



SUPERIOR TRIBUNAL DE JUSTIÇA

SAFS - Quadra 6 - Lote 1 - Trecho III - CEP 70095-900 - Brasília - DF - www.stj.jus.br

TERMO DE REFERÊNCIA - EPRO

0061/2024 (v11) - Lei 14133/2021

Processo STJ 38832/2023

Assunto: Solução para monitoramento e auditoria de acessos no ambiente do STJ - Lei 14133/2021

Requisitante: Coordenadoria de Planejamento e Gestão de Contratos de TIC

1. OBJETO

- 1.1. Registro de preço para fornecimento de serviço contínuo de solução de governança, compliance, segurança e auditoria de dados não estruturados, incluindo análise e segurança de credenciais de usuários de rede, coleta e correlacionamento de eventos com informações provenientes de análise de dados não estruturados e metadados. Incluindo serviços de suporte técnico assistido, instalação, treinamento com transferência de conhecimento do ambiente implantado, incluindo também serviço de apoio a análise, investigação e tratamento de incidentes de segurança.
- 1.2. O objeto desta contratação é caracterizado como comum, cujos padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado, e está definido como contratação de caráter contínuo, nos termos do inciso k do art. 4º da [Instrução Normativa STJ/GDG nº 10 de 28 de abril de 2022](#).

2. ESPECIFICAÇÃO DO OBJETO

- 2.1. A especificação abaixo visa oferecer a descrição completa e adequada das características e quantitativo do objeto:

LOTE 1 - Licenças e serviços para o STJ, órgão gerenciador

Item	Classificação	Especificação do objeto	Unidade	Quantidade
1	18333	Licença de uso de software de governança, compliance e segurança de dados sensíveis com análise comportamental de usuários do Microsoft Active Directory, servidores de arquivos on premise Windows ou Linux e NAS (network attached storage), incluindo segurança de credenciais de usuários do Microsoft Active Directory, com garantia e suporte do fabricante.	Usuário	4809
2	18333	Licença de uso de software de governança, compliance e segurança e proteção de dados sensíveis com análise comportamental de usuários para ambiente de nuvem (Microsoft Sharepoint online, Exchange online, Microsoft Teams, OneDrive) ou Google drive ou AWS s3), com garantia e suporte do fabricante.	Usuário	4809
3	183339	Serviço de instalação, implantação, parametrização e operacionalização para os itens 1 e 2.	Serviço	1
4	18376	Treinamento oficial para dez participantes.	Turma	1
5	183339	Serviço de apoio a análise, investigação e tratamento de incidentes de segurança, com duração de (1h) uma hora por semana.	Atividade Mensal	24

LOTE 2 - Licenças e serviços para o CJF, órgão participante

Item	Descrição	Especificação do objeto	Unidade	Quantidade
6333	1833	Licença de uso de software de governança, compliance e segurança de dados sensíveis com análise comportamental de usuários do Microsoft Active Directory, servidores de arquivos on premise Windows ou Linux e NAS (network attached storage), incluindo segurança de credenciais de usuários do Microsoft Active Directory, com garantia e suporte do fabricante.	Usuário	550
7333	1833	Licença de uso de software de governança, compliance e segurança e proteção de dados sensíveis com análise comportamental de usuários para ambiente de nuvem (Microsoft Sharepoint online, Exchange online, Microsoft Teams, OneDrive) ou Google drive ou AWS s3), com garantia e suporte do fabricante.	Usuário	550
8339	1833	Serviço de instalação, implantação, parametrização e operacionalização para os itens 6 e 7.	Serviço	1
9376	1837	Treinamento oficial para dez participantes.	Turma	1
1039	1839	Serviço de apoio a análise, investigação e tratamento de incidentes de segurança, com duração de (1h) uma hora por semana.	Mês	24

2.2. A vigência das licenças é de 24 (vinte e quatro) meses.

2.3. A descrição completa e adequada das características técnicas do objeto está detalhada no [ANEXO I](#).

3. VIGÊNCIA E PRORROGAÇÃO

3.1. DA CONTRATAÇÃO

- 3.1.1. A vigência será de 24 (vinte e quatro) meses contados da data de assinatura do contrato.
- 3.1.2. Os itens 1, 2, 5, 6, 7 e 10 poderão ser prorrogados por sucessivos períodos até a vigência máxima decenal, conforme disposto no artigo 107 da Lei 14.133/2021.
- 3.1.2.1. A prorrogação é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para o CONTRATANTE, permitida a negociação com a CONTRATADA, e da existência de créditos orçamentários consignados ao Superior Tribunal de Justiça no Orçamento Geral da União a cada exercício financeiro.
- 3.1.3. A minuta de contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência contratual e ao reajustamento de preços.

3.2. DA ATA DE REGISTRO DE PREÇOS

- 3.2.1. O prazo de vigência da ata de registro de preços será de **doze meses** contados do primeiro dia útil subsequente à data de sua divulgação no Portal Nacional de Contratações Públicas (PNCP), sem possibilidade de prorrogação.

4. JUSTIFICATIVA E FUNDAMENTAÇÃO

4.1. Para o STJ:

- 4.1.1. Na medida em que recursos tecnológicos foram disponibilizados aos servidores, colaboradores e aos cidadãos como um todo, aumentando a acessibilidade aos serviços ofertados pelo Tribunal da Cidadania, o risco associado a esta exposição crescente é proporcionalmente maior. Atualmente as fontes de informação são incrivelmente heterogêneas: existem informações relevantes em estações de trabalho, servidores de redes, contas de e-mail, sítio na internet, ferramentas de colaboração, dispositivos móveis, celulares, tablets, enfim, as opções são quase infinitas.

- 4.1.2. As informações do Tribunal se encontram espalhadas em diversos locais, e a utilização de plataformas em nuvem, ao mesmo tempo em que entregam uma velocidade e disponibilidade ímpares para otimizar os trabalhos da nobre atividade jurisdicional, também aumentam a dificuldade em monitorar todos os acessos aos dados do STJ. Por conseguinte, a probabilidade de ocorrerem acessos não autorizados cresce exponencialmente, e a viabilidade de auditar tamanha infinidade de repositórios de informações de forma não automatizada é absolutamente inviável.
- 4.1.3. Os dados da instituição se encontram pulverizados em inúmeros locais, de forma tanto estruturada quanto não estruturada. O STJ não dispõe de uma ferramenta centralizada para monitorar e auditar os acessos aos recursos tecnológicos ofertados pela Secretaria de Tecnologia da Informação e Comunicação. Desta forma, o risco de vazamentos não autorizados de informações, bem como acessos indevidos, publicações impróprias ou mesmo alterações de decisões da Corte é real.
- 4.1.4. Neste ponto, importante reforçar a necessidade de aderência de regulamentações associadas a privacidade e proteção de dados, como a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD); a Resolução CNJ nº 396, de 7 de junho de 2021 - institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ); as Normas Internacionais de Segurança da Informação (ISO 27001/27002/27005/22301) e CIS Control V.8 (Critical Security Controls), dentre outras.
- 4.1.5. **Problema a ser resolvido**
- 4.1.5.1. O STJ não dispõe de uma solução centralizada que viabilize o monitoramento, auditoria e proteção dos dados, que faça uma coleta em tempo real dos fluxos de metadados e uma análise dos dados nos mais diversos repositórios utilizados pela Corte.

4.1.5.2. As fontes de informação utilizadas no tribunal são extremamente heterogêneas, incluindo dados estruturados e não estruturados. Existe ainda o agravante de soluções na nuvem, que dificultam ainda mais o gerenciamento. É muito complexo conseguir monitorar possíveis acessos indevidos, vazamento de informações, credenciais compartilhadas, ainda mais considerando que os dados podem estar disponíveis em qualquer lugar do mundo. Antigamente, quando os repositórios eram apenas internos, esse trabalho já era complexo. Com os adventos dos serviços remotos tornou-se ainda mais difícil. Dados podem ser compartilhados por pastas, links remotos, dispositivos móveis, pendrives, e-mail, ferramentas de colaboração e mensagens instantâneas, as opções são muitas; e o risco inerente é igualmente grande.

4.1.5.3. Faz-se necessária a contratação de plataforma de segurança de dados que ofereça recursos avançados para classificar e proteger as informações confidenciais da organização, capaz de prover as seguintes características mínimas desejáveis:

- Visualização de dados, devendo oferecer uma interface gráfica intuitiva que permita aos usuários administradores visualizar de forma clara o acesso aos dados e as atividades dos usuários. Isso facilita a identificação de ameaças e permite adotar medidas imediatas para proteger as informações custodiadas;
- Aumentar a visibilidade e entendimento do ambiente de TIC, permitindo analisar o comportamento dos usuários e de objetos (como permissões, arquivos, metadados, dados não estruturados), auxiliando na identificação de padrões de uso, anomalias, áreas de risco e pontos de vulnerabilidade, permitindo uma melhor compreensão do cenário de segurança cibernética e orientando a implementação de medidas de proteção mais efetivas;
- Identificação de ameaças avançadas, por meio da análise de logs, eventos e atividades de usuários em busca de padrões e indicadores de comprometimento. Deve prover técnicas de análise comportamental e algoritmos de machine learning para identificar atividades que podem indicar a presença de ameaças avançadas, como ataques persistentes e furtivos;
- Deve ser compatível com ambiente Microsoft Active Directory on premises, Azure Active Directory (Microsoft entra ID), Office 365, Exchange, Sharepoint, Microsoft Teams e toda a solução Microsoft 365;
- Deve ser capaz de auditar as ações em credenciais do domínio;
- Deve ser capaz de auditar os acessos em servidores de arquivos;
- Deve realizar a classificação e identificação de informações sensíveis nos repositórios investigados;
- Deve incorporar recursos de inteligência artificial objetivando aprimorar as funcionalidades de análise e proteção de dados. Desta forma, identificando padrões e anomalias;
- Deve utilizar algoritmos de aprendizado de máquina para entender o comportamento padrão de usuários e identificar desvios, que podem indicar atividades maliciosas;
- Deve auxiliar na identificação e classificação dos dados nos mais variados tipos de repositórios, estruturados e não estruturados;
- Deve alertar acessos não autorizados em arquivos e possíveis adulterações não legítimas;
- A solução deve fornecer alta disponibilidade e redundância.

4.1.6. Resultados pretendidos

4.1.6.1. Os resultados a serem alcançados com esta contratação são:

- Atender requisitos regulatórios e de conformidade, com verificação de adequação a legislação pertinente no trato de informações e identificação de dados sensíveis;
- Emitir relatórios manuais ou automáticos das eventos identificados pela ferramenta;
- Análise de riscos e auditoria: fornece detalhes sobre acessos aos dados do Tribunal, ajudando na análise de riscos e em auditorias;
- Fornecer plataforma integrada para concessão de permissões: permitir um gerenciamento de concessão de permissões centralizado, auditado e contributivo, onde o próprio dono da informação pode controlar os acessos, tirando essa carga das equipes da Secretaria de Tecnologia e Comunicação.

4.1.6.2. Os resultados técnicos a serem alcançados com esta contratação são:

- Auditar acessos nos mais variados repositórios de dados do STJ;
- Controlar dados não estruturados e estruturados;
- Auditar ambiente Active Directory: alterações em GPOs do domínio, grupos do domínio, permissões de compartilhamentos, delegação de permissões, comportamento de usuário;
- Auditar servidores de arquivos Microsoft;
- Identificar compartilhamentos de arquivos não autorizados, que possam resultar em vazamento de informações do Tribunal;
- Auditar as ações em credenciais do domínio, como criação, reset de senha, deleção, adição ou remoção em grupos;
- Utilizar solução de inteligência artificial para identificar desvios de padrão, informação esta a ser utilizada em análises forenses de incidentes cibernéticos, possibilitando uma ação proativa do SOC;
- Monitorar atividades de usuários: monitoramento detalhado das atividades dos usuários em relação aos recursos tecnológicos;
- Identificar e classificar dados sensíveis: possibilita a identificação de dados sensíveis e classificação de informações críticas;
- Aplicar políticas de segurança que garantam que apenas usuários autorizados tenham acesso às informações;
- Mitigar ameaças internas: dificulta o vazamento indevido de informações confidenciais ou sensíveis;
- Proteger contra Ransomware e ataques cibernéticos: identifica padrões e comportamentos suspeitos, desvios de comportamentos, prevenindo e protegendo contra atores maliciosos;
- Controle de acesso baseado em função: implementa políticas de controle de acesso baseados na função;
- Resposta a incidentes: em casos de incidentes cibernéticos, viabiliza investigação forense com rastreabilidade detalhada, e ainda possibilita a realização de ações corretivas;
- Auditar ambiente Exchange Online;
- Auditar ambiente Azure, Sharepoint e Teams.

4.1.7. A contratação está prevista no código STI2024-092 do PCAq/2024 e no Plano de Contratações de STIC de que trata o art. 4º da Resolução CNJ n. 468/2022, aprovado pelo Comitê de Gestão ou de Governança de TIC do STJ, e está formalizada no Documento de Formalização de Demanda ([4049239](#)).

4.2. Para o CJF:

- 4.2.1. O Conselho lida diariamente com uma grande diversidade de informações, das quais algumas são protegidas por lei. A presente contratação tem por objetivo atender demandas relacionadas a proteção dessas informações somados aos esforços já empregados em outras frentes, como as práticas procedimentais para a Gestão da Segurança da Informação (eletrônica ou física), bem como antivírus e bloqueio de acessos indevidos aos ativos de TI.
- 4.2.2. Segundo o instituto de pesquisas técnicas e análises de tendências de TI - o GARTNER GROUP, cerca de 80% dos dados estratégicos estão armazenados em "base de dados não estruturadas" que se traduz em pastas, arquivos, vídeos, imagens, e-mails dentre outros, que tem como responsáveis (donos): departamentos, setores e pessoas. As informações do Conselho da Justiça Federal se encontram espalhadas em diversos locais, e a utilização de plataformas em nuvem, ao mesmo tempo em que entregam uma velocidade e disponibilidade ímpares para otimizar os trabalhos da nobre atividade jurisdicional, também aumentam a dificuldade em monitorar todos os acessos aos dados do CJF. Por conseguinte, a probabilidade de ocorrerem acessos não autorizados cresce exponencialmente, e a viabilidade de auditar tamanha infinidade de repositórios de informações de forma não automatizada é absolutamente inviável.
- 4.2.3. Estes dados são acessados diuturnamente pela rede do CJF e gerenciados por Sistemas Operacionais - SO que proporcionam os registros (logs) dos eventos (alteração, inclusão, exclusão e outros). Uma vez registrados tais eventos, que têm uma ordem de volume na casa de milhões, o SO não fornece forma eficiente de busca de informação para efeito por exemplo de auditoria; a interface é ineficiente para consultas e pesquisas, além de não fazer monitoramento e análise crítica de eventos visando detecção antecipada de situações indevidas, tornando inviável qualquer tipo de gerenciamento e auditoria de acesso a dados de forma real e imediata. Ou seja, com as ferramentas básicas que um analista de sistema operacional ou administrador de rede possui é praticamente inviável auditar quem acessou, modificou, apagou, renomeou ou enviou qualquer arquivo da referida "base não estruturada". Assim, o volume de usuários na rede interna multiplicados pelos eventos que cada um realiza diariamente, torna a atividade de auditoria, monitoramento e gerenciamento como uma "missão inexecutável", especialmente para a visão e gestão integrada dos serviços de AD (Microsoft Active Directory), servidor de Arquivos (Microsoft File Server) e sistema de correio eletrônico (Microsoft Exchange Server).

