PODER JUDICIÁRIO
DO ESTADO DO ACRE

ESTUDO TÉCNICO PRELIMINAR (TIC) Nº 12/2025

Processo Administrativo nº 2025-206

Contratação de empresa especializada para fornecer ao Poder Judiciário do Estado do Acre (PJAC) solução de gestão e controle de contas de usuários privilegiados (PAM).

Rio Branco, junho de 2025.

PODER JUDICIÁRIO
DO ESTADO DO ACRE

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

1. OBJETO

Contratação de empresa especializada para fornecer ao Poder Judiciário do Estado do Acre (PJAC) solução de gestão e controle de contas de usuários privilegiados (PAM - Privileged Access Management).

2. NECESSIDADE DA CONTRATAÇÃO

A segurança da informação é um pilar essencial para garantir a integridade, confidencialidade e disponibilidade dos sistemas e dados no Poder Judiciário do Acre (PJAC). Diante do crescimento das ameaças cibernéticas e da necessidade de conformidade com normativas específicas, torna-se necessária a implementação de uma solução de Privileged Access Management (PAM) para o controle e gerenciamento de acessos privilegiados. Essa necessidade está alinhada à Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), instituída pela Resolução CNJ nº 396/2021, e à Estratégia de Segurança da Informação do PJAC, conforme a Resolução do Tribunal Pleno Administrativo (TPADM) /PJAC nº 291/2023. Ambas as normativas estabelecem diretrizes para aprimorar a governança e a proteção dos ativos digitais do Judiciário.

Atualmente, o PJAC enfrenta desafios críticos relacionados à gestão de acessos privilegiados, o risco de acessos indevidos é uma preocupação constante, pois contas administrativas sem controle adequado podem ser exploradas em ataques internos ou externos. Por tanto, a ausência de rastreabilidade eficiente dificulta o monitoramento e a auditoria das ações executadas por usuários privilegiados, o que compromete a governança de segurança cibernética. O armazenamento e compartilhamento de senhas administrativas ocorrem de forma descentralizada, aumentando os riscos de vazamento de dados.

Há a necessidade de implementação de medidas para garantir a integridade, autenticidade e rastreabilidade dos acessos, o que reforça a necessidade de uma solução especializada para o gerenciamento de acessos privilegiados. Além disso, é essencial atender requisitos de segurança previstos na Lei Geral de Proteção de Dados (LGPD), na ISO 27001 e nas diretrizes do Conselho Nacional de Justiça (CNJ), os quais determinam controles mais rigorosos sobre acessos privilegiados, mitigação de riscos cibernéticos e a continuidade dos serviços críticos.

A aquisição de uma solução PAM tem como objetivo gerenciar credenciais privilegiadas de forma segura, armazenando-as em um cofre digital protegido e minimizando riscos de comprometimento. A ferramenta permitirá monitorar e registrar sessões administrativas, garantindo auditoria contínua. Ademais, reduzirá os riscos de

comprometimento de contas privilegiadas, impedindo ataques baseados em escalonamento de privilégios. Outro benefício esperado é a implementação do acesso Just-in-Time (JIT), concedendo privilégios apenas pelo tempo necessário para execução de tarefas críticas. A integração com autenticação multifator (MFA) reforçará a segurança no acesso às credenciais privilegiadas. A adoção do PAM contribuirá diretamente para a conformidade com as diretrizes de governança cibernética estabelecidas na Estratégia Nacional de Segurança Cibernética (ENSEC-PJ) do CNJ e na Estratégia de Segurança da Informação do PJAC, promovendo um ambiente digital mais seguro e resiliente.

A implementação de uma solução PAM trará diversos benefícios estratégicos e operacionais para o PJAC. O primeiro deles é a melhoria na segurança da infraestrutura de TI, reduzindo vetores de ataque relacionados a credenciais privilegiadas e acessos indevidos. O controle granular de acessos administrativos garantirá que privilégios sejam concedidos apenas quando estritamente necessários, conforme exigido pelas normativas de segurança cibernética. Além disso, a rastreabilidade e auditoria das atividades privilegiadas serão aprimoradas, permitindo um controle mais rigoroso sobre ações realizadas por usuários administrativos. A automação e centralização da gestão de credenciais também reduzirão a carga operacional da equipe de Secretaria de Tecnologia da Informação e Comunicação (SETIC), eliminando práticas manuais inseguras.

Diante dos desafios enfrentados e das exigências normativas, recomenda-se a realização de um estudo técnico aprofundado para avaliar soluções PAM disponíveis no mercado, seus custos, requisitos de implementação e aderência às necessidades do PJAC. Essa iniciativa fortalecerá a segurança cibernética do Tribunal e garantirá maior controle sobre acessos privilegiados, contribuindo para a proteção dos sistemas e dados institucionais. Por conseguinte, a adoção da solução PAM demonstrará o compromisso do PJAC com a governança de segurança cibernética, atendendo às determinações das Resoluções CNJ nº 396/2021 e TPADM PJAC nº 291/2023, bem como às diretrizes internacionais de segurança da informação.

3. DESCRIÇÃO DE REQUISITOS

- Manter as contas privilegiadas em um único repositório seguro;
- Implementar regras para autorização do uso das contas privilegiadas;
- Geração automática da senha no momento da retirada;
- Entrega de sessão autenticada, sem que o usuário tenha contato com a senha.
  Definir o tempo em que o usuário autorizado poderá usufruir da conta privilegiada;
- Registrar as ações realizadas em posse de conta privilegiada com possibilidade de gravação de sessão (gravação de telas);

- Melhorar controle sobre a utilização de recursos privilegiados do ambiente computacional.
  Obter o monitoramento das ações de funcionários e terceiros com o uso de credenciais privilegiadas;
- Melhorar qualidade na prestação de informações na investigação de incidentes de segurança;
- Melhorar qualidade na prestação de informações aos órgãos de controle;
- Rastrear o uso de contas privilegiadas no ambiente computacional;
- Os serviços com licenças perpétuas devem ser hospedados na infraestrutura do PJAC*, on premisses.*

3.1. Dos Requisitos Legais

Lei Complementar n° 123/2006: Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte, e dá outras providências;

Lei Federal nº 14.133/2021: Estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios;

Lei Federal nº 13.709/2018: Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

Decreto nº 7.845/2012: Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

IN SGD/ME nº 94/2022: Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. Instrução Normativa utilizada por falta de regulamentação local ou estadual vigente e atualizada.

A solução deverá atender aos critérios de sustentabilidade ambiental, seguindo, no que couber, as diretrizes da Instrução Normativa SLTI/MPOG nº 01, de 19/01/2010, quanto ao uso de materiais, observando que esses sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme Normas ABNT NBR - 15448-1 e 15448-2.

Os equipamentos que venham a ser utilizados, não poderão conter substâncias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs) em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substance).

