



CONSELHO DA JUSTIÇA FEDERAL

ESTUDO TÉCNICO PRELIMINAR Nº 0497062/2023

1 Análise de Viabilidade da Contratação (Art. 14, Resolução CNJ 468/2022)

1.1 Descrição da necessidade (Art. 18, § 1º, I, da Lei n. 14.133/2021)

A Segurança da Informação tem se consolidado cada vez mais como um aspecto imprescindível para a imagem e continuidade das atividades finalísticas das instituições, buscando garantir a integridade, disponibilidade e confidencialidade dos dados, sistemas e ambientes. Incidentes de segurança ocorridos com órgãos do Poder Judiciário vêm se tornando cada vez mais recorrentes e sofisticados, reforçando a necessidade de aprimoramento dos controles de segurança de TI para proteção contra ameaças diversas provenientes de ataques internos e externos à organização.

A solução de segurança de TI deve oferecer uma proteção eficaz contra uma ampla gama de ameaças, incluindo *malware*, *ransomware*, *phishing*, ataques de engenharia social e outras formas de intrusões cibernéticas. É crucial que a solução seja capaz de detectar e mitigar essas ameaças de forma proativa, minimizando o risco de danos aos sistemas do Conselho da Justiça Federal (CJF).

O CJF desempenha um papel fundamental na prestação de serviços judiciais garantindo a eficiência e a uniformidade na prestação jurisdicional no âmbito da Justiça Federal e uma violação de segurança bem-sucedida pode comprometer a disponibilidade, integridade, confidencialidade, e autenticidade das informações por meio de interrupção das operações, acesso indevido a informações organizacionais e pessoais, além da perda de dados críticos mantidos pelo órgão.

De acordo com relatórios recentes de instituições de segurança, houve um crescimento acentuado no número de ataques cibernéticos em todo o mundo. O cenário de ameaças inclui *malware* avançado, *ransomware*, *phishing*, engenharia social e outras formas de ataques sofisticados que visam comprometer a segurança dos sistemas e dados do CJF.

Ainda neste cenário de crescente número de ataques cibernéticos, organizações governamentais, incluindo órgãos do Poder Judiciário, estão se tornando alvos cada vez mais comuns para tais ataques.

Com base nesses cenários, fica evidente que o CJF enfrenta um risco crescente de violações de segurança cibernética. A contratação de uma solução de segurança de TI abrangente, incluindo a proteção de servidores de rede, estações de trabalho, serviço de *e-mail* e serviço de aplicações colaborativas Microsoft 365, com instalação e configuração especializadas, suporte técnico e garantia do fabricante, é uma medida crucial para mitigar tais riscos.

Essa solução buscar prover uma camada adicional de defesa contra as ameaças cibernéticas em constante evolução, garantindo a integridade, disponibilidade e confidencialidade dos sistemas e dados do CJF, bem como a continuidade de suas atividades finalísticas.

1.2 Motivação da contratação

O Conselho da Justiça Federal possui vigente o contrato CJF 31/2018, firmado com a empresa ALLTECH Soluções em tecnologia Ltda, cujo objeto é a contratação de solução de segurança para proteção de *endpoints*, dos servidores do Centro de Processamento de Dados (CPD ou *Data Center*) e do serviço de *e-mail*, com garantia de 60 (sessenta) meses, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico.

Com o fim da vigência deste contrato, assim como da vigência do direito de atualização das licenças de *antimalware* de *endpoints* e servidores e da solução de proteção do serviço de *e-mail*, em 26/12/2023, se faz necessária uma nova contratação para dar continuidade ao atendimento da demanda, além da

possibilidade de aprimoramento nos serviços prestados.

Apesar da qualidade já demonstrada da solução contratada em 2018, a equipe técnica de segurança da informação do CJF vislumbra a possibilidade de implementação de melhorias, que ocorrem por meio da inclusão de novas funcionalidades ou módulos voltados para a detecção e resposta de incidentes de segurança em níveis avançados incluindo análise de tráfego de rede.

Os serviços de proteção de *endpoint* mais atuais dispõem de funcionalidades que vão além da simples proteção contra ocorrências pontuais de *malwares* ou *ransomwares* nos dispositivos, mas também fornecem informações mais aprofundadas, que podem ser cruciais para identificação de ataques cibernéticos de maior magnitude contra o ambiente tecnológico deste Conselho.

