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

ESTUDO TÉCNICO PRELIMINAR

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1. OBJETO

Contratação de solução de segurança para gerenciamento de identidades e acesso, incluindo suporte técnico e atualização tecnológica do fabricante.

2. DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS

2.1. Identificação das necessidades de negócio

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.

2.2 Requisitos de negócio

2.2.1. Objetivo Geral:

Atender às demandas registradas nos Planos Anuais de Contratações (PAC) relacionadas à contratação de solução de segurança.

Viabilizar a segurança e controle das identidades e seus acessos relacionados aos sistemas e soluções de TIC.

Assegurar a proteção de dados armazenados e trafegados em soluções e sistemas governamentais

Minimizar riscos de segurança da informação decorrentes de vulnerabilidades em Sistemas Operacionais

2.2.2. Objetivos Específicos:

Prover mecanismos de segurança da informação

Abranger todos os tipos de acessos e identidades

Assegurar mecanismos de gerenciamento de privilégios elevados

Prover registros de uso de privilégios e trilhas de auditoria

Ganhar agilidade e eficiência no tratamento de incidentes e na criação de relatórios

Prover políticas para acessos adaptativos baseados em riscos e contextos conhecidos de uma autenticação

Prover múltiplo fator de autenticação para diversos casos de uso com capacidade de interpretação de risco adaptativo

Prover capacidade de acesso remoto a infraestrutura privilegiada e aplicações web de negócio sem VPN

Prover ganhos operacionais para recuperação de acessos e senhas

Gravação e proteção de sessões de aplicações do tipo web de negócio de forma não intrusiva.

Possuir a capacidade de disparar gatilhos de gravação em vídeo relacionado a ações do usuário na estação de trabalho que estejam cumprindo atividades críticas

Proteger identidades, credenciais e acessos de forma fim-a-fim

Deve se comunicar com outras ferramentas de segurança e ampla capacidade de integrações

Prover múltiplo fator de autenticação

2.3 Requisitos de Nível de Serviço (Suporte Técnico)

2.3.1. 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;

2.3.2. 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 CONTRATADA.. 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 solução ou em qualquer serviço que a compõe; para a configuração da solução; para aplicação de ações de respostas a incidentes ou parada ou indisponibilidade da solução.
MÉDIA	4h	8h	É aplicado para solicitações de criação/configuração de políticas nos demais serviços que compõem a solução; quando há problema, simultâneo ou não, nos elementos que compõem os serviços/solução, embora ainda estejam disponíveis.
BAIXA	4h	72h	É aplicado para solicitação de configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço/equipamentos.

2.3.3. 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;

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

2.3.5. 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:

2.3.6. 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;

2.3.7. 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;

2.3.8. 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;

2.3.9. 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.

2.3.10. 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;

2.3.11. 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;

2.3.12. 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;

2.3.13. 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;

2.3.14. 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;

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

2.6. Requisitos legais

Lei 8.666; Resolução CNJ 182/2013; Resolução CNJ 396/2021; Recomendação 02/2023 do CTIR Gov; Resolução nº 298, de 04 de agosto de 2021, do Superior Tribunal Militar.

2.7. Requisitos de manutenção

Não há

2.8. Requisitos Temporais

2.8.1. Cronograma de execução

2.8.1.1. 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;

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

2.8.1.3. 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.

2.9. Requisitos Sociais, ambientais e culturais

2.9.1. 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;

2.9.2. 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.

2.10. Requisitos de arquitetura tecnológica

GRUPO 1

2.10.1. A contratação pretendida, qual seja contratação de solução de “Gestão de

Credenciais Privilegiadas” tem como premissa principal prover os sistemas, aplicações e bancos de dados da JMU de maior segurança contra acessos indevidos, proporcionando proteção e armazenamento de senhas, controle, gerenciamento, monitoramento e auditoria de acesso a ativos, inclusive com rastreabilidade, via documentação de toda e qualquer intervenção.

2.10.2. Resumidamente, funciona da seguinte forma:

A “Gestão de Credenciais Privilegiadas” evita o compartilhamento de senhas de acessos privilegiados, provendo rastreabilidade e identificação de ocorrências nos sistemas, aplicações e bancos de dados, pois possuiu etapas tais como solicitação e aprovação, para então, em caso positivo, obtenção da senha requerida.