3.2. Dos Requisitos Temporais

A solução deverá ser entregue, instalada e implantada conforme eventos abaixo:

Evento	Descrição	Prazo	Responsável
01	Confirmação do Recebimento da Ordem de Serviço	Durante a vigência do Contrato	PJAC
02	Reunião Inicial e Apresentação do Projeto Executivo	Em até 10 (dez) dias úteis, contados a partir do evento 01	PJAC e CONTRATADA
03	Avaliação do Projeto Executivo	Em até 5 (cinco) dias úteis, contados a partir do evento 02	PJAC
04	Entrega dos produtos, equipamentos, softwares e licenças	Em até 45 (quarenta e cinco) dias úteis, contados a partir do evento 01	CONTRATADA
05	Emissão do Termo de Recebimento Provisório de Entrega de Equipamentos e Softwares	Em até 10 (dez) dias úteis, contados a partir do evento 04	PJAC
06	Instalação, configuração e operacionalização dos produtos, equipamentos e softwares, além da entrega do *As Built* e repasse de conhecimento	Em até 30 (trinta) dias úteis, contados a partir do evento 04 e em caso de aprovação do evento 03	CONTRATADA
07	Emissão do Termo de Recebimento Definitivo de Entrega de Equipamentos e Softwares	Em até 10 (dez) dias úteis, contados a partir do evento 06	PJAC

Para os itens relativos a treinamento, deverá ocorrer conforme eventos abaixo:

Evento	Descrição	Prazo	Responsável
01	Confirmação do Recebimento da Ordem de Serviço de Treinamento	Durante a vigência do Contrato	PJAC
02	Entrega do Cronograma de Treinamento	Até 7 dias úteis após o evento 01	CONTRATADA
03	Avaliação do Cronograma de Treinamento	Até 7 dias úteis após o evento 02	PJAC
04	Ajustes no Cronograma de Treinamento	Até 7 dias úteis após o evento 03	CONTRATADA
05	Execução dos Treinamentos	Até 30 dias úteis após o evento 04	CONTRATADA
06	Emissão do Termo de Recebimento Definitivo do Treinamento	Até 10 dias úteis após o evento 05	PJAC

3.3. Dos Requisitos de Segurança e Privacidade

Os serviços obedecerão, especialmente, às disposições legais da ABNT NBR 11515:2007 - Guia de práticas para segurança física, relativas ao armazenamento de dados.

A Contratada deverá exigir dos seus empregados, quando em serviço nas dependências do Contratante, o uso obrigatório de uniformes e crachás de identificação.

A Contratada não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado às informações de propriedade do PJAC.

A solução e os profissionais envolvidos na sua operacionalização deverão atender plenamente às seguintes condições:

a. Requisitos de segurança e procedimentos definidos para o acesso às dependências do PJAC, bem como requisitos de segurança da informação e de vedação de acesso e divulgação, conforme se aplique, a informações classificadas e privadas, e ainda a informações privilegiadas, isto é, aquelas que por qualquer motivo possam vir a representar vantagem mercantil competitiva;

b. Sigilo sobre iniciativas, projetos, decisões, dados e qualquer outro tipo de informação sensível de que venham a ter conhecimento durante a execução dos serviços, não podendo divulgá-las ou utilizá-las, durante a execução dos serviços e mesmo após seu encerramento, sem a expressa autorização do Ministério;

c. Deverão ser observados os requisitos de Segurança da Informação e Privacidade (SIP) de dados pessoais. Observar conformidade com o seguinte arcabouço legislativo:

- Decreto nº 9.637, de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação;
- ABNT NBR ISO 22301:2013 - Sistemas de gestão de continuidade de negócios;
- ABNT NBR ISO 22313:2015 - Orientações para uso da NBR 22301, no que tange à segurança e resiliência;
- ABNT NBR ISO 27031:2015 - Diretrizes para a prontidão e continuidade dos negócios de tecnologia da informação;
- ABNT NBR ISO 23081-1:2019 - Metadados para documentos de arquivo;
  ABNT NBR ISO/IEC 27037:2012 - Diretrizes para identificação, coleta, aquisição e preservação de evidência digital;
- ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27014:2013 - Governança de segurança da informação;
- ABNT NBR 16167:2013 - Diretrizes para classificação, rotulação e tratamento da informação;
- ABNT NBR ISO/IEC 27017:2016 - Código de prática para controles de segurança da informação com base
- ABNT NBR ISO/IEC 27002, para serviços em nuvem.

Obedecer à Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, considerando, principalmente:

> *[...]*
> *art. 7º - O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*
> *[...]*
> *III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;*
> *[...]*
> *art. 26 - O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.*
> *§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:*
> *[...]*
> *IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos.*
> *[...]*

A solução deverá obedecer, integralmente, às políticas de Segurança da Informação do PJAC, com assinatura de Termo de Confidencialidade pelos funcionários alocados na prestação de serviços.

A Contratada deverá comunicar imediatamente ao CONTRATANTE qualquer ocorrência de transferência, remanejamento ou demissão de funcionários envolvidos diretamente na execução do objeto, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do CONTRATANTE, porventura colocados à disposição para realização dos serviços contratados.

4. DESCRIÇÃO DA SOLUÇÃO

Gerenciar todo o ambiente sem a necessidade de instalação de agentes ou qualquer software nos sistemas-alvos ou dispositivos de rede.

Gerar vídeos ou logs de textos das sessões realizadas através da solução, armazenados em repositório seguro, criptografado e protegido contra qualquer alteração que comprometa a integridade dessas evidências;
Geração automática de senhas de alta complexidade de acordo com as regras de cada tecnologia e Política de Segurança da empresa.

Tanto appliances quanto sistemas operacionais que compõe a solução devem seguir padrões de ?hardening? atualizados constantemente pelo fabricante da solução.

O Banco de Dados deverá ser fornecido como parte integrante da solução.

Utilizar um banco de dados com as melhores práticas de segurança, deve estar em ambiente ?hardenizado?, com mecanismo de blindagem e criptografia do sistema operacional e documentação que comprove a contemplação destes requisitos.

Possibilitar a utilização de criptografia do banco de dados utilizado pela solução, para armazenar as senhas das credenciais gerenciadas por ela, devendo ainda ser compatível com pelo menos um dos seguintes métodos e padrões de criptografia:

a. AES com chaves de 256 bits;

b. FIPS 140-2;

c. Encriptação PKCS#11 ou superior por hardware utilizando dispositivos de HSM devidamente homologados pelo fabricante para a solução ofertada;

d. Para geração de hash, deve permitir a utilização do algoritmo SHA-256 ou variações superiores da família SHA-2.

A solução deverá prover mecanismos de criptografia de usuário e senha para conexão com base de dados.

A solução não deverá trafegar dados sensíveis em texto claro.

A solução deverá prover mecanismos de criptografia para informações sensíveis armazenadas em banco de dados compatível com o padrão AES com chaves de 256 bits.

A interface da solução, no acesso via navegador web, deverá utilizar o protocolo HTTPS.

O backup/restore de todos os dados e configurações da solução deve estar incluso e deve permitir ao administrador agendar backups para determinada data e hora e exportá-los para um servidor remoto.

