ARP-06.09/2023

ATA DE REGISTRO DE PREÇOS

VALIDADE: 12 (DOZE) MESES CONTADOS DE SUA ASSINATURA OU DA ÚLTIMA ASSINATURA DIGITAL REALIZADA

Aos 13 (treze) dias do mês de setembro de 2023, a **EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO – PRODAM-SP – S/A** situada nesta Capital, à Rua Libero Badaró, nº 425, Centro, São Paulo/SP, inscrita no CNPJ sob nº 43.076.702/0001-61, neste ato representada por seu **DIRETOR DE ADMINISTRAÇÃO E FINANÇAS** e por seu **DIRETOR DE INFRAESTRUTURA E TECNOLOGIA**, nos termos do artigo 66, da Lei Federal nº 13.303/16, com as alterações posteriores e do Decreto Municipal nº 62.100/2022, em face do resultado obtido no Pregão Eletrônico nº 06.001/2023, devidamente homologado pela Autoridade Competente, resolve celebrar a presente **ATA DE REGISTRO DE PREÇOS**, procedendo ao registro de preço do primeiro colocado para eventual e futura **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NO FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA E GOVERNANÇA DE DADOS EM APPLIANCE (HARDWARE DEDICADO), POSSIBILITANDO A IDENTIFICAÇÃO E CLASSIFICAÇÃO DE INFORMAÇÕES SENSÍVEIS, ANÁLISE EM TEMPO REAL E PREVENÇÃO DE COMPORTAMENTOS SUSPEITOS, CONTEMPLANDO SERVIÇOS DE INSTALAÇÃO, SUPORTE E MANUTENÇÃO, OPERAÇÃO ASSISTIDA E TREINAMENTO**, cujas descrições detalhadas encontram-se no **Anexo I – Termo de Referência** – desta Ata, nos seguintes termos.

CLÁUSULA I – DETENTORA E CADASTRO RESERVA

1.1. Figura como primeira classificada e DETENTORA desta Ata de Registro de Preços a empresa **OMEGA TECNOLOGIA DA INFORMACAO LTDA,** com sede na Rua Joci José Martins, nº 247, Edif. PME Offices Tower, andar 4 - sala 412, bairro Pagani, no Município de Palhoça, no Estado de Santa Catarina, CEP 88.132-148, inscrita no CNPJ sob o nº 04.808.453/0001-08, neste ato representada por seu sócio, Sr. **MANOEL FONSECA NETO**, portador da Cédula de Identidade RG. nº 3.081.522-3 SSP/SC e inscrito no CPF sob o nº 029.151.929-60.

1.2. **"CONSULTADAS AS EMPRESAS PARTICIPANTES DO PREGÃO ELETRÔNICO QUE PRECEDEU ESTA ATA, NOS TERMOS DO ARTIGO 66, INCISO V, DA LEI FEDERAL Nº 13.303/16, NENHUMA CONCORDOU EM FORNECER AO PREÇO OFERTADO, NA LICITAÇÃO, PELA DETENTORA DA ATA."**

CLÁUSULA II – OBJETO

2.1. A presente Ata de Registro de Preços tem por objeto futura e eventual contratação, pelos ÓRGÃOS PARTICIPANTES, de **EMPRESA ESPECIALIZADA NO FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA E GOVERNANÇA DE DADOS EM APPLIANCE (HARDWARE DEDICADO), POSSIBILITANDO A IDENTIFICAÇÃO E CLASSIFICAÇÃO DE INFORMAÇÕES SENSÍVEIS, ANÁLISE EM TEMPO REAL E PREVENÇÃO DE COMPORTAMENTOS SUSPEITOS, CONTEMPLANDO SERVIÇOS DE INSTALAÇÃO, SUPORTE E MANUTENÇÃO, OPERAÇÃO ASSISTIDA E TREINAMENTO**, conforme detalhamento e especificações técnicas constantes no Termo de Referência, na proposta comercial da CONTRATADA e demais documentos constantes no processo administrativo em epígrafe.

2.2. Deverão ser respeitadas todas as especificações técnicas e demais condições de fornecimento contidas no Termo de Referência – Anexo I desta Ata.

2.3. É vedado efetuar acréscimos nos quantitativos fixados nesta Ata de Registro de Preços, inclusive o acréscimo de que trata o § 1°, do artigo 81, da Lei Federal nº 13.303, de 30 de junho de 2016.

CLÁUSULA III - ÓRGÃO(S) PARTICIPANTE(S)

3.1. São órgãos e entidades públicas participantes do registro de preços aqueles constantes na Justificativa Técnica (doc. nº 086524787 do Processo SEI nº 7010.2023/0004811-7).

CLÁUSULA IV – ESPECIFICAÇÕES, QUANTITATIVOS E PREÇOS

4.1. Os preços e quantidades ora registrados são os seguintes:

Item	Descrição	Quantidade	Valor Unitário	Valor Total
1	Appliance (hardware dedicado) de inspeção de segurança	2	R$ 6.500.000,00	R$ 13.000.000,00
2	Suporte técnico, manutenção e garantia de appliance (hardware dedicado) para inspeção de segurança	24	R$ 162.500,00	R$ 3.900.000,00
3	Pacote de licenças de auditoria, análise de eventos e governança de dados para atender usuários / credenciais (sob demanda pelo período de 24 meses)	60.000	R$ 1.135,20	R$ 68.112.000,00
4	Serviço de Instalação e Configuração	1	R$ 250.000,00	R$ 250.000,00
5	Serviço de Operação Assistida (sob demanda pelo período de 23 meses)	60.000	R$ 63,95	R$ 3.837.000,00
6	Serviço de Treinamento, conforme especificação detalhada no termo de referência.	1	R$ 102.000,00	R$ 102.000,00
			TOTAL	**R$ 89.201.000,00**

4.2. O valor total registrado é de **R$ 89.201.000,00 (oitenta e nove milhões e duzentos e um mil reais).**

4.3. O preço registrado abrangerá os custos diretos e indiretos decorrentes do fornecimento do objeto, incluindo tributos (impostos, taxas, emolumentos, contribuições fiscais e parafiscais, entre outros), seguros, despesas de administração, lucro, custos de transporte, frete e demais despesas correlatas.

4.4. Os preços registrados têm caráter orientativo (preço máximo), cabendo ao gerenciador da Ata, bem como às unidades interessadas, a promover, obrigatoriamente, prévia pesquisa de preço que revele a conveniência da contratação.

4.5. Se o preço registrado se tornar superior aos valores praticados no mercado, o ÓRGAO GERENCIADOR adotará as seguintes providências:

4.5.1. Convocará a DETENTORA visando à negociação para a redução de preços e sua adequação ao mercado;

4.5.2. Frustrada a negociação, liberará a DETENTORA do compromisso assumido e cancelará o seu registro, respeitadas as contratações já celebradas;

4.6. Não logrando êxito na negociação, o ÓRGÃO GERENCIADOR cancelará o item objeto do preço negociado.

4.7. As condições gerais do fornecimento, tais como os prazos para entrega e recebimento do objeto, obrigações da DETENTORA na execução do contrato, penalidades aplicáveis, condições de faturamento e pagamento, e demais condições do ajuste encontram-se definidos na minuta do contrato e no Termo de Referência, Anexos e desta Ata.

CLÁUSULA V – VALIDADE DO REGISTRO DE PREÇOS

5.1. O prazo de validade do Registro de Preços será de 12 (doze) meses, contados a partir da data de sua assinatura, ou da última assinatura digital realizada, podendo ser prorrogado por novo período de 12 (doze) meses, desde que observadas as formalidades previstas no art. 99 do Decreto Municipal nº 62.100/22.

CLÁUSULA VI – CONTRATAÇÕES DECORRENTES DA ATA DE REGISTRO DE PREÇOS

6.1. Os fornecedores que assinarem a Ata de Registro de Preços estarão obrigados a celebrar as contratações que dela poderão advir, observadas as condições estabelecidas no Edital, em seus anexos e nesta Ata, ficando sujeita às penalidades cabíveis pelo descumprimento de quaisquer condições.

6.2. A existência de preços registrados não obriga a Administração a firmar as contratações decorrentes desta Ata, ficando-lhe facultada à utilização de outros meios, sem que caiba recurso ou indenização de qualquer espécie à empresa DETENTORA, respeitada a legislação relativa às licitações, sendo assegurado ao beneficiário do registro a preferência de contratação em igualdade de condições.

6.3. A contratação do objeto desta Ata será formalizada através da minuta de contrato constante no **Anexo VI** do Edital.

6.4. Se, por ocasião da formalização da contratação, algum dos documentos apresentados pela DETENTORA para fins de comprovação da regularidade fiscal e trabalhista, estiverem com prazo de validade expirado, esta será notificada para, no prazo de 2 (dois) dias úteis, comprovar sua situação de regularidade, sob pena de a contratação não se realizar.

6.5. Constitui condição para a celebração da contratação a comprovação, por parte da DETENTORA, de que se encontra em situação regular junto ao CADIN (Cadastro Informativo Municipal) do Município de São Paulo (Lei Municipal n.º 14.094/2005 e Decreto Municipal n.º 47.096/2006), mediante apresentação de certificado emitido através do site http://www3.prefeitura.sp.gov.br/cadin/

6.6. Caso haja alguma taxa ou emolumento cobrado por órgão contratante para a elaboração do instrumento contratual, o valor será pago pela DETENTORA desta Ata.

6.7. No prazo de 5 (cinco) dias úteis contados a partir da data da convocação, a DETENTORA deverá retirar as vias contratuais oriundas das contratações desta Ata, ou solicitar o envio por meio eletrônico, assinar e devolver, podendo este prazo ser prorrogado, por igual período, mediante solicitação justificada do interessado e aceita pela Administração.

6.8. O não comparecimento da DETENTORA para retirar as vias contratuais, ou quando solicitado o envio por meio eletrônico, a ausência de envio de confirmação de recebimento, importará na recusa à contratação, sujeita à aplicação das penalidades cabíveis.

6.9. A utilização desta Ata de Registro de Preços referente aos itens 3 e 5 da tabela constante do item 1.1 do Anexo I - Termo de Referência, por órgãos e entidades que não tenham participado do certame licitatório, quando admitida, obedecerá aos prazos, limites (individual e global) e demais condições estabelecidas no Edital que regeu o certame licitatório.

CLÁUSULA VII – PENALIDADES

7.1. A DETENTORA estará sujeita às penalidades previstas na Lei Federal nº 13.303/16 e suas atualizações e demais legislações pertinentes, sem prejuízo da aplicação de outras cabíveis, em especial:

a) Advertência no caso de atraso de até três dias para devolução das vias contratuais, nos prazos estabelecidos na Cláusula VI, item 6.7 deste instrumento;

b) Multa de até 2% (dois por cento) sobre o valor total a ser registrado, caso o atraso na devolução das vias contratuais seja superior a três dias úteis;

c) Multa de 10% (dez por cento) sobre o valor total registrado, no caso de rescisão e/ou cancelamento da respectiva Ata de Registro de Preços por culpa ou a requerimento da DETENTORA, sem motivo justificado e ou amparo legal.

CLÁUSULA VIII – CANCELAMENTO DO REGISTRO DE PREÇOS

8.1. A DETENTORA poderá ter seu registro cancelado quando:

8.1.1. Descumprir as condições da Ata de Registro de Preços;

8.1.2. Recusar a formalizar contratação decorrente deste Registro de Preços, sem motivo justificado e aceito pela Administração;

8.1.3. Não aceitar reduzir o preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado;

8.1.4. Inexecução total ou parcial de contrato decorrente desta Ata de Registro de Preços;

8.1.5. Transferência no todo ou em parte do instrumento contratual;

8.1.6. Der causa à rescisão administrativa de contrato decorrente deste Registro de Preços;

8.1.7. Razões de interesse público, devidamente motivadas e justificadas pela Administração.

8.2. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados, por razões de interesse público.

8.3. Na ocorrência de quaisquer das hipóteses acima descritas, serão garantidos à DETENTORA o contraditório e a ampla defesa.

8.4. A DETENTORA poderá ter o registro de preços cancelado, mediante solicitação, quando comprovar estar impossibilitada de cumprir as exigências desta Ata de Registro de Preços.

8.4.1. A solicitação da DETENTORA para cancelamento dos preços registrados deverá ser formulada com a antecedência de 30 (trinta) dias, respeitados os contratos já celebrados.

CLÁUSULA IX – DISPOSIÇÕES FINAIS

9.1. Integram esta Ata o Edital do Pregão nº 06.001/2023 (doc. nº 086908054 do Processo SEI nº 7010.2023/0004811-7) e a Proposta Comercial da DETENTORA (doc. nº 088220186 do Processo SEI nº 7010.2023/0004811-7).

9.2. Fica eleito o Foro da Comarca da Capital do Estado de São Paulo, com renúncia expressa de qualquer outro, por mais privilegiado que seja, para dirimir toda e qualquer questão decorrente da utilização da presente Ata.

9.3. Os casos omissos serão resolvidos de acordo com a Lei Federal nº 13.303/16 e atualizações subsequentes, bem como as demais normas aplicáveis.

E por estarem assim, justos e avençados, assinam as partes o presente instrumento em 2 (duas) vias de igual teor, perante as testemunhas abaixo.

São Paulo, 13 de setembro de 2023

gov.br Documento assinado digitalmente
MATEUS DIAS MARCAL
Data: 20/09/2023 17:10:28-0300
Verifique em https://validar.iti.gov.br

Pela PRODAM-SP: **MATEUS DIAS MARÇAL**
Diretor de Infraestrutura e Tecnologia

ELIAS FARES HADI:09443832895
Assinado digitalmente por ELIAS FARES HADI:09443832895
ND: C=BR, O=ICP-Brasil, OU=AC SOLUTI Multipla v5, OU=21308480000122, OU=Videoconferencia, OU=Certificado PF A3, CN=ELIAS FARES HADI:09443832895
Razão: Eu sou o autor deste documento
Localização:
Data: 2023.09.21 11:36:41-03'00'
Foxit PDF Reader Versão: 12.1.3

ELIAS FARES HADI
Diretor de Administração e Finanças

Assinado de forma digital por MANOEL FONSECA NETO:02915192960
Dados: 2023.09.18 19:00:25 -03'00'

Pela DETENTORA: **MANOEL FONSECA NETO**
Sócio

TESTEMUNHAS:

1) gov.br Documento assinado digitalmente
MARCO ROGERIO SORANZO CANCIAN
Data: 18/09/2023 19:05:26-0300
Verifique em https://validar.iti.gov.br

2) CAROLINA MAGNANI HIROMOTO
Assinado de forma digital por CAROLINA MAGNANI HIROMOTO
Dados: 2023.09.20 15:28:24 -03'00'

ANEXO I - TERMO DE REFERÊNCIA

1. OBJETO

ATA DE REGISTRO DE PREÇOS para futura e eventual CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NO FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA E GOVERNANÇA DE DADOS EM APPLIANCE (HARDWARE DEDICADO), POSSIBILITANDO A IDENTIFICAÇÃO E CLASSIFICAÇÃO DE INFORMAÇÕES SENSÍVEIS, ANÁLISE EM TEMPO REAL E PREVENÇÃO DE COMPORTAMENTOS SUSPEITOS, CONTEMPLANDO SERVIÇOS DE INSTALAÇÃO, SUPORTE E MANUTENÇÃO, OPERAÇÃO ASSISTIDA E TREINAMENTO.

1.1. Tabela de composição de itens Lote 01 (único):

Item	Descrição	Métrica	Quantidade Estimada	Valor Unitário (R$)	Valor Total (R$)
1	Appliance (hardware dedicado) de inspeção de segurança	Unidade	2		
2	Suporte técnico, manutenção e garantia de item 1 - *appliance* (hardware dedicado) para inspeção de segurança	Mensal	24		
3	Pacote de licenças de auditoria, análise de eventos e governança de dados para atender usuários / credenciais (sob demanda pelo período de 24 meses)	Unidade	60.000		
4	Serviço de Instalação e Configuração	Unidade	1		
5	Serviço de Operação Assistida (sob demanda pelo período de 23 meses)	Unidade	60.000		
6	Serviço de Treinamento, conforme especificação detalhada no Termo de Referência	Unidade	1		
VALOR TOTAL DO LOTE (ÚNICO)					

Os itens 1 a 5 descritos na tabela acima são imprescindíveis para o pleno funcionamento da solução, sendo, portanto, obrigatória na 1ª adesão sua contratação. A partir da 2ª adesão os itens 1, 2 e 4 não serão mais contratados pelos órgãos que já aderiram a ata. Embora o item 6 – Treinamento, faça parte da solução, a contratação/adesão será opcional.

A adesão dos itens 3 e 5, licenças de auditoria e serviço de operação assistida, embora seja obrigatória, ocorrerá sob demanda a depender da necessidade da Prodam ou de cada órgão (Carona), ou seja, não há obrigatoriedade de aderir as licenças e os serviços em sua totalidade (60.000) na 1ª adesão a ARP. As adesões ocorrerão durante a vigência da ATA, considerando os quantitativos e necessidade de cada órgão.