Além disso, provê a possibilidade de acompanhamento, em tempo real, de acessos, sendo possível a interrupção ou cancelamento deste, pelo responsável do gerenciamento de acessos privilegiados, em caso de desvio.

Os principais requisitos da demanda são:

● Solução de Gerenciamento de Acessos Privilegiados (PAM), com instalação e configuração;

Prover gestão e auditoria de acessos privilegiados por meio de credenciais privilegiadas para pelo menos 250 (duzentos e cinquenta) usuários, garantindo ao menos 250 acessos simultâneos com todas as funcionalidades habilitadas, inclusive a gravação de sessão, podendo dois ou mais usuários acessar a mesma credencial, sem comprometimento da performance ou rastreabilidade;

● Centralizar a visibilidade e controle de privilégio por meio de uma plataforma única de gerenciamento;

● Ser um repositório único das credenciais administrativas em todos os sistemas e ambientes da organização, resultando em redução de tempo de auditoria e investigações de incidentes.

● Possuir integração com o Active Directory desta JMU para delegação de acesso aos servidores gerenciados

GRUPO 2

2.10.3. A solução de autenticação de múltiplos fatores (MFA) é composta de diversos softwares e serviços, que possuem requisitos funcionais tecnológicos individualizados. A seguir estão listados os requisitos funcionais principais que definem a solução. As especificações técnicas mais detalhadas constarão no Termo de Referência.

2.10.4. Assinatura de serviço de autenticação por múltiplos fatores com conectores de integração com as soluções a seguir, permitindo ilimitadas integrações através desses conectores:

- VPN Cisco AnyConnect, Fortinet FortiVPN/FortiClient, Check Point VPN, Palo Alto VPN em estações de trabalho e dispositivos móveis com sistema operacional Android, iOS e Windows;
- Virtual Desktop Infrastructure – VDI, da VMware (Horizon 7);
- Microsoft Remote Desktop Protocol;
- Estações de trabalho Microsoft Windows 10 e superiores;
- Servidores Windows 2012 R2 e superiores;
- Secure Shell Linux/Unix;
- Security Assertion Markup Language – SAML;
- Active Directory Federation Services – ADFS;
- RADIUS;

Deve prover ao menos os seguintes fatores de autenticação:

- Push Notification (Notificação enviada para app instalado no dispositivo do usuário);
- Software Token – OTP (One Time Password);
- Hardware Token;
- OTP enviado por e-mail;
- OTP enviado por Short Message Service – SMS;
- Deve possuir integração ao cofre de senhas
- Deve possuir relatório de utilização do múltiplo fator de autenticação.
- Deve permitir uso de Hardware Token vou licompatíveis com o padrão OATH HOTP, WebAuth e FIDO2. A interface do token deverá ser USB ou USB-C.
- Deve comprovar uso de datacenter no Brasil, em caso de serviço em nuvem total ou parcial;
- A solução deve adotar token como segundo fator totalmente off-line.

2.12. Requisitos de garantia

O serviço de suporte deverá prestado continuamente por 60 meses. Nesse período, podem-se solicitar ajustes na configuração, atualizações e bibliotecas de conhecimento.

2.13. Requisitos de metodologia de trabalho

A metodologia de trabalho é a usual do Tribunal, adotada pelas equipes de Infraestrutura Tecnológica.

2.14. Requisitos de segurança da informação

2.14.1. 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.

2.14.2. 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.

2.14.3. 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:

2.14.3.1. 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;

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

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

2.14.3.4. 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;

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

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

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

2.14.3.8. . 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;

2.14.3.9. Circulares e comunicações internas do STM;

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

3. SOLUÇÕES DISPONÍVEIS NO MERCADO

3.1. Solução de PAM

3.1.1. Como solução mercadológica que venha a atender as necessidades deste Tribunal não se vislumbra outra que não seja a Contratação de empresa especializada no fornecimento de solução de gerenciamento de acessos privilegiados (PAM – Privileged Access Management), com diversas funcionalidades tais como análise comportamental, auditoria de credenciais, mitigações contra roubos e abusos de privilégios e aplicação do “privilégio mínimo” nos ativos protegidos, tudo isso com a finalidade de aumentar a proteção das credenciais utilizadas no âmbito do Tribunal e impedir que essas credenciais sejam usadas por agentes potenciais atacantes, prevenindo danos decorrentes de ataques cibernéticos que possam ser realizadas conta o tribunal. Cumpre destacar que, atualmente, o STM não possui ferramenta específica de proteção supramencionada e, conforme detalhamento do potencial da solução, busca a contratação da plataforma que apresentar melhor custo-benefício, em qualidade e preço a ser pago.