Ante ao exposto, faz-se necessária uma nova contratação visando atender à necessidade de prover segurança aos dispositivos e *e-mails* corporativos do CJF. Trata-se de contratação de soluções de segurança visando a prevenção de ataques cibernéticos em servidores de rede, estações de trabalho (*endpoints*), serviço de *e-mail* e Microsoft 365 voltada para o ambiente corporativo do CJF.

1.3 Demonstrativo dos resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis (Art. 18, § 1º, IX, da Lei n. 14.133/2021)

Os resultados a serem alcançados com esta contratação são:

- **Eficiência operacional:** A implementação de uma solução de proteção de TI abrangente proporcionará maior eficiência operacional no ambiente do CJF. Ao proteger *endpoints*, servidores e serviço de correio eletrônico, bem como garantir a segurança dos aplicativos de colaboração do Microsoft 365, o CJF reduzirá consideravelmente o risco de violações de segurança cibernética e interrupções no sistema. Isso resultará em um melhor aproveitamento dos recursos humanos, uma vez que a equipe de TI poderá direcionar seu tempo e esforço para atividades mais estratégicas, em vez de lidar com ameaças e incidentes de segurança.
- **Economicidade:** A solução de proteção abrangente contribuirá para a redução de custos no CJF. Ao prevenir ataques cibernéticos, minimizar o impacto de ameaças e evitar a perda de dados ou interrupções nas operações, o CJF evitará gastos significativos decorrentes da recuperação de incidentes, reparos de sistemas comprometidos e possíveis penalidades legais.
- **Aumento da produtividade:** A implementação de uma solução de proteção com funcionalidades de detecção, correlacionamento e resposta de incidentes resulta em maior produtividade e eficiência da equipe técnica de segurança de TI do CJF. Ao correlacionar os eventos recebidos dos *endpoints*, *Data Center*, serviço de *e-mail* corporativo e aplicativos de colaboração Microsoft 365, a equipe técnica conseguirá priorizar os incidentes mais críticos, de maior potencial de danos à segurança do Conselho, e automatizar a resposta a esses incidentes.
- **Fortalecimento da imagem institucional:** A solução de proteção abrangente também contribuirá para uma melhor governança de TI no CJF. Ao adotar medidas proativas para proteger seus ativos digitais, o CJF demonstrará um compromisso sólido com a segurança da informação e a conformidade regulatória. Isso fortalecerá a confiança dos cidadãos, dos parceiros e de outras instituições no CJF, reforçando sua reputação como uma organização responsável e confiável.

1.4 Demonstração da previsão da contratação no plano de contratações anual (Art. 18, § 1º, II, da Lei n. 14.133/2021)

A contratação está prevista no item 71 (Solução de segurança para proteção de servidores de rede, estações de trabalho, serviço de *e-mail* e Office 365) do Plano Anual de Contratações – 2023, acostado ao id. 0418266 do processo SEI n. 0000698-13.2022.4.90.8000.

1.5 Alinhamento entre a contratação e o planejamento estratégico

A contratação está alinhada com as seguintes diretrizes estratégicas aplicáveis ao Conselho da Justiça Federal:

1.5.1 Estratégia Nacional do Poder Judiciário 2021-2026 – Resolução CNJ n. 325, de 30 de junho de 2020:

- Macro desafio do Poder Judiciário: fortalecimento da estratégia nacional de TIC e de proteção de dados.

1.5.2 Estratégia Nacional de Segurança da Informação do Poder Judiciário – Resolução CNJ n. 396, de 7 de junho de 2021:

- Objetivos estratégicos: aumentar a resiliência às ameaças cibernéticas, permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

1.5.3 Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário 2021 – 2026 – Resolução CNJ n. 370 de 28 de janeiro de 2021:

- Objetivo estratégico: aprimorar a Segurança da Informação a Gestão de Dados.

1.5.4 Estratégia do Conselho da Justiça Federal – Portaria CJF n. 576, de 24 de junho de 2020:

- Objetivo estratégico: fortalecer a segurança da informação - promover ações que objetivam viabilizar e assegurar a disponibilidade, a integridade e a confidencialidade das informações, assim como a transparência e a proteção aos dados pessoais, desde a sua coleta até o seu processamento e o compartilhamento.

1.5.5 Plano Estratégico de Tecnologia da Informação da Justiça Federal – Resolução CJF n. 685, de 15 de dezembro de 2020:

- Objetivo estratégico: promover e fortalecer a segurança da informação digital na Justiça Federal.

