Expansão Da Solução De Gerenciamento De Ambiente Compartilhado, Para Inclusão De Funcionalidade De Conectividade Segura, Com Análise De Conteúdo E Aferimento A Normativos Internos A Usuários Digitais

ANEXO I

TERMO DE REFERÊNCIA

1. Objeto

Expansão da Solução de Gerenciamento de Ambiente Compartilhado, para inclusão de funcionalidade de conectividade segura, com análise de conteúdo e aferimento a normativos internos a usuários digitais.

A utilização do ambiente de uso comum trará as seguintes consequências para a administração:

- Economia de custos – manter um ambiente computacional exige altos investimentos em instalação, configuração, mão de obra especializada e um potente sistema de refrigeração o que ao final do mês aumenta os custos de energia elétrica e integração com parâmetros de economia limpa
- Escalabilidade – Adequação de escalabilidade nativa com valor de investimento com decorrência instantânea.
- Agilidade – Implantação ágil de novos recursos. O SESC-DF terá a disposição recursos ilimitados mediante a necessidade de negócio.
- Suporte 24 horas – Os ambientes de cloud são preparados e garantem a disponibilidade do serviço 24 horas por dia. Em caso de falhas, os sistemas automaticamente são transferidos para outro ambiente disponível.
- Armazenamento Ilimitado – O espaço de armazenamento na nuvem é fornecido sobre demanda.
- Backup – Realizar o backup de dados na nuvem é mais prático, rápido e barato do que em dispositivos físicos.

- Universalização do acesso – Com as aplicações na nuvem, o cliente poderá acessar os dados de onde estiver, desde que esteja conectado à internet.

2. Justificativa de Fabricante e Solução

A adoção, pela Administração Regional do Sesc/DF, do Regulamento de Licitações e Contratos, aprovado pela Resolução Sesc nº 1.252, de 06 de junho de 2012, aprovada pela Resolução Sesc/AR/DF nº 887/2012, estabelece em seu Art. 4º, parágrafo 1º que:

> *"Sempre que possível e conveniente, as compras deverão atender ao princípio da padronização, da compatibilidade de especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, de assistência técnica e das garantias oferecidas."*

Estabelece ainda no parágrafo 2º, inciso III:

> *"a justificativa da necessidade do tipo específico, quando citar marcas, modelos ou características que possam vir a direcionar a aquisição para um determinado material, bem ou serviço."*

Considerando-se ainda que o Tribunal de Contas da União – TCU, por intermédio das decisões nº 907/97, prolatada da sessão realizada em 11 de dezembro de 1997, publicada no Diário Oficial da União de 26 de dezembro de 1997 e 461/98, de 22 de julho de 1998 que consolidaram a interpretação de que os Serviços Sociais Autônomos não estão sujeitos aos estritos procedimentos da Lei nº 8.666/1993 e sim aos seus regulamentos próprios devidamente publicados.

O Sesc/AR/DF visando a continuidade e evolução técnica da solução de segurança em funcionamento em seu ambiente computacional, bem como, a manutenção e aprimoramento técnico de sua equipe de infraestrutura de rede, ratifica que todas as especificações técnicas exigidas nesse Termo de Referência espelham-se na solução hoje adotada e em produção no seu ambiente de rede corporativo.

3. Relação de Itens

Item	Descrição	Quantitativo
1	Solução de Software NetSkope Licenciamento de solução de segurança de acesso a internet composta de conectividade segura para Unidades Operacionais e implementação das funcionalidades de anti-malware, anti- ransonware e prevenção contra vazamento de dados proteção para nuvens corporativas e terceiras. NSKP-PKG-NG-SWG-PRO NSKP-NPA NSKP-SUPPORT-PRE	1000
2	Serviço de Operação Assistida da Base de Produtos Netskope. (Unidade: Horas)	8064

4. Especificação Técnica Global

4.1. Características de Fabricante

4.1.1. Conforme descrito no item 01 e ainda com necessidade de integração nativa da solução especificada com solução já utilizada pelo Sesc/AR/DF, admite-se para este processo no itens 01, apenas produtos do fabricante Netskope

4.1.2. Os Iten 02 é composto de serviços profissionais prestados para o adequado funcionamento do ambiente e dos softwares utilizados pelo SESC-DF

4.2.Caraterísticas de Validade Contratual e Suporte a Solução

4.2.1. Os produtos e serviços ofertados devem ser validos pelo período de 12 meses, assim como contratos de suporte manutenção

4.2.2. A Renovação do Contrato será executada de forma automática e obrigatória cada 12 meses, pelo período mínimo de 36 meses, e período máximo facultativo de mais 24 meses, em duas renovações anuais, totalizando 60 meses.

