TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

ESTUDO TÉCNICO PRELIMINAR - TJ/AM/SETIC/DVITIC

Responsáveis pela elaboração:

Washington Neto

Diogo Mendonça

Categoria do Objeto: Serviços de segurança da informação e privilégios de Acesso.

1. PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL

1.1. A contratação está prevista no Plano de Contratações Anual de 2024, aprovado pela Resolução TJAM nº 52/2023, podendo ser consultado através do link: https://bit.ly/pca2024.

1.2. A presente demanda encontra-se registrada sob o Código PCA SETIC-2024-25 do referido documento.

2. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. O TJAM possui diversos usuários internos, incluindo servidores, comissionados, terceirizados, estagiários, requisitados e afastados, além de inúmeros usuários externos que utilizam os sistemas e serviços disponibilizados, serviços digitais, sites e sistemas à sociedade.

2.1.1 Para o acesso dos envolvidos é imprescindível que os diversos recursos de Tecnologia da Informação e Comunicação, como, por exemplo: servidores, computadores, internet, sistemas, aplicações, serviços, e-mail, sites, dentre outros tantos, estejam seguros e acessíveis.

2.1.2 Cada novo sistema, equipamento e software que passa a integrar o parque computacional deste órgão, disponibiliza credenciais, contas e acessos de alto poder administrativo. Essas credenciais são as mais críticas e poderosas dentro da infraestrutura de TIC e da área de desenvolvimento. Sendo extremamente visadas por ataques cibernéticos para obter recursos e acesso a dados confidenciais.

2.2. Diante disso, garantir que toda essa gama de recursos tenha pleno funcionamento é uma competência da Secretaria de Tecnologia da Informação e Comunicação (SETIC). Nesse sentido, observa-se como principal desafio a garantia da sustentação do ambiente tecnológico, que requer trabalho constante devido às atualizações contínuas relacionadas a esta área.

2.2.1 Todo esse complexo de atividades é essencial para dar suporte seguro às áreas meio e finalísticas do TJAM, de modo que possam desempenhar suas funções legais e assim realizar a missão institucional, e caso alguma dessas áreas seja prejudicada, estará prejudicando também, diretamente, a função institucional perante o Governo e a sociedade.

2.2.2 Credenciais, contas e acessos administrativos são necessários para administradores, serviços e dispositivos acessarem sistemas críticos como, servidores, aplicações, bancos de dados, sistemas operacionais, switches, firewalls, roteadores, entre outros, localizados no data center local ou na nuvem.

2.2.3 Os acessos de alto privilégio podem parecer muito vantajosos em termos de prerrogativas de controle sobre o parque tecnológico, entretanto o cenário se torna rapidamente desencorajador quando se conhecem os riscos e ameaças envolvidas. Muitos riscos surgem como resultado desse tipo de acesso e podem advir de invasores externos e usuários maliciosos dentro da própria empresa.

2.2.4 Se uma conta, credencial ou acesso que fornece permissões privilegiadas para sistemas e ativos confidenciais é comprometida, isso pode resultar em danos significativos para o órgão e o governo, e permitir ao atacante realizar ações drásticas como: vazamento ou roubo de dados confidenciais que levam a problemas financeiros e danos à reputação, liberação de acesso a servidores de comando e controle (isso é tipicamente um sistema que permite que um atacante fique escondido em sua rede operando sistemas remotamente, extraindo dados, sem ser percebido), captura da atividade do usuário (como pressionamentos de tecla: tudo o que comunicar eletronicamente) e instalação de software indevido na máquina acessada (malware), bloqueio de usuários verdadeiros em suas máquinas para que apenas o invasor tenha acesso (ransomware), realização de mineração de moeda criptografada ilegal ou não autorizada.

2.3. As motivações também estão alinhadas com as recomendações de diferentes órgãos e instruções normativas à respeito da adoção de controles gerais de segurança da informação, dentre os quais destacam-se:

2.3.1 O decreto 10.222, de 5 de fevereiro de 2020, que dispõe sobre a Estratégia Nacional de Segurança Cibernética, tem como um dos seus objetivos a elevação do nível de proteção do Governo, onde cita: “Aperfeiçoar e manter atualizados os sistemas informacionais, as infraestruturas e os sistemas de comunicação dos órgãos públicos, em relação aos requisitos de segurança cibernética".

2.3.2 A Lei 13.709, de 14 de agosto de 2018, intitulada como a Lei Geral de Proteção de Dados Pessoais (LGPD), em seu artigo 46 cita que: “os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”.

2.3.3 A Resolução 370 de 28/01/2021, Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), onde orientada em seu preâmbulo pelos objetivos dos seguintes componentes: “Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados”.

2.3.4 Na Resolução 396 de 07/06/2021 do CNJ, que institui a Instituir a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ) no âmbito dos órgãos do Poder Judiciário, à exceção do Supremo Tribunal Federal (STF), destaca-se o artigo:

"Art. 9º São ações da ENSEC-PJ:

I - fortalecer as ações de governança cibernética;

II - elevar o nível de segurança das infraestruturas críticas;

III - estabelecer rede de cooperação do Judiciário para a segurança cibernética;

IV - estabelecer modelo centralizado de governança cibernética nacional."

2.3.5. Diante do exposto e considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e o risco de vazamento de credenciais, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas neste Tribunal, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

3. UNIDADE DEMANDANTE

3.1. Secretaria de Tecnologia da Informação e Comunicação do TJAM.

4. REQUISITOS DA CONTRATAÇÃO

4.1 O serviço objeto da contratação pretendida é a aquisição de produtos com características comuns de mercado e, também, possui natureza continuada, uma vez que ocorra a interrupção, pode comprometer a continuidade das atividades do TJAM, tendo em vista que a solução implementa segurança através da mediação de credenciais privilegiadas, desta forma, a interrupção da solução implica em interrupção no acesso aos recursos gerenciados pelas referidas credenciais. Além do mais, a Resolução CNJ 396/2021, que estabelece a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-JUD), em seu capítulo 8, artigo 29, que trata sobre gestão de usuários elabora as seguintes determinações:

> "Art. 29. Cada órgão do Poder Judiciário, com exceção do STF, deverá implementar a gestão de usuários de sistemas informatizados composta de:
> I – gerenciamento de identidades;
> II – gerenciamento de acessos; e
> III – gerenciamento de privilégios.
> Parágrafo único. A gestão de usuários será disciplinada por ato do Presidente do CNJ, que definirá o padrão a ser adotado para utilização de credenciais de login único e interface de interação dos sistemas, com o objetivo de uniformizar e garantir a experiência única de interação com os sistemas judiciais."

4.2. A Contratada deverá observar, no que couber, as práticas e os critérios de sustentabilidade disponíveis respectivamente no Guia Prático de Critérios de Sustentabilidade para Compras no TJAM e na Política Nacional de Resíduos Sólidos, instituída pela Lei nº 12.305, de 2 de agosto de 2010.

4.3. A duração do contrato de prestação de serviços de natureza continuada será de 12 meses.

4.4. Por tratar-se de serviço comum, já que possui padrões de desempenho e características gerais e específicas, usualmente encontradas no mercado, sugerimos que o objeto seja licitado por meio da modalidade Pregão Eletrônico por menor preço global.

4.5 A transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas promove uma relação mais transparente e colaborativa entre as partes envolvidas. Ao adquirir o conhecimento e expertise, o órgão e setor responsável pelo mantenimento das operações demonstram comprometimento e responsabilidade com o sucesso do projeto, fortalecendo a confiança de autonomia na execução de atividades com complexidade aceitável, minimizando o tempo de espera e retorno às operações em caso de interrupções.

4.5.1. A transferência de conhecimento é essencial para garantir a continuidade das operações e a qualidade dos serviços prestados. Ao compartilhar informações relevantes sobre processos, metodologias e expertise acumulada durante a execução do contrato, torna-se capaz de assegurar que o órgão CONTRATANTE esteja plenamente capacitado para dar continuidade às atividades, minimizando qualquer interrupção ou perda de eficiência.

4.5.2. Ainda dentro da necessidade de aprendizado e absorção de conhecimento, a transferência de tecnologia e técnicas empregadas é crucial para manter o progresso e o desenvolvimento do projeto ou serviço contratado. Ao repassar as ferramentas e os métodos utilizados, nos é possibilitado que possamos explorar plenamente os recursos e obter resultados satisfatórios. Isso também contribui para a autonomia da contratante no futuro, permitindo que ela faça melhorias e adaptações de acordo com as necessidades específicas.

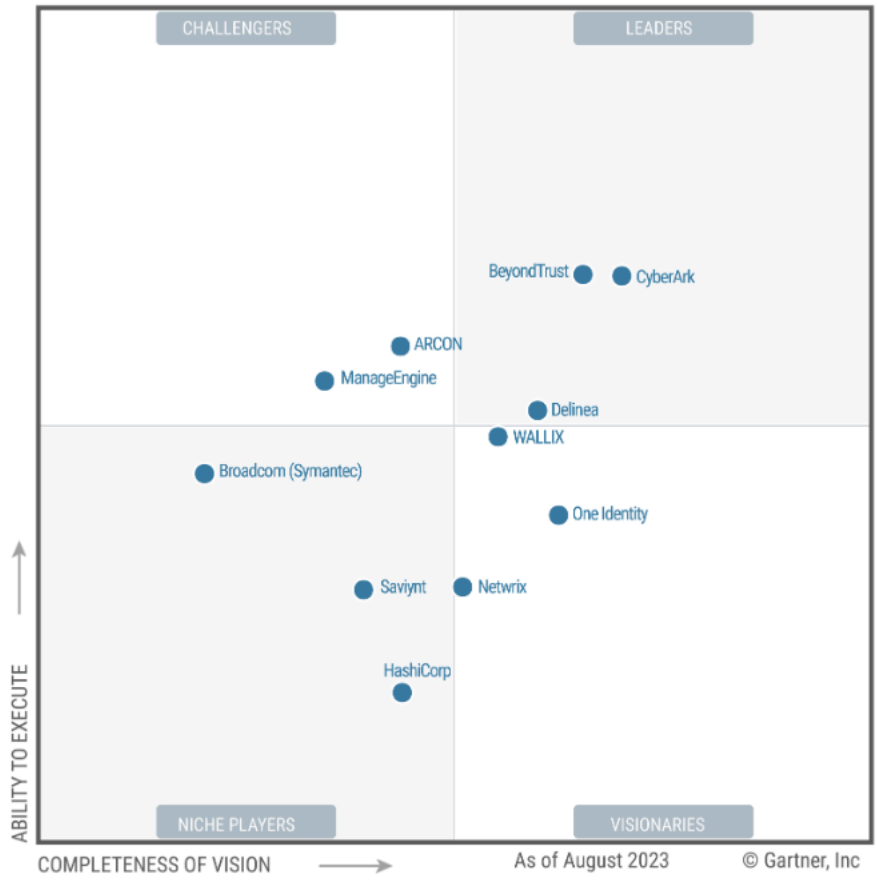
4.6. Por fim, sugerimos que se utilize o sistema de Registro de Preço para esta pretensa contratação.

