# CONTRATAÇÃO DE EMPRESA ESPECIALIZADA SOLUÇÃO PARA GESTÃO DE NUVEM PÚBLICA.

ANEXO I

TERMO DE REFERÊNCIA

## 1. Objeto

A aquisição da solução para gestão multicloud em Software como serviço (*Software as a Service*), com hospedagem em Nuvem privada.

## 2. Justificativa de Aquisição

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.

O provimento de serviços na modalidade IaaS e PaaS necessitam de uma nova abordagem de segurança, uma vez que dados dos comerciários serão migrados de uma estrutura tradicional *on-premise* para uma nuvem.

Ademais, tratar-se-á da migração de sistemas que são o núcleo central do SESC-DF para a modalidade proposta, trazendo novos desafios e a segurança é um deles.

Como foco central, a segurança desses ambientes deverá prover a capacidade de visibilidade em torno de ambientes em nuvem, inventariando todos os recursos que estão em uso, permitindo a análise de segurança quanto a boas práticas de conformidade estabelecidas por órgãos de segurança e por fim controlar o trânsito dos arquivos por meio de análises através de motores especializados contra agentes maliciosos e vazamento de informações sensíveis.

A adoção deste tipo de serviço tem por objetivo final proporcionar maior economicidade quanto a exposição de dados sensíveis dos comerciários do Distrito Federal, controle de agentes maliciosos que por fim visam a indisponibilidade dos sistemas centrais e a adoção de

boas práticas de segurança no ambiente computacional garantindo maior estabilidade, segurança e desempenho para as atividades corporativas do SESC-DF.

## 3. Relação de Itens

| Item | Descrição | Quantitativo |
|---|---|---|
| 01 | SOLUÇÃO PARA GESTÃO DE NUVEM PÚBLICA | 1 |

## 4. Especificação Técnica Global

4.1. Características Da Solução

4.1.1. Solução com Funcionalidades de inventário, gestão de postura e acesso seguro como alvo a nuvem pública contratada pelo SESC/AR/DF.

4.2. Caraterísticas de Validade Contratual

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

4.3. Característica de Atendimento e Serviço de Suporte

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

4.3.2. O tempo de atendimento deverá ser de no máximo 2 (duas) horas, que compreende o tempo entre a abertura do chamado na central de atendimento e o início do atendimento técnico realizado pela equipe de suporte;

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

chamado. Este será considerado o início para contagem dos prazos estabelecidos;

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

4.4. Características de Serviço de Instalação:

4.4.1. O serviço de instalação dos componentes e integração da solução pretendida deverá ser executada integralmente pelo fabricante da solução.

4.4.2. O fabricante da solução deverá arcar com os custos de deslocamento, hospedagem e alimentação do recurso alocado.

4.4.2.1. Do escopo macro a ser entregue pelo fabricante:

4.4.2.2. Integração via API com Microsoft Azure

4.4.2.3. Configuração dos padrões de segurança recomendados pelo fabricante.

4.4.2.4. Customização de um perfil para análise do ambiente Azure.

4.4.2.5. Configuração para acesso remoto seguro as aplicações hospedadas no Microsoft Azure e no Datacenter do SESC/DF

4.4.2.6. Confguração do perfil de malware para análise de Bloobs Azure e buckets S3 Amazon.

4.4.2.6.1. Integração de compartilhamento de IOC entre plataformas.

4.4.2.6.2. Configuração de um perfil de prevenção contra exposição de dados confidenciais (LGPD) em storages no Microsoft Azure.

4.4.2.6.3. A solução deverá prover autenticação integrada com Azure AD (Single Sign-on) para os usuários administradores da solução.

4.4.2.6.4. A solução deverá possuir integração com Microsoft Azure Active Directory para autenticar os acessos a aplicações hospedadas em ambientes em nuvem.

4.4.2.6.5. Regras de controle, em tempo real, para plataformas de nuvens, a exemplo GitHub, Azure, Azure DevOPS, Amazon AWS, dentre outras a critério do SESC-DF

4.5. Suporte especializado do fabricante

4.5.1. O Serviço deverá contemplar um Gerente de Sucesso para o acompanhamento da solução durante toda a vigência contratual, garantindo:

4.5.1.1. Compartilhar boas práticas de administração da solução

4.5.1.2. Documentação técnica para apoiar e sustentar uma determinada decisão técnica

4.5.1.3. Desenhar e apresentar junto aos decisores um roadmap estratégico para determinar os passos de proteção e governança

4.5.1.4. Prover Transferência de conhecimento pós-implantação

4.5.1.5. Fornecer liderança técnica e orientação para conduzir a implantação e operacionalização da plataforma de gestão de nuvem.

