TERMO DE REFERÊNCIA

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM SOLUÇÃO PARA PROVIMENTO DE SERVIÇOS DE SEGURANÇA POR MEIO DE NUVEM PRIVADA ESPECIALIZADA.

1. OBJETO

1.1. Pregão Eletrônico por Sistema de Registro de Preço para Contratação de objeto de natureza comum, solução de segurança da informação baseada em nuvem, por meio da plataforma Netskope, incluindo a disponibilização de licenças de uso, suporte técnico especializado, atualizações e serviços de implementação, com o objetivo de assegurar a proteção de dados, visibilidade e controle de acessos a aplicações em nuvem, tráfego web e ambientes híbridos, conforme condições, quantidades e exigências estabelecidas neste Termo de Referência.

2. JUSTIFICATIVA DA AQUISIÇÃO

2.1. Renovação e expansão da solução de segurança da informação Netskope, com agregação contratual dos contratos existentes Siged 26486-5/2022 e 92265-0/2022.

2.2. O Serviço do Comércio do Distrito Federal – SESC-DF, tem por premissa manter a inovação tecnológica como parte do seu objetivo de negócio para prover um serviço mais moderno e próximo aos seus filiados. Parte da inovação se dá pela nova arquitetura de serviços computacionais proposta por esta gestão para adoção de serviços em nuvens públicas, a exemplo: Microsoft Azure, Amazon AWS e Google Cloud.

2.2.1. A inovação está atrelada a tecnologia denominada Security Service Edge, cunhada pelo Gartner em 2019. Alinhada aos direcionamentos previstos na Evolução 2026, com o planejamento estratégico declarado, e visando atender as necessidades robustas, arrojadas e agressivas dos negócios existentes, dos novos negócios da empresa e atenta a divulgação de relatórios semanais, dos mais conceituados órgãos/institutos de pesquisa sobre cibersegurança, onde revelam que o Brasil voltou a integrar o ranking dos cinco países que mais sofrem ataques ransomware em todo o mundo, conforme noticiado pela Abranet (https://www.abranet.org.br/publicacoes/noticias/3056) - “O Brasil é o segundo país com mais ameaças ransomware, concentrando 10,57% das ameaças globais, atrás

apenas dos Estados Unidos, que representam 11,10%. Os outros países que compõem o Top 5 em número de ameaças ransomware são Índia, Vietnã e Turquia”

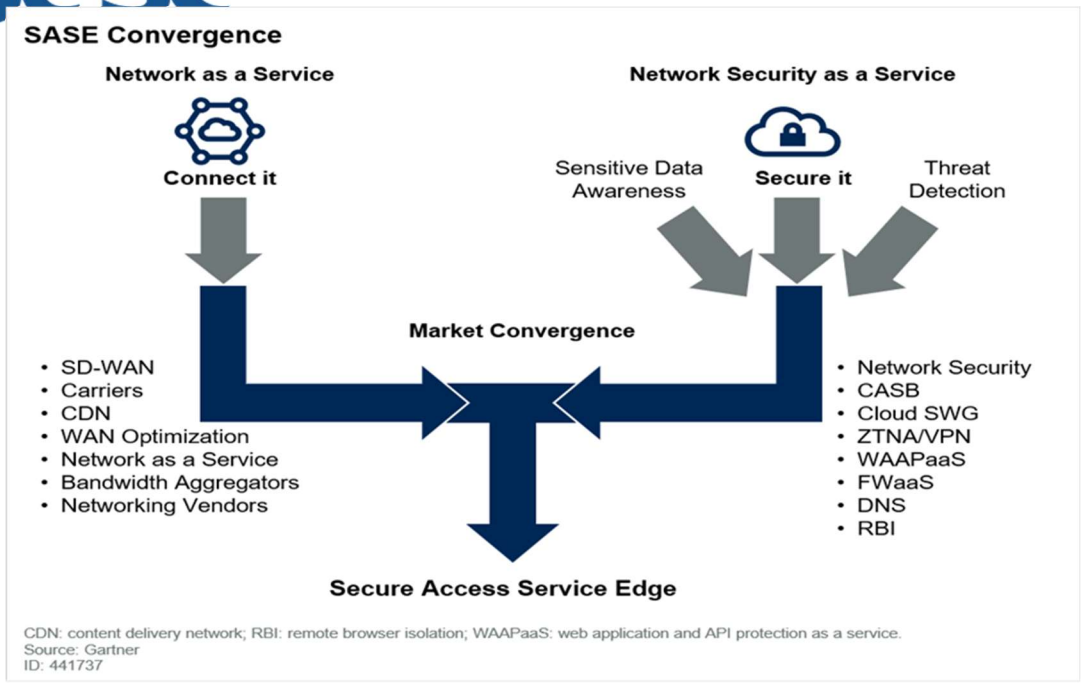
2.2.2. Considerando o panorama global, o Brasil ocupa atualmente, a 4ª posição no ranking, relacionado a ameaças digitais conforme noticiado através da CNN (https://www.cnnbrasil.com.br/economia/macroeconomia/brasil-e-o-4o-pais-da-america-latina-com-mais-ameacas-digitais-no-primeiro-semestre-de-2024-diz-pesquisa/#:~:text=Macroeconomia-,Brasil%20%C3%A9%20o%204%C2%BA%20pa%C3%ADs%20da%20Am%C3%A9rica%20Latina%20com%20mais,semestre%20de%202024%2C%20diz%20pesquisa&text=O%20Brasil%20foi%20o%204%C2%BA,empresa%20de%20seguran%C3%A7a%20cibern%C3%A9tica%20EST.):

> “O Brasil foi o 4º país na América Latina com mais ameaças digitais detectadas no primeiro semestre de 2024, segundo levantamento feito pele empresa de segurança cibernética EST. No período, o país registrou 201 mil ameaças (7,76%).”

2.2.3. Essa modalidade consiste na invasão “On-premise” ou nuvem, em servidores, estações de trabalho, notebooks e consequente sequestro dos dados, com desbloqueio mediante pagamento.

2.2.4. A proposta para esta arquitetura de segurança em nuvem é desenhada para modernizar o formato de proteção aos usuários do SESC-DF, uma vez que irá aplicar tal controle independentemente de onde o usuário esteja, seja dentro do SESC-DF ou em casa ou em deslocamento de viagem, garantindo a proteção de dados e proteção contra ameaças para usuários e dispositivos localizados em qualquer lugar e a qualquer momento, a partir de uma única borda fornecida na nuvem.

2.2.5. De um modo geral, para ampliar a capacidade de execução e em sua abrangência de visão, respostas a ataques cibernéticos e gerenciamento de riscos, é iminente a implantação de uma plataforma Security Service Edge (SSE), entregue na nuvem para lidar com essas mudanças, e que, após a implantação dos novos Firewalls NGFW e SD-WAN, irão convergir para a arquitetura Secure Access Service Edge (SASE).



2.3. **Acesso ZTNA (Zero Trust Network Access ou Acesso a Rede baseado na Confiança Zero)**

2.3.1. O ZTNA é baseado em autenticação e permite que o usuário realize o acesso apenas nas aplicações específicas que necessitar. Assim, tornando todo o restante da rede inacessível para estes usuários. Isso, sem dúvidas, representa um benefício considerável quando comparamos com as dificuldades e restrições que são normalmente impostas para o uso de VPNs.

2.3.2. Um dos grandes e talvez o mais importante benefício do uso do acesso ZTNA é a redução da superfície de ataque que diferente do acesso por meio das redes privadas virtuais (VPN), o ZTNA concede acesso apenas a serviços e aplicativos específicos, se baseando no conceito de confiança zero, enquanto as VPNs concedem acesso a uma rede inteira. Ou seja, o ZTNA consegue garantir um acesso seguro de forma granular.

2.3.3. E com o crescente número de usuários acessando recursos da empresa de forma remota, o modelo de Zero Trust passou a ser muito utilizado. Isso porque ele fortalece a segurança da empresa ao remover a confiança implícita e impor autenticação de usuário e dispositivo em toda rede. A solução de ZTNA se tornou ideal pois ajuda a eliminar lacuna de outras tecnologias e possibilita o acesso remoto com base em autenticação e no controle de permissões

2.3.4. Quando o ZTNA está em uso, o acesso aos recursos é concedido somente depois que o usuário é autenticado. Dessa forma, o usuário consegue acesso apenas

a aplicações específicas e que façam sentido para a realização do seu trabalho e todo o restante da rede fica inacessível. Sendo assim, primeiro é feita a autenticação do usuário e depois o ZTNA concede ao usuário acesso ao recurso específico por um túnel criptografado seguro. E esse processo é feito continuamente.

2.3.5. O ZTNA é importante não só para impedir que os usuários tenham visibilidade de outros recursos que ele não tenha permissão de acesso. Como também, para garantir a proteção contra ataques criminosos. Isso pois, caso um invasor consiga acesso, ele não seria capaz de acessar todos os aplicativos do SESC-DF.

2.4. **Serviços SWG (Secure Web Gateway – Gateway de Acesso Web Seguro)**

2.4.1. É uma solução de segurança projetada para proteger o tráfego da web em uma rede corporativa. Um SWG atua como intermediário entre os usuários da rede e a internet, inspecionando o tráfego de entrada e saída para detectar e bloquear ameaças e garantir o cumprimento das políticas de segurança da organização.

2.4.2. Essa implementação hoje em dia torna-se essencial para se proteger o ambiente corporativo de violações prevenindo ameaças em tempo real. Imagine um usuário tendo contato com malwares, ramsonware por exemplo, e trazê-lo para a sua rede interna pelo simples acesso a uma página web? O uso dessa tecnologia propõe a inspeção de tráfego SSL/TLS (tráfego criptografado) algo comum hoje. Ele analisa todo esse tráfego e consegue separar o que é tráfego legal do reconhecidamente ilegal ou prejudicial. O Gartner, em seu relatório Como se preparar para ataques de ransomware (gartner.com) destaca a importância de se utilizar SWG como uma camada de proteção não só para malwares, mas para o conjunto de objetos maliciosos que podem comprometer o ambiente. Senão vejamos:

2.4.2.1. O ataque começa com o ingresso — ou seja, o ponto inicial do ataque. Isso geralmente assume a forma de um site comprometido fornecido por meio de um ataque de phishing ou direcionado e pode incluir acesso obtido por meio de despejos de credenciais ou adquirido por meio de corretores de acesso. Gateways de e-mail seguro (SEGs) e gateways da Web seguros (SWGs) podem ajudar a fornecer camadas adicionais de proteção. Tecnologias como o isolamento da web também podem limitar o impacto.

2.4.2.2. A opção de escolha da solução de SWG em nuvem tem a clara intenção de proteger não somente aqueles acessos originados internamente, mas também aqueles realizados pelos usuários em atividade externa, home office.

2.5. **Serviços CASB (Cloud Access Security Broker – Agente de Segurança de Acesso à Nuvem)**

2.5.1. Um CASB é uma solução de segurança projetada para ajudar as organizações a protegerem dados, aplicativos e serviços que estão sendo acessados ou armazenados em ambientes de nuvem, como SaaS (Software as a Service), IaaS (Infrastructure as a Service) e PaaS (Platform as a Service).

2.5.2. O SESC-DF possui um contrato ativo da nuvem Microsoft 365. A adoção de tal plataforma permite o trabalho remoto da mesma forma que presencial sem os problemas hoje enfrentados com riscos em cima de serviços de VPN.

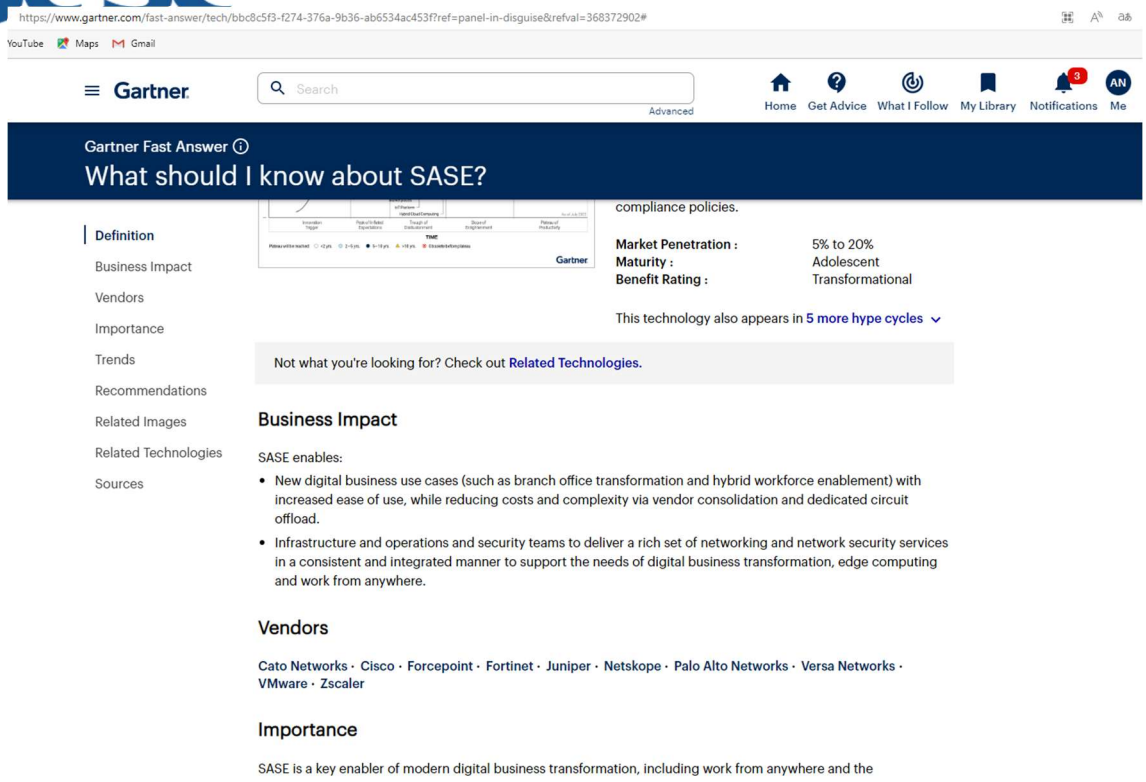
2.5.3. Quando mencionamos um serviço de CASB tratamos do objetivo de prevenir a Perda de Dados (DLP – Data Lost Prevention). O uso de tecnologias em conjunto reforça esse objetivo. Percebemos que associar o uso do SWG + CASB nos coloca no mesmo caminho do recomendado pelo Gartner (Guia de mercado para prevenção de perda de dados (gartner.com)).