5. LEVANTAMENTO DE MERCADO E JUSTIFICATIVA DA ESCOLHA DO TIPO DE SOLUÇÃO A CONTRATAR

5.1 Como solução mercadológica que venha a atender as necessidades deste Tribunal não se vislumbra outra que não seja a contratação de empresa especializada no fornecimento de solução de gerenciamento de acessos privilegiados (PAM – Privileged Access Management), com diversas funcionalidades tais como análise comportamental, auditoria de credenciais, mitigações contra roubos e abusos de privilégios e aplicação do "privilégio mínimo" nos ativos protegidos, tudo isso com a finalidade de aumentar a proteção das credenciais utilizadas no âmbito do Tribunal e impedir que essas credenciais sejam usadas por agentes potenciais atacantes, prevenindo danos decorrentes de ataques cibernéticos que possam ser realizadas conta o tribunal.

5.2 Sendo uma solução comum de mercado, existem diversos fabricantes que podem oferecer soluções de proteção de credenciais, com diferentes graus de qualidade e diversos preços a serem pagos. Sendo inviável avaliar todas as opções disponíveis, recorreu-se ao Gartner, que é empresa amplamente respeitada e prestigiada no campo da Tecnologia da Informação, servido como referência na área, para delimitar as melhores opções a serem consideradas em processos de aquisição.

Figure 1: Magic Quadrant for Privileged Access Management



5.3 O Gartner realiza a mensuração da qualidade e relevância de soluções de TI através de um gráfico que ficou conhecido como "Quadrante", o qual reflete os estudos publicados anualmente sobre categorias de produtos e serviços, cuja composição utiliza diversos critérios para medir a qualidade das soluções oferecidas pelas empresas que atuam naquela categoria. Como o TJAM preza pela qualidade das soluções contratadas para compor sua infraestrutura tecnológica, as soluções

consideradas foram as que se estavam mais bem posicionadas no quadrante “Leaders” (líderes) da avaliação mais recente, publicada em Agosto de 2023. Os fabricantes mais bem localizados neste quadrante foram avaliados com os melhores resultados em suas soluções oferecidas.

5.4 Ao que podemos verificar no quadrante do Gartner, os três fabricantes que estão melhor posicionados são a CyberArk, BeyondTrust e Delinea.Cumprindo lembrar que o TJAM ainda não possui qualquer solução de gerenciamento de acessos privilegiados.

5.5 Contratações públicas similares

5.5.1 Dado que o objeto da contratação é um elemento essencial para a construção de um ecossistema de segurança da informação no âmbito do TJAM, tendo sido observado a sua contribuição na garantia da segurança da informação no âmbito da administração pública municipal, estadual e federal, com diversos órgãos dos mais variados tamanhos e com a mais diversas funções o possuindo em sua infraestrutura de TI. As contratações mencionadas abaixo, guardadas as peculiaridades de cada órgão, são similares ao objeto que o TJAM pretende adquirir:

5.5.1.1 Destaca-se a solução contratada pelo Tribunal do Estado do Pará que, através da Ata de Registro de Preço (ARP) nº 16/2020 do Tribunal Regional do Trabalho da 8º Região, formalizada pelo Pregão Eletrônico 34/2020, registrou preços para o objeto: “aquisição de Solução de Gerenciamento de Acesso Privilegiado (Privileged Access Management – PAM) e Monitoramento e Análise Comportamental, com possibilidade de proteção, monitoramento, detecção e resposta a atividade de conta privilegiada, armazenamento de senhas e mitigação de riscos”.

5.5.1.2 A solução contratada pelo Tribunal Regional do Trabalho da 8ª Região (TRT8) que, através da Ata de Registro de Preço (ARP) nº 16/2020 gerada no Pregão Eletrônico 34/2020, registrou preços para o objeto: “aquisição de Solução de Gerenciamento de Acesso Privilegiado (Privileged Access Management – PAM) e Monitoramento e Análise Comportamental, com possibilidade de proteção, monitoramento, detecção e resposta a atividade de conta privilegiada, armazenamento de senhas e mitigação de riscos”.

5.5.1.3 Tribunal de Justiça do Distrito Federal e Territórios (TJDFT), através do item 1 do contrato 250/2019, gerado através do Pregão Eletrônico 065/2019, adquiriu solução similar ao objeto de contratação do TJPA. cujo objeto é a: “a aquisição, suporte e atualização de solução de segurança da informação para a gestão de acessos privilegiados, armazenamento de credenciais, que possibilite o isolamento, gravação e o monitoramento de sessões de ativos de TIC do CONTRATANTE por um período de até 36 (trinta e seis) meses, incluindo serviço de instalação e repasse de conhecimento”.

5.5.1.4 A Secretaria de Fazenda do Estado de Santa Catarina (SEFAZ-SC) que, através do Pregão Eletrônico 0024/2020, registrou preços para o objeto: “Contratação de empresa especializada objetivando o fornecimento de solução de segurança integrada em ambientes críticos, incluindo serviços de implantação da solução, repasse de conhecimento, garantia e suporte”.

5.5.1.5 A Imprensa Nacional que, através do Pregão nº 04/2021 e ATA de Registro de Preço 005/2022, registrou preços para o objeto: contratação de empresa especializada no fornecimento de Solução de Segurança para Privilégios e Acessos a Sistemas Críticos, incluindo instalação, atualização de versão, transferência de conhecimento, suporte técnico e garantia.

5.6. Escolha e Justificativa da Solução

5.6.1 As soluções oferecidas pelos fabricantes classificados como líderes no quadrante do Gartner, foram avaliadas pela SETIC e atendem aos padrões técnicos e de confiabilidade exigidos.

5.6.2. Comparativo de Requisitos Tecnológicos

5.6.2.1 Itens em Verde (Plenamente Atendido), Itens em Amarelo (Parcialmente Atendido) e Itens em Vermelho (Não atende);

Requisitos	Delinea	Cyberark	BeyoundTr
Prover mecanismos de segurança da informação			
Abranger todos os tipos de acessos e identidades			
Assegurar mecanismos de gerenciamento de privilégios elevados			
Prover registro de uso de privilégio e trilhas de auditoria			
Detectar e mitigar incidentes de forma mais eficaz através de mecanismos de inteligência artificial			
Ganhar agilidade e eficiência no tratamento de incidentes e na criação de relatórios			
Confiança zero (zero trust) para identidades			
Prover políticas para acessos adaptativos baseados em riscos e contextos conhecidos de uma autenticação			
Prover múltiplo fator de autenticação para diversos casos de uso com capacidade de interpretação de risco adaptativo			
Prover capacidade de acesso remoto a infraestrutura privilegiada e aplicações web de negócio sem VPN			
Prover ganhos operacionais para recuperação de acessos e senhas			
Gravação e proteção de sessões de aplicações do tipo web de negócio de forma não intrusiva			
Possuir a capacidade de disparar gatilhos de gravação em vídeo relacionado a ações do usuário na estação de trabalho que estejam cumprindo atividades críticas			
Proteger identidades, credenciais e acessos de forma fim-a-fim			
Proteger silos de armazenamento de credenciais em servidores e estações			
Possuir capacidade de definição de políticas granulares para cada etapa da proteção de identidades			
Deve se comunicar com outras ferramentas de segurança e ampla capacidade de integrações			
Portal de Login Único para aplicações (SSO, Single Sign-On)			
Gestão de senhas de aplicações de negócio que não suportam SingleSign-On (login único)			
Diretório em nuvem IDP (Identity Provider)			
Prover licenciamento em modalidade simples, preferencialmente, poridentidade			
Capacidade de gestão de senhas para usuários de negócio, com armazenamento em cofre de senhas			
Capacidade de controle de autenticação e autorização em nível granular para identidades não humanas			
Capacidade de proteção para chaves de API			
Capacidade de proteção de identidades não humanas em plataformas de conteinerização			
Disponibilizar pacote de desenvolvimento para proteção de identidades não humanas			
Capacidade de proteção de identidade não humanas para aplicações tradicionais (não conteinerizadas ou não nativas em nuvem)			

5.6.2.2 Agrupando o resultado da análise dos requisitos tecnológicos referente a cada uma das soluções, temos o seguinte quantitativo:

Requisitos	Delinea	Cyberark	BeyondTrust
Plenamente Atendido	7	27	7
Parcialmente Atendido	7	0	7
Não atendido	13	0	13

5.7. Baseado nos requisitos técnicos e em pesquisas de mercado, a CyberArk ganhou mais destaque ao longo dos últimos anos, sendo reconhecido como um dos principais fornecedores de soluções de gestão de privilégios. Além disso, constatou-se que foi a solução mais implantada nos órgãos públicos. Como exemplo: TJAP, TJPA, TJDFT, TRT8 e outros.

6. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

6.1. A solução escolhida deve abranger os itens descritos no quadro abaixo:

ITEM	CÓDIGO SIASG	ESPECIFICAÇÕES
1	27502	Solução de Segurança para Identidades e seus Privilégios – Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI, com garantia pelo período de 12 (doze) meses.
2	27502	Solução de Segurança para Identidades e seus Privilégios – Proteção para Aplicações Tradicionais, com garantia pelo período de 12 (doze) meses.
3	27502	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para servidores Windows e Linux, com garantia pelo período de 12 (doze) meses.
4	27502	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para Estações de Trabalho, com garantia pelo período de 12 (doze) meses.
5	26972	Serviço de instalação e configuração para Solução de Segurança para Identidades e seus Privilégios.
6	21172	Transferência de Conhecimento para Solução de Segurança para Identidades e seus Privilégios (turma)
7	27340	Serviço de Suporte Técnico Especializado

6.2 Solução de Segurança para Identidades e seus Privilégios – Proteção e Monitoração de Acessos

6.2.1. Características;
6.2.1.1. A solução deverá atender usuários físicos, equipamentos servidores, estações de trabalho e usuários lógicos e ativos de rede;
6.2.1.2. A solução deve apoiar, no mínimo, aos requisitos (artigos 6, 42, 43, 46, 48 e 50) da Lei Geral de Proteção de Dados-LGPD, como: Determinar como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar em caso de descumprimento; Proteger o acesso a dados pessoais sensíveis; Responsabilizar pessoal e responder a incidentes; Aplicar boas práticas de governança, através de regras que deverão respeitar os preceitos da lei, de maneira a mitigar os riscos inerentes ao tratamento de dados e implementar e demonstrar a efetividade das políticas de segurança relacionadas ao tratamento de dados;
6.2.1.3. Apoiando aos requisitos da LGPD a solução deverá proteger e monitorar acessos a dados pessoais sensíveis por meio da segurança de credenciais e acessos de alto privilégio em serviços críticos, detectando e respondendo rapidamente a incidentes de segurança, identificando e mitigando ações privilegiadas com comportamentos de alto risco, avaliando riscos e testando a efetividade dos processos de proteção de dados por meio de relatórios da solução com identificação e classificação do status de risco do ambiente privilegiado, demonstrando conformidade e prova de que os controles de segurança necessários estão nos lugares certos, provendo análise comportamental, auditoria e segurança dos acessos a sistemas por meio de todas credenciais administrativas de alto privilégio em dispositivos e sistemas-alvo diversos do ambiente;
6.2.1.4. Um sistema-alvo da solução é definido como um servidor, uma estação de trabalho, um ativo de rede e de segurança, dentre outros mencionados a seguir, cujas credenciais de acesso passem a ser protegidas e gerenciadas pela solução;
6.2.1.5. Um usuário da solução é definido como qualquer pessoa que acesse um sistema-alvo mediante logon na solução e uso de credenciais por ela gerenciadas;
6.2.1.6. Deve monitorar sessões, gravar, detectar, correlacionar e mitigar todos comportamentos anormais de, pelo menos, 75 usuários simultâneos acessando todos os sistemas-alvo, dentre eles servidores Linux/Unix ou Windows, Controladores de domínio Microsoft Active Directory, estações de trabalho Windows e demais ativos de rede e sistemas diversos ;
6.2.1.7. A solução deverá ser entregue com acesso remoto privilegiado seguro (externo a rede corporativa) para os usuários simultâneos mencionados, sem a entrega de credenciais privilegiadas e sem a necessidade de instalação e uso de clientes (do tipo VPN ou outros) nos dispositivos dos usuários remotos por todo período contratado;
6.2.1.8. A solução deverá ser entregue com acesso Single-sign-on e múltiplo fator de autenticação adaptativo para, no mínimo, os 75 usuários internos e/ou remotos (externos a rede corporativa) mencionados, por todo período contratado, suportando, no mínimo:
6.2.1.8.1. Usuário e senha dos diretórios suportados, aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para Biometria do tipo FaceID e através do leitor de digital, Smartphone push (Notificação para aprovar ou recusar uma autenticação), Geolocalização através de coordenadas GPS e banco de dados de IP, Suporte a tokens OATH OTP, autenticação na tela de login via QRcode sem a necessidade de digitar usuário e senha, com opção de forçar a biometria no dispositivo móvel, Entrega de código via SMS e chamada de voz, perguntas de segurança, notificações por e-mail e telefone celular, tokens OTP (on-line, off-line, por e-mail, hardware);
6.2.1.8.2. Autenticação auto-ajustada baseada no contexto de risco e segurança aprendidos pela solução, permitindo a criação de um perfil para cada usuário, aproveitando atributos históricos e situacionais específicos do mesmo, como localização, dispositivo, rede, horário e índice de risco de comportamento;
6.2.1.8.3. Análise de solicitações de autenticação em relação a padrões históricos, atribuição de índice de risco a cada tentativa de logon, geração de alertas e criação de políticas de bloqueio a serem acionadas quando um comportamento anômalo é detectado e de acesso simplificado quando o usuário é entendido como legítimo;
6.2.1.8.4. Permitir que os usuários adicionem e modifiquem fatores de autenticação diretamente em um portal com definição de período de desvio do múltiplo fator de autenticação;
6.2.1.8.5. Prover relatórios e dashboards customizáveis com detalhamento de informações em tempo real sobre as atividades de autenticação, como falhas na autenticação secundária, tentativas bem-sucedidas de login e os fatores de autenticação mais usados;
6.2.1.8.6. Entenda-se como sistemas-alvo os baseados, em no mínimo, as seguintes tecnologias: S.O.: Linux/Unix e Microsoft Windows; Hypervisors: Acrópolis (Nutanix), VMWare, RedHat KVM e Microsoft Hyper-V; Contas de usuários de sistemas e de serviço; Credenciais do Microsoft COM+, IIS, Apache TomCat, RedHat Jboss, Nginx; Objetos (usuários, grupos e computadores) do Microsoft Active Directory e LDAP; Contas de usuários e administradores de bancos de dados Microsoft SQL Server, Oracle, PostgreSQL; Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) – switches, roteadores, controladores/APs WiFi, SAN (Storage Area Network) e NAS (Network Attached Storage); Contas de usuários e administradores de consoles de gerenciamento de servidores e estações de trabalho; Contas de equipamentos dedicados à segurança, tais como Firewall, IPS, AntiSpam e filtros de conteúdo; Contas de equipamentos dedicados à segurança física, tais como câmeras de vigilância, catracas, etc.; Credenciais de nuvem em Google Workspace, VMWare ESXi, Azure, AWS, GCP, Office 365.
6.2.2. Gestão de dados do ciclo de vida e compartilhamento das contas privilegiadas, monitoramento e gravação de sessões privilegiadas:
6.2.2.1. A solução deve conceder acesso aos sistemas utilizando “Remote Desktop” e “SSH”, disponibilizados pelos sistemas-alvo do ambiente, sem que os usuários vejam qualquer senha e chave (vigentes no momento e providas para as aplicações e conexões remotas, devendo ser recuperadas de forma automática e transparente do repositório seguro de credenciais da solução), garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso a sistemas e aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte do usuário no S.O. do servidor de destino, possibilitando habilitar gravação da sessão, caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino;

6.2.2.2 A solução deve permitir Integração para gestão de acessos privilegiados em serviços de nuvem padrões de mercado, como Amazon Web Services (AWS), Google Cloud, IBM Cloud e Microsoft Azure, disponibilizando no mínimo as seguintes funcionalidades: Integração e gestão de acessos privilegiados em contas de serviços em nuvem; Integração com sessões de serviços de nuvem, incluindo início e finalização de sessão e Gravação e auditoria de acesso de sessões iniciadas em serviços de nuvem;
6.2.2.3. Deve possuir as sessões administrativas acessadas e monitoradas ao vivo, com compartilhamento de tela e controle de periféricos, como teclado e mouse (assistência remota), e por meio de gravação de comandos e vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os comandos e vídeos gerados possam ser indexados para pesquisa futura, permitindo o filtro de comandos e ações executadas ao longo da sessão gravada, possibilitando pesquisar ações específicas na sessão gravada;

6.2.2.4. Proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha (quantidade de caracteres), frequência de troca automatizada das senhas e chaves SSH, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas e mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também de contas que não são gerenciadas de forma centralizada por serviços de diretórios;
6.2.2.5. Descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados e propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas e descobrir e alterar credenciais em ambiente Windows, incluindo contas nomeadas, administradores 'built-in' e convidados, para determinar movimentações laterais (pass-the-hash), exibidas em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento;
6.2.2.6. Gerenciar, de forma segura, senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamento e garantir a implementação dos privilégios mínimos necessários, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado;
6.2.2.7. Possuir funcionalidade de "AD Bridge" para integração de servidores Linux/Unix no Active Directory, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD; Provisionar na plataforma Unix-like as contas e grupos do Active Directory que possuam permissão de acesso, de maneira automatizada e transparente;
6.2.2.8. Permitir a definição de Fluxos de Aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas, com as seguintes características: Personalização de fluxos: permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta, e aprovação de, pelo menos, um responsável; Permitir a aprovação perante um agendamento de ações administrativas; ou seja; a aprovação do acesso ocorrerá em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos; Ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo ou não que a conta descoberta seja gerenciada pela solução; Ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas; A descoberta automática deve ser realizada por buscas no Active Directory (AD) e por intervalos de endereços IP;
6.2.2.9. Oferecer em sua aplicação web diferentes visões e opções de acordo com as permissões dos usuários, mostrando, por exemplo, apenas as funcionalidades delegadas àquele usuário; Suportar métodos para registrar e relatar qualquer ação realizada e detectada pela solução, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados, aplicações syslog, notificações de e-mail;
6.2.2.10. Registrar cada acesso, incluindo os acessos via aplicação web, para solicitações de senha, aprovações, checkout's, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à console de gerenciamento da solução, tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas; logoff dos usuários; Alterações nas funções de delegação; Adições, deleções e alterações de senhas gerenciadas pela solução; Operações das senhas dos usuários, incluindo check-in e check-out, solicitações negadas e permitidas; Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e outros critérios;
6.2.2.11. Deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como: Lista de sistemas gerenciados; Senhas armazenadas; Eventos de alteração de senha; Permissões de acesso web; Auditoria de contas, sistemas e usuários; Alerta em tempo real;
6.2.3. Análise comportamental e mitigações de risco no ambiente crítico:

6.2.3.1. A solução deverá realizar a identificação e o correlacionamento de todas as ações citadas abaixo, montando perfis de comportamento gerais (usuários, acessos, credenciais, máquinas, outros) do ambiente privilegiado e acessos aos sistemas-alvo por meio da solução;
6.2.3.2. Deve combinar ações que caracterizam abusos, comportamentos anormais e fora dos padrões aprendidos/mapeados, aplicando ações mitigatórias automáticas como solicitação de nova autenticação multi-fator, suspensão e encerramento de sessões e troca das credenciais privilegiadas, em caso de atividades suspeitas de alto risco, detectando, no mínimo:
6.2.3.3. Acessos a solução: durante horários irregulares (quando um usuário recupera uma senha de conta privilegiada em uma hora irregular de acordo com seu perfil comportamental); durante dias irregulares (quando um usuário recupera uma senha de conta privilegiada em um dia irregular de acordo com seu perfil comportamental); através de IP irregular e desconhecido (quando um usuário acessa contas privilegiadas de um endereço IP ou sub-rede incomum, de acordo com seu perfil comportamental); não gerenciados (quando uma conexão com uma máquina é feita com uma conta privilegiada que não é gerenciada na solução);
6.2.3.3.1. Acessos gerais: excessivos a contas privilegiadas (quando um usuário acessa contas privilegiadas com mais frequência do que o normal, de acordo com seu perfil comportamental); a uma máquina; anômalos a várias máquinas (quando uma conta efetuou login em um grande número de máquinas inesperadas durante um tempo relativamente curto) e realizados fora da solução (diretamente no sistema-alvo); Usuários incomuns logando de uma máquina de origem conhecida; quando ocorrem indicações de atividade de um usuário inativo da solução; Atividades definidas como suspeitas detectadas em sessões privilegiadas (comandos e anomalias na solução);
6.2.3.3.1.1. Máquinas: acessadas a partir de endereços IP incomuns; acessadas durante horários irregulares, de acordo com seu padrão de utilização; Incomuns originando acessos;
6.2.3.3.1.2. Suspeita de roubo de credenciais, quando um usuário se conecta a uma máquina sem primeiro recuperar as credenciais necessárias da solução; Alteração de senha suspeita, quando é identificada uma solicitação para alterar ou redefinir uma senha ignorando a solução; Credenciais expostas de contas de serviço que se conectam ao LDAP em texto não criptografado;
6.2.3.3.1.3. Delegação não restrita, através da análise das contas de domínio, que recebem privilégios de delegação permissivos e, portanto, expõem o domínio a um alto risco; Contas privilegiadas com configuração SPN (nome principal de serviço) vulneráveis a ataques de força bruta e de dicionário off-line, permitindo que um usuário interno malicioso recupere a senha de texto sem criptografia da conta e Contas de serviço conectadas por meio de logon interativo;
6.2.3.4. Deve permitir a classificação de eventos por níveis de risco e respostas automáticas (suspensão e terminação de sessões) baseadas nos mesmos, com a possibilidade de colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador, permitindo a configuração de eventos críticos a serem reportados automaticamente, baseados em Comandos Linux, Comandos, janelas e aplicações Windows, expressões regulares para comandos em geral e eventos configurados manualmente, permitindo a atribuição de nível de risco customizado.
6.2.4. Segurança contra tomada de controle da rede por meio de credenciais do Active Directory – A solução deve proteger e monitorar Controladores de Domínio Active Directory contra roubo de identidade, acesso não autorizado e ataques visando a tomada de controle da rede via estrutura de diretórios, de acordo com as funções de monitoramento de atividades internas nos mesmos e tráfego de segmentos de rede que estes estejam instalados, para confirmação de integridade das solicitações e tickets Kerberos utilizados nos equipamentos e contas de usuário detectando, no mínimo:
6.2.4.1. Atividades anômalas em tempo real, típicas de ataques ao protocolo de autenticação Kerberos, como roubo de credenciais, movimentação lateral e escalonamento de privilégios; A extração e uso de um Kerberos TGT (ticket de concessão de tickets) da memória LSASS (Subsistema de autoridade de segurança local) em um host para obter acesso a outros recursos da rede (Pass-the-ticket);
6.2.4.2. A recuperação e exploração de hashes de senha armazenados no banco de dados do SAM (Security Accounts Manager) ou do Active Directory para representar um usuário legítimo (Pass-the-Hash); O uso do hash de uma conta de usuário para obter um ticket do Kerberos, que é usado para acessar outras contas e recursos de rede (Overpass-the-Hash);
6.2.4.3. A modificação das configurações de permissão de ticket do Kerberos para obtenção de acesso não autorizado aos recursos da rede - PAC Forjado (Manipulação de Certificado de Atributo de Privilégio); A obtenção de acesso ao KDC (Kerberos Key Distribution Center) para geração de token principal de segurança que fornece acesso completo a um domínio inteiro (Golden Ticket); A recuperação maliciosa de credenciais do controlador de domínio (DCSync);
6.2.5. Arquitetura e Segurança da Solução:
6.2.5.1. Incorporar medidas de segurança como Certificação Common Criteria (CC) – ISO/IEC 15408 – como garantia de segurança do método utilizado no desenvolvimento do sistema de repositório seguro de credenciais e Criptografia dos módulos da solução, a fim de proteger a informação em trânsito entre módulos da solução e aplicações web dos usuários finais e possibilitar a utilização de criptografia do banco de dados utilizado pela solução para armazenar as credenciais gerenciadas pela mesma, sendo compatível com; AES com chaves de 256 bits, FIPS 140-2 e Encriptação PKCS#11 ou superior;
6.2.5.2. Deve utilizar banco de dados em alta disponibilidade, para armazenamento de credenciais, com as melhores práticas de segurança: mecanismo de blindagem do sistema operacional através da desativação ou desinstalação de serviços e portas de acesso não essenciais ao funcionamento da solução. Caso o banco de dados utilizado para armazenamento de credenciais seja de terceiros, a solução deverá ser entregue com licenças de software, garantia e suporte que o compatibilize com a solução.
6.2.5.3. Suportar a implementação em parque computacional Windows Server 2012 R2, Windows Server 2016, Windows Server 2022 e/ou Linux em ambiente físico ou virtualizado com infraestrutura (servidores/software em ambiente virtualizado, S.O., camada de balanceamento/redirecionamento de tráfego, etc.) provida pela CONTRATANTE para implantação e uso da solução em alta disponibilidade.
6.2.5.4. Os elementos críticos da solução, como Repositório Seguro de credenciais, Gateways de Gravação e Monitoração Comportamental deverão ser instalados em alta disponibilidade ativo-ativo em cada uma das localidades (site principal e site redundante adicional), com chaveamento entre localidades (sites), garantindo que o processo seja transparente aos usuários conectados e a normalização das funcionalidades ocorra em até 5 (cinco) minutos, caso exista perda de comunicação e mecanismos para a recuperação de desastres compatível com soluções de backup e arquivamento disponíveis no mercado.

6.2.5.5. Prover, no mínimo, dois ambientes adicionais externos da solução em produção para testes e homologação, replicando as mesmas licenças e funcionalidades do ambiente de produção.

6.3. Solução de Segurança para Privilégios e Acessos – Proteção para Equipamentos Servidores:

6.3.1. Proteção local para Servidores Unix/Linux

6.3.1.1. As funcionalidades devem ser providas por meio de agentes instalados no sistema operacional dos servidores e permitir a proteção e controle dos privilégios em contas de usuário em equipamentos Unix, Linux, Solaris e AIX e associar os privilégios e comandos controlados às contas cadastradas no repositório seguro de credenciais, realizando o controle no próprio sistema operacional;

6.3.1.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem passar pelos monitores/gravadores de acessos) fazendo uso das funcionalidades instaladas no sistema operacional alvo.

6.3.1.3. Disponibilizar, como conjunto mínimo de atividades controladas no ativo de destino, as seguintes operações: criação e exclusão de arquivos e diretórios, mudança de nome de arquivos e diretórios, abertura de arquivos para escrita, comandos chown e chmod e ligações entre arquivos.

6.3.1.4. Implementar restrições, em uma plataforma, de maneira global ou em uma conta de usuário ou grupo de maneira granular.

6.3.1.5. Realizar o controle mediante interceptação do comando antes que ele seja executado, permitir a liberação de comandos privilegiados a usuários comuns, permitir que os comandos executados em sistemas monitorados sejam gravados em modo texto no repositório seguro de credenciais, permitir o agrupamento de comandos, bem como a utilização de coringas como (*), para uma definição ampla de parâmetros;

6.3.1.6. Permitir que sejam atribuídas permissões para usuários e grupos, inclusive do Active Directory e oferecer a capacidade de verificação da identidade da pessoa que executa comandos localmente no dispositivo alvo através de autenticação via usuário da ferramenta, LDAP ou RADIUS;

6.3.1.7. A solução deverá possuir funcionalidade que permita definir variáveis de ambiente no momento da execução de um comando, independentemente da definição realizada pelo usuário ou seu perfil. Sendo exigido no mínimo as seguintes variáveis: PATH, ENV, BASH_ENV, GLOBIGNORE, SHELLOPTS;

6.3.1.8. Possibilitar o uso da máscara de usuário na execução dos comandos (valores entre 0000 e 0777);

6.3.1.9. Impedir a utilização da técnica de ShellEscape, em que um programa autorizado e executado com privilégios permita a execução de outros programas e consequentemente escape dos controles definidos;

6.3.1.10. Disponibilizar a funcionalidade de restrição de Shell, que impossibilite que scripts e shells de sistema executem comandos não permitidos pelas regras definidas na solução;

6.3.1.11. Monitorar e exibir acessos e atividades realizadas no próprio sistema l) Possibilitar mapear e coletar atividades regulares de usuários através do modo observação, agregando e exportando os resultados para um perfil;

6.3.1.12. Prover um controle de comandos completo, com a possibilidade de criar uma lista de comandos permitidos e bloqueados (whitelisting/blacklisting), a serem alterados (criação de alias) ou prevenir que comandos sejam executados ou permitir trabalhar em Shell modificado/controlado;

6.3.1.13. Prover meios de permitir que os usuários executem comandos específicos e conduzam sessões remotamente baseado em regras sem autenticar-se diretamente utilizando credenciais privilegiadas;