A solução deverá manter a persistência de todos os relatórios e arquivos históricos, incluindo gravações de sessão, sem necessidade de resta1ração de backup, por pelo menos 90 (noventa) dias.

A solução deverá permitir retenção em backup de relatórios e logs da aplicação por pelo menos 2 (dois) anos.

A solução deve permitir retenção em backup das gravações de sessão por pelo menos 1 (um) ano.

O arquivo de backup não deverá conter nenhuma informação de conta e senha em texto claro.

No backup da chave mestra, ela deve poder ser dividida pelo sistema por uma quantidade parametrizada de partes, de modo que não permita a visualização do todo por uma única pessoa, mas apenas a parte devida a cada uma delas.

A solução deverá possibilitar a replicação em outros Data Centers.

No caso de falha de um dos servidores do cluster de cofre de senhas de alta disponibilidade local, cada um dos servidores deve tratar todas as requisições de acesso, sem nenhum prejuízo no desempenho ou nas funcionalidades.

Alterações realizadas no cluster de cofre de senhas de alta disponibilidade local deve ser automaticamente replicadas para os outros servidores de redundância, de forma síncrona e com delay máximo de 50ms.

Utilizar tecnologia de restrição e autenticação que inclua Assinatura Digital (Hash), e endereço IP do host ou conjunto de hosts a serem acessados pela solução.

A solução deve permitir compatibilidade com, no mínimo, os seguintes padrões: ISO 27001, PCI, SOX, GDPR, PQO BM&F, para implementação de controles de acesso a credenciais privilegiadas.

Possibilidade de comunicação com os serviços de diretório via protocolo LDAPS.

Suportar sincronização do relógio interno via protocolo NTP.

A solução deve possuir interface única, na mesma solução, para o gerenciamento de senhas e sessões.

A solução deve oferecer o provisionamento e gerenciamento de todas as contas privilegiadas, incluindo contas para a administração de aplicações de negócio, bancos de dados e dispositivos de redes, não se limitando apenas às contas de sistemas operacionais de servidores.

A solução deverá realizar sincronismo de data e relógio via protocolo NTP (Network Time Protocol) ou por meio do serviço de data e hora do sistema operacional.

A solução deverá prover mecanismos de atualização de segurança.

Ter uma console de configuração unificada para gerenciamento de contas e ativos agregados ao cofre de senhas;

Permitir o backup e o recovery de seu banco de dados, bem como das configurações de software estabelecidas, com as seguintes capacidades:

a. Permitir a execução de tarefas de backup e criptografia sem a necessidade de agentes de terceiro, provendo assim o maior nível possível de segurança e integridades dos dados a serem copiados;

b. Permitir a execução de backups automatizados através da programação/agendamento;

c. Permitir, através de interface gráfica, que administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros.

d. Extrair backups do sistema, logs e vídeos além das credenciais para um servidor localizado em Data Centers remotos caso seja necessário para restaurar todas as configurações e os dados da solução de cofre de senhas.

A solução deve permitir que você finalize todas as sessões em andamento, bloqueie o acesso a dispositivos predefinidos ou bloqueie todo o acesso a ele por um período definido.

4.1. Gerenciamento de senhas:

A solução deve permitir parametrização de políticas de segurança e força de senha pelo administrador do sistema, dentre as quais:

a. Conjunto de caracteres alfanuméricos, numéricos e caracteres especiais, podendo ser escolhidos também quais caracteres especiais serão permitidos, com possibilidade de não possibilitar caracteres repetidos, gerando senhas aleatórias;

b. Gerenciar chaves SSH e fazer Scan de servidores Linux e identificação e publicação de chaves SSH;

c. Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo;

d. Consolidação periódica de senhas para identificar senhas que foram alterados em sistema gerenciados;

e. Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legado;

f. Oferecer interface com visão personalizada exclusiva para Auditorias e Órgãos Reguladores, contendo os dispositivos e credenciais gerenciadas pela solução;

g. Fornecer uma área de transferência segura, para que o solicitante possa visualizar ou copiar a senha na tela de login do sistema de destino;

h. Prover área de transferência segura, de forma que o solicitante possa visualizar a senha ou copiá-la para a tela de login do sistema-alvo;

i. Liberação ou revogação de todos os acessos de uma determinada credencial de maneira automatizada e imediata;

j. Notificar, via e-mail ou SMS, novas solicitações de aprovação de acesso aos respectivos responsáveis pelas credenciais;

k. Permitir o monitoramento on-line do uso das contas e desligamento da sessão.

Apresentar o recurso "break glass" para acesso de emergência às contas, ou seja, permitirá acesso a ativos protegidos de forma emergencial, sem a necessidade de aprovação prévia em contas no qual o usuário não teria acesso, sem perda de rastreabilidade.

Oferecer a funcionalidade de "Discovery" para realizar busca de novos servidores, elementos de rede e bancos de dados, sendo capaz de levantar automaticamente as contas criadas nesses novos dispositivos incluindo a possibilidade de descobrir certificados SSL utilizado nos dispositivos gerenciados.

A ferramenta deverá cuidar do ciclo de vida completo de um certificado, possuindo as seguintes funcionalidades: Criação de uma requisição, assinatura, renovação e revogação de certificados.

A solução deverá possuir fluxos de aprovação, incluindo aprovação multinível para as seguintes funcionalidades: Assinatura de um .csr, renovação e instalação.

A solução deverá realizar o deploy de certificados no mínimo nos seguintes ambientes: Apache, IBM Websphere, F5 BigIP, IIS, Nginx, Tomcat.

A solução deve possibilitar a revogação de um certificado, não permitindo nenhuma interação com o certificado quando estiver revogado, apenas a renovação.

A solução deverá possuir relatórios e dashboards gerenciais que mostrem toda a base de certificados, centralizando as informações mais críticas de um certificado, como por exemplo certificados que estão próximos a vencer.

A solução deverá possibilitar a configuração de notificações multiníveis como por exemplo, um certificado a 90 dias para vencer irá notificar o analista, 60 dias para vencer irá notificar o gestor, e 30 dias irá notificar o gerente.

A solução deverá possibilitar a criação e importação de requisições de certificados (.csr).

A solução deverá se integrar com no mínimo as seguintes autoridades certificadoras: DigiCert, Godaddy, Microsoft CA, Comodo, GlobalSign e Let's Encrypt.

A solução deve possibilitar o saque de senha de um certificado baseado nas permissões que foram atribuídas para cada usuário. Todos os saques deverão ser auditados, e também deve ser possível passar por um processo de fluxo de aprovação com break the glass e aprovação multiníveis.

A solução deverá possibilitar a criação de organizações gerenciais de certificados dentro do sistema.

A solução deverá permitir a importação manual de um certificado, independentemente de qual formato ele seja.

Deve ser possível o envio de certificados por e-mail nos principais formatos, sendo no mínimo: der, pem, pfx, p7b.

Deve ser possível o download de certificados nos principais formatos, sendo no mínimo: der, pem, pfx, p7b.