2.5.4. Como se posiciona o mercado SASE segundo o Gartner

2.5.4.1. De acordo com o Gartner, para se atender às necessidades de SSE/SASE existe uma boa gama de fabricantes com possibilidades de atender ao objeto deste Estudo Técnico. Conforme verificamos no quadrante mágico de fevereiro de 2023 abaixo:

2.5.4.2. Gartner Fast Answer

2.5.4.2.1. Identificamos, ainda sobre o estudo do Gartner sobre o mercado de soluções SASE temos o seguinte:



2.5.4.3. Gartner Fast Answer

2.5.4.3.1. Dessa forma podemos garantir a competição necessária na disputa por esse projeto por parte do mercado. Outras observações que estamos considerando neste projeto são as dispostas, ainda, pelo Gartner no sentido de contratação de no máximo 3 (três) anos (contratos com no máximo 3 anos) para que se possa reavaliar e ajustar possíveis pontos de melhoria incluindo a análise se o provedor SASE está atendendo de maneira satisfatória e alinhado com as necessidades de negócio.

2.6. Ponto importante é que a arquitetura de rede do SESC-DF já está preparada para esse novo modelo de negócio denominado SASE. Através dos firewalls dispostos nas regionais e postos de atendimento, é possível alcançar este novo modelo de negócio trazendo mais agilidade e escalabilidade para o negócio do SESC-DF.

2.7. A contratação da plataforma Security Service Edge (SSE), tem como justificativa, acompanhar a tendência do mercado de tecnologia mundial, migração para a arquitetura Secure Access Service Edge (SASE), expandindo as capacidades da borda atual, aumentando a proteção de segurança de TIC de forma homogênea que além de permitirem a automação, a orquestração, a visibilidade, o gerenciamento centralizado dessa camada, prevenir e limitar a extensão de ataques cibernéticos, através do gerenciamento de vulnerabilidades, baseado em risco, dos ativos de

Tecnologia da Informação do SESC-DF, com análise contínua e adaptável de riscos e confiança, a fim de manter a confidencialidade, a disponibilidade e a integridade das informações, alcançando maior resiliência cibernética fim a fim.

2.8. Com a adoção de uma plataforma de segurança em nuvem, o SESC-DF deseja atingir os seguintes objetivos:

2.8.1. Agilidade: Capacidade de habilitar novos cenários de negócios digitais (aplicativos, serviços, APIs e dados compartilháveis para parceiros e contratados com menos exposição a riscos).

2.8.2. Melhor desempenho / latência: Roteamento otimizado para melhor conectividade com aplicações SaaS, Web e IaaS através de datacenters espalhados pelo território nacional provendo menor latência ao destino final.

2.8.3. Facilidade de uso: Por se tratar de uma aplicação SaaS, o SESC-DF espera atingir um uso facilitado, através da consolidação de múltiplos agentes e melhora na experiência do usuário, bem como adoção mais fácil de serviços.

2.8.4. Agilidade na adoção de novos serviços: Facilidade de mudança para projetos estratégicos, como mapeamento de requisitos de negócios, regulamentos e de acesso a aplicativos, para os recursos SSE.

2.8.5. Política centralizada com aplicação local: Gerenciamento centralizado baseado em nuvem com aplicação distribuída e tomada de decisão.

2.8.6. Definição de política centralizada, para prevenção de ameaças e proteção de dados.

2.8.7. Uso seguro da Web e da nuvem: Fornece visibilidade granular para qualquer atividade na nuvem, web e aplicações privadas;

2.8.8. Detectar e mitigar ameaças - Inspeções distribuídas que chegam o mais próximo possível do lugar e da maneira como os dados são acessados, seja na nuvem ou em um aplicativo privado.

2.8.9. Conectar e proteger trabalhadores remotos;

2.8.10. Identificar e proteger informações confidenciais;

2.8.11. Gerenciamento Unificado de Incidentes.

2.8.12. Controle de acesso sobre dispositivos gerenciados e não gerenciados.

2.8.13. Dados na nuvem e controles de permissão por meio de integrações de APIs

2.8.14. Aplicação de política de uso aceitável, com proteção avançada contra malware.

3. RELAÇÃO DE ITENS

	Item	Descrição	Quantitativo
LOTE ÚNICO	1	Solução de proteção acesso Web contra ameaças digitais.	1800
	2	Solução de acesso remoto as aplicações posicionadas em nuvem pública e interna.	1800
	3	Solução de segurança de acesso para resolução de nomes.	1800
	4	Solução de segurança para segurança do Office 365.	1800
	5	Solução de segurança para proteção de dados.	1800
	6	Solução para monitoramento de experiência digital do usuário.	1800
	7	Solução para proteção a rede pública Wi-Fi do SESC-DF.	50

4. DO REGISTRO DE PREÇO

4.1. A opção pela modalidade de Registro de Preço, prevista no Artigo 44 da Resolução SESC Nº 1.593/2024, se justifica plenamente para a Contratação de solução de segurança da informação baseada em nuvem, por meio da plataforma Netskope, incluindo a disponibilização de licenças de uso, suporte técnico especializado, atualizações e serviços de implementação para o SESC-AR/DF. Esta modalidade oferece flexibilidade operacional, eficiência administrativa e vantagens econômicas, adequando-se às necessidades estratégicas da contratação.

4.2. De acordo com o inciso I do Art. 44, trata-se de uma demanda recorrente, uma vez que as licenças possuem validade limitada (geralmente anual) e exigem renovação periódica para assegurar o funcionamento contínuo dos sistemas institucionais;

4.3. Conforme o inciso II do Art. 44, as especificações técnicas das licenças são padronizadas, com requisitos previamente definidos, o que favorece a consolidação da aquisição por meio do SRP;

4.4. O inciso IV do Art. 44, o Registro de Preço possibilita a contratação de bens e serviços por mais de um serviço social autônomo. Isso se alinha à visão estratégica do SESC-AR/DF de permitir que outros departamentos ou unidades do SESC-AR/DF ou do Sistema S possam, futuramente, aderir à Ata de Registro de Preço. Desta forma, o SESC e outras entidades podem ampliar os benefícios econômicos e operacionais dessa contratação, aumentando o poder de negociação e garantindo a padronização das soluções tecnológicas em diferentes unidades.

4.5. O uso do Registro de Preço garante maior controle e flexibilidade, uma vez que as contratações podem ser ajustadas conforme as necessidades específicas de cada unidade do SESC-AR/DF e outros possíveis aderentes, sem comprometer o prazo de execução ou o orçamento previamente estabelecido. O modelo também permite maior eficiência na gestão dos fornecedores e das garantias contratuais, conforme definido nos artigos 53 a 55 da Resolução SESC Nº 1.593/2024, assegurando que as aquisições sejam feitas de acordo com as condições e os prazos registrados, sem prejuízos para as partes envolvidas.

4.6. O prazo de vigência da ata de registro de preços será de 12 (doze meses), podendo ser prorrogado por interesse das partes até o limite de 36 (trinta e seis) meses, desde que a pesquisa de mercado demonstre que o preço atualizado se mantém vantajoso, com base no artigo art. 45, §2°, da Resolução Sesc nº 1.593/2024.

4.6.1. Prorrogada a Ata de Registro de Preço, ficam restabelecidos os termos e as condições iniciais da ata, inclusive quantitativos, nos termos do § 3º, do art. 45, da Resolução Sesc nº 1.593/2024

5. DA JUSTIFICATIVA DO MENOR PREÇO GLOBAL, LOTE ÚNICO E CARACTERÍTICA DA CONTRATAÇÃO

5.1. O fornecedor será selecionado por meio de procedimento licitatório na modalidade PREGÃO, sob a forma ELETRÔNICA, adotando o critério de julgamento de MENOR PREÇO GLOBAL

5.2. Aplica-se a modalidade de licitação por Pregão Eletrônico, com julgamento por menor preço global, visando dar celeridade e desburocratização ao procedimento licitatório, bem como sem perder a qualidade nas propostas, uma vez que a

competitividade nesta modalidade de licitação possui como uma grande característica, a ampla concorrência.

5.3. A contratação por preço global ensejará o planejamento e a racionalização do trabalho, a melhor gestão dos contratos, o adequado cumprimento de prazos e padrões de qualidade, além da atribuição de responsabilidade pelos serviços executados.

5.4. A contratação será feita em lote único:

5.4.1. Trata-se de uma licitação em que a natureza do objeto não permite o parcelamento nem divisões, em virtude de possível desvantagem ao SESC-AR/DF no momento da fiscalização do contrato, por se tratar de um serviço comum e um item depender do outro para que o serviço seja executado.

5.4.2. O fracionamento do objeto não se mostra viável na presente contratação, em virtude das suas características e suas obrigatórias interações, que impossibilitariam a atribuição, a diferentes contratadas, eventual responsabilidade por danos ou por defeito de execução.

6. DA DOTAÇÃO ORÇAMENTÁRIA

6.1. A despesa decorrente do objeto do presente TR correrá no presente exercício.

7. DA LEGISLACAO DE REFERÊNCIA

7.1. As licitações do Sesc não estão sujeitas à Lei Federal nº 14.133/2021, mas sim aos seus regulamentos próprios, conforme decisões 907/97 de 11/12/1997 e 461/98 de 22/07/1998, do Plenário do Tribunal de Contas da União (TCU) e as determinações contidas no Acórdão nº 1.664/2004, constante na Relação nº 033/2004 – 1ª Câmara, de 13/07/2004, e Acórdão nº 457/2005, da 2ª Câmara, de 29/03/2005, ambos do TCU.

7.2. As licitações do Sesc-AR/DF seguem a Resolução nº 1.593/2024, aprovada em 02/05/2024. A norma, em vigor desde o dia 02 de maio de 2024, altera, modifica e consolida o Regulamento de Licitações e Contratos do Sesc e revoga a Resolução Sesc nº 1.570/2023. No Sesc-AR/DF, as licitações são realizadas pela Seção de Licitações.

7.3. LEI Nº 12.305, DE 2 DE AGOSTO DE 2010. DOU de 03.08.2010. Institui a Política Nacional de Resíduos Sólidos; altera a Lei nº 9.605, de 12 de fevereiro de 1998.

8. QUALIFICAÇÃO TÉCNICA

8.1. Requisitos Técnicos:

8.1.1. De acordo com Especificações Técnicas – Anexo I deste processo.

8.1.1.1. No anexo I estão especificados os requisitos mínimos e obrigatórios para todos os itens da Tabela 01 – Escopo de Fornecimento, onde a licitante deverá apresentar junto a sua proposta comercial, as seguintes informações:

8.1.1.1.1. A composição de cada item do escopo de fornecimento, contendo marca, modelo, códigos, descritivo dos códigos, unidade, quantidades do conjunto, dentre outras informações que sejam necessárias ou solicitadas pelo SESC-AR/DF, com o objetivo de se identificar claramente os produtos utilizados para o fornecimento e prestação dos serviços.

8.1.2. A comissão permanente de licitação se reserva o direito de promover diligências através de contatos com o cliente para certificar-se da exatidão das informações constantes dos atestados e/ou certificados apresentados pelas licitantes.

8.1.3. Qualquer informação inexata ou inverídica apurada pela CPL, constante dos documentos de capacitação técnica implicará na inabilitação da respectiva licitante.

8.2. **Comprovações da Especificação Técnica:**

8.2.1. A licitante deve apresentar atestado(s) de capacidade técnica, comprovando em um ou mais atestados que forneceu ou presta(ou) serviços similares ao objeto.

8.2.2. Devem ser apresentados em papel timbrado da empresa, constando nome da pessoa jurídica, endereço completo, nome completo e cargo do signatário.

8.2.3. Essa exigência visa garantir que as soluções ofertadas pela licitante sejam fornecidas diretamente ou por meio de revendedores autorizados pelo fabricante e distribuidores autorizados, assegurando a qualidade, originalidade e a continuidade do suporte técnico durante toda a vigência contratual. A carta de autorização garante que a empresa licitante possui respaldo do fabricante para fornecimento e manutenção das soluções, evitando eventuais problemas relacionados à procedência, assim como o suporte adequado.

8.2.4. Os atestados poderão ser objetos de diligência a fim de se esclarecer quaisquer dúvidas quanto ao seu conteúdo.

8.2.5. Os documentos solicitados para comprovação da qualificação técnica da

licitante deverão ser enviados juntamente com a proposta comercial e tem o objetivo degarantir seu pleno atendimento ao instrumento convocatório. O não envio destes implicará em desclassificação.

9. DA QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

9.1. Certidão Negativa de Falência expedida pelo distribuidor da sede da pessoa jurídica.

9.2. Balanço Patrimonial e Demonstrações Contábeis referentes do último exercício social, ou balanço de abertura, no caso de empresa recém-constituída, (já exigíveis e apresentados na forma de lei, registrados nos órgãos competentes) que comprovem a situação financeira da empresa (vedada a sua substituição por balancetes ou balanços provisórios). Esta situação será comprovada com base na obtenção dos seguintes índices contábeis:

I. Liquidez Geral (LG) = $\frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo não Circulante}} \geq 1$

II. Solvência Geral (SG) = $\frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo não Circulante}} \geq 1$

III. Liquidez Corrente (LC) = $\frac{\text{Ativo Circulante}}{\text{Passivo Circulante}} \geq 1$

9.3. E demais especificações descritas no Edital.

10. DAS OBRIGAÇÕES DA CONTRATANTE

10.1. Prestar todas as informações e os esclarecimentos que venham a ser solicitados pela Contratada;

10.2. Responsabilizar-se pela observância das leis, decretos, regulamentos, portarias e demais normas legais, federal, estadual e municipal, direta e/ou indiretamente, aplicáveis ao Contrato;

10.3. Responsabilizar-se pela lavratura do respectivo contrato, com base resolução 1593/2024;

10.4. Assegurar os recursos orçamentários e financeiros para custear o contrato;

10.5. Pagar a importância correspondente à aquisição ou aquisições;

10.6. Fiscalizar a execução do contrato, através de servidor especialmente designado.

10.7. Rejeitar qualquer material entregue equivocadamente ou em desacordo com as especificações mínimas exigidas neste termo de referência.