4.2.4. Neste ponto, importante reforçar a necessidade de aderência de regulamentações associadas a privacidade e proteção de dados, como a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD); a Resolução CNJ nº 396, de 7 de junho de 2021 - institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ); as Normas Internacionais de Segurança da Informação (ISO 27001/27002/27005/22301) e CIS Control V.8 (Critical Security Controls), dentre outras.

4.2.5. **Problema a ser resolvido**

4.2.5.1. A contratação de uma solução de auditoria de dados ajuda a mitigar e solucionar uma série de problemas relacionados à segurança e gerenciamento de dados. Aqui estão alguns exemplos:

1. Identificação de ameaças internas: pode ajudar a identificar atividades suspeitas de usuários internos, como acesso não autorizado a dados sensíveis, compartilhamento indevido de informações confidenciais, entre outros.
2. Proteção contra vazamento de dados: pode detectar e alertar sobre tentativas de vazamento de dados, ajudando a prevenir incidentes de segurança que possam resultar na perda ou exposição de informações sensíveis.
3. Cumprimento de normas e regulamentações: oferece recursos para ajudar as empresas a cumprir normas como GDPR, LGPD e outras regulamentações de proteção de dados, fornecendo relatórios e auditorias detalhadas sobre o uso e acesso aos dados.
4. Melhoria na visibilidade e controle dos dados: fornece uma visão abrangente das atividades de dados em toda a rede, permitindo que as empresas identifiquem áreas de risco, monitorem o acesso aos dados e implementem políticas de segurança mais eficazes.
5. Detecção de ransomware e malware: pode ajudar a identificar atividades suspeitas associadas a ransomware e malware, permitindo uma resposta rápida para mitigar os danos causados por essas ameaças.
6. Aprimoramento da segurança do Active Directory: pode ajudar a proteger o Active Directory contra ameaças internas e externas, identificando e corrigindo configurações inadequadas que possam colocar em risco a segurança da rede.

4.2.5.2. A implementação de uma solução de auditoria de dados deve ser parte de uma estratégia abrangente de segurança da informação, que inclua políticas claras, treinamento sobre segurança cibernética dos servidores e prestadores e outras medidas de proteção de dados.

4.2.6. Resultados pretendidos

4.2.6.1. A adoção de uma solução de auditoria de dados proporcionará inúmeros benefícios ao CJF, dentre eles:

1. Auditar acessos nos mais variados repositórios de dados (file server, sharepoint, exchange, onedrive, etc);
2. Controlar dados não estruturados e estruturados;
3. Auditar ambiente Active Directory: alterações em GPOs do domínio, grupos do domínio, permissões de compartilhamentos, delegação de permissões, comportamento de usuário;
4. Auditar servidores de arquivos Microsoft;
5. Identificar compartilhamentos de arquivos não autorizados, que possam resultar em vazamento de informações;
6. Auditar as ações em credenciais do domínio, como criação, reset de senha, deleção, adição ou remoção em grupos;
7. Utilizar solução de inteligência artificial para identificar desvios de padrão, informação que será utilizada em análises forenses de incidentes cibernéticos, possibilitando uma ação proativa do SOC;
8. Monitorar atividades de usuários: monitoramento detalhado das atividades dos usuários em relação aos recursos tecnológicos;
9. Identificar e classificar dados sensíveis: possibilita a identificação de dados sensíveis e classificação de informações críticas;
10. Aplicar políticas de segurança que garantam que apenas usuários autorizados tenham acesso às informações;
11. Mitigar ameaças internas: dificulta o vazamento indevido de informações confidenciais ou sensíveis;
12. Proteger contra Ransomware e ataques cibernéticos: identifica padrões e comportamentos suspeitos, desvios de comportamentos, prevenindo e protegendo contra atores maliciosos;

13. Controle de acesso baseado em função: implementa políticas de controle de acesso baseados na função;
14. Resposta a incidentes: em casos de incidentes cibernéticos, viabiliza investigação forense com rastreabilidade detalhada, e ainda possibilita a realização de ações corretivas;
15. Auditar ambiente Exchange On-premises e Online;
16. Auditar ambiente Azure, Sharepoint e Teams.

4.3. Registro de Preços

- 4.3.1. A justificativa para o registro de preços se enquadra no inciso III do artigo 3º do Decreto n. 11.462/2023, *in verbis*:

"Art. 3º O SRP poderá ser adotado quando a Administração julgar pertinente, em especial:

[...]

III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas;"

5. METODOLOGIA DO QUANTITATIVO ESTIMADO

5.1. Para o STJ:

- 5.1.1. O licenciamento deve englobar toda a estrutura de Datacenter do Superior Tribunal de Justiça, tanto *on-premises* quanto na nuvem.
- 5.1.2. A solução é licenciada pelo quantitativo de usuários do ambiente.
- 5.1.3. Para uma estimativa assertiva da quantidade de usuários, esta equipe de planejamento da contratação se baseou no Contrato 056/2022 (LINK), que versa sobre a contratação de licenças da fabricante Microsoft. Conforme o Primeiro Termo Aditivo deste Contrato (LINK), o licenciamento atual engloba 4809 usuários. O mesmo quantitativo pode ser observado ao consultar a coordenação de relacionamento (CORE) do STJ, que informou a atual alocação de licenças Microsoft conforme imagem abaixo:

 Office 365 E1	1567	1461	106
 Office 365 E3	3242	3170	72

5.1.4. Na imagem, têm-se licenças totais, atribuídas e disponíveis, respectivamente. Fazendo-se um somatório das licenças totais de usuários para Office 365 E1 e Office 365 E3: $1567 + 3242 = 4809$. Valor que está de acordo com as definições do primeiro termo aditivo do Contrato 056/2022.

5.1.5. Isto posto, esta equipe de planejamento da contratação estima a necessidade de 4809 licenças da solução de auditoria de ambiente Microsoft.

5.2. Para o CFJ:

5.2.1. Para uma estimativa assertiva da quantidade de usuários dos produtos MS, tomou-se como base o Contrato CJF n. 019/2023 (LINK), que versa sobre a contratação de licenças da fabricante Microsoft, que atualmente engloba licenciamento para 550 usuários.

6. REQUISITOS DE SUSTENTABILIDADE

6.1. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERANDO O CICLO DE VIDA DO OBJETO

6.1.1. Primeiramente, cabe avaliar aspectos que indiquem um resultado de contratação mais vantajoso, sob a perspectiva do STJ, considerando aspectos do ciclo de vida objeto. Nesse contexto, o ciclo de vida do objeto (software e serviço de manutenção), perpassa as seguintes fases:

1. desenvolvimento do produto (ideação, definição, design);
2. extração de matéria-prima e insumos;
3. processo produtivo;
4. logística (embalagens, transporte, comércio local);
5. consumo (real necessidade, quantitativos, durabilidade) e,
6. destinação final.

Na contratação em comento, cabe fazer as seguintes considerações:

Fases 1, 2, 3: do ponto de vista da produção, soluções de software não mais exigem objetos físicos para proporcionar a instalação e utilização do serviço. O acesso é concedido de forma digital através de uma chave de acesso. Assim, dada a imaterialidade do serviço de monitoramento e observabilidade a ser prestado, não se vislumbra impactos ambientais diretos comumente associados a fabricação de produtos como uso de recursos naturais, emissão de gases de efeitos estufa, geração de resíduos decorrente do processo de fabricação etc.

Fase 4: como se trata de licença de software, não haverá impactos associados a embalagens e transporte para uso do serviço. Todavia, quanto ao serviço de manutenção técnica, havendo necessidade de visitas presenciais, haverá custos ambientais associados ao transporte da equipe até as instalações do STJ.

Fase 5: por ser eminentemente digital, o maior impacto do serviço a ser adquirido está relacionado ao consumo de energia para a realização do monitoramento contínuo das aplicações. Todavia, considerando que esse é um serviço já prestado ao STJ, não se prevê consumo maior de energia.

Fase 6: por se tratar de um serviço digital, não se prevê a geração de resíduos. Quanto à manutenção, esta também se dá principalmente no bom funcionamento do software e sua compatibilidade com o hardware já existente. Assim, não se vislumbra a priori, a geração de resíduos significativa nas manutenções.

6.1.2. A CONTRATADA deverá adotar as normas federais, estaduais e distritais e declarar ter conhecimento da Política de Sustentabilidade do STJ, dando cumprimento aos dispositivos da [Instrução Normativa STJ/GDG n. 4 de 16 de janeiro de 2024](#). Os seus profissionais deverão estar informados sobre as boas práticas voltadas ao consumo consciente, à redução de desperdício e à coleta seletiva, com o objetivo de contribuir para a preservação do meio ambiente e dos recursos públicos.

7. REQUISITOS DE SEGURANÇA CIBERNÉTICA

- 7.1. **Controle de Acesso Granular:** a solução deve fornecer acesso granular à console, permitindo a definição de permissões específicas para usuários e grupos, limitando o acesso apenas ao necessário para realizar suas funções.
- 7.2. **Monitoramento de Atividades de Usuários:** deve ser capaz de monitorar e registrar atividades de usuários em tempo real, identificando comportamentos suspeitos ou não autorizados.
- 7.3. **Detecção de Ameaças Internas:** É essencial que a solução possa detectar e responder a ameaças internas, como acesso não autorizado por funcionários ou vazamento de dados.
- 7.4. **Auditoria e Relatórios de Segurança:** Deve oferecer recursos abrangentes de auditoria e geração de relatórios para ajudar na conformidade regulatória e na identificação de vulnerabilidades de segurança.
- 7.5. **Proteção de Dados Sensíveis:** deve identificar e proteger dados sensíveis contra acesso não autorizado ou vazamento.
- 7.6. **Monitoramento de Alterações em Permissões de Arquivos :** deve ser capaz de monitorar e registrar alterações nas permissões de arquivos e pastas, ajudando a evitar o acesso não autorizado.
- 7.7. **Criptografia de Dados em Repouso e em Movimento:** deve oferecer recursos de criptografia para proteger os dados tanto em repouso quanto em movimento, garantindo que eles permaneçam seguros, mesmo se forem interceptados.
- 7.8. **Integração com Soluções de Segurança Existente:** deve viabilizar a integração com outras soluções de segurança cibernética do STJ, possibilitando uma arquitetura de segurança em camadas.

- 7.9. **Atualizações e Suporte Contínuos:** deve oferecer atualizações regulares de segurança e suporte técnico abrangente para garantir que sua implementação permaneça protegida contra as últimas ameaças cibernéticas.
- 7.10. **Conformidade com Padrões de Segurança:** deve estar em conformidade com:
- 7.10.1. Instrução Normativa STJ/GDG nº 30 de 28 de novembro de 2023 - Institui a Política de Governança de Tecnologia da Informação e Comunicação do Superior Tribunal de Justiça.
 - 7.10.2. Resolução STJ/GDG nº 12 de 27 de abril de 2023 - Estabelece diretrizes para a Política de Segurança da Informação do Superior Tribunal de Justiça.
 - 7.10.3. Resolução nº 468 de 15/07/2022, Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ).
 - 7.10.4. Resolução CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).
 - 7.10.5. Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).
 - 7.10.6. Portaria Nº 162 de 10 de junho de 2021 (e anexos), que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).
 - 7.10.7. LGPD - Lei Geral de Proteção de Dados (Lei no 13.709/2018), e Marco Civil da Internet Lei no 12.965/2014.

8. SUBCONTRATAÇÃO

- 8.1. Não será permitida a subcontratação do objeto contratual.

9. EMPRESAS REUNIDAS EM CONSÓRCIO

- 9.1. Não será permitida a participação de empresas reunidas em consórcio, em decorrência de o objeto não possuir quantitativo, dimensões e especificações técnicas complexas que exijam a atuação de mais de uma empresa para prestação dos serviços, assim como não exigem a junção de esforços de segmentos distintos destinados à sua produção. Trata-se de serviços comumente comercializado por diversas empresas que atuam individualmente no mercado. Ademais, a experiência de licitações anteriores do mesmo objeto, em que não foi permitida a participação de empresas reunidas em consórcio, foi bem-sucedida e competitiva, a exemplo dos Pregões Pregões 43/2023 (3992839) e 14/2023 (3992849), entre outros

10. GARANTIA DA CONTRATAÇÃO

- 10.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei n. 14.133/21, no percentual de 3% sobre o valor anual do contrato, e condições descritas nas cláusulas do contrato.
- 10.1.1. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.
- 10.1.2. A garantia, nas modalidades caução, fiança bancária e título de capitalização, deverá ser prestada em até 10 (dez) dias úteis após a assinatura do contrato.
- 10.1.3. O contrato oferece maior detalhamento das regras que serão aplicadas à garantia da contratação.

11. FORMA DE ADJUDICAÇÃO

- 11.1. A adjudicação será realizada pelo critério de julgamento MENOR PREÇO POR LOTE, mediante realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, para registro de preços com fulcro no art. 3º, inciso III, do Decreto n. 11.462/2023.
- 11.2. A necessidade de agrupamento dos itens decorre por estarem intrinsecamente relacionados, já que se trata das licenças, instalação, parametrização, treinamento e serviços de apoio operacional, investigação e análise de alertas e comportamentos suspeitos.

12. DOCUMENTAÇÃO DE HABILITAÇÃO

12.1. A **habilitação técnica** será comprovada mediante apresentação dos seguintes documentos:

12.1.1. ATESTADO DE CAPACIDADE TÉCNICA DA EMPRESA:

12.1.1.1. Certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado ou, quando for o caso, regularmente emitidos pelo conselho profissional competente, ou, se implementado e regulamentado, o respectivo registro cadastral emitido na forma dos §§ 3º e 4º do art. 88 da Lei n. 14.133/2021, que demonstrem que a licitante já forneceu licenças de software, permanente ou por subscrição, referente a solução PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS PARA AMBIENTE ON-PREMISE ou AMBIENTE DE NUVEM (MICROSOFT SHAREPOINT ONLINE OU GOOGLE DRIVE OU AWS S3), incluindo serviços de parametrização, operacionalização e implantação, no quantitativo mínimo de: **2.000 (dois mil) usuários para o Lote 1 e 275 (duzentos e setenta e cinco) usuários para o Lote 2**, cujo(s) atestado(s) de capacidade técnica comprove fornecimentos de pelo menos um dos Itens 1 ou 2 (ou similar) para o Lote 1 e um dos Itens 5 ou 6 (ou similar) para o Lote 2 deste Termo de Referência, podendo ser aceito o somatório de atestados;

12.1.2. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

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

12.1.4. Os atestados de capacidade técnico-operacional deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

12.1.5. Os atestados apresentados poderão ser objeto de diligência a critério da Administração, para a verificação da autenticidade do conteúdo. Se encontrada divergência entre o especificado no atestado de capacidade e o apurado em eventual diligência, além da desclassificação no presente processo licitatório, fica sujeita às penalidades cabíveis.

12.2. A licitante deverá apresentar a documentação de habilitação jurídica, de habilitação fiscal, social e trabalhista e de qualificação econômico-financeira exigida no capítulo DA FASE DE HABILITAÇÃO do instrumento convocatório.