4.5.1.6. Auxiliar na configuração e ajuste de políticas, configuração de aprimoramentos do produto e revisões periódicas de políticas.

4.5.1.7. Executar um plano estratégico de realização e obtenção de valor e retorno sobre investimento, conforme casos de uso que estejam alinhados às necessidades de segurança e do negócio

4.5.1.8. Apoio técnico para os administradores da solução

4.5.1.9. Apoio executivo para CISO/CSO.

5. SOLUÇÃO PARA GESTÃO DE NUVEM PÚBLICA

5.1. Características Gerais da solução

5.1.1. Deverá possuir suporte a ambientes multi-cloud, em especial Microsoft Azure ou Amazon AWS.

5.1.1.1. Deverá garantir o monitoramento de:

5.1.1.2. 10 Contas administrativas;

5.1.1.3. 200 Recursos (Computacionais, Storage, VPC)

5.1.1.4. 1 Tb de análise para dados em repouso quanto a Malware e prevenção contra vazamento de dados.

5.1.1.5. 1.200 Usuários corporativos

5.2. Características Técnicas da Solução:

5.2.1. A Plataforma SASE deverá integrar com serviços IaaS/PaaS para prover inventário e visibilidade da configuração para atender a requisitos de segurança e conformidade

5.2.2. A plataforma SASE deverá prover funcionalidades de análise de postura, prevenção de vazamento de dados e artefatos maliciosos

5.2.3. A Plataforma SASE deverá integrar via API's nativas e disponibilizadas pelos fabricantes de ambientes IaaS/PaaS

5.2.4. Deverá suportar integração via API com, no mínimo, os seguintes serviços IaaS/PaaS:

5.2.4.1. Amazon AWS;

5.2.4.2. Microsoft Azure;

5.2.5. A solução deverá ser capaz de gerir ambientes multicloud (AWS e Azure, por exemplo) identificando problemas de configuração e em caso de identificação de alguma não conformidade.

5.2.6. A Plataforma deverá se integrar de maneira nativa, via API, com o serviço Microsoft Azure e Amazon AWS;

5.2.7. O inventário deverá apresentar informações como:

5.2.7.1. Redes Virtuais

5.2.7.2. Storages

5.2.7.3. Bases de Dados

5.2.7.4. Usuários

5.2.7.5. Máquinas

5.2.7.6. Grupos de Segurança

5.2.7.7. Perfis de Usuário

5.2.8. Deverá constar na base de inteligência da solução perfis de verificação de conformidade, baseado em boas práticas para cada plataforma IaaS/PaaS tendo como base benchmarks de segurança.

5.2.9. Os perfis de validação de conformidade e segurança, deverão conter regras específicas para cada uma das plataformas IaaS/PaaS (AWS, Azure, GCP) com base em padrões mundiais, conforme segue:

5.2.9.1. Cloud Security Alliance - Cloud Controls Matrix

5.2.9.2. NIST CyberSecurity Framework

5.2.9.3. NIST 800-53

5.2.9.4. Center for Internet Security Benchmarks

5.2.9.5. PCI - DSS

5.2.9.6. SOC2 Trust Services Criteria

5.2.9.7. Boas práticas (AWS, Azure, GCP)

5.2.9.8. Cada perfil deve possuir uma série de validadores, indicando controles específicos para cada um dos perfis indicados e plataformas.

5.2.9.9. Deve possuir suporte a integração via API com a plataforma de desenvolvimento GitHUB;

5.2.9.10. Para adaptar-se aos ambientes dinâmicos, a solução deverá ser capaz de criar perfis customizados, com regras configurados especificamente para o ambiente em questão

5.2.9.11. Os perfis, customizados ou padrão da solução, deverão ser incluídos em políticas que deverão conter os seguintes parâmetros:

5.2.9.11.1.1. Plataforma IaaS/PaaS

5.2.9.11.1.2. Conta associada

5.2.9.11.1.3. Perfil, incluindo alerta e as regras associadas

5.2.9.11.1.4. Ação

5.2.9.12. Ao identificar um artefato malicioso em um storage em nuvem, o Indicador de Comprometimento identificado pela solução (Hash do arquivo), deverá ser compartilhado com a solução da Checkpoint existente no ambiente do SESC-DF, de maneira nativa.