10.8. Nomear Gestor e Fiscal para acompanhar e fiscalizar a execução dos contratos;

10.9. Receber o objeto do certame prestado pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas.

10.10. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis.

11. DAS OBRIGAÇÕES DA CONTRATADA

11.1. A CONTRATADA deve cumprir todas as obrigações constantes neste Termo de Referência, em seus anexos e na sua proposta, assumindo exclusivamente seus os riscos e as despesas decorrentes do bom e do perfeito fornecimento do objeto e, ainda:

11.2. Observar as normas de qualidade determinadas por legislação própria vigente, a fim de garantir o fiel cumprimento deste instrumento;

11.3. Entregar, nos prazos previstos neste instrumento, após a solicitação, o objeto conforme descrito na Ordem de Compra ou documento formal emitido pelo CONTRATANTE;

11.4. Reparar, no prazo de 3 (três) dias, contados da notificação, sem qualquer ônus para o CONTRATANTE, o objeto deste, devolvido por não atendimento às exigências técnicas estipuladas neste instrumento;

11.5. Recolher as taxas, impostos, fretes e outras despesas oriundas do fornecimento do objeto deste Instrumento, inclusive nos casos de devolução abrangidos pela determinação anterior;

11.6. Responsabilizar-se pelos prejuízos financeiros decorrentes da falha no fornecimento do objeto;

11.7. A contratada cumprirá fielmente com as obrigações assumidas por meio deste Termo de Referência, podendo a contratante aplicar ao vencedor as penalidades cabíveis previstas em contrato, em caso de não cumprimento do estabelecido.

11.8. A inobservância ao disposto nos itens anteriores, deste item, implicará no não pagamento do valor devido ao fornecedor, até que ocorra a necessária regularização.

11.9. O descumprimento das especificações solicitadas implicará no não recebimento do objeto por parte do Sesc-AR/DF.

11.10. A Contratada deverá apresentar documento fiscal válido correspondente ao fornecimento, no momento da entrega.

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

11.12. A contratada deverá responder de forma imediata a todas as solicitações de contato do contratante, seja presencial, telefone ou e-mail.

11.13. Em nenhuma hipótese a contratada poderá alegar desconhecimento, incompreensão, dúvidas ou esquecimento de qualquer detalhe especificado neste Termo de Referência.

11.14. Demais condições, conforme Anexo II – Especificação Técnica;

12. PARTICIPAÇÃO DE CONSÓRCIOS E COOPERATIVAS:

12.1. É vedada a participação de consórcio de empresas, qualquer que seja sua forma de constituição.

12.2. Justificativa para a vedação:

12.2.1. A ausência de consórcio não trará prejuízos a competitividade do certame, a vedação visa tratar exatamente o oposto que seria o estímulo da competição entre os fornecedores do ramo;

12.2.2. Corroborando essa tese, o professor Marçal Justen Filho, no seu livro Lei de Licitações e Contratos Administrativos, leciona que:

> "Em regra, o consórcio não é favorecido ou incentivado pelo nosso Direito. Como instrumento de atuação empresarial, o consórcio pode conduzir a resultados indesejáveis. A formação de consórcios acarreta risco de dominação do mercado, através de pactos de eliminação de competição entre os empresários. No campo de licitações, a formação de consórcios poderia reduzir o universo da disputa. O Consórcio poderia retratar uma composição entre eventuais interessados, em vez de estabelecerem disputa entre si, formalizariam acordo para eliminar a competição";

12.2.3. A vedação visa também prevenir outros riscos, conforme abaixo:

12.2.3.1. Dificuldade de avaliação das propostas: em licitações que envolvem consórcios, pode ser mais difícil avaliar as propostas apresentadas, uma vez que várias empresas estão envolvidas no processo. Isso pode prejudicar a transparência e a competitividade do certame, bem como aumentar o risco de erros

ou favorecimentos;

12.2.3.2. Complexidade na execução do contrato: a execução de contratos com consórcios pode ser mais complexa e demandar maior coordenação entre as empresas envolvidas. Isso pode aumentar o risco de atrasos, conflitos e problemas na entrega do objeto contratado; e

12.2.3.3. Risco de inadimplência: a participação de consórcios pode aumentar o risco de inadimplência, uma vez que a responsabilidade pelos compromissos assumidos é dividida entre as empresas participantes. Isso pode gerar incertezas quanto à capacidade do consórcio de cumprir com as obrigações do contrato.

13. DIREITOS AUTORAIS E DE PROPRIEDADE INTELECTUAL:

13.1. Pertencem ao SESC-AR/DF o direito patrimonial e a propriedade intelectual das informações e dados que forem manipulados nos equipamentos e resultados produzidos em consequência da licitação, entendendo-se por resultados, quaisquer estudos, relatórios, descrições técnicas e documentação didática, em papel ou em mídia eletrônica;

13.2. Não será permitida a cessão, citação ou qualquer referência pública a nenhum dos trabalhos realizados com a exceção dos autorizados pelo SESC-AR/DF.

14. DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

14.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da entrega do objeto deste, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por um ou mais representantes da Contratante, especialmente designados.

14.2. O representante da Contratante deverá ter a experiência necessária para o acompanhamento e controle da entrega do produto do contrato.

14.3. A execução dos contratos deverá ser acompanhada e fiscalizada por meio de instrumentos de controle.

14.4. Durante a execução do objeto, o fiscal deverá monitorar o nível de qualidade do objeto, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

14.5. O fiscal deverá apresentar ao preposto da CONTRATADA a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da

prestação dos serviços realizados.

14.6. Em hipótese alguma, será admitido que a própria CONTRATADA materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

14.7. O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais.

14.8. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela Contratada ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual.

15. DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

15.1. O objeto deste deverá ser entregue de acordo com a necessidade do CONTRATANTE, em 30 (trinta) dias, após a emissão e comprovação de recebimento da Ordem de Compras.

15.2. O objeto deste poderá ser rejeitado, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades;

15.3. Se, durante o recebimento provisório, constatar-se que o objeto deste está em desacordo com o solicitado, fora da especificação ou incompletos, a CONTRATADA será notificada e deverá sanar as pendências em até 30 (trinta) dias corridos ficando suspenso o prazo de recebimento definitivo. A despesas referentes ao saneamento das pendências, ocorrerá às expensas da CONTRATADA.

15.4. O gestor do contrato analisará toda documentação apresentada pela fiscalização técnica e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicará as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções; e

15.5. O gestor emitirá termo circunstanciado para efeito de recebimento definitivo dos serviços de implantação, com base nos relatórios e documentação apresentados, e comunicará a CONTRATADA para que emita a Nota Fiscal ou Fatura com o valor exato dimensionado pela fiscalização com base no Instrumento de Medição de Resultado (IMR), ou instrumento substituto.

15.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato.

16. SANÇÕES ADMINISTRATIVAS

16.1. Em caso de inexecução total, parcial, ou qualquer outra inadimplência, sem motivo de força maior, a empresa contratada estará sujeita, sem prejuízo da responsabilidade civil e criminal, no que couber, garantida a prévia defesa, às penalidades previstas na legislação aplicável, para as seguintes hipóteses:

16.1.1. por atraso injustificado:

16.1.1.1. multa de 1% (um por cento) ao dia, até o 30º (trigésimo) dia, incidente sobre o valor correspondente a Ordem de Compra – OC, limitado esse percentual a 10%(dez por cento); e

16.1.1.2. multa de 1,5% (um vírgula cinco por cento) ao dia, a partir do 31º (trigésimo primeiro) dia de atraso, incidente sobre o valor da OC, sem prejuízo da rescisão deste a partir do 60º (sexagésimo) dia de atraso.

16.1.2. por inexecução parcial ou total:

16.1.2.1. advertência;

16.1.2.2. multa de 5% (cinco por cento) sobre o valor do Contrato; e

16.1.2.3. suspensão do direito de licitar ou contratar com a contratante, por um prazo não superior a 3 (três) anos, inclusive quando recusar-se a assinar o Contrato.

16.2. Impedimento do direito de Licitar com abrangencia Nacional, por prazo minimo de 4(quatro) e máximo de 6(seis) anos:

16.2.1. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a exeecução do contrato;

16.2.2. Fraudar a licitação ou praticar ato fraudulento na execução do contrato;

16.2.3. Comportar-se de modo indoneo ou cometer fraude de qualquer natureza;

16.2.4. Praticar atos ilicítos com vistas a frustar os objetivos da licitação.

16.3. Quando não pagos em dinheiro, os valores das multas eventualmente aplicadas serão deduzidos, pelo Sesc- AR/DF, do pagamento devido e, quando for o caso, cobrados judicialmente.

16.4. Quando se tratar de inexecução parcial, o valor da multa deverá ser

proporcional ao valor do produto que deixou de ser entregue.

16.5. Em caso de reincidência por atraso injustificado, será a adjudicatária penalizada nos termos da Resolução Sesc nº. 1.593/2024.

17. DA SUBCONTRATAÇÃO

17.1. O A CONTRATADA não poderá subcontratar, os serviços/fornecimentos objeto deste contrato.

17.2. A subcontratação dos serviços/dos fornecimentos pela CONTRATADA, ou de parte deles, será considerada inadimplemento contratual e permitirá:

17.2.1. Solicitar a imediata paralisação dos serviços/fornecimentos ou de parte deles;

17.2.2. Exigir a desmobilização imediata da subcontratada;

17.2.3. Aplicar as penalidades previstas no contrato;

17.2.4. Solicitar a rescisão do contrato.

18. DOS CRITÉRIOS AMBIENTAIS, SOCIAIS E CULTURAIS ADOTADOS

18.1. A CONTRATADA deve comprometer-se a adotar políticas empresariais de eliminação de desperdícios e redução de consumo de bens consequentes da exploração de riquezas naturais, tais como: água tratada, consumo de energia elétrica; a promoção do adequado tratamento de rejeitos como papel, de instrumentos, de equipamentos elétrico-eletrônicos obsoletos, oportunizando suas reciclagens; além de promover ações de responsabilidade social e cidadania;

18.2. A CONTRATADA deverá acondicionar os materiais entregues em embalagem individual adequada, com o menor volume possível e que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

18.3. A CONTRATADA deverá respeitar as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos.

18.4. Em atendimento as diretrizes da Lei 12.305, de 02/08/2010, que institui a política Nacional de Resíduos Sólidos, será exigido que a CONTRATADA se responsabilize pelo mecanismo de logística reversa. Este consiste em um conjunto de ações, procedimentos e meios para viabilizar a restituição dos resíduos para a CONTRATADA. Neste sentido, um dos objetivos do projeto é a redução, reutilização, reciclagem, tratamento dos resíduos sólidos e disposição final

ambientalmente adequada dos rejeitos produzidos pelo processo de impressão, em especial dos cartuchos de toner utilizados.

19. DO PAGAMENTO

19.1. O pagamento pelo fornecimento do objeto deste instrumento, será efetuado diretamente na conta bancária indicada pela CONTRATADA, no prazo de até 30 (trinta) dias após a entrega com nota fiscal devidamente atestada pelo CONTRATANTE.

19.1.1. O pagamento ocorrerá em parcela única.

19.2. Deverá estar especificada a quantidade fornecida, com o respectivo valor unitário e total e a comprovação de recebimento pelo CONTRATANTE.

19.3. Nos valores apresentados na nota fiscal, já estarão inclusos taxas, fretes, impostos, seguros e outros encargos legais decorrentes do cumprimento do objeto.

19.4. O CONTRATANTE não efetuará pagamento por meio de boleto bancário.

19.5. A nota fiscal deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais.

19.6. Conforme preceitua a jurisprudência pacífica do Tribunal de Contas da União – TCU, mesmo que não haja a regularização fiscal da empresa contratada, não haverá retenção de pagamento de produto já fornecido.

19.7. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação qualquer obrigação que lhe for imposta, em virtude de penalidade ou inadimplência, sendo que o atraso decorrente do inadimplemento de obrigações da CONTRATADA, não gerará direito ao pleito de reajustamento de preços.

19.8. Caso o faturamento apresente alguma incorreção, a nota fiscal será devolvida para a devida correção e o prazo de pagamento alterado sem quaisquer ônus para o CONTRATANTE.

19.9. As demais regras para o pagamento dos serviços estão estabelecidas no Edital.

20. DO REAJUSTE

20.1. Os valores registrados e contratados não sofrerão reajuste durante o 1º (primeiro) ano de vigência, qualquer que seja a justificativa, salvo por disposições legais.

20.2. Havendo interesse na renovação, o valor contratado poderá ser reajustado pela variação do INPC/IBGE, considerando, para apuração do índice de reajuste, os 12 (doze) meses anteriores ao penúltimo mês de vencimento da vigência contratual em vigor, mediante comunicação por escrito com, pelos menos, 30 (trinta) dias de antecedência ou acordo entre as partes.

21. Requisitos da Proposta

21.1. Para fins de registro e controle das propostas e lances durante a fase pública do pregão, o objeto licitado foi configurado em quantidades como ITEM, com base no preço unitário utilizado na composição do preço de referência. Esses preços unitários de referência representam o valor MÁXIMO que o Sesc-AR/DF está disposto a pagar pelo equipamento, conforme pesquisa de mercado prévia realizada junto às empresas.

21.2. Deverá ser comprovado pela LICITANTE, na fase aceitação como anexo da proposta de preço, por meio de documento expedido pelo fabricante, que os equipamentos descritos na proposta de preços continuam sendo fabricados;

21.3. A LICITANTE deverá apresentar, juntamente com sua Proposta de Preços, carta ou declaração dos fabricantes ou distribuidores oficiais dos equipamentos comprovando ser revendedora autorizada dos produtos ofertados.

21.3.1. As cartas podem ser emitidas por distribuidor oficial.

21.4. Tal solicitação justifica-se por:

21.5. Garantia e Suporte Técnico: Revendedores autorizados têm um relacionamento formal com o fabricante, o que pode facilitar a obtenção de suporte técnico e garantias mais eficientes. Isso é importante para garantir a manutenção adequada dos equipamentos ao longo do tempo.