4.2.3. Durante todo o período de garantia contratado o serviço de suporte deverá ser suprido 24x7 (vinte e quatro horas por dia, sete dias por semana,) para toda a solução ofertada, incluindo chamados técnicos;

4.2.4. Os chamados deverão ser abertos no fabricante ou em sua rede credenciada, através de número telefônico 0800 ou equivalente à ligação local, fornecendo neste momento o número, data e hora de abertura do chamado.

4.2.5. A garantia técnica deverá abranger a manutenção corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive substituição de peças, partes, componentes de acessórios e atualizações de software durante o prazo de garantia, sem representar qualquer ônus para a contratante;

5. Solução de Software NetSkope

5.1.1. A solução proposta deve ser parte contida de uma Plataforma SASE mais abrangente, composta por:

5.1.2. Plano de Controle: Core da solução capaz de tomar decisões de Rede e Segurança baseando-se em critérios como identidade do usuário, estado do dispositivo, hora do dia, geolocalização, latência, destino e aplicação

5.1.3. Rede: Backbone do fabricante responsável por conectar os usuários, de maneira otimizada, à internet.

5.1.4. Arquitetura de Rede e Segurança: Capacidades baseadas em micros serviços para prover componentes de rede e segurança totalmente integrados a plataforma, provendo todo o contexto de acesso e proteção em nuvem.

5.1.5. Endpoints: Inclui todos os usuários, dispositivos e aplicações com capacidade de se conectar diretamente aos serviços de segurança providos pela Plataforma.

5.1.6. Appliances: Capacidade de integrar ambientes on-premise e localidades remotas com a plataforma por meio de redirecionamento seguro, a exemplo: NGFW ou Equipamentos SD-WAN

5.1.7. A Plataforma SASE deverá possuir painel de governança completo, permitindo uma visão situacional e granular das atividades dos usuários e seus respectivos acessos as aplicações, sejam elas SaaS, On-Premise ou Web.

5.1.8. Para melhor visibilidade, a plataforma deve empregar decodificação de aplicações que se utilizam de API ou JSON, garantindo melhor visibilidade inspeção.

5.1.9. A integração com serviços SaaS Sancionados não deve depender única e exclusivamente das API's fornecidas pelo provedor de serviço, sendo possível o redirecionamento do tráfego diretamente para a plataforma e o processamento deste em tempo real.

5.1.10. A plataforma SASE deve oferecer controles de proteção de dados e de ameaças com visibilidade e controle granular das atividades para os protocolos HTTP e HTTPS.

5.1.11. Em cada Datacenter, a solução deverá prover inspeção do tráfego admitido pela plataforma.

5.1.12. A plataforma SASE deverá possuir relacionamento direto com os principais provedores de serviços IaaS, serviços SaaS e CDN’s.

5.1.13. A plataforma SASE deverá ser escalável em todos os módulos descritos, não havendo limitadores, como por exemplo:

5.1.14. Throughput,;

5.1.15. Uso de datacenters;

5.1.16. Quantidade máxima de usuários;

5.1.17. Throughput de tráfego criptografado;

5.1.18. Quantidade de aplicações internas redirecionadas

5.1.19. A solução deverá processar o tráfego admitido em território brasileiro, não sendo aceito modelos de redirecionamento de tráfego (virtual pop) ou posicionamento em nuvens públicas.

5.1.20. O fabricante deverá dedicar, no mínimo, 1 datacenter no Brasil para processamento do tráfego em território brasileiro.

5.1.21. Em caso de indisponibilidade no Datacenter situado em território brasileiro, será aceito que outro Datacenter seja capaz de processar o tráfego sem necessidade de chaveamentos manuais ou redirecionamentos de tráfego.