6.3.2. Proteção local para Servidores Windows

6.3.2.1. Realizar varredura e inventário de aplicações instaladas no sistema operacional;

6.3.2.2. As funcionalidades devem ser providas por meio de agentes instalados no sistema operacional dos servidores e permitir a proteção e controle dos privilégios;

6.3.2.3. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem ser através dos monitores/gravadores de acessos);

6.3.2.4. Oferecer opções de execução sem aviso: de aplicações com privilégios em modo explícito e transparente, monitorada de aplicações em modo explícito e transparente, com restrições de aplicações em modo explícito e transparente;

6.3.2.5. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa e disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;

6.3.2.6. Suportar, no mínimo, as versões Windows Server 2003 SP2 x32 & x64, Windows Server 2008 x32 & x64, Windows Server 2008 R2 x64, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019 e Windows Server 2022;

6.3.2.7. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;

6.3.2.8. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;

6.3.2.9. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;

6.3.2.10. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;

6.3.2.11. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, deve permitir a criação de políticas reutilizáveis, contendo, no mínimo, os seguintes tipos de aplicações ou tipos de arquivos: executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX, objetos COM;

6.3.2.12. Implementar a verificação de checksum do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;

6.3.2.13. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;

6.3.2.14. Utilizar eventos reportados na interface da ferramenta para criação de novas políticas ou incluí-los em políticas existentes;

6.3.2.15. Permitir agrupar aplicações com base em suas características, para facilitar a inserção de novas aplicações aos grupos ou políticas de segurança de aplicações já criadas;

6.3.2.16. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da interface de gerência;

6.3.2.17. Disponibilizar o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;

6.3.2.18. Monitorar e exibir acessos e atividades realizadas na própria solução;

6.3.2.19. Deve permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;

6.3.2.20. Deve realizar varreduras fazendo uso das funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes nas máquinas e uni-los ao inventário populado mediante detecção durante a execução;

6.3.2.21. Deve verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional alvo ou órgãos de controle de ameaças, como por exemplo o VirusTotal.com ou similares;

6.3.2.22. Deve permitir a execução automática de tipos desconhecidos de arquivo, de acordo com sua origem, mesmo possuindo restrições;

6.3.2.23. Possibilitar o monitoramento e a criação de evidência em vídeo de certas execuções de arquivo e de execuções sob certas condições definidas em política;

6.3.2.24. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional alvo;

6.3.2.25. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;

6.3.2.26. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;

6.3.2.27. Oferecer monitoramento de atividade maliciosa dos processos em execução, visando detectar tentativas de roubo de credenciais;

6.3.2.28. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, a solução deve alertar, reportar e bloquear atividade anômala de arquivos e usuários durante a interação com bases de senhas no formato hash, como por exemplo, SAM local e LSASS;

6.3.2.29. Caso o dispositivo não possa estar conectado de forma permanente aos monitores/gravadores de acessos da solução e repositório seguro de credenciais, deve, de forma autônoma e off-line, gerenciar as senhas das credenciais locais, aplicando políticas de randomização e sincronização das senhas definidas na central da solução;

6.3.2.30. Permitir o envio de arquivos suspeitos, executados sob sua supervisão, para soluções de análise de ameaça do tipo Sandbox;

6.3.2.31. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados;

6.3.2.32. Permitir criar uma whitelist, onde é configurado todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada;

6.3.2.33. Possuir uma integração com Windows UAC, e conter relatórios do uso de prompts aos usuários feitos pelo UAC;

6.3.2.34. Suportar a guarda de políticas de hosts que não façam parte do Active Directory ii) Manter todas as políticas em cache e serem aplicadas ao endpoint, ainda que o mesmo não esteja conectado à rede corporativa;

6.3.2.35. Deve permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada;

6.3.2.36. Deve suportar adição múltiplas mensagens, estas mensagens devem possibilitar edição e suportar múltiplas linguagens;
6.3.2.37. Deve possuir capacidade de relatórios de aplicações e eventos de usuários inclusos na solução;
6.3.2.38. Realizar varredura e inventário de aplicações instaladas no sistema operacional;
6.3.2.39. Deve permitir a configuração de “iscas”, como senhas e credenciais falsas de administrador local para detecção de ataques em andamento e bloqueio proativo;

6.3.3. Solução de Segurança para Privilégios e Acessos – Proteção para Estações de Trabalho:
6.3.3.1. As funcionalidades devem ser instaladas no sistema operacional das estações de trabalho e permitir a proteção dos ativos;
6.3.3.2. As funcionalidades devem ser instaladas no sistema operacional das estações de trabalho e permitir o controle dos privilégios;
6.3.3.3. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem ser através dos monitores/gravadores de acessos);
6.3.3.4. Oferecer opções de execução sem aviso: de aplicações com privilégios em modo explícito e transparente, monitorada de aplicações em modo explícito e transparente, com restrições de aplicações em modo explícito e transparente;
6.3.3.5. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa e disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;
6.3.3.6. Suportar, no mínimo, as versões de estações de trabalho: Windows XP SP3, Windows Vista SP1, Windows 7 x32 & x64, Windows 8/8.1 x32 & x64, Windows 10 x32 & x64, Windows 11 x32 & x64;
6.3.3.7. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;
6.3.3.8. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;
6.3.3.9. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;
6.3.3.10. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;
6.3.3.11. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, deve permitir a criação de políticas reutilizáveis, contendo, no mínimo, os seguintes tipos de aplicações ou tipos de arquivos: executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX, objetos COM;
6.3.3.12. Implementar a verificação de checksum do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;
6.3.3.13. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;
6.3.3.14. Utilizar eventos reportados na interface da ferramenta para criação de novas políticas ou incluí-los em políticas existentes;
6.3.3.15. Permitir agrupar aplicações com base em suas características, para facilitar a inserção de novas aplicações aos grupos ou políticas de segurança de aplicações já criadas;
6.3.3.16. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da interface de gerência;
6.3.3.17. Disponibilizar o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;
6.3.3.18. Monitorar e exibir acessos e atividades realizadas na própria solução;
6.3.3.19. Deve permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;
6.3.3.20. Deve realizar varreduras fazendo uso das funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes nas máquinas e uni-los ao inventário populado mediante detecção durante a execução;
6.3.3.21. Deve verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional alvo ou órgãos de controle de ameaças, como por exemplo o VirusTotal.com ou similares;
6.3.3.22. Deve permitir a execução automática de tipos desconhecidos de arquivo, de acordo com sua origem, mesmo possuindo restrições;
6.3.3.23. Possibilitar o monitoramento e a criação de evidência em vídeo de certas execuções de arquivo e de execuções sob certas condições definidas em política;
6.3.3.24. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional alvo;
6.3.3.25. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;
6.3.3.26. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;
6.3.3.27. Oferecer monitoramento de atividade maliciosa dos processos em execução, visando detectar tentativas de roubo de credenciais;
6.3.3.28. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, a solução deve alertar, reportar e bloquear atividade anômala de arquivos e usuários durante a interação com bases de senhas no formato hash, como por exemplo, SAM local e LSASS.
6.3.3.29. Caso o dispositivo não possa estar conectado de forma permanente aos monitores/gravadores de acessos da solução e repositório seguro de credenciais, deve, de forma autônoma e off-line, gerenciar as senhas das credenciais locais, aplicando políticas de randomização e sincronização das senhas definidas na central da solução;
6.3.3.30. Permitir o envio de arquivos suspeitos, executados sob sua supervisão, para soluções de análise de ameaça do tipo Sandbox;
6.3.3.31. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados;
6.3.3.32. Permitir criar uma whitelist, onde é configurado todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada;
6.3.3.33. Possuir uma integração com Windows UAC, e conter relatórios do uso de prompts aos usuários feitos pelo UAC;
6.3.3.34. Suportar a guarda de políticas de hosts que não façam parte do Active Directory;
6.3.3.35. Manter todas as políticas em cache e serem aplicadas ao endpoint, ainda que o mesmo não esteja conectado à rede corporativa;
6.3.3.36. Deve permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada;
6.3.3.37. Deve suportar adição múltiplas mensagens, estas mensagens devem possibilitar edição e suportar múltiplas linguagens;
6.3.3.38. Deve possuir capacidade de relatórios de aplicações e eventos de usuários inclusos na solução;
6.3.3.39. Realizar varredura e inventário de aplicações instaladas no sistema operacional;
6.3.3.40. Deve permitir a configuração de “iscas”, como senhas e credenciais falsas de administrador local para detecção de ataques em andamento e bloqueio proativo;
6.3.3.41. A solução deverá ser capaz de atender minimamente os seguintes casos de uso para requisitar um e mais fatores de autenticação:
6.3.3.41.1. Nas telas de login e desbloqueio de sistemas operacionais Windows e MacOs;
6.3.3.41.2. Multi Fator de autenticação para soluções de VPN via RADIUS ou SAML;
6.3.3.41.3. Qualquer dispositivo ou sistema operacional que suporte RADIUS;
6.3.3.41.4. Plugin para ADFS (IDP, Identity Provider), Active Directory Federation Services;
6.3.3.41.5. Sob demanda utilizando o protocolo Oauth e REST APIs;
6.3.3.41.6. Para realizar o autosserviço de reset de senha ou desbloqueio de usuário;
6.3.3.42. A solução deverá ser capaz de oferecer minimamente os seguintes métodos para múltiplo fator de autenticação:
6.3.3.43. Usuário e senha dos diretórios suportados na solução:
6.3.3.43.1. Através de aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para;
6.3.3.43.2. Biometria do tipo FaceID;
6.3.3.43.3. Biometria através do leitor de digital;
6.3.3.43.4. Smartphone push (Notificação para aprovar ou recusar uma autenticação);
6.3.3.43.5. Geolocalização através de coodernadas GPS e banco de dados de IPs;
6.3.3.43.6. Suporte a tokens OATH OTP;
6.3.3.43.7. Autenticação na tela de login via QRcode sem a necessidade de digitar usuário e senha, com opção de forçar a biometria no dispositivo móvel;
6.3.3.43.8. Confirmação de código via e-mail;
6.3.3.44. Clientes do tipo OATH OTP (exemplo, Google Authenticator);
6.3.3.45. Autenticadores que suportem FIDO2 / U2F, minimamente suportando:
6.3.3.45.1. Windows Hello;
6.3.3.45.2. Yubikey;