21.5.1. Qualidade e Conformidade: Fabricantes geralmente impõem padrões rigorosos para seus revendedores autorizados. Ao exigir que os licitantes sejam revendedores autorizados, a entidade licitante pode buscar garantir que os equipamentos adquiridos atendam aos padrões de qualidade e conformidade estabelecidos pelo fabricante.

21.6. Acesso a Atualizações e Peças de Reposição: Revendedores autorizados têm mais chances de ter acesso a atualizações de software, firmware e peças de reposição originais. Isso é crucial para manter os equipamentos funcionando de maneira eficiente e segura ao longo do tempo.

21.7. Treinamento Especializado: Revendedores autorizados muitas vezes recebem treinamento especializado diretamente do fabricante. Isso significa que estão mais bem preparados para instalar, configurar e manter os equipamentos de acordo com as especificações do fabricante.

21.8. Evitar Falsificações e Produtos Ilegítimos: Exigir que os licitantes sejam revendedores autorizados pode ajudar a evitar a aquisição de equipamentos falsificados, adulterados ou de procedência duvidosa. Isso contribui para a integridade e segurança das operações da entidade licitante.

21.9. Atualização Tecnológica: Revendedores autorizados geralmente estão mais atualizados em relação às últimas tecnologias e inovações dos produtos do fabricante. Isso pode ser crucial, especialmente em setores onde a tecnologia está em constante evolução.

22. GARANTIA DE PROPOSTA

22.1. A Garantia de Proposta corresponde ao valor exigido do licitante no momento da apresentação da proposta, sendo limitada a 1% (um por cento) do valor estimado do contrato.

22.2. A garantia da proposta será devolvida aos licitantes no prazo de 10 (dez) dias úteis, contado da assinatura do contrato ou a data que for declarada fracassada a Licitação.

22.3. A Garantia de Proposta poderá ser apresentada por meio de uma das seguintes modalidades:

22.3.1. Caução em dinheiro, por meio de depósito em conta específica a ser informada pelo Sesc DF;

22.3.2. Fiança bancária, emitida por instituição financeira autorizada pelo Banco Central do Brasil;

22.3.3. Seguro-garantia, emitido por empresa devidamente registrada na Superintendência de Seguros Privados (SUSEP).

22.4. O comprovante da Garantia de Proposta deverá ser apresentado junto à documentação de habilitação da empresa.

22.5. A Garantia de Proposta poderá ser retida pelo Sesc DF, sem direito à devolução, nos seguintes casos:

22.5.1. Se o licitante vencedor recusar-se a assinar o contrato dentro do prazo estabelecido;

22.5.2. Se houver descumprimento de quaisquer obrigações assumidas na proposta apresentada;

22.5.3. Se for constatada fraude ou má-fé na participação do certame.

22.6. Penalidades por Descumprimento

22.6.1. O não cumprimento da exigência de apresentação da Garantia de Proposta resultará na inabilitação automática do licitante, sem prejuízo de outras penalidades previstas no edital.

22.6.2. Caso ocorra a retenção da Garantia de Proposta por descumprimento das condições estabelecidas, a empresa poderá ser penalizada conforme a legislação vigente, incluindo impedimento de participação em novos certames por período determinado.

23. DA GARANTIA CONTRATUAL

23.1. A CONTRATADA deverá apresentar ao SESC, no prazo máximo de 10 (dez) dias, contados da data de entrega da via assinada do contrato, comprovante de prestação de garantia, que cubra todo o prazo contratual acrescido de 90 (noventa) dias, correspondente ao percentual de 5% (cinco por cento) do valor atualizado do contrato, podendo optar por caução em dinheiro, fiança bancária ou seguro garantia;

23.2. A garantia mencionada neste item deverá ser renovada a cada prorrogação do Contrato, se houver, devendo seu valor ser atualizado nas mesmas condições contratuais.

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

a) prejuízos advindos do não cumprimento do objeto do Contrato;

b) prejuízos diretos causados ao Sesc-AR/DF, decorrentes de culpa ou dolo durante a execução do Contrato;

c) obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela licitante vencedora.

d) serviços que tenham que ser contratados com terceiros para corrigir falhas dos serviços executados pela licitante vencedora;

e) multas aplicadas por órgãos públicos;

f) débitos porventura existentes para com o INSS e FGTS; e

g) danos contra terceiros não cobertos pelo seguro específico.

23.4. A garantia do contrato terá vigência durante todo o prazo de execução da obra ou serviços, devendo se estender até o prazo de 3 (três) meses, após término da vigência contratual.

23.5. Se o valor da garantia for utilizado total ou parcialmente, em pagamento de qualquer obrigação, a empresa contratada deverá proceder à respectiva reposição no prazo de 3 (três) dias úteis, contada da data em que for notificada pelo Sesc-AR/DF.

23.6. Após o cumprimento fiel e integral do Contrato, a garantia prestada será liberada ou restituída à adjudicatária, no prazo de até 10 (dez) dias úteis, após formalizada sua solicitação.

23.7. Ao término da vigência do Contrato, a garantia retida somente será liberada ante a comprovação de que a empresa pagou todas as verbas rescisórias trabalhistas, se for o caso, decorrentes da Contratação. Caso esse pagamento não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas trabalhistas diretamente pelo Sesc-AR/DF.

24. DA VIGÊNCIA CONTRATUAL

24.1. A vigência será de 12 (doze) meses, prorrogada obrigatória e automaticamente por períodos iguais e sucessivos, pelo período mínimo de 36 (trinta e seis) meses e máximo de 60 (sessenta) meses.

24.2. A vigência poderá ser prorrogada de acordo com o interesse das partes, até o limite previsto no Regulamento de Licitações e Contratos do Sesc e do Senac, conforme Resolução SESC nº 1593/2024, de 02/05/2024.

25. ENTREGA.

25.1. Local de entrega:

Unidades	Endereço:
Sesc SEDE	Setor de Indústria e Abastecimento – SIA, Trecho 02, Quadra 02, Lotes 1.130. CEP: 71.200-020

26. DAS CARACTERÍSTICAS DA CONTRATAÇÃO

26.1. O fornecedor será selecionado por meio de procedimento licitatório na

modalidade PREGÃO, sob a forma ELETRÔNICA, adotando o critério de julgamento de MENOR PREÇO Global.

27. Do Preço de Referência

27.1. O valor de referência para a contratação será sigiloso conforme termos do parágrafo único do art. 3º da Resolução nº 1.593/2024.

27.1.1. Com o preço referencial de forma oculta é possível propiciar propostas mais econômicas e competitivas no certame.

28. DA JUSTIFICATIVA DO MENOR PREÇO GLOBAL

28.1. Aplica-se a modalidade de licitação por Pregão Eletrônico, com julgamento por menor preço global, visando dar celeridade e desburocratização ao procedimento licitatório, bem como sem perder a qualidade nas propostas, uma vez que a competitividade nesta modalidade de licitação possui como uma grande característica, a ampla concorrência.

28.2. A contratação por preço global ensejará o planejamento e a racionalização do trabalho, a melhor gestão dos contratos, o adequado cumprimento de prazos e padrões de qualidade, além da atribuição de responsabilidade pelos serviços executados.

29. SUBCONTRATAÇÃO:

29.1. NÃO SERA PERMITIDA a subcontratação do objeto licitatório, inclusive do atendimento técnico.

29.2. O A CONTRATADA não poderá subcontratar, no todo ou em parte, os serviços/fornecimentos objeto deste contrato.

29.3. A subcontratação dos serviços/dos fornecimentos pela CONTRATADA, ou de parte deles, será considerada inadimplemento contratual e permitirá:

29.4. Solicitar a imediata paralisação dos serviços/fornecimentos ou de parte deles;

29.5. Exigir a desmobilização imediata da subcontratada;

29.6. Aplicar as penalidades previstas no contrato;

29.7. Solicitar a rescisão do contrato.

30. PARTICIPAÇÃO DE CONSÓRCIOS E COOPERATIVAS:

30.1. É vedada a participação de consórcio de empresas, qualquer que seja sua forma de constituição.

30.2. Justificativa para a vedação:

30.2.1. A ausência de consórcio não trará prejuízos a competitividade do certame, a vedação visa tratar exatamente o oposto que seria o estímulo da competição entre os fornecedores do ramo;

30.2.2. Corroborando essa tese, o professor Marçal Justen Filho, no seu livro Lei de Licitações e Contratos Administrativos, leciona que:

> "Em regra, o consórcio não é favorecido ou incentivado pelo nosso Direito. Como instrumento de atuação empresarial, o consórcio pode conduzir a resultados indesejáveis. A formação de consórcios acarreta risco de dominação do mercado, através de pactos de eliminação de competição entre os empresários. No campo de licitações, a formação de consórcios poderia reduzir o universo da disputa. O Consórcio poderia retratar uma composição entre eventuais interessados, em vez de estabelecerem disputa entre si, formalizariam acordo para eliminar a competição";

30.2.3. A vedação visa também prevenir outros riscos, conforme abaixo:

30.2.3.1. Dificuldade de avaliação das propostas: em licitações que envolvem consórcios, pode ser mais difícil avaliar as propostas apresentadas, uma vez que várias empresas estão envolvidas no processo. Isso pode prejudicar a transparência e a competitividade do certame, bem como aumentar o risco de erros ou favorecimentos;

30.2.3.2. Complexidade na execução do contrato: a execução de contratos com consórcios pode ser mais complexa e demandar maior coordenação entre as empresas envolvidas. Isso pode aumentar o risco de atrasos, conflitos e problemas na entrega do objeto contratado;

30.2.3.3. Risco de inadimplência: a participação de consórcios pode aumentar o risco de inadimplência, uma vez que a responsabilidade pelos compromissos assumidos é dividida entre as empresas participantes. Isso pode gerar incertezas quanto à capacidade do consórcio de cumprir com as obrigações do contrato.

31. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

31.1. As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no Edital.

31.2. Os critérios de qualificação econômica a serem atendidos pelos Licitantes estão previstos no Edital.

31.3. Os critérios para a Qualificação Técnica devem ser atendidos pelas Licitantes, por meio dos seguintes documentos:

31.3.1. O(s) licitante(s) deverá(ão) apresentar atestado de Capacidade Técnica fornecido por pessoa jurídica de direito público ou privado, comprovando a experiência da licitante em relação ao objeto deste, incluindo a prestação de serviços de instalação, suporte técnico e operação assistida.

31.3.2. No(s) atestado(s) devem estar explícitos: a identificação da pessoa jurídica que está fornecendo o atestado, o responsável pelo setor encarregado do objeto em questão e a especificação dos serviços executados ou em execução. Poderá ser necessário diligenciar a pessoa jurídica indicada no Atestado de Capacidade Técnica, visando obter informações sobre o serviço prestado;

31.3.3. Os atestados deverão ser válidos e conter a descrição pormenorizada do serviço prestado incluindo equipamentos e sistemas, bem como informações sobre o número do contrato vinculado, a sua vigência e a data de início dos serviços prestados; e

31.3.4. Somente poderão ser aceitos atestados de capacidade técnica expedidos após a conclusão do contrato ou se decorrido, no mínimo, um ano do início de sua execução, exceto se houver sido firmado para ser prestado em prazo inferior.

31.3.5. Será permitido o somatório de atestados ou declarações para fins de comprovação da qualificação técnica da licitante.

31.3.6. É vedada participação de pessoas jurídicas que tenham funcionários do Sesc-AR/DF e dirigentes em seus quadros societários.

32. DA COMUNICAÇÃO

32.1. GARANTIA ON-SITE.

32.2. A CONTRATADA deverá manter um responsável pelo projeto de implantação da solução, capaz de resolver questões técnicas e administrativas, o qual deverá ser o ponto de contato com a equipe do Sesc-AR/DF.

32.3. O mecanismo formal de comunicação entre o Sesc-AR/DF e a contratada

se dará mediante emissão de correspondência com os respectivos anexos que venham a ser necessários para o eficaz entendimento da comunicação e sua formalização.

32.4. A CONTRATADA disponibilizará para abertura de chamados e-mail, número 0800 ou site as suas expensas para solicitação de substituição de peças ou equipamentos.

32.5. A abertura de chamados técnicos deverá ser realizada por telefone (0800 ou de custo local em Brasília), ou por sistema WEB/e-mail.

32.6. Os chamados técnicos terão origem em decorrência de qualquer problema detectado pela equipe do Sesc-AR/DF no tocante ao pleno estado de funcionamento do(s) equipamento(s), inclusive problemas relacionados com instalação, configuração e atualização.

32.7. Na abertura do chamado técnico junto à Central de Atendimento serão fornecidas, no mínimo, as seguintes informações:

32.8. marca, modelo e número de série do(s) equipamento(s);

32.9. problema observado;

32.10. nome, telefone, e-mail do profissional do Sesc-AR/DF responsável pela solicitação;

32.11. nível de severidade do chamado.

32.12. O fornecedor informará o número do chamado técnico no ato da comunicação efetuada pela equipe do Sesc-AR/DF, o qual servirá de referência para acompanhamento do chamado, inclusive após o encerramento do chamado.

32.13. O fornecedor terá o prazo de 02 (duas) horas para início do atendimento do chamado e 08 horas para sua resolução.

33. DIREITOS AUTORAIS E DE PROPRIEDADE INTELECTUAL:

33.1. Pertencem ao SESC-AR/DF o direito patrimonial e a propriedade intelectual das informações e dados que forem manipulados nos equipamentos e resultados produzidos em consequência da licitação, entendendo-se por resultados, quaisquer estudos, relatórios, descrições técnicas e documentação didática, em papel ou em mídia eletrônica;

33.2. Não será permitida a cessão, citação ou qualquer referência pública a nenhum dos trabalhos realizados com a exceção dos autorizados pelo SESC-AR/DF.

34. DA SEGURANÇA DA INFORMAÇÃO

34.1. A CONTRATADA e seus profissionais envolvidos no projeto deverão seguir os seguintes procedimentos e premissas de segurança envolvidos na prestação dos serviços:

34.1.1. Manter sigilo sobre todo e qualquer assunto de interesse do Sesc-AR/DF ou de terceiros de que tomar conhecimento em razão da execução dos serviços contratados, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa;

34.1.2. Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do Sesc-AR/DF;

34.1.3. Não veicular publicidade acerca do contrato, salvo se houver prévia autorização do Sesc- AR/DF;

34.1.4. Manter sigilo de todas as informações a que tiveram acesso inclusive após o término da vigência contratual ou eventual rescisão; e

34.1.5. Assinar Termo de Termo de Confidencialidade e Sigilo.

34.1.6. na utilização de aplicações como VoIP, streaming de dados e Videoconferência, que requerem uma alta disponibilidade e baixa latência.