5.1.22. A Plataforma SASE deverá ser capaz de redirecionar o acesso a aplicações internas hospedadas no datacenter do SESC- DF

5.1.23. Solução deverá se basear no modelo Zero Trust Network Access.

5.1.24. Solução deverá garantir a restrição de privilégio apenas a aplicação, não permitindo a movimentação lateral.

5.1.25. A Plataforma SASE deverá assegurar a criptografia da sessão, utilizando tunelamento seguro (TLS 1.3).

5.1.26. Deve possuir integração com provedores de identidade para sincronização de usuários e grupos.

5.1.27. A Plataforma SASE deve restringir o acesso a aplicações por meio da classificação e validação da conformidade do dispositivo, rotulando-o como:

5.1.28. Gerenciado: Com características definidas pelo administrador, a exemplo: Existência de Criptografia de Disco, Existência de uma determinada chave de registro associada a um valor, Host inserido no domínio, Processo específico em execução.

5.1.29. Não Gerenciado: Não atende as características definidas pelo administrador.

5.1.30. A Plataforma SASE deverá permitir indicar o host e porta específicos que respondem por uma determinada aplicação, restringindo o acesso por usuário.

5.1.31. A solução deve ser capaz de continuamente solicitar ao usuário que autentique novamente antes de ter acesso as aplicações privadas.

5.1.32. A Plataforma SASE deverá tornar disponível a aplicação a partir de configuração na console, sem a necessidade de convergência ou alteração de rotas locais para adequação ao serviço.

5.1.33. A Plataforma SASE deverá, por meio do agente instalado, avaliar a conformidade do dispositivo antes de liberar o acesso a aplicações SaaS públicas, aplicações privadas e acesso Web, a depender da:

5.1.34. Presença de criptografia de Disco;

5.1.35. Presença de processo em execução;

5.1.36. Presença de arquivos em disco;

5.1.37. Se a máquina pertence a um domínio do Active Directory;

5.1.38. Existência de Certificado Digital no dispositivo.

5.1.39. Após admissão e pré-processamento do tráfego a plataforma SASE deverá ser capaz de identificar os seguintes classificadores como origem do tráfego:

5.1.40. Usuário ou Grupo de Usuários;

5.1.41. Endereço IP;

5.1.42. Sistema Operacional;

5.1.43. Classificação do dispositivo;

5.1.44.

5.1.45. A Plataforma SASE deverá prover um painel único de visibilidade, sendo esta baseada no conceito Nuvem SaaS.

5.1.46. A Plataforma SASE deve ser capaz de decodificar aplicações e serviços em nuvem que se disfarçam em tráfego Web para entendimento do conteúdo e aplicar proteção relacionadas a:

5.1.47. Proteção contra vazamento de dados;

5.1.48. Proteção contra ameaças (malware, phishing e ataques);

5.1.49. O Perfi de monitoramento de credenciais deve possuir a capacidade de detectar, no mínimo, as seguintes anomalias no padrão de uso dos aplicativos em nuvem:

5.1.50. Detectar atividade suspeita de violação de proximidade no acesso as aplicações quando, por exemplo, em um curto intervalo de tempo, as mesmas credenciais de acesso forem usadas para fazer login na mesma aplicação a partir de localidades distantes;

5.1.51. Deve ser possível customizar a distância entre os dois locais e o espaço de tempo entre um e evento e outro;

5.1.52. Deve ser possível criar listas brancas para redes confiáveis a fim de evitar falso-positivos;

5.1.53. Detectar atividade suspeita de usuários que fizerem download em massa de arquivos das aplicações em nuvem;

5.1.54. Deve ser possível customizar a quantidade de arquivos baixados por tempo para que seja gerado o alerta de atividade suspeita;

5.1.55. Detectar atividade suspeita de credenciais sendo compartilhadas entre usuários da instituição;

5.1.56. Deve ser capaz de identificar um vazamento de dados a partir de uma instância corporativa com destino a uma instância pessoal de nuvem;

5.1.57. A plataforma SASE deve prover visibilidade e inspeção para URL's, garantindo o entendimento do conteúdo e aplicar proteções relacionadas a:

5.1.58. Proteção contra vazamento de dados;

5.1.59. Proteção contra ameaças (malware, phishing e ataques);

5.1.60. A Plataforma SASE deverá interceptar e inspecionar o tráfego Web, garantindo:

5.1.61. Descoberta de aplicações SaaS

5.1.62. Controle de acesso para dispositivos gerenciados e BYOD

5.1.63. Acesso contextual as aplicações

5.1.64. A Plataforma SASE deve habilitar proteções contra ameaças avançadas, incluindo ameaças em nuvem, como por exemplo:

5.1.65. Cloud Phishing;

5.1.66. Cloud Payload Delivery;

5.1.67. Callback;

5.1.68. Deve prover controle de dados confidenciais e classificados importados para mídias sociais, mensagens, aplicativos de notas, fóruns, dentre outros.