1.5.6 Plano Diretor de Tecnologia da Informação 2021 – 2023 - Portaria CJF n. 600, de 11 de fevereiro de 2021:

- Iniciativa 4: Aprimorar serviços de TI do CJF.
- Iniciativa 6: Manter serviços de TI em operação.
- Iniciativa 13: Aperfeiçoar a infraestrutura de TI do CJF.
- Iniciativa 15: Aprimorar a Segurança da Informação do CJF e da JF.

1.6 Contratações correlatas e/ou interdependentes (Art. 18, § 1º, XI, da Lei n. 14.133/2021)

1.6.1 Contrato CJF n. 031/2018 - Contratação de solução de segurança para proteção de *endpoint* e *Data Center*, com garantia de 60 (sessenta) meses, contemplando os serviços de instalação e configuração, transferência de conhecimento e suporte técnico (Ata de Registro de Preços n. 015/2018-CJF);

1.6.2 Contrato CJF n. 008/2020 - Contratação de Serviços Gerenciados de Segurança da Informação;

1.6.3 Contrato CJF n. 013/2021 - Contratação de solução de segurança da informação do Conselho da Justiça Federal – CJF para proteção da Nuvem Privada da Justiça Federal - NUJUF (Solução de proteção para ambiente de Data Center virtual), contemplando fornecimento de equipamentos (*appliances*), licenciamento de *software*, serviços de instalação e configuração, suporte técnico e garantia.

1.7 Definição dos requisitos (Art. 18, § 1º, III, da Lei n. 14.133/2021)

1.7.1 Requisitos de negócio

1.7.1.1 Necessidade 1: Assegurar níveis de serviços de segurança da informação

adequados ao negócio.

1.7.1.2 Funcionalidade 1: Suporte técnico em regime ininterrupto (24x7) para o caso de falhas e interrupções do serviço

1.7.1.2.1 Ator Envolvido 1: Contratada.

1.7.1.2.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.1.2.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.1.2.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.1.2.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.1.3 Funcionalidade 2: Cobertura de garantia do fabricante durante todo o período de vigência do contrato

1.7.1.3.1 Ator Envolvido 1: Contratada.

1.7.1.3.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.1.3.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.1.3.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.1.4 Necessidade 2: Visualização integrada de detecções e riscos e a automatização de ações.

1.7.1.5 Funcionalidade 1: Interoperabilidade da solução de detecção e resposta avançada de incidentes e automação de respostas a partir do correlacionamento de dados recebidos pelas demais soluções que compõem o objeto.

1.7.1.5.1 Ator Envolvido 1: Contratada.

1.7.1.5.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.1.5.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.1.5.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.1.6 Funcionalidade 2: Console de administração unificada para gestão de riscos e eventos de segurança.

1.7.1.6.1 Ator Envolvido 1: Contratada.

1.7.1.6.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.1.6.3 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.1.7 Necessidade 3: Unificação das soluções de proteção dos ambientes tecnológicos do CJF e da NUJFE.

1.7.1.8 Funcionalidade 1: Registro de preços que contemple o licenciamento completo das soluções e a possibilidade de aquisição das licenças que vencem em 2023 e em 2024, abrangendo todos os ativos a serem protegidos no ambiente da NUJUFE.

1.7.1.8.1 Ator Envolvido 1: Contratada.

1.7.1.8.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.1.8.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.1.8.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2 Requisitos técnicos

1.7.2.1 Necessidade 1: Proteger os dispositivos finais de usuários (*endpoints*), servidores de rede e aplicações colaborativas do pacote Microsoft 365 contra ameaças cibernéticas.

1.7.2.2 Funcionalidade 1: Detecção e remoção de *malware* (vírus, *ransomware* e outras ameaças de *softwares* maliciosos).

1.7.2.2.1 Ator Envolvido 1: Contratada.

1.7.2.2.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.2.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.2.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.2.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.2.3 Funcionalidade 2: Monitoramento do tráfego de rede entre os ativos de rede com objetivo de detectar atividades maliciosas pela análise do tráfego de rede.

1.7.2.3.1 Ator Envolvido 1: Contratada.

1.7.2.3.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.3.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.3.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.3.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.2.4 Funcionalidade 3: Prevenção de intrusões em nível de *host* (HIPS) em tempo real para identificar e bloquear atividades suspeitas ou maliciosas visando prevenir ataques como exploração de vulnerabilidades conhecidas.

1.7.2.4.1 Ator Envolvido 1: Contratada.

1.7.2.4.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.4.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.4.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.4.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.2.5 Funcionalidade 4: Definição de políticas para controle dos aplicativos que podem ser instalados ou executados.

