PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR
PRSTM/SECSTM/DITIN/COTEC

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de empresa para a aquisição de licenças de proteção de usuários com acessos privilegiados, proteção de usuários externos/remoto, serviço de autenticação por múltiplos fatores, instalação, suporte técnico especializado e treinamento, **pelo Sistema de Registro de Preços.**

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

A Justiça Militar da União (JMU) passou a integrar o Poder Judiciário a partir da Constituição de 1934 e seus julgamentos seguem a mesma sistemática do Judiciário Brasileiro.

Na condição de serviço público, a JMU submete-se também ao Princípio da Continuidade, também conhecido como Princípio da Permanência, o qual veda a estas instituições a opção pela interrupção de suas atividades em face dos potenciais prejuízos para o cidadão e para a sociedade. Neste sentido, a Constituição Federal de 1988 em seu § 6º do artigo 37, determina que "[...] pessoas jurídicas de direito público [...] responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa."

Considerando o princípio da continuidade, e na esteira da invasão sofrida pelo Superior Tribunal de Justiça (STJ) em novembro de 2020, o Conselho Nacional de Justiça, órgão responsável pelo controle da atuação administrativa e financeira dos tribunais, manifestou-se na Resolução nº 396 para consolidar estratégia de segurança, a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). O documento, que abrange todos os Tribunais Nacionais, visa que tais tribunais busquem ações para elevar o nível da segurança cibernética do ecossistema digital do Poder Judiciário brasileiro. Entre outras medidas, a Resolução CNJ nº 396/2021 tornam obrigatórias ações dos Tribunais no sentido de remover ou mitigar riscos de que ataques como o perpetrado contra o STJ, não voltem a prejudicar a prestação jurisdicional ao ponto de interromper suas atividades.

Assim sendo, uma solução de gerenciamento de identidades e acesso mostra-se essencial para a garantia dos requisitos de confidencialidade, disponibilidade e integridade das informações custodiadas pelo Tribunal, condição indispensável à continuidade do negócio e ao cumprimento de seus propósitos institucionais. Em resumo, a presente contratação visará:

Prover gerenciamento único de contas e identidades privilegiadas por meio de cofre de senhas, responsável pela geração, revogação, versionamento, armazenamento e controle de credenciais de acesso;

Prover controle de sessões privilegiadas por meio de proxy de conexão, capaz de monitorar e auditar acessos remotos;

Implementar modelo administrativo de privilégios mínimos no acesso a ativos de tecnologia, incluindo o controle de aplicativos, monitoramento de serviços e filtragem de comandos;

Prover rápida identificação, contenção e erradicação de ameaças em sessões privilegiadas;

Prover monitoramento em tempo real por meio da coleta, análise e monitoramento de logs gerados em acessos privilegiados, essenciais à correta detecção, classificação e priorização de incidentes de segurança.

3. OBJETIVOS A SEREM ALCANÇADOS POR MEIO DA CONTRATAÇÃO

3.1. Dentre os benefícios, destacam-se:

3.1.1. Tornar o ambiente do STM mais seguro e inclusivo no ambiente digital;

3.1.2. Aumentar a resiliência às inevitáveis ameaças cibernéticas;

3.1.3. Estabelecer governança de segurança cibernética;

3.1.4. Fortalecer a gestão integrada de ações de segurança cibernética; e

3.1.5. Permitir a manutenção e continuidade dos serviços, ou o seu restabelecimento em menor tempo possível, na eventualidade de algum incidente.

3.1.6. Atender ao art. 29, da Resolução CNJ nº 396/2021, quanto à implementação da gestão de usuários de sistemas informatizados composta de: gerenciamento de identidades, gerenciamento de acessos; e gerenciamento de privilégios.

4. MODALIDADE E TIPO DE LICITAÇÃO

Por se tratar de contratação de bens e serviços comuns, nos termos do parágrafo único do art. 1º da Lei nº 10.520/02, o certame licitatório será realizado por meio de Sistema de Registro de Preços, na modalidade Pregão, em sua forma eletrônica, do tipo menor preço global.

Como a aquisição pretendida será em grupos e a a contratação não se dará logo após a licitação, tendo em vista que a instalação de algumas licenças dependeram da instalação de outras, sugerimos a aplicação da modalidade de Sistema de Registro de Preços.

Por se tratar de bens usuais no mercado e passíveis de serem definidos de forma objetiva, o objeto em questão se enquadra na definição de bens e serviços comuns

5. PARCELAMENTO DO OBJETO E ADJUDICAÇÃO

Objetivando reduzir a complexidade da gestão do contrato, reduzir os custos de administração, a solução será agrupada em dois grupo, não sendo objeto de parcelamento os itens de cada grupo, a adjudicação do objeto de contratual deverá ser feita a uma ou mais empresas a fim de garantir a economia de escala para Administração, já que a prática do mercado consiste em ofertar maiores descontos à medida em que se aumenta a quantidade de produtos contratados. Outrossim, tal medida permite racionalizar os custos com pessoal dedicado às atividades de planejamento da contratação, de escolha do fornecedor e de gestão e fiscalização do contrato, em consonância com os princípios constitucionais da economicidade e da eficiência.

6. ALINHAMENTO ENTRE A CONTRATAÇÃO DE FORNECIMENTO E O PLANEJAMENTO ESTRATÉGICO DA JMU

A análise, está em consonância com a necessidade de prover uma solução capaz de atender as demandas da JMU, de forma a atingir os objetivos propostos por este projeto, em especial possibilitar a realização de análises em tempo exíguo para tomadas de decisão, viabilizando inclusive emissão de relatórios gerenciais e ampliação do conhecimento sistêmico organizacional.

Objetivo: Fortalecer a governança e a segurança de dados e informações.

Estratégia: Compatibilizar a infraestrutura e as soluções de TIC às necessidades da JMU.

Iniciativa: Aperfeiçoar a gestão e a proteção de dados e informações.

7. ESTUDOS

Os Estudos Técnicos Preliminares (Documento de Oficialização da Demanda – DOD, a Análise de Viabilidade da Contratação, a Sustentação do Contrato, a Estratégia para a Contratação e a Análise de Riscos) foram realizados pela equipe de Planejamento de conforme determinado o art. 12, § 1º, da Resolução nº 182/13, do CNJ.

8. RELAÇÃO ENTRE A DEMANDA PREVISTA E OS SERVIÇOS A SEREM CONTRATADOS

Entende-se que as demandas previstas e projetadas pela COTEC a serem atendidas pela contratação da solução de PAM (Privileged Access Management) e MFA (Mullti-factor authentication), serão cobertas em sua plenitude, durante o período de vigência de 60 meses, através do contrato estabelecido entre o CONTRATANTE e a CONTRATADA. Abaixo estão elas listadas:

GRUPO 1			
ITEM	**PRODUTO**	**UNIDADE**	**QTD**

1.	Proteção de usuários com acessos privilegiados	UN	250
2.	Proteção de usuários externos/Remoto	UN	100
3.	Serviço de instalação e configuração	UN	1
4.	Suporte Técnico Especializado	Mensal	60
5.	Treinamento	UN	1

GRUPO 2			
ITEM	**PRODUTO**	**UNIDADE**	**QTD**
1.	Licença de serviço de autenticação por múltiplos fatores	UN	3.000
2.	Serviço de instalação e configuração	UN	1
3.	Suporte Técnico Especializado	Mensal	60
4.	Treinamento	UN	1

A quantidade de 3.000 licenças para o item 1 do Grupo 2, tem como justificativa a expectativa de aumento no quadro efetivo de pessoal da JMU, além disso, a solução protege todos os usuários (estagiáros e terceirizados) que porventura tiverem login e senha para acesso a rede interna do STM.

9. JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

Com a constante modernização e ampliação dos aparatos de Tecnologia da Informação dentro de uma instituição, cresce a preocupação das entidades públicas e privadas sobre a proteção dos dados e da privacidade dos seus cidadãos. Além disso, algumas normativas governamentais como, por exemplo, a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018), em vigor, PDA – Plano de Dados Abertos e a lei n° 12.965/2014 - Marco Civil da Internet, que descrevem aprimoramentos e regras de segurança no ambiente de TIC visando a proteção e conservação dos dados e consequentemente da privacidade das pessoas, faz com que empresas e instituições públicas e privadas necessitam investir cada vez mais em recursos tecnológicos para segurança da informação, mas além de investir, é importante prezar pela economia que poderia ser comprometida decorrente do não cumprimento destas regulamentações exigidas nas leis apresentadas.

Outrossim, considerando que o foco de um atacante (hacker) é tentar descobrir um usuário com senha fraca, comprometendo a conta do usuário e com isso conseguir almejar privilégios para burlar a segurança e conseguir derrubar serviços e obter informações, o comportamento do usuário com suas senhas é de extrema importância.

Embora a boa prática no ambiente corporativo, recomende fortemente que os usuários evitem usar senhas fracas, não usem senhas pessoais para acessar sistemas, alterem suas senhas com frequência, dentre outras medidas, a senha do usuário é, da perspectiva de segurança, certamente o ponto mais fraco e vulnerável.