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

Figure 1: Magic Quadrant for Privileged Access Management

Source: Gartner (July 2022)

3.2. Solução MFA

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

Figure 1: Magic Quadrant for Access Management

Source: Gartner (November 2022)

3.3. O Gartner realiza a mensuração da qualidade e relevância de soluções de TI através de um gráfico que ficou conhecido como “Quadrante”, o qual reflete os estudos publicados anualmente sobre categorias de produtos e serviços, cuja composição utiliza diversos critérios para medir a qualidade das soluções oferecidas pelas empresas que atuam naquela categoria.

4. CONTRATAÇÕES SIMILARES REALIZADAS POR OUTROS ÓRGÃOS OU ENTIDADES DA ADMINISTRAÇÃO PÚBLICA

4.1. CONTRATO N.º 50/2022 - TCU

4.2. CONTRATO N.º36/2022 - TRE-SE

5. DETALHAMENTO DAS ALTERNATIVAS EXISTENTES

. DETALHAMENTO DAS ALTERNATIVAS EXISTENTES				
Requisitos	Itens da Solução	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	todos	X		
A solução encontra-se implantada em outro órgão ou entidade da Justiça Militar?	todos		X	
A Solução está disponível no Portal do Software Público Brasileiro?	todos		X	
A solução é um software livre ou público?	todos		X	

A solução é aderente às politicas, premissas e especificações técnicas definidas pelos padrões MNI?	todos		X	
A solução é aderente às regulamentações da ICP-Brasil?	todos		X	
A solução é aderente às premissas e especificações técnicas e funcionais do Moreq-Jus?	todos		X	

6. ESTIMATIVA DE PREÇO

GRUPO 1

a) Proposta empresa NCT - 3190719

GRUPO 1					
ITEM	**PRODUTO**	**UNIDADE**	**QTD**	**Valor Unitário**	**Valor**
1.	Proteção de usuários com acessos privilegiados	UN	250	3,360.00	840,00
2.	Proteção de usuários externos/Remoto	UN	100	10,600.00	1,060,
3.	Serviço de instalação e configuração	UN	1	224,000.00	224,00
4.	Suporte Técnico Especializado	Mensal	60	3,200.00	192,00
5.	Treinamento	UN	1	55,000.00	55,000

b) proposta empresa Enter Company - 3190721

GRUPO 1					
ITEM	**PRODUTO**	**UNIDADE**	**QTD**	Valor Unitário	Valor
1.	Proteção de usuários com acessos privilegiados	UN	250	4.000,00	1.000.
2.	Proteção de usuários externos/Remoto	UN	100	11.920,00	192.00
3.	Serviço de instalação e configuração	UN	1	250.000,00	250.00
4.	Suporte Técnico Especializado	Mensal	60	4.000,00	240.00
5.	Treinamento	UN	1	60.000,00	60.000

c) BeyondTrust - 3190725

GRUPO 1					
ITEM	**PRODUTO**	**UNIDADE**	**QTD**	Valor Unitário	Valor
1.	Proteção de usuários com acessos privilegiados	UN	250	R$ 4.780,00	R$ 1.1
2.	Proteção de usuários externos/Remoto	UN	100	R$ 13.145,00	R$ 1.3
3.	Serviço de instalação e configuração	UN	1	R$ 347.200,00	R$ 347
4.	Suporte Técnico Especializado	Mensal	60	R$ 18.290,00	R$ 1.0
5.	Treinamento	UN	1	R$ 823.840,00*	R$ 823

***Valor desconsiderado**

d) INOVAZUL - 3190731

GRUPO 1					
ITEM	**PRODUTO**	**UNIDADE**	**QTD**	Valor Unitário	Valor
1.	Proteção de usuários com acessos privilegiados	UN	250	R$ 3.760,10	R$ 940
2.	Proteção de usuários externos/Remoto	UN	100	R$ 10.999,00	R$ 1.0
3.	Serviço de instalação e configuração	UN	1	R$ 261.800,00	R$ 261
4.	Suporte Técnico Especializado	Mensal	60	R$ 4.230,54	R$ 253
5.	Treinamento	UN	1	R$ 65.000,00	R$ 65.

e) Contrato Similar - TCU - 3190732

GRUPO 1					
ITEM	**PRODUTO**	**UNIDADE**	**QTD**	Valor Unitário	Valor
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	R$ 120.000,00	R$ 120
4.	Suporte Técnico Especializado	Mensal	60	R$ 37.600,00	R$ 2.2
5.	Treinamento	UN	1	R$ 50.000,00	R$ 50.