5.2.9.13. A Solução deverá prover capacidade de integrar, por meio de STIX/TAXII informações de ameaça com destino a solução pretendida e esta orquestrar o envio para demais plataformas, a exemplo: EDR, SIEM ou SOAR.

5.2.9.14. A solução deverá prover análise de dados em repouso em bloobs Azure, garantindo as seguintes capacidades:

5.2.9.14.1. Deverá prover mais de 40 templates de regulamentação, dentre eles HIPAA, GDPR, PCI e LGPD.

5.2.9.14.2. Deverá possuir mais de 3.000 identificadores em mais de 1.500 tipos de arquivos.

5.2.9.14.3. Para a identificação de máscaras, deverá suportar Regex customizadas, padrões e dicionários.

5.2.9.14.4. Deverá suportar o fingerprint de arquivos identificando com grau de similaridade, permitindo até mesmo a identificação de padrões em tabelas (Exact data Match) inclusive.

5.2.9.14.5. Deverá suportar Inteligência Artificial e Machine Learning para identificação de documentos (ex: código fonte) e imagens (Exemplo: Screenshot, Whiteboard, Passaporte).

5.2.9.15. A solução deverá prover capacidade de identificação de máscaras que violem LGPD.

5.2.9.16. A solução deverá prover controle de identificação de instâncias através da análise de tráfego, em tempo real, sem dependência de API, para ambientes multi-cloud, apresentando:

5.2.9.16.1. ID do SESC-DF indicando a tenant corporativa;

5.2.9.16.2. ID de Terceiros, indicando que a tenant não é corporativa;

5.2.9.17. A solução deverá prover identificação de tenant para ambientes SaaS/IaaS;

5.2.9.18. A solução deverá ser capaz de implementar controle de atividades para ambientes Azure em tempo real, com a granularidade para as seguintes atividades

5.2.9.18.1. Publish;

5.2.9.18.2. Start;

5.2.9.18.3. Reboot;

5.2.9.18.4. Upload;

5.2.9.18.5. View;

5.2.9.18.6. Shutdown;

5.2.9.19. A solução deverá garantir controle em tempo real, sem depender de API, para o ambiente Microsoft Azure DevOPS.

5.2.9.20. A solução deverá prover total integração com a plataforma de desenvolvimento GitHub, sem depender de API, garantindo granularidade para os seguintes controles:

5.2.9.20.1. Bloqueio para acesso a instâncias do GitHub de cunho pessoal ou de terceiros.

5.2.9.20.2. Liberação de acesso a instância do Github do SESC/DF

5.2.9.20.3. Controle de Upload;

5.2.9.20.4. Controle de Compartilhamento;

5.2.9.20.5. Controle de Post;

5.2.9.20.6. Controle de Deleção;

5.2.9.21. A solução deverá prover o monitoramento de credencial para os usuários do SESC/DF, garatindo no mínimo:

5.2.9.21.1. Identificação do usuário interno com a credencial vazada;

5.2.9.21.2. Identificação do usuário pessoal relacionado a credencial vazada;

5.2.9.21.3. Identificação da fonte do vazamento;

5.2.9.22. Através da análise do tráfego em tempo real, a solução deverá prover capacidade de entendimento via análise comportamental para:

5.2.9.22.1. Deleção em massa de dados;

5.2.9.22.2. Download em massa;

5.2.9.22.3. Sucessivas falhas de login;

5.2.9.22.4. Upload em massa;

5.2.9.22.5. Atividade geograficamente distantes;

5.2.9.22.6. Eventos raros, nunca visto;

5.2.9.22.7. Compartilhamento de credencial para acesso;

5.2.9.22.8. Movimentação suspeita de dados entre nuvens, Exemplo: Download a partir de um storage em nuvem e upload em uma instância do OneDrive Pessoal do colaborador.