2. VIGÊNCIA

2.1. O Registro de Preços terá vigência de 12 (doze) meses, a contar da data de última assinatura ou da sua última assinatura digital, podendo ser prorrogada, nos termos art. 99 do Decreto Municipal nº 62.100, de 27 de dezembro de 2022.

2.2. Os contratos originados durante o período de vigência deste Registro de Preços terão vigência por 02 (dois) anos a contar de sua última assinatura ou da sua última assinatura digital, podendo ser prorrogado conforme dispõe o art. 71 da Lei Federal nº 13.303/2016.

2.3. Durante o período de vigência, estarão inclusas todas as atualizações necessárias para o perfeito funcionamento da solução.

3. ESPECIFICAÇÃO TÉCNICA

3.1. A solução deverá atender aos requisitos técnicos mínimos abaixo indicados e as seguintes CARACTERÍSTICAS GERAIS:

3.1.1. Deverá ser fornecido um painel de eventos, inspeção e segurança de credenciais/usuários.

3.1.2. O painel deverá possuir um mecanismo nativo para gestão de usuários que podem acessar o painel de visualização, incluindo integração nativa com os seguintes sistemas de diretório de usuários: Active Directory, LDAP e Keycloak/RH-SSO.

3.1.3. O painel deverá ser desenvolvido em tecnologia web based, acessível através de protocolo https, e possuir compatibilidade comprovada com o objeto.

3.1.4. O painel deverá criptografar com chave simétrica toda a comunicação com as fontes geradoras de eventos, e ao armazenar eventos em base de dados, anonimizar o campo que contém a informação de nome de usuário, seja este um CPF, matrícula, e-mail ou uma string (ex: nome.sobrenome).

3.1.5. As informações disponibilizadas no painel de visualização deverão ser orientadas a intervalo de datas, e fornecer estatísticas dos eventos de segurança que são protegidas pela solução, tais como: Usuários que mais geram eventos de segurança no ambiente protegido; Endereços IPs que mais geram eventos de segurança no ambiente protegido; Incidentes de segurança mais frequentes;

3.1.6. O painel deverá permitir visualizar detalhes de cada evento de segurança coletado;

3.1.7. Permitir filtrar eventos por usuário (credencial);

3.1.8. Permitir filtrar eventos por endereço IP de origem entre outros.

3.1.9. Deverá ser fornecido 02 (duas) unidades de appliance físico para atender ao volume de usuários estabelecido no quadro de itens, o appliance deverá ter o dimensionamento (size) definido pelo fabricante.

3.1.10. Os equipamentos deverão possuir quantidade de memória e processamento suficientes para atender a todas as funcionalidades e desempenho solicitados neste termo de referência.

3.2. ITEM 1 - Appliance (02 - hardware dedicado) de inspeção de segurança

3.2.1. Deverá ser fornecido 02 (duas) unidades de appliance (hardware dedicado) redundantes, a fim de garantir que, caso haja quaisquer intercorrências, a segunda unidade instalada suportará a disponibilidade dos serviços contemplados na solução;

3.2.2. Deverá possuir instalado e licenciado no mínimo 2 (duas) portas de comunicação Ethernet de velocidade de 10 Gigabit por segundo;

3.2.3. Deverá possuir instalado e licenciado no mínimo 2 (duas) portas de comunicação Ethernet de velocidade de 1 Gigabit por segundo;

3.2.4. O equipamento deverá ser instalado em rack com largura padrão de 19 polegadas;

3.2.5. Deverá possuir instalado, no mínimo, 64 (sessenta e quatro) núcleos físicos x86_64;

3.2.6. Deverá possuir instalado no mínimo 1024 (mil e vinte e quatro) GB de memória RAM DDR4 ECC REG;

3.2.7. Deverá possuir instalado no mínimo 02 (dois) discos rígidos do tipo SSD (Solid State Drive) de no mínimo 30TB cada;

3.2.8. Deverá dispor de fonte de alimentação redundante hot-swap com tensão de entrada de 110V / 220V AC automática padrão Hot swap;

3.2.9. Deverá dispor de recurso para gerenciamento padrão Lights-Out-Management, IPMI v2.0 ou similar, com interface de rede Ethernet RJ-45 dedicada;

3.2.10. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

3.2.11. Possuir pelo menos 2 (duas) portas USB para conexão de dispositivos externos;

3.2.12. Deverá suportar no mínimo 120.000 (cento e vinte mil) de conexões simultâneas;

3.2.13. Deverá suportar no mínimo 500.000 (quinhentas mil) novas conexões por segundo;

3.2.14. O throughput total do appliance deverá ser no mínimo de 44Gbps em full-duplex;

3.2.15. Deverá realizar rotinas internas diárias de backup e permitir backup remoto de configuração;

3.3. ITEM 2 – Suporte técnico, manutenção e garantia do item 1 - appliance (hardware dedicado) para inspeção de segurança para 24 (vinte e quatro) meses

3.3.1. Os serviços de suporte técnico e garantia abrangem: Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;

3.3.2. Os serviços de suporte técnico e garantia abrangem todas as soluções fornecidas pela contratada no âmbito dessa contratação;

3.3.3. Os serviços de suporte técnico poderão ser prestados de forma remota ou presencial no endereço da CONTRATANTE;

3.3.4. Os bens e produtos adquiridos devem ser licenciados de forma que o suporte e a garantia permitam as atualizações dos sistemas e ferramentas durante a vigência do contrato.

3.3.5. Deverão estar incluídas tanto as atualizações de segurança, quanto as atualizações para novas versões dos softwares licenciados, quando disponibilizadas, independente da política de comercialização do fabricante;

3.3.6. Todos os sistemas ou ferramentas que fazem parte da solução deverão ser disponibilizados na versão mais recente disponibilizada pelo fabricante;

3.3.7. A CONTRATADA deve garantir que todas as personalizações e configurações realizadas sejam automaticamente portadas para novas versões em caso de atualização, reinstalação ou upgrade, dispensando a necessidade de migrações ostensivas e onerosas, sem ônus para a CONTRATANTE.

3.3.8. Os serviços de manutenção, garantia, atualização e suporte técnico da solução deverão ser realizados durante toda a vigência contratual, a partir da data de emissão do Termo de Aceite e Recebimento referente à implantação e operacionalização da solução no ambiente tecnológico da PRODAM, e deverá contemplar obrigatoriamente no mínimo:

3.3.8.1. A realização dos serviços pelo período (em meses) indicado no quadro de itens do presente termo de referência;

3.3.8.2. As novas versões do objeto contratado deverão ser disponibilizadas em até 5 (cinco) dias corridos, a partir do lançamento oficial da versão.

3.3.9. Caso os serviços de manutenção e suporte técnico para todos os componentes da solução não forem executados diretamente pela Contratada, mas sim pelo próprio Fabricante ou por empresa(s) representante(s) ou credenciada(s) por este, a Contratada deverá comunicar tal fato à PRODAM, e assegurar que todos os padrões de atendimento e demais requisitos contratuais serão cumpridos. O aceite por parte da PRODAM do atendimento não exime a Contratada da responsabilidade integral pelo atendimento e cumprimento dos prazos acordados.

3.3.10. Somente serão aceitas soluções originais do fabricante dos componentes da solução.

3.3.11. O objeto do presente termo de referência deverá ter garantia total com suporte técnico 24x7 de 24 (vinte e quatro) meses, no mínimo, on-site.

3.3.12. O prazo de garantia técnica iniciará na data de emissão do Termo de Aceite e Recebimento;

3.3.13. Durante a garantia a contratada deverá prestar assistência técnica e responsabilizar-se pela integralidade e bom funcionamento do objeto do contratado.

3.3.14. A garantia deve prever que a contratada é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o

objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

3.3.15. O atendimento deverá ser sob o regime 24x7 (24 horas por dia,7 dias na semana), com disponibilidade de Central de Atendimento para abertura de chamados via sistema, e-mail, ligação gratuita (“0800”) ou por Ordem de Serviço (O.S.).

3.3.16. O acesso para ‘downloads’ de ‘patches’, ‘fixes’, ‘drivers’ e quaisquer outras atualizações necessárias, devem estar disponíveis 24x7 (vinte e quatro horas por dia, sete dias por semana), durante todo o período de suporte, e podem ser feitos através de http ou ftp, no sítio do fabricante do ‘software’;

3.3.17. A Contratante deve ter o direito de realizar a atualização do software durante todo o período de suporte técnico, por uma versão mais recente quando disponibilizada, e sempre que julgar necessário. As novas versões devem estar disponíveis para ‘download’, no sítio do fabricante do ‘software’;

3.3.18. Caso seja necessária a utilização de senha para ‘download’ de ‘patches’, ‘fixes’, ‘drivers’ e quaisquer outras atualizações no sítio do fabricante do ‘software’, esta deverá ser fornecida diretamente à Contratante, durante todo o período de manutenção;

3.3.19. Todo e qualquer licenciamento deverá ser feito em nome da Contratante, durante todo o período de manutenção;

3.3.20. A vigência contratual abrangerá a prestação de suporte, manutenção e atualização da solução pelo período de 24 (vinte e quatro) meses a partir da emissão do Termo de Aceite e Recebimento.

3.3.21. Durante o período de vigência contratual, o licitante vencedor deverá atender às solicitações da CONTRATANTE, em qualquer horário, respeitando as condições e níveis de serviço especificados.

3.3.22. Entende-se por “Garantia” ou “Suporte” ou “Manutenção”, doravante denominada unicamente como “Garantia”, toda atividade do tipo “corretiva” não periódica que variavelmente poderá ocorrer, durante todo o período de garantia; esta possui suas causas em falhas e erros no hardware ou software, e trata da correção dos problemas atuais e não iminentes de desenvolvimento do mesmo. Esta “Garantia” inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, devendo contemplar, sem nenhum ônus, as seguintes atividades incluindo, mas não se limitando a:

3.3.22.1. Recuperação de desastres, desinstalações, reconfigurações ou reinstalações decorrentes de falhas de software ou hardware;

3.3.22.2. Atualização da versão de software – toda e qualquer evolução incluindo correções em bibliotecas, “patches”, “fixes”, “service packs”, “releases”, “versions”, “builds”, vacinas extras específicas, “updates”, “upgrades”, e englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado;

3.3.22.3. Qualquer correção decorrente de erros ou falhas cometidas na execução dos serviços contratados e/ou decorrentes de integração e adequação sistêmica, desde que, comprovadamente, não tenham se dado em função de falhas nas especificações feitas pela PRODAM.

3.3.22.4. Os serviços de manutenção e suporte técnico deverão ser executados com base nos seguintes parâmetros:

3.3.23. Modalidade de Atendimento

MODALIDADE	DESCRIÇÃO
Atendimento Telefônico (Help Desk)	Chamados abertos através de ligação telefônica, e-mail ou sistema Web, em regime de 24x7: 24 horas por dia, 7 dias por semana.
Atendimento Remoto	Atendimento remoto de chamados técnicos, por meio de acesso remoto via VPN, "TeamViewer", "Cisco Webex" "SysAid" ou outra ferramenta similar, desde que tecnicamente viável e mediante autorização expressa da PRODAM conforme os padrões de segurança do Instituto, objetivando análise e solução remota dos problemas apresentados.
Atendimento Presencial (on-site)	Atendimentos técnicos executados nas dependências da PRODAM, através de visita de profissional especializado, com a finalidade de resolver os chamados.

3.3.24. Quando couber, no caso de atendimento remoto por meio de ferramenta adequada (via VPN, por exemplo), este deverá ser comunicado previamente à CONTRATANTE, que efetuará o cadastramento do responsável pelo atendimento, e disponibilizará os recursos necessários para a execução da demanda.

3.3.25. Todo o serviço de suporte técnico/manutenção deve ser solicitado inicialmente via Help Desk, ficando a transferência do atendimento para o Atendimento Remoto condicionado à autorização da PRODAM.

3.3.26. Todo o serviço de suporte técnico/manutenção solicitado inicialmente via Help Desk, deve ser transferido para o Atendimento Presencial quando o atendimento do Help Desk não for suficiente para solução do problema sem a intervenção presencial de um técnico.

3.3.27. Definição de prazos

PRAZO	DESCRIÇÃO
Início de Atendimento	Período que compreende o tempo entre o registro de abertura do chamado técnico até o primeiro contato do técnico e/ou comparecimento de um técnico ao local (quando necessário).
Solução de Contorno	Período compreendido entre o "Início de Atendimento" e a apresentação de solução de contorno, sendo definida como uma alternativa que viabilize a operacionalização do ambiente até o

	tratamento definitivo do incidente.
Solução Definitiva	Período decorrente entre o "Início de Atendimento" até omomento em que a solução for disponibilizada em plena e perfeita condição de funcionamento no local onde está implantada, estando condicionada à aprovação e ateste da equipe técnica da PRODAM, conforme o caso.

3.3.28. A critério da PRODAM o Início do Atendimento, assim como sua execução poderá ser agendado ou adiado e, nestes casos, a contagem de horas para a resolução do chamado fica prorrogada para ser contabilizada a partir da data do novo agendamento.

3.3.29. A Contratada poderá solicitar a prorrogação de qualquer dos prazos de início e término de atendimento de chamados, desde que o faça antes do seu vencimento e com a devida justificativa.

3.3.30. Níveis de Severidade

SEVERIDADE	DESCRIÇÃO	ATENDIMENTO
CRÍTICA	Incidente que ocasiona a inoperância total da solução ou de algum componente, com a indisponibilidade para qualquer tipo de funcionalidade, comprometendo de forma crítica o ambiente negocial da PRODAM.	Os chamados de Severidade CRÍTICA deverão ser atendidos a qualquer hora do dia ou da noite (cobertura 24x7), seja em dia útil, final de semana ou feriado, e não poderão ser interrompidos até a recuperação plena do funcionamento da Solução, mesmo que se estenda para períodos noturnos e dias não úteis como sábados, domingos e feriados. O atendimento cuja severidade for classificada como CRÍTICA deverá ser realizado obrigatoriamente ON-SITE.
ALTA	Incidente que ocasiona a inoperância parcial da solução ou de algum componente, com o comprometimento do funcionamento e/ou performance da solução, porém sem interrupção completa.	Os chamados de Severidade ALTA deverão ser atendidos a qualquer hora do dia ou da noite (cobertura 24 x 7), seja em dia útil, final de semana ou feriado e não poderão ter o atendimento interrompido até a recuperação plena do funcionamento da Solução, mesmo que se estenda para períodos noturnos e dias não úteis como sábados, domingos e feriados.Os chamados de Severidade ALTA poderão ser opcionalmente

		atendidos on- site a critério da PRODAM.
MÉDIA	Incidente que não ocasiona indisponibilidade do sistema, contudo afeta de modo significativo a performance desta, sendo preliminarmente solucionado temporariamente mediante aplicação de solução de contorno disponível.	Os chamados de Severidade MÉDIA deverão ser atendidos em dias úteis, em horário comercial (das 8:00 às 18:00), e opcionalmente em final de semana ou feriado, conforme agendamento prévio.
BAIXA	Atividades que não impactam na disponibilidade da solução, como diagnósticos, configurações, consultas técnicas, esclarecimentos.	Os chamados de suporte de Severidade BAIXA opcionalmente poderão ser atendidos em dias úteis, em horário comercial (das 8:00 às 18:00).

3.3.31. A severidade do chamado poderá ser reavaliada quando verificado que esta foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e resolução.

3.3.32. Acordo de Nível de Serviço

Para o atendimento das atividades demandadas, a Contratada deverá atender os seguintes prazos constantes no quadro a seguir, conforme o nível de severidade aplicado:

SEVERIDADE	INÍCIO DE ATENDIMENTO	SOLUÇÃO DE CONTORNO	SOLUÇÃO DEFINITIVA
CRÍTICA	Até 2 horas	Até 24 horas	Até 72 horas
ALTA	Até 4 horas	Até 48 horas	Até 96 horas
MÉDIA	Até 8 horas	Até 72 horas	Até 120 horas
BAIXA	Até 12 horas	Até 96 horas	Até 240 horas

3.3.32.1. Casos em que a Contratada não puder executar os serviços de suporte até o limite dos prazos de atendimento, tais chamados não atendidos deverão ser devidamente documentados, contendo a justificativa da Contratada e o aceite do Gestor, observando-se o preceito da razoabilidade e considerando-se os prejuízos à Contratante. Em caso de não aceite da justificativa por parte da Contratante, serão aplicadas as penalidades cabíveis à Contratada.

3.3.32.2. O não atendimento a um chamado técnico somente poderá ser justificado em casos de motivo de força maior ou por dependência da CONTRATANTE; neste caso, a Contratada deverá formalizar antecipadamente ao Gestor do Contrato ou ao Fiscal Técnico os motivos que impedem a execução do serviço demandado.