VALOR MÉDIO PARA A CONTRATAÇÃO - GRUPO 1

GRUPO 1					
ITEM	**PRODUTO**	**UNIDADE**	**QTD**	Valor Unitário	Valo
1.	Proteção de usuários com acessos privilegiados	UN	250	R$ 3.975.02	R$ 9
2.	Proteção de usuários externos/Remoto	UN	100	R$ 11.666,00	R$ 1.16
3.	Serviço de instalação e configuração	UN	1	R$ 240.600,00	R$ 2
4.	Suporte Técnico Especializado	Mensal	60	R$ 7.430,13	R$ 4
5.	Treinamento	UN	1	R$ 57.500,00	R$ 5
TOTAL					R$ 3.10

GRUPO 2

a) Empresa YSSY - 3271395

GRUPO 2					
ITEM	**PRODUTO**	**UNIDADE**	**QTD**	Valor Unitário	Valor T
1.	Licença de serviço de autenticação por múltiplos fatores	UN	3.000	R$ 639,47	R$ 1.91
2.	Serviço de instalação e configuração	UN	1	R$ 54.822,79	R$ 54.8
3.	Suporte Técnico Especializado	Mensal	60	R$ 1.938,00	R$ 116.
4.	Treinamento	UN	1	R$ 21.365,00	R$ 21.3

b) Empresa AllTech - 3271401

GRUPO 2					
ITEM	**PRODUTO**	**UNIDADE**	**QTD**	Valor Unitário	Valor
1.	Licença de serviço de autenticação por múltiplos fatores	UN	3.000	R$ 675,00	R$ 2.0
2.	Serviço de instalação e configuração	UN	1	R$ 53.000,00	R$ 53.
3.	Suporte Técnico Especializado	Mensal	60	R$ 2.000,00	R$ 120
4.	Treinamento	UN	1	R$ 35.000,00	R$ 35.

c) Empresa WIseIT - 3271392

GRUPO 2					
ITEM	**PRODUTO**	**UNIDADE**	**QTD**	Valor Unitário	Valor
1.	Licença de serviço de autenticação por múltiplos fatores	UN	3.000	R$ 718,00	R$ 2.1
2.	Serviço de instalação e configuração	UN	1	R$ 57.653,00	R$ 57.
3.	Suporte Técnico Especializado	Mensal	60	R$ 2.124,00	R$ 127
4.	Treinamento	UN	1	R$ 32.645,00	R$ 32.

d) Contrato Similar - TRE-SE 3190734

GRUPO 2					
ITEM	**PRODUTO**	**UNIDADE**	**QTD**	Valor Unitário	Valo
1.	Licença de serviço de autenticação por múltiplos fatores	UN	3.000	R$ 390,00	R$ 1.17

2.	Serviço de instalação e configuração	UN	1	R$ 11.292,00	R$11.
3.	Suporte Técnico Especializado	Mensal	60	xxxx	xxxx
4.	Treinamento	UN	1	R$ 22.500,00	R$ 2

VALOR MÉDIO PARA A CONTRATAÇÃO - GRUPO 2

GRUPO 2					
ITEM	**PRODUTO**	**UNIDADE**	**QTD**	Valor Unitário	Valo
1.	Licença de serviço de autenticação por múltiplos fatores	UN	3.000	R$ 605,61	R$ 1.81
2.	Serviço de instalação e configuração	UN	1	R$ 44.191,94	R$ 4
3.	Suporte Técnico Especializado	Mensal	60	R$ 2.020,66	R$ 1
4.	Treinamento	UN	1	R$ 27.877,50	R$ 2
TOTAL					R$ 2.02