6.3.3.45.3. Google Titan Key;
6.3.3.45.4. MacOS TouchID;
6.3.3.46. Perguntas e respostas previamente configuradas;
6.3.3.47. Permitir que os usuários realizem o autosserviço de reset de senha e desbloqueio de usuário utilizando os métodos de múltiplo fator de autenticação citados para verificação positiva através do portal da solução, tela de login de sistemas operacionais Windows e através de REST APIs oferecidas pela solução;
6.3.3.48. Para cada caso de uso ou conjunto de casos de uso de múltiplo fator de autenticação citados, a solução de ser capaz de identificar os atributos de contexto de cada autenticação para disponibilizar os melhores métodos definidos para a autenticação, suportando minimamente:
6.3.3.48.1. Endereçamento IP;
6.3.3.48.2. Dia da Semana;
6.3.3.48.3. Datas específicas;
6.3.3.48.4. Janelas de tempo entre duas datas;
6.3.3.48.5. Janelas de tempo entre horários (exemplo, horário comercial);
6.3.3.48.6. Tipo do Sistema Operacional;
6.3.3.48.7. Tipo do Browser;
6.3.3.48.8. Perfis configurados na solução;
6.3.3.48.9. País que está sendo realizado o acesso;
6.3.3.48.10. Se é um dispositivo gerenciado;
6.3.3.48.11. Autenticação via certificado;
6.3.3.48.12. Nível de Risco da autenticação medido por um motor de análise de comportamento dos usuários;
6.3.3.49. A solução deve ter capacidade de detectar casos de uso e perfis de autenticação já validados pelo usuários e não requisitar mais os mesmos durante um período de tempo configurado pelo administrador da solução, evitando desta forma repetidas validações em um curto espaço de tempo;
6.3.3.50. O conjunto de fatores de autenticação disponibilizados devem ser baseados durante o acesso através de regras especificadas no item anterior e segregados por:
6.3.3.50.1. Conjunto de aplicações;
6.3.3.50.2. Uma única aplicação;
6.3.3.50.3. Regras para o autosserviço de reset de senha e desbloqueio de usuário;
6.3.3.50.4. Portal do Administrador;
6.3.3.50.5. Portal do Usuário;
6.3.3.51. A solução deve prover um aplicativo móvel para Android e IOS com as seguintes características:
6.3.3.51.1. Depois de efetuado o login apresentar as aplicações WEB disponíveis para realizar o SSO, através de um conjunto de ícones onde cada um representa uma aplicação que o usuário tem o direito de efetuar o SSO já integrado com os navegadores instalados nos dispositivos móvel;
6.3.3.51.2. Prover login através do scan de QRcode no portal web permitindo SSO sem identificação de usuário e senha;
6.3.3.51.3. Configurar OATH OTP adicionais provenientes de outras soluções;
6.3.3.51.4. Configurar OATH OTP para autenticação multi fator nos sistemas operacionais Windows (telas de login e bloqueio) quando os mesmos estão desconectados da internet;
6.3.3.51.5. Verificar dispositivos registrados (dispositivos móveis e sistemas operacionais);
6.3.3.51.6. Integração nativa com FaceID, TouchID, leitor biométrico dos dispositivos móveis alavancando os mesmos para autenticação biométrica durante login nas aplicações;
6.3.3.51.7. Reportar coordenadas GPS para os sistemas que utilizam geolocalização;
6.3.3.52. O aplicativo deve suportar autenticação do tipo push, onde o usuário tem a escolha de aceitar ou recusar o desafio, esta notificação de conter minimamente: IP de origem de acesso, Data e Hora, Cidade / Geolocalização do acesso, Aplicação sendo acessada;
6.3.3.53. A solução dever ser baseada em algoritmos de aprendizado de máquina (Machine Learning) não supervisionados, ou seja, os modelos estatísticos com os casos de uso já prontos e calibrados;
6.3.3.54. A solução deve medir o risco da autenticação verificando o comportamento histórico da identidade através do conjunto dos seguintes atributos;
6.3.3.55. Geo Velocidade, medindo velocidade de deslocamento do login, comparando a localização do último login com a atual, evitando “viagens impossíveis”, e traçando o comportamento do usuário neste quesito, por exemplo, pessoas que viajam muito podem ter uma pontuação de risco baixa mesmo que sua Geo Velocidade seja maior que pessoas que não viajam;
6.3.3.56. Geo Localização: medindo o risco da autenticação verificando sua localização geográfica do acesso atual em comparação com o seu comportamento usual;
6.3.3.57. Dia da Semana: medindo o risco da autenticação verificando o dia da semana do acesso atual em comparação com seu comportamento usual;
6.3.3.58. Horário do Acesso: mede o risco da autenticação verificando o horário do acesso atual em comparação com seu comportamento usual;
6.3.3.59. Sistema Operacional: mede o risco da autenticação verificando o Sistema Operacional do acesso atual em comparação com seu comportamento usual;
6.3.3.60. Falhas de login consecutivas, mede o risco da autenticação verificando as falhas de login consecutivas do acesso atual em comparação com seu comportamento usual iii) Deve prover a personalização das faixas de pontuação (0 a 100) para os administradores da solução para, no mínimo, as categorias: Sem risco, Risco Baixo, Risco Médio e Risco Alto;
6.3.3.61. Deve prover para os administradores da solução a personalização da influência na medição do risco para cada atributo citado neste item. Por exemplo, para a CONTRATANTE a geo velocidade pode ser um fator que não possui relevância, desta forma deve ser possível configurar a influência deste risco como baixa na modelagem de risco da plataforma;
6.3.3.62. O risco calculado durante a autenticação pelo motor de análise do comportamento dos usuários deve ser compartilhado com funções de Múltiplo Fator de autenticação e Single Sign-On que realizam o login para os casos de uso citados neste documento e utilizar como contexto para:
6.3.3.62.1. Requisitar múltiplos fatores de autenticação de forma dinâmica;
6.3.3.62.2. Permitir o login sem o uso de múltiplos fatores;
6.3.3.62.3. Negar a autenticação;
6.3.3.63. Deve prover para os administradores da solução a capacidade de explorar os dados históricos através de dashboards, filtros e gráficos configuráveis sendo possível verificar os alertas e os fatores que os influenciaram, além da exploração dos eventos capturados e seus atributos;
6.3.3.64. Deve prover gráficos de linha do tempo, donuts, mapas com geolocalização dos eventos, gráfico de barras, tabelas analíticas, e mapas de relacionamento, sendo suas dimensões e categorias personalizáveis;
6.3.3.65. Deve ser capaz de exportar os dados dos alertas, riscos calculados, eventos para, no mínimo, CSV, adicionalmente gravar as visualizações na solução para consultas posteriores;
6.3.3.66. Deve possuir integração com fontes de inteligência cibernética de terceiros reconhecidas no mercado, como, por exemplo, Palo Alto Cloud;
6.3.3.67. Deve possuir interface para envio de alertas de forma automatizada, suportando, no mínimo E-mail com conteúdo do alerta e Webhooks (ex: envio de mensagem para um canal do Microsoft Teams ou Slack;
6.3.3.68. Possuir dashboards pré-configurados com informações e gráficos com as seguintes características:
6.3.3.68.1. Utilização do Motor de Análise do Comportamento dos Usuários;
6.3.3.68.2. Comportamento dos usuários na utilização das aplicações;
6.3.3.68.3. Visão sobre a segurança das aplicações;
6.3.3.68.4. Mapa com a geolocalização das autenticações;
6.3.3.68.5. Visão sobre o comportamento dos Endpoints (Mobile e Computadores);
6.3.3.68.6. Visão sobre o comportamento das Identidades;

6.3.4. Serviço especializado para implementação, configuração e transferência de conhecimento da solução de Segurança para Sistemas Críticos:
6.3.4.1. O serviço de implementação e configuração deve ser executado em até 30 dias após a instalação da solução no ambiente do TJAM;
6.3.4.2. O serviço de transferência de conhecimento abrange, entre outras, as seguintes atividades:
6.3.4.2.1. Elaboração de documentação técnica e de usuário;
6.3.4.2.2. Transferência de conhecimentos relacionados ao desenvolvimento, implantação e manutenção no ambiente do TJAM;
6.3.4.2.3. Levantamento de informações junto aos usuários, objetivando a definição e elaboração de regras e políticas;
6.3.4.2.4. Corrigir ou apoiar em problemas e defeitos em funcionalidades já existentes;

6.3.4.2.5. Realização de operação assistida e monitoramento de ambientes entregues com a solução;
6.3.4.2.6. Orientar na utilização dos softwares instalados no TJAM com a utilização das melhores práticas e orientações dos fabricantes;
6.3.4.2.7. Apoiar na atualização, instalação e/ou reinstalação de novas versões e dos produtos instalados no TJAM minimizando impactos;
6.3.4.2.8. Apoiar na configuração/parametrização do sistema em novas máquinas;
6.3.4.2.9. Orientar no levantamento de informações que possibilite a identificação de novas necessidades, detectadas no ambiente do TJAM;
6.3.4.2.10. Diagnosticar o bom funcionamento das ferramentas instaladas, garantindo a máxima utilização dos recursos oferecidos;
6.3.4.2.11. Identificar e elaborar proposição de melhoria em performance, desempenho, tunning, disponibilidade e confiabilidade em ambientes;
6.3.4.2.12. Otimizar a reinstalação e/ou adaptação das ferramentas em outros equipamentos que não seja onde originalmente os sistema e produtos foram instalados;
6.3.4.2.13. Definir metodologia, elaborar relatórios e projetos e acompanhar a configuração e utilização de solução de alta disponibilidade, repassando aos técnicos da TI do TJAM as melhores práticas para uso da solução, quanto a parametrização e configuração dos componentes e ferramentas utilizadas no TJAM;
6.3.4.2.14. Esclarecer dúvidas e orientar os técnicos de TI do TJAM, sobre integração das soluções, abrangendo as diversas plataformas existentes no ambiente computacional do TJAM;
6.3.4.2.15. Apoiar no planejamento, na execução e na avaliação das mudanças no ambiente;
6.3.4.2.16. Analisar patches, correções e novas versões e sugerir a aplicação ou não dos mesmos no ambiente;
6.3.4.2.17. Apoiar no planejamento, na execução e na avaliação das atualizações de versões e aplicação de patches da ferramenta;
6.3.4.2.18. Apoiar no planejamento, na execução e na avaliação de implantação de novas aplicações ou atualização de aplicações no ambiente;
6.3.4.2.19. Efetuar a transferência de tecnologia para a equipe do TJAM;

6.3.5. Solução de segurança para identidades e acessos – Proteção para Aplicações Tradicionais

6.3.5.1 Uma aplicação gerenciada é definida como a aplicação que faz uso direto dos recursos e credenciais gerenciadas pela solução para concessão de acesso ao seu ambiente (substituindo o uso de credenciais hard coded, por exemplo).