34.1.7. O modelo do Termo de Confidencialidade e Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes no Sesc-AR/DF, a ser assinado pelo representante legal da CONTRATADA, se encontra no Apêndice II.

34.1.8. O modelo do Termo de Confidencialidade e Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes no Sesc-AR/DF, a ser assinado pelo representante legal da CONTRATADA, se encontra no Apêndice II.

34.1.9. O modelo do Termo de Ciência da declaração de manutenção de sigilo e das normas de segurança vigentes no Sesc-AR/DF, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação se encontra no Apêndice III.

35. CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

35.1. A CONTRATADA deverá atender os critérios de sustentabilidade e observar

as regras ambientais para atividades potencialmente poluidoras previstas na legislação pertinente.

35.2. A CONTRATADA se compromete a destinar todos os resíduos de forma ambientalmente correta, sempre priorizando materiais que sejam menos agressivos ao meio ambiente e possibilitem reutilização futura, bem como deverá dar ênfase nos princípios da redução, reutilização e reciclagem.

35.3. O desfazimento de qualquer material gerado para uso no Sesc-AR/DF deve ser de acordo com a Política Nacional de Resíduos Sólidos (Lei 12.305/2010) e manejado adequadamente até sua destinação e/ou disposição final.

35.4. Para cumprir essa obrigação legal, a empresa que irá fazer o descarte dos resíduos deverá dar prioridade à destinação final ambientalmente adequada de resíduos que inclui a reutilização, a reciclagem, a compostagem, a recuperação, o aproveitamento energético e por último a disposição final em aterros sanitários visando mitigar danos adversos ao meio ambiente e os riscos à saúde pública. Caso os resíduos sejam reaproveitados fora do Sesc-AR/DF, os resíduos devem ser descaracterizados.

35.5. O material licitado não deverá conter substâncias perigosas em concentração acima da recomendada na diretiva RoCHS (Restriciton of Certain Hazardous Substances), tais como mercúrio (Hg), CHUMBO (Pb), dentre outros.

35.6. Toda coleta de resíduos deve ser acompanhada de Manifesto de Transporte de Resíduos (MTR) e Certificado de Destinação.

Brasília 23/04/2025

_____Silvio Ricardo Lira _____

Gerente Adjunto de Tecnologia

DOCUMENTOS ANEXOS

Seguem anexos a este Termo de Referência os seguintes documentos.

APÊNDICE I – Especificações Técnicas

APÊNDICE II– Modelo do Termo de Confidencialidade e Sigilo

APÊNDICE III – Modelode Termo de Ciencia

APÊNDICE IV – Modelo de Proposta de Preço; e

BRASÍLIA, ___ de _____ de 2025.

Edital elaborado por:

Nome	**Cargo**	**Matrícula**
Silvio Ricardo Lira da Conceição	Gerente Adjunto de Área	6888
Unidade Demandante: Gerência de Tecnologia - GETEC		

Informações: Gestor, Fiscal e Substituto do Contrato

Nome	**Cargo**	**Matrícula**
Paulo Henrique Campos Castanheira	Gestor Contrato	6600
Ricardo Bittencourt	Fiscal de Contrato	2630
Silvio Ricardo Lira da Conceição	Fiscal Substituto	6888

APÊNDICE I AO TERMO DE REFERÊNCIA

ESPECIFICAÇÕES TÉCNICAS

1. Detalhamento do Objeto

1.1. Especificação Técnica dos Itens do Objeto:

1.1.1. Solução de proteção acesso Web contra ameaças digitais

1.1.1.1. A solução de proxy em nuvem, deve oferecer controles de proteção de dados e de ameaças com visibilidade e controle granular das atividades em sites web, aplicações saas e iaas.

1.1.1.2. Deverá ser capaz de processar tráfego Web (HTTP/HTTPS) nas portas 80, 443 e em portas customizadas, a exemplo: 8443, 8080, 8081.

1.1.1.3. Não serão aceitas soluções que necessitem inserir componentes on-premises para redirecionamento do tráfego ou mesmo que tratamento local parcial.

1.1.2. A solução deverá estar licenciada e suportar os seguintes métodos para encaminhamento do tráfego para a solução de Proxy em nuvem:

1.1.2.1. Integração com o NGFW via túnel IPSEC;

1.1.2.2. Integração com o NGFW via túnel GRE;

1.1.2.3. Proxy Explícito em nuvem;

1.1.2.4. Cliente nativo do próprio fabricante;

1.1.2.5. Proxy Reverso em nuvem para proteger aplicações SaaS;

1.1.3. A solução deverá permitir granularidade para construção de políticas de acesso a sites web, aplicações SaaS e IaaS, englobando as seguintes condições:

1.1.3.1. Identificação do usuário e grupo;

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

1.1.3.3. Categoria da aplicação SaaS;

1.1.3.4. Marcação de uma aplicação;

1.1.3.5. Nível de risco da aplicação SaaS;

1.1.3.6. Geolocalização do usuário;

1.1.3.7. Geolocalização do recurso remoto (URL/SaaS);

1.1.3.8. Controle granular de atividades (upload, post, edit, share, view, download, send).

1.1.3.9. Risco do usuário

1.1.4. A solução de proxy em nuvem deverá prover:

1.1.4.1. Descoberta, visibilidade e controle do tráfego Shadow IT para o tráfego Saas, IaaS e Web;

1.1.4.2. Inspeção de túneis criptografados baseados em TLS versões 1.2 e 1.3.

1.1.4.3. Base contendo mais de 120 categorias de URL e serviço de classificação dinâmico de URLs;

1.1.4.4. Customização de categorias para filtragem web, incluindo listas de bloqueio e de permissão;

1.1.4.5. Identificar aplicações SaaS corporativas e pessoais, com associação da instância para cada uma delas, através de uma base contendo mais de 80.000 aplicações SaaS.

1.1.4.6. Visibilidade e controle em tempo real de acesso a URLs, por meio de classificação baseado em categorias;

1.1.4.7. Prevenção contra vazamento de dados em aplicações SaaS corporativas, aplicações saas terceiras (ShadowIT), sites web e IaaS;

1.1.4.8. Prevenção contra acesso a sites maliciosos;

1.1.4.9. Prevenção contra download de artefatos maliciosos;

1.1.4.10. Prevenir a comunicação de aplicações cliente instaladas na estação de trabalho;

1.1.4.11. Prevenção contra-ataques via web, bloqueando tentativas de exploração remota da estação de trabalho;

1.1.4.12. Identificar credenciais expostas em vazamentos disponibilizados na internet;

1.1.4.13. Proteger contra tráfego de aplicações não autorizadas instaladas no desktop;

1.1.5. O fabricante da solução deverá disponibilizar cliente nativo, garantindo os seguintes requisitos mínimos:

1.1.5.1. O cliente nativo do fabricante deverá ser responsável diretamente por identificar o datacenter com melhor disponibilidade para conectividade, encaminhando o tráfego para processamento na estrutura do fabricante.

1.1.5.2. Suporte amplo a plataformas de sistemas operacionais, incluindo Microsoft Windows, MacOS, Linux Ubuntu, iOS, Chromebook e Android.

1.1.5.3. Deverá possibilitar a checagem de conformidade com base em parâmetros locais, levando em consideração:

1.1.5.3.1. Processo em execução;

1.1.5.3.2. Chave registro;

1.1.5.3.3. Bitlocker habilitado;

1.1.5.3.4. Domínio do Active Directory;

1.1.5.3.5. Certificado;

1.1.5.4. Deverá possuir arquitetura leve e com encaminhamento do tráfego para análise em nuvem, não devendo realizar nenhum tipo de processamento local, como política de acesso web, análise de malware, vazamento de dados e até mesmo análise comportamental do usuário.

1.1.5.5. As exceções relacionadas ao tráfego que não deverão ser redirecionadas para a estrutura do fabricante em questão para processamento, devem ser aplicadas localmente. Apesar da aplicação local das exceções, a solução deverá permitir o envio do log de acesso ao console central.

1.1.5.6. Deverá apresentar métodos para resolução de eventuais problemas, como a capacidade de realizar testes de banda e captura de pacotes para eventuais diagnósticos de problemas.

1.1.5.7. Deverá apresentar comunicação segura através da troca de certificados, baseada no protocolo TLS, sem que haja necessidade de inserir interface túnel para comunicação com o datacenter do fabricante;

1.1.5.8. Através de testes contínuos, o cliente deverá identificar a estrutura de datacenter do fabricante com melhor disponibilidade/menor latência para conectividade, garantindo melhor experiência ao usuário;

1.1.6. A solução de Proxy deverá atender aos seguintes casos de uso, voltados a filtragem de url's:

1.1.6.1. Caso de Uso: A solução deverá prevenir o acesso a URLs associadas as categorias de Pornografia, Drogas, Atividades Criminais e Apostas.

1.1.6.2. Controle de acesso a categorias que impõem risco de segurança aos usuários - Caso de Uso: A solução deverá prevenir o acesso a URLs associadas às categorias de Botnets, DGA, Command Control, Sites Maliciosos e Phishing.

1.1.6.3. Controle de acesso a categorias não categorizadas pelo fabricante - Caso de Uso: A solução deverá prevenir o acesso a URLs não conhecidas pela base de inteligência do fabricante.

1.1.6.4. Permitir a criação de categorias customizadas baseadas em listas contendo regex ou domínios - Caso de Uso: A solução deverá permitir o acesso em caráter de exceção a uma URL ou Domínio associado a uma categoria bloqueada.

1.1.6.5. Controle de acesso - Caso de Uso: A solução deverá empregar controles para bloqueios de ações em aplicações SaaS, como print, delete, rename, upload, download, post, form-post, dentre outras.

1.1.6.6. Caso de Uso: A solução deverá permitir a conexão direta para categorias que incluem sites de Bancos e serviços financeiros.

1.1.6.7. Bloqueio de propagandas - Caso de uso: a solução deverá permitir o bloqueio de propaganda através de categorias específicas.

1.1.6.8. Categorização dinâmica - Caso de uso: A solução deverá utilizar análise textual do conteúdo de uma página e dinamicamente determinar a categoria para a URL.

1.1.6.9. Bloqueio de conteúdo explícito em páginas de busca - Caso de Uso: A solução deverá possibilitar o bloqueio de imagens pornográficas e outros conteúdos indesejados em ferramentas de busca como Google, Yahoo e Bing.

1.1.6.10. Controle de Upload/Download baseado em risco da aplicação - Caso de Uso: A solução deverá bloquear as ações de upload e download para aplicações SaaS de alto risco;

1.1.6.11. Arquivo criptografado - Caso de Uso: A solução deverá possibilitar a identificação de arquivos protegidos por senha e prover o bloqueio da ação de download.

1.1.6.12. Domain Fronting - Caso de Uso: A solução deverá identificar domínios utilizados por autores maliciosos que escondem a localização atual de um servidor C2 (Command and Control).

1.1.6.13. Shadow IT - Caso de Uso: A solução deverá prover painel específico identificando todas as aplicações descobertas e catalogadas pela solução, contendo o nome, risco e categoria da aplicação.

1.1.6.14. Caso de Uso: através de relatórios específicos, a solução deverá apresentar, de acordo com a aplicação desejada, usuários internos que fizeram uso da aplicação, apresentando volume de dados trafegados, bem como a questão de incidentes relacionados a malware e vazamento de dados.

1.1.6.15. Caso de Uso: A solução deverá permitir a atribuição de uma marcação pré-disponível na solução a fim de identificar, por exemplo, aplicações corporativas.

1.1.6.16. Caso de Uso: A solução deverá permitir a atribuição de marcação customizada, indicando uma aplicação e até mesmo um grupo de aplicações. Tais marcações poderão ser utilizadas na construção de políticas de acesso.

1.1.6.17. Caso de Uso: A solução deverá apresentar as atividades suportadas para cada aplicação, bem como a instância da aplicação identificada através da análise do tráfego.

1.1.6.18. Caso de Uso: através da análise do tráfego encaminhado a solução, deverá estabelecer uma linha base de risco para as aplicações SaaS acessadas, sem a necessidade de upload de logs de fontes terceiras.

1.1.6.19. Caso de uso: A solução deverá identificar instâncias nas aplicações: Google Mail, Google Drive, Microsoft Onedrive for Business,

Microsoft Sharepoint for Business, Microsoft Teams, Microsoft Outlook, Microsoft Live Suite, Okta, Amazon S3, Amazon EC2, Github, Dropbox, ChatGPT, Atlassian Confluence e Jira, Google Calendar, Microsoft Power BI, Service Now, Slack, Microsoft Azure, Amazon IAM.

1.1.6.20. Caso de Uso: A solução, por meio da descoberta de aplicações shadow it, deverá empregar base de dados contendo o registro de aplicações SaaS, garantindo análise profunda de tais aplicações, bem como a identificação do risco ao acessar tal aplicação, permitindo inclusive a criação de bloqueios baseada em aplicações através do risco.

1.1.6.21. Aplicações SaaS/IaaS - Caso de uso: A solução deverá identificar de maneira nativa a aplicação Youtube e também o canal do SESC-DF, permitindo acesso apenas ao canal informado, bloqueando os demais vídeos, tal recurso não deverá empregar o uso de listas customizadas ou integração com API v3 do Youtube.

1.1.6.22. Caso de uso: A solução deverá garantir, permitindo através de marcação, identificar a instância corporativa do Github e diferenciar de instâncias terceiras.

1.1.6.23. Caso de uso: A solução deverá garantir controle de acesso aos comandos realizados com destino a amazon ec2 e s3 via aws cli, garantindo incluso aplicar controles contra vazamento de dados.

1.1.6.24. Caso de uso: A solução deverá garantir controle de acesso ao microsoft azure via powershell cli.

1.1.6.25. Caso de uso: A solução deverá restringir o recebimento e envio de arquivos do tipo foto, áudio e arquivos no Whatsapp Web;

1.1.6.26. Caso de Uso: A solução deverá permitir o upload/download de arquivos com destino a instância do Microsoft Office 365 do SESC-DF e prevenção de upload e demais aplicações SaaS de Webmail e Cloud Storage.