3.3.32.3. Todos os serviços deverão ser prestados em consonância com as melhores práticas e recomendações de mercado e do Fabricante da solução.

3.3.32.4. Um chamado técnico só poderá ser dado como concluído após verificação e aceite do responsável da CONTRATANTE.

3.3.32.5. Chamados fechados sem anuência da Contratante ou sem que a(s) demanda(s) tenha(m) sido de fato resolvida(s) deverão ser reabertos e os prazos contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.

3.3.32.6. A Contratada deverá manter um cadastro das pessoas indicadas pela Contratante, as quais poderão efetuar abertura e autorizar o fechamento de chamados.

3.3.32.7. Cada pessoa cadastrada no sistema deverá receber identificação e senha que permitam acesso seguro ao sistema de informação da Contratada, de maneira a evitar que pessoas não autorizadas possam acionar o serviço.

3.3.32.8. A conclusão do atendimento técnico se dará quando ocorrer a "Solução Definitiva" do problema mencionado no chamado (Severidades CRÍTICA, ALTA e MÉDIA), e/ou sanando a dúvida (Severidade BAIXA), estando a conclusão condicionada à aprovação do Fiscal Técnico do Contrato.

3.3.32.9. É vedado à Contratada interromper o atendimento até que o serviço seja recolocado em pleno estado de funcionamento, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados, não cabendo custos adicionais à Contratante.

3.3.32.10. Em caso de vício(s) insanável(is) nos componentes da solução que impossibilitem o funcionamento da solução de segurança, o(s) componente(s) defeituoso(s) deverá(ão) ser substituído(s) definitivamente em até 10 (dez) dias úteis após a notificação da Contratante, juntamente com a descrição sucinta e precisa do problema ocorrido.

3.3.32.11. Sempre que houver quebra de Acordo de Nível de Serviços, a Contratante emitirá notificação à Contratada, que terá prazo máximo de 5 (cinco) dias corridos, contados a partir do recebimento do ofício, para apresentar as justificativas para as falhas verificadas. Caso não haja manifestação dentro desse prazo ou caso a Contratante entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme o nível de serviço transgredido.

3.3.32.12. Na ocorrência de uma situação emergencial na qual já exista chamado técnico aberto, é esperado que tanto o atendimento quanto o restabelecimento da solução sejam feitos de forma imediata, sem a necessidade de abertura de novo chamado técnico.

3.3.32.13. Chamados fechados sem anuência da Contratante ou sem que a(s) demanda(s) tenha(m) sido de fato resolvida(s) deverão ser reabertos e

os prazos contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.

3.3.32.14. Os chamados técnicos só poderão ser encerrados após expressa anuência do Gestor do Contrato ou do Fiscal Técnico.

3.3.32.15. Chamados fechados sem anuência da PRODAM ou sem que a(s) demanda(s) tenha(m) sido de fato resolvida(s) deverão ser reabertos e os prazos contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.

3.3.32.16. A Contratada deverá manter um cadastro das pessoas indicadas pela PRODAM, as quais poderão efetuar abertura e autorizar o fechamento de chamados.

3.3.32.17. Cada pessoa cadastrada no sistema deverá receber identificação e senha que permitam acesso seguro ao sistema de informação da Contratada, de maneira a evitar que pessoas não autorizadas possam acionar o serviço.

3.3.32.18. No fechamento do chamado deverá ser emitido, por parte da Contratada, um "Relatório Técnico de Atendimento", a ser encaminhado à PRODAM, apresentando no mínimo as seguintes informações:

- Número de identificação do chamado;
- Data e hora do chamado;
- Data e hora do início e do término do atendimento;
- Total de horas utilizadas para atendimento completo;
- Severidade da ocorrência;
- Identificação do problema/incidente;
- Solução de contorno aplicada (quando couber);
- Solução definitiva aplicada.

3.4. ITEM 3 - Licenças de auditoria, análise de eventos e governança de dados para atender usuários/credenciais 60.000 pelo período de 24 meses

3.4.1. As licenças serão contratadas sob demanda, de acordo com as necessidades da CONTRATANTE;

3.4.2. Poderá ser contratada 01 (uma) ou mais licenças de acordo com a necessidade da CONTRATANTE;

3.4.3. As licenças serão utilizadas durante a vigência contrato;

3.4.4. A solução deverá ser de um único fabricante ou totalmente integrada através de console de visualização de eventos disponibilizados em uma única interface gráfica que forneça indicadores e possibilite auditorias de eventos.

3.4.5. Caso a solução ofertada necessite reter o log nativo de auditoria do Active Directory e Servidor de Arquivos, o hardware deverá garantir o armazenamento destes logs pelo período contratado, e deverá ser contemplado na proposta comercial.

3.4.6. A solução descrita neste item deve possuir as seguintes funcionalidades globais:

a) Auditar ações sobre objetos do Active Directory, Servidor de Arquivos Windows e aplicações web;
b) Executar ações proativas com base na auditoria, inclusive para múltiplos objetos;
c) Gerar alerta com base nas informações auditadas;
d) Automatizar tarefas repetitivas, comum ou complexas;
e) Monitorar e analisar comportamentos suspeitos de usuários.

3.4.7. A solução deve oferecer funcionalidades de permissão granular de acesso aos servidores de diretórios de usuários Microsoft Active Directory, permitindo a configuração de permissões detalhadas.

3.4.8. A solução deve ser capaz de gerar logs e relatórios detalhados das atividades realizadas nesses servidores, permitindo a análise do comportamento dos usuários por meio de uma interface de monitoramento unificada que integre dados de outros repositórios. Além disso, a solução deve emitir alertas em tempo real em caso de comportamentos suspeitos ou atividades maliciosas nos servidores de diretórios;

3.4.9. A solução deve disponibilizar uma console nativa, acessível por meio de um servidor de aplicação;

3.4.10. A solução deve apresentar KPIs de compliance relacionados aos recursos monitorados do Active Directory, permitindo a visualização das informações de segurança de forma clara e objetiva;

3.4.11. A solução deverá ser capaz de fornecer indicadores-chave de desempenho (KPIs) de conformidade de segurança em relação aos recursos monitorados no File Server.

3.4.12. A solução deve possuir visibilidade da hierarquia do serviço de Diretórios de Usuários através de interface gráfica;

3.4.13. A solução deve possuir a visibilidade de todos os domínios, Unidades Organizacionais, Computadores, Grupos e outros objetos do domínio através de uma única interface gráfica e igualmente sob forma de relatório;

3.4.14. A solução deve permitir a monitoração de vários domínios simultaneamente por meio de uma única console de gerência, que possibilite a auditoria dos diferentes domínios de forma centralizada;

3.4.15. Deve fornecer método para assinalar ou associar um ou mais usuários como "Proprietário(s)" de um grupo.

3.4.16. A solução deve permitir a configuração de diferentes níveis de acesso e segurança para suas funcionalidades, possibilitando o uso por diferentes equipes com demandas específicas e restrição de acesso à funções específicas de acordo com o perfil de cada usuário.

3.4.17. A solução deverá possuir as funcionalidades de permissionamento, registro de eventos, relatórios e análise comportamental dos usuários em

plataformas de servidores de arquivos Windows, NAS (Network Attached Storage) e diretório de serviços Active Directory;

3.4.18. A solução deve permitir aos usuários administrativos realizar as seguintes ações através da interface gráfica da solução:

a) Criar novos usuários;
b) Criar novos grupos de segurança;
c) Alterar parâmetros de usuários já existentes;
d) Alterar membros de grupos de segurança;
e) Excluir usuários;
f) Excluir computadores;
g) Reconfigurar senhas;
h) Desbloquear usuários; e
i) Habilitar e desabilitar usuários.

3.4.19. A solução deve permitir as ações abaixo, de uma só vez, através da seleção de múltiplos usuários:

a) Deleção;
b) Reset de senha;
c) Desbloqueio da conta;
d) Habilitação e desabilitação.

3.4.20. A solução deve suportar a utilização de servidores em ambiente virtualizado (VMWare Vsphere 6 ou superior) para todos os seus componentes;

3.4.21. A solução deve possibilitar a configuração de credencial diferente para cada servidor/serviço e volume a ser monitorado;

3.4.22. A solução deve permitir autenticação direta no Active Directory sem a necessidade de login a cada acesso do usuário à console;

3.4.23. A solução deve realizar a descoberta automática de contas privilegiadas de usuários administrativos, contas executivas e de serviço.

3.4.24. A solução deve ser capaz de automatizar o processo de remoção de acessos globais reduzindo a capacidade de dados;

3.4.25. Para servidor de arquivos:

a) A solução deverá fornecer funcionalidade de ajuste aos diretórios com herança de permissões quebradas, podendo o processo ser automatizado e agendado;

b) A solução deve permitir a criação de pastas que sejam reconhecidas automaticamente na interface gráfica e possam ser usadas pelos usuários sem a necessidade de configurações adicionais;

c) A solução deverá possuir compatibilidade no mínimo com as versões Windows Server 2008 e 2008-R2, Windows Server 2012 e 2012-R2.

d) Caso seja necessária a instalação de agente nos servidores de arquivos, este agente deve possuir um mecanismo de monitoramento de desempenho dos servidores onde atua, de modo a não permitir que o nível de consumo de recursos ultrapasse limites definidos e configuráveis;

3.4.26. A solução deverá disponibilizar no mínimo as funcionalidades de visibilidade dos dados, usuários e grupos de segurança, gerenciamento de permissionamento, auditoria e relatórios de todas as plataformas monitoradas que devem estar disponíveis em uma única interface gráfica integrada;

3.4.27. A solução deverá fornecer método para assinalar ou associar um ou mais usuários como "Proprietário(s)" de uma pasta.

3.4.28. A solução deverá mostrar em uma mesma interface toda a base de usuários e de dados monitorados, exibindo para cada pasta ou arquivo a visualização gráfica interativa das listas de controle de acesso incluindo grupos, subgrupos e seus respectivos membros, incluindo herança de permissão ativa/desativada e indicação de compartilhamento;

3.4.29. A ferramenta deverá prover filtros para visualizar todos os objetos de dados de forma gráfica incluindo pastas protegidas e únicas;

3.4.30. A ferramenta não deve restringir a quantidade das listas de acesso (ACLs) coletadas e/ou armazenadas;

3.4.31. A solução deverá possuir a opção de aplicação das alterações utilizando uma credencial diferente da credencial do usuário logado na interface gráfica assim, a modelagem pode ser feita por um usuário e efetivada por outro usuário, este último, com permissões de alterações no Active Directory;

3.4.32. A solução deverá permitir que seja salva a credencial de aplicação de alterações para uso futuro;

3.4.33. A solução deverá fornecer a visibilidade sobre aplicações de alteração que estão pendentes e o histórico das alterações aplicadas através da console;

3.4.34. A solução deve permitir a modelagem de permissionamento de maneira gráfica, incluindo a simulação do impacto de mudanças no permissionamento de grupos e usuários, e da remoção de permissões excessivas, inclusão de novos grupos e identificação de quais usuários serão afetados com estas trocas de permissões;

3.4.35. A solução ofertada deve manter o log das operações de abrir, criar, apagar, modificar, copiar, renomear e acesso negado

3.4.36. As ações dos usuários apresentadas pela solução, devem conter informações completas de cada uma das operações com:

a) data e horário;
b) nome do servidor;
c) tipo do objeto;
d) caminho (path) dos dados;
e) domínio;
f) objeto impactado; e
g) nome do usuário.

3.4.37. A solução deve permitir filtragem gráfica, ordenação e agrupamento dos logs;

3.4.38. A solução deverá identificar em uma mesma tela todas as atividades de um determinado usuário ou determinada pasta de todos os repositórios monitorados e diretórios de usuários;

3.4.39. A solução deve fornecer resumo gráfico das atividades auditadas, incluindo:

a) visualização dos usuários mais e menos ativos;
b) visualização dos diretórios mais e menos acessados;
c) visualização dos diretórios onde um usuário ou um grupo de usuários estejam acessando; e
d) visualização dos usuários que estejam acessando um diretório.

3.4.40. A solução deve permitir que os usuários realizem pesquisas baseados em critérios como:

a) data do evento;
b) servidor ou plataforma em que o evento ocorreu;
c) tipo de evento; e
d) arquivos ou diretórios acessados.
e) Classificação de dados sensíveis

3.4.41. A solução deve ter a capacidade de detectar informações confidenciais ou sensíveis em arquivos ou dados através da pesquisa de palavras-chave definidas em dicionários pré-definidos pelo fabricante ou personalizados pelo usuário;

3.4.42. A solução deve exibir na mesma interface gráfica das informações sobre permissionamento e ACL's, a quantidade de informações sensíveis e qual tipo de informação sensível classificada para facilitar a identificação de potenciais repositórios e pastas expostas;

3.4.43. A solução deve disponibilizar filtros de classificação de dados sensíveis nas consultas aos logs de auditoria e relatórios elaborados;

3.4.44. A solução deve possibilitar a visão, diretamente da aplicação, das expressões regulares ou strings que fizeram com que esse arquivo fosse considerado como sensível, para cada arquivo marcado;

3.4.45. A solução deve gerar recomendações de revogação de acesso aos dados classificados para redução de acesso às informações sensíveis;

3.4.46. A solução deve integrar a funcionalidade de classificação de dados sensíveis com soluções de terceiros para estender a habilidade de ambos;

3.4.47. A solução deve possibilitar a limitação de escopo dentro dos sistemas de arquivos a ser analisado;

3.4.48. A solução deve estar apta à configuração de um dicionário referente à Lei nº 13.709/2018 – Lei de Geral de Proteção de Dados (LGPD), de modo a proporcionar a identificação de arquivos que possuam informações sensíveis, tais como: nome, CPF, gênero, nacionalidade, telefone, endereço, CEP, data de nascimento, título de eleitor e carteira nacional de habilitação (CNH).

3.4.49. A solução deve permitir a definição de partes específicas do arquivo a serem analisadas no escopo, tais como:

a) Colunas específicas de arquivos Excel (xls);
b) Cabeçalho, rodapé e marca d'água de arquivos Microsoft Office; e
c) Links de arquivos Microsoft Office e PDF.

3.4.50. Permissionamento:

3.4.50.1. A solução deve permitir que as alterações sejam aplicadas por meio de uma credencial distinta daquela utilizada pelo usuário logado na interface gráfica. Dessa forma, um usuário pode modelar as alterações e outro usuário com permissões para alterar o Active Directory pode efetivá-las;

3.4.50.2. A solução deverá permitir que seja salva a credencial de aplicação de alterações para uso futuro;

3.4.50.3. A solução deve permitir o rastreamento das alterações solicitadas que aguardam aprovação e manter um histórico das alterações já aplicadas, acessível através da aplicação;

3.4.50.4. Deve possibilitar a visibilidade total sobre o serviço de diretório de usuários, a estrutura do diretório e permissões de usuários e grupos, assim como objetos do Active Directory on-premise;

3.4.50.5. Deve ser possível diferenciar e consultar os objetos do Active Directory on–premise.

3.4.51. Registro de Eventos (LOG):

3.4.51.1. A solução deverá fornecer todas as funcionalidades citadas abaixo sem a necessidade de retenção dos logs nativos do Windows. Caso a solução ofertada necessite habilitar o log de auditoria do Windows File Server, o hardware deverá garantir o armazenamento destes logs pelo período contratado, e deverá ser contemplado na proposta comercial.

3.4.51.2. Visibilidade de todos os domínios, unidades organizacionais, computadores, grupos e outros objetos do domínio;

3.4.51.3. A solução deve ser capaz de exibir a trilha de auditoria de todas as atividades do Active Directory; contendo informações de quem realizou as alterações no Active Directory, qual alteração realizada e quando ocorreu.

3.4.51.4. A solução deve fornecer uma console única para visibilidade de permissionamento que apresente todos os eventos de todos os usuários e plataformas monitoradas;

3.4.51.5. A solução deve coletar os eventos das plataformas monitoradas de forma contínua e automática;

3.4.51.6. A solução deverá manter o registro das operações do servidor de arquivos de abrir, criar, apagar, modificar, copiar, renomear e acesso negado;

3.4.51.7. As ações dos usuários apresentadas pela solução, devem conter informações completas de cada uma das operações com: data e horário nome do servidor, tipo do objeto, caminho (path) dos dados, domínio, objeto impactado e nome do usuário.

3.4.51.8. A solução deve permitir filtragem gráfica, ordenação e agrupamento dos logs;

3.4.51.9. A solução deve fornecer resumo gráfico das atividades auditadas, incluindo a visualização dos usuários mais e menos ativos;

3.4.51.10. A solução deve permitir que os usuários realizem pesquisas baseados em critérios como: data do evento, servidor ou plataforma em que o evento ocorreu, tipo de evento e arquivos ou diretórios acessados.