5.1.69. Capacidade de aplicar políticas granulares a nível de atividade em mais de 10 aplicativos do pacote O365

5.1.70. Capacidade de aplicar políticas de nível de atividade granular no pacote O365

5.1.71. Capacidade de aplicar políticas granulares de nível de atividade para OneDrive

5.1.72. Capacidade de impor políticas granulares de nível de atividade para o SharePoint

5.1.73. Capacidade de aplicar políticas granulares de nível de atividade para Yammer

5.1.74. Capacidade de aplicar políticas granulares de nível de atividade para o Word Online

5.1.75. Capacidade de aplicar políticas granulares de nível de atividade para o PowerPoint Online

5.1.76. Capacidade de aplicar políticas de nível de atividade granular para o Outlook.com

5.1.77. Capacidade de aplicar políticas granulares de nível de atividade para o Exchange Online

5.1.78. Capacidade de aplicar políticas granulares de nível de atividade para o Power BI

5.1.79. Capacidade de aplicar políticas granulares de nível de atividade para o Dynamics CRM

5.1.80. Capacidade de impor políticas granulares de nível de atividade para o Skype for Business

5.1.81. Capacidade de aplicar políticas granulares de nível de atividade para Teams

5.1.82. O Perfil de proteção deverá garantir o controle contra movimentação de dados sensíveis nos ambientes:

5.1.83. URL's

5.1.84. Aplicações SaaS Sancionadas;

5.1.85. Aplicações SaaS Não Sancionadas;

5.1.86. Deve conter mais de 40 modelos de conformidade regulamentar, incluindo templates pré-definidos como LGPD e GDPR;

5.1.87. Deve possuir nativamente perfis de DLP pré-definidos baseados em normas regulamentares (Exemplo: PCI, GDPR e LGPD) e permitir também a criação de perfis customizados;

5.1.88. Deve possuir, no mínimo, 3 mil identificadores nativos de dados incluindo identificadores brasileiros com validadores para: CNH, CNPJ, CPF e Número de conta bancária brasileira, endereços brasileiros, nomes brasileiros, placa de veículo, renavam, RG, número social e título de eleitor;

5.1.89. Deve permitir a criação de dicionários de dados baseados em palavras-chave, frases e expressões regulares para serem usados nas regras de DLP;

5.1.90. Deve permitir a criação de regras customizadas de DLP através de expressão regulares, dicionários e palavras chaves com opção de uso de operadores boleanos;

5.1.91. Deve possuir a capacidade de detectar informações confidenciais em, no mínimo, 500 tipos de arquivos distintos

5.1.92. A Plataforma SASE deve ser capaz de inspecionar o tráfego criptografado e inspecionar aplicações legítimas que hospedem artefatos maliciosos;

5.1.93. Através da capacidade de inspeção do tráfego deve incluir a decodificação de aplicações com capacidade de identificar:

5.1.94. Ações (Upload, Download, create, Edit, Print, Share, dentre outras);

5.1.95. Instância da Aplicação SaaS;

5.1.96. Usuário da aplicação (pessoal e corporativo);

5.1.97. Geolocalização;

5.1.98. A Plataforma SASE deverá proteger o acesso do usuário aos dados corporativos, controlando a exposição dos mesmos quanto a movimentação entre nuvens (Serviço SaaS sancionado para Serviço SaaS não sancionado)

5.1.99. A Plataforma SASE deve possuir base própria de aplicações SaaS, com capacidade de controle granular, oferecendo no mínimo:

5.1.100. Identificação do usuário ou grupo;

5.1.101. Validação do dispositivo (gerenciado ou não gerenciado);

5.1.102. Categoria da Aplicação SaaS;

5.1.103. Nível de Risco da aplicação SaaS;

5.1.104. Controle granular de atividades (Upload, Share, Edit, Post, Print, Create, Download, dentre outros);

5.1.105. A Plataforma SASE deverá aplicar controles em tempo real, garantindo que ações sejam controladas, para:

5.1.106. Aplicações SaaS Sancionadas;

5.1.107. Aplicações SaaS Não Sancionadas;

5.1.108. Sítios Web;

5.1.109. O Fabricante da plataforma SASE deve ter em sua base de inteligência a capacidade de conhecer, decodificar, controlar e indicar o risco associado para mais de 30 mil aplicações