13. MODELO DE EXECUÇÃO DO OBJETO

13.1. A CONTRATADA deverá ter conhecimento e capacitação técnica para fornecer e prestar os serviços abaixo relacionados:

13.1.1. A execução do objeto consistirá no fornecimento de licenças, instalação e suporte técnico do fabricante conforme especificações contidas no [ANEXO I](#) deste documento;

13.1.1.1. Após a assinatura da ata de registro de preços, a solicitação de execução do objeto será requerida pelo gestor da contratação mediante pedido de compra e, após empenhamento, formalizada por contrato:

13.1.1.1.1. A CONTRATADA deverá comprovar o registro das licenças junto ao fabricante, em nome do STJ;

13.1.1.1.2. Para o **Lote 1**, o STJ irá requerer a execução integral do quantitativo de todos os itens;

13.1.1.1.3. Para o **Lote 2**, o CJF poderá requerer a execução integral do quantitativo de todos os itens durante a vigência da Ata.

13.1.1.2. Após recebimento do plano de implantação, nos termos do item anterior, a equipe técnica avaliará o plano no prazo de até 5 (cinco) dias úteis, que se manifestará pela aprovação ou rejeição por meio do termo de recebimento provisório;

13.1.1.3. Em caso de rejeição, a equipe técnica deve emitir parecer com as recomendações, que devem ser atendidas pela CONTRATADA em um novo plano de implantação no prazo de até 5 (cinco) dias corridos após recebimento do parecer de rejeição;

13.1.1.4. Somente após aprovação do plano pela equipe técnica será emitido termo de recebimento definitivo.

13.1.2. Entregar documento, definido como Plano de Implantação, que deverá conter cronograma da entrega, instalação e configuração dos produtos que fazem parte da solução contratada, previsão de recursos, pessoas envolvidas, atividades a serem desenvolvidas pelo CONTRATANTE e CONTRATADA e indicar os principais riscos e forma de mitigação, no prazo de 30 (trinta) dias corridos, a contar da assinatura do contrato;

- 13.1.3. As licenças que fazem parte da solução de auditoria deverão ser entregues no prazo máximo de 60 (sessenta) dias corridos a contar da assinatura do contrato.
- 13.1.4. Concluir, no prazo de até 30 (trinta) dias corridos, a contar da emissão do termo de recebimento definitivo do plano de implantação, a instalação e configuração da solução (item 3 do Lote 1 e item 8 do Lote 2 do objeto), em plena compatibilidade com o ambiente computacional do CONTRATANTE e em conformidade com a proposta técnica apresentada, cumprindo todas as demais cláusulas de garantia e atendimento técnico constantes deste Termo de Referência, nos prazos e termos estipulados;
- 13.1.4.1. A CONTRATADA seguirá as normas e procedimentos internos referentes à implementação de mudanças no ambiente de produção de TIC do STJ;
- 13.1.4.2. Os serviços de instalação e configuração da solução obedecerão às seguintes fases principais:

Atividade	Descrição	Responsável
1	Instalação da solução no ambiente do STJ	CONTRATADA
2	Configuração inicial da solução	CONTRATADA
3	Adequação de configurações da solução em uso para solução contratada;	CONTRATADA
4	Monitoramento inicial do funcionamento;	CONTRATADA e STJ
5	Recebimento definitivo;	STJ

- 13.1.5. Durante o prazo contratual, o CONTRATANTE deve ter direito de atualização de versões dos softwares fornecidos. Tal garantia faz parte dos itens 1 e 2 do Lote 1 e itens 6 e 7 do Lote 2 deste Termo de Referência;
- 13.1.6. Caso alguma versão de software tenha sido descontinuada pela fabricante, é responsabilidade da CONTRATADA realizar a atualização ou troca de produto por alternativa suportada pelo fabricante;
- 13.1.7. Durante o período contratual, a CONTRATADA deverá executar sem ônus adicionais a correção de falhas (bugs) de software;

13.1.8. O CONTRATANTE deverá ter direito a abertura de chamados diretamente junto ao fabricante, com quantidade ilimitada de solicitações. Tal direito advém dos itens 1 e 2 do Lote 1 e itens 6 e 7 do Lote 2 deste Termo de Referência;

13.1.9. A abertura de chamados com o fabricante deve ocorrer por meio de central de abertura de chamados 24x7, telefone, e-mail ou sítio dedicado;

13.1.10. Os chamados de suporte abertos com o fabricante deverão ser priorizados por nível de urgência conforme abaixo:

Se ve ri da de	Descrição	Tempo para início de atendim ento	Tempo para solução após o registro do chamado
1	Impacto crítico impossibilitando o uso do sistema, como: a) Interrupção total do funcionamento da solução; b) Falha de hardware. Fonte queimada. Refrigeração inadequada. Interface de rede sem conectividade. Problemas que requeiram troca de componentes ou do equipamento. c) Conexões intermitentes entre redes. Perdas significativas de pacotes;	até 60 minutos	Em até 12 (doze) horas
2	Impacto significativo prejudicando a operação do sistema, como: a) Perda de acesso à console de gerência sem interrupção do serviço. b) Indisponibilidade de acesso aos logs em tempo real;	até 90 minutos	Em até 24 (vinte e quatro) horas

3	Problemas ou dúvidas criando algumas restrições à operação do sistema, como: a) Erros durante a configuração de regras, criação de objetos, criação de perfis de segurança; b) Comportamento da solução em desacordo com o especificado na documentação técnica, que não causam interrupções mais limitam a utilização da solução;	até 120 minutos	Em até 48 (quarenta e oito) horas
4	Problemas ou dúvidas que não afetam a operação do sistema, como: a) Sanar dúvidas sobre configuração de recursos e funcionalidades da solução ofertada;	até 120 minutos	Em até 72 (setenta e duas) horas

13.1.11. O prazo para iniciar o atendimento se inicia a partir do instante do acionamento do suporte;

13.1.12. O atendimento das severidades 1 e 2 deverão ser prestadas de forma ininterrupta, ainda que o prazo para solução do problema avance sobre dia não útil;

13.1.13. O atendimento das severidades 3 e 4 descritas na tabela acima poderão ser transferidas para o próximo dia útil caso o prazo para solução do problema alcance dia não útil.

13.1.14. **Treinamento**

13.1.14.1. O início do treinamento ocorre após emissão do termo de recebimento definitivo da implantação e autorização por meio da emissão da ordem de serviço.

13.1.14.1.1. O início do treinamento deve ocorrer no prazo máximo de 15 (quinze) dias corridos após emissão da ordem de serviço.

13.1.14.2. O treinamento oficial do fabricante poderá ser realizado de forma remota (on-line) ou presencial, conforme solicitado pelo CONTRATANTE.

- 13.1.14.3. Após a solicitação do treinamento, a CONTRATADA terá o prazo de 7 (sete) dias úteis para apresentar o programa e o cronograma de treinamento.
- 13.1.14.4. Caso o CONTRATANTE solicite alterações no programa de treinamento, a CONTRATADA terá até 2 (dois) dias úteis para apresentação de uma nova versão do programa.
- 13.1.14.5. A CONTRATADA deverá realizar treinamento para uma turma com 10 (dez) servidores indicados pelo CONTRATANTE;
- 13.1.14.6. O treinamento deve ter carga horária mínima de 20 (vinte) horas.
- 13.1.14.7. O escopo do treinamento deve cobrir conceitos de configuração, operação, administração, gerência, otimização, resolução de problemas e gestão de todos os componentes da solução de forma que os servidores e colaboradores capacitados possam colocar a solução em produção, bem como planejar mudanças de configuração no ambiente considerando, ainda:
 - 13.1.14.7.1. O detalhamento dos componentes da solução, suas definições, suas interconexões e todas as informações técnicas necessárias ao seu pleno funcionamento e operação;
 - 13.1.14.7.2. A orientação sobre os componentes, procedimentos de instalação e administração das soluções, explorando todas as funcionalidades exigidas na especificação técnica do fabricante;
 - 13.1.14.7.3. A orientação sobre a topologia lógica da solução implantada;
 - 13.1.14.7.4. A carga horária máxima diária será de 8h (oito horas). O treinamento deverá ocorrer em dias úteis e em horário comercial;
 - 13.1.14.7.5. O treinamento deverá admitir mais participantes na condição de ouvintes (limitados a quatro ouvintes);

- 13.1.14.7.6. Deverá ser disponibilizado material didático em formato digital, sem custo adicional para o CONTRATANTE. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês);
- 13.1.14.7.7. Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa, carga horária e período de realização;
- 13.1.14.7.8. A CONTRATADA deverá aplicar um questionário de avaliação para preenchimento obrigatório de todos os participantes, previamente acordado com a fiscalização do contrato. Será considerado como satisfatório o percentual de aprovação acima de 70% (setenta por cento);
- 13.1.14.7.9. O questionário de avaliação será aplicado na última aula do treinamento;
- 13.1.14.7.10. Caso o treinamento oficial do fabricante não seja satisfatório em relação aos aspectos relacionados à carga horária, programa apresentado e estrutura, este deverá ser realizada novamente, sem ônus adicional ao CONTRATANTE;
- 13.1.14.7.11. O treinamento oficial do fabricante deverá ser realizado por técnicos qualificados e certificados pelo fabricante.

13.1.15. Serviço de apoio operacional, investigações análise de alertas e comportamentos suspeitos

- 13.1.15.1. O início da execução dos itens 5 e 10 ocorre após emissão do termo de recebimento definitivo da implantação e autorização por meio da emissão da ordem de serviço.
 - 13.1.15.1.1. A distribuição das quatro horas mensais ao longo do mês ficará a cargo do CONTRATANTE.
 - 13.1.15.1.2. O referido item deve ser executado e faturado mensalmente.

13.1.15.2. A CONTRATADA deverá prover o serviço de apoio operacional, investigação e análise de alertas e comportamentos suspeitos, com atendimento remoto para solução através profissional da CONTRATADA em horário a ser definido pela CONTRATANTE, podendo ser no período matutino ou vespertino não excedendo 4 (quatro) horas mensais.

13.1.15.3. O serviço consiste:

13.1.15.3.1. No fornecimento de informações e esclarecimentos solicitados pelo CONTRATANTE;

13.1.15.3.2. Em intervenções técnicas para solução de incidentes e problemas que estejam impactando a solução;

13.1.15.3.3. Em orientações técnicas sobre melhores práticas para uso da solução;

13.1.15.3.4. Em intervenções técnicas para parametrização e configuração da solução.

13.1.15.4. Este serviço não pode ser confundido com os serviços de suporte/garantia e manutenção, já contemplados na solução (fazem parte dos itens 1 e 2 do Lote 1 e itens 6 e 7 do Lote 2 da solução).

13.1.15.5. A CONTRATADA deverá prestar os serviços com duração de 1 (uma) hora semanal, compreendendo, mas não se limitando, ao seguinte escopo de atendimento da solução:

13.1.15.5.1. Identificar quem tem acesso à uma pasta;

13.1.15.5.2. Geração de relatório de conformidade técnica "health check";

13.1.15.5.3. Identificar que pasta determinado usuário tem permissão para acessar;

13.1.15.5.4. Identificar quais pastas um grupo global tem acesso;

13.1.15.5.5. Identificar permissões dos usuários de compartilhamento e NTFS nas pastas;

13.1.15.5.6. Identificar permissões dos grupos de compartilhamento e NTFS nas pastas;

- 13.1.15.5.7. Identificar pastas que contém dados sensíveis;
- 13.1.15.5.8. Identificar arquivos que contém dados sensíveis;
- 13.1.15.5.9. Identificar pastas com dados ociosos por mais de 90 dias;
- 13.1.15.5.10. Identificar proprietário de determinada pasta;
- 13.1.15.5.11. Visualizar eventos realizados dentro dos servidores de arquivos (Arquivos/Pastas abertos, modificados, criados, apagados e outros);
- 13.1.15.5.12. Recomendações e Modelagem;
- 13.1.15.5.13. Criar regras de classificação para dados sensíveis;
- 13.1.15.5.14. Identificar quem são os membros do grupo do AD;
- 13.1.15.5.15. Identificar que grupo determinado usuário pertence;
- 13.1.15.5.16. Identificar contas sem política de senha;
- 13.1.15.5.17. Identificar contas sem atividade de logon por mais de 90 dias;
- 13.1.15.5.18. Identificar contas ativadas sem expiração de senha;
- 13.1.15.5.19. Identificar contas desabilitadas;
- 13.1.15.5.20. Visualizar eventos realizados dentro do AD;
- 13.1.15.5.21. Remediação de contas de computador que são contas de administrador;
- 13.1.15.5.22. Identificar quem tem acesso à uma caixa de e-mail específica;
- 13.1.15.5.23. Identificar quais caixas de e-mail determinado usuário tem acesso;
- 13.1.15.5.24. Identificar quem tem acesso à uma pasta pública, e quais são essas pastas;
- 13.1.15.5.25. Visão completa e bidirecional das permissões;
- 13.1.15.5.26. A caixa de correio na qual a operação foi executada;

- 13.1.15.5.27. O item ou mensagem em que a operação foi executada (Sujeito, ID da mensagem da Internet, Horário de envio, Remetente, Destinatários (incluindo Cópia oculta), Tipo de item (e-mail, compromisso, tarefa, etc.), Anexos);
- 13.1.15.5.28. Em qual pasta da caixa de correio o item está localizado;
- 13.1.15.5.29. De qual cliente (Outlook/OWA) e versão do cliente o item foi enviado;
- 13.1.15.5.30. De qual endereço IP o item foi enviado;
- 13.1.15.5.31. Recomendações e Modelagem;
- 13.1.15.5.32. Identificação de propriedade de dados;
- 13.1.15.5.33. Detecção de notificação de atividade suspeita;
- 13.1.15.5.34. Investigar alertas através da dashboard;
- 13.1.15.5.35. Configurar e-mail, syslog ou snmp para recebimento de alerta;
- 13.1.15.5.36. Habilitar alertas importantes de segurança, como:
- 13.1.15.5.37. Comportamento anormal: acesso a uma quantidade incomum de dados confidenciais ociosos;
- 13.1.15.5.38. Atividade de criptografia detectada;
- 13.1.15.5.39. Ataque de downgrade de criptografia;
- 13.1.15.5.40. Criptografia de múltiplos arquivos;
- 13.1.15.5.41. Arquivo criptografado por ransomware;
- 13.1.15.5.42. Padrão imediato detectado: as ações do usuário se assemelham a ransomware;
- 13.1.15.5.43. Falha de operação em uma ferramenta de exploit;
- 13.1.15.5.44. Possível escalção de privilégio;
- 13.1.15.5.45. Suspeita de ataque de força bruta;
- 13.1.15.5.46. Possível replicação do AD;

13.1.15.5.47. Visualizar trilha de auditoria a partir do alerta;

13.1.15.6. A CONTRATADA deverá disponibilizar profissional qualificado na solução para o atendimento.

13.1.15.7. O profissional da CONTRATADA, o qual será responsável pelo apoio operacional, deverá possuir certificação do fabricante para realização atendimento.

13.1.15.8. O profissional da CONTRATADA deverá propor e tomar as ações necessárias para o ambiente do CONTRATANTE seguindo as melhores práticas do fabricante.

13.1.15.9. O profissional deverá apoiar a equipe do CONTRATANTE com emissão de relatórios da solução, com intuito de melhoria contínua do ambiente.

13.1.15.10. A CONTRATADA deverá emitir relatório mensal com as atividades realizadas ao longo do mês em questão, que será utilizado como meio para os atestes mensais da efetiva realização do serviço de apoio operacional.