O Gartner, instituto mundial renomado de previsão e consultoria na área de TIC, no aspecto de Segurança da Informação, desde 2019 vem afirmando que investimento em soluções para proteção das credenciais deve estar no topo de prioridade das empresas. Fonte: https://www.gartner.com/en/documents/3900996-top-10-security-projects-for-2019 https://www.gartner.com/en/documents/4003658

Sendo assim é dever da DITIN formalizar e conduzir o macroprocesso de segurança da informação nos ativos de TIC, garantir que os ativos críticos, os riscos, as ameaças, as vulnerabilidades e os incidentes de segurança sejam identificados, monitorados e priorizados por meio de controles efetivos.

Nesse contexto, impera a necessidade de contratação de uma solução que centralize e permita uma gestão dos usuários de vários sistemas críticos, sendo eles usuários privilegiados, externos ou de negócio, é uma necessidade para trazer melhor administração, gestão e auditoria de acessos à infraestrutura de rede e à todas as informações acerca dos diversos sistemas existentes no parque tecnológico do STM, entrando em conformidade com as regulamentações das leis que exigem o cumprimento da segurança da informação e dados.

Assim sendo, a Solução de proteção de usuários com acesso privilegiados, proteção de usuários externos/remoto e serviço de autenticação por múltiplos fatores demonstram ser a melhor opção para alcançar os objetivos que o STM pretende com a aquisição.

Estas tecnologias são capazes de oferecerem todos os recursos elencados e avaliados

neste estudo técnico.

10. ESPECIFICAÇÃO TÉCNICA

GRUPO 1			
ITEM	**PRODUTO**	**UNIDADE**	**QTD**
1.	Proteção de usuários com acessos privilegiados	UN	250
2.	Proteção de usuários externos/Remoto	UN	100
3.	Serviço de instalação e configuração	UN	1
4.	Suporte Técnico Especializado	Mensal	60
5.	Treinamento	UN	1

GRUPO 2			
ITEM	**PRODUTO**	**UNIDADE**	**QTD**
1.	Licença de serviço de autenticação por múltiplos fatores	UN	3.000
2.	Serviço de instalação e configuração	UN	1
3.	Suporte Técnico Especializado	Mensal	60
4.	Treinamento	UN	1

10.1. ESPECIFICAÇÃO DO OBJETO - GRUPO 1

10.1.1. ITEM 1: SOLUÇÃO PARA PROTEÇÃO DE USUÁRIOS COM ACESSOS PRIVILEGIADOS

10.1.1.1. A solução deverá incluir um conjunto de softwares, do mesmo fabricante, com licenciamento por subscrição necessários ao atendimento dos requisitos mínimos especificados

10.1.1.2. Gerenciamento de chaves

10.1.1.2.1. As credenciais devem ser geridas pela solução, mitigando problemas de segurança relacionados ao compartilhamento de contas que são armazenadas localmente em dispositivos e para as contas que não são gerenciadas de forma centralizada por serviços de diretórios;

10.1.1.2.2. A solução deve descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados incluindo tarefas agendadas do Windows (Scheduled tasks), Serviços Windows e Pools de conexão do IIS. Além disso, a solução deve apresentar um relatório com detalhes de quais serviços do Windows estão usando credenciais e propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas;

10.1.1.2.3. A solução deve descobrir e alterar credenciais Windows, incluindo contas nomeadas, administradores 'built-in' e convidados;

10.1.1.2.4. A solução deve gerenciar credenciais de Banco de Dados, incluindo Microsoft SQL Server, Teradata, PostgreSQL, Oracle, MongoDB, MySQL e Sybase ASE;

10.1.1.2.5. A solução deve descobrir e alterar credenciais privilegiadas e acesso por chaves SSH em ambientes Linux e Unix; incluindo a possibilidade de identificar as contas privilegiadas com ID 0 ('0') e contas que não possuem ID zero, porém, são privilegiadas através do uso de ´sudo´ (configuradas no Sudoers);

10.1.1.2.6. Gerenciar credenciais em interfaces de gerenciamento de servidores "out-of-band", suportando ao menos Dell DRAC e HP iLO;

10.1.1.2.7. A solução deve descobrir e alterar credenciais do Active Directory (AD) e todos os outros serviços de diretório compatíveis com LDAP, sem necessidade de adaptações ou scripts;

10.1.1.2.8. Controlar e monitorar sessões usando protocolos padrões e acesso

remoto, incluindo RDP, HTTP/HTTPS e SSH;

10.1.1.2.9. A Solução deverá prover segurança de acessos a sistemas críticos por meio de credenciais administrativas, e estar licenciada para, no mínimo, 250 usuários ou dispositivos;

10.1.1.2.10. A solução deverá ser entregue licenciada para ser implantada em arquitetura on-premise ou em nuvem que garanta alta disponibilidade para todas as funcionalidades, com opção ativo-ativo ou ativo-passivo local, com failover automático;

10.1.1.2.11. A solução poderá ser ofertada na modalidade appliance físico, appliance virtual, ou instalação e configuração de máquina virtual feita pelo fornecedor.

10.1.1.2.12. Se ofertado em appliance físico:

10.1.1.2.13. Cada appliance deverá ser instalado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários;

10.1.1.2.14. Os recursos de processamento e memória da solução Appliance deverão ser suficientes para a implementação de todas as funcionalidades descritas nesta especificação;

10.1.1.2.15. Todos os equipamentos necessários à prestação dos serviços devem ser novos e de primeiro uso.

10.1.1.2.16. Para as soluções ofertadas em virtual appliance ou máquina virtual, os recursos de hardware serão fornecidos pela CONTRATANTE. Os softwares e o virtual appliance deverá ser baseada em ambiente VMWare ESXi com S.O.s Windows server e Linux;

10.1.1.2.17. O Banco de Dados poderá ser fornecido como parte integrante da solução, ou se a solução utilizar o banco de dados externo, o CONTRATANTE fornecerá desde que compatível com o SQL Server da Microsoft;

10.1.1.2.18. A solução deve incorporar medidas de segurança como Certificação Common Criteria (CC) – ISO/IEC 15408 – como garantia de segurança do método utilizado no desenvolvimento do sistema de repositório seguro de credenciais e Criptografia dos módulos da solução, a fim de proteger a informação em trânsito entre módulos da solução e aplicações web dos usuários finais e possibilitar a utilização de criptografia do banco de dados utilizado pela solução para armazenar as credenciais gerenciadas e FIPS 140-2;

10.1.1.2.19. Para fins de auditoria e conformidade, a solução deve oferecer no mínimo os seguintes relatórios:

10.1.1.2.19.1. Lista de contas e idade de senhas desde o último descobrimento;

10.1.1.2.19.2. Atividades de mudanças feitas na solução por qualquer usuário;

10.1.1.2.19.3. Detalhamento de grupos e usuários, detalhando permissões hierárquicas;

10.1.1.2.19.4. Lista de contas gerenciadas com idade de senha;

10.1.1.2.19.5. Lista de sistemas gerenciados;

10.1.1.2.19.6. Atividades de retirada de senhas e sessões;

10.1.1.2.19.7. Eventos de alteração de senha;

10.1.1.2.19.8. Auditoria de contas;

10.1.1.2.19.9. Atividades de atualização de senhas;

10.1.1.2.19.10. Atividades de sessões remotas;

10.1.1.2.19.11. Detalhes das próximas atualizações de senha programadas;

10.1.1.2.19.12. Sistemas que estão usando uma conta de serviço para iniciar um ou mais serviços.

10.1.1.2.20. Ser implantado com os recursos mínimos e suficientes para o provimento do serviço, incluindo a criptografia do sistema operacional e do sistema de gerenciamento de banco de dados (hardening);

10.1.1.2.21. Ser capaz de monitorar sessões, gravar sessões, capturar telas, coletar, armazenar e indexar logs de teclas pressionadas em teclado (keystrokes) em acessos privilegiados, garantindo os seguintes requisitos:

10.1.1.2.21.1. Alerta ao usuário privilegiado que a sessão está sendo gravada;

10.1.1.2.21.2. Monitoramento por meio de gravação de vídeos, em formato padrão de execução da solução; Monitoramento ao vivo, permitindo ao usuário supervisor, previamente configurado, realizar ações de lock/unlock, suspender e terminar a conexão;

10.1.1.2.21.3. Pesquisa forense de eventos de segurança em todas as sessões gravadas, incluindo comandos digitados, copiar e colar arquivos e execução de softwares;

10.1.1.2.22. Possuir funcionalidade de discovery, capaz de buscar e registrar novos ativos alvo, garantindo as seguintes condições:

10.1.1.2.22.1. Capacidade de realizar buscas no Active Directory e em blocos de endereços IP, podendo ser realizada por demanda, agendada e rotina periódica;

10.1.1.2.22.2. Levantamento de contas administrativas em cada ativo;

10.1.1.2.22.3. Levantamento de ativos e de suas respectivas identidades em grupos, de acordo com parâmetros previamente configurados;

10.1.1.2.22.4. Classificação automática de contas locais e de domínio;

10.1.1.2.22.5. Identificação de contas de serviços e de tarefas em ambientes Microsoft Windows;

10.1.1.2.22.6. Identificação de contas locais e que possuam chaves SSH em ambientes Unix/Linux;

10.1.1.2.23. Integrar-se à solução de Security Information and Event Management (SIEM);

10.1.1.2.24. Integrar-se à solução de Hardware Security Module (HSM) utilizando PKCS#11;

10.1.1.2.25. Possuir mecanismo de backup e restore de todos os dados e configuração da solução, incluindo recurso de exportação para um servidor remoto;