6.3.5.2 Deve permitir a integração de servidores de aplicação e o repositório digital seguro, eliminando a necessidade de senhas e chaves SSH embutidas em aplicações, scripts e arquivos de configuração.

6.3.5.3 Deve possuir mecanismo de segurança que evite a parada de aplicações críticas, mantendo a entrega das credenciais em caso de queda da rede ou parada total da solução que gerencia as credenciais por meio do repositório seguro.

6.3.5.4 Deve fornecer credenciais, pelo menos, via consulta de rede ou Web service.

6.3.5.5 Deve garantir a entrega de credenciais localmente nos servidores de aplicação, garantindo baixa latência para aplicações de missão crítica.

6.3.5.6 Deve manter um cache local atualizado das credenciais utilizadas no servidor de aplicação, a fim de prevenir falhas na comunicação com o repositório seguro e trazer velocidade às consultas

6.3.5.7 Deve suportar redundância de credenciais, oferecendo, de maneira transparente, mais de um usuário e senha à aplicação crítica, de forma que se evite qualquer possível indisponibilidade mínima durante o processo de troca de senhas;

6.3.5.8 Deverá oferecer SDKs documentados para integração com aplicações em Java, C/C++ e .Net

6.3.5.9 Deverá suportar a utilização de executável para scripts e aplicações nativas em plataforma Windows

6.3.5.10 Deverá suportar a utilização integração com servidores WebSphere, WebLogic, JBoss e Tomcat, para fornecimento de credenciais via XML datasources

6.3.5.11 Deverá suportar a autenticação de aplicações que consultam credenciais, permitindo definir o caminho da aplicação, usuário do sistema operacional, endereço do servidor e hash do código.

6.3.5.12 Ser disponibilizada com um SDK (Software Development Kit) que pode ser configurado para permitir que aplicações possam Solicitar as credenciais sob demanda, ao invés de utilizar credenciais estáticas;

6.3.5.13 Atualizar informações de contas automaticamente no banco de dados de senhas;

6.3.5.14 Inscrever automaticamente dispositivos alvo, sem aguardar por atualizações dinâmicas;

6.3.5.15 Alterar senhas em texto claro (incorporado em aplicações), de forma segura no banco de dados de senhas;

6.3.5.16 Visando a garantia do funcionamento da solução como um todo, este item deve ser entregue com total integração com o item 1 desta especificação.

6.4. Catálogo e/ou Amostras

6.4.1 Deverá ser apresentado catálogo, folder, manual ou sítio da internet que comprove que todos os materiais e equipamentos a serem utilizados atendem rigorosamente as especificações técnicas mínimas exigidas.

6.4.2 Não há necessidade de apresentar amostra de nenhum item.

6.4.3 A Divisão de Tecnologia da Informação e Comunicação do TJAM, sito a Avenida André Araújo s/n, Prédio Desembargador Arnoldo Péres - Bairro Aleixo – CEP 69.060-000 será a responsável por receber e validar os objetos desta contratação.

6.5 Vistoria Técnica.

6.5.1 As interessadas poderão realizar, sob o acompanhamento de servidor especialmente designado, vistoria aos locais de execução dos serviços, no todo ou em parte, em data e horário previamente acordados segundo a conveniência deste Órgão, com o objetivo de conhecer as instalações onde serão executados os serviços e sanar as dúvidas porventura existentes, a fim de subsidiar a elaboração das propostas a serem submetidas ao certame;

6.5.2 As visitas deverão ser previamente agendadas, com 72 (setenta e duas) horas de antecedência, pelo telefone (92) 2129-6779 – DIVISÃO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, no período das 8 às 14hs, ou via e-mail através de: infra.tic@tjam.jus.br.

6.6 Planejamento e execução dos serviços

6.6.1 A Contratada deverá instalar e configurar os serviços nas dependências do TJAM e/ou remotamente de modo a viabilizar a execução do objeto.
6.6.2 Se houver necessidade ou risco de interrupção do serviço, a implantação deverá ser realizada em horário específico a ser indicado pela Divisão de Infraestrutura de TIC, podendo ser realizada em finais de semana ou feriados, sem qualquer custo adicional para o TJAM.

6.6.3 Os trabalhos serão coordenados e acompanhados por técnicos do TJAM e deve haver repasse de conhecimento durante a execução dos serviços.
6.6.4 Para efeitos de aceite definitivo, a conclusão dos serviços de instalação e configuração será dada pela entrega da solução adquirida em pleno funcionamento, de acordo com as especificações.
6.6.5 No caso de serviços sob demanda, o prazo de entrega será aquele definido nas Ordens de Serviço.

6.7 Local e Prazos de Execução

6.7.1 Em até 10 (dez) dias corridos, contados da assinatura do contrato, recebimento da Nota de Empenho e da Ordem de Serviço.

6.7.2 A CONTRATADA deverá entregar um projeto executivo para a implantação dos serviços contendo no mínimo:

6.7.2.1 Responsável pela implantação.

6.7.2.2 Cronograma de implantação.

6.7.2.3 3. Cronograma de reuniões de acompanhamento.

6.7.3 A CONTRATADA deverá concluir os serviços de instalação e ativação de todo o objeto nos seguintes prazos:

6.7.3.1. Em até 30 (trinta) dias corridos, contados da entrega do projeto executivo pela CONTRATADA.

6.7.3.3. Durante a implantação, independente da periodicidade das reuniões de acompanhamento, a CONTRATADA deverá apresentar semanalmente relatórios do andamento das ações previstas no cronograma.

6.7.4. Os desalinhamentos no cronograma que possam comprometer as datas previstas para as entregas devem ser informados a CONTRATANTE a fim de buscar alternativas de remediação dos problemas.

6.7.5. Considera-se o serviço ativado quando, após comunicação oficial da CONTRATADA informando a efetiva instalação, configuração e disponibilização do serviço, for realizado teste de conectividade pelos técnicos da CONTRATANTE, identificado o atendimento de todos os requisitos técnicos para os links, inclusive de monitoração.

6.7.6. O não cumprimento dos prazos e das condições de entrega dos serviços sujeitará a CONTRATADA às sanções administrativas previstas no Termo de Referência.

6.8 Forma de Execução dos serviços

6.8.1 A execução dos serviços será sob demanda, no regime de empreitada por preço unitário.

6.8.2 Todos os itens serão atendidos por fornecedor único, uma vez que os serviços pretendidos estão intrinsecamente relacionados. A adjudicação dos itens para empresas diferentes poderia resultar na aquisição de soluções incompatíveis, o que acarretaria prejuízo à CONTRATANTE.

6.9 Previsão dos Recursos

6.9.1 Para a execução dos serviços de instalação e configuração, a licitante Contratada deverá alocar profissionais devidamente habilitados pelo fabricante.

6.9.2 A licitante deverá apresentar, no mínimo, um profissional certificado, dentro da equipe que irá executar os serviços.

6.10 Garantia ou Assistência Técnica

6.10.1 Cada produto deverá ser entregue ao TJAM na sua versão e release mais recente e durante a vigência do contrato deverá ser atualizado sem custo adicional.

6.10.2 A contratada deve possuir contrato de representante do fornecedor da solução.

6.10.3 Para a solução envolvida na contratação, a Contratada deverá prever garantia dos produtos, durante a vigência do contrato, a partir da data de sua ativação, fornecendo sem custo adicional todos os ajustes às falhas que porventura forem encontradas. Garantia integral durante 12 (doze) meses, “on-site” com atendimento vinte e quatro horas por dia e sete dias por semana, a contar da data de homologação do produto, contra qualquer defeito ou problema em toda a solução.
6.10.4. A Contratada, durante o período de garantia, se obriga ao fornecimento dos componentes de software, para manutenções, update de produtos, suporte técnico ou ampliações, de forma que possam ser mantidas todas as funcionalidades inicialmente contratadas. Caso haja neste período a descontinuidade de fabricação dos componentes, deve ser também garantida à total compatibilidade dos itens substitutos com os originalmente fornecidos.

6.11. Solicitação de Serviços

6.11.1 A CONTRATADA deverá disponibilizar canais de comunicação, tais como número de telefone, endereço de correio eletrônico ou plataforma de abertura de chamados para atendimento de suporte técnico e consultoria.

6.11.2 A CONTRATADA deverá indicar um funcionário para que seja ponto de contato (preposto) entre o TJAM e a CONTRATADA.

6.11.3 Despesas relativas ao preposto serão de exclusiva responsabilidade da CONTRATADA.

6.12 Instrumento de Medição de Resultado (IMR) ou de Acordo de Nível de Serviço (ANS)

6.12.1 Os serviços deverão ser prestados tendo sua qualidade medida por meio de Acordo de Nível de Serviço – ANS

6.12.2 Havendo qualquer interrupção no funcionamento da solução o TJAM efetuará abertura de chamado reportando todos os sintomas.

6.12.3 Os níveis de serviço serão classificados conforme as severidades Emergencial, Grave e Normal.

6.12.4 Todos os prazos especificados na tabela "Acordo de Nível de Serviço / Penalidades" são contados a partir da abertura do respectivo número de identificação do chamado.

6.12.5 A abertura do chamado com fornecimento do seu número de identificação (protocolo de atendimento) deve ocorrer no prazo máximo de 15 minutos a partir da tentativa de contato pela Contratante com o número fornecido pela Contratada.