A solução deve permitir o gerenciamento de certificados independentemente de qual formato ele é. Essa informação deverá ser transparente ao administrador.

A solução deverá ter uma funcionalidade para delegar um responsável, que será notificado em relação a qualquer acontecimento relacionado a aquele certificado.

A solução deve possuir dashboards gerenciáveis que mostre todos os certificados ativos gerenciados, separando por diversos tipos de regras de negócio, como vencimento, nível de segurança e a localização dos certificados.

A solução deve possibilitar a renovação de certificados, podendo também alterar informações de um certificado e gerar um histórico para que seja um possível regaste de informações.

A solução deve permitir a instalação programada de um certificado, podendo ser selecionado dia, hora e data que será instalada, e também em quais dispositivos aquele certificado será instalado.

A solução deve possuir uma funcionalidade para renovar automaticamente certificados quando o certificado estiver: X dias antes do vencimento, na data do vencimento, e X dias após o vencimento.

A solução deve possuir uma inteligência para fazer a avaliação de segurança de um certificado, levando em consideração pelo menos 5 critérios de segurança.

A solução deve gerenciar os certificados de uma maneira que não considere o formato dos certificados, ou seja, na requisição, assinatura, renovação e instalação dos certificados, o administrador não deve saber quais são os formatos necessários, isso deve estar embutido na inteligência da aplicação.

Possibilidade de bloqueio de comandos específicos, com opção de interromper a sessão caso o usuário execute um comando indevido.

Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas.

Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado.

Possibilidade de geração de relatórios baseados nos logs e exportá-los para arquivos em formato ?.csv?.

A funcionalidade deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, macros, chamadas executáveis, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, RPC, WinRM, SSH, API REST HTTP/HTTPS.

As senhas geradas automaticamente pela solução de cofre de senhas devem seguir os seguintes requisitos:

a. Poder determinar a quantidade de caracteres;

b. Ser composta por números, letras maiúsculas, letras minúsculas e por caracteres especiais;

c. Poder ser pré-definidas quais caracteres especiais poderão ser utilizados;

d. Aleatórias de modo que dentro do histórico de uma conta seja improvável encontrar duas senhas iguais;

e. Não seja baseada em palavra de dicionário.

A solução deve permitir a criação de políticas de senhas de forma hierárquica ou em níveis de segurança, possibilitando a criação de senhas diferenciadas para grupos de ativos de diferentes plataformas ou criticidades.

Possuir mecanismo para exportar arquivo com as últimas senhas para repositório remoto, de forma criptografada e protegida por senha de dupla custódia para recuperações de senhas no caso de falha total da solução.

A solução deve possibilitar políticas de senha que impeça visualização simultânea de credenciais, sessões, bem como também configurar o tempo de expiração das senhas baseadas por visualização e data de expiração. Também deve ser possível escolher dias específicos da semana e horários que as credenciais poderão expirar.

A solução deve gerenciar senhas privilegiadas de aplicações, de modo a evitar situação de senhas embutidas em códigos-fonte.

A solução deve ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas ou domínios distintos.

A solução não deverá depender da instalação de agentes para realizar a troca de senhas.

Checkout/CheckIn de credencial: A solução deve redefinir a credencial (senha) no ambiente para os casos de visualização da senha pelo solicitante nos processos de checkout de credencial.

A solução deve ter a capacidade de realizar a reconciliação de credenciais automaticamente.

4.2. Rotação de Senhas:

a. Troca automática de senhas para Servidores (Unix, Linux, Windows), Bancos de Dados (MS SQL, ORACLE, MYSQL, PostgreSQL);

b. Aplicações Web, Dispositivos de Rede, Mainframe;

c. A solução deverá realizar a troca automática da senha da ligação entre servidores MS SQL server com Linked Servers;

d. Geração automática de senhas de força/complexidade de acordo com as regras de cada tecnologia e Política de Segurança da empresa;

e. Flexibilidade para configuração de força de senha gerada;

f. Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo;

g. Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legado;

h. Possibilidade de executar trocas de senhas por meio de automações que interagem com páginas web, tanto para sistemas externos reconhecidos, como para sistemas internos desenvolvidos por equipes internas;

i. Armazenamento de histórico de senhas por equipamento;

j. Registro de troca executadas;

k. Relatório de acompanhamento de trocas;

l. Relatório de erros de trocas;

m. Alertas de falha ou sucesso de trocas;

n. Possibilidade de reconfiguração/customização de scripts ou plugin de troca de senhas para configuração de casos que exijam parâmetros específicos para rotação de senhas;

o. Configuração de políticas de trocas de senhas com agendamento programado ou por ocorrências de eventos com especificação de parâmetros de prazo para a troca;

p. Disponibilizar os Templates de troca de senha de forma que possam ser abertos, editáveis e auditáveis;

q. Templates com linguagem acessível e fácil interpretação;

r. Rastreabilidade de Alteração de Templates;

s. Troca de senhas em aplicações HTTP/HTTPS com templates .

4.3. Controle de Acesso:

a. A solução deve ser capaz de limitar a execução de comandos críticos pelos usuários cadastrados;

b. A solução deve ser capaz de prover acesso externo sem a necessidade de instalação de Agent ou utilização de VPN;

c. A solução deve permitir o controle de execução de comandos críticos por, pelo menos, ?whitelist? e ?blacklist?.

d. A solução deve permitir o início e a condução de sessões dentro do próprio navegador, dispensando o uso de clients externos como omstsc.exe e o putty.exe;

e. A solução deve possuir tempo de expiração de sessão configurável pelo administrador do sistema.

f. A solução deve suportar a desconexão da sessão por atividade/uso indevido de comandos pré-cadastrados no sistema;

g. A solução deve permitir a criação de grupos de usuários.

h. Bloqueio ou alerta de comandos com alertas, interrupção de sessão ou apenas o registro de execução - baseado em blacklist;

i. Bloqueio ou alerta de comandos com alertas, interrupção de sessão ou apenas o registro de execução - baseado em whitelist;

j. Possibilidade de bloqueio e auditoria de comandos específicos;

k. Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas;

l. Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado;

m. Marcação de pontuação de comandos de acordo com nível de risco de cada comando.

A solução deve permitir a atribuição de privilégios a grupos de usuários, associados a um ou mais alvos gerenciados.

A Solução deve permitir integração com ferramentas de gestão de incidentes (ITSM) para validar tickets abertos durante processo de aprovação de acesso.

A solução deve permitir acesso simultâneo ao cofre de senhas e as contas privilegiadas por dois ou mais usuários.

A solução deve viabilizar a segregação de funções entre usuários de uma mesma aplicação gerenciada.

A solução deve fornecer funcionalidade para revogar imediatamente todas as sessões remotas para um usuário conectado.

A solução deve permitir acesso simultâneo à credenciais privilegiadas por dois ou mais usuários.

Acessos simultâneos a credenciais, senhas e dispositivos não devem possuir comprometimento da rastreabilidade.