10.1.1.2.26. A solução deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, que podem ser exportados em formatos editáveis e não editáveis, suportando no mínimo dois dos formatos: HTML, PDF, CSV, XLSX ou XLS;

10.1.1.2.27. Prover relatórios de conformidade que disponibilizem operações, incluindo lista de sistemas gerenciados, eventos de alteração de senha, auditoria de contas e alertas de segurança

10.1.2. ITEM 2: PROTEÇÃO DE USUÁRIOS EXTERNOS/REMOTO

10.1.2.1. Incluir o fornecimento de módulo de acesso remoto seguro, on-premise ou em nuvem, garantindo o acesso a 100 usuários ou dispositivos;

10.1.2.2. Suportar o acesso externo a rede sem qualquer necessidade de utilização de VPN ou método similar de acesso;

10.1.2.3. Permitir o acesso remoto, no mínimo, aos seguintes sistemas operacionais:

10.1.2.3.1. Microsoft Windows 10 e superiores.;

10.1.2.3.2. Servidores Windows Server 2012 e superiores;

10.1.2.3.3. Linux Red Hat Enterprise 7.0 e superiores.

10.1.2.4. Utilizar protocolos de comunicação fazendo uso de criptografia TLS 1.2 ou superior;

10.1.2.5. Suportar o funcionamento a redes que não estão conectadas diretamente a internet e a redes seguras;

10.1.2.6. Suportar o acesso sem necessidade de permissão prévia para o acesso a desktops e servidores;

10.1.2.7. Possibilitar o acesso a dispositivos de rede via SSH, como roteadores e switches;

10.1.2.8. Disponibilizar aos usuários, console de acesso Web para a solução, sem a necessidade de instalação de plug-ins ou agentes;

10.1.2.9. Suportar provedores externos de identidades para autenticação, incluindo, no mínimo, servidores LDAP, Active Directory, RADIUS e Kerberos, bem como atribuir privilégios com base na hierarquia e nas configurações de grupo já´especificadas nos respectivos servidores;

10.1.2.10. Integrar-se com soluções de autenticação de duplo fator através de protocolo RADIUS, Single Sign-on via SAML ou OIDC e Time-Based One-Time Password (TOTP);

10.1.2.11. Suportar o uso de um certificado assinado por uma autoridade certificadora válida;

10.1.2.12. Permitir o agendamento para liberação do acesso remoto, incluindo notificação por e-mail aos destinatários designados;

10.1.2.13. Permitir forçar o encerramento da sessão remota pelo supervisor, com notificação ao cliente;

10.1.2.14. Prover monitoramento ao vivo e gravação da sessão, com registro completo das atividades executadas durante a sessão executada pelos usuários;

10.1.2.15. Limitar o acesso a aplicativos especificados no sistema remoto, incluindo a acesso a área de trabalho remota;

10.1.2.16. Suportar filtro de comandos durante as sessões SSH, visando evitar que o usuário inadvertidamente use um comando que pode causar danos ao servidor acessado;

10.1.2.17. Suportar a injeção automática de credenciais em sistemas Windows, permitindo que os usuários autentiquem ou elevem privilégios sem revelar credenciais, bem como a ação de “executar como”;

10.1.2.18. Suportar a injeção automática de credenciais em sistemas Unix/Linux, permitindo que os usuários autentiquem ou elevem privilégios sem revelar credenciais, bem como a utilização em conjunto com o sudo;

10.1.2.19. Suportar o acesso com os seguintes modos:

10.1.2.19.1. Através de clientes instalados;

10.1.2.19.2. Através de agente de proxy local, que permite o acesso a sistemas autônomos em uma rede, sem cliente pré-instalado;

10.1.2.19.3. Acesso via agente de proxy local, que permite o acesso a sistemas em uma rede remota que não tenha uma conexão de internet nativa;

10.1.2.20. Suportar Remote Desktop Protocol (RDP), permitindo que os usuários colaborem em sessões auditadas e gravadas;

10.1.2.21. Prover acesso a dispositivos de rede habilitados para SSH através de um cliente de proxy efetuando a conexão localmente;

10.1.2.22. Prover acesso a páginas Web, onde os usuários receberão apenas uma

conexão a uma página Web local em uma sessão auditada e gravada;

10.1.2.23. Permitir o monitoramento em tempo real das sessões de acesso feitas a ativos publicados na ferramenta;

10.1.2.24. Permitir a configuração de tempos limites para sessões ociosas, em que seja possível definir o tempo máximo para que um usuário inativo seja desconectado automaticamente;

10.1.2.25. Permitir que os usuários transfiram arquivos da máquina em que está conectado para o sistema remoto, através da console da solução e sem necessidade de uso de ferramentas de terceiros;

10.1.2.26. Permitir que os usuários compartilhem sessões de acesso com outros usuários do sistema, permitindo que os administradores colaborem em uma mesma sessão. Esta colaboração deve ser possível com usuários internos e externos através de convite;

10.1.2.27. Oferecer aos usuários conectados a capacidade de ver informações do sistema sem que seja necessário ter acesso a console do ativo;

10.1.2.28. Oferecer aos usuários a capacidade de executar tarefas do sistema fora do compartilhamento de tela, como por exemplo reiniciar um serviço em servidores com sistema operacional Windows;

10.1.2.29. Oferecer a opção de prover acesso à linha de comandos dos servidores sem a necessidade de compartilhamento de tela, permitindo aos administradores a execução de comandos remotos via conexões lentas de internet.

10.2. ESPECIFICAÇÃO DO OBJETO - GRUPO 2

10.2.1. ITEM 1 - LICENÇA DE SERVIÇO DE AUTENTICAÇÃO POR MÚLTIPLOS FATORES

10.2.1.1. Especificações Técnicas

10.2.1.1.1. A solução não deve limitar a quantidade de aplicações a ser utilizada.

10.2.1.1.2. A solução permite a autenticação de usuários por múltiplos fatores para os seguintes ambientes e produtos:

10.2.1.1.3. VPN Cisco AnyConnect, Fortinet FortiVPN/FortiClient, Check Point VPN, Palo Alto VPN, SonicWALL, OpenVPN (incluindo OpenVPN em PFSense), em estações de trabalho e dispositivos móveis com sistema operacional Android, iOS e Windows, no mínimo. A solução deve permitir que o servidor de VPN obtenha a lista de grupos autorizados para o usuário a partir do diretório de autenticação;

10.2.1.1.4. Virtual Desktop Infrastructure – VDI, da VMware, permitindo aos usuários o uso do cliente VMware Horizon 7 (ou superior) ou o uso de navegador para iniciar conexões, com no mínimo Windows, MacOs, Linux, Android e iOS;

10.2.1.1.5. Microsoft Remote Desktop Protocol – RDP, com o uso do Microsoft Remote Desktop Gateway;

10.2.1.1.6. Microsoft Remote Desktop Protocol – RDP, sem o uso do Microsoft Remote Desktop Gateway;

10.2.1.1.7. Estações de trabalho Microsoft Windows 10 e superiores;

10.2.1.1.8. Servidores Windows 2012 R2 e superiores (incluindo Windows Server 2022);

10.2.1.1.9. Secure Shell – SSH para acesso a servidores Linux através de estações de trabalho e dispositivos móveis que utilizam no mínimo Windows, Android e iOS. A solução deve suportar autenticação de usuários em diretório OpenLdap e AD, protocolo ssh suportado nas versões de Sistemas operacionais Oracle Linux 6, 7, 8 e superiores, Red Hat 6, 7, 8 e superiores;

10.2.1.1.10. Estações de trabalho Microsoft Windows 10 e superiores;.

10.2.1.2. Especificação do Produto

10.2.1.2.1. A solução fornece Application Programming Interface - APIs ou Software Development kit - SDKs que possam ser utilizadas por aplicações para autenticação de usuários e provisionamento de dispositivos. O padrão de comunicação com as APIs fornecidas é do tipo REST JSON;

10.2.1.2.2. A solução fornece funcionalidade que permite compartilhar os logs, por agendamento, com a ferramenta de SIEM – Security Information Event Management; A solução possibilita que as conexões de saída para a internet sejam realizadas através de servidor de proxy; solução possui suporte a auto provisionamento do usuário;

10.2.1.2.3. A solução fornece mecanismos de contingência para que, caso ocorra a interrupção da conexão de internet ou indisponibilidade do serviço, os usuários possam continuar se autenticando no ambiente;

10.2.1.2.4. A solução fornece a capacidade de avisar ao usuário, quando ocorre algum erro, através de mensagens que ajudam a identificar a causa sem expor informações críticas;

10.2.1.2.5. A solução fornece capacidade de integração com o Security Assertion Markup Language – SAML;

10.2.1.2.6. A solução fornece capacidade de integração com o Active Directory Federation Services – ADFS;

10.2.1.2.7. A solução fornece capacidade de integração com Remote Authentication Dial-In User Service – RADIUS;

10.2.1.2.8. A solução fornece capacidade de disponibilizar pelo menos os seguintes fatores de autenticação:

10.2.1.2.9. Push Notification (Notificação enviada para app instalado no dispositivo do usuário);

10.2.1.2.10. Software Token – OTP (One Time Password);

10.2.1.2.11. Hardware Token;

10.2.1.2.12. OTP enviado por Short Message Service – SMS;

10.2.1.2.13. A solução possui capacidade de permitir criação de políticas para definir quais usuários terão obrigatoriedade de utilização de múltiplo fator de autenticação;

10.2.1.2.14. A solução possui capacidade de permitir criação de políticas baseadas no comportamento do usuário (MFA Adaptativo) para permitir o acesso ou não ao ambiente, pelo menos para os seguintes itens:

10.2.1.2.15. Redes autorizadas;

10.2.1.2.16. Baseado em políticas globais aplicadas ou por aplicações;

10.2.1.2.17. A solução é compatível com os navegadores Microsoft Internet Explorer 11, Microsoft Edge e/ou Google Chrome 75 ou superior, esta por sua vez, também deve ser compatível com navegadores de dispositivos móveis com sistema operacional Android e iOS no mínimo;

10.2.1.2.18. A solução desconecta a interface de administração quando houver período de tempo definido sem atividade;

10.2.1.2.19. A solução permite que os usuários possam optar, a cada autenticação, por acessar estações de trabalho e servidores Microsoft Windows através de uma das formas abaixo:

10.2.1.2.20. Utilizando cartão inteligente com certificado x.509 protegido por senha (PIN), sem a exigência de fator de autenticação adicional da solução;

10.2.1.2.21. Utilizando conta e senha do Active Directory, com a exigência de fator de autenticação adicional da solução.