13.1.16. Cronograma de Execução

E T A P A S	DESCRIÇÃO	PRAZO
	1 Reunião de alinhamento	Até 15 (quinze) dias corridos após assinatura do contrato
	2 Entregar Plano de Implantação	Até 30 (trinta) dias corridos, a contar da assinatura do contrato
	3 Entregar as licenças da solução (itens 1 e 2 do Lote 1 e itens 6 e 7 do Lote 2)	Até 60 (sessenta) dias corridos a contar da assinatura do contrato
	4 Emitir termo de recebimento provisório referente à entrega das licenças (itens 1 e 2 do Lote 1 e itens 6 e 7 do Lote 2) e plano de implantação e treinamento (item 4 do Lote 1 e item 9 do Lote 2)	Até 5 (cinco) dias úteis, contados da entrega das licenças, do plano de implantação e do encerramento do treinamento
	5 Instalação e configuração (item 3 do Lote 1 e item 8 do Lote 2)	Até 30 (trinta) dias corridos, a contar da emissão do termo de recebimento definitivo do plano de implantação

6	Emitir termo de recebimento provisório referente ao item 3	Até 5 (cinco) dias úteis, contados da entrega da implantação
7	Emitir termo de recebimento definitivo referente à instalação e configuração (item 3 do Lote 1 e item 8 do Lote 2) e plano de implantação	Até 5 (cinco) dias úteis, contados da finalização do recebimento provisório do plano de implantação e da implantação
8	Emitir termo de recebimento definitivo referente à entrega das licenças (itens 1 e 2 do Lote 1 e itens 6 e 7 do Lote 2)	Até 5 (cinco) dias úteis, a contar da emissão do termo de recebimento definitivo da implantação
9	Realizar treinamento	Até 15 dias corridos após emissão da Ordem de Serviço
10	Emitir termo de recebimento definitivo do Treinamento (item 4 do Lote 1 e item 9 do Lote 2)	Até 5 (cinco) dias úteis, após confirmação da finalização do treinamento e entrega da lista de presença
11	Iniciar serviço de apoio operacional (item 5 do Lote 1 e item 10 do Lote 2)	Imediatamente após a emissão do Termo de Recebimento Definitivo do item 3 do Lote 1 e item 8 do Lote 2

14. GARANTIA OU ASSISTÊNCIA TÉCNICA

- 14.1. O prazo de garantia técnica dos serviços executados, incluindo a garantia legal, será de, no mínimo, 24 (vinte e quatro) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.
- 14.2. A garantia será prestada com vistas a manter os softwares fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o CONTRATANTE.
- 14.3. A garantia abrange a realização da manutenção corretiva dos softwares pela própria CONTRATADA, ou, se for o caso, por meio de assistência autorizada pelo próprio fabricante, de acordo com as normas técnicas específicas.
- 14.4. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos softwares, compreendendo correção de "bugs", atualizações de segurança e demais correções necessárias.

- 14.5. A garantia técnica contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

15. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

- 15.1. A avaliação da execução do objeto consiste na verificação da sua conformidade com a especificação e os prazos estabelecidos neste termo de referência e na proposta da CONTRATADA, bem como com o quantitativo requerido na ordem de serviço.
- 15.2. Para fins de pagamento, também serão considerados os seguintes critérios de aferição da execução contratual:
- a) o fornecimento dos quantitativos formalizados no contrato oriundo da execução da ata de registro de preços;
 - b) os serviços de instalação, configuração e repasse de conhecimento; e
 - c) o registro das licenças junto ao fabricante, em nome do STJ.
- 15.3. A avaliação da execução dos itens 1 e 2 do Lote 1 e item 6 e 7 do Lote 2 utilizará a verificação do cumprimento do Acordo Mínimo de Serviço (ANS) para os serviços continuados de garantia, manutenção e suporte técnico e, na hipótese de não cumprimento, sofrerá a aplicação de multa, conforme regras dispostas no Capítulo [21](#).

Inconformidade	Referência	Pontuação
Violação de prazo para início de atendimento para solicitações de severidade 1	A cada hora violada	4
Violação de prazo para início de atendimento para solicitações de severidade 2	A cada hora violada	3
Violação de prazo para início de atendimento para solicitações de severidade 3	A cada hora violada	2
Violação de prazo para início de atendimento para solicitações de severidade 4	A cada hora violada	1

- 15.4. Para avaliação do item 5 do Lote 1 e item 10 do Lote 2, será indicada glosa de 10% sobre o valor mensal, pela hora de serviço de apoio a investigação, análise de alertas e comportamentos suspeitos não prestado no mês.
- 15.4.1. Na hipótese de não cumprimento de no mínimo 3 (três) horas de serviços no mês, será aplicada multa, conforme regras dispostas no Capítulo [21](#).

15.5. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

- i. não produziu os resultados acordados,
- ii. deixou de executar, ou não executou com a qualidade mínima exigida as atividades contratadas; ou
- iii. deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

16. RECEBIMENTO DO OBJETO

16.1. Os itens 1 e 2 do Lote 1 e itens 6 e 7 do Lote 2 serão recebidos **provisoriamente**, após confirmação da entrega dos itens, pelos fiscais técnico e administrativo, mediante termos detalhados, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

16.1.1. As licenças serão recebidas provisoriamente no prazo de 5 (cinco) dias úteis, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

16.1.1.1. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

16.1.1.2. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

16.1.1.3. O prazo da disposição acima será contado do recebimento de comunicação formal do fim da entrega das licenças.

16.2. O item 3 do Lote 1 e o item 8 do Lote 2 serão recebidos **provisoriamente**, no prazo de 5 (cinco) dias úteis a contar da comunicação formal da CONTRATADA do término da implantação, pelos fiscais técnico e administrativo, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

- 16.3. O item 4 do Lote 1 e o item 9 do Lote 2 serão recebidos **provisoriamente**, no prazo de 5 (cinco) dias úteis a contar da comunicação formal da CONTRATADA do término do treinamento, pelos fiscais técnico e administrativo, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.
- 16.4. Os serviços previstos no item 5 do Lote 1 e item 10 do Lote 2, serão recebidos **provisoriamente**, no prazo de 5 (cinco) dias úteis, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo, da seguinte forma:
- 16.4.1. Relatório de manutenções executadas no mês de referência, emitido pela CONTRATADA até o 5º (quinto) dia útil do mês subsequente, contendo o histórico das manutenções corretivas, diagnóstico e recomendações resultantes das preventivas e estatísticas de desempenho e capacidade no período.
- 16.4.2. O fiscal técnico emitirá o Relatório de Atividades Mensais, no prazo de 5 (cinco) dias úteis a contar do recebimento do relatório da CONTRATADA, com a conferência de execução e recomendações das atividades. Após, o fiscal técnico o submeterá ao fiscal requisitante para análise dos resultados, proposição de descontos, quando for o caso, e aprovação dos serviços; e, ao fiscal administrativo, para análise do cumprimento das exigências de caráter administrativo.
- 16.4.3. Aprovado pelos fiscais técnico, requisitante e administrativo, o Relatório de Atividades Mensais, que será considerado, para todos os efeitos, o termo de recebimento provisório e será encaminhado, pelo fiscal requisitante, para ciência da CONTRATADA para aprovação e emissão da nota fiscal do valor apurado pela fiscalização.
- 16.4.4. O fiscal técnico do contrato realizará o recebimento provisório do objeto relativo ao cumprimento das exigências de caráter técnico.
- 16.4.5. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato no que se refere ao cumprimento das exigências de caráter administrativo.

16.4.6. Para efeito de recebimento provisório, ao final de cada período de faturamento, os fiscais técnico e requisitante do contrato irão apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à CONTRATADA, registrando no Relatório de Atividades Mensais a ser encaminhado ao gestor do contrato, observados os seguintes procedimentos:

i. será considerado como ocorrido o recebimento provisório com a entrega do Relatório de Atividades Mensais ou, em havendo mais de um a ser feito, com a entrega do último;

ii. a CONTRATADA fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Relatório de Atividades Mensais;

iii. o recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

16.5. As licenças dos itens 1 e 2 do Lote 1 e itens 6 e 7 do Lote 2 serão recebidos **definitivamente** no prazo de 5 (cinco) dias úteis, a contar do recebimento provisório do item 3 do Lote 1 e item 8 do Lote 2, por comissão designada pelo Secretário de Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado, comunicando-se à empresa que emita a Nota Fiscal ou Fatura.

16.6. O recebimento **definitivo** dos itens 3 e 4 do Lote 1 e itens 8 e 9 do Lote 2 ocorrerá no prazo de 5 (cinco) dias úteis, a contar do recebimento provisório do item 3 do Lote 1 e item 8 do Lote 2, por comissão designada pelo secretário de Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado, comunicando-se à empresa que emita a Nota Fiscal ou Fatura.

- 16.7. Os serviços do item 5 do Lote 1 e item 10 do Lote 2 serão recebidos **definitivamente** pelo gestor do contrato, no prazo de 5 (cinco) dias úteis, a contar do recebimento da fatura, acompanhada do Relatório de Atividades Mensais aprovado pela fiscalização, mediante termo que ateste a qualidade dos serviços prestados e consequente aceitação mediante termo detalhado, comunicando a empresa para que emita a Nota Fiscal ou Fatura com o valor exato dimensionado pela fiscalização.
- 16.8. O objeto poderá ser rejeitado, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituído no prazo de 5 (cinco) dias úteis, a contar da notificação da CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades
- 16.9. No caso de controvérsia sobre a execução do objeto, quanto à qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei n. 14.133, de 2021, comunicando-se à empresa para que emita a Nota Fiscal no que se refere à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.
- 16.10. O prazo para a solução, pela CONTRATADA, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela equipe de fiscalização durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.
- 16.11. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.
- 16.12. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens da contratação nem a responsabilidade ético-profissional pela perfeita execução do contrato.

17. FATURAMENTO, LIQUIDAÇÃO E PAGAMENTO

17.1. LIQUIDAÇÃO

- 17.1.1. Recebida a Nota Fiscal ou documento de cobrança equivalente e, se for o caso, os demais documentos exigidos para o recebimento do objeto, ocorrerá o prazo de 10 (dez) dias úteis para fins de liquidação, prorrogáveis por igual período, nos termos do art. 7º, §3º, da [Instrução Normativa SEGES/ME n. 77/2022](#).

- 17.1.1.1. No prazo de que trata o *caput* anterior estão computados os prazos de recebimento definitivo do objeto estabelecidos nos itens [16.5.16.6](#) e [16.7](#) deste documento.
- 17.1.1.2. O prazo de que trata o *caput* será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei n. 14.133, de 2021.
- 17.1.2. Recebida a Nota Fiscal ou documento de cobrança equivalente e, se for o caso, os demais documentos exigidos para o recebimento do objeto, ocorrerá o prazo de 10 (dez) dias úteis para fins de liquidação, prorrogáveis por igual período, nos termos do art. 7º, §3º, da [Instrução Normativa SEGES/ME n. 77/2022](#).
- 17.1.3. Para fins de liquidação, o gestor encaminhará o processo de pagamento à Secretaria de Orçamento e Finanças, que será responsável por verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:
1. o prazo de validade;
 2. a data da emissão;
 3. os dados do contrato e do órgão CONTRATANTE;
 4. o período respectivo de execução do contrato;
 5. o valor a pagar; e
 6. eventual destaque do valor de retenções tributárias cabíveis.
- 17.1.4. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, o processo de pagamento será restituído ao gestor, o qual manterá a nota fiscal sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao CONTRATANTE.
- 17.1.5. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta *on-line* ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no [art. 68 da Lei n. 14.133, de 2021](#).

- 17.1.6. A Administração verificará as Certidões Negativas de Débito da Receita Federal, de Regularidade do FGTS e a Negativa Trabalhista e a existência de ocorrências impeditivas diretas no SIAFI, todos requisitos relacionados à manutenção das condições exigidas para a habilitação na licitação.
- 17.1.7. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, o gestor providenciará sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do gestor.
- 17.1.8. Persistindo a irregularidade, o gestor comunicará a Secretaria de Administração para que sejam adotadas as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.
- 17.1.9. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.

17.2. PRAZO DE PAGAMENTO

- 17.2.1. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme item anterior, e do recebimento dos autos na seção responsável pela emissão dos documentos de pagamento no SIAFI.
- 17.2.2. O inadimplemento do pagamento na data aprazada, conforme disposto no subitem anterior, desde que motivado pelo CONTRATANTE, acarretará a atualização monetária do valor devido à CONTRATADA, calculada *pro rata tempore*, até a data do efetivo pagamento, com base no último percentual divulgado do Índice Nacional de Preços ao Consumidor Amplo - IPCA.

17.3. FORMA DE PAGAMENTO

- 17.3.1. Para os itens 1, 2, 3 e 4 do Lote 1 e itens 6, 7, 8 e 9 do Lote 2, o pagamento será realizado no valor total da parcela executada após a liquidação da despesa do objeto, por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pela CONTRATADA.

- 17.3.1.1. As soluções avaliadas são comercializadas na forma de licenças pagas antecipadamente ou mensal aos fabricantes. A forma de pagamento, pode ser mensal, bianual ou pagamento único. Quanto maior o prazo, menor será o custo por ano. O pagamento mensal mostrou-se mais onerosa, sendo mais vantajoso o pagamento único. Qualquer outra forma de pagamento será mais onerosa, pois as licitantes irão repassar os custos de financiamento.
- 17.3.1.2. Caso o objeto não seja executado, a CONTRATADA deverá devolver o valor antecipado, corrigido monetariamente conforme regra constante deste Termo de Referência, sem prejuízo da aplicação das sanções cabíveis.
- 17.3.2. As licenças dos itens 1 e 2 do Lote 1 e itens 6 e 7 do Lote 2 e os serviços dos 3 e 4 do Lote 1 e 8 e 9 do Lote 2 devem ser pagos após emissão do termo de recebimento definitivo.
- 17.3.3. O item 5 do Lote 1 e item 10 do Lote 2 que trata de serviço de apoio operacional, investigação e análise de alertas e comportamentos suspeitos será pago mensalmente, após a liquidação da despesa, por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pela CONTRATADA.
- 17.3.3.1. O faturamento deverá ser mensal, mediante a apresentação da nota fiscal consolidada, determinando-se o valor total aprovado pelo CONTRATANTE no relatório mensal de atividades, descontando-se as deduções aplicadas em função do não atendimento dos níveis de serviços definidos neste termo de referência.
- 17.3.3.2. Para todas as propostas de deduções do valor mensal, será obrigatório o resumo descritivo do fator incidente e, quando for o caso, serem anexadas as documentações comprobatórias de não atendimento dos resultados exigidos e/ou do não atendimento das atividades acordadas pelo CONTRATANTE.
- 17.3.3.3. As deduções deverão ser aplicadas quando não atenderem ao resultado esperado e/ou quando a ordem de serviço não for concluída dentro do prazo previsto.