5.1.110. O centro de inteligência do fabricante deve pontuar o índice de risco no uso de cada uma as aplicações SaaS não sancionadas;

5.1.111. Deve possuir associar o índice de risco de uma determinada aplicação ou categoria de aplicações a uma regra de bloqueio em tempo real

5.1.112. Deve permitir que as aplicações em nuvem possam ser comparadas na interface gráfica da solução onde as características de uma aplicação possam analisadas em relação a outra. Ex: Microsoft One Drive e ICloud;

5.1.113. O sistema de comparação de aplicativos em nuvem deve ser capaz permitir uma avaliação das aplicações a fim de apoiar a instituição a determinar se o uso de um determinado aplicativo deve ser permitido ou bloqueado.

5.1.114. Ao realizar a comparação entre aplicações, a plataforma deverá apresentar os seguintes resultados:

5.1.115. Informações sobre recuperação de desastre e continuidade de negócios. Exemplo: o backup dos dados é feito em local geograficamente separado do datacenter principal, etc;

5.1.116. Informações sobre como a proteção de dados é feita. Exemplo: dados criptografados em repouso, dados criptografados em trânsito, etc;

5.1.117. Informações sobre incidentes;

5.1.118. Certificações e normas que a aplicação está aderente. Exemplo: PCIDSS, SOC-1, SOC-2 e SOC-3;

5.1.119. Informações sobre privacidade dados. Exemplo: ao armazenar dados na aplicação, o cliente é o proprietário dos dados?

5.1.120. O sistema de classificação das aplicações de nuvem cadastradas pelo fabricante deve possuir, no mínimo, as seguintes informações sobre as aplicações:

5.1.121. Nível de aderência a GDPR;

5.1.122. Categoria da aplicação;

5.1.123. Funções suportadas pela aplicação. Ex: post, share, send, etc;

5.1.124. Nível de risco para o negócio da empresa;

5.1.125. Violações que a aplicação já sofreu em ataques cibernéticos com informações sobre a data e a fonte da violação;

5.1.126. A plataforma SASE deve ser capaz de ter visibilidade frente ao tráfego on-premises por meio de análise de logs das soluções de SIEM, Proxy e Firewall implantados

5.1.127. A solução deverá permitir o envio automatizado da carga de logs a ser inspecionada

5.1.128. Ao administrador, deve ser facultada a criação/customização de interpretadores de logs a partir da própria console gráfica da solução

5.1.129. Deve ser possível testar o parser de um log a partir da própria console gráfica da solução com exibição dos eventos extraídos;

5.1.130. O perfil de proteção contra ameaças deve conter as seguintes capacidades:

5.1.131. Análise de artefatos por meio de assinaturas;

5.1.132. Análise de artefatos por meio de heurística;

5.1.133. Análise comportamental de artefatos Portable Executable utilizando modelos de Machine Learning;

5.1.134. A Plataforma SASE deverá ser capaz, por meio de integração com SIEM, NGFW e EDR, suplementar o SOC com IOC’s (Hashes e URL), para que seja possível rastrear um ataque onde quer que ele aconteça.

5.1.135. O perfil de proteção deverá garantir a proteção contra exploração remota do cliente;

5.1.136. A Plataforma SASE deve permitir a descoberta automática de aplicações por meio da inspeção e decodificação do tráfego, garantindo visibilidade completa, sem a necessidade de importar logs de dispositivos terceiros;

5.1.137. A Plataforma SASE deverá garantir a inspeção e visibilidade de URL's, garantidas por meio de uma base de conhecimento do fabricante com mais de 100 categorias disponíveis.

5.1.138. A Plataforma SASE deve prover controles granulares de forma a controlar e garantir o acesso seguro a URL's, garantindo:

5.1.139. Controle de Acesso por URL ou Categoria de URL

5.1.140. Identificação do usuário ou grupo;

5.1.141. Controle granular de atividades;

5.1.142. Geolocalização do acesso;

5.1.143. A Plataforma SASE deve ter a capacidade de analisar dinamicamente as URL's acessadas;

5.1.144. A Plataforma SASE deve, por meio da interceptação direta do tráfego, identificar ataques direcionados ao cliente, garantindo a não exploração dele.