10.2.1.2.22. A solução utiliza recursos em nuvem, assim como componentes instalados no ambiente on-premises.

10.2.1.2.23. Os componentes on-premises seguem as seguintes especificações:

10.2.1.2.24. Servidores Virtuais para aplicações, software básico:

10.2.1.2.25. Servidores Virtuais ou appliance em ambiente VMware 6.7 ou superior;

10.2.1.2.26. Sistema Operacional Windows 2016 e superior preferencialmente Windows Server 2019 e Windows Server 2022:

10.2.1.2.27. Microsoft IIS 10 e superior;

10.2.1.2.28. Microsoft .NET Framework 4.7 ou superior;

10.2.1.2.29. Sistema Operacional Red Hat Linux versão 7 releases atual e superiores;

10.2.1.2.30. Sistema Operacional Oracle Linux versão 7 releases atual e superiores:

10.2.1.2.31. Sistema Operacional Red Hat Linux versão 8 releases atual e superiores;

10.2.1.2.32. Sistema Operacional Oracle Linux versão 7 releases atual e superiores:

10.2.1.2.33. A solução permite portabilidade de informações, dados, base de conhecimento, nos formatos: CSV, XML, PDF ou outro formato de arquivo estruturado;

10.2.1.2.34. A solução armazena de forma segura as senhas de contas de administradores não sincronizadas com diretório (AD/LDAP);

10.2.1.2.35. A solução é acessível para os administradores da solução, via interface web e não necessitar de complementos, plug-ins ou extensões para seu pleno funcionamento;

10.2.1.3. Controle de acessos

10.2.1.3.1. A solução permite a criação de diferentes perfis de usuários, com diferentes níveis de autorização, permissões e visões, garantindo que as permissões de acesso sejam gerenciadas a partir da interface da solução;

10.2.1.3.2. A solução fornece nativamente suporte à integração Single Sign On - SSO, permitindo a autenticação na interface de administração utilizando recursos de federação, através do uso de Security Assertion Markup Language – SAML. Neste cenário deve ser possível exigir fator adicional de autenticação da solução;

10.2.1.3.3. A solução possui recurso para o provisionamento e desprovisionamento dos usuários, com a integração e sincronização com o serviço de diretório AD e/ou LDAP ou através de chamadas de API;

10.2.1.3.4. A solução permite que somente usuários administradores devam ser capazes de criar, alterar ou remover usuários e suas permissões associadas conforme perfis;

10.2.1.3.5. Para o provisionamento das autorizações de acesso dos usuários na interface de administração da solução, são utilizada ao menos uma das seguintes alternativas:

10.2.1.3.6. Integração com o serviço de diretório AD ou LDAP: a associação de usuários aos grupos de usuários (perfis) é obtida do serviço de diretório AD ou LDAP;

10.2.1.3.7. Uso de API fornecida para que crie ou remova associações de usuários aos perfis;

10.2.1.3.8. A solução suporta múltiplos domínios de Microsoft Active Directory;

10.2.1.3.9. A solução suporta a utilização pelo usuário para autenticação em múltiplos dispositivos, com no mínimo os sistemas operacionais Windows, Android e iOS;

10.2.1.3.10. A solução disponibiliza portal self-service ao usuário para provisionamento do seu dispositivo;

10.2.1.3.11. O portal self-service de autoatendimento (auto-registro) possui no mínimo autenticação com usuário e senha de diretório (AD/LDAP) ou através de integração SAML;

10.2.1.3.12. A solução possibilita o envio de código/QRCode para endereço de e-mail do usuário, sendo obrigatório que seja do domínio designado;

10.2.1.3.13. A solução disponibiliza o conceito de passwordless ao usuário, e funciona com os seguintes métodos:

10.2.1.3.14. Windows Hello;

10.2.1.3.15. FaceID ou TouchID;

10.2.1.3.16. Android Biometris ou Samsung Fingerprint/reconhecimento facial;

10.2.1.3.17. WebAuthn;

10.2.1.3.18. FIDO2

10.2.1.3.19. A solução permite que o usuário possa desprovisionar seu (s) próprio (s) dispositivo (s) ou fornecer API para chamada;

10.2.1.3.20. A solução possibilita que o usuário não consiga remover a exigência do uso do fator adicional da solução;

10.2.1.4. Auditoria

10.2.1.4.1. A solução é capaz de registrar todas as atividades realizadas, tanto de usuários quanto de administradores, gerando log com, no mínimo, as informações de data e hora, usuário, endereço de origem e informações completas das operações;

10.2.1.4.2. A solução registra as falhas e exceções em log com informações suficientes para identificação da falha, com no mínimo as informações de data e hora, usuário, endereço de origem, informações completas das operações e depuração da falha ou exceção;

10.2.1.4.2. A solução mantém o histórico de todas as informações geradas pela solução e que sofreram inclusões, alterações e exclusões por parte dos usuários da solução;

10.2.1.4.3. A solução garante que estes registros estejam protegidos contra alteração e exclusão;

10.2.1.4.4. A solução permite a consulta e exportação das trilhas de auditoria, logs e históricos;

10.2.1.4.5. A solução possibilita que não sejam permitidas conexões oriundas da internet para o ambiente interno;

10.2.1.5. Relatórios

10.2.1.5.1. A solução possui relatório de utilização do múltiplo fator de autenticação;

10.2.1.5.2. A solução permite a geração de relatórios nos formatos HTML, XML, DOCX, PDF ou CSV;

10.3. ITEM 03 – GRUPO 1 E ITEM 02 – GRUPO 2: SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

10.3.1. Para fins de volumetria, considera-se cada unidade deste item igual a 01 (um) dia (8 horas).

10.3.2. Compreende-se nesta etapa a instalação da solução a ser realizada no prazo de até 90 dias consecutivos, contados a partir do primeiro dia útil após a data da última assinatura do Contrato.

10.3.3. No momento anterior da assinatura do termo de recebimento provisório, a Contratada será requisitada para reunião de kick-off do projeto com a finalidade de montar o escopo de trabalho. Este escopo deverá conter as atividades, prazos e responsáveis da execução para acompanhamento da evolução do projeto.

10.3.4. Durante esta etapa, a equipe da Contratada deverá estar disponível nos horários de instalação definidos pela equipe da Contratante.

10.3.5. As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou final de semana.

10.3.6. Para esta etapa a Contratante disponibilizará a infraestrutura de hardware e software necessários e já existentes em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução.

10.3.7. A montagem e instalação de todos os componentes que componham solução adquirida são de responsabilidade da Contratada.

10.3.8. Os componentes de software deverão estar na versão mais atualizada da solução.

10.3.9. A Contratada deverá listar à Contratante todas as informações necessárias para a correta instalação e configuração da solução.

10.3.10. A Contratante deverá providenciar as informações necessárias para a correta instalação da solução.

10.3.11. A Contratada prestará a transferência de conhecimento no formato hands-on para a equipe técnica da instituição na implantação da solução, ao longo das atividades de configuração, bem como durante atividades de suporte e customização.

10.3.12. A Contratada deverá, ao final da implantação, elaborar documentação técnica dos procedimentos realizados durante a implantação.

10.3.13. A Contratante acompanhará e contabilizará a utilização de dias/horas.

10.4. ITEM 04 – GRUPO 1 E ITEM 3 – GRUPO 2: SUPORTE TÉCNICO ESPECIALIZADO

10.4.1. Os serviços de suporte técnico serão prestados vinte quatro (24) horas por dia, sete (7) dias por semana inclusive sábados, domingos e feriados durante dos todos os dias do ano;

10.4.2. Os serviços de suporte técnico serão acionados a partir do registro de indisponibilidade gerado pelo monitoramento (quando for o caso) e/ou por meio de abertura de chamado (ticket) a critério da equipe técnica da CONTRATANTE. Esses chamados serão classificados conforme as severidades especificadas a seguir:

Severidade	Início do atendimento	Término do atendimento	Característica
ALTA	2h	4h	É aplicado quando há indisponibilidade na soluçã qualquer serviço que a compõe; para a configuraç solução; para aplicação de ações de respostas a ou parada ou indisponibilidade da solução.
MÉDIA	4h	8h	É aplicado para solicitações de criação/configur políticas nos demais serviços que compõem a solu quando há problema, simultâneo ou não, nos eleme compõem os serviços/solução, embora ainda esteja disponíveis.
BAIXA	4h	72h	É aplicado para solicitação de configuração, man preventivas, esclarecimentos técnicos relativos aprimoramento do serviço/equipamentos.