- 17.3.3.4. A CONTRATADA deverá ser comunicada, por meio do relatório mensal de serviços, informando o total a ser faturado, assim como as deduções e descontos aplicados, devendo a mesma apor a ciência e devolver ao Gestor juntamente com a nota fiscal.
- 17.3.4. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- 17.3.5. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
- 17.3.5.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.
- 17.3.6. O contratado regularmente optante pelo Simples Nacional, nos termos da [Lei Complementar nº 123, de 2006](#), não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

18. OBRIGAÇÕES DA CONTRATADA

- 18.1. Além de cumprir as condições estabelecidas neste termo de referência e na minuta de contrato, a CONTRATADA deverá:
- 18.1.1. Executar fielmente o objeto contratado, de acordo com as normas legais, em conformidade com a proposta apresentada e as orientações do CONTRATANTE, observando sempre os critérios de qualidade;
- 18.1.2. Fornecer a solução objeto desta contratação atendendo às especificações técnicas contidas no [ANEXO I.](#), com garantia e suporte técnico durante toda vigência contratual.
- 18.1.3. Assegurar que os serviços de instalação e configuração da solução sejam executados por técnicos certificados pelos fabricantes dos produtos, devendo ser apresentada a correspondente documentação de certificação;
- 18.1.4. Fornecer, a qualquer momento, todas as informações pertinentes ao objeto que o CONTRATANTE julgue necessário conhecer ou analisar;

- 18.1.5. Submeter seus empregados, durante a permanência nas dependências do CONTRATANTE, aos regulamentos de segurança e disciplina por este instituído, dando-lhes conhecimento formal, em especial, da Política de Prevenção e Combate do Assédio Moral, do Assédio Sexual e de todas as formas de discriminação, disposta na Instrução Normativa STJ/GP n. 17 de 14 de abril de 2023, e das regras constantes do Código de Conduta do Superior Tribunal de Justiça;
- 18.1.6. Comunicar ao CONTRATANTE, no caso de atualização de versão de qualquer dos itens contratados, que esta encontra-se disponível para *download* no sítio do fabricante;
- 18.1.7. Testar todos os serviços depois de concluídos, na presença da área demandante e/ou da fiscalização do CONTRATANTE, ficando sua aceitação final dependente das características do desempenho apresentado;
- 18.1.8. Executar a configuração complementar da solução, de acordo com o cronograma, auxiliando e acompanhando a equipe técnica do CONTRATANTE;
- 18.1.9. Disponibilizar número telefônico do fabricante, com atendimento ininterrupto 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, para fins de abertura de chamados técnicos, assim como para acompanhamento da solução de problemas;
- 18.1.10. Para atividades que não possuam rotinas e processos proativos normatizados, deverão ser analisadas junto com o CONTRATANTE as melhores maneiras de ativação e/ou desempenho dos serviços, executando, após autorização, as implantações necessárias e os processos de controle até que a solução esteja totalmente funcional;
- 18.1.11. Realizar todos os trabalhos sem que haja a necessidade de parada do ambiente em produção, exceto aquelas predeterminadas com a equipe do CONTRATANTE. Do mesmo modo, deverão ser observadas as rotinas internas do STJ e CJP, cujo andamento em hipótese nenhuma deverá ser prejudicado em razão de quaisquer das atividades acima mencionadas;
- 18.1.12. Manter em ambiente virtual controlado, os registros individuais rastreáveis de tratamento realizados, com cada acesso, data, horário, para responsabilização, em caso de eventuais omissões, desvios ou abusos.

18.1.12.1. Na hipótese do disposto acima, os bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pelo Tribunal nas hipóteses previstas na LGPD.

18.1.13. A CONTRATADA se responsabilizará:

18.1.13.1. Pelas ações e recomendações de seus analistas e consultores, bem como pelos efeitos delas advindos, na execução do objeto contratado e por ocasião dos acessos, privilégios ou informações obtidas em função das atividades por estes executados;

18.1.13.2. Pelos danos causados ao STJ ou a terceiros, decorrentes de sua culpa ou dolo, não excluindo ou reduzindo essa responsabilidade à fiscalização ou o acompanhamento da entrega dos insumos pelo CONTRATANTE;

18.1.14. A CONTRATADA assumirá, sem que haja responsabilização do CONTRATANTE, todos os encargos, tributos e multas, devendo:

18.1.14.1. Arcar com todas as despesas relativas à execução dos serviços, tais como mão de obra, ferramentas, equipamentos, taxas, emolumentos, encargos sociais;

18.1.14.2. Arcar com as despesas decorrentes de qualquer infração cometida por seus recursos e corpo técnico, inclusive com os descontos previstos, quando da execução dos serviços especificados neste Termo de Referência.

18.1.15. Assumir a responsabilidade por:

18.1.15.1. Todos os encargos fiscais e comerciais resultantes desta contratação;

18.1.15.1.1. A inadimplência da CONTRATADA, com referência aos encargos estabelecidos no item anterior, não transfere à Administração do CONTRATANTE a responsabilidade de pagamento, nem pode onerar o objeto deste contrato, razão pela qual a CONTRATADA renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o CONTRATANTE.

- 18.1.15.2. Pelo pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais, em consequência de fato a ela imputável e relacionada com a execução do objeto deste contrato;
 - 18.1.15.3. Pelos materiais, produtos, ferramentas, instrumentos e equipamentos disponibilizados para a execução dos serviços, não cabendo ao CONTRATANTE qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer;
 - 18.1.15.4. Por todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios, resultantes de ações judiciais que o CONTRATANTE for compelida a responder por força desta contratação.
- 18.2. A CONTRATADA não poderá, em nenhuma hipótese, efetuar mudanças nas características técnicas da solução, definidas pelo fabricante, a fim de atender as especificações desse projeto.
- 18.3. Garantir o direito de uso da solução objeto da contratação, acompanhado dos respectivos manuais de instalação e de utilização em meio eletrônico ou impresso, disponibilizados na língua portuguesa ou inglesa.
- 18.4. Executar os procedimentos de instalação e configuração em conformidade com as recomendações do fabricante, documentações existentes e as boas práticas de mercado, e também de acordo com o que consta no [ANEXO I.4.](#) deste Termo de Referência;

19. OBRIGAÇÕES DO CONTRATANTE

- 19.1. Além de exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, deverá o CONTRATANTE:
- 19.1.1. Proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais, inclusive permitir o acesso de representantes, prepostos ou empregados da CONTRATADA às dependências do CONTRATANTE, observadas as normas de segurança institucional do Tribunal;

- 19.1.2. Emitir decisão sobre reajustamento de preços e reequilíbrio econômico-financeiro, respectivamente, nos prazos de 39 e de 76 dias úteis, e sobre as demais solicitações e reclamações relacionadas à execução do presente contrato, no prazo de noventa dias corridos, todos os prazos a contar da data do protocolo do requerimento, admitida a prorrogação motivada por igual período, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do contrato;
- 19.1.2.1. O referido prazo ficará suspenso enquanto a CONTRATADA não cumprir as diligências do CONTRATANTE.
- 19.1.3. Receber o objeto no prazo e condições estabelecidas;
- 19.1.4. Notificar a CONTRATADA, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para ser por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;
- 19.1.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela CONTRATADA;
- 19.1.6. Efetuar o pagamento à CONTRATADA do valor incontroverso correspondente à execução do objeto, no prazo, forma e condições estabelecidas neste termo de referência;
- 19.1.7. Aplicar à CONTRATADA as sanções previstas na lei, no instrumento convocatório e neste termo de referência;
- 19.1.8. Cientificar o órgão de representação judicial para adoção das medidas cabíveis quando do descumprimento de obrigações pela CONTRATADA;
- 19.1.9. Notificar os emitentes das garantias contratuais, quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

20. DA PROTEÇÃO DE DADOS

- 20.1. Assinar TERMO DE CONFIDENCIALIDADE, na forma do [ANEXO II](#), sobre todos os dados acessados no STJ, a ser emitido pelo CONTRATANTE, no qual estará expresso a responsabilidade pelos atos praticados pelos profissionais que, sob a responsabilidade da CONTRATADA, prestarem os serviços.
- 20.2. A CONTRATADA terá acesso somente a endereços IP, logs, queries e métricas que não possuem dados pessoais ou sigilosos.

- 20.3. Adotar boas práticas de governança que estabeleçam as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais, levando em consideração a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos decorrentes de tratamento de dados de titulares.
- 20.4. Declarar ter conhecimento da Política de Segurança do STJ, da Política de Proteção de Dados Pessoais do STJ e do Código de Conduta do STJ, dando cumprimento aos dispositivos desses normativos. Deverá coletar a ciência dos seus empregados em relação a essas normas a partir do início da atuação deles na execução dos serviços da presente contratação, de manter estrita observância às normas internas e à Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- 20.5. Realizar o tratamento de dados pessoais conforme instruções fornecidas pelo CONTRATANTE, além de manter estrita observância às normas internas e à Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

21. INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

- 21.1. Sem prejuízo da incidência de outras disposições previstas no instrumento convocatório, na hipótese de falha na execução do contrato, a CONTRATADA fica sujeita à:

21.1.1. **Advertência**, quando a CONTRATADA der causa à inexecução parcial de obrigação contratual principal ou acessória de pequena relevância, caso não se justifique a imposição de penalidade mais grave, nos termos do art. 156, § 2º, da Lei 14.133/2021.

21.1.2. **Multa moratória:**

21.1.2.1. de **0,5%** por dia de atraso na entrega das licenças, sobre o valor da parcela executada em desconformidade com o prazo previsto neste termo de referência, até o limite de trinta dias;

21.1.2.2. de **0,5%** por dia de atraso na execução do item 3 do Lote 1 e item 8 do Lote 2, sobre o valor da parcela executada em desconformidade com o prazo previsto neste termo de referência, até o limite de trinta dias;

- 21.1.2.3. de **0,5%** por dia de atraso na entrega do plano de implantação de que trata o item [13.1.1.](#) , sobre o valor da parcela executada em desconformidade com o prazo previsto neste termo de referência, até o limite de trinta dias;
- 21.1.2.4. de **1,5%** por dia de atraso para início do item 4 do Lote 1 e item 9 do Lote 2, sobre o valor da parcela executada em desconformidade com o prazo previsto neste termo de referência, até o limite de trinta dias;
- 21.1.2.5. de **10%** sobre o **valor da parcela não cumprida**, em caso de reincidência pelo descumprimento dos níveis de serviços de severidade 1;
- 21.1.2.6. de **5%** sobre o **valor da parcela não cumprida**, em caso de reincidência por 3 vezes consecutivas, pelo descumprimento dos níveis de serviços de severidade 2;
- 21.1.2.7. de **3%** sobre o **valor da parcela não cumprida**, em caso de reincidência por 4 vezes consecutivas, pelo descumprimento dos níveis de serviços de severidade 3;
- 21.1.2.8. de **1%** sobre o **valor da parcela não cumprida**, em caso de reincidência por 5 vezes consecutivas, pelo descumprimento dos níveis de serviços de severidade 4;
- 21.1.2.9. de **5%** sobre o **valor total do item 5 do Lote 1 e item 10 do Lote 2**, pelo descumprimento da prestação do serviço por mais de 3 (três) horas no mês;
- 21.1.2.10. A aplicação de multa de mora não impedirá que a Administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções previstas.

21.1.3. Multa compensatória:

- 21.1.3.1. de **20%** sobre o **valor da parcela não cumprida**, no caso de inexecução parcial do objeto, caso haja interesse do CONTRATANTE na continuidade da execução do contrato, observado que o valor final apurado para a multa não poderá ser inferior a 0,5% do valor total do contrato, nos termos do § 3º do art. 156 da Lei n. 14.133/2021;

21.1.3.2. de **30%** sobre o **valor total do contrato**, no caso de **inexecução parcial ou total do objeto**, caso não haja interesse do **CONTRATANTE** na continuidade da execução do contrato em razão de descumprimento pela CONTRATADA de qualquer das condições avençadas, o que ensejará a extinção do contrato, conforme dispõe o inciso I do art. 138 da Lei n. 14.133, de 2021.

22. MODELO DE GESTÃO DA CONTRATAÇÃO

- 22.1. Esta contratação deverá ser executada fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei n. 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.
- 22.2. As comunicações entre o CONTRATANTE e a CONTRATADA devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
- 22.3. Após a assinatura da ata de registro de preço e do contrato, o CONTRATANTE poderá convocar, a critério da equipe de gestão da contratação, o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.
- 22.4. A reunião inicial contará com a presença do gestor, dos fiscais técnico, requisitante e administrativo e dos membros da comissão de recebimento definitivo, cuja pauta observará o seguinte:
- a) apresentação do preposto da empresa;
 - b) entrega do termo de compromisso e termo de ciência;
 - c) prestação de esclarecimentos relativos a questões operacionais, administrativas e de gestão de contrato;
 - d) repasse à contratada dos conhecimentos necessários à execução dos serviços;
 - e) registro da reunião em ata.
- 22.5. O CONTRATANTE poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

22.6. A equipe de gestão do CONTRATANTE será composta por gestor e fiscais técnico, requisitante, administrativo e comissão de recebimento designados pelo secretário de Administração do STJ, os quais adotarão as orientações do Manual de Fiscalização e Gestão de Contratos do STJ e, no âmbito do CJF, dos normativos internos daquele órgão.

22.6.1. No âmbito do STJ:

22.6.1.1. A fiscalização técnica caberá a servidor a ser indicado pela Coordenadoria de Segurança da Informação e Defesa Cibernética - CSID.

22.6.1.2. A fiscalização requisitante caberá ao titular da Coordenadoria de Segurança da Informação e Defesa Cibernética - CSID.

22.6.1.3. A fiscalização administrativa caberá a servidor a ser indicado pela Seção de Monitoramento e Planejamento de Contratos de TIC - SMTIC.

22.6.1.4. A gestão do contrato caberá a servidor a ser indicado pela Seção de Gestão de Contratações de TIC - SCONT;

22.6.1.5. A comissão de recebimento definitivo será composta por servidores indicados pela Coordenadoria de Segurança da Informação e Defesa Cibernética - CSID.

22.6.1.6. A equipe de gestão da contratação também contará com comissão de recebimento designada pelo Secretário de Administração.

22.6.2. No âmbito do CJF, a equipe de fiscalização e gestão da contratação será designada pela autoridade competente daquele órgão.

22.7. PREPOSTO

22.7.1. A CONTRATADA designará formalmente o preposto da empresa, antes do início da prestação dos serviços, para atuar como seu representante e interlocutor autorizado a receber, encaminhar e responder questões técnicas, legais e administrativas referentes à presente contratação.

22.7.2. O CONTRATANTE poderá solicitar a substituição do preposto indicado que não atenda satisfatoriamente às necessidades da execução contratual.