1.7.2.5.1 Ator Envolvido 1: Contratada.

1.7.2.5.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.5.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.5.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.5.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.2.6 Funcionalidade 5: Proteção de dados armazenados por meio de criptografia.

1.7.2.6.1 Ator Envolvido 1: Contratada.

1.7.2.6.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.6.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.6.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.6.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.2.7 Funcionalidade 6: Monitoramento e registro de atividades dos usuários nos

dispositivos finais e servidores de rede.

1.7.2.7.1 Ator Envolvido 1: Contratada.

1.7.2.7.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.7.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.7.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.7.5 Ator Envolvido 5: Demais áreas do CJP.

1.7.2.8 Funcionalidade 7: Análise de comportamento com utilização de aprendizado de máquina e algoritmos para identificar atividades anormais.

1.7.2.8.1 Ator Envolvido 1: Contratada.

1.7.2.8.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.8.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.8.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.8.5 Ator Envolvido 5: Demais áreas do CJP.

1.7.2.9 Funcionalidade 8: Geração e disponibilização de painéis detalhadas sobre a segurança dos *endpoints*, incluindo informações sobre ameaças detectadas, ações tomadas e conformidade com políticas de segurança.

1.7.2.9.1 Ator Envolvido 1: Contratada.

1.7.2.9.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.9.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.9.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.9.5 Ator Envolvido 5: Demais áreas do CJP.

1.7.2.10 Funcionalidade 9: Detecção, correlacionamento e resposta automatizada de incidentes identificados.

1.7.2.10.1 Ator Envolvido 1: Contratada.

1.7.2.10.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.10.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.10.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.10.5 Ator Envolvido 5: Demais áreas do CJP.

1.7.2.11 Funcionalidade 12: Monitoramento e análise do tráfego de rede visando identificar atividades maliciosas ou suspeitas.

1.7.2.11.1 Ator Envolvido 1: Contratada.

1.7.2.11.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.11.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.11.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.11.5 Ator Envolvido 5: Demais áreas do CJP.

1.7.2.12 Necessidade 2: Proteger o serviço de e-mail corporativo do CJP contra ameaças cibernéticas.

1.7.2.13 Funcionalidade 1: Identificação e bloqueio de mensagens indesejadas ou não

solicitadas, como *e-mails* de *phishing*, *spam*, *e-mails* em massa não autorizados e conteúdo malicioso por meio de filtros de *spam*.

1.7.2.13.1 Ator Envolvido 1: Contratada.

1.7.2.13.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.13.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.13.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.13.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.2.14 Funcionalidade 2: Verificação e detecção de *e-mails* em busca de sinais de atividades suspeitas ou tentativas de engenharia social (*phishing*).

1.7.2.14.1 Ator Envolvido 1: Contratada.

1.7.2.14.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.14.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.14.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.14.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.2.15 Funcionalidade 3: Verificação e análise de anexos de *e-mail* em busca de *malware*, vírus e outras ameaças.

1.7.2.15.1 Ator Envolvido 1: Contratada.

1.7.2.15.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.15.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.15.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.15.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.2.16 Funcionalidade 4: Verificação e reescrita de URLs contidas nos *e-mails* para identificação de links maliciosos ou suspeitos.

1.7.2.16.1 Ator Envolvido 1: Contratada.

1.7.2.16.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.16.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.16.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.16.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.2.17 Funcionalidade 5: Verificação de autenticidade do remetente de *e-mails* por meio de mecanismos de autenticação, como SPF (*Sender Policy Framework*), DKIM (*DomainKeys Identified Mail*) e DMARC (*Domain-based Message Authentication, Reporting, and Conformance*).

1.7.2.17.1 Ator Envolvido 1: Contratada.

1.7.2.17.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.17.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.17.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.17.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.2.18 Funcionalidade 6: Monitoramento e registro de atividades relacionadas ao envio,

recebimento e manipulação de mensagens de *e-mail*.

1.7.2.18.1 Ator Envolvido 1: Contratada.

1.7.2.18.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.18.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.18.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.18.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.2.19 Funcionalidade 7: Permitir que *e-mails* suspeitos ou potencialmente indesejados sejam isolados e retidos em uma área de quarentena pessoal, para análise e eventual liberação.