10.4.3. Faculta-se a CONTRATADA realizar medidas de contorno temporariamente, mantendo as mesmas funcionalidades e técnicas, quando então, a partir de seu pleno estado de funcionamento, ficará suspensa a contagem do prazo de solução definitiva;

10.4.4. O prazo máximo para a substituição temporária ou medida de contorno será de 30 (trinta) dias;

10.4.5. A CONTRATADA deverá substituir, no prazo máximo de 10 (dez) dias úteis, qualquer appliance, software ou componentes da solução ofertada, que venha a se enquadrar em, pelo menos, um dos seguintes casos:

10.4.5.1. Ocorrência de 3 (três) ou mais chamados técnicos de manutenção corretiva dentro de um período contínuo de 30 (trinta) dias; soma dos tempos de paralisação que ultrapasse 20 (vinte) horas dentro de um período contínuo de 30 (trinta) dias;

10.4.5.2. No caso de inviabilidade da solução definitiva do problema apresentado no equipamento, software, peça e componente, independentemente do enquadramento nos casos previstos no subitem anterior, faculta-se A CONTRATADA promover a sua substituição em caráter definitivo;

10.4.6. A substituição definitiva será admitida com anuência da CONTRATANTE, após prévia avaliação técnica quanto às condições de uso e compatibilidade do equipamento, software, peça e componente ofertado, em relação àquele que está sendo substituído;

10.4.7. Quando da ocorrência de falhas que tornem o serviço/solução indisponível por mais de 30 (trinta) minutos, A CONTRATADA deverá entregar à CONTRATANTE, juntamente com o relatório técnico mensal, a descrição detalhada da ocorrência, suas causas e as ações corretivas realizadas para tornar o serviço/solução novamente disponível.

10.4.8. A CONTRATADA deverá manter registro dos eventos, que porventura tenham provocado interrupções na solução dentro do período do faturamento mensal, de modo a justificar à CONTRATANTE a não consideração de tempos de inoperância, causados por falta de energia elétrica nas dependências da CONTRATANTE, por ações ou solicitações da CONTRATANTE ou ainda por manutenções programadas;

10.4.9. Será considerado o Prazo de Solução Definitiva como o tempo decorrido entre o registro de um chamado e a solução definitiva para efeito dos níveis exigidos;

10.4.10. Os chamados de severidade ALTA poderão ser atendidos on-site, a critério da CONTRATANTE. É vedado a CONTRATADA interromper o atendimento até que o serviço seja efetivamente recolocado em pleno estado de funcionamento, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados. A interrupção do suporte técnico de um chamado desse tipo de severidade por parte da CONTRATADA e que não tenha sido previamente autorizado pela CONTRATANTE, poderá ensejar em aplicação de penalidades previstas;

10.4.11. A CONTRATANTE encaminhará a CONTRATADA, quando da reunião de alinhamento de expectativas, relação nominal de até 5 (cinco) usuários que terão login e senha com perfis de acessos distintos aos serviços que compõem a solução bem como para abrir chamados. Esses perfis serão criados a critério da CONTRATANTE e configurados pela CONTRATADA;

10.4.12. Essa lista poderá ser ajustada durante o período de vigência do contrato a título de adequação às necessidades da CONTRATANTE mediante anuência e aceite da CONTRATADA, sem ônus para a CONTRATANTE;

10.4.13. Pelo não cumprimento do índice mínimo de DISPONIBILIDADE previsto, serão aplicadas as penalidades previstas em contrato.

A aferição dos níveis de serviço referente aos chamados de suporte técnico da solução será realizada por meio do indicador descrito no quadro a seguir:

NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) PARA CHAMADO DE SUPORTE TÉCNICO

CRITICIDADE	TEMPO PARA SOLUÇÃO (TS) DOS CHAMADOS (EM HORAS)	DESCRIÇÃO	PENALIDADES	
Severidade 1	TS ≤ 4	Im problema grave ou degradação que impede a replicação de um ambiente de produção existente. A replicação está inativa. Os negócios não podem ser conduzidos e a produtividade é severamente afetada. Não é possível recuperar ou migrar um aplicativo e nenhuma solução alternativa está disponível. O ambiente de produção é afetado ou indisponível.	Até 4 horas corridas de atraso, **além** do tempo para a solução	Advertência; Havendo recorrência, multa de 0,1% (zero vírgula um por cento) por hora de atraso, calculada sobre o valor da solução.
			Superior a 4 horas e inferior ou igual a 8 horas corridas de atraso, **além** do tempo para a solução.	Multa de 0,2% (zero vírgula dois por cento) por hora de atraso, calculada sobre o valor da solução, sem prejuízo ao item anterior.
			Superior a 8 horas corridas, **além** do tempo para a solução.	Multa de 0,4% (zero vírgula quatro por cento) por hora de atraso, calculada sobre o valor da solução, sem prejuízo ao item anterior, e outras sanções administrativas a critério da CONTRATANTE.
Severidade 2	TS ≤ 8	Uma falha parcial ou degradação em que a solução CONTRATADA não está com força total, mas a replicação está disponível. A produtividade é parcialmente impactada. A recuperação é possível, no entanto, o RPO ou o RTO não está cumprindo o SLA.	Até 4 horas corridas de atraso, **além** do tempo para a solução.	Advertência; Para as demais ocorrências, multa de 0,05% (zero vírgula zero cinco por cento) por hora de atraso,calculada sobre o valor da solução.
			Superior a 6 horas e inferior ou igual a 12 horas corridas de atraso, **além** do tempo para a solução.	Multa de 0,1% (zero vírgula um por cento) por hora de atraso, calculada sobre o valor da solução, sem prejuízo ao item anterior.
			Superior a 12 horas corridas de atraso, **além** do tempo para a solução.	Multa de 0,2% (zero vírgula dois por cento) por hora de atraso, calculada sobre o valor da solução, sem prejuízo ao item anterior, e outras sanções administrativas.

Severidade 3	TS ≤ 96	Um impacto leve e não crítico. Uma condição limitada está ocorrendo, no entanto, ela pode ser facilmente contornada com uma solução alternativa.	Até 4 horas corridas de atraso, **além** do tempo para a solução.	Advertência; Para as demais ocorrências, multa de 0,05% (zero vírgula zero cinco por cento) por hora de atraso,calculada sobre o valor da solução.
			Superior a 4 horas e inferior ou igual a 12 horas corridas de atraso, **além** do tempo para a solução.	Multa de 0,1% (zero vírgula um por cento) por hora de atraso, calculada sobre o valor da solução, sem prejuízo ao item anterior.
			Superior a 12 horas corridas de atraso, além do tempo para a solução.	Multa de 0,2% (zero vírgula dois por cento) por hora de atraso, calculada sobre o valor da solução, sem prejuízo ao item anterior, e outras sanções administrativas.
Severidade 4	TS ≤ 144	consulta sobre a funcionalidade do produto. A funcionalidade da solução não é afetada.	Até 12 horas corridas de atraso, além do tempo para a solução.	Advertência; Para as demais ocorrências, multa de 0,05% (zero vírgula zero cinco por cento) por hora de atraso,calculada sobre o valor da solução.

10.5. ITEM 05 – Grupo 1 e ITEM 4 – Grupo 2: TREINAMENTO

10.5.1. Treinamento da solução fornecida a ser ministrado pela CONTRATADA;

10.5.2. Instrutor deverá possuir certificação, nível expert, da solução entregue;

10.5.3. Carga horária mínima de 20 HORAS

10.5.4. Treinamento a ser realizado para até 08 participantes;

10.5.5. Deverão ser abordados conceitos teóricos e atividades práticas de laboratório;

10.5.6. O treinamento poderá ser realizado de forma remota;

10.5.7. As aulas remotas deverão ser gravadas e disponibilizadas para a equipe da CONTRATANTE.

10.5.8. O idioma das aulas deverá ser em português;

10.5.9. Deverá ser entregue material didático composto de apostila em formato digital ou impresso. O material didático poderá ser em português ou inglês.

10.5.10. Deverão ser abordados, no mínimo, os seguintes tópicos:

10.5.11. Visão geral da solução;

10.5.12. Configurações iniciais;

10.5.13. Instalação, configuração, administração e monitoramento da solução;

10.5.14. Integração com ferramentas e sistemas;

10.5.15. Replicação da solução;

10.5.16. Uso de dispositivos e credenciais;

10.5.17. Configuração de grupos de acesso;

10.5.18. Autenticação e autorização de acesso;

10.5.19. Gravação e monitoramento de sessões;

10.5.20. Alertas, eventos, agendamentos, atualizações e troubleshooting;

10.5.21. Geração de relatórios;

10.5.22. Backup e recuperação da solução;

10.6. Requisitos legais

2.1.1. A Resolução CNJ 396/2021, que estabelece a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-JUD), em seu capítulo 8, artigo 29, que trata sobre gestão de usuários elabora as seguintes determinações:

• “Art. 29. Cada órgão do Poder Judiciário, com exceção do STF, deverá implementar a gestão de usuários de sistemas informatizados composta de:

I – gerenciamento de identidades;

II – gerenciamento de acessos; e

III – gerenciamento de privilégios.