Possibilitar via script, a criação de novos conectores baseado em acessos SSH e RDP, para que seja possível suportar novas interfaces de autenticação de ativos.

A solução deverá permitir o gerenciamento e monitoramento de sessões do Microsoft Azure.

Ser compatível com sistemas operacionais: Windows Server 2008 ou superior, Red Hat Enterprise, Debian, CentOS, IBM zOS, Solaris, Ubuntu Server.

Ser compatível com aplicações Windows: contas de serviço e pools de aplicações do IIS.

Ser compatível com sistemas gerenciadores de bancos de dados: Oracle, Oracle RAC, MSSQL, MySQL, Sybase ASE e IQ, MongoDB, PostgreSQL.

Ser compatível com appliances de segurança: Cisco, IBM, SourceFire.

Ser compatível com dispositivos de rede: Cisco, D-Link, HP, 3com, Alcatel, Foundry, Brocade, ARUBA, Huawei.

Ser compatível com aplicações: WebLogic, JBOSS, Tomcat, Peoplesoft, Oracle Application Server, Apache e IIS;
Ser compatível com serviços de Diretórios: AD, LDAP.

Ser compatível com ambientes virtuais: VMware e Openstack.

Ser compatível com storages: Hitachi, Isilon, EMC, Huawei, Netapp, Pure Storage e IBM.

Ser disponibilizado um SDK (Software Development Kit) ou API (Application Programming Interface) que pode ser configurado para permitir que aplicações clientes possam:

a. Solicitar credenciais e dispositivos;

b. Cadastro e alteração credenciais e dispositivos;

c. Solicitar chaves SSH;

d. Cadastro e alteração de chaves SSH.

Ser compatível com aplicações em nuvem como Rackspace, IBM SmartCloud, Microsoft Azure, Hyper-V, Google Cloud Platform, GoGrid, Vmware vCenter Server, Amazon AWS.

4.4. Cadastro de Ativos:

Cadastro de equipamentos parametrizado manualmente.

Atributos como Marca, Modelo, Fabricante, Localidade, Grupo abertos para configuração do administrador da ferramenta independente do fabricante. A solução deve armazenar senhas para aplicações e serviços online.

A solução deve armazenar documentos e arquivos.

A solução deve armazenar notas.

A solução deve possuir registro de acesso a informações privilegiadas.

A solução deve ter a possibilidade de compartilhar informações com outros usuários.

A solução deve possuir APIs para gerenciar itens do cofre.

A solução deve guardar diferentes versões de um segredo que possam ser restauradas.

A solução deve oferecer importação em lote de senhas, notas, documentos e arquivos.

A solução deve oferecer migração das informações do LastPass.

A solução deve possuir um dashboard administrativo com opções de ambiente.

A solução deve possuir uma extensão de navegador para Google Chrome.

Utilizando a extensão deve ser possível salvar senhas diretamente do website acessado.

A solução deverá ser flexível no processo de aprovação para o acesso a contas privilegiadas (acessos pré-aprovados, acessos com aprovação única e e acessos com aprovações multiníveis).

A solução deverá permitir a configuração de fluxos de aprovação diferenciados por criticidade e características da conta, como contras privilegiadas e contas de uso por terceiros.

A solução deverá permitir a alteração, por parte do aprovador, do período de acesso solicitado por um usuário.

Caso uma solicitação de acesso seja aprovada, a sessão e o privilégio concedido deverão expirar automaticamente ao final do período autorizado.

O acesso ao fluxo de solicitação e aprovação deve ser possível de ser realizado de forma remota e segura.

A solução deve possuir função para revogar todos os acessos de uma pessoa de maneira imediata.

A solução deve oferecer um campo para que seja inserido um número identificador de demanda ou mudança ao qual o acesso estará associado.

A solução deve oferecer interface para usuários e auditores, provendo mecanismos de controle de acesso flexíveis para criar visões/grupos personalizados de dispositivos gerenciados e contas privilegiadas.

A solução deverá prover mecanismo de acesso emergencial a saque de senhas cadastradas na solução.

O acionamento do acesso emergencial deve notificar os aprovadores via e-mail ou pela interface da ferramenta.

5. LEVANTAMENTO DE MERCADO

Foi realizado um levantamento de mercado, no qual foram identificadas as seguintes ferramentas:

- **CyberArk:** gerencia credenciais privilegiadas, armazenando-as em um cofre seguro e aplicando rotação automática de senhas. Ele permite controle rigoroso de acessos, gravação de sessões e auditoria detalhada das atividades. Possui integração com diversos sistemas e usa autenticação multifator para reforçar a segurança;
- **SenhaSegura:** oferece armazenamento seguro de credenciais, controle de acessos privilegiados e rastreamento de atividades. Suas funcionalidades incluem cofre de senhas, autenticação reforçada, gravação de sessões e relatórios detalhados de auditoria. Também permite integração com diretórios corporativos para facilitar a gestão.

Após análise, dessas ferramentas que gerenciam o acesso remoto, foi a diagnosticado que uma ferramenta de PAM atende os requisitos e as necessidades deste Poder.

6. ESTIMATIVA DAS NECESSIDADES

6.1. Cluster para prover os recursos para a solução

Para garantir alta disponibilidade e desempenho da solução de PAM, é necessário o provisionamento de um ambiente em cluster com licenciamento perpétuo. Essa estrutura assegura a continuidade dos serviços críticos de gerenciamento de acessos privilegiados mesmo em caso de falha de um dos nós, além de permitir escalabilidade e balanceamento de carga nativo.

6.2. Cluster Balanceador de carga para prover os recursos para a solução

O balanceador de carga é essencial para distribuir uniformemente o tráfego entre os nós do cluster com licenciamento perpétuo, otimizando o desempenho da aplicação e evitando sobrecarga de recursos. Além disso, contribui para a resiliência da solução ao permitir failover transparente para os usuários.

6.3. Gerir Usuários com acesso privilegiado

Usuários com privilégios administrativos representam os maiores riscos à segurança da informação. O gerenciamento centralizado dessas contas permite aplicar controle de acesso, rastreabilidade, autenticação forte, rotatividade de senhas e concessão de privilégios temporários, mitigando riscos de uso indevido, vazamentos ou acessos não

autorizados. Assim, estima-se uma a quantidade de 150 licenças perpétuas atenderá a necessidade do PJAC, considerando principalmente os servidores da SETIC.

6.4. Gerir Servidores físicos e virtuais

A gestão de acessos privilegiados a servidores é crítica para garantir que apenas usuários autorizados e auditados realizem operações sensíveis. A solução PAM deve permitir o controle, monitoramento e auditoria de acessos administrativos nas 400 máquinas físicas e virtuais geridas pela Secretaria de Tecnologia da Informação e Comunicação, com licenciamento perpétuo.

6.5. Gerir Equipamentos de conectividade de Rede

Equipamentos como switches, roteadores e firewalls compartilham credenciais administrativas. A solução de PAM deve ter controle rigoroso sobre esses acessos, com rotação de senhas, registro de sessões e prevenção de escalonamento indevido, para fortalecer a segurança da infraestrutura de rede em 300 equipamentos geridos pela Divisão de Infraestrutura de Tecnologia da Informação, com licenciamento perpétuo.