3.4.51.11. A solução deve possibilitar alterar o conjunto de dados (colunas) retornados da consulta aos eventos de acordo com a necessidade da informação;

3.4.51.12. A solução deve suportar a auditoria dos seguintes eventos do Directory Service:

a) Criação de deleção de dos objetos;
b) Membros adicionados e removidos de grupos de segurança;
c) Alteração nas propriedades do objeto do AD;
d) Requisição de acesso;
e) Autenticação de conta;
f) Reset de senhas;
g) Bloqueio e desbloqueio de conta;
h) Criação e deleção de conta;
i) Habilitação e desabilitação de conta;
j) Permissão adicionada e removida a objeto do AD;
k) Proprietário alterado;
l) Modificação de configuração de GPO (Group Policy);
m) Criação, alteração e deleção de link de GPO (Group Policy).

3.4.52. Relatórios:

3.4.52.1. A solução deverá gerar relatórios nos formatos CSV, HTML, XLS e PDF;

3.4.52.2. A solução deverá permitir que relatórios sejam extraídos sob demanda uma única vez ou agendados e enviados com frequência definida;

3.4.52.3. A solução deverá permitir o agendamento para envio de relatórios pelo correio eletrônico ou para um compartilhamento no servidor de arquivos;

3.4.52.4. O envio dos relatórios por e-mail deve ser feito a partir da própria solução, ou seja, sem a utilização de software de terceiros e deve suportar o protocolo SSL sobre SMTP;

3.4.52.5. Permitir, no mínimo, a emissão dos seguintes relatórios:

3.4.52.6. Relatório de todas as permissões de determinado usuário nos repositórios monitorados.

3.4.52.7. Relatório de usuários inativos;

3.4.52.8. Relatório de usuários desabilitados que ainda fazem parte de grupos de segurança;

3.4.52.9. Relatório de histórico de membros de grupos de segurança;

3.4.52.10. Relatório de estatísticas, métricas e gráficos com informações sobre usuários, grupos e permissões ao longo de determinado período;

3.4.52.11. Relatório de estatísticas de autenticação e falha de autenticação;

3.4.52.12. Relatório de lista de usuários administradores em grupos não administrativos;

3.4.52.13. Relatório dos alertas de comportamento anômalo identificados;

3.4.52.14. Relatório de auditoria das ações dos usuários na console;

3.4.52.15. Relatório sobre as alterações, versão alterada e quais foram as mudanças realizadas em GPOs (Group Policy).

3.4.52.16. Relatório de todos os usuários com permissões em determinada pasta.

3.4.52.17. Relatório dos acessos aos arquivos;

3.4.52.18. Relatório de onde há permissões concedidas a grupos globais (Everyone, Domain Users, Users, Authenticated Users);

3.4.52.19. Relatório de SIDs não resolvidos e usuários com permissão direta em pastas;

3.4.52.20. Relatório de dados inativos;

3.4.52.21. Relatório de histórico de permissões;

3.4.52.22. Relatório de estatísticas, métricas e gráficos com informações sobre pastas e permissões ao longo de determinado período;

3.4.52.23. Relatório comparativos dos sistemas de arquivos monitorados;

3.4.52.24. Relatório de lista de permissões de usuários desabilitados;

3.4.52.25. Relatório de pastas sem administradores;

3.4.52.26. Relatório dos alertas de comportamento anômalo identificados;

3.4.52.27. Relatório com as recomendações de revogação de permissão gerados pela análise comportamental realizada sobre os usuários e recursos monitorados;

3.4.52.28. Relatório de estatística de acesso, utilização por tipo de arquivos, eventos por usuários e distribuição por tipos de eventos;

3.4.52.29. A solução deverá disponibilizar as informações produzidas sobre dados sensíveis sob formato de relatórios;

3.4.53. Alertas:

3.4.53.1. A solução, com base nos dados de auditoria, deve ser capaz de assimilar o comportamento padrão dos usuários e dos recursos monitorados, de modo que desvios e anormalidades nesses comportamentos sejam identificados automaticamente;

3.4.53.2. A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos – ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar acesso a dados que o usuário usualmente não acessa;

3.4.53.3. Os alertas devem ser apresentados também em dashboard web que apresente:

a) quantidade de alertas e suas severidades em determinado período,
b) usuários mais alertados em determinado período,
c) tipos de alertas que mais ocorreram,
d) máquinas que forma mais utilizadas para as ações suspeitas,

3.4.53.4. O dashboard deve apresentar os eventos que motivaram o alerta para que o time de segurança possa fazer investigação forense;

3.4.53.5. A lista desses eventos deve ser customizável, podendo ser filtrada, exibidas ou ocultadas colunas e agregada por valores das colunas exibidas;

3.4.53.6. A solução deve possibilitar, nos alertas em tempo real, configurar para que um usuário, uma pasta, um período ou uma ação específica seja alertada caso ocorra ação que os envolva;

3.4.53.7. A solução deve permitir que sejam configurados alertas em tempo real para eventos da auditoria habilitada;

3.4.53.8. A solução deve possibilitar que os alertas serão iniciados com base nos dados da auditoria, tais como usuário, ação, data e hora, ação realizada;

3.4.53.9. A solução deverá possuir a capacidade de monitorar, analisar e emitir alertas sobre comportamentos anômalos em servidores de arquivos Windows;

3.4.53.10. A solução deve contemplar a assinatura de uma base de conhecimentos do fornecedor de alertas pré- configurados de eventos suspeitos tais como:

a) excessos de ações com acessos negadas;
b) tentativas de elevação de privilégios;
c) excesso de tentativas de autenticação ou contas bloqueadas;
d) excesso de atividades em dados parados e/ou inativos;
e) alterações anormais em GPO (Group Policy);
f) excesso de ações em um curto espaço de tempo.
g) atividades anômalas;
h) grupos de segurança, GPO's (Group Policy) e outros objetos de Active Directory modificados ou removidos;
i) escalações de privilégios; e
j) modificação de permissões em diretórios de usuários;
k) classificação dos alertas dentro de um cenário de ataque cibernético.

3.4.53.11. O dashboard deve mostrar as propriedades do Active Directory do usuário alertado, que são essenciais para a análise forense do alerta gerado;

3.4.53.12. Para análise forense do usuário mais alertado, o dashboard deve possuir página que agregue dados importantes do comportamento daquele usuário;

3.4.53.13. A solução deve ser capaz de alertar quando houver modificações de permissões em diretórios de usuários;

3.4.53.14. A solução deve contemplar a assinatura de uma base de conhecimentos do fornecedor de alertas pré- configurados de eventos suspeitos tais como:

a) ataques de sequestro de dados (ransomware);
b) detecção de ferramentas nocivas ao ambiente;
c) excessos de ações com acessos negadas;
d) acessos indevidos dos administradores nos dados da empresa;
e) excesso de atividades em dados parados e/ou inativos;
f) excesso de ações em um curto espaço de tempo.
g) atividades anômalas;
h) acesso a dados sensíveis;
i) arquivos sensíveis são acessados ou excluídos;

3.4.53.15. A solução deve ser capaz de alertar e enviar email para acesso a dados sensíveis;

3.4.53.16. A solução deverá fornecer sistema de alerta em tempo real, capaz de alarmar atividades em sistema de arquivos (File Server), para no mínimo:

a) deleção;
b) abertura;
c) movimentação; e
d) acessos negados.

3.4.53.17. A solução deverá fornecer sistema de alerta em tempo real deve ser capaz de alarmar atividades em ambiente Active Directory, para no mínimo:

a) elevação de privilégios, e
b) inclusão/exclusão de grupos e usuários;

3.4.53.18. Os alertas devem ser gerados em SNMP, Syslog, visualizador de eventos do Windows, E-mail e devem ser capazes de realizar a execução de um script previamente configurado.

3.4.54. Análise Comportamental

3.4.54.1. A solução deve realizar a análise comportamental dos usuários e fazer recomendações de alteração, revogação de acesso, trocas de grupos e permissões aos dados não estruturados dos servidores monitorados;

3.4.54.2. A solução deve identificar, de modo automático, usuários com acesso a pastas e/ou arquivos indevidos sugerindo a revogação de acesso;

3.4.54.3. A solução deve fornecer em modo gráfico recomendações sobre permissionamento excessivo, baseado na análise de atividade de acesso;

3.4.54.4. A solução deve permitir identificação gráfica de atividades de acesso anormais;

3.4.54.5. A solução deverá ser capaz de analisar em tempo real e prevenir comportamentos suspeitos em aplicações web, mesmo que estas não estejam integradas ao Active Directory, atendendo minimamente os seguintes requisitos:

a) Comunicar-se através de API HTTP REST ou UDP com a aplicação web protegida, calculando e fornecendo em tempo real um score de risco e o nível de risco que este score representa, para cada evento de autenticação que ocorre em uma dada aplicação.

b) Assegurar a comunicação entre a solução e a aplicação web protegida através de criptografia de chaves simétricas.

c) Possibilitar a criação e configuração de políticas de risco, possuindo no mínimo 4 níveis de risco parametrizáveis a serem definidos em cada política.

d) Fornecer para cada autenticação analisada o score de risco processado acompanhado da ação (permitir, notificar, desafiar ou bloquear) indicada para o nível de risco do evento em questão, de acordo com a política definida.

e) Possibilitar o agrupamento de credencias, de modo que uma credencial possa estar associada a mais de uma aplicação web protegida.

f) Não exigir tokens, dispositivos móveis, códigos ou outras informações adicionais para o processamento de eventos.

g) Ser capaz de processar e fornecer o score de risco tanto para autenticações com a credencial e senha corretos como para autenticações com credencial e/ou senha incorretos.

h) possuir uma base de inteligência de segurança para ser utilizada na mensuração do risco dos acessos, construída com informações próprias e públicas (OSINT), de modo a identificar IPs de má reputação e/ou utilizados para serviço de proxy.

i) Realizar a mensuração de risco no processo de autenticação sem armazenar e sem ter acesso a senha da credencial em questão, em nenhuma hipótese.

j) Construir padrão de comportamento de uma credencial com base no histórico de seu uso, composto minimamente por navegador, dispositivo, localização geográfica (cidade e país), sistema operacional, identificador do provedor de internet.

k) Identificar desvios no padrão de comportamento de uma credencial, possibilitando o envio de notificações, apresentação de desafios (token, captcha ou similares) e bloqueio de acesso, a depender da política de risco definida.

l) Realizar a mensuração de risco de todos os acessos levando em consideração o padrão de comportamento da credencial e a base de inteligência de segurança.

m) Todos os eventos processados e armazenados pela solução deverão ser georreferenciados de acordo com o endereço IP de origem, contendo minimamente país, cidade, latitude e longitude.

n) Permitir a notificação de usuários com base em política de risco, através do disparo via SMTP de e- mail, possibilitando a redação de mensagem personalizada em editor HTML, contendo detalhes do evento em questão como cidade de acesso, data e hora, ip de origem, navegador e um link para que o usuário responda se reconhece o acesso ou não.

o) Inserir no padrão de comportamento da credencial novas informações quando o usuário confirma através da notificação recebida a veracidade do acesso.

p) Possibilitar o envio de e-mail para administrador quando um usuário nega a veracidade de um acesso através da notificação recebida.

q) Ser capaz de bloquear o processo de autenticação de usuários com base no score de risco do evento, mesmo quando a credencial e a senha forem corretamente imputadas no ato da autenticação.

r) Identificar ataques do tipo “força bruta”, elevando de forma automática e proporcional o score de risco do IP de origem do acesso com base no número de tentativas de autenticações fracassadas em um curto intervalo de tempo.

s) A reputação das origens detectadas como geradores de ataques de força bruta deverá decair após determinado tempo, e o tempo de decaimento da reputação deverá aumentar em função da recorrência de tentativas de ataques de força bruta.

t) Enviar eventos, cifrados nativamente com chave simétrica, via webhook para URL a ser configurada em interface gráfica, com base na política de risco definida.

u) Elevar o score de risco de uma credencial ao detectar mudança geográfica de longa distância.

v) Identificar os top 10 usuários que representam maior atividade de risco acumulado em um intervalo de tempo escolhido, informando o nome do usuário (credencial) e score de risco acumulado.

w) Segmentar os eventos processados por credencial, possibilitando navegar por todos os eventos de uma dada credencial, informando no mínimo os seguintes detalhes de cada evento: Cidade, coordenadas geográficas, nome do navegador utilizado, nome do dispositivo utilizado no acesso, endereço ip de origem, score de risco e resultado da ação com base na política definida, código identificador do ISP (internet service provider) e descritivo com análise do evento.

x) Possuir gráfico que represente os eventos de uma credencial específica em um intervalo de tempo escolhido, distinguindo-os pelos níveis de risco definidos em política.

y) Possuir dashboard para visualização de eventos no formato de representação de mapa geográfico que possibilite distinguir diferentes níveis de risco, detalhando informações como cidade, usuário, score de risco do evento, data e hora do evento.

z) Possuir dashboard para visualização do risco organizacional em um intervalo de tempo escolhido, segmentado por aplicação protegida ou não, distinguindo o volume de eventos que representam o risco mitigado, o risco em mitigação (pendente) e o risco assumido.

aa) Possuir integração com soluções do tipo "single- sign-on", disponibilizando no mínimo, de forma nativa, o RH-SSO e Keycloak.

bb) Possuir integração nativa com a autenticação de tecnologias de mercado, sendo minimamente wordpress, openssh, cloudflare, moodle e keycloak.

cc) Ser capaz de processar eventos originados em IPv4 e IPv6.

dd) Possuir identificador único para todos os eventos processados pela solução.

ee) Possuir mecanismo de processamento e armazenamento de eventos baseado em tecnologias escaláveis.

ff) Possuir mecanismo de dissuasão de ataques de força-bruta baseado em desafio criptográfico a ser decifrado pelo navegador cliente, sem necessidade de interação dos usuários da aplicação protegida.

gg) O nível de dificuldade do desafio criptográfico deverá ser parametrizável.

3.4.54.6. Todas os softwares fornecidos deverão ser licenciados pelo período mínimo de 24 (vinte e quatro) meses, e contemplar garantia, suporte e atualização dos respectivos fabricantes.

3.4.54.7. O licenciamento fornecido deverá atender a quantidade de usuário /credencial indicado na Tabela de Composição de Itens do presente termo de referência;

3.5. ITEM 4 – Serviço de Instalação e Configuração

3.5.1. Os serviços de instalação e configuração deverão compreender, no mínimo:

a) a implantação completa do projeto, ou seja, deverão contemplar todos os componentes de hardware e software no ambiente tecnológico da PRODAM;

b) responsabilização por todos os instrumentais necessários durante o período de implantação e testes de aceitação;

c) instalação e configuração de todo ferramental tecnológico fornecido para atender as funcionalidades e requisitos descritos.

d) providenciar o planejamento de testes, fornecendo um "Plano de Homologação e Testes" contendo todo o processo de homologação dos

produtos e detalhamento dos testes que serão executados para validar a solução implementada;

e) execução de uma série de testes funcionais básicos para verificar o perfeito funcionamento do ambiente, seguindo os procedimentos definidos no "Plano de Homologação e Testes", sendo tais testes a serem obrigatoriamente executados nos componentes de hardware e software envolvidos no projeto;

f) elaboração da "Documentação e Finalização do Projeto", que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e ou gerencial.

3.5.2. Durante a implantação da solução, a Contratada deverá realizar, entre outras atividades: instalação física dos appliances e instalação de softwares.

3.5.3. Caberá à Contratada a disponibilização de todos os recursos necessários, tais como hardwares, softwares, recursos humanos necessários à instalação da solução.

3.6. ITEM 5 - SERVIÇO DE OPERAÇÃO ASSISTIDA – PELO PERÍODO DE 23 MESES

3.6.1. O Serviço de Operação Assistida será contratado sob demanda, de acordo com as necessidades da CONTRATANTE;

3.6.2. Para cada licença será contratado 01 (um) Serviço de Operação Assistida;

3.6.3. Poderá ser contratado 01 (um) ou mais serviços de operação, de acordo com a necessidade da CONTRATANTE;

3.6.4. O serviço será prestado durante a vigência contrato;

3.6.5. O serviço de operação assistida servirá para que a contratada, através de equipe própria e comprovadamente especializada na solução, execute serviços inerentes às rotinas técnicas operacionais dos softwares fornecidos.