7. ANÁLISE E COMPARAÇÃO DOS CUSTOS TOTAIS DAS SOLUÇÕES IDENTIFICADAS

GRUPO 1

Para a aquisição de todas as licenças do Grupo 1 (itens 1 e 2) será necessário o valor médio de R$ 2.160.355,00. Para os itens 2 e 4 o custo será de R$ 298.100,00. O custo total médio do item 4 será de R$ 445.807,80, dividido conforme tabela abaixo:

2023	2024	2025	2026	2027	2028
2 meses	12 meses	12 meses	12 meses	12 meses	10 meses
R$ 14.860,26	R$ 89.161,56	R$ 89.161,56	R$ 89.161,56	R$ 89.161,56	R$ 74.301,30

GRUPO 2

Para a aquisição de todas as licenças do Grupo 2 (itens 1) será necessário o valor médio de R$ 1.816.830,00. Para os itens 2e 4 o custo será de R$ 72.069,44. O custo total médio do item 3 será de R$ 121.239,60, dividido conforme tabela abaixo:

2023	2024	2025	2026	2027	2028
2 meses	12 meses	12 meses	12 meses	12 meses	10 meses
R$ 4.041,32	R$ 24.247,92	R$ 24.247,92	R$ 24.247,92	R$ 24.247,92	R$ 20.206,60

8. ESCOLHA DA SOLUÇÃO

8.1. 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.

8.2. 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.

8.3. 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.

8.4. 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

8.5. Sendo assim é dever do departamento de tecnologia 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.

8.6. 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.

8.7. 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.

9. DESCRIÇÃO DA SOLUÇÃO

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

9.1. ESPECIFICAÇÃO DO OBJETO - GRUPO 1

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

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

9.1.1.2. Gerenciamento de chaves

9.1.1.2.1. 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;

9.1.1.2.2. 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;

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

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

9.1.1.2.5. 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);

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

9.1.1.2.7. 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;

9.1.1.2.8. Controlar e monitorar sessões usando protocolos padrões e acesso remoto, incluindo RDP, HTTP/HTTPS e SSH;

9.1.1.2.9. 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;

9.1.1.2.10. 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;

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

9.1.1.2.12. Se ofertado em appliance físico:

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

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

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

9.1.1.2.16. 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;

9.1.1.2.17. 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;

9.1.1.2.18. 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;

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

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

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

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

9.1.1.2.19.4. Lista de contas gerenciadas com idade de senha;

9.1.1.2.19.5. Lista de sistemas gerenciados;

9.1.1.2.19.6. Atividades de retirada de senhas e sessões;

9.1.1.2.19.7. Eventos de alteração de senha;

9.1.1.2.19.8. Auditoria de contas;

9.1.1.2.19.9. Atividades de atualização de senhas;

9.1.1.2.19.10. Atividades de sessões remotas;

9.1.1.2.19.11. Detalhes das próximas atualizações de senha programadas;

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

9.1.1.2.20. 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);

9.1.1.2.21. 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:

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

9.1.1.2.21.2. 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;

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

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

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

9.1.1.2.22.2. Levantamento de contas administrativas em cada ativo;

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

9.1.1.2.22.4. Classificação automática de contas locais e de domínio;

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

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

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

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

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

9.1.1.2.26. 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;

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

9.1.2. ITEM 2: PROTEÇÃO DE USUÁRIOS EXTERNOS/REMOTO

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

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

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

9.1.2.3.1. Microsoft Windows 10 e superiores.;

9.1.2.3.2. Servidores Windows Server 2012 e superiores;

9.1.2.3.3. Linux Red Hat Enterprise 7.0 e superiores.

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

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

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

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

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

9.1.2.9. 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;

9.1.2.10. 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);

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

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

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

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

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

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

9.1.2.17. 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”;

9.1.2.18. 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;

9.1.2.19. Suportar o acesso com os seguintes modos:

    9.1.2.19.1. Através de clientes instalados;

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

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

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

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

9.1.2.22. Prover acesso a páginas Web, onde os usuários receberão apenas uma conexão a uma página Web local em uma sessão auditada e gravada;

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

9.1.2.24. 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;

9.1.2.25. 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;

9.1.2.26. 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;

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

9.1.2.28. 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;

9.1.2.29. 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.