6.6. Gerir Aplicações não conteinerizadas com senha embutida (hard coded)

Muitas aplicações legadas armazenam senhas embutidas em arquivos de configuração ou código-fonte, a ferramenta deve gerenciar as credenciais, evitando exposição e reduzindo a superfície de ataque em 30 aplicações com essas características, com licenciamento perpétuo.

6.7. Gerir Usuários externos com acesso remoto seguro

A solução deverá oferecer acesso remoto a terceiros com controle granular, sem exposição de senhas, com autenticação multifator, gravação de sessão e revogação automática. Garantindo que 20 empresas e/ou pessoas prestadoras de serviços no PJAC consigam acessar de forma privilegiada, monitorada e controlada os serviços necessários para a prestação de serviço, considerando que esse serviço deverá utilizar a infraestrutura em nuvem da contratada, este item será contratado sob o modelo de subscrição pelo período de 36 meses.

6.8. Gerenciar Certificados Digitais

A gestão manual de certificados digitais pode resultar em expiração não planejada, indisponibilidade de sistemas e falhas de segurança. O módulo de gerenciamento de certificados do PAM deve automatizar o ciclo de vida (emissão, renovação, revogação e deploy) de 4 certificados geridos pelo PJAC. Este serviço deverá utilizar a infraestrutura em nuvem da contratada, assim, este item será contratado sob o modelo de subscrição pelo período de 36 meses.

6.9. Serviço de instalação e configuração da solução

A implementação inicial deve ser realizada por equipe especializada para garantir a aderência à arquitetura recomendada pelo fabricante, integrar os diversos ativos da infraestrutura (servidores, switches, AD, bancos de dados) e aplicar boas práticas de segurança. Isso reduz riscos de má configuração e acelera a entrada em operação.

6.10. Manutenção e suporte técnico da solução por 36 meses

O suporte técnico contínuo garante atualização de segurança, correções de bugs, acesso ao suporte de segundo e terceiro nível do fabricante, e suporte a incidentes. Além disso, permite ajustes na solução à medida que novos sistemas são integrados ou requisitos regulatórios evoluem. Portanto, o item será do tipo subscrição por 36 meses.

6.11. Treinamento para a solução

Capacitar a equipe técnica do PJAC é essencial para garantir o uso correto da ferramenta, configuração de políticas de segurança, integração com sistemas, geração de relatórios e resposta a incidentes. O treinamento reduz dependência do fornecedor e fortalece a autonomia institucional na administração da ferramenta. Assim é necessário treinar uma turma com até 15 servidores, com foco em operação, manutenção e gestão da solução.

As quantificações apresentadas foram obtidas a partir de levantamento técnico detalhado realizado sobre a infraestrutura de TI do PJAC, considerando ativos críticos, usuários com perfil de acesso elevado e aplicações sensíveis. O processo foi conduzido pela Subsecretaria de Segurança da Informação e Infraestrutura de Tecnologia da Informação e Comunicação, com a participação direta do corpo técnico especializado da Subsecretaria, assegurando a representatividade das demandas operacionais e o alinhamento com os requisitos técnicos da solução a ser adotada.

7. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

A pesquisa de preços para a estimativa de custos desta contratação será realizada com base em Atas de Registro de Preços vigentes em órgãos públicos com escopo semelhante ao pretendido, de forma a garantir realismo orçamentário e aderência técnica, conforme determina o art. 23, §1º, inciso II da Lei nº 14.133/2021.

Assim, será considerado o quantitativo levantando nesse estudo e usando como referência:

- **Ata de Registro de Preços nº 18/2025**, firmada pelo Ministério Público do Estado do Piauí (MPPI), cujo objeto é a contratação de solução de Privileged Access Management (PAM), incluindo licenciamento, serviços e suporte técnico.

Ferramenta SenhaSegura Edital Nº. 90004/2025 ? ARP Nº. 0994935 - Ministério Público de Estado do Piauí					
Item	**Descrição**	**Tipo**	**Qtd.**	**ATA Nº. 18/2025 MPPI**	**Valor Total**
1	Cluster para prover os recursos para a solução	Licença perpétua	1	R$ 299.999,00	R$ 299.999,00
2	Cluster Balanceador de carga prover os recursos para a solução	Licença perpétua	1	R$ 299.999,00	R$ 299.999,00

3	Gerir usuários com acesso privilegiado	Licença perpétua	150	R$ 6.599,00	R$ 989.850,00
4	Gerir servidores físicos e virtuais	Licença perpétua	400	R$ 329,00	R$ 131.600,00
5	Gerir equipamentos de conectividade de Rede	Licença perpétua	300	R$ 129,00	R$ 38.700,00
6	Gerir aplicações não conteinerizadas com senha embutida (hard coded)	Licença perpétua	30	R$ 2.999,00	R$ 89.970,00
7	Gerir usuários externos com acesso remoto seguro	Subscrição	20	R$ 5.500,00	R$ 110.000,00
8	Gerenciamento de certificados digitais	Subscrição	4	R$ 9.200,00	R$ 36.800,00
9	Serviço de instalação e configuração da solução	Unidade	1	R$ 48.000,00	R$ 48.000,00
10	Manutenção e suporte técnico da solução por 36 meses	Subscrição	1	R$ 800.000,00	R$ 800.000,00
11	Treinamento para turma da solução	Unidade	1	R$ 51.558,00	R$ 51.558,00
Total					**R$ 2.896.476,00**

- **A Ata de Registro de Preços nº 031/2024** do Tribunal de Justiça do Estado do Amazonas (TJAM), proveniente do Pregão Eletrônico nº 040/2024, que trata da contratação de solução de segurança para identidades e privilégios, com abrangência sobre servidores, aplicações, suporte técnico e transferência de conhecimento.

Ferramenta CyberArk Pregão Nº. 040/2024 ? ARP Nº. 031/2024 - Tribunal De Justiça Do Estado Do Amazonas					
Item	**Descrição**	**Tipo**	**ATA Nº. 031/2024 TJ/AM**	**Qtd.**	**Valor Total**
1	Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI (12 meses)	und	R$ 14.895,85	150	R$ 2.234.377,50
2	Proteção para Aplicações Tradicionais (12 meses)	und	R$ 8.500,00	30	R$ 255.000,00
3	Proteção Local para servidores Windows e Linux (12 meses)	und	R$ 3.369,80	400	R$ 1.347.920,00
5	Serviço de instalação e configuração da solução	und	R$ 120.000,00	1	R$ 120.000,00
6	Transferência de conhecimento (por turma)	und	R$ 47.250,00	1	R$ 47.250,00
7	Serviço de Suporte Técnico Especializado (mensal)	mês	R$ 21.000,00	36	R$ 756.000,00
Total					**R$ 4.760.547,50**

A utilização dessas atas como referência está fundamentada no art. 23, §1º, inciso II da Lei nº 14.133/2021, que autoriza a adoção de contratos e atas de outros órgãos como parâmetro para estimativas de preços, desde que o objeto seja compatível.