3.6.6. O serviço de operação assistida deverá ser executado remotamente ou, quando solicitado, pontualmente presencial.

3.6.7. A execução dos serviços será mensal, pelo período (em meses) indicado no quadro de itens do presente termo de referência, tendo seu início definido a partir do segundo mês do contrato;

3.6.8. As seguintes atividades técnicas operacionais compõem o serviço de operação assistida:

3.6.9. Troubleshooting;

3.6.10. Apoio na investigação de incidentes, quando solicitado pela CONTRATANTE;

3.6.11. Backup de configurações;

3.6.12. Atualização de software ou aplicação de patch;

3.6.13. Análise, validação e aprovação de políticas, quando necessário;

3.6.14. Criação, alteração e configuração de novas políticas, de acordo com o solicitado pela CONTRATANTE;

3.6.15. Confecção de relatórios mensais com indicadores e atividades realizadas;

3.6.16. Para realização dos Serviços de Apoio e Suporte Técnico Especializados a CONTRATADA deverá disponibilizar profissionais certificados pelo fabricante da solução, cuja comprovação deverá ser apresentada no momento da assinatura do contrato;

3.6.17. O Serviço de operação assistida será mensurado como um serviço mensal e deverá ser atestado através de relatório técnico emitido pela CONTRATADA e encaminhado juntamente com a da Nota Fiscal Eletrônica de Serviços a partir do 1º (primeiro) dia do mês subsequente à prestação do serviço;

3.7. ITEM 6 – SERVIÇO DE TREINAMENTO

3.7.1. Os treinamentos deverão contemplar a explanação teórica e prática para administradores da solução adquirida.

3.7.2. Os treinamentos poderão ser remotos ou a CONTRATANTE disponibilizará em seu ambiente uma sala para a execução dos treinamentos, com infraestrutura e apoio básicos (mesas, cadeiras, projetor, tela de projeção, computadores); em caso de impossibilidade de realização no ambiente da CONTRATANTE, caberá à Contratada arcar com toda a infraestrutura (salas, instalações e equipamentos, recursos audiovisuais, coffee-break etc.).

3.7.3. O treinamento a ser ofertado não possui obrigatoriedade de ser oficial do Fabricante da solução, contudo deve ser baseado em documentação oficial ou autorizado por ele.

3.7.4. A carga mínima exigida para este treinamento é de 20 horas.

3.7.5. A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 4 (quatro) horas de instrução diária, com a possibilidade de dividir a turma em dois períodos.

3.7.6. Poderão ser demandadas a quantidade de no mínimo 01 (uma) turma com 10 (dez) participantes e no máximo 02 (duas) turmas com 05 (cinco) participantes em cada turma.

3.7.7. A CONTRATANTE resguardar-se-á do direito de acompanhar e avaliar o treinamento com instrumento próprio e, caso a mesma não atinja os requisitos mínimos especificados, esta deverá ser reestruturada e aplicada novamente, sem nenhum custo adicional à CONTRATANTE.

3.7.8. O conteúdo programático do treinamento deverá contemplar, no mínimo, mas não se restringindo, informações necessárias a:

a) Procedimentos de instalação física e lógica;

b) Procedimentos necessários à configuração técnica e à completa operação do produto;

c) Procedimentos de manutenção do produto que devem ser realizados pelos técnicos do Instituto;

d) Apresentação geral da solução fornecida;

e) Descrição detalhada das partes e componentes de toda a solução, apresentando suas características funcionais;

f) Introdução do conceito de classificação, monitoramento e auditoria de dados e comportamento de usuários;

g) Visão completa da estrutura do AD, com possibilidades de administrar seu repositório de usuários e grupos de segurança utilizando uma interface única, juntamente com a gestão de seus servidores de arquivos;

h) Auditoria eficiente do Active Directory e File Server, fornecendo à equipe de TI visibilidade de todos os eventos ocorridos;

i) Gestão e controle de Permissionamento, de Registro de Eventos, de Análise Comportamental e Forense de todas as plataformas monitoradas;

j) Criação e/ou emissão de Relatórios, visando facilitar o controle sobre o que acontece em todos os ambientes;

k) Alertas de eventos, quando alguma ação for disparada;

l) Consultas e pesquisas de eventos fora de comportamento normal.

m) Auditoria de autenticação em aplicações web.

n) Outros tópicos da solução necessários ao pleno domínio da solução e suas Integrações poderão ser explanados em comum acordo ente as partes na Reunião Inicial de Projeto.

3.7.9. Quando da conclusão do treinamento, a Contratada disponibilizará à CONTRATANTE relatório da execução do evento, contendo no mínimo os seguintes dados:

a) Nomes dos participantes e respectivo controle de frequência;
b) Conteúdo do treinamento aplicado;
c) Data e Hora;
d) Carga horaria executada.

4. DAS OBRIGAÇÕES DA CONTRATADA

4.1. A Contratada deve cumprir todas as obrigações constantes neste Termo de Referência, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

4.2. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta;

4.3. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem

vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

4.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

4.5. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

4.6. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à Contratante;

4.7. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços;

4.8. Prestar todo esclarecimento ou informação solicitada pela Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução dos serviços;

4.9. Paralisar, por determinação da Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;

4.10. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do contrato;

4.11. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado;

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

4.13. Submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo;

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

4.15. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

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

4.17. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante;

4.18. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia

adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

4.19. A contratada deverá prestar serviço de manutenção, atualização e suporte técnico da solução de proteção de dados durante toda a vigência contratual, a partir da data de emissão do Termo de Aceite e Recebimento referente à implantação e operacionalização da solução no ambiente tecnológico do Instituto, e deverá contemplar obrigatoriamente no mínimo:

4.20. Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;

4.21. Atualização dos softwares fornecidos se houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos;

4.22. Correções de falhas (bugs) de software durante o período contratual, sendo executadas pela Contratada e/ou pelo Fabricante da solução, sem ônus adicionais;

4.23. Entrega, por parte da Contratada, de manuais técnicos e/ou documentação da solução, já entregues anteriormente, em caso de alterações dos mesmos, sem ônus adicionais para a Contratante;

4.24. As novas versões do objeto contratado deverão ser disponibilizadas em até 5 (cinco) dias corridos, a partir do lançamento oficial da versão.

4.25. Caso os serviços de manutenção e suporte técnico para todos os componentes da solução não forem executados diretamente pela Contratada, mas sim pelo próprio Fabricante ou por empresa(s) representante(s) ou credenciada(s) por este, a Contratada deverá comunicar tal fato à CONTRATANTE, e assegurar que todos os padrões de atendimento e demais requisitos contratuais serão cumpridos. O aceite por parte da CONTRANTE do atendimento não exime a Contratada da responsabilidade integral pelo atendimento e cumprimento dos prazos acordados.

4.26. Somente serão aceitas soluções originais do fabricante dos componentes da solução.

4.27. A Contratada deverá disponibilizar acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (website) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, "troubleshootings", com pesquisa efetuada através de ferramentas de busca) e atualizações.

4.28. Assegurar à Contratante: Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, exigida, inclusive, a capacitação dos técnicos da Contratante ou da nova empresa que continuará a execução dos serviços, sempre que necessário.

4.29. Dentre as rotinas de execução dos trabalhos e etapas a serem executadas a contratada deverá realizar as seguintes atividades:

a) Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;

b) Atualização dos softwares fornecidos se houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos;

c) Correções de falhas (bugs) de software durante o período contratual, sendo executadas pela Contratada e/ou pelo Fabricante da solução, sem ônus adicionais;

d) Entrega, por parte da Contratada, de manuais técnicos e/ou documentação da solução, já entregues anteriormente, em caso de alterações dos mesmos, sem ônus adicionais para a Contratante;

e) As novas versões do objeto contratado deverão ser disponibilizadas em até 5 (cinco) dias corridos, a partir do lançamento oficial da versão.

f) instalar e configurar toda a solução (módulos) de auditoria para o ambiente Microsoft nos serviços de Active Directory (AD), Microsoft Windows File Server, nos hardwares de destino;

g) instalar e configurar todos os produtos do fornecimento da solução (módulos) de auditoria para Classificação de Dados Sensíveis, nos hardwares de destino;

h) instalar e configurar todos os produtos do fornecimento da solução (módulos) de Análise em tempo real e prevenção de comportamentos suspeitos, nos hardwares de destino;

i) executar a integração de todos os produtos da solução, de modo a não prejudicar as atividades mantidas nos locais, podendo ser exigida a realização de algumas fases em horários noturnos e fins de semana para que seja cumprido o cronograma de entrega da Contratante;

j) providenciar o planejamento de testes, fornecendo um "Plano de Homologação e Testes" contendo todo o processo de homologação dos produtos e detalhamento dos testes que serão executados para validar a solução implementada;

k) executar uma série de testes funcionais básicos para verificar o perfeito funcionamento do ambiente, seguindo os procedimentos definidos no "Plano de Homologação e Testes", sendo tais testes a serem obrigatoriamente executados nos componentes de hardware e software envolvidos no projeto;

l) elaborar a "Documentação e Finalização do Projeto", que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e ou gerencial.

4.30. Durante a implantação da solução, a Contratada deverá realizar, entre outras atividades: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, tunning, resolução de problemas e implementação de segurança.

4.31. Caberá à Contratada a disponibilização de todos os recursos necessários, tais como hardwares, softwares, recursos humanos necessários à instalação da solução.

4.32. Caberá à Contratada a disponibilização de ferramentas / scripts de retorno imediato ao estado original da estrutura da Contratante caso a instalação e migração dos produtos /softwares da Contratada apresente falha.

4.33. A Contratada realizará adequação/configuração da solução fornecida ao longo da etapa de migração e realização de novas configurações.

5. OBRIGAÇÕES DA CONTRATANTE

5.1. Prover acesso a rede física ou lógica sob demanda;

5.2. Ajustes na rede lógica da Prodam quando necessário;

5.3. Prover informações do ambiente de infraestrutura da Prodam para colaborar na solução de problemas;

5.4. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

5.5. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

5.6. A função de gestão e fiscalização do contrato recairá sobre o mesmo servidor, com as atribuições conforme a seguir especificadas:

a) Fiscal do Contrato: agirá de forma ativa e preventiva, observando o cumprimento, pela contratada, de todas as regras previstas contratualmente, além de buscar os resultados esperados do pacto com redução efetiva das inconsistências nos procedimentos de sua execução e, ainda, registrar todas as ocorrências relacionadas com a execução do contrato e encaminhar informações ao gestor do contrato.

b) Gestor do Contrato irá controlar o processo referente ao contrato, zelando para que constem todos os documentos relativos à contratação, tais como: termo de referência/projeto básico, termo de contrato, ordem de serviço, portarias de nomeação/alteração de fiscal do contrato sempre que ocorrerem, termos aditivos, termos de apostilamento, documentos fiscais, liquidações, obrigatoriedade de retenção na fonte dos tributos, entre outros. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;

5.7. Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;

5.8. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da Contratada, no que couber;

5.9. Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;

5.10. Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

5.11. Arquivar, entre outros documentos, projetos, as built, especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas.

6. CONFIDENCIALIDADE:

6.1. A CONTRATADA deverá zelar pelo sigilo de quaisquer informações referentes à estrutura, sistemas, usuários, contribuintes, topologia, e ao modo de funcionamento e tratamento das informações da CONTRATANTE, durante e após fim do contrato, salvo se houver autorização expressa da Contratante para divulgação;

6.2. Não haverá nenhum tipo de facilidade de acesso remoto, tão menos envio de forma automática ou controlada de informações (backdoor) originadas de software/hardware contratado ou adquirido sem o conhecimento e formal autorização da Contratante. A não observância desse fato poderá ser considerada espionagem e será motivo de processo civil e criminal conforme legislação vigente.

7. PENALIDADES

7.1. Caso haja atraso no período de resposta da abertura de um chamado (2 horas), haverá multa de 0,1% por hora de atraso, calculado sobre o valor mensal de suporte técnico do contrato;

7.2. Caso o tempo para atendimento de suporte da CONTRATADA ultrapasse as horas, contadas a partir da abertura do chamado, haverá multa de:

a) Severidade 1: 2% por hora de atraso, calculado sobre o valor mensal do suporte técnico;
b) Severidade 2: 1% por hora de atraso, calculado sobre o valor mensal do suporte técnico;
c) Severidade 3: 0,5% por hora de atraso, calculado sobre o valor mensal do suporte técnico;
d) Severidade 4: 0,1% por hora de atraso, calculado sobre o valor mensal do suporte técnico;

7.3. Caso haja atraso na instalação e Configuração da solução, será aplicada multa de 1% ao dia de atraso, calculado sobre o valor do item 4 da Tabela e Composição de Itens;

7.4. Caso haja atraso na prestação dos Serviços de Apoio e Suporte Especializado (nível 1 e 2), será aplicada a multa de 1% ao dia de atraso, calculado sobre o valor do item 2 da Tabela de Composição de Itens;

7.5. Caso haja atraso no início dos Treinamentos, será aplicada multa de 1% calculado sobre o valor total do item 6 da Tabela de Composição de Itens;

7.6. Caso haja atraso na entrega, prevista no item 9.1, será aplicada multa de 1% por dia de atraso, calculado sobre o valor total do contrato.

7.7. Caso haja atraso no prazo de entrega do Certificação de Conclusão dos Treinamentos estabelecido no item 10.3, alínea “b” será aplicada multa de 0,5% sobre o valor total do item “6” da Tabela de Composição de Itens.

8. QUALIFICAÇÃO TÉCNICA

8.1. A CONTRATADA deverá apresentar, em seu nome, atestado (s) de capacidade técnica operacional, emitido por pessoa jurídica de direito público ou privado, comprovando a execução de atividade pertinente e compatível em características e quantidades, com o objeto a ser contratado.

8.2. Será considerado o atestado compatível se comprovado no mínimo a execução, e fornecimento de Solução para inteligência, segurança e governança de dados com identificação e classificação de informações sensíveis, da mesma natureza e compatível com o objeto descrito no Termo de Referência, incluindo os serviços de configuração, suporte e manutenção da solução, contemplando, no mínimo 10% (dez por cento), ou seja, no mínimo de 6.000 licenças de um total de 60.000 licenças, conforme Tabela de Composição de Itens – subitem "3".

8.3. Atestado(s) Técnico(s) deve ser apresentado em papel timbrado, datado e assinado com identificação do atestante (nome, cargo, e-mail e telefone), contendo descrição dos itens e quantidades fornecidas.

8.4. Será aceito o somatório de atestados para comprovação do volume mínimo de licenças contemplados pela solução.

8.5. Caso o licitante não seja o fabricante das soluções ofertadas, deverá apresentar comprovação de que a LICITANTE possui autorização do fornecedor da solução para comercializar, instalar e prestar suporte no Brasil para o produto especificado. A comprovação deverá ser feita por meio de declaração do fornecedor oficial dos produtos que compõem a solução e destinada a PRODAM e com referência explícita a este processo de aquisição.

8.6. Devido às características e criticidade das informações coletadas, armazenadas e processadas, com o intuito de garantir integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade de as informações serem utilizadas para perícia forense inclusive como provas judiciais, a solução auditoria, análise de eventos e governança de dados deverá ter certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação como a ISO/IEC 27001 ou similares.

8.7. A licitante deverá apresentar, juntamente com sua proposta comercial: catálogos, folder, manuais e demais documentos técnicos que comprovem a aderência da solução as especificações técnicas mínimas a serem indicadas no termo de referência.

8.8. Para fins de verificação de adequação da solução ofertada as especificações técnicas detalhadas apresentadas nesse Termo de Referência deverão ser comprovadas em uma Matriz ponto-a- ponto contendo, de forma organizada, o item do Termo de Referência, O NOME DO ARQUIVO DA DOCUMENTAÇÃO ORIGINAL DO FABRICANTE e a indicação do número da página que comprove o atendimento ao item.

8.9. A habilitação da empresa melhor classificada ficará condicionada, ainda, à comprovação das especificações gerais e funcionalidades deste Termo de Referência. Para tanto, deverá executar um Teste de Bancada, disponibilizando-o à CONTRATANTE;

8.10. A empresa melhor classificada deverá atender **TODOS** os **"REQUISITOS A SEREM AVALIADOS" no teste de bancada. O não atendimento de quaisquer dos requisitos ensejará na desclassificação da licitante**.

8.11. Caso a licitante não atenda as exigências de habilitação do Teste de Bancada ou qualquer dos documentos de habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda integralmente as exigências do Edital.

8.12. A licitante melhor classificada deverá prestar apoio e esclarecimentos necessários durante a apresentação e execução do Teste de Bancada, dando subsídios para que a PRODAM possa homologar a solução proposta.

8.13. Teste de Bancada será realizado no endereço da PRODAM – Rua Pedro de Toledo, 983, Vila Clementino, São Paulo, ou em endereço a ser definido pela CONTRATANTE dentro do município de São Paulo, em horário comercial, de segunda a sexta-feira, das 8h às 12h e das 13h às 17h.