1.7.2.19.1 Ator Envolvido 1: Contratada.

1.7.2.19.2 Ator Envolvido 2: SUSTI - Subsecretaria de Segurança da Tecnologia da Informação.

1.7.2.19.3 Ator Envolvido 3: SUTEC - Subsecretaria de Tecnologia e Suporte Técnico.

1.7.2.19.4 Ator Envolvido 4: STI - Secretaria de Tecnologia da Informação.

1.7.2.19.5 Ator Envolvido 5: Demais áreas do CJF.

1.7.2.20 Funcionalidade 8: Geração de relatórios sobre a segurança dos *e-mails*, incluindo estatísticas de *spam*, ameaças bloqueadas, atividades de autenticação e conformidade com políticas de segurança.

1.7.2.20.1 Ator Envolvido 1: Contratada.

1.7.2.20.2 Ator Envolvido 2: Área de segurança da informação ou segurança de TI.

1.7.2.20.3 Ator Envolvido 3: Área de infraestrutura de TI.

1.7.2.20.4 Ator Envolvido 4: Área de atendimento ao usuário de TI.

1.7.2.20.5 Ator Envolvido 5: Usuários internos dos serviços de TI (magistrados, servidores, prestadores de serviço).

1.7.3 Requisitos de suporte

1.7.3.1 Será prestado suporte técnico em regime ininterrupto (24x7) para o caso de falhas e interrupções do serviço, com direito a atualizações de versões da solução que incorporem correções de defeitos e melhorias implementadas pelo fabricante.

1.7.4 Requisitos de capacitação

1.7.4.1 A contratada deverá realizar a transferência de conhecimento das principais funcionalidades da solução para a equipe técnica do CJF por meio de treinamento nas tecnologias da solução nas seguintes condições:

1.7.4.1.1 Uma turma de até cinco participantes.

1.7.4.1.2 Repasse dos conceitos e da utilização das funcionalidades sob perspectiva de administração da solução, contemplando como conteúdo todos os requisitos especificados neste instrumento.

1.7.4.1.3 Carga horária mínima de 20 horas.

1.7.5 Critérios de sustentabilidade

1.7.5.1 A CONTRATADA será responsabilizada por qualquer prejuízo que venha causar ao CJF por ter suas atividades suspensas, paralisadas ou proibidas por falta de cumprimento de normas ligadas ao *software* e ainda aos serviços elencados no presente Termo de Referência.

1.7.5.2 A CONTRATADA deverá, para a execução do contrato, fornecer aos empregados os

equipamentos de segurança que se fizerem necessários, para a execução de serviços, conforme disposto no art. 6º, inciso IV, da Instrução Normativa SLTI/MPOG n. 01, de 19 de janeiro de 2010;

1.7.5.3 A CONTRATADA deverá se atentar às normas em vigor atinentes à sustentabilidade expressas na 2ª edição do Manual de Sustentabilidade de compras e contratos do Conselho da Justiça Federal, instituído pela Portaria CJF n. 96, de 10 de fevereiro de 2023;

1.7.5.4 A CONTRATADA deverá respeitar a legislação vigente e as normas técnicas, elaboradas pela ABNT e pelo INMETRO para aferição e garantia de aplicação dos requisitos mínimos de qualidade e acessibilidade do *software* e ainda dos serviços elencados neste Termo de Referência.

1.7.6 Requisitos legais e normativos aplicáveis ao objeto da contratação

1.7.6.1 Resolução CJF n. 6/2008, alterada pela Resolução CF n. 687, de 15 de dezembro de 2020, que dispõe sobre a implantação da Política de Segurança da Informação do Conselho e da Justiça Federal de 1º e 2º graus;

1.7.6.2 Portaria CJF n. 303/2018, que define as normas a serem seguidas no CJF, relativas à utilização de recursos de tecnologia da informação, de forma a minimizar os riscos à segurança da informação na instituição;

1.7.6.3 Portaria CNJ n. 162/2021, 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); e

1.7.6.4 Portaria CJF n. 413/ 2014, que dispõe sobre a aprovação da Política de Controle Acesso Lógico, que veda a utilização de identificação genérica e de uso compartilhado para acesso aos recursos de rede.

1.7.7 Requisitos de confidencialidade

1.7.7.1 Requisito 1: A contratada e os prestadores de serviço deverão se comprometer formalmente a manter a confidencialidade e o sigilo de todas as informações restritas do contratante.

1.7.8. Requisitos temporais

1.7.8.1 A entrega da solução deverá ocorrer no prazo estipulado em contrato.

1.7.8.2 A contratada deverá assumir integralmente o suporte e garantia dos produtos descritos imediatamente após a emissão do Termo de Recebimento Definitivo da solução.