6.12.6 O atendimento aos chamados pode ocorrer remotamente ou de forma presencial. Atendimentos remotos não resolvidos que ultrapassem 24 horas devem ser continuados de forma presencial.

6.12.7 Após a conclusão do suporte, a Contratada comunicará ao TJAM e solicitará autorização para o fechamento do chamado. Caso o TJAM não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela Contratada. Neste caso, o TJAM informará as pendências relativas ao chamado aberto.

6.12.8 Sempre que houver quebra dos ANS, o TJAM emitirá notificação à Contratada, que terá o prazo de, no máximo, 5 (cinco) dias úteis, contados a partir do recebimento da notificação, para apresentar as justificativas para as falhas verificadas.

6.12.9 Caso não haja manifestação dentro desse prazo ou caso o TJAM entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação das penalidades previstas, conforme o nível de atendimento transgredido.

6.12.10 Caso não sejam observados os prazos para atendimento previstos, incidirão glosas, calculadas sobre o valor do contrato, e penalidades conforme o disposto na tabela a seguir:

			Acordo de Nível de Serviço / Penalidades
Severidade	Prazos	Descrição Severidade	
1 - Emergencial	6 Horas	Até 2 horas corridas de atraso.	1 – Advertência; 2 – Havendo recorrência, multa de 0,8%(zero ví
		Superior a 2 horas e inferior ou igual a 8 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços	3 – Multa de 1,0% (um por cento) por hora de a
		Superior a 8 horas corridas.	4 – Multa de 1,2% (um vírgula dois por cento) p administrativas a critério da Contratante.
2 - Grave	12 Horas	Até 4 horas corridas de atraso.	5 – Advertência; 6 – Para as demais ocorrências, multa de 0,6% (
		Superior a 4 horas e inferior ou igual a 24 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	– Multa de 0,8% (zero vírgula oito por cento) po
		Superior a 24 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	8 – Multa de 1.0% (um por cento) por hora de a critério da Contratante.
3 - Normal	24 Horas	Até 48 horas corridas de atraso.	9 – Advertência; 10 – Para as demais ocorrências, multa de 0,5% 11. – Se o somatório das multas aplicadas com r rescisão do Contrato, independentemente de apl

6.13 Dos prazos para recebimento provisório e definitivo

6.13.1 O recebimento será feito em duas etapas:

6.13.1.1 Recebimento provisório: No prazo máximo de 30 dias úteis após a entrega e configuração inicial dos produtos para posterior averiguação.

6.13.1.2 Recebimento definitivo: No prazo máximo de 30 dias úteis a contar da data de emissão do termo de recebimento provisóio.

6.13.2 O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança na execução do objeto, nem ético-profissional pela perfeita execução do objeto, dentro dos limites estabelecidos pela lei ou pelo Contrato.

7. DA NECESSIDADE DE FORMALIZAÇÃO DE CONTRATO

7.1. Deverá ser formalizado contrato para os serviços previstos neste Estudo Técnico Preliminar (ETP), tendo em vista as características do objeto a ser contratado, com a existência de obrigações futuras, incluindo a garantia, continuidade e confiabilidade do mesmo.

8. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

8.1. Tendo por objetivo promover a proteção das credenciais administrativas utilizadas no âmbito dos sistemas computacionais do TJAM, além de criar mecanismos que impeçam a utilização dessas credenciais com o objetivo de potenciais ataques cibernéticos, prevenindo danos e principalmente evitando solução de continuidade na prestação jurisdicional, estima-se adquirir:

ITEM	ESPECIFICAÇÕES	QUANTIDADE MÍNIMA POR CONTRATAÇÃO	QUANTIDADE TOTAL
1	Solução de Segurança para Identidades e seus Privilégios – Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI, com garantia pelo período de 12 (doze) meses.	50	75
2	Solução de Segurança para Identidades e seus Privilégios – Proteção para Aplicações Tradicionais, com garantia pelo período de 12 (doze) meses.	20	40
3	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para ervidores Windows e Linux, com garantia pelo período de 12 (doze) meses.	200	400
4	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para Estações de Trabalho, com garantia pelo período de 12 (doze) meses.	2500	3500
5	Serviço de instalação e configuração para Solução de Segurança para Identidades e seus Privilégios.	1	1
6	Transferência de Conhecimento para Solução de Segurança para Identidades e seus Privilégios (turma)	1	2
7	Serviço de Suporte Técnico Especializado	12	12

9. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

9.1 Os valores estimados para esta contratação seguem na planilha abaixo.

Item	Descrição	Unid	Qnt Total	Preço (R$)	
				Unit	Total
1	Solução de Segurança para Identidades e seus Privilégios – Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI, com garantia pelo período de 12 (doze) meses..	Unidades	75	R$ 4.800,00	R$ 360.000,00
2	Solução de Segurança para Identidades e seus Privilégios – Proteção para Aplicações Tradicionais, com garantia pelo período de 12 (doze) meses.	Unidades	40	R$ 4.050,00	R$ 162.000,00
3	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para ervidores Windows e Linux, com garantia pelo período de 12 (doze) meses.	Unidades	400	R$ 632,00	R$ 252.800,00
4	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para Estações de Trabalho, com garantia pelo período de 12 (doze) meses.	Unidades	3500	R$ 236,00	R$ 826.000,00
5	Serviço de instalação e configuração para Solução de Segurança para Identidades e seus Privilégios.	Unidades	1	R$ 355.000,00	R$ 355.000,00
6	Transferência de Conhecimento para Solução de Segurança para Identidades e seus Privilégios (turma)	Unidades	2	R$ 31.000,00	R$ 62.000,00
7	Serviço de Suporte Técnico Especializado	Unidades	12	R$ 23.500,00	R$ 282.000,00
	Valor Estimado Total				R$ 2.299.800,00

10. JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

10.1 O objeto da contratação possui características comuns e usuais, fornecido por várias empresas, porém deverá ser realizada por único fornecedor. O parcelamento do objeto, neste caso, é inviável já que não se justifica técnica e economicamente, além do que a solução de TI contratada é composta de serviços integrados e correlatos que visam manter em funcionamento toda infraestrutura de solução.

11. CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

11.1 Não há contratações correlatas.

12. RESULTADOS PRETENDIDOS

12.1 Economicidade, eficácia, eficiência: com esta pretensa contratação, busca-se preservar os investimentos realizados no ambiente do TJAM, mantendo-se a eficácia, integração e a qualidade da plataforma de segurança em um ambiente de TI complexo como o do TJAM, bem como reduzir possíveis impactos gerados pela indisponibilidade dos serviços e sistemas de TIC e também evitar a reimplementação das barreiras de seguranças já em operação do TJAM;

12.2. Melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis: com a efetivação da contratação, o CONTRATANTE poderá direcionar seus esforços na capacitação da equipe técnica da SETIC para matérias mais relevantes, estratégicas e alinhadas com o negócio do TJAM, já que durante o período de vigência dos equipamentos o corpo técnico da SETIC adquiriu amplo conhecimento e experiência na solução de segurança atual;

12.3. Impactos ambientais positivos: não se aplica;

12.4. Melhoria da qualidade de produtos ou serviços oferecidos à sociedade: com a efetivação da contratação, a tendência esperada é a de menos ataques cibernéticos, reduzindo-se assim as indisponibilidades nos serviços oferecidos à sociedade.

13. PROVIDÊNCIAS PARA ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO

13.1 Não haverá necessidade de adequação de ambiente.

14. IMPACTOS AMBIENTAIS

14.1 Pelo fato da solução a ser adquirida ser totalmente baseada em software, não haverá impactos ambientais relevantes a serem considerados em sua implantação.

15. SERVIÇOS DE MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

15.1 Esta pretensa contratação, por tratar-se de um softtware, não prevê manutenção física e/ou assistênica técnica, somente garantia, conforme item 6.10, assim como também a contratação do serviço de suporte técnico especializado, destacada pelo item 7 do tópico 6.1.

16. DECLARAÇÃO DE VIABILIDADE (OU NÃO) DA CONTRATAÇÃO

16.1 Considerando todo o exposto acima, esta Secretaria de Tecnologia da Informação e Comunicação declara que a aquisição da Solução de Segurança para Gestão de Credenciais e Acessos da Cyberark é fundamental e viável, dada a necessidade de tornar o Judiciário do Estado do Amazonas mais seguro e inclusivo no ambiente digital, aumentar a resiliência às inevitáveis ameaças cibernéticas, estabelecer governança de segurança cibernética e fortalecer a gestão integrada de ações de segurança cibernética. Cumprindo lembrar que o TJAM ainda não possui qualquer solução de gerenciamento de acessos privilegiados.

17. OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS

17.1 A contratada deverá garantir as melhores práticas relacionadas à Segurança da Informação e à Lei Geral de Proteção de Dados Pessoais (LGPD), principalmente, no que diz respeito aos dados pessoais tratados durante a configuração dos privilégios.

17.2 A contratada durante a execução do objeto, deve implementar medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados.

17.3 Será exigido da Contratada que cada profissional que venha a prestar serviços assine um termo de compromisso, pelo qual se comprometerá a manter o sigilo das informações.

17.4 A Contratada deverá manter sigilo absoluto a respeito de quaisquer dados, informações e artefatos, contidos em documentos e mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos, independentemente da classificação de sigilo conferido pelo TJAM a tais documentos.

Manaus, data registrada no sistema.

Washington Alves da Cunha Neto	**Diogo Mendonça de Sousa**	**Breno Figueiredo Corado**
Assessor de Segurança da Informação e Proteção de Dados	Diretor da Divisão de Infraestrutura de Tecnologia da Informação e Comunicação	Secretário de Tecnologia da Informação e Comunicação
Assinado Digitalmente	Assinado Digitalmente	Assinado Digitalmente

Documento assinado eletronicamente por **WASHINGTON NETO**, **Coordenador(a)**, em 04/04/2024, às 18:28, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **DIOGO MENDONCA DE SOUSA**, **Diretor(a)**, em 04/04/2024, às 18:30, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BRENO FIGUEIREDO CORADO**, **Secretário(a)**, em 05/04/2024, às 05:43, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1502255** e o código CRC **CB53A34F**.