Parágrafo único. A gestão de usuários será disciplinada por ato do Presidente do CNJ, que definirá o padrão a ser adotado para utilização de credenciais de login único e interface de interação dos sistemas, com o objetivo de uniformizar e garantir a experiência única de interação com os sistemas judiciais.”

2.1.2. Preservação da integridade e da confidencialidade dos dados dos usuários, sejam eles internos ou externos para conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

2.1.3. Adequação às diretrizes constantes na Recomendação 02/2023 do CTIR Gov.

2.1.4. Adequação às diretrizes constantes na Resolução nº 298, de 04 de agosto de 2021, do Superior Tribunal Militar.

10.7. Requisitos de manutenção

10.7.1. O suporte técnico deve iniciar logo após a assinatura do termo de aceite dos serviços de instalação e configuração e deverá ser realizado de forma contínua, e obrigatoriamente, pelo fabricante da ferramenta ou empresa prestadora de serviços devidamente credenciada;

10.7.2. Direito de atualização de software e pacotes de correção;

10.7.3. Direito de upgrade do produto para a última versão estável;

10.8. Requisitos Temporais

10.8.1. Cronograma de execução

10.8.1.1. O prazo máximo de entrega, instalação e implantação do objeto licitado será de 60 (sessenta) dias corridos, contados a partir da data de assinatura do Contrato;

10.8.1.2. Os serviços de instalação deverão ser executados por, pelo menos, 1 (um) técnico certificado pelo fabricante da solução;

10.8.1.3. A Contratada deverá apresentar o(s) produto(s) conforme padrão do fabricante, fazendo constar a identificação do(s) produto(s) e demais informações exigidas na legislação em vigor.

10.9. Requisitos Sociais, ambientais e culturais

10.9.1. A CONTRATADA deve comprovar cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei Federal n° 8.213/1991;

10.9.2. Com fundamento no o artigo 3º, § 2º, da Lei Federal nº 8.666/1993, havendo eventual empate entre propostas, ou entre propostas e lances, o critério de desempate será aquele previsto no artigo 3º, § 2º, da Lei Federal nº 8.666/1993, assegurando-se a preferência, sucessivamente, aos bens e serviços:

a. Produzidos no País;

b. Produzidos ou prestados por empresas brasileiras;

c. Produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia do País;

d. Produzidos ou prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

10.10 Requisitos de implantação

10.10.1. A instalação deverá ser nas dependências do STM.

10.11. Requisitos de garantia

10.11.1. O serviço de suporte envolverá todas as atividades necessárias para garantir a operação contínua do produto. Desta forma, farão parte do escopo das atividades de suporte:

a) Resolução de dúvidas e esclarecimentos relativos à utilização e configuração das funcionalidades;

b) Resolução de problemas que limitem ou impeçam o desenvolvimento e/ou execução de aplicações que façam uso efetivo das funcionalidades;

10.11.2. A CONTRATADA deverá disponibilizar canais de acesso 24 horas por dia, 7 dias por semana, através de número de telefone de discagem gratuita (0800) e/ou Internet, para abertura de chamados técnicos objetivando a resolução de problemas e dúvidas quanto ao funcionamento do produto. Todos os chamados, independente de sua criticidade, deverão ser abertos em um único número telefônico.

10.12. Requisitos de segurança da informação

10.12.1. O fornecedor deverá cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do STM.

10.12.2. Deverá, ainda, manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de que tomar conhecimento em razão da execução do objeto deste processo de contratação, respeitando todos os critérios de sigilo, segurança e inviolabilidade, aplicáveis aos dados, informações, regras de negócio, documentos, entre outros.

10.12.3. As informações a serem tratadas de forma sigilosa, restrita e confidencial são aquelas que, por sua natureza, são consideradas como de interesse restrito ou confidencial, e não podem ser de conhecimento de terceiros, como por exemplo:

10.12.3.1. Dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, não podendo, sob qualquer pretexto serem divulgadas, reproduzidas ou utilizadas por terceiros sob pena de lei, independentemente da classificação de sigilo conferida pelo STM a tais documentos;

10.12.3.2. Resultados, parciais ou totais, sobre produtos gerados;

10.12.3.3. Programas de computador, seus códigos-fonte e códigos-objeto, bem como suas listagens e documentações;

10.12.3.4. Toda a informação relacionada a programas de computador existentes ou em fase de desenvolvimento no âmbito do STM e rotinas desenvolvidas por terceiros, incluindo fluxogramas, estatísticas, especificações, avaliações, resultado de testes, arquivo de dados, versões “beta” de quaisquer programas, dentre outros;

10.12.3.5. Documentos relativos à lista de usuários do STM e seus respectivos dados, armazenados sob qualquer forma;

10.12.3.6. Metodologias e ferramentas de serviços, desenvolvidas pelo STM;

10.12.3.7. Parte ou totalidade dos modelos de dados que subsidiam os sistemas de informações do STM, sejam eles executados interna ou externamente;

10.12.3.8. . Parte ou totalidade dos dados ou informações armazenadas nas bases de dados que subsidiam os sistemas de informações do STM, sejam elas residentes interna ou externamente;

10.12.3.9. Circulares e comunicações internas do STM;

10.12.3.10. Quaisquer processos ou documentos classificados como RESTRITO ou CONFIDENCIAL pelo STM.

10.13. Da aderência à Lei nº 13.709/2018

10.13.1. As partes se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, nos termos da Lei Geral de Proteção de Dados - LGPD (Lei n. 13.709, de 14 de agosto de 2018).

10.13.2. É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

10.13.3. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do instrumento contratual.

10.13.4. Os dados pessoais tornados públicos por este contrato deverão ser resguardados pelas partes, observados os princípios de proteção de dados previstos no art. 6º da Lei n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados).

10.13.5. A CONTRATADA fica obrigada a comunicar ao CONTRATANTE em até 24 (vinte e quatro) horas qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da Lei Geral de Proteção de Dados.

10.13.6. Durante toda a execução do objeto licitado, o tratamento de dados pessoais deverá se limitar ao mínimo necessário para a execução do objeto, sendo observados:

a) a compatibilidade com a finalidade especificada;

b) o interesse público; e

c) a regra de competência administrativa aplicável à situação concreta.

10.13.7. Os dados devem ser eliminados, quando não autorizada sua conservação, nos termos do art. 16 da LGPD, após o término de seu tratamento nas hipóteses previstas no art. 15 da referida lei.

10.13.8. A CONTRATADA deverá promover a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do CONTRATANTE em caso de desligamento de funcionário das atividades inerentes à execução do presente Contrato.

10.13.9. A CONTRATADA não poderá disponibilizar ou transmitir a terceiros, sem prévia autorização por escrito, informação, dados pessoais ou base de dados a que tenha acesso em razão do cumprimento do objeto contratual.

10.13.10. Encerrada a vigência do contrato ou após a satisfação da finalidade pretendida, a CONTRATADA interromperá o tratamento dos dados pessoais disponibilizados pelo CONTRATANTE e, em no máximo trinta dias, sob instruções e na medida do determinado por este, eliminará completamente os Dados Pessoais e todas as cópias porventura existentes (seja em formato digital ou físico), salvo quando a CONTRATADA tenha que manter os dados para cumprimento de obrigação legal.

10.13.11. A CONTRATADA ficará obrigada a assumir total responsabilidade pelos danos patrimoniais, morais, individuais ou coletivos que venham a ser causados em razão do descumprimento de suas obrigações legais no processo de tratamento dos dados compartilhados pelo CONTRATANTE.

10.13.12. Eventuais responsabilidades serão apuradas de acordo com o que dispõe a Seção III, Capítulo VI da LGPD.

11. CERTIFICAÇÕES E COMPATIBILIDADES

11.1. A qualificação técnica será comprovada, por meio do seguinte documento:

11.2. Declaração do fabricante ou da própria licitante informando ser revenda autorizada do Fabricante; que deverá ser encaminhada junto à Proposta da licitante

11.3. Atestado de capacidade técnica comprovando que a licitante forneceu serviços compatíveis com o objeto solicitado;

11.4. Entende-se como atividades compatíveis, para efeito de qualificação técnica, a comprovação de que a licitante implantou o mesmo software ofertado em empresa com, no mínimo, 100 (cem) usuários;

11.5. As declarações/atestados apresentados pela própria licitante devem ser emitidas em papel timbrado com nome completo da empresa, endereço, CNPJ, bem como a assinatura do responsável técnico ou legal da empresa;

11.6. Nessas declarações/atestados, a licitante deverá declarar estar de acordo com as normas e solicitações do edital e ciente que a declaração incompleta, falsa, dúbia ou em desacordo com o especificado neste termo de referência, implica na sua automática desclassificação do certame, sem prejuízo de demais sanções legais.

