PODER JUDICIÁRIO
DO ESTADO DO ACRE

MINUTA DO TERMO DE REFERÊNCIA Nº 52/2025

Processo nº 2025-206

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), conforme itens abaixo:

Item	Necessidades	Tipo	CATSER	Qtd.	Valor Unitário	Valor Total
1	Cluster para prover os recursos para a solução	Licença perpétua	27464	1		
2	Cluster Balanceador de carga prover os recursos para a solução	Licença perpétua	27464	1		
3	Gerir usuários com acesso privilegiado	Licença perpétua	27464	150		
4	Gerir servidores físicos e virtuais	Licença perpétua	27464	400		
5	Gerir equipamentos de conectividade de Rede	Licença perpétua	27464	300		
6	Gerir aplicações não conteinerizadas com senha embutida (hard coded)	Licença perpétua	27464	30		
7	Gerir usuários externos com acesso remoto seguro por 36 meses	Subscrição	27502	20		
8	Gerenciamento de certificados digitais por 36 meses	Subscrição	27502	4		
9	Serviço de instalação e configuração da solução	Unidade	26972	1		
10	Manutenção e suporte técnico da solução por 36 meses	Subscrição	25992	1		
11	Treinamento para turma da solução	Unidade	3840	1		

Os serviços objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

O prazo de vigência da contratação é de 36 (doze) meses contados da assinatura, prorrogável por até 5 anos, na forma do artigo 106 da Lei n° 14.133, de 2021.

O fornecimento dos serviços de subscrição (itens 7, 8 e 10) são enquadrados como continuados, sendo a vigência plurianual mais vantajosa, conforme Estudo Técnico Preliminar.

O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

O objeto da contratação está previsto no Plano de Contratações Anual 2025, conforme detalhamento a seguir:

I) ID PCA no PNCP: 04034872000121-0-000006/2025;

II) Data de publicação no PNCP: 29/01/2025;

III) Id do item no PCA: 106;

IV) Classe/Grupo: 583 - LICENÇA DE SOFTWARE;

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

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.

3.1. 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.

3.2. 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 .

3.3. 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.

3.4. 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.

4. REQUISITOS DA CONTRATAÇÃO

- 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;
- As Licenças devem ser caráter perpétuas;
- Os serviços devem ser hospedados na infraestrutura do TJAC, *on premisses.*

4.1. 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).

4.2. 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

4.3. 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.

4.4. Dos Requisitos de Segurança e Privacidade

4.4.1. Sustentabilidade:

Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.4.2. Subcontratação

Não é admitida a subcontratação do objeto contratual.
O contrato oferece maior detalhamento das regras que serão aplicadas em relação à subcontratação, caso admitida.

4.4.3. Garantia da contratação

Não haverá exigência da garantia da contratação dos artigos 96 e seguintes da Lei nº 14.133, de 2021, pelas razões constantes do Estudo Técnico Preliminar.

O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. Condições de Entrega

O prazo de entrega dos serviços é de 15 dias, contados da emissão do empenho.

Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 15 (QUINZE) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

Os serviços deverão ser executados no seguinte endereço:

Tribunal de Justiça do Estado do Acre
Rua Desembargador Jorge Araken, s/n. Via Verde.
CEP: 69.915-631 - Rio Branco-AC - (68) 3302-0408.

6. MODELO DE GESTÃO DO CONTRATO

O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

As comunicações entre o órgão e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

O órgão poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Após a assinatura do contrato ou instrumento equivalente, o órgão poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

6.1. Fiscalização

A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

FISCAL TÉCNICO: Gerson Oliveira da Silva Junior - Matrícula: 7002070

FISCAL ADMINISTRATIVO:

GESTOR: Elson Correia de Oliveira Neto - Matrícula: 7001778

Futuras alterações de gestor e fiscal de contrato, serão efetivadas por portaria da Presidência.

6.2. Fiscalização Técnica

O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

6.3. Fiscalização Administrativa

O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada para a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

6.4. Gestor do Contrato

O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

7.1. Recebimento

O recebimento definitivo ocorrerá no prazo de 10 (dez) dias úteis, a contar do recebimento da nota fiscal, após a verificação e atesto do fiscal técnico da nota fiscal e consequente aceitação mediante **termo recebimento definitivo.**

Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até 05 (cinco) dias úteis.

O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

O recebimento definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens nem a responsabilidade ético-profissional pela perfeita execução do contrato.

7.2. Liquidação

Recebida a Nota Fiscal, correrá o prazo de dez dias para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.]

O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

o prazo de validade;

a data da emissão;

os dados do contrato e do órgão contratante;

o quantitativo dos serviços;

o valor a pagar; e

eventual destaque do valor de retenções tributárias cabíveis.

Havendo erro na apresentação da nota fiscal, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta *on-line* ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

A Administração deverá realizar consulta ao SICAF para:

a) verificar a manutenção das condições de habilitação exigidas no edital;

b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

7.3. Prazo de pagamento

O pagamento será efetuado no prazo de até 10 (dez) dias contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice **IPCA** de correção monetária.

7.4. Forma de pagamento

O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

8.1. Forma de seleção e critério de julgamento da proposta

fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, modo aberto, com adoção do critério de julgamento pelo MENOR PREÇO.

8.2. Forma de fornecimento

O fornecimento do objeto nos itens 7, 8 e 10 são considerados como serviço continuado.

8.3. Exigências de habilitação

Para fins de habilitação, deverá o licitante comprovar, dentre outros requisitos, os seguintes:

8.4. Qualificação Técnica

Comprovação de aptidão para o fornecimento de bens compatíveis com o objeto desta contratação, por meio da apresentação de certidões ou atestados, emitido por pessoas jurídicas de direito público ou privado.

Será admitida, para fins de comprovação, a apresentação de diferentes atestados executados de forma concomitante.

Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

O custo estimado total da contratação é de R$ 2.896.476,00 (dois milhões, oitocentos e noventa e seis, quatrocentos e setenta e seis reais), conforme custos unitários apostos em anexo no comparativo de preços (D18932).

10. ADEQUAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no orçamento do Tribunal de Justiça do Estado do Acre.

A contratação será atendida pela seguinte dotação:

I) Programa de Trabalho: 203.617.02.061.2293.2214.0000 - MANUT. DAS ATIVIDADES DO FUNDO ESPECIAL DO PJ;
II) Fonte de Recursos: 2760 - Recursos de Emolumentos, taxas e custas;
III) Elemento de Despesa: 33904000000000 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

Rio Branco, 26 de junho de 2025.

Documento assinado eletronicamente por **GERSON OLIVEIRA DA SILVA JUNIOR**, **Chefe de Divisão** em 08/07/2025 às 14:01:08.