22.8. GESTOR

- 22.8.1. O gestor coordenará a fiscalização da execução da ata de registro de preços e do contrato, da avaliação da qualidade e dos resultados obtidos, bem como do registro de informações atualizadas que viabilizem a tomada de decisão relacionada à formalização dos procedimentos de prorrogação, reequilíbrio, alteração, pagamento, eventual aplicação de sanções e extinção do contrato.
- 22.8.2. Caberá ao gestor, além das demais atribuições estabelecidas no Manual de Fiscalização e Gestão de Contratos do STJ e, no âmbito do CJF, dos seus normativos internos:
- 22.8.2.1. Emitir ordens de serviço e solicitar à CONTRATADA a correção de pendências constatadas na execução do contrato;
 - 22.8.2.2. Avaliar eventuais atrasos nos prazos de entrega ou ocorrências que possam gerar dificuldades à conclusão do objeto contratado e submetê-las à autoridade superior para deliberação;
 - 22.8.2.3. Zelar pelo fiel cumprimento do objeto contratado sob sua supervisão e, sempre que requerido, submeter previamente à deliberação da Secretaria de Administração pedido de modificação/alteração de projeto ou de fornecimento, que deverá ser encaminhado com a justificativa da CONTRATADA, mediante apresentação de documento comprobatório dos fatos alegados, e a manifestação do gestor;
 - 22.8.2.4. Devolver, mediante justificativa e notificação formal, nota fiscal apresentada pela CONTRATADA quando for observada irregularidade que inviabilize o ateste e pagamento do serviço/fornecimento prestado;
 - 22.8.2.5. Acompanhar os resultados alcançados em relação à execução da obrigação do contrato para receber e atestar as notas fiscais e encaminhá-las à unidade competente para pagamento, após conferência completa da documentação exigida no contrato;
 - 22.8.2.6. Acompanhar a manutenção das condições de habilitação da CONTRATADA, para fins de empenho de despesa e de pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

- 22.8.2.7. Informar à Secretaria de Administração, tempestivamente, o descumprimento contratual por parte da CONTRATADA e sugerir a aplicação das sanções previstas no instrumento convocatório e/ou no contrato, conforme orientações contidas na Instrução Normativa STJ/GDG n. 10/2023 e nos normativos internos do CJF, conforme o caso;
- 22.8.2.8. Confeccionar e assinar o termo de recebimento definitivo do item 5 do Lote 1 e item 10 do Lote 2, com base nas informações produzidas no recebimento provisório, mediante termo detalhado que comprove o atendimento das exigências contratuais no prazo estabelecido neste termo de referência;
- 22.8.2.9. Elaborar o relatório final para divulgação no Portal Nacional de Contratações Públicas (PNCP) com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.
- 22.8.2.10. Na gestão da ata de **registro de preços**, caberá ao gestor:
- 22.8.2.10.1. Solicitar a contratação do objeto, mediante a apresentação do pedido de compra, indicando o número da ata, quantidade e descrição do produto, local, prazo, horário de entrega e valor;
 - 22.8.2.10.2. Realizar periodicamente a pesquisa de mercado para comprovação da vantajosidade dos preços registrados;
 - 22.8.2.10.3. Conduzir eventuais negociações dos preços registrados para propor a sua revisão;
 - 22.8.2.10.4. Propor a revogação da ata ou o cancelamento do registro do fornecedor;
 - 22.8.2.10.5. Manifestar-se sobre os estudos dos órgãos públicos não participantes interessados em utilizar a ata, se for o caso;
 - 22.8.2.10.6. Controlar a quantidade registrada, o saldo e os limites de cada item para adesão, se for o caso;
 - 22.8.2.10.7. Manifestar-se pela prorrogação da ata de registro de preço, com a indicação do quantitativo a ser renovado.

22.9. FISCAL TÉCNICO

22.9.1. O fiscal técnico realizará o acompanhamento e a fiscalização da execução do contrato em seus aspectos técnicos, a quem caberá, além das demais atribuições estabelecidas no Manual de Fiscalização e Gestão de Contratos do STJ e, no âmbito do CJF, dos seus normativos internos:

22.9.1.1. Verificar se na execução do objeto a especificação, o valor unitário ou total, a quantidade e os prazos estão de acordo com o estabelecido neste termo de referência;

22.9.1.2. Anotar em processo específico, quando autuado para esse fim, todas as ocorrências relativas à execução do contrato, com a indicação do que for necessário à regularização das faltas ou defeitos observados;

22.9.1.3. Monitorar constantemente o nível de qualidade dos serviços para evitar eventuais incorreções, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas;

22.9.1.4. Registrar e informar ao gestor as atividades desempenhadas e todas as pendências constatadas na execução do contrato;

22.9.1.5. Confeccionar e assinar o termo de recebimento provisório mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico referente aos serviços de acordo com as regras deste termo de referência;

22.9.1.6. Informar ao gestor sobre eventual incapacidade técnica da empresa na execução contratual;

22.9.1.7. Propor ao gestor, na hipótese de descumprimento contratual, a aplicação de sanções à CONTRATADA, de acordo com as regras estabelecidas no ato convocatório e neste termo de referência, observando os procedimentos estabelecidos na Instrução Normativa STJ/GDG n. 10/2023 e nos normativos internos do CJF, conforme o caso;

22.9.1.8. Elaborar, quando exigido, relatórios, laudos e pareceres das atividades de fiscalização técnica da execução do contrato;

22.9.1.9. Realizar vistorias, atestando o cumprimento das orientações técnicas e indicações de segurança;

22.9.1.10. Auxiliar o gestor do contrato com as informações necessárias, na elaboração do documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pela CONTRATADA.

22.10. FISCAL ADMINISTRATIVO

22.10.1. O fiscal administrativo realizará o acompanhamento dos aspectos administrativos contratuais quanto às obrigações previdenciárias, fiscais e trabalhistas e quanto ao controle do contrato no que se refere a revisões, reajustes e providências tempestivas nas hipóteses de inadimplemento, a quem caberá, além das demais atribuições estabelecidas no Manual de Fiscalização e Gestão de Contratos do STJ e nos normativos internos do CJF, conforme o caso;

22.10.1.1. Prestar apoio técnico e operacional ao gestor do contrato, com a realização das tarefas relacionadas ao controle dos prazos relacionados ao contrato e à formalização de apostilamentos e termos aditivos, ao acompanhamento do empenho, do pagamento e, se for o caso, das garantias e glosas;

22.10.1.2. Verificar a manutenção das condições de habilitação da CONTRATADA, com a solicitação dos documentos comprobatórios pertinentes, caso necessário;

22.10.1.3. Atuar tempestivamente na solução de eventuais problemas relacionados ao descumprimento das obrigações contratuais e reportar ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;

22.10.1.4. Participar da atualização do relatório de riscos durante a fase de gestão do contrato, em conjunto com o fiscal técnico;

22.10.1.5. Auxiliar o gestor do contrato com as informações necessárias, na elaboração do documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pela CONTRATADA;

22.10.1.6. Realizar o recebimento provisório do objeto do contrato, em conjunto com o fiscal técnico, mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

22.11. FISCAL REQUISITANTE

22.11.1. O fiscal requisitante realizará o acompanhamento e a fiscalização da execução do contrato em seus aspectos negociais, a quem caberá, além das demais atribuições estabelecidas no Manual de Fiscalização e Gestão de Contratos do STJ:

22.11.1.1. Fiscalizar a execução dos serviços demandados e propor os ajustamentos necessários para fiel desempenho e atendimento dos objetivos das ordens de serviço;

22.11.1.2. Receber, conferir e aprovar os relatórios de serviços encaminhados pela CONTRATADA;

22.11.1.3. Analisar a qualidade dos serviços realizados pela CONTRATADA e aplicar as deduções e/ou descontos quando não atendidos os padrões exigidos;

22.11.1.4. Analisar e aprovar o Relatório Mensal de Atividades e encaminhá-lo à CONTRATADA para ciência e emissão da nota fiscal e ao gestor do contrato para providências subsequentes;

22.11.1.5. Confeccionar e assinar, junto com os fiscais técnico e administrativo, o termo de recebimento provisório, observadas as regras estabelecidas no Capítulo [16](#) deste documento, que comprove o cumprimento das exigências de caráter técnico referente ao fornecimento e aos serviços de acordo com as regras contratuais.

22.12. COMISSÃO DE RECEBIMENTO

22.12.1. Compete à comissão confeccionar e assinar o termo de recebimento definitivo dos itens 1, 2, 3 e 4 do Lote 1 e itens 6, 7, 8 e 9 do Lote 2, com base nas informações produzidas no recebimento provisório, mediante termo detalhado que comprove a conformidade do objeto com as especificações e os prazos estabelecidos no termo de referência.

23. ADEQUAÇÃO ORÇAMENTÁRIA

23.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados ao Superior Tribunal de Justiça no Orçamento Geral da União.

23.2. A contratação será atendida pela seguinte dotação:

- i. Gestão/Unidade: **50001**
- ii. Fonte de Recursos: **100000000**;
- iii. Programa de Trabalho: **02.061.0033.4236.0001**;
- iv. Natureza de Despesa: **33.90.40**;

23.3. A existência de créditos orçamentários vinculados à contratação será atestada pelo STJ a cada exercício financeiro.

23.4. A adequação orçamentária para as despesas decorrentes da presente contratação para o Conselho da Justiça Federal está prevista no documento 5441603.

24. VALOR ESTIMADO DA CONTRATAÇÃO

24.1. O valor da despesa foi estimado com base em pesquisa de preços, conforme documento 5414226 e descrição abaixo:

a. Lote 1 - Produtos e serviços para o STJ, órgão gerenciador: R\$ 21.826.523,65 (vinte e um milhões, oitocentos e vinte e seis mil, quinhentos e vinte e três reais e sessenta e cinco centavos);

b. Lote 2 - Produtos e serviços para o CJF, órgão participante: R\$ 2.749.104,58 (dois milhões, setecentos e quarenta e nove mil, cento e quatro reais e cinquenta e oito centavos).

LOTE 1 - Produtos e serviços para o STJ, órgão gerenciador:				
Item	Especificação do objeto	Unidade	Quantidade	Valor unitário e total

1	Licença de uso de software de governança, compliance e segurança de dados sensíveis com análise comportamental de usuários do Microsoft Active Directory, servidores de arquivos on premise Windows ou Linux e NAS (network attached storage), incluindo segurança de credenciais de usuários do Microsoft Active Directory, com garantia e suporte do fabricante.	U s u á r i o	4 8 0 9 8 8	R \$ 10 2. 2 7 6, 8 2	R\$ 10 9 49 5 15 9 2
2	Licença de uso de software de governança, compliance e segurança e proteção de dados sensíveis com análise comportamental de usuários para ambiente de nuvem (Microsoft Sharepoint online, Exchange online, Microsoft Teams, OneDrive) ou Google drive ou AWS s3), com garantia e suporte do fabricante.	U s u á r i o	4 8 0 9 8 5	R \$ 10 2. 7 3 4. 8 5	R\$ 10 7 47 3 93 6 5
3	Serviço de instalação, implantação, parametrização e operacionalização para itens 1 e 2.	S e r v i ç o	1	R \$ 3 9. 7 5 0, 0 0	R\$ 39 7 50 0 0
4	Treinamento oficial para dez participantes.	T u r m a	1	R \$ 3 8. 2 0 0, 0 0	R\$ 38 2 00 0 0
5	Serviço de apoio a análise, investigação e tratamento de incidentes de segurança, com duração de (1h) uma hora por semana.	M ê s	a t é 2 4 7	R \$ 2. 1 5 2, 6 7	R\$ 51 6 64 0 8
TOTAL				R\$ 21 8 26 5 23 6 5	

LOTE 2 - Produtos e serviços para o CJF, órgão participante:

Item	Especificação do objeto	Unidade	Quantidade	Valor unitário	Valor total
6	Licença de uso de software de governança, compliance e segurança de dados sensíveis com análise comportamental de usuários do Microsoft Active Directory, servidores de arquivos on premise Windows ou Linux e NAS (network attached storage), incluindo segurança de credenciais de usuários do Microsoft Active Directory, com garantia e suporte do fabricante.	Usuário	550	R\$ 2.385,71	R\$ 1.312.140,50
7	Licença de uso de software de governança, compliance e segurança e proteção de dados sensíveis com análise comportamental de usuários para ambiente de nuvem (Microsoft Sharepoint online, Exchange online, Microsoft Teams, OneDrive) ou Google drive ou AWS s3), com garantia e suporte do fabricante.	Usuário	550	R\$ 2.377,00	R\$ 1.307.350,00
8	Serviço de instalação, implantação, parametrização e operacionalização para itens 7 e 8.	Serviço	1	R\$ 39.750,00	R\$ 39.750,00
9	Treinamento oficial para dez participantes.	Turma	1	R\$ 38.200,00	R\$ 38.200,00
10	Serviço de apoio a análise, investigação e tratamento de incidentes de segurança, com duração de (1h) uma hora por semana.	Mês	24	R\$ 2.152,67	R\$ 51.664,08

TOTAL	R\$ 2. 74 9. 10 4, 58
-------	---

ANEXO I - ESPECIFICAÇÃO TÉCNICA

1. Características gerais:

- 1.1. A solução de auditoria deverá ser de um único fabricante;
- 1.2. A solução deve disponibilizar console web ou cliente que poderá ser acessada através do servidor de aplicação e estações de trabalho dos usuários com acesso autorizado;
- 1.3. A solução deverá possibilitar integração, de forma direta ou indireta, de suas informações com sistemas de DLP (Data Lost Prevention) e SIEM;
- 1.4. Caso seja necessária instalação de qualquer agente nos servidores a serem monitorados, o processo não deve impactar na disponibilidade dos servidores ou serviços;
- 1.5. O agente deve possuir um mecanismo de monitoramento de desempenho dos servidores onde atua, de modo a não permitir que o nível de consumo de recursos ultrapasse limites definidos e configuráveis;
- 1.6. A solução deve oferecer a possibilidade de configurações de diferentes níveis de segurança às suas funcionalidades, podendo, desta forma, ser utilizada por diferentes equipes com variadas demandas de atividades e com acesso restrito a diferentes funções;
- 1.7. A solução de governança de dados deverá ter certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação como a ISO/IEC 27001 ou similares;
- 1.8. A solução deve suportar a utilização de servidores virtualizados para os componentes;
- 1.9. A solução deve possibilitar a configuração de credencial diferente para cada servidor/serviço a ser monitorado;
- 1.10. A solução deverá fazer recomendações de melhores práticas a serem aplicadas no ambiente;
- 1.11. Por se tratar de software de proteção de dados sensíveis com análise comportamental de usuários para ambiente de nuvem o fabricante ou a solução governança de dados deverá ser certificada ISO/IEC 27017;
- 1.12. Por se tratar de software de proteção de dados sensíveis o fabricante ou a solução governança de dados deverá ser certificada ISO/IEC 27018 que trata os dados pessoais;

- 1.13. Por se tratar de software de proteção de dados sensíveis o fabricante ou a solução governança de dados deverá ser certificada ISO/IEC 27701 que trata do gerenciamento de privacidade da informação dentro da organização.
- 1.14. A solução deverá permitir a exportação de relatórios de forma manual por meio da interação do usuário e no modo automatizado em: HTML, PDF, CSV e Excel;
- 1.15. A ferramenta deve permitir que relatórios sejam extraídos sob demanda uma única vez ou agendados e enviados com frequência definida;
- 1.16. A ferramenta deve permitir o agendamento para envio de relatórios pelo correio eletrônico ou para um compartilhamento no servidor de arquivos;
- 1.17. A ferramenta deve fornecer relatório de todas as permissões de determinado usuário nos repositórios monitorados;
- 1.18. A ferramenta deve fornecer relatório de todos os usuários com permissões em determinada pasta;
- 1.19. A ferramenta deve fornecer relatório dos acessos aos arquivos;
- 1.20. Fornecer relatórios de dados e usuários inativos;
- 1.21. A solução deve fornecer relatório de histórico de permissões;
- 1.22. A solução deve fornecer relatório de histórico de membros de grupos de segurança;
- 1.23. A solução deve oferecer relatórios de estatísticas, métricas e gráficos com informações sobre usuários, grupos, pastas e permissões ao longo de determinado período;
- 1.24. A solução deve fornecer relatório dos alertas de comportamento anômalo identificados;
- 1.25. A solução deve fornecer relatório com as recomendações de revogação de permissão gerados pela análise comportamental realizada sobre os usuários e recursos monitorados;
- 1.26. A solução deve oferecer relatório de estatística de acesso, utilização por tipo de arquivos, eventos por usuários e distribuição por tipos de eventos;
- 1.27. A solução deve fornecer relatório de auditoria das ações dos usuários na console;