8.14. Após a análise da documentação, respeitada a ordem de classificação do certame, o pregoeiro comunicará, via chat, a licitante que atenda ao edital quanto à documentação habilitatória, para que proceda ao agendamento do Teste de Bancada junto à área técnica através do e-mail helena@prodam.sp.gov.br, conforme disposto a seguir:

8.15. A empresa vencedora da etapa de lances, convocada via chat na sessão do Pregão, terá 2 dias úteis para agendamento através do e-mail helena@prodam.sp.gov.br, sob pena de desclassificação pelo não cumprimento deste prazo;

8.16. O prazo para início do Teste de Bancada não será superior a 5 dias úteis após o agendamento;

8.17. Caso a empresa convocada não atenda os prazos, será considerada desclassificada;

8.18. As demais empresas, interessadas em assistir ao Teste de Bancada terão dois dias úteis para agendamento através do e- mail helena@prodam.sp.gov.br, a partir da convocação do pregoeiro à empresa que realizará o teste, indicando até 2 (dois) técnicos ou representantes legais da licitante, devidamente identificados por meio de vínculo contratual ou procuração, como "Técnico de Acompanhamento da Licitante Participante". O não cumprimento deste prazo, ensejará na queda do direito de assistir à realização do teste;

8.19. Não será permitida a substituição de qualquer Técnico de Acompanhamento da licitante participante sem a autorização prévia da PRODAM;

8.20. Não será permitida a comunicação direta entre qualquer Técnico de Acompanhamento da licitante participante e a Equipe Técnica da licitante convocada. Qualquer comunicação ou questionamento deve ser dirigido unicamente à Equipe Técnica da PRODAM;

8.21. A não observância dessa regra de comunicação poderá causar o descredenciamento da Equipe Técnica da licitante convocada ou de qualquer técnico de acompanhamento da licitante participante;

REQUISITO A SER AVALIADO	ATENDE OU NÃO ATENDE
ITEM 3	-
A solução ofertada para este item deverá ser do mesmo fabricante e totalmente integrada de forma nativa constantes nestas especificaçõestécnicas;	
A solução deve efetuar as funcionalidades de permissionamento, Log, Relatórios, Análise Comportamental e Alerta dos servidores dediretórios de usuários Microsoft Active Directory, e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados;	
A solução deve possuir visibilidade da hierarquia do serviço deDiretórios de Usuários através de interface gráfica;	

REQUISITO A SER AVALIADO	ATENDE OU NÃO ATENDE
A solução deve possuir a visibilidade de todos os domínios, Unidades Organizacionais, Computadores, Grupos e outros objetos do domínioatravés de uma única interface gráfica e igualmente sob forma de relatório;	
Caso a solução ofertada necessite reter o log nativo de auditoria do Active Directory, o hardware sem ponto único de falha necessário para o armazenamento destes logs por 60 (sessenta) meses deverá sercontemplado na proposta.	
Devido às características e criticidade das informações coletadas, armazenadas e processadas, com o intuito de garantir integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade de as informações serem utilizadas para perícia forense inclusive como provas judiciais, a solução deverá ter certificação utilizada pelaadministração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação como a ISO/IEC 27001 ou similares.	
A solução deve permitir aos usuários administrativos realizar asseguintes ações através da interface gráfica da solução:	
Criar novos usuários;	
Criar novos grupos de segurança;	
Alterar parâmetros de usuários já existentes;	
Alterar membros de grupos de segurança;	
Excluir usuários;	
Excluir computadores;	
Reconfigurar senhas;	
Desbloquear usuários; e	
Habilitar e desabilitar usuários.	
A solução deve permitir as ações abaixo, de uma só vez, através daseleção de múltiplos usuários:	
Deleção;	
Reset de senha;	
Desbloqueio da conta;	
Habilitação e desabilitação.	
A solução deve permitir a emissão de, no mínimo, os seguintesrelatórios específicos:	
Visibilidade de todos os Domínios, Unidades Organizacionais,Computadores, Grupos e outros objetos do domínio;	

REQUISITO A SER AVALIADO	ATENDE OU NÃO ATENDE
Trilha de auditoria de todas as atividades do Active Directory; e	
Trilha de auditoria de quem realizou alterações no Active Directory, qual foi a alteração feita e quando a alteração ocorreu.	
A solução deverá possuir a opção de aplicação das alterações utilizando uma credencial diferente da credencial do usuário logado na interface gráfica assim, a modelagem pode ser feita por um usuárioe efetivada por outro usuário, este último, com permissões de alterações no Active Directory;	
A solução deverá fornecer a visibilidade sobre aplicações de alteração que estão pendentes e o histórico das alterações aplicadas através da console;	
A solução deve coletar os eventos das plataformas monitoradas de forma contínua e automática;	
A solução deve apresentar todos os eventos de todos os usuários e detodas as plataformas monitoradas na mesma console de visibilidade de permissionamento;	
As ações dos usuários apresentadas pela solução, devem conter informações completas de cada uma das operações com:	
data e horário;	
nome do servidor;	
tipo do objeto;	
caminho (path) dos dados;	
domínio;	
objeto impactado; e	
nome do usuário.	
A solução deve permitir filtragem gráfica, ordenação e agrupamentodos logs;	
A solução deverá fornecer todas as funcionalidades citadas abaixo sem a necessidade de retenção dos logs nativos do Windows. Caso asolução ofertada necessite habilitar o log de auditoria do Windows File Server, o hardware sem ponto único de falha necessário para o armazenamento destes logs deverá ser contemplado na proposta;	
A solução deverá disponibilizar no mínimo as funcionalidades de visibilidade dos dados, usuários e grupos de segurança, gerenciamento de permissionamento, auditoria e relatórios de todas as plataformas monitoradas que devem estar disponíveis em uma única interface gráfica integrada;	
A solução deverá fornecer método para assinalar ou associar um oumais usuários como "Proprietário(s)" de uma pasta.	
A solução deverá mostrar em uma mesma interface toda a base de usuários e de dados monitorados, exibindo para cada pasta ou arquivo a visualização gráfica interativa das listas de controle de acesso incluindo grupos, subgrupos e seus	

REQUISITO A SER AVALIADO	ATENDE OU NÃO ATENDE
respectivos membros, incluindo herança de permissão ativa/desativada e indicação decompartilhamento;	
A solução deverá possuir a opção de aplicação das alterações utilizando uma credencial diferente da credencial do usuário logado na interface gráfica assim, a modelagem pode ser feita por um usuárioe efetivada por outro usuário, este último, com permissões de alterações no Active Directory;	
A solução deverá permitir que seja salva a credencial de aplicação dealterações para uso futuro;	
A solução deverá fornecer a visibilidade sobre aplicações de alteração que estão pendentes e o histórico das alterações aplicadas através da console;	
A solução deve permitir a modelagem de permissionamento demaneira gráfica, incluindo a simulação do impacto de mudanças no permissionamento de grupos e usuários, e da remoção de permissões excessivas, inclusão de novos grupos e identificação de quais usuários serão afetados com estas trocas de permissões;	
A solução ofertada deve manter o log das operações de abrir, criar,apagar, modificar, copiar, renomear e acesso negado	
As ações dos usuários apresentadas pela solução, devem conter informações completas de cada uma das operações com:	
data e horário;	
nome do servidor;	
tipo do objeto;	
caminho (path) dos dados;	
domínio;	
objeto impactado; e	
nome do usuário.	
A solução deverá identificar em uma mesma tela todas as atividades de um determinado usuário ou determinada pasta de todos os repositórios monitorados e diretórios de usuários;	
A solução deve fornecer resumo gráfico das atividades auditadas,incluindo:	
visualização dos usuários mais e menos ativos;	
visualização dos diretórios mais e menos acessados;	
visualização dos diretórios onde um usuário ou um grupo de usuários estejam acessando;	
visualização dos usuários que estejam acessando um diretório.	

REQUISITO A SER AVALIADO	ATENDE OU NÃO ATENDE
A solução deve permitir que os usuários realizem pesquisas baseadosem critérios como:	
data do evento;	
servidor ou plataforma em que o evento ocorreu;	
tipo de evento; e	
arquivos ou diretórios acessados.	
A solução, com base nos dados de auditoria, deve ser capaz de assimilar o comportamento padrão dos usuários e dos recursos monitorados, de modo que desvios e anormalidades nesses comportamentos sejam identificados automaticamente;	
A solução deve permitir que sejam configurados alertas em temporeal para eventos da auditoria habilitada;	
A solução deve possibilitar, nos alertas em tempo real, configurar para que um usuário, uma pasta, um período ou uma ação específicaseja alertada caso ocorra ação que os envolva;	
A solução deve possibilitar que os alertas serão iniciados com base nos dados da auditoria, tais como usuário, ação, data e hora, ação realizada;	
A solução deve contemplar a assinatura de uma base de conhecimentos do fornecedor de alertas pré-configurados de eventossuspeitos tais como:	
ataques de sequestro de dados (ransomware);	
detecção de ferramentas nocivas ao ambiente;	
excessos de ações com acessos negadas;	
acessos indevidos dos administradores nos dados da empresa;	
tentativas de elevação de privilégios;	
excesso de tentativas de autenticação ou contas bloqueadas;	
excesso de atividades em dados parados e/ou inativos;	
alterações anormais em GPO (Group Policy);	
excesso de acessos em caixas postais de uma única máquina; e	
excesso de ações em um curto espaço de tempo.	
Os alertas devem ser gerados em SNMP, Syslog, visualizador de eventos do Windows, E-mail e devem ser capazes de realizar a execução de um script previamente configurado.	

REQUISITO A SER AVALIADO	ATENDE OU NÃO ATENDE
Os alertas devem ser apresentados também em dashboard web queapresente:	
quantidade de alertas e suas severidades em determinado período,	
usuários mais alertados em determinado período,	
tipos de alertas que mais ocorreram,	
máquinas que forma mais utilizadas para as ações suspeitas, e	
classificação dos alertas dentro de um cenário de ataque cibernético.	
O dashboard deve apresentar os eventos que motivaram o alerta paraque o time de segurança possa fazer investigação forense;	
No dashboard, a partir de um alerta selecionado, a solução deve exibirpágina que liste todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser customizável, podendo ser filtrada, exibidas ou ocultadas colunas e agregada por valores das colunas exibidas.	
O dashboard deve possuir página com KPIs de compliance e segurança dos servidores e recursos monitorados (Active Directory eFile Server) e a partir desses KPIs, deve ser possível abrir a lista cominformações detalhadas.	
A solução deverá ser totalmente compatível e integrada ao módulode análise de comportamento dos usuários e alerta em tempo real.	
Os alertas deverão ser identificados e apresentados no portal web de alertas integradamente aos alertas de comportamento suspeitos de forma que possam ser correlacionados nas investigações forense.	
A solução deverá ser capaz de analisar em tempo real e prevenir comportamentos suspeitos em aplicações web, mesmo que estas nãoestejam integradas ao Active Directory, atendendo minimamente osseguintes critérios:	
Comunicar-se através de API HTTP REST ou UDP com a aplicaçãoweb protegida, calculando e fornecendo em tempo real um score de risco e o nível de risco que este score representa, para cada evento de autenticação que ocorre em uma dada aplicação.	
Assegurar a comunicação entre a solução e a aplicação webprotegida através de criptografia de chaves simétricas.	
Possibilitar a criação e configuração de políticas de risco, possuindono mínimo 4 níveis de risco parametrizáveis a serem definidos em cada política.	
Fornecer para cada autenticação analisada o score de risco processado acompanhado da ação (permitir, notificar, desafiar ou bloquear) indicada para o nível de risco do evento em questão, deacordo com a política definida.	
Possibilitar o agrupamento de credencias, de modo que uma credencial possa estar associada a mais de uma aplicação webprotegida.	
Não exigir tokens, dispositivos móveis, códigos ou outrasinformações adicionais para o processamento de eventos.	
Ser capaz de processar e fornecer o score de risco tanto paraautenticações com a credencial e senha corretos como para autenticações com credencial e/ou senha incorretos.	

REQUISITO A SER AVALIADO	ATENDE OU NÃO ATENDE
Possuir uma base de inteligência de segurança para ser utilizada namensuração do risco dos acessos, construída com informações próprias e públicas (OSINT), de modo a identificar IPs de má reputação e/ou utilizados para serviço de proxy.	
Realizar a mensuração de risco no processo de autenticação sem armazenar e sem ter acesso a senha da credencial em questão, emnenhuma hipótese.	
Construir padrão de comportamento de uma credencial com base nohistórico de seu uso, composto minimamente por navegador, dispositivo, localização geográfica (cidade e país), sistema operacional, identificador do provedor de internet.	
Identificar desvios no padrão de comportamento de uma credencial,possibilitando o envio de notificações, apresentação de desafios (token, captcha ou similares) e bloqueio de acesso, a depender da política de risco definida.	
Realizar a mensuração de risco de todos os acessos levando em consideração o padrão de comportamento da credencial e a base deinteligência de segurança.	
Todos os eventos processados e armazenados pela solução deverão ser georreferenciados de acordo com o endereço IP de origem, contendo minimamente país, cidade, latitude e longitude.	
Permitir a notificação de usuários com base em política de risco, através do disparo via SMTP de e-mail, possibilitando a redação demensagem personalizada em editor HTML, contendo detalhes do evento em questão como cidade de acesso, data e hora, ip de origem, navegador e um link para que o usuário responda se reconhece o acesso ou não.	
Inserir no padrão de comportamento da credencial novas informações quando o usuário confirma através da notificaçãorecebida a veracidade do acesso.	
Possibilitar o envio de e-mail para administrador quando um usuário nega a veracidade de um acesso através da notificação recebida.	
Ser capaz de bloquear o processo de autenticação de usuários combase no score de risco do evento, mesmo quando a credencial e a senha forem corretamente imputadas no ato da autenticação.	
Identificar ataques do tipo “força bruta”, elevando de forma automática e proporcional o score de risco do IP de origem doacesso com base no número de tentativas de autenticações fracassadas em um curto intervalo de tempo.	
A reputação das origens detectadas como geradores de ataques de força bruta deverá decair após determinado tempo, e o tempo de decaimento da reputação deverá aumentar em função da recorrênciade tentativas de ataques de força bruta.	
Enviar eventos, cifrados nativamente com chave simétrica, via webhook para URL a ser configurada em interface gráfica, combase na política de risco definida.	
Elevar o score de risco de uma credencial ao detectar mudançageográfica de longa distância.	
Identificar os top 10 usuários que representam maior atividade de risco acumulado em um intervalo de tempo escolhido, informando onome do usuário (credencial) e score de risco acumulado.	
Segmentar os eventos processados por credencial, possibilitando navegar por todos os eventos de uma dada credencial, informando no mínimo os seguintes detalhes de cada evento: Cidade, coordenadas geográficas, nome do navegador utilizado, nome dodispositivo utilizado no acesso, endereço ip de origem, score de risco e resultado da ação com base na política definida, código identificador do ISP (internet service provider) e descritivo com análise do evento.	

REQUISITO A SER AVALIADO	ATENDE OU NÃO ATENDE
Possuir gráfico que represente os eventos de uma credencial específica em um intervalo de tempo escolhido, distinguindo-ospelos níveis de risco definidos em política.	
Possuir dashboard para visualização de eventos no formato de representação de mapa geográfico que possibilite distinguir diferentes níveis de risco, detalhando informações como cidade,usuário, score de risco do evento, data e hora do evento.	
Possuir dashboard para visualização do risco organizacional em umintervalo de tempo escolhido, segmentado por aplicação protegida ou não, distinguindo o volume de eventos que representam o risco mitigado, o risco em mitigação (pendente) e o risco assumido.	
Possuir integração com soluções do tipo “single-sign-on”, disponibilizando no mínimo, de forma nativa, o RH-SSO eKeycloak.	
Possuir integração nativa com a autenticação de tecnologias demercado, sendo minimamente wordpress, openssh, cloudflare, moodle e keycloak.	
Ser capaz de processar eventos originados em IPv4 e IPv6.	
Possuir identificador único para todos os eventos processados pelasolução.	
Possuir mecanismo de processamento e armazenamento de eventosbaseado em tecnologias escaláveis.	
Possuir mecanismo de dissuasão de ataques de força-bruta baseado em desafio criptográfico a ser decifrado pelo navegador cliente, semnecessidade de interação dos usuários da aplicação protegida.	
O nível de dificuldade do desafio criptográfico deverá ser parametrizável.	

9. PRAZO DE ENTREGA

9.1. A solução de TIC deverá ser plenamente implementada pela Contratada no ambiente da PRODAM em no máximo 120 (cento e vinte) dias corridos, a partir da assinatura do instrumento contratual.

9.2. A Instalação, Configuração e ativação da solução será a partir do primeiro mês de contrato, bem como o início dos serviços associados ao objeto.

9.3. As licenças de auditoria, análise de eventos e governança serão contratadas sob demanda e deverão ser entregues 05 dias úteis após a emissão da Ordem de Serviço pela CONTRATANTE:

9.3.1. As licenças serão utilizadas durante a vigência contratual;

9.3.2. As licenças serão instaladas pela CONTRATADA.

9.4. Serviços de Treinamento e Operação Assistida terão sua execução e início a partir do segundo mês de contrato.

9.5. A reunião inicial de alinhamento com a Contratada, deverá ocorrer em no máximo 5 (cinco) dias corridos, a partir da assinatura do instrumento contratual.