As referidas ARP's apresentam alta aderência funcional aos requisitos definidos neste ETP, abrangendo componentes como gerenciamento de acessos privilegiados, cofre de senhas, acesso remoto seguro, instalação, suporte e treinamento. Além de representar uma contratação pública recente e de escopo semelhante

8. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Considerando a interdependência entre os componentes que compõem a solução de Privileged Access Management (PAM) - tais como software, serviços de instalação, suporte técnico e capacitação - a contratação deverá ocorrer em lote único. Essa abordagem visa garantir a plena compatibilidade entre os elementos da solução, assegurar a integração adequada entre suas partes e viabilizar o cumprimento dos prazos de implantação estabelecidos.

A fragmentação em lotes distintos comprometeria a efetividade da solução, dificultando a interoperabilidade, a rastreabilidade e a centralização do suporte técnico, além de potencialmente aumentar os custos operacionais e os riscos contratuais. A unificação da contratação em um único processo permite, ainda, consolidar a responsabilidade técnica e contratual em um único fornecedor, evitando falhas de integração e conflitos de escopo.

Dessa forma, a contratação não será parcelada, por se tratar de uma solução única e integrada, nos termos do disposto na Súmula TCU nº 247 e na Instrução Normativa SGD/ME nº 01/2019. Além disso, a adoção de um contrato unificado proporciona economia de escala, facilita o acompanhamento técnico e administrativo do contrato e contribui para uma melhor experiência de uso da solução por parte dos usuários.

9. RESULTADOS PRETENDIDOS

Com a implantação de uma solução de Privileged Access Management (PAM), espera-se alcançar os seguintes resultados e benefícios para o Poder Judiciário do Estado do Acre (PJAC):

a. Centralização da gestão e governança dos acessos privilegiados aos ativos de tecnologia da informação;

b. Automação de políticas de controle e uso de credenciais privilegiadas, promovendo maior padronização e segurança;

c. Incremento da segurança e auditoria no uso de contas privilegiadas, com rastreabilidade detalhada;

d. Armazenamento seguro de credenciais privilegiadas em cofre digital único e criptografado;

e. Definição de regras para autorização, concessão e expiração de acessos privilegiados (acesso Just-in-Time);

f. Geração automática e rotativa de senhas, reduzindo o risco de reutilização ou vazamento;

g. Entrega de sessões autenticadas sem a exposição da senha ao usuário final;

h. Definição de janela de tempo para uso autorizado das contas privilegiadas, com revogação automática;

i. Registro completo das ações executadas durante o uso das contas privilegiadas, com possibilidade de gravação de tela e geração de trilhas de auditoria;

j. Aumento do controle e da visibilidade sobre o uso de contas administrativas e de alto privilégio no ambiente computacional do PJAC;

k. Monitoramento detalhado das ações realizadas por servidores e terceiros com acesso privilegiado, promovendo maior responsabilização;

l. Melhoria na qualidade e rapidez da resposta a incidentes de segurança da informação;

m. Melhoria na prestação de informações aos órgãos de controle e auditoria;

n. Rastreabilidade completa do uso de contas privilegiadas, contribuindo para a conformidade com normas como LGPD, ISO 27001 e resoluções do CNJ.

10. PROVIDÊNCIAS PARA ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO

Não foram identificadas necessidades de adequações tecnológicas, estruturais ou organizacionais para a implantação da solução proposta. O atual parque tecnológico do Poder Judiciário do Estado do Acre (PJAC) já dispõe de infraestrutura compatível, incluindo equipamentos, rede e ambientes de virtualização, aptos a receber e suportar os itens contemplados neste Estudo.

11. IMPACTOS AMBIENTAIS E SUSTENTABILIDADE

A contratação observará diretrizes de sustentabilidade conforme o art. 11 da Lei nº 14.133/2021, com as seguintes medidas:

- Uso de servidores virtualizados, evitando aquisição de novos equipamentos e reduzindo o consumo de energia;
- Eliminação de impressão de documentos, priorizando registros digitais;
- Atividades conduzidas remotamente, sem necessidade de deslocamentos físicos.

Essas ações contribuem para a redução de impactos ambientais e reforçam a eficiência da contratação.

12. ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO

Considerando os riscos identificados relacionados à gestão de acessos privilegiados, a necessidade de conformidade com normativas como a Lei Geral de Proteção de Dados (LGPD), a ISO/IEC 27001, e as Resoluções CNJ nº

396/2021 e TPADM PJAC nº 291/2023, bem como os benefícios esperados com a adoção de uma solução de Privileged Access Management (PAM).

A aquisição da solução permitirá fortalecer a segurança da informação institucional, elevar o nível de governança sobre os acessos administrativos, reduzir a exposição a riscos cibernéticos e atender plenamente aos requisitos legais e normativos aplicáveis ao Poder Judiciário. Além disso, a contratação em lote único garante a compatibilidade técnica entre os módulos, facilita a integração nativa entre os componentes da solução e contribui para a economicidade e eficiência na gestão contratual.

No processo de avaliação técnica e econômica, **a ferramenta SenhaSegura** se destacou como a **opção mais vantajosa para o PJAC**. A escolha está fundamentada nos seguintes fatores:

- Aderência integral aos requisitos funcionais e de segurança estabelecidos neste Estudo;
  Capacidade de integração com múltiplos ativos da atual infraestrutura (servidores, aplicações, dispositivos de rede e certificados digitais);
- Vantagem econômica identificada na pesquisa de preços, com base nas Atas de Registro de Preços do Ministério
- Público do Piauí (ARP MPPI nº 23/2023) e do Tribunal de Justiça do Amazonas (ARP TJAM nº 031/2024), cujos preços praticados são compatíveis com a realidade do mercado e aderentes ao escopo desta contratação.

Ante o exposto, temos a solução final a ser contratada na tabela a seguir:

Item	Necessidades	Tipo	Qtd.
1	Cluster para prover os recursos para a solução	Licença perpétua	1
2	Cluster Balanceador de carga prover os recursos para a solução	Licença perpétua	1
3	Gerir usuários com acesso privilegiado	Licença perpétua	150
4	Gerir servidores físicos e virtuais	Licença perpétua	400
5	Gerir equipamentos de conectividade de Rede	Licença perpétua	300
6	Gerir aplicações não conteinerizadas com senha embutida (hard coded)	Licença perpétua	30
7	Gerir usuários externos com acesso remoto seguro por 36 meses	Subscrição	20
8	Gerenciamento de certificados digitais por 36 meses	Subscrição	4
9	Serviço de instalação e configuração da solução	Unidade	1
10	Manutenção e suporte técnico da solução por 36 meses	Subscrição	1
11	Treinamento para turma da solução	Unidade	1

A ferramenta SenhaSegura é uma solução consolidada no mercado nacional e internacional de Privileged Access Management (PAM), comercializada por diversos representantes, integradores e canais autorizados, o que garante a ampla competitividade necessária à contratação pública. A indicação da solução como referência técnica não implica em direcionamento, mas sim em alinhamento com os requisitos funcionais, operacionais, orçamentários e normativos estabelecidos neste Estudo Técnico Preliminar. Nos termos do art. 46, §1º da Lei nº 14.133/2021, a Administração

pode indicar marcas como parâmetro de desempenho ou qualidade, desde que comprovada a viabilidade de competição, o que se confirma neste caso pela existência de múltiplos fornecedores habilitados no mercado para o fornecimento da referida solução.

