.3.10 POST Body Parameter;

1.10.24.3.11 POST Body Parameter Name;

ANEXO B - TERMO DE CONFIDENCIALIDADE

1. OBJETO DA CONTRATAÇÃO

1.1 Contratação de serviço que disponibiliza, por meio de Computação em Nuvem, na modalidade Plataforma como Serviço (PaaS), , a serem executados de forma continuada pelo período de 12 meses.

2. TERMO DE CONFIDENCIALIDADE

[Qualificação: nome, nacionalidade, CPF, identidade (nº, data e local de expedição), filiação e endereço], perante o(a) [órgão ou entidade], declaro ter ciência inequívoca da legislação sobre o tratamento de informação classificada cuja divulgação possa causar risco ou dano à segurança da sociedade ou do Estado, e me comprometo a guardar o sigilo necessário, nos termos da Lei n° 12.527. de 18 de novembro de 2011, e a:

a)tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo(a) [órgão ou entidade] e preservar o seu sigilo, de acordo com a legislação vigente;

b) preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo a terceiros;

c)não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito; e

d) não copiar ou reproduzir, por qualquer meio ou modo:

(i) informações classificadas em qualquer grau de sigilo;

(ii) informações relativas aos materiais de acesso restrito do (da) [órgão ou entidade], salvo autorização da autoridade competente.

Declaro que [recebi] [tive acesso] ao (à) [documento ou material entregue ou exibido ao signatário], e por estar de acordo com o presente Termo, o assino na presença das testemunhas abaixo identificadas.

DE ACORDO

CONTRATANTE	**CONTRATADA**
<Nome> Matrícula: <Matr.>	**<Nome>** Matrícula: <Matr.>

TESTEMUNHAS

Testemunha 1	**Testemunha 2**
<Nome> <Qualificação>	**<Nome>** <Qualificação>

_____, _____ de _____de 20____.

ANEXO C - MODELO DE ORDEM DE SERVIÇO

ORDEM DE SERVIÇO **Art. 32 da Instrução Normativa SGD/ME nº 01/2019**			
1. IDENTIFICAÇÃO			
N° IDENTIFICADOR DA OSFB			
N° CONTRATO			
EMPRESA CONTRATADA / CNPJ:			
OBJETO DO CONTRATO:			
GESTOR DO CONTRATO: [*caput* art. 32 da IN 01/2019/SGD]	NOME:		
	E-MAIL:	TELFONE:	MATRÍCULA:
REQUISITANTE: [Inc. IV do art. 32 da IN 01/2019/SGD]	NOME:		

	ORDEM DE SERVIÇO **Art. 32 da Instrução Normativa SGD/ME nº 01/2019**		
	1. IDENTIFICAÇÃO		
	E-MAIL:	TELFONE:	MATRÍCULA:

2. ESPECIFICAÇÃO DOS SERVIÇOS (Inc. I e II do art. 32 da IN 01/2019/SGD)

ITEM/GRUPO:

ID	DESCRIÇÃO	UND	QTDE/VOLUME	VL UNITÁRIO	VL TOTAL ITEM
VALOR TOTAL ESTIMADO:					

3. CRONOGRAMA (Inc. III do art. 32 da IN 01/2019/SGD)

GRUPO/ITEM/ID	PRAZO (EM DIAS)	DATA INÍCIO	DATA ENTREGA

4. INFORMAÇÃOES COMPLEMENTARES

5. CIÊNCIA DA CONTRATADA

PREPOSTO DA CONTRATADA: [art. 32 da IN 01/2019/SGD]	NOME:		
	E-MAIL:	TELFONE:	CPF:

Brasília/DF, xx de xxxx de xxxx.

(*) Modelo meramente exemplificativo

ANEXO D - MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

TERMO DE RECEBIMENTO PROVISÓRIO

Identificação

Contrato:		**N° da OS / OFB:**	
Objeto:			
Contratante:			
Contratada:			

Por este instrumento, atestamos que os serviços (ou bens), relacionados na O.S. acima identificada, foram recebidos nesta data e serão objeto de avaliação quanto à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos pela Contratante.

Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até xx dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Projeto Básico correspondente ao Contrato supracitado.

De Acordo

CONTRATANTE	**CONTRATADA**
Fiscal Técnico do Contrato	**Preposto**
_____ ***<Nome>*** **Matrícula: *<Matr.>***	**_____** ***<Nome>*** ***<Qualificação>***

_____, _____ de _____ de 20_____.

ANEXO E - MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

TERMO DE RECEBIMENTO DEFINITIVO

Identificação

Contrato Número:		**N° da OS / OFB:**	
Objeto:			
Gestor do Contrato:			
Fiscal Requisitante do Contrato:			

Por este instrumento, os servidores acima identificados atestam que o(s) serviço(s) ou bem(ns) integrantes da Ordem de Serviço ou de Fornecimento de Bens acima identificada possui(em) qualidade compatível com a especificada no Projeto Básico e do Contrato supracitado.

De Acordo

CONTRATANTE	**CONTRATADA**
Fiscal Técnico do Contrato	**Preposto**
_____ ***<Nome>*** **Matrícula: *<Matr.>***	**_____** ***<Nome>*** ***<Qualificação>***

_____, _____ de _____ de 20_____.

ANEXO F - ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

SEI nº (10412326)

Documento assinado eletronicamente por **Filipe Carneiro Guimarães**, **Analista de Sistemas**, em 23/09/2022, às 14:56 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Victor Hugo De Souza Peçanha**, **Integrante Técnico**, em 23/09/2022, às 15:10 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Wanessa Queiroz de Souza Oliveira**, **Subsecretária de Planejamento e Tecnologia da Informação**, em 23/09/2022, às 20:54 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Ivancir Gonçalves da Rocha Castro Filho**, **Coordenador-Geral de Recursos Logísticos**, em 26/09/2022, às 12:43 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Elizangela Jaines**, **Chefe da Divisão de Licitações e Compras**, em 04/11/2022, às 14:40 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.