9.6. Entende-se por fornecimento do objeto a execução completa dos serviços e tarefas previstas.

10. ACEITE

10.1. Após a instalação e configuração, a equipe técnica da PRODAM emitirá o "Termo de Aceite e Recebimento" em até 5 (cinco) dias úteis após a formalização pela CONTRATADA da finalização do processo da instalação/configuração (operação) da solução e confirmação que todos os quesitos estão sendo cumpridos conforme esse Termo de Referência.

a) Entende-se pela instalação e configuração a disponibilização de todas as soluções contratadas, instaladas nos equipamentos descritos no planejamento inicial, devidamente identificadas pela solução de gerenciamento.

10.2. Após a entrega e instalação das Licenças de Auditoria, Análise de Eventos e Governança de Dados a equipe técnica da CONTRATANTE emitirá o Termo de Aceite de Entrega e Recebimento das Licenças.

10.3. Após a finalização dos treinamentos, a equipe técnica da PRODAM emitirá o "Termo de Aceite de Conclusão de Treinamento" em até 5 (cinco) dias úteis após a formalização pela CONTRATADA da finalização do processo de treinamento e confirmação que todos os quesitos foram cumpridos conforme esse Termo de Referência.

a) Caso o treinamento fornecido não esteja de acordo com o que foi especificado, o Termo de Aceite de Conclusão de Treinamento não será emitido, devendo a CONTRATADA fornecer novo treinamento que contemple todos os requisitos necessários;

b) A CONTRATADA deverá emitir "Certificado de Conclusão", em até 15 dias úteis após o término do treinamento;

c) Caso o certificado de conclusão do treinamento fornecido não seja emitido de acordo com o que foi especificado, o Termo de Aceite de Conclusão de Treinamento não será emitido, devendo a CONTRATADA providenciar sua emissão;

11. CONDIÇÕES DE FATURAMENTO

11.1. O faturamento do Appliance (hardware dedicado) de inspeção de segurança (ITEM 1) será efetuado integralmente, em parcela única, a partir da entrega pela CONTRATADA à CONTRATANTE e após a emissão pela CONTRATANTE do Termo de Aceite e Recebimento", anexo XI.

11.2. O faturamento do serviço de Suporte Técnico, Manutenção e Garantia do item 1 appliance (hardware dedicado) para inspeção de segurança (ITEM 2) será efetuado em parcelas mensais de igual valor, a partir da emissão pela CONTRATANTE do "Termo de Aceite e Recebimento", anexo XI.

11.3. O faturamento das Licenças para Auditoria, Análise de Eventos e Governança de Dados (ITEM 3) será em parcela única, a partir da entrega pela CONTRATADA à CONTRATANTE e após emissão pela CONTRANTANTE do Termo de Aceite e Recebimento das Licenças", anexo XIV.

11.4. O faturamento dos Serviços de Instalação e Configuração da solução (ITEM 4), será efetuado em parcela única, após a emissão pela CONTRATANTE do "Termo de Aceite e Recebimento", anexo XI.

11.5. O faturamento do Serviço de Operação Assistida (ITEM 5) será efetuado em parcelas mensais de igual valor, a partir da emissão 65 TR_TIC INTELIGÊNCIA, SEGURANÇA E GOVERNANÇA DE DADOS_V5 – 14-07-2023 pela CONTRATANTE do "Termo de Aceite e Recebimento das Licenças", anexo XIV.

11.6. O faturamento dos Treinamentos (ITEM 6) ministrados pela CONTRATADA, será efetuado em parcela única ao término de cada turma de treinamento e após a emissão pela CONTRATANTE do Termo de Aceite e Recebimento do Treinamento, anexo XII.

12. PROPOSTA PARA CONDIÇÕES DE PAGAMENTO

12.1. A Nota Fiscal Eletrônica de Serviços deverá ser emitida e encaminhada à CONTRATANTE, através do setor competente, por meio do endereço eletrônico gfl@prodam.sp.gov.br, caso o CONTRATANTE seja a PRODAM. Nos casos em que a CONTRATANTE seja uma Secretaria ou outro órgão público que aderir à ARP, o modo de entrega deverá ser estabelecido quando da formalização do instrumento contratual.

12.2. Após o recebimento da Nota Fiscal Eletrônica de Serviços, a CONTRATANTE disporá de até 05 (cinco) dias úteis para emissão do Termo de Aceite de Pagamento, anexo X, aprovando os serviços prestados.

12.3. O pagamento será realizado por intermédio de crédito em conta corrente ou por outra modalidade que possa vir a ser determinada pelo departamento responsável da CONTRATANTE, em 30 (trinta dias) dias corridos a contar da data de emissão do Termo de Aceite de Pagamento.

12.4. Caso a Nota Fiscal Eletrônica de Serviço contenha divergências com relação ao estabelecido no Instrumento Contratual, a CONTRATANTE ficará obrigada a comunicar a empresa CONTRATADA, formalmente, o motivo da não aprovação no prazo de 05 (cinco) dias úteis. A devolução da Nota Fiscal Eletrônica de serviços, devidamente, regularizada pela CONTRATADA, deverá ser efetuada em até 05 (cinco) dias úteis da data de comunicação formal realizada pela CONTRATANTE.

12.5. Em caso de atraso de pagamento dos valores devidos à CONTRATADA, mediante requerimento formalizado por esta, incidirão juros moratórios calculados utilizando-se o índice oficial de remuneração básica da caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança, para fins de compensação da mora (TR + 0,5% "pro-rata tempore"), observando-se para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorreu.

ANEXO II - MINUTA DO INSTRUMENTO CONTRATUAL

PROCESSO SEI Nº 7010.2023/0004811-7

MODALIDADE DE CONTRATAÇÃO: PREGÃO ELETRÔNICO Nº 06.001/2023

CONTRATO PARA FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA E GOVERNANÇA DE DADOS EM APPLIANCE (HARDWARE DEDICADO), POSSIBILITANDO A IDENTIFICAÇÃO E CLASSIFICAÇÃO DE INFORMAÇÕES SENSÍVEIS, ANÁLISE EM TEMPO REAL E PREVENÇÃO DE COMPORTAMENTOS SUSPEITOS, CONTEMPLANDO SERVIÇOS DE INSTALAÇÃO, SUPORTE E MANUTENÇÃO, OPERAÇÃO ASSISTIDA E TREINAMENTO.

CONTRATANTE: EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO – PRODAM-SP S/A, com sede na Rua Líbero Badaró n.º 425, Centro, no Município de São Paulo, no Estado de São Paulo, CEP 01.009-905, inscrita no CNPJ sob n.º 43.076.702/0001-61, neste ato representada por seu Diretor _____, Sr(a). **_____,** portador da cédula de identidade RG. nº _____ e inscrito no CPF/MF sob nº _____ e por seu Diretor de _____, Sr(a). **_____,** portador da cédula de identidade RG. nº _____ e inscrito no CPF/MF sob nº _____.

CONTRATADA: ....., com sede na ..... n.º ....., no Município de ....., no Estado de ....., CEP ....., inscrita no CNPJ sob n.º ....., neste ato representada por ....., portador da Cédula de Identidade RG n.º ..... SSP/.... e inscrito no CPF/MF sob o n.º .....**.**

As partes acima qualificadas resolveram, de comum acordo, celebrar o presente contrato, mediante as seguintes cláusulas e condições:

CLÁUSULA I – OBJETO

1.1. O presente contrato tem por objeto o **FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA E GOVERNANÇA DE DADOS EM APPLIANCE (HARDWARE DEDICADO), POSSIBILITANDO A IDENTIFICAÇÃO E CLASSIFICAÇÃO DE INFORMAÇÕES SENSÍVEIS, ANÁLISE EM TEMPO REAL E PREVENÇÃO DE COMPORTAMENTOS SUSPEITOS, CONTEMPLANDO SERVIÇOS DE INSTALAÇÃO, SUPORTE E MANUTENÇÃO, OPERAÇÃO ASSISTIDA E TREINAMENTO**, conforme descrições constantes no **Termo de Referência – ANEXO I**, da Proposta Comercial da CONTRATADA e demais documentos constantes do processo administrativo em epígrafe.

CLÁUSULA II – OBRIGAÇÕES DA CONTRATADA E CONTRATANTE

2.1. São obrigações da CONTRATADA:

a) Cumprir fielmente todas as obrigações estabelecidas no **Termo de Referência – ANEXO I** deste instrumento, garantindo a qualidade dos serviços prestados;

b) Para a assinatura do Instrumento Contratual, a CONTRATADA deverá apresentar todos os documentos relativos à regularidade fiscal, e ainda estar em situação regular junto ao CADIN (Cadastro Informativo Municipal) do **Município de São Paulo (Lei Municipal n.º 14.094/2005 e Decreto Municipal n.º 47.096/2006**), mediante consulta ao site http://www3.prefeitura.sp.gov.br/cadin/.

c) Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de qualificação exigidas no momento da contratação, podendo a CONTRATANTE exigir, a qualquer tempo durante a vigência do contrato, a comprovação das condições que ensejaram sua contratação, devidamente atualizadas e o envio das certidões a seguir elencadas, em formato digital (arquivo PDF) para o e-mail contratosfornecedores@prodam.sp.gov.br e para o gestor do contrato a ser definido oportunamente:

i. Certidão Negativa de Débitos relativa aos Tributos Federais e a Dívida Ativa;
ii. Certidão de Regularidade do FGTS (CRF);
iii. Certidão Negativa de Débitos Tributários e da Dívida Ativa Estadual;
iv. Certidão Negativa de Débitos de Tributos Municipais (Mobiliários);
v. Certidão Negativa de Débitos Trabalhistas (CNDT);
vi. Certidão Negativa de Falência ou Recuperação Judicial.

d) Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, e responderá por danos causados, nos termos do art. 76 da Lei nº 13.303/2016;

e) Dar ciência imediata e por escrito a CONTRATANTE de qualquer anormalidade que verificar na execução do contrato;

f) Prestar a CONTRATANTE, por escrito, os esclarecimentos solicitados e atender prontamente as reclamações sobre a execução do contrato;

g) Responder pelos encargos trabalhistas, previdenciários, fiscais, comerciais e tributários, resultantes da execução deste contrato, nos termos do **artigo 77, da Lei Federal nº 13.303/16**.

2.2. São obrigações da **CONTRATANTE**:

a) Exercer a fiscalização do contrato, designando fiscal (is) pelo acompanhamento da execução contratual; procedendo ao registro das ocorrências e adotando as providências necessárias ao seu fiel cumprimento, tendo por parâmetro os resultados previstos no contrato

b) Fornecer à CONTRATADA todos os dados e informações necessários à execução do contrato;

c) Efetuar o pagamento devido, de acordo com o estabelecido neste contrato.

d) Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis;

e) Comunicar a CONTRATADA formalmente (por e-mail) todas e quaisquer ocorrências relacionadas com a prestação dos serviços objeto deste Contrato.

CLÁUSULA III – VIGÊNCIA CONTRATUAL

3.1. O contrato terá vigência de ____ (_____) meses, contados a partir da data de sua assinatura, ou da data da última assinatura digital realizada, podendo ser prorrogado até o limite de 5 (cinco) anos, conforme dispõe o artigo 71, da Lei Federal nº. 13.303/2016.

3.2. Qualquer alteração, prorrogação e/ou acréscimos ou supressões que vierem a ocorrer no decorrer deste contrato será objeto de termo aditivo, previamente justificado e autorizado pela CONTRATANTE.

CLÁUSULA IV – PREÇO

4.1. O valor total do presente contrato é de R$ _____ (_____) e seguirá as regras previstas na **Cláusula VI – Faturamento e Condições de Pagamento**.

4.2. No valor acima já estão incluídos todos os tributos e encargos de qualquer espécie que incidam ou venham a incidir sobre o preço do presente contrato.

4.3. Resta vedado o reajuste do valor contratual por prazo inferior a 12 (doze) meses contados após um ano da data-limite para apresentação da proposta comercial ou do último reajuste, conforme disposto na **Lei Federal nº 10.192 de 14/10/2001**, ou, se novas normas federais sobre a matéria autorizarem o reajustamento antes deste prazo.

4.4. Após o período inicial de 12 (doze) meses de vigência, caso haja prorrogação, o contratado poderá ter seus preços reajustados, aplicando-se a variação do Índice de Preços ao Consumidor IPC/FIPE a contar da data da apresentação da proposta.

CLÁUSULA V – GARANTIA CONTRATUAL (Art. 70, §1º da Lei Federal nº 13.303/16)

5.1. A CONTRATADA deverá prestar garantia contratual no prazo máximo de 15 (quinze) dias a contar da assinatura do contrato, na forma do **artigo 70, § 1º da Lei Federal nº 13.303/16**, no valor de R$ _____ (_____), correspondente a 5% (cinco por cento) do valor contratado, observando os procedimentos a seguir elencados.

5.2. A garantia, qualquer que seja a modalidade escolhida, deverá abranger um período mínimo de três meses após o término da vigência contratual, devendo a garantia assegurar a cobertura de todos os eventos ocorridos durante a sua validade, ainda que o sinistro seja comunicado depois de expirada a vigência da contratação ou validade da garantia.

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

5.3.1. Prejuízos advindos do inadimplemento total ou parcial do objeto do contrato.

5.3.2. Prejuízos diretos causados à CONTRATANTE decorrentes de culpa ou dolo da CONTRATADA durante a execução do contrato.

5.3.3. Multas, moratórias e compensatórias, aplicadas pela CONTRATANTE.

5.3.4. Obrigações trabalhistas e previdenciárias relacionadas ao contrato e não adimplidas pela CONTRATADA.

5.4. A CONTRATADA deverá informar, expressamente, na apresentação da garantia, as formas de verificação de autenticidade e veracidade do referido documento junto às instituições responsáveis por sua emissão.

5.5. No caso de seguro-garantia, a instituição prestadora da garantia contratual deve ser devidamente autorizada pela Superintendência de Seguros Privados – SUSEP e, no caso de fiança bancária, pelo Banco Central do Brasil.

5.6. A insuficiência da garantia não desobriga a CONTRATADA quanto aos prejuízos por ela causados, responsabilizando-se por todas as perdas e danos apurados pela CONTRATANTE que sobejarem aquele valor.

5.7. Para cobrança pela CONTRATANTE de quaisquer valores da CONTRATADA, a qualquer título, a garantia poderá ser executada, a partir do 3º (terceiro) dia, contado da resposta NÃO CONHECIDA E/OU IMPROCEDENTE acerca da notificação judicial ou extrajudicial à CONTRATADA, na hipótese do não cumprimento de suas obrigações contratuais.

5.7.1. Se o valor da garantia for utilizado, total ou parcialmente, cobrança de penalidade aplicada ou pagamento de qualquer obrigação da CONTRATADA, deverá ser efetuada a reposição do valor no prazo de 15 (quinze) dias úteis, contados da data em que for notificada para fazê-lo.

5.8. Caso haja aditamento contratual que implique alteração do valor, a garantia oferecida deverá ser atualizada.

5.9. Não sendo a garantia executada por força de penalidade administrativa e não havendo débitos a saldar com a CONTRATANTE, a garantia prestada será devolvida ao término do contrato.

5.10. Quando prestada em dinheiro, a garantia será devolvida por meio de depósito em conta bancária e corrigida pelos índices da poupança, salvo na hipótese de aplicações de penalidades pecuniárias ou necessidade de ressarcimento de prejuízos causados pela CONTRATADA à CONTRATANTE ou a terceiros, hipóteses em que será restituído o saldo remanescente.

5.10.1. Na hipótese de garantia em dinheiro, a CONTRATADA deverá enviar uma cópia do depósito bancário para o e-mail contratosfornecedores@prodam.sp.gov.br, identificando o contrato e a que título foi realizado o depósito.

CLÁUSULA VI – FATURAMENTO E CONDIÇÕES DE PAGAMENTO

6.1. CONDIÇÕES DE FATURAMENTO

6.1.1. O faturamento do Appliance (hardware dedicado) de inspeção de segurança (ITEM 1) será efetuado integralmente, em parcela única, a partir da entrega pela CONTRATADA à CONTRATANTE e após a emissão pela CONTRATANTE do Termo de Aceite e Recebimento, anexo.

6.1.2. O faturamento do serviço de Suporte Técnico, Manutenção e Garantia do item 1 appliance (hardware dedicado) para inspeção de segurança (ITEM 2) será efetuado em parcelas mensais de igual valor, a partir da emissão pela CONTRATANTE do "Termo de Aceite e Recebimento".

6.1.3. O faturamento das Licenças para Auditoria, Análise de Eventos e Governança de Dados (ITEM 3) será em parcela única, a partir da entrega pela CONTRATADA à CONTRATANTE e após emissão pela CONTRATANTE do Termo de Aceite e Recebimento das licenças.

6.1.4. O faturamento dos Serviços de Instalação e Configuração da solução (ITEM 4), será efetuado em parcela única, após a emissão pela CONTRATANTE do "Termo de Aceite e Recebimento".