Portanto, a contratação é tecnicamente adequada, oportuna e alinhada aos objetivos estratégicos do PJAC.

13. ANÁLISE DE RISCO

A seguir, apresenta-se a análise preliminar dos principais riscos associados à contratação, implantação e operação da solução de Privileged Access Management (PAM), com respectivas medidas de mitigação:

Risco Identificado	Probabilidade	Impacto	Classificação	Medida de Mitigação Proposta
1. Incompatibilidade técnica entre componentes da solução	Média	Alto	Alto	Aquisição em lote único, com solução integrada e homologada pelo mesmo fornecedor
2. Fornecedor não entregar funcionalidades conforme especificações	Baixa	Alto	Médio	Elaboração de requisitos técnicos detalhados, realização de testes de aceite e cláusulas contratuais específicas
3. Falha na implantação e integração com ativos de TI existentes (AD, servidores, rede etc.)	Média	Alto	Alto	Exigir serviços de instalação e configuração por equipe certificada; acompanhamento técnico pela DITEC
4. Resistência à adoção da solução por parte dos usuários técnicos	Média	Médio	Médio	Inclusão de treinamento para equipe do PJAC; sensibilização e apoio da alta gestão
5. Ausência de suporte técnico adequado durante o ciclo contratual	Baixa	Alto	Médio	Contratação de suporte técnico com SLA definido por 36 meses; avaliação prévia da capacidade técnica do fornecedor
6. Vulnerabilidades de segurança na solução implementada	Baixa	Alto	Alto	Exigir certificações de segurança da solução (ISO 27001, FIPS 140-2, entre outras) e atualizações regulares
7. Obsolescência tecnológica ou descontinuidade da solução	Baixa	Médio	Baixo	Escolha de solução consolidada e contrato com cláusulas de continuidade
8. Estimativa de preço incompatível com valores de mercado	Baixa	Médio	Baixo	Pesquisa de preços com base em duas atas de registro de preços públicas recentes (MPPI e TJAM)
9. Eventual indisponibilidade da solução durante incidentes	Média	Alto	Alto	Implantação em cluster de alta disponibilidade com balanceador de carga; monitoramento contínuo
10. Risco de sobreposição de funções e acessos excessivos	Média	Alto	Alto	Uso de políticas de privilégio mínimo, segregação de funções

				e rastreabilidade de ações via PAM

14. ADERÊNCIA DAS SOLUÇÕES DISPONÍVEIS ÀS POLÍTICAS DO GOVERNO

REQUISITOS	SIM	NÃO	NÃO APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X		
A Solução está disponível no Portal do Software Público Brasileiro?		X	
A Solução é um software livre ou software público?		X	
A Solução é aderente às políticas, premissas e Especificações técnicas definidas pelos Padrões e PING, e-MAG?			X
A Solução é aderente às regulamentações da ICP Brasil			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus)?			X

15. DA EQUIPE DE PLANEJAMENTO

Nome	Cargo	Setor
Elson Correia de Oliveira Neto	Secretário de Tecnologia da Informação e Comunicação	SETIC
Gerson Oliveira da Silva Junior	Chefe da Divisão de Segurança da Informação	DISEG

16. MODELO DE EXECUÇÃO E GESTÃO DO CONTRATO

- **Modelo de Gestão do Contrato:** O modelo deve descrever como a execução do objeto será acompanhada e fiscalizada pelo órgão ou entidade;

- **Fiscalização:** Deve haver fiscalização para garantir a correta execução do contrato, com a possibilidade de apoio dos órgãos de assessoramento jurídico e controle interno;
- **Gestão de Riscos:** Deve haver análise dos riscos que podem comprometer o sucesso da contratação e a boa execução contratual. O contrato deve refletir a alocação de riscos estabelecida na matriz;
- **Reajustamento e Repactuação:** O contrato deve prever índices de reajustamento de preço com data-base vinculada à data do orçamento, podendo ser estabelecido mais de um índice;
- **Acompanhamento da Execução:** A execução do contrato deve ser monitorada, com a emissão de relatórios de acompanhamento;
- **Responsabilidade do Contratado:** O contratado é o único responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato, exceto em serviços contínuos com regime de dedicação exclusiva de mão de obra, onde pode haver responsabilidade solidária ou subsidiária da Administração.

17. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO

Considerando os riscos identificados relacionados à gestão de acessos privilegiados, a necessidade de conformidade com normativas como a LGPD, a ISO 27001 e as Resoluções CNJ nº 396/2021 e TPADM TJAC nº 291/2023, bem como os benefícios esperados com a adoção de uma solução de Privileged Access Management (PAM), conclui-se que a contratação é tecnicamente adequada, com a escolha da ferramenta **SenhaSegura** como a melhor alternativa, conforme apontamento no item 12. (ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO), de forma oportuna e alinhada aos objetivos estratégicos do TJAC.

A aquisição da solução permitirá fortalecer a segurança da informação institucional, elevar o nível de governança sobre os acessos administrativos, reduzir a exposição a riscos cibernéticos e atender aos requisitos legais e normativos aplicáveis. Além disso, a contratação em lote único garante a compatibilidade técnica, facilita a integração entre os componentes da solução e contribui para a economicidade e eficiência na gestão contratual.

Dessa forma, a contratação proposta é recomendada como a alternativa mais vantajosa para a Administração, sob os aspectos técnico-operacional, normativo e estratégico.

18. DECLARAÇÃO DE VIABILIDADE

A equipe responsável pelo estudo e planejamento da contratação, após a execução e conclusão dos estudos técnicos preliminares descritos neste documento, declara ser viável, essencial e urgente a efetivação da presente contratação sob o risco da materialização de riscos elevados à conformidade tecnológica e de segurança da informação neste egrégio PJAC, com consequente impacto às suas atividades jurisdicionais.

Para conferir a autenticidade do documento, utilize um leitor de QRCode ou acesse o endereço **http://appgrp.tjac.jus.br/grp/acessoexterno/programaAcessoExterno.faces?codigo=670270** e informe a chancela **OUKY.7Y8X.BQ2U.7GJV**

Documento assinado eletronicamente por **ELSON CORREIA DE OLIVEIRA NETO**, **Secretário** em 07/07/2025 às 15:30:31.

Documento assinado eletronicamente por **GERSON OLIVEIRA DA SILVA JUNIOR**, **Chefe de Divisão** em 07/07/2025 às 15:13:27.