9.2. ESPECIFICAÇÃO DO OBJETO - GRUPO 2

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

9.2.1.1. Especificações Técnicas

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

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

9.2.1.1.3. 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;

9.2.1.1.4. 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;

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

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

9.2.1.1.7. Estações de trabalho Microsoft Windows 10 e superiores;

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

9.2.1.1.9. 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;

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

9.2.1.2. Especificação do Produto

9.2.1.2.1. 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;

9.2.1.2.2. 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;

9.2.1.2.3. 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;

9.2.1.2.4. 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;

9.2.1.2.5. A solução fornece capacidade de integração com o Security Assertion Markup

Language – SAML;

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

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

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

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

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

9.2.1.2.11. Hardware Token;

9.2.1.2.12. OTP enviado por Short Message Service – SMS;

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

9.2.1.2.14. 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:

9.2.1.2.15. Redes autorizadas;

9.2.1.2.16. Baseado em políticas globais aplicadas ou por aplicações;

9.2.1.2.17. 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;

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

9.2.1.2.19. 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:

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

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

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

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

9.2.1.2.24. Servidores Virtuais para aplicações, software básico:

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

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

9.2.1.2.27. Microsoft IIS 10 e superior;

9.2.1.2.28. Microsoft .NET Framework 4.7 ou superior;

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

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

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

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

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

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

9.2.1.2.35. 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;

9.2.1.3. Controle de acessos

9.2.1.3.1. 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;

9.2.1.3.2. 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;

9.2.1.3.3. 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;

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

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

9.2.1.3.6. 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;

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

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

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

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

9.2.1.3.11. 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;

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

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

9.2.1.3.14. Windows Hello;

9.2.1.3.15. FaceID ou TouchID;

9.2.1.3.16. Android Biometris ou Samsung Fingerprint/reconhecimento facial;

9.2.1.3.17. WebAuthn;

9.2.1.3.18. FIDO2

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

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

9.2.1.4. Auditoria

9.2.1.4.1. 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;

9.2.1.4.2. 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;

9.2.1.4.2. 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;

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

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

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

9.2.1.5. Relatórios

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

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

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

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

9.3.2. 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.

9.3.3. 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.

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

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

9.3.6. 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.

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

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

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

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

9.3.11. 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.

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

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

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

9.4.1. 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;

9.4.2. 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 CONTRATADA. 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 solução ou em qualquer serviço que a compõe; para a configuração da solução; para aplicação de ações de respostas a incidentes ou parada ou indisponibilidade da solução.
MÉDIA	4h	8h	É aplicado para solicitações de criação/configuração de políticas nos demais serviços que compõem a solução; quando há problema, simultâneo ou não, nos elementos que compõem os serviços/solução, embora ainda estejam disponíveis.
BAIXA	4h	72h	É aplicado para solicitação de configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço/equipamentos.

9.4.3. 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;

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

9.4.5. 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:

9.4.6. 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;

9.4.7. 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;

9.4.8. 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;

9.4.9. 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.

9.4.10. 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;

9.4.11. 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;

9.4.12. 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;

9.4.13. 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;

9.4.14. 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;

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

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

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

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

9.5.3. Carga horária mínima de 20 HORAS

9.5.4. Treinamento a ser realizado para até 08 participantes;

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

9.5.6. O treinamento poderá ser realizado de forma remota;

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

9.5.8. O idioma das aulas deverá ser em português;

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

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

9.5.11. Visão geral da solução;

9.5.12. Configurações iniciais;

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

9.5.14. Integração com ferramentas e sistemas;

9.5.15. Replicação da solução;

9.5.16. Uso de dispositivos e credenciais;

9.5.17. Configuração de grupos de acesso;

9.5.18. Autenticação e autorização de acesso;

9.5.19. Gravação e monitoramento de sessões;

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

9.5.21. Geração de relatórios;

9.5.22. Backup e recuperação da solução;

10. ALINHAMENTO DA SOLUÇÃO

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.

11. BENEFÍCIOS ESPERADOS

11.1. Dentre os benefícios, destacam-se:

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

11.1.2. Aumentar a resiliência às inevitáveis ameaças cibernéticas;

11.1.3. Estabelecer governança de segurança cibernética;

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

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

11.1.6. 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.

12. RELAÇÃO ENTRE A DEMANDA PREVISTA E A CONTRATADA

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.

13. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE

Não há

SUSTENTAÇÃO DO CONTRATO

1. OBJETO

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.

2. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

A sustentação da solução não requer disponibilização, por parte do órgão, de recursos materiais e/ou humanos além dos já existentes no STM.