- 1.28. A solução deve oferecer relatório sobre as alterações, versão alterada e quais foram as mudanças realizadas em GPOs;
 - 1.29. A solução deve coletar o log das plataformas monitoradas de forma contínua e automática e normatizar essas informações em banco de dados as informações das plataformas monitoradas;
 - 1.30. A solução deve apresentar todos os logs de todos os usuários na mesma console de visibilidade de permissionamento da plataforma monitorada;
 - 1.31. Os logs apresentados pela solução ofertada devem conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto, caminho (path) dos dados, domínio, arquivo impactado e nome do usuário;
 - 1.32. A solução deverá permitir filtragem gráfica, ordenação e agrupamento dos logs;
 - 1.33. A solução deverá permitir que os usuários realizem pesquisas baseadas em critérios como: data do evento, servidor ou plataforma em que o evento ocorreu, tipo de evento, arquivos ou diretórios acessados;
 - 1.34. Deve ser possível alterar o conjunto de dados (colunas) retornados da consulta aos logs de acordo com a necessidade da informação.
 - 1.35. A solução deve fornecer visibilidade em tempo real sobre quem tem acesso a dados sensíveis, locais de armazenamento e utilização.
 - 1.36. A solução deve detectar ameaças e comportamentos suspeitos, por meio de uma análise comportamental sobre atividades anômalas que possam indicar possíveis violações de segurança ou uso indevido.
 - 1.37. A solução deve classificar e rotular os dados conforme conteúdo e importância.
 - 1.38. A solução deve gerenciar e controlar os privilégios de acesso. Deve permitir que sejam criadas políticas granulares de acesso.
 - 1.39. A solução deve possibilitar que seja concedida a administração das permissões em pastas para o dono do dado, de forma que um dono consiga por si só, via portal da solução, conceder e controlar os acessos atribuídos em sua pasta.
- 2. Itens 1 e 6 - software para proteção de dados e análise comportamental de usuários do Microsoft Active Directory e servidores de arquivos.**

- 2.1. A solução deve efetuar as funcionalidades de permissionamento, Log, Relatórios e Análise Comportamental dos usuários nos servidores de diretórios de usuários Microsoft Active Directory, servidores de arquivos on-premise Windows ou Linux e NAS (Network Attached Storage);
 - 2.1.1. A solução deverá suportar no mínimo, para servidores de arquivos, Windows server e Linux para no mínimo as seguintes distribuições: Red Hat Enterprise Linux em todas as suas versões ativas, SUSE Linux Enterprise Server Versão 15 SP2 LTSS e 15 SP3, Oracle Linux 7 ou superior;
- 2.2. A solução deve permitir alteração das permissões dos diretórios através de sua interface gráfica;
- 2.3. Caso a solução ofertada necessite reter o log nativo de auditoria do Active Directory, o hardware sem ponto único de falha necessário para o armazenamento destes logs por 24 (vinte e quatro) meses deverá ser contemplado na proposta;
- 2.4. A solução deve fornecer todas as funcionalidades citadas neste documento sem a necessidade de retenção dos logs nativos do Windows em infraestrutura local. Caso a solução ofertada necessite habilitar o log de auditoria do Windows File Server, o hardware sem ponto único de falha necessário para o armazenamento destes logs por no mínimo 24 (vinte e quatro) meses deverá ser contemplado na proposta.
- 2.5. A solução deve possuir visibilidade da hierarquia do serviço de Diretórios de Usuários por meio de interface gráfica;
- 2.6. A solução deve possuir a visibilidade de todos os domínios on-premise, Unidades Organizacionais, Computadores, Grupos e outros objetos do domínio através de uma única interface gráfica e também em formato de relatório;
- 2.7. A solução deve ter trilha de auditoria classificável e pesquisável de todas as atividades do Active Directory em uma única interface gráfica e também em formato de relatório;
- 2.8. A solução deverá ser capaz rastrear quem fez alterações no Active Directory, qual foi a alteração feita e quando nesta mesma interface gráfica e em formato de relatório;
- 2.9. A solução deve suportar a auditoria dos seguintes eventos do Directory Service:
 - 2.9.1. Membros adicionados e removidos de grupos de segurança;

- 2.9.2. Alteração nas propriedades do objeto do AD;
 - 2.9.3. Requisição de acesso;
 - 2.9.4. Autenticação de conta;
 - 2.9.5. Reset de senhas;
 - 2.9.6. Bloqueio e desbloqueio de conta;
 - 2.9.7. Criação e deleção de conta;
 - 2.9.8. Habilitar e desabilitar a conta;
 - 2.9.9. Modificação de configuração de GPO;
 - 2.9.10. Criação de link de GPO;
 - 2.9.11. Deleção de link de GPO;
 - 2.9.12. Modificação de link de GPO;
 - 2.9.13. Deleção dos logs de auditoria;
 - 2.9.14. Alteração na hora do sistema;
 - 2.9.15. Alterações nas políticas de Sistema e de domínio;
 - 2.9.16. Alteração nas configurações de auditoria de um objeto;
 - 2.9.17. Renovação de ticket de serviço Kerberos;
 - 2.9.18. Criação e modificação de confiança de domínio;
 - 2.9.19. Acesso ao hash de senha de conta do domínio;
 - 2.9.20. Alteração de senha de administrador DSRM.
- 2.10. Deverá ser possível fazer o gerenciamento de objetos do AD através da console da solução. É necessário que os usuários administradores sejam capazes de realizar as seguintes ações através da interface gráfica da solução:
- 2.10.1. Criar novos usuários;
 - 2.10.2. Criar novos grupos de segurança;
 - 2.10.3. Alterar parâmetros de usuários já existentes;
 - 2.10.4. Alterar membros de grupos de segurança;

- 2.10.5. Excluir usuários;
 - 2.10.6. Excluir computadores;
 - 2.10.7. Reconfigurar senhas;
 - 2.10.8. Desbloquear usuários;
 - 2.10.9. Habilitar e desabilitar usuários.
- 2.11. Deve ser possível realizar as ações abaixo de uma só vez através da seleção de múltiplos usuários:
- 2.11.1. Deleção; Reset de senha;
 - 2.11.2. Desbloqueio da conta;
 - 2.11.3. Habilitar e Desabilitar.
- 2.12. A solução deve notificar o administrador sobre qualquer mudança fora das políticas ou configuração que possa ter sido realizada;
- 2.13. Deve possuir visualização de indicadores de risco para o Active Directory com configurações que podem ser exploradas por usuários maliciosos, como: Admins com SPNs, contas habilitadas porém sem uso e contas sem senha;
- 2.14. A solução ofertada deve manter o log das operações de abrir, criar, apagar, modificar, renomear e acesso negado aos arquivos e pastas;
- 2.15. A solução deve fornecer funcionalidade de ajuste aos diretórios com herança de permissões quebradas;
- 2.16. A solução deve possibilitar a criação de pastas que sejam automaticamente reconhecidas na interface gráfica e que possam ser automaticamente usadas pelos usuários;
- 2.17. A solução deverá fornecer a visão das permissões efetivas, ou seja, agregando permissões de Compartilhamento e NTFS;
- 2.18. A solução deve fornecer método para assinalar ou associar um ou mais usuários como "Proprietário(s)" de uma pasta ou grupo;

- 2.19. A solução deve ser capaz de identificar qual dado ou arquivo contém informações sensíveis ou confidenciais por meio de busca em seu conteúdo por informações definidas em dicionários fornecidos pelo fabricante ou por informações definidas e customizadas pelo usuário;
- 2.20. A solução deve exibir na mesma interface gráfica das informações sobre os permissionamentos e ACL's, a quantidade de informações sensíveis e qual tipo de informação sensível classificada para facilitar a identificação de potenciais repositórios e pastas superexpostos;
- 2.21. As informações produzidas pela solução sobre dados sensíveis devem ser disponibilizadas em forma de relatórios;
- 2.22. As consultas aos logs de auditoria e relatórios devem suportar filtros de classificação de dados sensíveis;
- 2.23. A solução deve demonstrar em sua console a quantidade de dados sensíveis descobertos nos arquivos e pastas;
- 2.24. A solução deve gerar recomendações de revogação de acesso aos dados classificados para redução de acesso às informações sensíveis;
- 2.25. A ferramenta deve permitir integração com ferramentas do DLP (Data Loss Prevention) de classificação de dados sensíveis e informar em relatório onde estes dados se encontram dentro do sistema de arquivos da solução;
- 2.26. Deve ser possível limitar escopo dentro dos sistemas de arquivos a ser analisado;
- 2.27. Deve ser possível definir partes específicas do arquivo a serem analisadas no escopo como: Colunas específicas de arquivos do tipo Microsoft Excel, cabeçalho, rodapé e marca d'água de arquivos Microsoft Office, links de arquivos Microsoft Office e PDF;
- 2.28. A solução deve ser capaz de identificar dados que possuam informações referente a Lei de Geral de Proteção de Dados (LGPD) como por exemplo: nome, CPF, passaporte, religião, gênero, nacionalidade, entre outros;
- 2.29. Baseada nos dados de auditoria, a solução deve ser capaz de aprender o comportamento padrão dos usuários e dos recursos monitorados, para que desvios e anormalidades nesses comportamentos sejam identificados automaticamente;

- 2.30. A solução deve fazer a análise em tempo real e prevenção de comportamentos suspeitos no AD e servidores de arquivos monitorados de forma integrada em console centralizada;
- 2.31. A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar acesso a dados que o usuário não costuma acessar;
- 2.32. Nos alertas em tempo real, deve ser possível configurar para que um usuário, uma pasta, um período ou uma ação específica seja alertada caso ocorra ação que os envolva;
- 2.33. Os alertas poderão ser iniciados com base nos dados da auditoria, tais como usuário, ação, data e hora, ação realizada;
- 2.34. Deve ser contemplada a assinatura de uma base de conhecimentos do fornecedor de alertas pré-configurados de eventos suspeitos tais como: Grupos de segurança, GPO's e outros objetos de Active Directory modificados ou removidos; Escalações de privilégios; Modificação de permissões em diretórios Ataques de sequestro de dados (ransomware); Detecção de ferramentas nocivas ao ambiente; Excessos de ações com acessos negadas; Acessos indevidos dos administradores nos dados da empresa; Tentativas de elevação de privilégios; Excesso de tentativas de autenticação ou contas bloqueadas; Excesso de atividades em dados parados e/ou inativos; Alterações anormais em GPO; ataques de força bruta; ataques de pass-the-hash; ataques de golden ticket; ataques de enumeração de contas;
- 2.35. Os alertas devem ser gerados em SNMP, Syslog, visualizador de eventos do Windows, E-mail e devem ser capazes de realizar a execução de um script previamente configurado;
- 2.36. Os alertas devem ser apresentados também em dashboard web que apresente: quantidade de alertas e suas severidades em determinado período, usuários mais alertados em determinado período, tipos de comportamentos suspeitos que mais ocorreram, máquinas que foram mais utilizadas para as ações suspeitas, classificação dos alertas dentro de um cenário de ataque cibernético;
- 2.37. O dashboard deve apresentar os eventos que motivaram o alerta para que o time de segurança possa fazer investigação forense;
- 2.38. O dashboard deve mostrar as propriedades do AD do usuário alertado que são essenciais para a análise forense do alerta gerado;

- 2.39. Para análise forense do usuário mais alertado, o dashboard deve possuir página que agregue dados importantes do comportamento daquele usuário. Isso permite que se identifique o cenário do possível ataque;
- 2.40. No dashboard, a partir de um alerta selecionado, a solução deve exibir página que liste todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser customizável podendo ser filtrada, exibidas ou ocultas as colunas e agregada por valores das colunas exibidas;
- 2.41. O dashboard deve apresentar KPIs de compliance e segurança dos servidores e recursos monitorados como quantidade de arquivos, pastas, permissões e dados expostos;
- 2.42. A dashboard deve apresentar relatórios qualitativos, ou seja, listas com estes itens fora de compliance;
- 2.43. A solução deve permitir integrar-se facilmente ao SIEM e em soluções de gerenciamento de ativos;
- 2.44. A solução deverá executar remediação automatizada de permissões e as configurações deverão ser feitas de forma integrado à console de visualização gráfica das pastas dos servidores de arquivos;
- 2.45. A solução deverá automatizar a remediação das permissões das pastas e arquivos expostos a usuários em excesso;
- 2.46. A solução deverá automatizar a reparação das pastas com herança quebrada nos servidores de arquivos aumentando assim a segurança das informações armazenadas;
- 2.47. A solução deverá identificar, através da integração com os dados de auditoria coletados, os usuários que serão impactados pela remediação para permitir a criação de regras customizadas para remover permissões de grupos de segurança sem que os acessos às pastas e arquivos dos usuários sejam afetados;
- 2.48. A solução deverá apresentar o número de pastas que serão corrigidas por cada regra criada;
- 2.49. A solução deverá permitir a execução de rollback caso as expectativas não sejam alcançadas;

- 2.50. Para a remoção de permissões de grupos de segurança do AD das pastas, a solução deverá verificar nos eventos de auditoria se há usuários utilizando essas permissões para acesso às informações. Em caso positivo, a solução deve criar automaticamente novos grupos de segurança e inserir os usuários que acessam as informações a partir das permissões concedidas aos grupos globais;
- 2.51. A solução deverá fornecer a possibilidade de criação de regras customizáveis em que deverá ser possível alterar o escopo das pastas que terão as ACLs reparadas e a forma como essas ACLs serão reparadas;
- 2.52. A solução deverá permitir que nas ACLs em que há erro de ordem das permissões, a solução deverá ser capaz de reordená-la;
- 2.53. A solução deverá ser capaz de forçar a propagação correta das permissões para as pastas filhas quando houver erro na herança;
- 2.54. A solução deverá ser capaz de forçar a propagação correta das permissões do usuário "proprietário" das pastas e arquivos quando esta estiver erroneamente faltante;
- 2.55. A solução deverá permitir que as permissões de ACLs órfãs sejam retiradas conforme melhores práticas da Microsoft e a herança corrigida;
- 2.56. A solução deverá permitir que as permissões sejam mantidas, a pasta sinalizada como uma pasta com permissões únicas, que tem outras permissões adicionadas além das permissões herdadas da pasta pai;
- 2.57. A solução deverá permitir a alteração do escopo de aplicação da regra de reparação automatizada das permissões;
- 2.58. A solução deverá permitir a definição de credencial de serviço ou de credencial de usuário para execução das regras de reparação automatizada das permissões;
- 2.59. A solução deverá apresentar a estimativa de tempo que cada regra criada levará para ser executada;
- 2.60. A solução deverá permitir o agendamento das execuções das regras de reparação automatizada das permissões de forma que elas possam ser executadas recorrentemente ou uma única vez;
- 2.61. A solução deverá permitir a definição de limites de horário para execução das regras;