5.1.145. Por se tratar de uma plataforma em nuvem, é obrigatória a adoção de boas práticas mínimas de segurança, dentre elas:

5.1.146. O design e o desenvolvimento da plataforma SASE têm que seguir as recomendações do Open Web Application Security Project (OWASP).

5.1.147. A ferramenta deve ser submetida a avaliações periódicas e testes de penetração, também realizados por terceiros, como parte de sua metodologia de ciclo de vida.

5.1.148. A Plataforma SASE deverá garantir, por meio da sua arquitetura, capacidade de inspeção de tráfego criptografado, utilizando os métodos mais atuais de criptografia (TLS 1.3) de comunicações, além de possuir total escalabilidade ao permitir a inspeção de todo o tráfego admitido a plataforma.

5.1.149. Para efeitos práticos, o fabricante deve considerar 100% do tráfego criptografado, a ser inspecionado, normalizado e tratado.

5.1.150. Por meio do seu backbone e da arquitetura de rede e segurança, após admissão do tráfego o mesmo deverá sofrer toda parte de normalização e inspeção nos microserviços hospedados na plataforma SASE, sem que ocorra redirecionamentos e re-roteamento entre partes on-premise e em nuvem, como forma de melhorar a experiência no usuário

5.1.151. A Plataforma SASE deverá atuar como um roteador em nuvem, garantindo baixa latência e canal seguro, para aplicações privadas, seja ela On-Premises ou Cloud Pública

5.1.152. A solução não deverá se basear em tecnologias de VPN para fechamento do túnel seguro

5.1.153. Deverá ser capaz de prover predisposições de acesso distintas para o mesmo usuário, porém fazendo uso de máquinas com perfis distintos (Gerenciada e Não Gerenciada)

5.1.154. A Plataforma SASE deverá prover acesso seguro e controlado baseado nos protocolos TCP e UDP

5.1.155. Deverá prover acesso a aplicações baseada nas seguintes aplicações

5.1.156. SSH - TCP Porta 22

5.1.157. HTTP - TCP Portas 80, 443 e Customizadas

5.1.158. RDP - TCP 3389 e UDP 3389

5.1.159. SQL Server - TCP 1333, 1434 | UDP 1434

5.1.160. SMB - TCP 445

5.1.161. FTP - TCP 21

5.1.162. O acesso seguro as aplicações definidas poderão ser restritas, no mínimo, para:

5.1.163. Usuário Único

5.1.164. Múltiplos Usuários

5.1.165. Grupos de Usuário

5.1.166. Unidade Organizacional (OU)

5.1.167. Para cada acesso, a política deverá prover as seguintes possibilidades:

5.1.168. Alerta

5.1.169. Permissão

5.1.170. Bloqueio

5.1.171. Deve ser possível determinar apenas o endereço IP e porta de acesso da aplicação sem a necessidade de determinar um segmento de rede interno que o usuário remoto terá acesso;

5.1.172. Ao se conectar remotamente na solução para acesso a uma aplicação interna, a máquina remota não deve ter acesso, nem ser atribuído em um segmento de rede interna como em um sistema de VPN tradicional;

5.1.173. A solução deve ser capaz de continuamente solicitar ao usuário que autentique novamente antes de ter acesso as aplicações privadas em um iDP externo.

5.1.174. A solução deverá permitir o acesso diferenciado para um mesmo usuário conforme as seguintes condições:

5.1.175. Máquinas em Conformidade: A partir de uma máquina gerenciada, com pré-requisitos de segurança identificados, deve permitir o acesso a aplicação

5.1.176. Máquinas não Conformes: A partir de uma máquina gerenciada, uma estação que não atenda aos requisitos de segurança, deve bloquear o acesso a aplicação

5.1.177. A Plataforma SASE deverá tornar disponível a aplicação a partir de configuração na console, sem a necessidade de convergência ou alteração de rotas locais para adequação aos serviços

6. Serviço de Operação Assistida da Base de Produtos Netskope

6.1. A contratada deverá disponibilizar, sob demanda, horas de serviços técnicos especializados em segurança da informação, de forma a atender aos seguintes requisitos:

6.1.1. execução de até 8.064 (oito mil e sessenta e quatro) horas;

6.1.2. os serviços elegíveis a serem executados irão se limitar, exclusivamente, aos seguintes casos:

6.1.2.1. elaboração de pareceres em segurança da informação;

6.1.2.2. elaboração de relatórios gerenciais;

6.1.2.3. análise de segurança em elementos que sejam de propriedade da contratada ou que não estejam no escopo desse projeto;

6.1.2.4. suporte aos planos de melhoria na infraestrutura de segurança do SESC/DF;

6.1.2.5. suporte a mudanças de arquitetura do ambiente do SESC, sobretudo aos aspectos de segurança envolvidos;

6.1.2.6. avaliação de incidentes, incluindo a indicação de atualizações ou procedimento necessários para mitigar possíveis vulnerabilidades;

6.1.2.7. apoio na definição e implementação de mecanismos futuros de monitoramento de segurança;

6.1.2.8. configuração de segurança e atualização de versão de softwares da solução contratada;

6.1.2.9. orientação quanto a procedimentos de auditoria no ambiente computacional do SESC;

6.1.2.10. elaboração, em conjunto com o SESC, de planos de conscientização de usuários que proporcionem maior grau de segurança;

6.1.2.11. quaisquer serviços ou procedimentos realizados deverão ser previamente aprovados pela CONTRATANTE por meio de Ordem de Serviço, em comum acordo entre o SESC e a contratada, sendo que o tempo

necessário ao atendimento deverá ser previamente definido na respectiva Ordem de Serviço;

6.1.2.12. a prorrogação do prazo de execução de uma Ordem de Serviço somente será possível mediante apresentação, pela contratada, de relatório de impacto contendo justificativas plausíveis, devidamente aceitas pela CONTRATANTE, ou por interesse desta, em caso de impedimento devidamente justificado que dificulte ou não permita a execução dos serviços;

6.1.2.13. as ordens de serviço só serão consideradas concluídas após a entrega da documentação dos procedimentos e da configuração resultante nas bases e nos padrões definidos pelo SESC (incluindo documento as-built);

6.1.2.14. para recebimento dos serviços será preenchido o Termo de Recebimento de Serviços.

6.1.2.15. o SESC deve avaliar os serviços entregues em até 10 (dez) dias úteis contados da entrega dos serviços exigidos;

6.1.2.16. a contratada deverá reapresentar o serviço corrigindo eventuais observações feitas pelo SESC em até 10 (dez) dias úteis, a contar da comunicação;

6.1.2.17. estando todos os elementos necessários, a CONTRATANTE fará o recebimento definitivo dos serviços no prazo máximo de 15 (quinze) dias úteis;

6.1.2.18. para a recebimento definitivo será preenchido o Termo de Recebimento de Serviços.

6.1.2.19. o SESC somente autorizará o pagamento das faturas emitidas após o recebimento definitivo dos serviços, realizado mensalmente, de acordo com os níveis mínimos de serviço estabelecidos.

6.2. os chamados abertos somente poderão ser fechados após autorização do SESC;

6.3. a contratada deverá realizar os devidos escalonamentos de acordo com a criticidade e nível de atendimento do incidente ou problema reportado pelo cliente ou pelo sistema de monitoração;

6.4. após resolução de um chamado técnico, a empresa contratada deverá encaminhar ao SESC relatório contendo descrição do chamado aberto, procedimento de resolução adotado e outros adicionais que poderão ser executados para que o problema ocorrido não se repita;

6.5. a contratada deverá fornecer mensalmente os relatórios abaixo descritos:

6.5.1. dados, informações, indicadores e métricas que permitam quantificar o percentual de disponibilidade da central de atendimento da contratada, detalhados para a central de atendimento telefônico e para o portal na Internet;

6.5.2. atividades de suporte e manutenção, com pelo menos descrição de: problemas, correções, aplicações de patches, mudanças de configuração e eventos ocorridos no período;

6.5.3. chamados abertos no período, ações corretivas tomadas, tempos para execução das atividades;

6.5.4. diagnóstico dos ambientes monitorados, obtido por meio do cruzamento das informações obtidas nos logs coletados;

6.5.5. relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a qualidade e desempenho dos serviços prestados em relação ao atingimento ou não dos níveis mínimos de serviço.