1.1.6.27. Caso de Uso – Office 365: Deve permitir as ações de upload e download com direção a instância do SESC-DF no Microsoft Office 365 One Drive.

1.1.6.28. Caso de Uso – SaaS Cloud Storage: Deve bloquear a ação de upload e download para a categoria Cloud Storage

1.1.6.29. Caso de Uso – Webmail: Deve bloquear a ação de upload para a categoria Webmail.

1.1.6.30. Caso de Uso: Caso a aplicação não seja catalogada, a solução deve possibilitar a criação de um conector customizado a fim de identificar as ações customizadas para posterior bloqueio na plataforma.

1.1.6.31. Malware - Caso de Uso: A solução deve realizar a análise de downloads realizados a partir de sites web e aplicações SaaS e ao identificar um artefato malicioso, deverá prevenir a ação de download.

1.1.6.32. Caso de Uso: deve identificar artefatos maliciosos hospedados em categorias Cloud Storage e Webmail para ação Download

1.1.6.33. Caso de Uso: Deve ser capaz de prevenir o download de arquivos executáveis.

1.1.6.34. Controle de acesso a partir de dispositivos não gerenciados - Caso de Uso: Ao falhar na validação de conformidade, a estação de trabalho será considerada "não gerenciada" e deverá ter o acesso restrito a aplicações SaaS corporativas.

1.1.6.35. Vazamento de dados - A solução deverá inspecionar todo o canal criptografado, inclusive de aplicações da Microsoft, garantindo visibilidade e controle contra vazamento de dados, em especial, em mensagens diretas entre usuários no Microsoft Teams, garantindo o bloqueio em tempo real.

1.1.6.36. Inspeção TLS - A solução deverá permitir a configuração de quais categorias de URL e domínios que devam ter a inspeção do túnel TLS desativada.

1.1.6.37. A solução deverá possibilitar o uso de certificado emitido pela CA do SESC-DF.

1.1.7. A solução deverá permitir a configuração de quais aplicações SaaS que devam ter a inspeção do túnel TLS ativada.

1.1.8. Para aplicações Web 2.0 a solução deverá oferecer controles granulares, dentre eles:

1.1.8.1. Facebook: Prevenir o vazamento de dados na ação de POST e bloquear as ações de POST, LIKE, SHARE e UPLOAD;

1.1.8.2. Youtube: bloquear as ações de DELETE, LIKE, SHARE, POST e VIEW;

1.1.8.3. Twitter: Prevenir o vazamento de dados nas ações POST e UPLOAD e ser capaz de bloquear as ações de POST, FOLLOW e DELETE;

1.1.8.4. Pastebin: Prevenir o vazamento de dados via ação POST e controlar ações de POST, DELETE e CREATE.

1.1.9. A solução deverá possibilitar a liberação de um período de hora por dia para acesso a Youtube e Mídias Sociais.

1.1.10. A solução deverá permitir, de maneira nativa, a criação de regras para permitir o acesso à plataforma do Office 365 Corporativo e negar o acesso às instâncias pessoais da Microsoft Live Suite(Exemplo: Hotmail, OneDrive Live, Outlook).

1.1.11. A solução deverá permitir, de maneira nativa, a criação de regras para permitir controles menos retritivos a instância do Github bloquear ações como Post, Share, Create, Login e Upload para instâncias terceiras

1.1.12. A solução deverá permitir a identificação da instância corporativa da instância da Amazon AWS e Microsoft Azure, garantindo controles específicos como Shutdown, Reboot, Download, View, Publish e Upload.

1.1.13. A solução deverá permitir a identificação de instâncias corporativas e terceiras para as aplicações do Microsoft Office 365, garantindo ainda a aplicação de políticas de acesso granular as aplicações OneDrive for Business, Sharepoint, Word Online, Outlook, Teams, PowerBI, Yammer, Sway, Planner e Painel administrativo do Office 365.

1.1.14. A solução deverá permitir a identificação de instâncias corporativa e terceira para as aplicações do Google Workspace, garantindo a aplicação de políticas granulares para Google Chat/Hangout, Google Drive, Google Mail e Google Calendar.

1.1.15. Deverá proteger o acesso do usuário aos dados corporativos, controlando a exposição dos mesmos quanto a movimentação entre nuvens (Serviço SaaS Microsoft Office 365 para Serviço SaaS não sancionado);

1.1.16. A solução deverá possuir nativamente categorias relacionadas a risco de segurança, prevenindo contra:

1.1.16.1. Phishing

1.1.16.2. Domínios DGA

1.1.16.3. Botnets

1.1.16.4. Sites comprometidos

1.1.16.5. Servidores Command/Control

1.1.16.6. Distribuição de malware

1.1.16.7. Spam

1.1.16.8. Spyware

1.1.17. Ao identificar o acesso a uma URL não categorizada, registrada recentemente, sem conteúdo e domínio observado recentemente pela base de urls da solução, a mesma deverá empregar o recurso de isolamento de browser (RBI).

1.1.18. O recurso de isolamento, deverá permitir a customização das ações permitidas na página confinada, permitindo o bloqueio de ações como Cópia, Cola, pop-up, upload de arquivos, download de arquivos e impressão.

1.1.19. Ao aplicar o recurso de isolamento, deve ser possível tornar a página "apenas leitura", não permitindo que o usuário insira dados na página isolada.

1.1.20. Deverá permitir para o usuário final a identificação de que a página está sendo isolada por meio da solução proposta.

1.1.21. A solução deverá contemplar o controle de acesso a aplicações saas corporativas a partir de computadores pessoais, sem requerer cliente nativo, apenas integrado com o iDP (Azure AD) para redirecionar a conexão para a solução proposta. Dentre as aplicações, a solução deverá prover suporte para:

1.1.21.1. Microsoft Office 365;

1.1.21.2. Amazon AWS;

1.1.21.3. Microsoft Azure;

1.1.22. A solução deverá contemplar o controle de acesso a aplicações saas corporativas a partir de computadores pessoais, garantindo, por exemplo, o bloqueio de ações como download, delete e preview no Microsoft Outlook;

1.1.23. A solução deverá contemplar o controle de acesso a aplicações saas corporativas a partir de computadores pessoais, garantindo, por exemplo, o bloqueio de edição em documentos do Word Online.

1.2. Solução de acesso remoto as aplicações posicionadas em nuvem pública e interna

1.2.1. Deverá atuar como um roteador em nuvem, garantindo baixa latência e canal seguro, para aplicações privadas hospedadas no datacenter do SESC-DF;

1.2.2. Será permitida a inclusão de um appliance físico ou virtual no Datacenter do SESC-DF, denominado conector, para a comunicação segura entre nuvem do fabricante e servidores internos.

1.2.3. A solução deverá fornecer o acesso à aplicação apenas, não ao contexto de rede.

1.2.4. Deverá permitir o redirecionamento seguro para mais de 400 (quatrocentas) aplicações internas.

1.2.5. A solução deverá prover os seguintes métodos de acesso a aplicações privadas:

1.2.5.1. Cliente nativo da solução, com suporte a Microsoft Windows, MacOS, Linux e iOS;

1.2.5.2. Portal de aplicação, com acesso granular as aplicações desejadas;

1.2.5.3. Acesso via browser, sem requerer o uso do cliente nativo;

1.2.6. Deverá ser capaz de autorizar o acesso ou não a aplicações internas baseada no perfil da máquina.

1.2.7. Deverá ser capaz de continuamente solicitar ao usuário que autentique novamente antes de ter acesso às aplicações privadas;

1.2.8. O acesso deve ser dedicado e exclusivo a aplicação designada na rede, não sendo permitido acesso irrestrito a um host ou a rede.;

1.2.9. Deverá prover acesso seguro e controlado baseado nos protocolos TCP, UDP e TCP/UDP;

1.2.10. Deverá prover acesso a aplicações baseada nas seguintes aplicações:

1.2.10.1. SSH - TCP Porta 22;

1.2.10.2. HTTP - TCP Portas 80, 443 e Customizadas;

1.2.10.3. RDP - TCP 3389 e UDP 3389;

1.2.10.4. SQL Server - TCP 1333, 1434 | UDP 1434;

1.2.10.5. SMB - TCP 445;

1.2.10.6. FTP - TCP 21.

1.2.10.7. Ingresso no domínio do SESC-DF.

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

1.2.11.1. Usuário Único;

1.2.11.2. Múltiplos Usuários;

1.2.11.3. Grupos de Usuário;

1.2.11.4. Unidade Organizacional (OU).

1.2.12. Para cada acesso, a política deverá prover múltiplas possibilidades de ações, dentre elas:

1.2.12.1. Permissão;

1.2.12.2. Bloqueio;

1.2.13. 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;

1.2.14. 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;

1.2.15. Deverá ser capaz de continuamente solicitar ao usuário que autentique novamente antes de ter acesso às aplicações privadas em um iDP externo.

1.2.15.1. A solução deverá suportar a importação de usuários a partir do Microsoft Active Directory instalado no SESC-DF.

1.2.15.2. Caso não seja suportado, deverá prover iDP para autenticação.

1.2.16. A solução deverá prover acesso a aplicações Web (HTTPS) sem a necessidade de instalação de agentes.

1.2.17. Deverá permitir o acesso diferenciado para um mesmo usuário conforme as seguintes condições:

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

1.2.19. Máquinas não conformes: A partir de uma máquina gerenciada, uma estação que não atenda aos requisitos de segurança, deve bloquear o acesso à aplicação.

1.3. Solução de segurança de acesso para resolução de nomes

1.3.1. A solução deverá suportar a resolução de nomes através dos métodos:

1.3.1.1. Cliente nativo;

1.3.1.2. Túnel IPSEC;

1.3.1.3. Túnel GRE;

1.3.2. A solução deverá prover monitoramento passivo das resoluções de DNS realizadas pelos clientes, identificando domínios categorizados como:

1.3.2.1. Command Control;

1.3.2.2. Phishing;

1.3.2.3. Botnet;

1.3.2.4. Spam;

1.3.2.5. Malware;

1.3.2.6. Spyware;

1.3.3. A solução deverá possibilitar o bloqueio de DNS over HTTPS/TCP 443;

1.3.4. Deve ser possível aplicar as ações de liberação, bloqueio ou Sinkhole a uma requisição DNS.

1.3.5. A solução deverá ser capaz de distinguir os diferentes tipos de requisições DNS: A, NS, CNAME, SOA, PTR, MX, TXT, AAAA, SRV, CERT e ANY.

1.3.6. Deve empregar capacidade de identificar domínios registrados recentemente (Newly Registered Domains)

1.3.7. Deve empregar técnicas para identificação de requisições DNS com destino a domínio gerado por algoritmo (DGA).

1.3.8. Deverá permitir criar listas customizadas de autorização e bloqueio de requisições DNS.

1.3.9. A solução deverá ser capaz de identificar e bloquear requisições de DNS tuneladas.

1.3.9.1. Deverá suportar o controle de resolução DNS, baseada em:

1.3.9.2. DNS over UDP/53;

1.3.9.3. DNS over TCP/53;

1.3.9.4. mDNS - UDP 5353

1.4. Solução de segurança para segurança do Office 365

1.4.1. A solução deve se integrar com o provedor de serviço, via Interface de Programação de Aplicação (API), garantindo visibilidade, controle e descoberta de dados.

1.4.2. A integração deverá ser nativa sem exigir a instalação de equipamentos on-premise para redirecionamento do tráfego ou emprego de clientes para redirecionamento do tráfego.

1.4.3. A solução deverá garantir visibilidade e controle de aplicações quando utilizadas no Browser, dispositivos móveis e aplicativos no desktop em máquinas não gerenciadas.

1.4.4. A solução de CASB API deverá atender as seguintes características:

1.4.4.1. Realizar o inventário e inspecionar o conteúdo armazenado nos serviços SaaS, independente de quando ele tenha sido criado ou carregado.

1.4.4.2. Classificar o documento quanto a exposição perante a usuários internos e usuários externos.

1.4.4.3. Identificar e proteger conteúdo sensível armazenado no serviço SaaS, de acordo com perfil do motor de DLP;

1.4.4.4. A solução deverá permitir ao SESC-DF determinar onde serão armazenados os metadados do incidente registrado pela solução.

1.4.4.5. Como resultante de uma ação de monitoramento de um usuário suspeito, a solução deverá guardar evidências para posterior medidas legais;

1.4.4.6. Ao identificar um conteúdo sensível a solução deverá permitir a retenção temporária do mesmo, para posterior análise administrativa;

1.4.4.7. Proteger contra armazenamento de artefatos maliciosos no serviço SaaS;

1.4.5. Garantir controle de acesso por meio de ações como restrição de acesso, revogação do compartilhamento e quarentenar conteúdo sensível.

1.4.6. Prover painel consolidado e acionável com as informações levantadas pela solução;

1.4.7. A solução deverá conter um leque de integrações pré-definido com os principais provedores de serviços em nuvem, dentre eles:

1.4.7.1. Microsoft Office 365 - OneDrive

1.4.7.2. Microsoft Office 365 - Outlook

1.4.7.3. Microsoft Office 365 - Sharepoint

1.4.7.4. Microsoft Office 365 – Teams

1.4.7.5. Microsoft Office 365 - Yammer

1.4.8. Com base na integração via API, a solução deverá atender aos seguintes casos de uso:

1.4.8.1. Criar uma lista de documentos acessíveis publicamente em uma instância do serviço Office 365.

1.4.8.2. Criar uma lista de documentos compartilhados externamente armazenados na instância do serviço Office 365.

1.4.8.3. Criar uma lista de documentos privados armazenados na instância do serviço Office 365.

1.4.8.4. Criar uma lista de usuários com links não expirados

1.4.9. Para a aplicação Microsoft Office 365 – OneDrive for Business, a solução deverá empregar as seguintes capacidades:

1.4.9.1. A solução deverá realizar todo o inventário do conteúdo armazenado na aplicação, garantindo a apresentação do nome do arquivo, tipo de arquivo, proprietário do arquivo, com quem está compartilhado e histórico de versões do arquivo.