1.7.9 Requisitos de Segurança

1.7.9.1 Durante a prestação dos serviços a contratada deverá seguir a Política de Segurança e as normas de segurança emitidas pelo Comitê de Segurança da Informação da Justiça Federal – CSI-JUS e pela Comissão Local de Segurança da Informação dos órgãos partícipes, bem como os procedimentos das unidades gestoras do contrato.

1.8 Alternativas de soluções e análise de mercado de Tecnologia da Informação e Comunicação (Art. 18, § 1º, V, da Lei n. 14.133/2021)

Em levantamento preliminar de alternativas, incluindo o estudo realizado acerca de soluções utilizadas por outros entes da Administração Pública, foram encontradas as seguintes opções:

1.8.1 Alternativa 1: Contratação de solução de proteção de *endpoints*, *Data Center*, *antispam* e *Microsoft 365* atualmente em uso pelo CJF com expansão de novas funcionalidades de detecção e resposta avançada de incidentes.

1.8.1.1 Solução: Realização de licitação de renovação da solução atualmente em uso, com a inclusão de novas funcionalidades, e concorrência entre os parceiros autorizados do fabricante Trend Micro.

1.8.1.1.1 Custo estimado: R\$ 4.412.000,00, para 36 (trinta e seis) meses.

1.8.1.1.2 Análise: Esta alternativa se mostra viável tecnicamente pois o fabricante Trend Micro, atual fornecedor das soluções de segurança objeto desta contratação, é capaz de atender aos requisitos técnicos e de negócio para proteção do ambiente do CJF. A licitação seria nomeada (*part number*) e reduziria o custo administrativo da contratação. Contudo, a concorrência estaria limitada aos parceiros deste fabricante.

1.8.2 Alternativa 2: Contratação de solução de proteção de *endpoints*, *Data Center*, *antispam* e *Microsoft 365* com expansão de novas funcionalidades de detecção e resposta avançada de incidentes em ampla concorrência.

1.8.2.1 Solução: Realização de licitação na qual seja possível tanto a renovação das soluções em uso, com a inclusão de novas funcionalidades, quanto o fornecimento de soluções novas de outros fabricantes de segurança.

1.8.2.1.1 Custo estimado: R\$ 3.645.894,65

1.8.2.1.2 Análise: Esta alternativa é viável tecnicamente pois tanto o fabricante das soluções de segurança atuais quanto os concorrentes são capazes de atender aos requisitos técnicos e de negócio para a proteção no ambiente do CJF. Nesta opção se faz necessário especificar detalhadamente as especificações técnicas que deverão ser atendidas pelos fornecedores e, portanto, possui um maior custo administrativo para a equipe técnica. Porém, ficaria assegurada a competitividade do certame.

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1, 2	X		
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Federal?	1, 2	X		
A Solução está disponível no Portal do <i>Software</i> Público Brasileiro?	1, 2			X
A Solução é um <i>software</i> livre ou <i>software</i> público?	1, 2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1, 2			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1, 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq-Jus?	1, 2			X

1.9 Registro de soluções consideradas inviáveis

1.9.1 Alternativa 1: Implantação de solução de *software* livre / *software* público (de código aberto)

Nesta alternativa, o CJF realizaria a substituição dos produtos da solução atualmente em uso por produtos equivalentes de *software* livre / *software* público (de código aberto).

1.9.1.1 Solução 1: Implantação de solução de *software* livre / *software* público (de código aberto);

1.9.1.1.1 Análise: Dentre as desvantagens e limitações que tornam esta alternativa inviável para o CJF destaca-se o suporte técnico e recursos limitados das soluções disponíveis, impossibilidade de integração ou interoperabilidade com os demais ativos do ambiente tecnológico do CJF, dificuldade de instalação, transição e administração da solução devido ao corpo técnico reduzido do CJF, possibilidade de ocorrência de custos ocultos não passíveis de mapeamento prévio e ausência de garantias contratuais que poderiam deixar a organização em uma posição vulnerável em caso de problemas

significativos com a solução implantada. E principalmente, não há *software* livre que atualmente atenda plenamente aos requisitos técnicos e de negócio.

1.9.1.2 Solução 2: Realização de licitação com os parceiros do fabricante da solução atual do CJF apenas para os produtos atualmente em uso no CJF.