- 2.62. A solução deve apresentar em relatório o resultado da execução das regras com o caminho da pasta e arquivo, a ação executada sobre a permissão, os grupos de segurança e usuários afetados, a permissão afetada e erros e alertas da execução;
- 2.63. A solução deverá permitir a extração dos relatórios de execução das regras de remediação;
- 2.64. A solução deverá exibir para cada pasta dos recursos monitorados a visualização gráfica e interativa das listas de controle de acesso incluindo grupos, subgrupos e seus respectivos membros;
- 2.65. A interface gráfica deverá permitir a busca por um usuário ou grupo e apresentar graficamente seus níveis de permissão nos diretórios dos recursos monitorados. Esta visibilidade deve incluir herança de permissão ativa/desativada e indicação de compartilhamento.
- 3. Itens 2 e 7 - software para governança, compliance, segurança e proteção de dados e análise comportamental de usuários em ambiente de nuvem Microsoft (Sharepoint online, exchange online, teams, onedrive) ou Google drive ou AWS S3.**
- 3.1. A solução deverá suportar todas as funcionalidades descritas nas [ANEXO I.1.](#) - características gerais - para os repositórios de nuvem corporativa: (Microsoft, Sharepoint Online, Exchange Online, Microsoft teams, Microsoft OneDrive) ou Google Drive ou AWS S3;
- 3.2. O CONTRATANTE deverá optar por licenciamento da solução de descoberta de dados sensíveis para repositório de nuvem corporativa coletiva Microsoft ou Google ou AWS;
- 3.3. A solução deverá coletar trilha de auditoria de acesso dos usuários aos dados armazenados no repositório de nuvem monitorado;
- 3.4. A solução deverá permitir a filtragem gráfica da trilha de auditoria;
- 3.5. A solução deverá normalizar e analisar permissões dos usuários aos dados da nuvem corporativa coletiva;
- 3.6. A solução deverá apresentar todos os usuários que têm permissões e quais permissões cada usuário tem em uma pasta ou arquivo armazenado no repositório;
- 3.7. A solução deverá apresentar todos os dados que um usuário selecionado tem acesso e qual tipo de permissão;

- 3.8. A solução deverá demonstrar dados sensíveis compartilhados externamente e expostos publicamente;
- 3.9. A solução deverá descobrir configurações incorretas no repositório;
- 3.10. A solução deverá apresentar métricas e configurações incorretas que podem afetar a segurança do ambiente, como: pastas e repositórios expostos publicamente, dados inativos;
- 3.11. A solução deverá fornecer recomendações de como corrigir rapidamente configurações incorretas do ambiente monitorado.
- 3.12. A solução deve ser capaz de identificar qual dado ou arquivo contém informações sensíveis ou confidenciais por meio de busca em seu conteúdo por informações definidas em dicionários fornecidos pelo fabricante ou por informações definidas e customizadas pelo usuário.
- 3.13. A solução deve exibir na mesma interface gráfica das informações sobre os permissionamentos e ACL's, a quantidade de informações sensíveis e qual tipo de informação sensível classificada para facilitar a identificação de potenciais repositórios e pastas superexpostos.
- 3.14. A solução deverá ter suas funcionalidades de descoberta de dados sensíveis para repositórios de nuvem Google ou Microsoft ou AWS.
- 3.15. As informações produzidas pela solução sobre dados sensíveis devem ser disponibilizadas em forma de relatórios.
- 3.16. As consultas aos logs de auditoria e relatórios devem suportar filtros de classificação de dados sensíveis.
- 3.17. A solução deverá identificar atividades de contas pessoais externas acessando os dados armazenados nos repositórios de nuvem;
- 3.18. A solução deve demonstrar em sua console a quantidade de dados sensíveis descobertos nos arquivos e pastas.
- 3.19. A solução deve integrar a funcionalidade de classificação de dados sensíveis com soluções de terceiros para estender a habilidade de ambos.
- 3.20. A ferramenta deve permitir integração com ferramentas do DLP (Data Loss Prevention) de classificação de dados sensíveis e informar em relatório onde estes dados se encontram dentro do sistema de arquivos da solução.

- 3.21. Deve ser possível limitar escopo dentro dos sistemas de arquivos a ser analisado;
- 3.22. A solução deve ser capaz de identificar dados que possuam informações referente a Lei de Geral de Proteção de Dados (LGPD) como por exemplo: nome, CPF, passaporte, religião, gênero, nacionalidade, entre outros.
- 3.23. As funcionalidades descritas nas características gerais devem se aplicar às caixas postais e pastas públicas dos servidores de correio eletrônico Microsoft Exchange, e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios dedados não estruturados monitorados.
- 3.24. A solução descrita neste item deve possuir as seguintes funcionalidades globais: Auditar acesso, modificação e remoção de caixas postais e listas do ambiente de correio eletrônico; Gerar alerta com base nas informações auditadas; Monitorar e analisar comportamentos suspeitos de usuários; Gerar relatórios sobre o ambiente de correio eletrônico.
- 3.25. A solução deve suportar Exchange Online.
- 3.26. A solução deverá monitorar os eventos das caixas postais dos usuários e as pastas públicas do Exchange;
- 3.27. A solução deverá monitorar os eventos das caixas postais dos usuários do Exchange sem a necessidade de habilitação de auditoria nativa do Exchange (journaling e diagnostics);
- 3.28. A solução deverá coletar, os seguintes eventos:
- 3.28.1. Pasta criada;
 - 3.28.2. Pasta apagada;
 - 3.28.3. Pasta movida;
 - 3.28.4. Pasta aberta;
 - 3.28.5. Pasta renomeada;
 - 3.28.6. Permissão adicionada a pasta;
 - 3.28.7. Permissão removida de pasta;
 - 3.28.8. Permissão de pasta alterada;
 - 3.28.9. Mensagem copiada;

- 3.28.10. Mensagem criada;
- 3.28.11. Mensagem aberta;
- 3.28.12. Mensagem apagada;
- 3.28.13. Logon;
- 3.28.14. Mensagem enviada "em nome de";
- 3.28.15. Mensagem enviada "como";
- 3.28.16. Mensagem editada;
- 3.28.17. Permissão adicionada a mailbox;
- 3.28.18. Permissão removida de mailbox;
- 3.29. Baseada nos dados de auditoria, a solução deve ser capaz de aprender o comportamento padrão dos recursos monitorados, para que desvios e anomalias nesses comportamentos sejam identificados automaticamente e alertados em tempo real.
- 3.30. A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar eventos anormais que tenham ocorrido nas plataformas monitoradas.
- 3.31. O painel web deve possibilitar e a visualização: de todos os alertas e seus eventos em determinado período; Usuários se comportando de forma suspeita que dispararam alertas; Tipos de alertas mais disparados; Dispositivos mais alertados;
- 3.32. Deve ser possível, a partir de selecionado evento alertado, fazer filtragem e correlacionamento com outros eventos como, por exemplo, o comportamento dos usuários do mesmo departamento do usuário alertado ou acessos ao mesmo tipo de informação sensível identificado pela solução;
- 3.33. A solução deverá apresentar a razão para um alerta ter sido disparado;
- 3.34. A solução deverá apresentar detalhes dos alertas gerados como usuário envolvido, dispositivo envolvido, dados envolvidos e período do comportamento suspeito;

- 3.35. A solução deverá apresentar detalhes do usuário envolvido no alerta como: habilitado ou desabilitado, se estava ativo ou inativo no ambiente, se esteve envolvido em outros alertas, se é uma conta privilegiada;
- 3.36. A solução deverá apresentar detalhes do dispositivo envolvido no alerta: se é o dispositivo normalmente utilizado pelo usuário envolvido no alerta, se esteve envolvido em outros alertas;
- 3.37. A solução deverá apresentar detalhes dos dados envolvidos no alerta: se estava inativo, se já havia sido acessado pelo usuário envolvido no alerta, se já havia sido acessado pelos pares do usuário envolvido no alerta, se são dados sensíveis ou estava em watchlist.

4. Itens 3 e 8 - Serviço de Instalação e Configuração

- 4.1. A CONTRATADA será inteiramente responsável pela implantação da solução adquirida, de forma a não comprometer o funcionamento da solução;
- 4.2. A CONTRATADA deverá efetuar instalação e configuração realizada de acordo com as recomendações do fabricante;
- 4.3. Os serviços de instalação e configuração deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante em seus manuais de instalação e configuração ou artigos técnicos;
- 4.4. A solução, deverá ser entregue com todas as funcionalidades, recursos, componentes, acessórios, softwares e licenciamentos necessários ao seu pleno funcionamento;
- 4.5. A instalação da solução, incluindo todos os componentes e acessórios, será realizada pela CONTRATADA, com acompanhamento de uma equipe destacada pelo CONTRATANTE;
- 4.6. A CONTRATADA deverá providenciar um profissional certificado pelo fabricante na solução para garantir a conformidade da instalação e a configuração dos equipamentos e softwares que compõem a solução;
- 4.7. A instalação, configuração e testes da solução deverão ser feitos com o acompanhamento de técnicos do CONTRATANTE, visando o repasse de conhecimento e observados os padrões de gerenciamento de manutenção e segurança do CONTRATANTE;
- 4.8. Deverá ser fornecida documentação de toda a implementação e configuração dos produtos adquiridos;

- 4.9. Fica a critério do CONTRATANTE, definir o horário de instalação e configuração da solução, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno, se for o caso;
- 4.10. Atividades associadas à implantação com a necessidade eventual de interrupção de serviços em produção, deverão ocorrer fora do expediente normal do Tribunal e estarão sujeitas ao planejamento e aprovação prévia da equipe técnica do CONTRATANTE;
- 4.11. A CONTRATADA deverá comunicar o CONTRATANTE a conclusão da instalação e entregar toda documentação técnica (As Built) em até 10 (dez) dias corridos após a conclusão da instalação;
- 4.12. A documentação técnica (As Built), deverá ser aprovada pela equipe do CONTRATANTE, e caso necessário, os ajustes solicitados deverão ser realizados pela CONTRATADA em até 05 (cinco) dias após a análise da equipe do CONTRATANTE;
- 4.13. As atividades de instalação deverão ser acompanhadas pela equipe técnica do CONTRATANTE, devendo a CONTRATADA:
- 4.13.1. Efetuar o repasse técnico referente à instalação, implementação e operacionalização da solução, com transferência dos procedimentos básicos de configuração e operação utilizados;
 - 4.13.2. O repasse técnico, procedimentos e operacionalização deverão cobrir conhecimentos mínimos necessários para administração, configuração, otimização, resolução de problemas básicos e utilização da solução.
- 4.14. A equipe técnica do CONTRATANTE deverá disponibilizar analistas ou técnicos para o acompanhamento das atividades definidas nos itens acima.

ANEXO II - TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO

1. O **Superior Tribunal de Justiça**, com sede no SAF Sul, Quadra 06, Lote 01, Brasília-DF, CNPJ n. 00.488.478/0001-02, denominado CONTRATANTE, e, de outro lado, a **[nome da contratada]**, sediada **[endereço da contratada]**, CNPJ n. **[00.000.000/0000-00]**, denominada CONTRATADA;

CONSIDERANDO a assinatura do CONTRATO STJ N.º **[XXX/202X]** ou CONTRATO CJF N.º **[XXX/202X]**, celebrado com a CONTRATADA para fornecimento e prestação dos serviços objeto do contrato;

CONSIDERANDO a Lei n. 11.419/2006, que dispõe sobre a informatização do processo judicial, permitindo o processamento de ações judiciais por meio de autos total ou parcialmente digitais, utilizando, preferencialmente, a rede mundial de computadores e acesso por meio de redes internas e externas e determinando que os processos eletrônicos deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados, sendo dispensada a formação de autos suplementares, dentre outras determinações;

CONSIDERANDO a necessidade de ajustar as condições para regular o uso dos dados, regras de negócio, documentos, informações, sejam elas escritas, verbais ou de qualquer outro modo apresentadas, tangíveis ou intangíveis, entre outras, doravante denominadas simplesmente de INFORMAÇÕES, que a CONTRATADA tiver acesso em virtude da execução contratual;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE;

CONSIDERANDO a necessidade de manter sigilo e confidencialidade, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do Superior Tribunal de Justiça de que a CONTRATADA tomar conhecimento em razão da execução do CONTRATO, respeitando todos os critérios estabelecidos aplicáveis às INFORMAÇÕES;

CONSIDERANDO a necessidade de manter sigilo e confidencialidade, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do Superior Tribunal de Justiça de que a CONTRATADA tomar conhecimento em razão da execução do CONTRATO, respeitando todos os critérios estabelecidos aplicáveis às INFORMAÇÕES;

Cláusula Primeira - DO OBJETO

1.1 Constitui objeto deste instrumento o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao acesso de informações sensíveis e sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução dos serviços

celebrados entre as partes.

Cláusula Segunda - DOS CONCEITOS E DEFINIÇÕES

2.1 Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

2.2 Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

2.3 Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pelo CONTRATANTE.

2.4 Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômicos, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

2.5 Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgações possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Cláusula Terceira - DAS INFORMAÇÕES SIGILOSAS

3.1 Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada.

3.2 O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não à execução do serviço, doravante denominadas INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações da prestação de serviços celebrado entre as partes.

3.3 A CONTRATADA se obriga a manter o mais absoluto sigilo e confidencialidade com relação a todas e quaisquer INFORMAÇÕES que venham a ser fornecidas pelo STJ, a partir da assinatura do contrato, devendo ser tratadas como INFORMAÇÕES CONFIDENCIAIS, salvo aquelas prévia e formalmente classificadas com tratamento diferenciado pelo STJ;

Parágrafo Primeiro - Comprometem-se, as partes, a não revelar, copiar, transmitir,

reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do serviço em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do serviço.

Parágrafo Segundo - As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto.

Parágrafo Terceiro - As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

- a) Sejam comprovadamente de domínio público no momento da revelação;
- b) Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
- c) Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta - DOS DIREITOS E OBRIGAÇÕES

4.1 As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do serviço, em conformidade com o disposto neste TERMO.

Parágrafo Primeiro - A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do CONTRATANTE.

Parágrafo Segundo - A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do serviço sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I - A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro - A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros da extensão e danos ocorridos devido ao ataque cibernético, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

Parágrafo Quarto - Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I - Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes;

II - Os produtos gerados na execução do CONTRATO, bem como as INFORMAÇÕES repassadas à CONTRATADA, são única e exclusiva propriedade intelectual do STJ;

III - A CONTRATADA obriga-se a não tomar qualquer medida com vistas a obter, para si ou para terceiros, os direitos de propriedade intelectual relativos aos produtos gerados e às INFORMAÇÕES que venham a ser reveladas durante a execução do CONTRATO;

Parágrafo Quinto - A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do serviço.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I - Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II - Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III - Comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV - Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta - DA VIGÊNCIA

5.1 O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a assinatura contratual até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão da execução do serviço.

Cláusula Sexta - DAS PENALIDADES

6.1 A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão dos CONTRATOS firmados entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme artigos 155 a 163 da Lei n. 14.133/2021.

Cláusula Sétima - DISPOSIÇÕES GERAIS

7.1 Este TERMO é parte integrante e inseparável do CONTRATO STJ N.º [XXX/202X] o u CONTRATO CJF N.º [XXX/202X], que é parte independente e regulatória deste instrumento;

Parágrafo Primeiro - Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações deles decorrentes, ou se constatando casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios da legalidade, de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo - O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro - Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I - O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II - A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao contrato celebrado entre as partes;

III - A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV - Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentações brasileiras pertinentes;

V - O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado

pelas partes;

VI - Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII - O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao contrato celebrado entre as partes;

VIII - Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava - DO FORO

8.1 As questões decorrentes deste Termo serão processadas e julgadas na Justiça Federal, no foro da cidade de Brasília, Seção Judiciária do Distrito Federal.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO é assinado pelas partes na forma eletrônica, nos termos da Lei n. 11.419/2006.



Documento assinado eletronicamente por **Tiemi Umebara, Assistente IV**, em 30/08/2024, às 18:05, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Leandro Gabriel Bastos Ferreira, Analista Judiciário, Área de Apoio Especializado - Suporte em Tecnologia da Informação**, em 02/09/2024, às 11:46, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Vitor Gabriel Jaime Paiva, Chefe da Seção de Segurança da Informação**, em 02/09/2024, às 14:19, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.stj.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **5442782** e o código CRC **899836C0**.