1.4.9.2. Deve identificar arquivos compartilhados com usuários externos, bem como a permissão de acesso dada pelo proprietário;

1.4.9.3. Apresentar e classificar os arquivos quanto a exposição, devendo identificar arquivos com acesso público, privado e interno;

1.4.9.4. Deve permitir ao administrador da solução, baixar o arquivo que viole uma política de detecção de vazamento de dados;

1.4.9.5. Deve possuir capacidade de apresentar quais usuários foram identificados com malware, a partir de um artefato malicioso;

1.4.9.6. Além da identificação dos compartilhamentos externos, a solução deve permitir a remoção do link de compartilhamento público e restringir o acesso ao arquivo a pessoas selecionadas;

1.4.9.7. Através da integração com o Microsoft Information Protection (MIP), deverá permitir a importação dos labels previamente criados e utilizá-los para auxiliar no inventário e classificação de documentos;

1.4.10. Para a aplicação Microsoft Office 365 – Exchange Online, a solução deverá empregar as seguintes capacidades:

1.4.10.1. Analisar todos os e-mails enviados a domínios externos, incluindo anexo e o corpo do e-mail, quanto a violação a máscaras de LGPD (CNH, CPF, RG, Título de Eleitor);

1.4.10.2. Apresentar a análise, indicando minimamente o remetente, destinatário ou destinatários e o conteúdo identificado que levou a geração do alerta na ferramenta.

1.4.10.3. Quanto às políticas de DLP estabelecidas, a solução deverá monitorar e apresentar os maiores remetentes, os maiores destinatários e os principais domínios que receberam tais e-mails.

1.4.11. Para a aplicação Microsoft Office 365 – Sharepoint, a solução deverá empregar as seguintes capacidades:

1.4.11.1. A solução deverá realizar todo o inventário do conteúdo armazenado na aplicação, garantindo a apresentação do nome do arquivo, tipo de arquivo, proprietário do arquivo, com quem está compartilhado e histórico de versões do arquivo.

1.4.11.2. Deve identificar arquivos compartilhados com usuários externos, bem como a permissão de acesso dada pelo proprietário;

1.4.11.3. Apresentar e classificar os arquivos quanto a exposição, devendo identificar arquivos com acesso público, privado e interno;

1.4.11.4. Deve permitir ao administrador da solução, baixar o arquivo que viole uma política de detecção de vazamento de dados;

1.4.11.5. Deve possuir capacidade de apresentar quais usuários foram identificados com malware, a partir de um artefato malicioso;

1.4.11.6. Além da identificação dos compartilhamentos externos, a solução deve permitir a remoção do link de compartilhamento público e restringir o acesso ao arquivo a pessoas selecionadas;

1.4.11.7. Através da integração com o Microsoft Information Protection (MIP), deverá permitir a importação dos labels previamente criados e utilizá-los para auxiliar no inventário e classificação de documentos;

1.4.11.8. Deve identificar arquivos maliciosos hospedados;

1.4.12. Deve realizar análise de configuração do Office 365 baseado em padrões de mercado como NIST, CIS, dentre outros.

1.4.13. Deve analisar a configuração em torno do Exchange, Azure AD e OneDrive.

1.4.14. Deve possuir painel identificando as aplicações checadas e validações que apresentaram falha, bem como indicar como se corrige tal falha.

1.4.15. Deve apresentar análise de plugins conectados ao office 365.

1.5. Solução de segurança para proteção de dados

1.5.1. A solução contra vazamento ser aderente ao modelo chamado Zero Trust Data Protection, englobando os módulos:

1.5.1.1. E-mail;

1.5.1.2. Endpoint;

1.5.1.3. Web;

1.5.1.4. casb api;

1.5.1.5. ztna;

1.5.2. Para fins de facilitar a gestão das políticas, ao criar um perfil de monitoramento, este deve ser possível de ser replicado nos mais diversos módulos, sem a necessidade de criar novos modelos ou padrões para proteção de dados;

1.5.3. A solução deverá possuir padrões pré-definidos de mercado, como PCI-DSS, GDPR, HIPAA, GLBA, AMRA, EC Directive 2003, PHIPA, PIPEDA, LGPD e California Consumer Privacy Act.

1.5.4. Apesar da disponibilidade de padrões pré-definidos, a solução deverá permitir a criação de perfis customizados através do uso de identificadores disponíveis na solução (regex, dicionário) e de identificadores customizados sob demanda.

1.5.5. Para cada perfil de monitoramento a solução deverá permitir a associação a perfis de arquivos ao qual o monitoramento deve ser aplicado (exemplo: apenas pdf, word, documentos de processamento de texto, dentre outros).

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

1.5.7. A solução deverá permitir o monitoramento de carregamento de informações sensíveis em sites web, saas e iaas e em caso de tentativa de vazamento de dados, a solução deverá apresentar um popup pedindo a justificativa para proceder com a ação.

1.5.8. O perfil de monitoramento deverá observar as tecnologias de monitoramento básicas e avançadas englobando desde técnicas tradicionais como o uso de expressões regulares, dicionários, como também o uso de motores de aprendizagem contínua para identificação de padrões, como exemplo códigos fonte e currículo.

1.5.9. O perfil de monitoramento deverá observar as tecnologias de monitoramento básicas e avançadas englobando desde técnicas tradicionais como o uso de expressões regulares, dicionários, fingerprint, exact data match, mas também o uso de motores de aprendizagem contínua para identificação de padrões, como exemplo códigos fonte, informações financeiras, legais, identificação pessoal, informações médicas, recursos humanos e captura de tela.

1.5.10. A solução deverá permitir o treinamento de modelos de machine learning pré-existentes para identificar documentos sigilosos de interesse para proteção.

1.5.11. A solução deverá possibilitar o uso de técnicas de monitoramento de informações em documentos, planilhas, zip, 7zip, bases de dados, apresentações e arquivos texto.

1.5.12. A solução deverá possuir identificadores padrões, customizados e técnicas avançadas para construção de regras contando com as seguintes capacidades:

1.5.13. Deverá possuir identificadores pessoais brasileiros nativos, incluindo base com nomes, carteira nacional de habilitação, registro geral, cadastro de pessoa física, passaporte, NIS, cadastro nacional de pessoa jurídica, placa de carro, renavam e título de eleitor.

1.5.14. O identificador do tipo cadastro de pessoa física deverá possuir validação do dígito validador para CPF, indicando quando for válido ou inválido, obrigado a solução a agir caso identifique um registro válido.

1.5.15. Deverá possuir identificadores nativos referente a dados financeiros, como cartão de crédito, IBAN, contas bancárias e banking routing number;

1.5.16. Deverá possuir identificadores nativos a dados médicos como procedimentos médicos (ICD-10), condições médicas (ICD-10) e bases com nomes de componentes e nomes de remédios.

1.5.17. Deverá empregar recursos avançados de identificação textual, através do uso de OCR (Optical Character Recognition) para identificação de dados sensíveis em imagens;

1.5.18. Deverá empregar o uso de técnicas baseadas em fingerprint para identificar similaridade entre documentos analisados com opção de indicar a porcentagem de similaridade a ser aplicada para efeitos comparativos.

1.5.19. Deverá utilizar os labels previamente criadas no Microsoft AIP para criação do perfil de proteção contra vazamento;

1.5.20. A solução deverá permitir utilizar modelos de machine learning pré-existentes para identificar documentos desejados para adaptar o modelo e proteger contra vazamento de dados.

1.5.21. As técnicas mencionadas para identificação de dados sensíveis deverão ser transversais, ou seja, deverão ser aplicadas independente do vetor de proteção, incluindo:

1.5.21.1. Proteção para Endpoints;

1.5.21.2. Proteção para E-mail;

1.5.21.3. Proteção para aplicações SaaS via CASB API;

1.5.21.4. Proteção para web, saas e iaas via Proxy;

1.5.21.5. Proteção de aplicações internas via ZTNA;

1.5.22. O módulo de dlp deverá ser extensível a estações de trabalho, protegendo a cópia indevida para dispositivos locais, abrangendo:

1.5.22.1. Controle de dispositivo: A solução deverá permitir a restrição de uso de recursos locais como dispositivos usb, drivers de rede e impressora.

1.5.22.2. Controle de conteúdo: A solução deverá permitir a associação de perfis de proteção contra vazamento de dados para controlar o envio de informações para dispositivos usb e impressoras.

1.5.23. Em caso de falha de conectividade com a nuvem, a solução de endpoint deverá permitir o bloqueio total de dispositivos, de forma a não permitir a movimentação de dados.

1.5.24. A solução deverá permitir a criação de condição para cópia de arquivos com destino a dispositivos usb e impressora baseados na classificação do dispositivo.

1.5.25. Caso a estação de trabalho esteja sem conectividade com o datacenter do fabricante, a solução deverá bloquear qualquer tentativa de cópia para dispositivos usb.

1.5.26. A solução deverá permitir indicar aplicações saas de origem como condicional para permitir a cópia de um arquivo para dispositivos usb externos.

1.5.27. O módulo de prevenção contra vazamento de dados deverá ser extensível ao e-mail, englobando não apenas dispositivos monitorados via agente nativo, mas também computadores pessoais e até mesmo dispositivos móveis, permitindo que a solução realize a análise de todos os e-mails enviados pelos motores contra vazamento de dados, permitindo:

1.5.27.1. Análise de e-mails trocados entre colaboradores internos;

1.5.27.2. Análise de e-mails trocados entre colaboradores internos com destino a domínios externos;

1.5.28. O módulo de monitoramento de e-mail deverá permitir a integração e redirecionamento seguro através dos seguintes métodos:

1.5.28.1. Integração com Microsoft Outlook (saas) para redirecionamento seguro e análise pela solução proposta.

1.5.28.2. Através de integração com o Microsoft Exchange SaaS deve ser possível estabelecer fluxos de aprovação de liberação de mensagens indesejadas e até mesmo utilizar quarentena para reter e-mails para posterior revisão.

1.5.28.3. Através do cliente nativo, túnel ipsec e gre, a solução deverá interceptar o tráfego com destino a sites web, aplicações saas corporativas, aplicações saas terceiras (shadow it) e iaas, permitindo aplicar controles relacionados a prevenção contrafuga de dados;

1.5.29. A solução deverá ser capaz de empregar controle contra vazamento de dados em:

1.5.29.1. Aplicação SaaS Corporativa: Através da identificação da instância corporativa, a solução deverá aplicar controles específicos contra vazamento de dados, incluindo aplicações como microsoft office 365, google workspace, slack, dropbox, box, github, e servicenow.

1.5.29.2. Aplicação SaaS públicas (Shadow IT): Através da identificação de aplicações não corporativas ou pessoais, a solução deverá aplicar controles restritivos contra vazamento de dados, incluindo a capacidade de identificar mais de 80.000 aplicações e aplicar controles.

1.5.29.3. Aplicações SaaS terceiras: Através da identificação de aplicações corporativas, porém pertencentes a empresas terceiras, a solução deverá aplicar controles de acesso mais restritivos, bem como associar perfis de dlp contra vazamento de dados.

1.5.29.4. Sites Web: Através da identificação de urls baseadas em categorias nativas e customizadas, a solução deverá prevenir o envio de informações que indiquem potencial vazamento de dados.

1.5.29.5. Aplicações IaaS: Através da identificação de aplicações IaaS, como Amazon AWS (S3), Google GCP e Microsoft Azure, a solução deverá identificar a extração e envio de informações não autorizados conforme política contra vazamento de dados.

1.5.29.6. Aplicações IA generativa: Através da identificação de aplicações de IA generativa, como ChatGPT, Google Bard, Github copilot, a solução deverá prover controles inteligentes para identificação de máscaras de dados e controles de envio de informações sensíveis.

1.5.30. A solução deverá identificar informações confidenciais em imagens, através de tecnologia de OCR, com destino a aplicações saas, iaas e sites web, permitindo que o bloqueio em caso de uso indevido ocorra em tempo real;

1.5.31. A solução deverá identificar código fonte baseado em tecnologia de machine learning para identificação e bloqueio quanto ao mal uso

em aplicações não autorizadas, a exemplo: envio de códigos fonte para o chatgpt.

1.5.32. A solução deverá identificar chaves aws programáticas em códigos fonte, prevenindo que tal tipo de informação seja carregada em sites web, aplicações saas e iaas.

1.5.33. A solução deverá prevenir o envio de códigos fonte para instâncias não autorizadas do github, permitindo o envio de códigos fonte para apenas a instância corporativa do github.

1.5.34. A solução deverá prevenir o envio de credenciais corporativas para aplicações do tipo formulário, exemplo: google forms, permitindo a identificação do usuário e domínio por meio de expressão regular.

1.5.35. A solução deverá identificar aplicações corporativas saas e iaas, permitindo associar a classificação do dispositivo, bem como a geolocalização

1.5.36. A solução deverá bloquear a o upload de arquivos para aplicações saas, sites web e aplicações iaas baseado no quantitativo de registros identificados no arquivo acima do limite estabelecido como permitido, exemplo: 50 CPF 's..

1.5.37. A solução deverá permitir o upload de arquivos para aplicações saas, sites web e aplicações iaas baseado no baixo quantitativo de registros existentes no arquivo, permitindo que o usuário tome a decisão permitindo prosseguir com o carregamento mediante justificativa e cancelar caso não deseje prosseguir.

1.5.38. A solução deverá inspecionar mensagens diretas encaminhadas entre usuários no Microsoft Teams, garantindo a visibilidade e análise pelos motores de DLP, garantindo que caso haja mensagem com conteúdo sensível, a mesma deve ser bloqueada em tempo real.

1.5.39. A solução deverá suportar a integração com aplicações SaaS corporativas (sancionadas) via API, garantindo a descoberta, visibilidade dos dados existentes e por fim estabelecer controles basedos em políticas contra vazamento de dados.

1.5.40. Para a aplicação Microsoft Office 365 – OneDrive for Business, a solução deverá empregar as seguintes capacidades:

1.5.40.1. A solução deverá realizar todo o inventário do conteúdo armazenado na aplicação, garantindo a apresentação do nome do arquivo, tipo de arquivo, proprietário do arquivo, com quem está compartilhado e histórico de versões do arquivo.