1.9.1.2.1 Análise: Esta alternativa é inviável pois não atende aos requisitos técnicos necessários para o enfrentamento das ameaças de segurança que se tornam cada vez mais complexas. Não contempla a implementação de novas funcionalidades e módulos de segurança voltados para a detecção, correlacionamento centralizado, resposta automatizada à incidentes e monitoramento e análise constante do tráfego de rede para identificação das atividades maliciosas ou suspeitas no ambiente.

1.10 Análise e comparação entre as estimativas de custos totais de propriedade das soluções de TIC

Solução	Custo mensal	Custo anual (12 meses)
Realização de licitação <u>apenas com os parceiros autorizados do fabricante da solução atual do CJF</u> , para os produtos atualmente em uso no CJF <u>com expansão de novas funcionalidades de detecção e resposta avançada de incidentes.</u>	R\$ 122.555,55	R\$ 1.470.666,66
Realização de licitação <u>com ampla concorrência</u> para as funcionalidades de proteção atualmente implementadas no ambiente do CJF <u>com expansão de novas funcionalidades de detecção e resposta avançada de incidentes.</u>	R\$ 101.274,85	R\$ 1.215.298,21

1.11 Justificativa da escolha da alternativa de solução a contratar

1.11.1 Alternativa/Solução escolhida:

Alternativa 2: Contratação de solução de proteção de *endpoints*, *Data Center*, *antispam* e Microsoft 365 com expansão de novas funcionalidades de detecção e resposta avançada de incidentes em ampla concorrência.

1.11.2 Custo estimado: R\$ 3.645.894,65

1.11.3 Justificativa:

No que concerne aos aspectos técnicos, as duas alternativas são semelhantes uma vez que devem fornecer as funcionalidades de segurança existentes bem como deverão incorporar as funcionalidades de segurança para a detecção avançada, resposta a ameaças cibernéticas em tempo real, de forma integrada, e com possibilidade de automação para tratamento dos incidentes identificados.

No que se refere à possibilidade de concorrência, as duas alternativas possuem fornecedores em número suficiente para, teoricamente, ocorrer um mínimo de concorrência. Sendo que na alternativa 1 a concorrência se daria entre os fornecedores do fabricante fornecedor da solução atualmente em uso no órgão. Enquanto na alternativa 2 a concorrência se daria entre os fornecedores dos fabricantes de segurança capazes de atender aos requisitos técnicos e de negócio previstos. A alternativa 2 se mostra mais vantajosa pois possibilita as duas formas de fornecimento, seja renovação ou substituição, e a garantia da maior competição possível. Garantindo transparência e a adoção dos mesmos critérios de atendimento das especificações técnicas, de forma justa e imparcial.

No que tange aos aspectos financeiros, a alternativa 2 se mostra mais vantajosa por permitir que diversos fabricantes que atendam aos requisitos técnicos e de negócio possam participar do pregão. Desde modo, espera-se que em virtude da concorrência maior haja redução nas propostas das

empresas na etapa de lances. É importante salientar que o investimento já realizado pelo órgão na última contratação será preservado pois a licitante vencedora deverá ofertar o menor preço global da solução, já considerando o custo de renovação das licenças previamente adquiridas. A competição entre diversos fabricantes acaba por reduzir o preço final da contratação pois, no mínimo, força o fabricante da atual solução a baixar seus preços, o que normalmente não ocorreria em uma renovação nominada.

Quanto aos aspectos de viabilidade e conformidade, a alternativa 2, visa assegurar a viabilidade e a conformidade legal do processo de aquisição. A licitação com ampla concorrência atende aos princípios da administração pública de competitividade, isonomia e transparência, assegurando que a escolha dos fornecedores seja baseada em critérios objetivos e impessoais.

Dessa forma, a contratação dos solução de proteção de *endpoints*, *Data Center*, *antispam* e Microsoft 365 atualmente em uso pelo CJF com expansão de novas funcionalidades, Alternativa 2, apresenta-se como uma escolha adequada e estratégica para o CJF, assegurando a melhor relação custo-benefício, eficiência técnica e conformidade legal no processo de aquisição desses itens essenciais para a segurança da instituição.

1.12 Descrição da solução de TI a contratar como um todo (Art. 18, § 1º, VII, da Lei n. 14.133/2021)

Contratação de solução de segurança de TI para proteção de estações de trabalho, *Data Center*, *e-mail* corporativo e aplicativos Microsoft 365 contemplando instalação e configuração, transferência de conhecimento e suporte técnico com garantia do fabricante para atender as necessidades do Conselho da Justiça Federal, pelo prazo de 36 (trinta e seis) meses. Tais serviços são de prestados de forma contínua, conforme classificação da Instrução Normativa CJF n. 12/2022, art. 5º, inciso XXIII, alínea *k*.