12. ENTREGA DA SOLUÇÃO

12.1. O prazo máximo de entrega, instalação e implantação do objeto licitado será de 60 (sessenta) dias corridos, contados a partir da data de assinatura do Contrato;

13. LOCAL DE INSTALAÇÃO

13.1. A instalação da solução dos grupos 1 e 2 deverá ser feita na sede do Superior Tribunal Militar - Setor de Autarquias Sul, Praça dos Tribunais Superiores - Cep.: 70.098-900 - Brasília - DF

14. OBRIGAÇÕES DA CONTRATADA

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

14.2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

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

14.4. Apresentar os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso.

14.5. Apresentar à CONTRATANTE, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço.

14.6. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade à CONTRATANTE.

14.7. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração.

14.8. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a CONTRATADA relatar à CONTRATANTE toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função.

14.9. Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.

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

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

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

14.13. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

14.14. Assegurar à Contratante:

14.14.1. O direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente, permitindo à CONTRATANTE distribuir, alterar e utilizar estes sem limitações; e

14.14.2. Os direitos autorais da solução, do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua utilização sem que exista autorização expressa da CONTRATANTE, sob pena de multa, sem prejuízo das sanções civis e penais cabíveis.

14.15. Deter instalações, aparelhamento e pessoal técnico adequado, disponíveis para a realização do objeto da licitação.

15. CONTRATANTE

15.1. Designar gestor que efetuará sua representação perante a CONTRATADA para determinação, avaliação, acompanhamento e aprovação dos serviços por ela realizados;

15.2. Prestar os esclarecimentos que venham a ser solicitados pela CONTRATADA, no que diz respeito ao contrato;

15.3. Proporcionar à contratada todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal nº 8.666/1993 e suas alterações posteriores.

15.4. Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.

15.5. Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.

15.6. Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste Termo.

15.7. Aplicar as penalidades previstas em lei e neste instrumento.

16. SIGILO DAS INFORMAÇÕES

16.1. A CONTRATADA obriga-se, durante o curso do Contrato e após o seu término, ao mais completo e absoluto sigilo com relação a toda informação de qualquer natureza referente às atividades do CONTRATANTE, das quais venha a ter conhecimento ou venha a ter acesso por força do cumprimento do presente Contrato, não podendo sob qualquer pretexto, utilizá-las para si, invocar, revelar, reproduzir ou delas dar conhecimento a terceiros, responsabilizando-se em caso de descumprimento da obrigação assumida por eventuais perdas e danos e sujeitando-se às cominações legais, nos termos da Lei 4.595 de 31.12.1964 e demais leis correlatas;

16.2. “Informações Confidenciais" significam os dados ou informações confidenciais desenvolvidas ou adquiridas pelo CONTRATANTE ou pela Licitante vencedora e cuja divulgação ou utilização não autorizada, por qualquer das partes, poderá ser prejudicial a um ou a outro;

16.3. O CONTRATANTE e a Licitante vencedora tratarão sigilosamente todas as informações confidenciais, produtos e materiais que as contenham, não podendo ser copiados ou reproduzidos, publicados, divulgados ou de outra forma colocados à disposição, direta ou indiretamente, de qualquer pessoa, a não ser empregados e agentes do CONTRATANTE e/ou da Licitante vencedora que deles necessitem para desempenhar as suas funções no CONTRATANTE, sem que para tanto seja devido o consentimento prévio do CONTRATANTE ou

comunicado da empresa vencedora;

16.4. As partes se obrigam a instruir sua equipe e prepostos a respeito das presentes disposições, as quais deverão ser observadas mesmo após o término ou cancelamento do futuro CONTRATO.

17. DIREITOS DE PROPRIEDADE, MARCAS, PATENTES E DIREITOS AUTORAIS

17.1. Quaisquer reproduções ou cópias de produtos e/ou bens e direitos cujos direitos de propriedade, marcas, patentes ou direitos autorais estiverem sob a responsabilidade da LICITANTE vencedora resultantes dos Serviços, incluindo documentação a eles correlata, em qualquer idioma, que forem desenvolvidos especificamente pela Licitante vencedora (para o CLIENTE) sob os dispositivos do futuro CONTRATO são de propriedade exclusiva do CONTRATANTE e deverão: (I) ser claramente designados como confidenciais, (II) incluir todas as marcas e indicações que façam referência ao proprietário, conforme apropriado, e (III) ter o mesmo grau de confidencialidade, proteção e legitimidade do original.

18. DA FISCALIZAÇÃO E ACOMPANHAMENTO

18.1. O acompanhamento e a fiscalização do contrato caberão à Equipe de Gestão do Contrato, que será instituída pelo Diretor-Geral, após a assinatura das partes;

18.2. No momento da assinatura do Contrato, a Contratada indicará um preposto para representá-la, sendo este responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao Contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual;

18.3. Assinado o contrato, o Diretor-Geral do Contratante instituirá a Equipe de Gestão da Contratação, composta por:

18.3.1. Gestor do Contrato: servidor com atribuições gerenciais, técnicas ou operacionais, relacionadas ao processo de gestão do contrato, para coordenar, supervisionar e controlar a execução do contrato, a fim de garantir o atendimento dos objetivos do Contratante;

18.3.2. Fiscal Demandante do Contrato: servidor representante da Diretoria de Tecnologia da Informação, competente para fiscalizar o contrato quanto aos aspectos funcionais da solução;

18.3.3. Fiscal Técnico do Contrato: servidor representante da Área da Diretoria de Tecnologia da Informação, competente para fiscalizar o contrato quanto aos aspectos técnicos da solução;

18.3.4. Fiscal Administrativo do Contrato, servidor representante da Área Administrativa, competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

18.4. A existência e a atuação da fiscalização pelo Contratante em nada restringe a responsabilidade, única, integral e exclusiva da Contratada, no que concerne à execução do contrato.

19. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

19.1. A Equipe de Planejamento desta contratação é composta pelos servidores Wilson Marques de Souza Filho (Integrante Demandante), Márcio Coelho Marques (Integrante Técnico) e Luiz Gustavo Costa Reis (Integrante Administrativo).

19.2. A indicação do Integrante Administrativo consta do Documento de Oficialização da Demanda – DOD, de acordo com o inc. III, do § 5º, do art. 12, da Resolução nº 182, de 17 de outubro de 2013, do Conselho Nacional de Justiça.

19.3. A Equipe de Planejamento da Contratação foi instituída pelo Senhor Diretor-Geral, em conformidade com o inc. IV, do § 7º, do art. 12, da mesma Resolução.

20. EQUIPE DE APOIO À CONTRATAÇÃO

A Equipe de Apoio à Contratação é composta pelos integrantes da Equipe de Planejamento da Contratação e tem como finalidade subsidiar a Área de Licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes (redação dada pelo inc. XI, do art. 2º, da Resolução nº

182/13, do CNJ).

21. VIGÊNCIA DO CONTRATO

21.1. A vigência contratual referente aos grupo 1 (itens 1, 2 e 3) e grupo 2 (itens 1 e 2) será de 90 dias.

21.2. A vigência do contrato referente ao item 4 do grupo 1 e item 3 do grupo 2 será de 60 meses e deve iniciar logo após a assinatura do termo de aceite dos serviços de instalação e configuração e deverá ser realizado de forma contínua, e obrigatoriamente, pelo fabricante da ferramenta ou empresa prestadora de serviços devidamente credenciada;

21.3. A vigência contratual para o item 5 do grupo 1 e item 4 do grupo 2 será de 12 meses, a contar de sua assinatura.

22. PAGAMENTO

22.1. O pagamento referente aos itens 1, 2, 3 e 5 do grupo 1 será efetuado em parcela única, após o termo de aceite definitivo.

22.2. O pagamento referente aos itens 1, 2 e 4 do grupo 2 será efetuado em parcela única, após o termo de aceite definitivo.

22.3. O pagamento referente aos item 4 do grupo 1 e item 3 do grupo 2 será efetuado em parcelas mensais.

22.4. Para efeitos de pagamento, a CONTRATADA deverá apresentar documento de cobrança constando, de forma discriminada a efetiva realização do objeto adquirido, informando o nome e numero do banco, a agência e o número da conta corrente em que o crédito deverá ser efetuado.

22.5. Deverá apresentar juntamente com o documento de cobrança a comprovação de que cumpriu as seguintes exigências, cumulativamente:

22.5.1. Certidão de regularidade com a Seguridade Social;

22.5.2. Certidão de regularidade com o FGTS;

22.5.3. Certidão de regularidade com a Fazenda Federal;

22.5.4. Certidão Negativa de Débitos Trabalhistas;

22.5.5. Certidão de regularidade com a Fazenda Estadual e Municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da Lei.

22.6. Os documentos de cobrança deverão ser enviados via peticionamento eletrônico.

Caso o objeto contratado seja faturado em desacordo com as disposições previstas no Edital e neste Termo de Referência ou sem a observância das formalidades legais pertinentes, a CONTRATADA deverá emitir e apresentar novo documento de cobrança, não configurando atraso no pagamento.

22.7. Após o atesto do documento de cobrança, que deverá ocorrer no prazo de até 05 (cinco) dias úteis contado do seu recebimento, o responsável deverá encaminhá-lo para pagamento.

22.8. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido de Alguma forma para o fato, a atualização financeira devida, entre a data que deveria ser efetuado o pagamento e a data correspondente ao efetivo pagamento, será calculada da seguinte forma, devendo a atualização prevista nesta condição ser incluída em nota fiscal a ser apresentada posteriormente:

AF = I x N x VP , onde:

AF = atualização financeira devida;

I = 0,0001644 (índice de atualização dia);

N = número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = valor do pagamento devido.