1.5.40.2. Deve identificar arquivos compartilhados com usuários externos, bem como a permissão de acesso dada pelo proprietário;

1.5.40.3. Apresentar e classificar os arquivos quanto a exposição, devendo identificar arquivos com acesso público, privado e interno;

1.5.40.4. Deve permitir ao administrador da solução, baixar o arquivo que viole uma política de detecção de vazamento de dados;

1.5.40.5. Além da identificação dos compartilhamentos externos, a solução deve permitir a remoção do link de compartilhamento público e restringir o acesso ao arquivo a pessoas selecionadas;

1.5.40.6. Através da integração com o Microsoft Information Protection (MIP), deverá permitir a importação dos labels previamente criados e utilizá-los para auxiliar no inventário e classificação de documentos;

1.5.40.7. Deve analisar e identificar arquivos quanto a violação de máscaras de dados pessoais brasileiros (CNH, CPF, Título de Eleitor e NIS);

1.5.40.8. Para a aplicação Microsoft Office 365 – Exchange Online, a solução deverá empregar as seguintes capacidades:

1.5.40.9. Analisar todos os e-mails enviados a domínios externos, incluindo anexo e o corpo do e-mail, quanto a violação a máscaras de LGPD (CNH, CPF, RG, Título de Eleitor);

1.5.40.10. Apresentar a análise, indicando minimamente o remetente, destinatário ou destinatários e o conteúdo identificado que levou a geração do alerta na ferramenta.

1.5.40.11. Quanto às políticas de DLP estabelecidas, a solução deverá monitorar e apresentar os maiores remetentes, os maiores destinatários e os principais domínios que receberam tais e-mails.

1.5.40.12. Para a aplicação Microsoft Office 365 – Sharepoint, a solução deverá empregar as seguintes capacidades:

1.5.40.13. A solução deverá realizar todo o inventário do conteúdo armazenado na aplicação, garantindo a apresentação do nome do arquivo, tipo de arquivo, proprietário do arquivo, com quem está compartilhado e histórico de versões do arquivo.

1.5.40.14. Deve identificar arquivos compartilhados com usuários externos, bem como a permissão de acesso dada pelo proprietário;

1.5.40.15. Apresentar e classificar os arquivos quanto a exposição, devendo identificar arquivos com acesso público, privado e interno;

1.5.40.16. Deve permitir ao administrador da solução, baixar o arquivo que viole uma política de detecção de vazamento de dados;

1.5.40.17. Deve possuir capacidade de apresentar quais usuários foram identificados com malware, a partir de um artefato malicioso;

1.5.40.18. Além da identificação dos compartilhamentos externos, a solução deve permitir a remoção do link de compartilhamento público e restringir o acesso ao arquivo a pessoas selecionadas;

1.5.41. Através da integração com o Microsoft Information Protection (MIP), deverá permitir a importação dos labels previamente criados e utilizá-los para auxiliar no inventário e classificação de documentos;

1.5.41.1. Deve analisar e identificar arquivos quanto a violação de máscaras de dados pessoais brasileiros (CNH, CPF, Título de Eleitor e NIS);

1.5.41.2. Para a aplicação Microsoft Office 365 – Teams, a solução deverá empregar as seguintes capacidades:

1.5.41.3. Inventariar os usuários internos, times e usuários externos conectados a times expostos publicamente.

1.5.41.4. Deve ser capaz de prevenir o envio de mensagens que viole máscaras de dados pessoais brasileiros (CNH, CPF, Título de Eleitor e NIS) em canais do Teams;

1.5.41.5. Deve ser capaz de prevenir o envio de documentos que viole máscaras de dados pessoais brasileiros (CNH, CPF, Título de Eleitor e NIS) em canais do Teams;

1.5.41.6. Deve ser capaz de prevenir o envio de mensagem direta, que viole máscaras de dados pessoais brasileiros (CNH, CPF, Título de Eleitor e NIS) no Teams;

1.5.42. A solução deverá permitir o monitoramento e controle contra download de dados em aplicações privadas via protocolos HTTP/HTTPS, situadas no datacenter on-premises quanto em estruturas em nuvem pública.

1.5.42.1. A solução deverá possuir painel de gestão dos incidentes identificados, independente do vetor, mantendo todos os registros em um painel centralizado.

1.5.42.2. O Painel de gestão deverá concentrar as informações de identificação de tentativas de vazamento, com possibilidade de indicar o tempo de retenção, variando desde 24 horas até 90 dias, e com possibilidade no uso de filtros para buscar o incidente desejado.

1.5.42.3. Deverá possuir workflow de tratamento de incidente, permitindo designar uma determinada investigação a um usuário em específico, possibilitando a visibilidade do ciclo de tratamento.

1.5.42.4. No painel, caso seja identificado um determinado vazamento mais crítico do que a solução marcou inicialmente, o responsável pelo caso pode assinalar uma nova severidade para o caso.

1.5.42.5. Deve ser possível exportar o incidente, tanto um sumário com as informações apresentadas, quanto em detalhes, para permitir uma melhor investigação.

1.5.42.6. O incidente deverá conter detalhamento suficiente para apoiar o processo investigativo, incluindo:

1.5.42.6.1. Timestamp - data e hora ocorrido;

1.5.42.6.2. Método de deteção;

1.5.42.6.3. Atividade;

1.5.42.6.4. Ação tomada pela solução;

1.5.42.6.5. Violações identificadas;

1.5.42.6.6. Política que detectou o incidente;

1.5.42.6.7. Quantidade de violações;

1.5.42.7. Detalhes do que gerou a violação, apresentando dados do documento, a exemplo: nome, cnh e cpf;

1.5.42.8. Severidade do incidente;

1.6. Solução para monitoramento de experiência digital do usuário

1.6.1. A solução deverá prover módulo capaz de monitorar a experiência de acesso do usuário com destino a aplicações SaaS;

1.6.2. Através de um mapa global, deverá indicar a geolocalização de cada usuário do SESC-DF, apresentando ainda, através de cores intuitivas, a experiência de acesso.

1.6.3. No painel especializado de monitoramento, a solução deverá apresentar a quantidade de usuários monitorados, bem como usuários com baixa experiência, bem como aplicações impactadas.

1.6.4. Para os usuários apresentados, deverá apresentar um valor de classificação da experiência, permitindo ainda a associação com o dispositivo em uso.

1.6.5. Ao identificar um usuário com baixa experiência, deve ser possível investigar mais as razões pelas quais afetam o acesso do usuário, para tal, deverá permitir coletar informações da estação de trabalho, incluindo:

1.6.5.1. O valor de classificação da solução durante as últimas 48 horas.

1.6.5.2. Detalhes sobre o sistema operacional e dispositivo em uso;

1.6.5.3. Endereços IP associados (Público e Privado);

1.6.5.4. Aplicações acessadas;

1.6.5.5. Caminho completo, desde a estação até a aplicação SaaS, passando pelo centro de processamento do fabricante, indicando perda de pacote e latência entre cada um dos nós.

1.6.5.6. Métricas locais como uso de cpu, memória, disco, sinal wi-fi e consumo de rede;

1.7. Solução para proteção a rede pública wi-fi do SESC-DF;

1.7.1. A solução deverá proteger a rede sem fio do SESC-DF contra acessos maliciosos e indevidos.

1.7.2. Deverá se integrar através de túneis IPSEC e GRE.

1.7.3. A solução de proxy em nuvem deverá prover:

1.7.3.1. Inspeção de túneis criptografados baseados em TLS versões 1.2 e 1.3.

1.7.4. Base contendo mais de 120 categorias de URL e serviço de classificação dinâmico de URLs;

1.7.5. Customização de categorias para filtragem web, incluindo listas de bloqueio e de permissão;

1.7.6. Identificar aplicações SaaS corporativas e pessoais, com associação da instância para cada uma delas, através de uma base contendo mais de 80.000 aplicações SaaS;

1.7.7. Visibilidade e controle em tempo real de acesso a URLs, por meio de classificação baseado em categorias;

1.7.8. Prevenção contra vazamento de dados em aplicações SaaS corporativas, aplicações saas terceiras (ShadowIT), sites web e IaaS;

1.7.9. Prevenção contra acesso a sites maliciosos;

1.7.10. Prevenção contra download de artefatos maliciosos;

1.7.11. Prevenir a comunicação de aplicações cliente instaladas na estação de trabalho;

1.7.12. Prevenção contra-ataques via web, bloqueando tentativas de exploração remota da estação de trabalho;

1.7.13. Identificar credenciais expostas em vazamentos disponibilizados na internet;

1.7.14. A solução deverá suportar um volume total de 50 Gb de acessos mensais.

APÊNDICE II AO TERMO DE REFERÊNCIA

MODELO DE TERMO DE CONFIDENCIALIDADE E SIGILO

GERÊNCIA DE COMPRAS E CONTRATOS

Processo Pregão Nº _/2025

A empresa [RAZÃO SOCIAL], pessoa jurídica com sede em [ENDEREÇO], inscrita no CNPJ/MF com o n.º [N.º DE INSCRIÇÃO NO CNPJ/MF], neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente CONTRATADA, por tomar conhecimento de informações sobre o ambiente computacional do Serviço Social do Comércio – Administração Regional do DF, doravante denominado simplesmente CONTRATANTE, aceita as regras, condições e obrigações constantes do presente Termo.

1. O objetivo deste **TERMO DE CONFIDENCIALIDADE E SIGILO** é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do CONTRATANTE reveladas à CONTRATADA em razão da execução dos serviços objeto do contrato n.º __/20__, doravante denominado simplesmente CONTRATO, bem como assegurar o respeito às normas de segurança vigentes naquele órgão durante a realização dos serviços.

2. A expressão “informação restrita” abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, dentre outros.

3. A CONTRATADA compromete-se a não reproduzir e/ou dar conhecimento a terceiros, sem a anuência formal e expressa do

CONTRATANTE, das informações restritas reveladas.

4. A CONTRATADA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no CONTRATO, as informações restritas reveladas.

5. A CONTRATADA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao CONTRATANTE, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.

6. A CONTRATADA declara conhecer e se compromete a seguir e divulgar entre seus colaboradores envolvidos na execução do CONTRATO a Política Corporativa de Segurança da Informação do CONTRATANTE e normativos correlatos.

7. A CONTRATADA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo, conforme especificado no instrumento convocatório do processo licitatório que deu origem ao CONTRATO.

8. A CONTRATADA obriga-se a informar imediatamente ao CONTRATANTE qualquer violação das regras de sigilo estabelecidas neste Termo que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo.

9. A CONTRATADA obriga-se a informar ao CONTRATANTE a relação de colaboradores que estarão envolvidos na execução do CONTRATO e a fornecer ao CONTRATANTE a Declaração de Ciência do Termo de Manutenção de Sigilo e das Normas de Segurança Vigentes de cada colaborador.

10. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CONTRATANTE, ou uso inadequado de conta de acesso ao ambiente computacional do CONTRATANTE,

possibilitará a imediata rescisão de qualquer contrato firmado entre o CONTRATANTE e a CONTRATADA sem qualquer ônus para o CONTRATANTE. Nesse caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridas pelo CONTRATANTE, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

11. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CONTRATANTE, possibilitará a imediata rescisão de qualquer contrato firmado entre o CONTRATANTE e a CONTRATADA sem qualquer ônus para o CONTRATANTE. Nesse caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridas pelo CONTRATANTE, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

12. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do CONTRATANTE.

E, por aceitar todas as condições e as obrigações constantes do presente Termo, a CONTRATADA assina o presente termo através de seus representantes legais.

Brasília, ___ de _____ de 2025.

[NOME DA EMPRESA CONTRATADA]

_____ _____

Nome: Nome:

APÊNDICE III AO TERMO DE REFERÊNCIA

MODELO DE TERMO DE CIÊNCIA

GERÊNCIA DE COMPRAS E CONTRATOS

PREGÃO ELETRÔNICO Nº _/2025

A _____, inscrita no CNPJ sob o n.º _____, com sede _____, , por intermédio de seu representante legal _____, portador da Cédula de Identidade n.º_____, expedida pela _____ e CPF n.º _____, DECLARA para fins de atendimento aos procedimentos internos de gestão contratual e, ainda, ao , que se compromete a manter em sigilo, ou seja, não revelar ou divulgar as informações identificadas como confidenciais ou de caráter não público recebidas durante e após a prestação dos serviços no Sesc-AR/DF, tais como: informações técnicas, operacionais, administrativas, econômicas, financeiras e quaisquer outras informações, escritas ou verbais, fornecidas ou que venham a ser de nosso conhecimento, sobre os serviços licitados, ou que a ele se referem.

A violação dos termos deste instrumento resultará na aplicação das penalidades cabíveis ao infrator, cíveis e criminais, nos termos da lei, obrigando-lhe, ainda, a isentar e/ou indenizar o Sesc-AR/DF de todo e qualquer dano, perda, prejuízo ou responsabilidade, em virtude de demandas, ações, custas e despesas que porventura venha sofrer como resultado da violação do disposto neste instrumento.

Brasília, ___ de _____ de 2025

_____

Assinatura do representante legal

APÊNDICE IV AO TERMO DE REFERÊNCIA

MODELO DE PROPOSTA DE PREÇO

GERÊNCIA DE COMPRAS E CONTRATOS

Processo Nº _/2025

1.2. Proposta que faz a empresa _____para Contratação de solução de segurança da informação baseada em nuvem, por meio da plataforma Netskope, incluindo a disponibilização de licenças de uso, suporte técnico especializado, atualizações e serviços de implementação, com o objetivo de assegurar a proteção de dados, visibilidade e controle de acessos a aplicações em nuvem, tráfego web e ambientes híbridos, conforme condições, quantidades e exigências estabelecidas neste Termo de Referência, pelo prazo de 12 (Doze) meses, para atender as necessidades do Sesc-AR/DF, conforme tabela abaixo:

LOTE ÚNICO

	Item	Descrição	Quant.	Valor
LOTE ÚNICO	1	Solução de proteção acesso Web contra ameaças digitais	1800	
	2	Solução de acesso remoto as aplicações posicionadas em nuvem pública e interna	1800	
	3	Solução de segurança de acesso para resolução de nomes	1800	
	4	Solução de segurança para segurança do Office 365	1800	
	5	Solução de segurança para proteção de dados	1800	
	6	Solução para monitoramento de experiência digital do usuário	1800	
	7	Solução para proteção a rede pública wi-fi do SESC-DF	50	

(Observação: transcrever os valores totais em algarismos e por extenso)