5.2.9.22.8.1. Deverá ser capaz de analisar todo download feito a partir de storagem em nuvem, em tempo real, quanto as políticas de DLP estabelecidas.

5.2.9.22.8.2. Ao fazer um Download de um dado que viole uma LGPD com origem em um Bloob para a máquina local, a solução deverá,

em tempo real, prevenir cópias do mesmo para nuvens terceiras que tenham baixa reputação conforme centro de inteligência do fabricante.

5.2.9.22.8.3. A Solução deverá ser capaz de restringir o acesso ao ambiente Azure, em tempo real, para máquinas que não atendam aos requisitos mínimos de conformidade, como por exemplo:

5.2.9.22.8.3.1. Máquina está no domínio do SESC;

5.2.9.22.8.3.2. Máquina possui o processo do antivírus em execução;

5.2.9.22.8.3.3. Máquina possui uma chave de registro que indique a existência do cliente da Checkpoint;

5.2.9.22.8.3.4. Máquina possui um arquivo que indique a instalação do sistema interno do SESC/DF.

5.2.9.22.8.3.5. Caso a máquina seja identificada como fora do padrão, o mesmo deverá ter o acesso reduzido a Azure, como por exemplo:

1. Não deverá permitir o shutdown de nenhum workload.

5.2.9.22.8.3.6. A solução deverá prover o controle de cópias de código do Github para nuvens terceiras, como por exemplo: Zippyshare e WeTransfer.

5.2.9.22.8.3.7. A solução deverá suportar integração com Azure RMS Encryption.

5.2.9.22.8.3.8. A solução deverá prover regra de DLP com capacidade de entendimento na quantidade de objetos identificados em um determinado vazamento, aumentando o grau de risco do evento conforme a quantidade de dados identificados.

5.2.9.22.8.3.9. A solução deverá prover dados de forense, identificando os dados identificados no vazamento.

1. A solução deverá ser capaz de apresentar uma retenção legal quando o SESC/DF identificar a necessidade de judicializar algum tipo de vazamento interno, mantendo a rastreabilidade do dado e apresentando informações de:
    1. Data
    2. Arquivo
    3. Política
    4. Violação
    5. Proprietário do Arquivo

5.2.9.22.8.3.10. Opcionalmente, o administrador, ao identificar um arquivo que viole as regras de LGPD, poderá:

1. Entrar em contato com o proprietário;
2. Fazer o download dos arquivos;

5.2.9.22.8.3.11. A solução deverá controlar o download/upload de artefatos maliciosos com destino a Azure, garantindo:

1. Controle via API;
2. Controle em tempo real;

5.2.9.22.8.3.12. Para análise de malware, a solução deverá empregar, minimamente:

1. Antivirus de assinatura;
2. Machine Learning;
3. Sandbox;

5.2.9.22.8.3.13. A solução deverá prover capacidade de acesso remoto seguro baseando-se no conceito Zero Trust Network Access.

5.2.9.22.8.3.14. A autenticação do acesso deverá ser totalmente integrada com Azure AD para autorização a acesso ao recurso de rede pretendido.

5.2.9.22.8.3.15. A solução deverá ser capaz de prover acesso seguro a aplicações que sejam executadas nos protocolos TCP e UDP, garantindo, no mínimo acesso as seguintes aplicações:

1. SSH – TCP/22
2. HTTP – TCP/80,443,8080,8443
3. RDP – TCP/3389,8267,9967
4. SQL Server – TCP/1333,1434 | UDP/1434
5. SMB – TCP/445
6. FTP – TCP/21

5.2.9.22.8.3.16. Solução deverá possuir capacidade de gerir acesso a aplicações tanto na nuvem pública, quanto ao ambiente on-premise do SESC/DF.

5.2.9.22.8.3.17. A solução deverá ter capacidade de customização das portas das aplicações pretendidas, permitindo a conexão em portas TCP/UDP que não são padrão de mercado.

5.2.9.22.8.3.18. A solução deverá prover acesso ao ambiente sem exposição de gateways a internet, garantindo que o acesso seja feito somente pelo bloco de endereços ip através de túnel seguro.

5.2.9.22.8.3.19. A solução deverá ser capaz de mascarar o endereçamento dos servidores internos, apresentado

endereçamento falso quando conectado pela solução de acesso remoto.