2.2. ESTRATÉGIA DE CONTINUIDADE DO FORNECIMENTO DA SOLUÇÃO DE TIC EM EVENTUAL INTERRUPÇÃO CONTRATUAL

EVENTO	AÇÃO CONTINGÊNCIA	RESPONSÁVEL PELA AÇÃO
Inexecução contratual	Havendo qualquer evento de inexecução contratual, que acarrete no distrato, os serviços de manutenção corretiva em garantia serão realizados por outra empresa a ser contratada, analisando previamente a vantajosidade da contratação, a continuidade da garantia pelo fabricante, sem prejuízo da aplicação das penalidades previstas.	Equipe de gestão do contrato

2.3. ATIVIDADES DE TRANSIÇÃO CONTRATUAL E DE ENCERRAMENTO DO CONTRATO

AÇÃO	RESPONSÁVEL

A contratada deve, em conformidade com o parágrafo único do artigo 111 da Lei nº 8.666/93, promover transição contratual e repassar para o contratante e/ou para a nova contratada todos os dados, documentos e elementos de informação utilizados na execução dos serviços.	Equipe de gestão do contrato

2.4 TRANSFERÊNCIA FINAL DE CONHECIMENTOS SOBRE A EXECUÇÃO E A MANUTENÇÃO DA SOLUÇÃO DE TIC

ATIVIDADE	RESPONSÁVEL
Faltando 45 dias para o encerramento do contrato, a CONTRATADA deverá fazer repasse de todas as tecnologias utilizadas nos projetos ainda em andamento, deverá, ainda, apresentar as atividades que estão em andamento, as que deverão ser concluídas até o final do contrato, bem como justificar as que não poderão ser atendidas. A critério do CONTRATANTE o referido repasse poderá ocorrer em prazo menor que os 45 dias.	Equipe de gestão do contrato

2.4.2 REVOGAÇÃO DE PERFIS DE ACESSO

ATIVIDADE	RESPONSÁVEL
NÃO SE APLICA	

2.4.3 ELIMINAÇÃO DE CAIXAS POSTAIS

ATIVIDADE	RESPONSÁVEL
NÃO SE APLICA	NÃO SE APLICA

3. ESTRATÉGIA DE INDEPENDÊNCIA

Não se aplica

3.2 DIREITOS DE PROPRIEDADE INTELECTUAL (Lei nº 9.610, de 19 de fevereiro de 1998)

Todos os produtos gerados na vigência do contrato serão de propriedade do CONTRATANTE, em conformidade com o artigo 111, da Lei nº 8.666/93, com a Lei nº 9.609/98, que dispõe sobre propriedade intelectual de programa de computador, e com a Lei nº 9.610/98, que dispõe sobre direito autoral, sendo vedada a comercialização destes, a qualquer título, por parte da CONTRATADA.

FUNDAMENTAÇÃO

Em conformidade com o art. 16, da Resolução nº 182, de 17 de outubro de 2013, do Conselho Nacional de Justiça (CNJ) e, subsidiariamente, com a Lei nº 8.666, de 21 de junho de 1993.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

INTEGRANTE TÉCNICO	INTEGRANTE DEMANDANTE	INTEGRANTE ADMINISTRATIVO
Marcio Coelho Marques	Wilson Marques de Souza Filho	**Luis Gustavo Costa Reis**

VALIDAÇÃO DA SUSTENTAÇÃO DO CONTRATO

Autoridade da Área Demandante

Ianne Carvalho Barros

ESTRATÉGIA PARA A CONTRATAÇÃO

1. OBJETO

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.

2. NATUREZA DO OBJETO COM A INDICAÇÃO DOS ELEMENTOS NECESSÁRIOS PARA CARACTERIZAR O BEM E/OU SERVIÇO A SER CONTRATADO

A natureza do objeto a ser contratado é comum nos termos do parágrafo único, do art. 1°, da Lei 10.520, de 2002., além de:

a) ser possível especificar o serviço usando parâmetros usuais de mercado;

b) ser possível medir o desempenho da qualidade usando parâmetros usuais de mercado.

3. PARCELAMENTO DO OBJETO COM A DEMONSTRAÇÃO DA VIABILIDADE OU NÃO DA DIVISÃO

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.