6.6. Níveis Mínimos de Serviços (SLA)

6.6.1. Serão estabelecidos os seguintes prazos máximos de conclusão das atividades, os indicadores utilizados na mensuração da qualidade dos serviços e os respectivos fatores de abatimento pelo descumprimento dos níveis mínimos de serviço associados:

Atividade	Nivel minimo de serviço	IndMeta	Indicador para NMS	Fator de peso da atividade (FPA)
1 - Gerenciamento de regras e políticas	120 minutos após abertura de chamado	120 minutos	regra implementada	0,5
2- Alteração de configurações	240 minutos após abertura de chamado	240 minutos	configuração implementada	0,5
3 - Chamados Emergenciais (limitados a 20 por mês e relacionados apenas a gerenciamento de regras ou alteração de configurações)	20 minutos após abertura do chamado	20 min	chamado concluído	1
4 - Verificação e filtragem de logs	24 horas após a abertura do chamado	24 horas	Arquivo de Log enviado ao requisitante	0,25
5- atualização de plataformas por meio da implementação de patches e fixes	5 dias após a liberação das atualizações pelo fabricante.	5 dias	Patch e fix instalados	0,5
6- registro de incidentes se segurança pela contratada	10 minutos após primeiro registro ou sintoma relacionado ao evento	10 min	chamado aberto	0,1
7 - Início de atuação para resolução de incidentes	15 minutos após a abertura de chamado pelo cliente ou pela contratada]	15 min	registro das ações tomadas no chamado pelo resposável pela resolução	0,5
8 - Resolução de incidentes que provoquem indisponibilidade dos serviços e que não necessitem substituição de peças	60 minutos após a abertura do chamado pelo cliente ou contratada	60 min	chamado concluído	1,5
9 - resolução de incidentes que não provoquem indisponibilidade dos serviços	240 minutos após abertura de chamado	240 minutos	chamado concluído	0,5

10 - Resolução de incidentes que provoquem indisponibilidade dos serviços e que necessitem de substituição de partes e peças	2 dias úteis após a abertura do chamado pelo cliente ou contratada	3 dias úteis	chamado concluído	2

1. os Fatores de Abatimento por Desempenho de Serviço (FADS) serão calculados com base na comparação dos resultados alcançados na execução das atividades com os níveis de serviço definidos na Tabela acima.

2. o FADS será calculado como somatório das ocorrências realizadas para cada uma das atividades definidas, conforme fórmula a seguir:

$$\mathbf{FADS_K = [(n*FPA_K)/100]*VMC_K}$$

FADS é o Fator de Abatimento por Desempenho de Serviço;
k é o item de serviço contratado
n é a quantidade de ocorrências da atividade que não atenderam o NMS definido;
FPA é o Fator de Peso da Atividade;
VMC é o valor mensal do contrato;

7. Instalação e Configuração da Solução caso necessária

7.1.1.1. Caberá à CONTRATADA a elaboração e execução do plano de implementação, envolvendo:

7.1.1.2. Documentação de planejamento e implementação detalhada;

7.1.1.3. Configuração das funcionalidades de firewall conforme políticas discutidas com o responsável nomeado pelo CONTRATANTE;

7.1.1.4. Migração de regras e políticas se for o caso;

7.1.1.5. Criação dos usuários administradores da solução;

7.1.1.6. Criação de perfis de usuários diversos da solução;

7.1.1.7. Realização de backup das configurações;

7.1.1.8. Operação Assistida de Funcionamento da Solução, que consiste na disponibilização de um técnico para sanar quaisquer dúvidas e problemas que ocorrerem nos primeiros 10 (dez) dias úteis de operação da solução;

7.1.1.9. Testes de Aceite e Funcionamento;

7.1.1.10. Fornecimento da documentação de todo o projeto;

7.1.1.11. A instalação dos equipamentos deverá ser efetuada pela CONTRATADA ou Fabricante de forma remota ou presencial, conforme orientação do Serviço de Infraestrutura, observados os seguintes itens:

7.1.1.12. Todos os componentes necessários para o correto funcionamento dos equipamentos ofertados devem ser fornecidos pela CONTRATADA;

7.1.1.13. A entrega deverá ocorrer no prazo máximo de 10 dias a contar da assinatura do contrato.