6.1.5. O faturamento do Serviço de Operação Assistida (ITEM 5) será efetuado em parcelas mensais de igual valor, a partir da emissão pela CONTRATANTE do "Termo de Aceite e Recebimento das Licenças".

6.1.6. O faturamento dos Treinamentos (ITEM 6) ministrados pela CONTRATADA, será efetuado em parcela única ao término de cada turma de treinamento e após a emissão pela CONTRATANTE do Termo de Aceite e Recebimento do Treinamento.

6.2. CONDIÇÕES DE PAGAMENTO

6.2.1. A Nota Fiscal Eletrônica de Serviços deverá ser emitida e encaminhada à CONTRATANTE, através do setor competente, por meio do endereço eletrônico gfl@prodam.sp.gov.br, caso o CONTRATANTE seja a PRODAM. Nos casos em que a CONTRATANTE seja uma Secretaria ou outro órgão público que aderir à ARP, o modo de entrega deverá ser estabelecido quando da formalização do instrumento contratual.

6.2.2. Após o recebimento da Nota Fiscal Eletrônica de Serviços, a CONTRATANTE disporá de até 05 (cinco) dias úteis para emissão do Termo de Aceite de Pagamento, aprovando os serviços prestados.

6.2.3. O pagamento será realizado por intermédio de crédito em conta corrente ou por outra modalidade que possa vir a ser determinada pelo departamento responsável da CONTRATANTE, em 30 (trinta dias) dias corridos a contar da data de emissão do Termo de Aceite de Pagamento.

6.2.4. Caso a Nota Fiscal Eletrônica de Serviço contenha divergências com relação ao estabelecido no Instrumento Contratual, a CONTRATANTE ficará obrigada a comunicar a empresa CONTRATADA, formalmente, o motivo da não aprovação no prazo de 05 (cinco) dias úteis. A devolução da Nota Fiscal Eletrônica de serviços, devidamente, regularizada pela CONTRATADA, deverá ser efetuada em até 05 (cinco) dias úteis da data de comunicação formal realizada pela CONTRATANTE.

6.2.5. Em caso de atraso de pagamento dos valores devidos à CONTRATADA, mediante requerimento formalizado por esta, incidirão juros moratórios calculados utilizando-se o índice oficial de remuneração básica da caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança, para fins de compensação da mora (TR + 0,5% "pro-rata tempore"), observando-se para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorreu.

CLÁUSULA VII – MATRIZ DE RISCOS

7.1. Tendo como premissa a obtenção do melhor custo contratual mediante a alocação do risco à parte com maior capacidade para geri-lo e absorvê-lo, as partes identificam os riscos decorrentes da presente relação contratual e, sem prejuízo de outras previsões contratuais, estabelecem os respectivos responsáveis na Matriz de Riscos constante no **ANEXO ___** parte integrante deste contrato.

7.2. É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados, na Matriz de Riscos, como de responsabilidade da CONTRATADA.

CLÁUSULA VIII – CONFORMIDADE

8.1. A CONTRATADA, com relação às atividades, operações, serviços e trabalhos vinculados ao objeto do presente contrato, declara e garante o cumprimento dos dispositivos da **Lei Anticorrupção – Lei 12.846/2013, e dos dispositivos 327, *caput*, § § 1º e 2º e 337-D do Código Penal Brasileiro**.

8.2. A CONTRATADA deverá defender, indenizar e manter a CONTRATANTE isenta de responsabilidade em relação a quaisquer reivindicações, danos, perdas, multas, custos e despesas, decorrentes ou relacionadas a qualquer descumprimento pela CONTRATADA das garantias e declarações previstas nesta cláusula e nas Leis Anticorrupção.

8.3. A CONTRATADA reportará, por escrito, para o endereço eletrônico a ser fornecido oportunamente, qualquer solicitação, explícita ou implícita, de qualquer vantagem pessoal feita por empregado da CONTRATANTE para a CONTRATADA ou para qualquer membro da CONTRATADA, com relação às atividades, operações, serviços e trabalhos vinculados ao objeto do presente contrato.

8.4. Para a execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma a ele não relacionada, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma, nos termos do **Decreto n.º 56.633/2015.**

8.5. O descumprimento das obrigações previstas nesta Cláusula poderá submeter à CONTRATADA à rescisão unilateral do contrato, a critério da CONTRATANTE, sem prejuízo da aplicação das sanções penais e administrativas cabíveis e, também, da instauração do processo administrativo de responsabilização de que tratam a **Lei Federal nº 12.846/2013.**

CLÁUSULA IX – DA PROTEÇÃO DE DADOS

9.1. A **CONTRATADA**, obriga-se, sempre que aplicável, a atuar no presente Contrato em conformidade com a legislação vigente sobre Proteção de Dados Pessoais e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, não colocando, por seus atos ou por omissão a **PRODAM-SP** em situação de violação das leis de privacidade, em especial, a **Lei nº 13.709/2018 – Lei Geral de Dados Pessoais ("LGPD").**

9.2. Caso exista modificação dos textos legais acima indicados ou de qualquer outro, de forma que exija modificações na estrutura do escopo deste Contrato ou na execução das atividades ligadas a este Contrato, a **CONTRATADA** deverá adequar-se às condições vigentes. Se houver alguma disposição que impeça a continuidade do Contrato conforme as disposições acordadas, a **PRODAM-SP** poderá resolvê-lo sem qualquer penalidade, apurando-se os serviços prestados e/ou produtos fornecidos até a data da rescisão e consequentemente os valores devidos correspondentes.

9.3. A **CONTRATADA** se compromete a:

i) Zelar pelo uso adequado dos dados aos quais venha a ter acesso, cuidando da sua integridade, confidencialidade e disponibilidade, bem como da infraestrutura de tecnologia da informação;

ii) Seguir as instruções recebidas da **PRODAM-SP** em relação ao tratamento dos Dados Pessoais, além de observar e cumprir as normas legais vigentes aplicáveis, sob pena de arcar com as perdas e danos que eventualmente possa causar à **PRODAM-SP**, aos seus colaboradores, clientes e fornecedores, sem prejuízo das demais sanções aplicáveis;

iii) Responsabilizar-se, quando for o caso, pela anonimização dos dados fornecidos pela **PRODAM-SP;**

iv) A **CONTRATADA** deverá notificar a **PRODAM-SP** em 24 (vinte e quatro) horas de **(i)** qualquer não cumprimento (ainda que suspeito) das obrigações legais relativas à proteção de Dados Pessoais; **(ii)** qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais; e **(iii)** qualquer violação de segurança no âmbito das atividades da **CONTRATADA**;

v) A **CONTRATADA** deverá notificar a **PRODAM-SP** sobre quaisquer solicitações dos titulares de Dados Pessoais que venha a receber, como, por exemplo, mas não se limitando, a questões como correção, exclusão, complementação e bloqueio de dados, e sobre as ordens de tribunais, autoridade pública e regulamentadores competentes, e quaisquer outras exposições ou ameaças em relação à conformidade com a proteção de dados identificadas pelo mesmo;

vi) Auxiliar a **PRODAM-SP** com as suas obrigações judiciais ou administrativas aplicáveis, de acordo com a LGPD e outras leis de privacidade aplicáveis, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança.

9.4. A **CONTRATADA** deverá manter registro das operações de tratamento de Dados Pessoais que realizar, bem como implementar medidas técnicas e organizacionais necessárias para proteger os dados contra a destruição, acidental ou ilícita, a perda, a alteração, a comunicação

ou difusão ou o acesso não autorizado, além de garantir que o ambiente (seja ele físico ou lógico) utilizado para o tratamento de Dados Pessoais é estruturado de forma a atender os requisitos de segurança, os padrões de boas práticas de governança e os princípios gerais previstos na legislação e nas demais normas regulamentares aplicáveis.

9.5. A **PRODAM-SP** terá o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade da **CONTRATADA** com as obrigações de Proteção de Dados Pessoais, sem que isso implique em qualquer diminuição da responsabilidade que a **CONTRATADA** possui perante a LGPD e este Contrato.

9.6. A **CONTRATADA** declara conhecer e que irá seguir todas as políticas de segurança da informação e privacidade da **PRODAM**, bem como realizará treinamentos internos de conscientização a fim de envidar os maiores esforços para evitar o vazamento de dados, seja por meio físico ou digital, acidental ou por meio de invasão de sistemas de software.

9.7. O presente Contrato não transfere a propriedade de quaisquer dados da **PRODAM-SP** ou dos clientes desta para a **CONTRATADA**.

9.8. A **PRODAM-SP** não autoriza a **CONTRATADA** a usar, compartilhar ou comercializar quaisquer eventuais elementos de dados, que se originem ou sejam criados a partir do tratamento de Dados Pessoais, estabelecido por este Contrato.

CLÁUSULA X – SANÇÕES ADMINISTRATIVAS

10.1. A CONTRATADA está sujeita às penalidades previstas na **Lei Federal nº 13.303/16**, sem prejuízo da apuração de perdas e danos, em especial:

a) Advertência por escrito;

b) **Multa de até 10% (dez por cento**) sobre o valor total do instrumento contratual ou da parcela correspondente, se o serviço prestado estiver em desacordo com as especificações contidas no **Termo de Referência – ANEXO I** do Edital;

c) **Multa de 1%** (um por cento) sobre o valor total do instrumento contratual, ou parcela equivalente, pelo descumprimento de qualquer outra condição fixada neste contrato e não abrangida nas alíneas anteriores, e na reincidência, o dobro, sem prejuízo da responsabilidade civil e criminal que couber;

d) **Multa de 20% (vinte por cento)** sobre o valor total do instrumento contratual, no caso de rescisão e/ou cancelamento do contrato por culpa ou a requerimento da CONTRATADA, sem motivo justificado ou amparo legal, a critério da CONTRATANTE.

e) **Suspensão** temporária de participação em licitação e **impedimento** de contratar com a PRODAM-SP, pelo prazo de até 02 (dois) anos.

f) Demais sanções encontram-se enumeradas no item 7 do Termo de Referência – ANEXO I.

10.2. Para a cobrança, pela CONTRATANTE, de quaisquer valores da CONTRATADA, a qualquer título, a garantia contratual prevista neste instrumento poderá ser executada na forma da lei.

10.3. Previamente a aplicação de quaisquer penalidades a CONTRATADA será notificada pela CONTRATANTE a apresentar defesa prévia, no prazo de 10 (dez) dias úteis, contados do recebimento da notificação que será enviada ao endereço constante do preâmbulo do Contrato.

10.4. Considera-se recebida a notificação na data da assinatura do aviso de recebimento ou, na ausência deste, a data constante na consulta de andamento de entrega realizada no site dos correios, sendo certificado nos autos do processo administrativo correspondente qualquer destas datas.

10.4.1. Caso haja recusa da CONTRATADA em receber a notificação, esta será considerada recebida na data da recusa, contando a partir desta data o prazo para interposição da defesa prévia.

10.5. A aplicação de penalidade de multa não impede a responsabilidade da CONTRATADA por perdas e danos decorrente de descumprimento total ou parcial do contrato.

10.6. A aplicação de quaisquer multas pecuniárias não implica renúncia, pela PRODAM-SP, do direito ao ressarcimento dos prejuízos apurados e que sobejarem o valor das multas cobradas.

10.7. As decisões da Administração Pública referentes à efetiva aplicação da penalidade ou sua dispensa serão publicadas no Diário Oficial Cidade de São Paulo, sendo certo que a aplicação das penalidades de advertência e multa se efetivará apenas pela publicação no referido Diário, desnecessária a intimação pessoal.

CLÁUSULA XI – RESCISÃO

11.1. A **PRODAM-SP** poderá rescindir o presente contrato, nos termos do **artigo 473, do Código Civil**, nas seguintes hipóteses:

a) Inexecução total do contrato, incluindo a hipótese prevista no **artigo 395, parágrafo único do Código Civil;**
b) Atraso injustificado no início do serviço;
c) Paralisação do serviço, sem justa causa e prévia comunicação à **PRODAM-SP**;
d) Cometimento reiterado de faltas na sua execução que impeçam o prosseguimento do contrato;
e) Transferência, no todo ou em parte, deste contrato, sem prévia e expressa autorização da CONTRATANTE;
f) Decretação de falência;
g) Dissolução da sociedade;
h) Descumprimento do disposto no **inciso XXXIII do artigo 7º da Constituição Federal**, que proíbe o trabalho noturno, perigoso ou insalubre a menores de 18 anos e qualquer trabalho a menores de 16 anos, salvo na condição de aprendiz, a partir de 14 anos;
i) Prática pela CONTRATADA de atos lesivos à Administração Pública previstos na **Lei nº 8.429/1992 (Lei de Improbidade Administrativa) e Lei nº 12.846/2013 (Lei Anticorrupção);**
j) Prática de atos que prejudiquem ou comprometam a imagem ou reputação da PRODAM, direta ou indiretamente;

11.1.1. A rescisão a que se refere esta cláusula, deverá ser precedida de comunicação escrita e fundamentada da parte interessada e ser enviada à outra parte com antecedência mínima de 10

(dez) dias.

11.2. Desde que haja conveniência para a **PRODAM-SP**, a rescisão amigável é possível, por acordo entre as partes devidamente reduzido a termo no competente processo administrativo.

11.3. Poderá haver também rescisão por determinação judicial nos casos previstos pela legislação.

11.4. A rescisão administrativa ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.

11.5 Não constituem causas de rescisão contratual o não cumprimento das obrigações aqui assumidas em decorrência dos fatos que independam da vontade das partes, tais como os que configurem caso fortuito e força maior, previstos no **artigo 393, do Código Civil**.

11.6 Os efeitos da rescisão do contrato serão operados a partir da comunicação escrita, ou, na impossibilidade de notificação do interessado, por meio de publicação oficial; ou da decisão judicial, se for o caso.

CLÁUSULA XII – DISPOSIÇÕES GERAIS

12.1. Os termos e disposições deste contrato prevalecerão sobre quaisquer outros entendimentos ou acordos anteriores entre as partes, explícitos ou implícitos, referentes às condições nele estabelecidas.

> **12.1.1** O presente instrumento e suas cláusulas se regulam pela Lei Federal nº 13.303/16, em casos omissos, pelos preceitos do ordenamento jurídico brasileiro aplicáveis aos entes de natureza pública e privada à hipótese de contratação.

12.2. A CONTRATADA deverá, sob pena de rejeição, indicar o número deste contrato do **Edital do Pregão Eletrônico PE nº 06.001/2023** nas faturas pertinentes, que deverão ser preenchidas com clareza, por meios eletrônicos, à máquina ou em letra de forma.

12.3. A inadimplência do contratado quanto aos encargos trabalhistas, fiscais e comerciais não transfere à empresa pública ou à sociedade de economia mista a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato ou restringir a regularização e o uso das obras e edificações, inclusive perante o Registro de Imóveis.

12.4. A mera tolerância do descumprimento de qualquer obrigação não implicará perdão, renúncia, novação ou alteração do pactuado.

12.5. Na hipótese de ocorrência de fatos imprevisíveis que reflitam nos preços dos serviços, tornando-o inexequível, poderão as partes proceder a revisão dos mesmos, de acordo com o disposto no **artigo 81, § 5º, da Lei Federal nº 13.303/16**.

12.6. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e o CONTRATANTE, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

12.7. A formalização do presente contrato abrange as disposições contratuais e de todos os seus anexos.

CLÁUSULA XIII – VINCULAÇÃO AO EDITAL

13.1. O cumprimento deste contrato está vinculado aos termos do **Edital do Pregão Eletrônico nº 06.001/2023** e seus anexos e à proposta da CONTRATADA.

CLÁUSULA XIV – FORO

14.1. As partes elegem o Foro Cível da Comarca da Capital de São Paulo, com renúncia de qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas que possam surgir no decorrer da execução deste contrato.

E por estarem assim, justas e contratadas, assinam as partes o presente instrumento em 2 (duas) vias de igual teor, perante 2 (duas) testemunhas abaixo.

São Paulo/SP, _____ de _____ de 20__.

CONTRATANTE:

CONTRATADA:

TESTEMUNHAS:

1. 2.

ANEXO III - MATRIZ DE RISCOS

Risco	Definição	Alocação (público, privado ou compartilhado)	Impacto (alto, médio, baixo)	Probabilidade (frequente, provável, ocasional, remota ou improvável)	Mitigação (medidas, procedimentos ou mecanismos para minimizar)
Aumento da quantidade de usuários/credenciais prevista (60.000)	Inclusão de novos usuários na ferramenta, aumentando a quantidades de licenças previstas	Compartilhado	Médio	Remota	Revisar o contrato e incluindo a nova quantidade usuários/credenciais
Mudanças Tributárias	Mudanças na legislação tributária que aumente ou diminua custo, exceto mudança na legislação do IR	Compartilhado	Médio	Remota	Recomposição do equilíbrio econômico-financeiro.