4. ADJUDICAÇÃO DO OBJETO COM A INDICAÇÃO E JUSTIFICATIVA DA FORMA ESCOLHIDA, DEMONSTRANDO SE O OBJETO PODE SER ADJUDICADO A UMA OU A VÁRIAS EMPRESAS, SE POR ITENS OU POR GRUPO DE ITENS

Considerando o disposto no §1º do artigo 23 da lei 8666/93 onde as obras, serviços e compras efetuadas pela Administração serão divididas em tantas parcelas quantas se comprovarem técnica e economicamente viáveis. Os itens especificados de cada grupo estão fortemente integrados entre si, sendo necessária sua execução por uma mesma empresa para que não se configure conflito de competências quando da solicitação e/ou cobrança das atividades realizadas, além de reduzir a complexidade da gestão do contrato, reduzir seus custos de administração e reduzir os riscos operacionais e conflitos. Desta forma, os itens objeto do presente termo de referência serão agrupados

Dessa forma, a adjudicação será integralmente realizada a um único fornecedor para cada grupo pelo menor preço global.

5. MODALIDADE E O TIPO DE LICITAÇÃO COM A INDICAÇÃO E A JUSTIFICATIVA PARA AS ESCOLHAS

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

6. CLASSIFICAÇÃO ORÇAMENTÁRIA COM A INDICAÇÃO DA FONTE DE RECURSO DO ORÇAMENTO DO ÓRGÃO PREVISTO PARA ATENDER À NECESSIDADE DE CONTRAÇÃO DE SOLUÇÃO DE TI DEMANDADA

A despesa ocorrerá à conta de dotação consignada à Justiça Militar da União pela Lei Orçamentária para o exercício de 2020, Plano de Trabalho SEG0; Natureza de despesa: **3.3.90.40**; mediante emissão de nota de empenho.

7. VIGÊNCIA COM A INDICAÇÃO DO PRAZO DE GARANTIA DOS BENS E/OU PRESTAÇÃO DOS SERVIÇOS CONTRATADOS

21.1. O prazo de execução referente aos grupos 1, 2 e 3 e itens 3 e 7 será de até 30 dias, após o recebimento da nota de empenho.

21.2. A vigência do contrato referente ao item 8 será de 12 meses, a contar de sua assinatura

8. INDICAÇÃO DOS TERMOS CONTRATUAIS

8.1. OBRIGAÇÕES DA CONTRATADA

8.1.1. 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.

8.1.2. 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.

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

8.1.4. 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.

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

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

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

8.1.8. 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.

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

8.1.10. 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.

8.1.11. 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.

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

8.1.13. 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.

8.1.14. Assegurar à Contratante:

8.1.14.1. 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

8.1.14.2. 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.

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

8.2. OBRIGAÇÕES DA CONTRATANTE

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

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

8.2.3. 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.

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

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

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

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

8.EQUIPE DE APOIO À CONTRATAÇÃO COM A INDICAÇÃO DE SEUS INTEGRANTES

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).

9.EQUIPE DE GESTÃO DA CONTRATAÇÃO COM A INDICAÇÃO DE SEUS INTEGRANTES

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

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

FUNDAMENTAÇÃO

Em conformidade com o art. 16, da Resolução nº 182, de 17 de outubro de 2013, do Conselho Nacional de Justiça (CNJ) e, subsidiariamente, com a Lei nº 8.666, de 21 de junho de 1993.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

INTEGRANTE TÉCNICO	INTEGRANTE DEMANDANTE	INTEGRANTE ADMINISTRATIVO
Marcio Coelho Marques	**Wilson Marques de Souza Filho**	**Luis Gustavo Costa Reis**

VALIDAÇÃO DA ESTRATÉGICA PARA A CONTRATAÇÃO

Ianne Carvalho Barros - Diretor da DITIN

Autoridade da Área Demandante

Documento assinado eletronicamente por **WILSON MARQUES DE SOUZA FILHO**, **COORDENADOR DE TECNOLOGIA**, em 07/07/2023, às 16:32 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUIS GUSTAVO COSTA REIS**, **CHEFE DO NÚCLEO DE GESTÃO ADMINISTRATIVA**, em 07/07/2023, às 16:51 (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 07/07/2023, às 19:08 (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 10/07/2023, às 13:26 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Setor de Autarquias Sul, Praça dos Tribunais Superiores - Bairro Asa Sul - CEP 70098-900 - Brasília - DF