23. DO REAJUSTE DE PREÇOS

23.1. Para o grupo 1 (itens 1, 2, 3 e 5) e grupo 2 (itens 1, 2 e 4) os valores são fixos e irreajustáveis.

23.2. Para os itens 04 (grupo 1) e 03 (grupo 2), poderá haver reajuste anual de preços para as parcelas do contrato, de acordo com o Índice de Custo da Tecnologia da

Informação (ICTI), do Instituto de Pesquisa Econômica Aplicada (IPEA), ou outro índice que venha a ser adotado pelo Governo Federal, em substituição àquele, observado o interregno mínimo de um ano a partir da data da proposta:

22.1.1. o pedido de reajuste de preços deverá ocorrer antes da assinatura do termo de prorrogação contratual, sob pena de preclusão.

23.3. Para efeito de cálculo dos reajustes será utilizada a seguinte fórmula:

$$R = V \frac{I - IO}{IO}, \text{ onde:}$$

R = valor do reajustamento procurado;

V = valor contratual do serviço;

I = valor do índice relativo ao mês do reajuste, conforme definido no contrato;

IO = valor do índice inicial, correspondente ao mês da apresentação da proposta.

23.4. Por ocasião do pedido de reajuste, caberá à Contratada apresentar planilha dos cálculos, de acordo com fórmula do item 22.2.

23.5. Caberá à Contratada, por ocasião do reajustamento de preços, apresentar faturas distintas, sendo uma correspondente aos preços iniciais contratados e outra, suplementar, relativa ao valor do reajustamento devido e pactuado pelas partes.

23.6. Ocorrendo o primeiro reajuste, os subsequentes só poderão ocorrer obedecendo ao prazo mínimo de um ano, a contar do início dos efeitos do último reajuste.

23.7. O reajuste de que trata o Item 23.2 poderá sofrer alteração posterior, total ou parcial, decorrente da adoção, pelo Governo Federal, de medidas ou normas financeiras com força de lei.

24. RESCISÃO CONTRATUAL

24.1. A inexecução total ou parcial do contrato enseja a sua rescisão, conforme disposto nos arts. 77 a 80 da Lei no 8.666/93:

24.1.1. Os casos de rescisão contratual deverão ser formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

24.2. A rescisão do contrato poderá ser:

24.2.1. Determinada por ato unilateral e escrito do Contratante, nos casos enumerados nos incisos I a XII, XVII e XVIII, do art. 78 da Lei nº 8.666/93;

24.2.2. Amigável, por acordo entre as partes, desde que haja conveniência para o Contratante;

24.2.3. Judicial, nos termos da legislação vigente sobre a matéria.

24.3. A rescisão administrativa ou amigável será precedida de autorização escrita e fundamentada da autoridade competente.

25. DESPESA ORÇAMENTÁRIA

25.1. A despesa ocorrerá à conta de dotação consignada à Justiça Militar da União pela Lei Orçamentária para o exercício de 2023, por meio dos seguintes Encargos do Plano de Ação (Código e Identificação) e emissão de respectivas Notas de Empenho:

25.1.1. As despesas decorrentes da presente contratação serão provenientes do Programa de Trabalho: SEG0; Elemento de Despesa 3.3.90.40

26. ACRÉSCIMO OU SUPRESSÃO DO OBJETO

26.1. A critério da Administração, o objeto desta licitação poderá ser acrescido ou suprimido em até 25% do valor inicial contratado atualizado, observado o disposto no art. 65, §§ 1º e 2º, da Lei nº 8.666/93.

26.2. O acréscimo ou supressão contratual não poderá exceder os limites estabelecidos no § 1º do art. 65 da Lei nº 8.666/93, salvo a supressão decorrente de acordo celebrado entre as partes.

27. CONSIDERAÇÕES GERAIS

27.1. A equipe técnica envolvida na prestação dos serviços deverá possuir conhecimento e experiência conforme os requisitos técnicos para a prestação dos serviços descritos neste Termo de Referência;

27.2. A CONTRATADA, às suas expensas, deverá disponibilizar um profissional destacado para a gestão do relacionamento com a CONTRATANTE, o qual, além de possuir conhecimentos e capacidade profissionais necessários, deverá ter competência para resolver imediatamente todo e qualquer assunto relacionado com os serviços contratados;

27.3. A ausência ou omissão da fiscalização do CONTRATANTE não eximirá a CONTRATADA das responsabilidades oriundas deste contrato;

27.4. Todos os softwares e recursos computacionais utilizados pela CONTRATADA, necessários para o atendimento do objeto do contrato, deverão ser devidamente legalizados, em conformidade com as leis de Software (nº 9.609/98) e do Direito Autoral (nº 9.610/98);

27.5. Caso haja a necessidade de alocar equipamentos de informática nas dependências do CONTRATANTE, de propriedade da CONTRATADA, como computadores, switches, hubs, roteadores e impressoras, estes, obrigatoriamente, antes de conectar-se com a rede corporativa, deverão estar de acordo com a Política de Segurança da CONTRATANTE.

27.6. Caso haja necessidade de acessos remotos, por parte dos funcionários da CONTRATADA, o CONTRATANTE deverá ser informado, por escrito, da necessidade de utilização do referido meio e a CONTRATADA deverá ratificar que está de acordo com a Política de Segurança da Informação e o Termo de Confidencialidade, respectivamente;

28. SANÇÕES ADMINISTRATIVAS

28.1. Com fundamento no art. 7º da Lei n. 10.520/2002 e nos artigos 86 e 87 da Lei n. 8.666/1993, a CONTRATADA ficará sujeita, assegurada prévia e ampla defesa, às seguintes penalidades:

a) advertência;

b) multa nas condições e percentuais estabelecidos no Termo de Referência;

c) suspensão temporária de participação em licitação e impedimento de contratar com o STM, por prazo não superior a 2 (dois) anos;

d) impedimento de licitar e contratar com a União e descredenciamento do SICAF, pelo prazo de até 5 (cinco) anos;

e) declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada com base na alínea “c” dessa cláusula.

28.2. As sanções previstas nas alíneas "a", "c" e “e” do caput desta cláusula poderão ser aplicadas, cumulativamente ou não, à pena de multa.

28.3. A penalidade prevista na alínea "d" desta cláusula também poderá ser aplicada à CONTRATADA, caso tenha sofrido condenação definitiva por fraudar recolhimento de tributos, praticar ato ilícito visando frustrar os objetivos da licitação ou demonstrar não possuir idoneidade para contratar com a Administração.

28.4. Excepcionalmente, desde que devidamente justificado no processo administrativo, o CONTRATANTE poderá efetuar a retenção do valor presumido da multa, e, concomitantemente, instaurar regular processo administrativo oportunizando à CONTRATADA o exercício do contraditório e da ampla defesa.

28.5. As penalidades serão obrigatoriamente registradas no SICAF, e sua aplicação deverá ser precedida da concessão da oportunidade de ampla defesa para CONTRATADA, na forma da lei.

28.6. Os instrumentos de requerimentos, de defesas prévias e de recursos eventualmente interpostos pela CONTRATADA deverão ser instruídos com os documentos hábeis à prova das alegações neles contidas.

28.6.1. Referidos documentos probatórios deverão ser apresentados em suas versões originais e/ou em versões autenticadas, por cartórios extrajudiciais ou por servidores da Administração Pública, sob pena de, a critério exclusivo do CONTRATANTE, não serem avaliados.

29. FUNDAMENTO LEGAL

A elaboração deste Termo de Referência fundamenta-se no disposto na Lei nº 10.520, de 17 de julho de 2002, nos Decretos nº 10.024, de 20 de setembro de 2019, na Resolução nº 182, de 17 de outubro de 2013, do Conselho Nacional de Justiça, e, subsidiariamente, na Lei nº 8.666, de 21 de junho de 1993.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO		
Em cumprimento ao exposto no § 1º do art. 13 da Resolução nº 182, de 17 de outubro de 2013, do Conselho Nacional de Justiça, a Equipe de Planejamento da Contratação submete os Estudos Preliminares e o Termo de Referência à aprovação do Diretor de Tecnologia da Informação, titular da Área Demandante.		
INTEGRANTE TÉCNICO	**INTEGRANTE DEMANDANTE**	**INTEGRANTE ADMINISTRATIVO**
Márcio Coelho Marques	**Wilson Marques de Souza Filho**	**Luiz Gustavo Costa Reis**
VALIDAÇÃO DO TERMO DE REFERÊNCIA		
Autoridade da Área Demandante - Ianne Carvalho Barros - Diretor da DITIN		

Documento assinado eletronicamente por **WILSON MARQUES DE SOUZA FILHO**, **COORDENADOR DE TECNOLOGIA**, em 16/08/2023, às 16:12 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARCIO COELHO MARQUES**, **ANALISTA JUDICIÁRIA - Apoio Especializado - Análise de Sistemas**, em 16/08/2023, às 16:38 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUIS GUSTAVO COSTA REIS**, **INTEGRANTE ADMINISTRATIVO**, em 16/08/2023, às 17:38 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **IANNE CARVALHO BARROS**, **DIRETOR DE TECNOLOGIA DA INFORMAÇÃO**, em 16/08/2023, às 18:14 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.stm.jus.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **3336750** e o código CRC **65E6B848**.