1.13 Relação entre a demanda prevista e a quantidade dos bens e/ou serviços a serem contratados (Art. 18, § 1º, IV, da Lei n. 14.133/2021)

O quantitativo do licenciamento dos produtos da solução foi baseado em levantamento por meio de ferramentas de gerência do ambiente do CJF e da NUJUFÉ abrangendo todas as estações de trabalho, servidores de rede e de armazenamento (*storage*), usuários Microsoft 365 e caixas de correio corporativas, conforme informado no quadro da Estimativa preliminar do custo total da contratação deste documento.

Para o licenciamento das estações de trabalho e servidores de armazenamento foram consideradas as quantidades calculadas para o contrato CJF 031/2018 e que continuam atendendo à quantidade contabilizada em julho/23.

O licenciamento de caixas de correio considerou o total de caixas postais gerenciadas pelo serviço de *e-mail* corporativo MS Exchange, tanto de usuários e quanto de unidades (caixas corporativas).

O quantitativo de usuários Microsoft 365 foi baseado no total de licenças Office 365 E1e Microsoft 365 E3 constante no id. 0465117 do processo SEI n. 0003441-13.2022.4.90.8000.

O quantitativo de licenças para proteção de *Data Center* está incluído tanto o ambiente de *Data Center* do CJF quanto da NUJUFÉ. Para o ambiente do CJF, são necessárias 20 (vinte) licenças de *sockets*, das quais, atualmente, 18 (dezoito) estão cobertas pelo Contrato CJF n. 031/2018, com validade até 26/12/23. Para o ambiente da NUJUFÉ, são necessárias 40 (quarenta) licenças de *sockets*, as quais estão cobertas pelo Contrato CJF n. 013/2021, com validade até 08/08/24. Desta maneira, para este último, a demanda somente será realizada em 2024 mediante emissão de Ordem de Serviço para a Contratada.

O serviço de instalação e configuração está previsto para ocorrer em uma única atividade assim que as licenças e agentes da solução estejam disponíveis conforme cronograma de entrega.

O serviço de suporte técnico mensal está dimensionado para atendimento durante toda a vigência do contrato estipulado para 36 meses.

O repasse de conhecimento está dimensionado para a equipe de administração de soluções de segurança do CJF e eventuais servidores relacionados com a administração da solução em uma turma de até 5 participantes.

1.14 Estimativa preliminar do custo total da contratação (Art. 18, § 1º, VI, da Lei n. 14.133/2021)

ITEM	DESCRIÇÃO	UNIDADE	QTD	PREÇO UNITÁRIO	PREÇO TOTAL
1	Proteção para estações de trabalho	Dispositivo	580	R\$ 411,23	R\$ 238.515,72
2	Proteção para Serviço de <i>E-mail</i>	Usuário	1300	R\$ 176,92	R\$ 230.000,00
3	Proteção para Microsoft 365	Usuário	550	R\$ 272,73	R\$ 150.000,00
4	Proteção para <i>Data Center</i>	Socket	60	R\$ 20.731,71	R\$ 1.243.902,60
5	Proteção para Storage	Servidor	2	R\$ 30.000,00	R\$ 60.000,00
6	Inspeção de Tráfego de Rede (NDR) para 4Gbytes	Solução	1	R\$ 1.450.000,00	R\$ 1.450.000,00
7	Instalação e Configuração	Serviço	1	R\$ 25.000,00	R\$ 25.000,00
8	Suporte Técnico Mensal	Meses	36	R\$ 6.500,00	R\$ 234.000,00
9	Repasse de conhecimento para até 5 participantes	Turma	1	R\$ 14.476,33	R\$ 14.476,33
TOTAL:					R\$ 3.645.894,65

1.15 Necessidades de adequação do ambiente do órgão para viabilizar a execução contratual (Art. 18, § 1º, X, da Lei n. 14.133/2021)

Não há necessidade de adequação do ambiente do CJF tendo em vista tratar-se de solução que operará no ambiente computacional já existente.

2 Sustentação do Contrato

2.1 Recursos materiais e humanos necessários à execução contratual

2.1.1 Recursos orçamentários estimados:

2.1.1.1 Recurso 1: Orçamento

2.1.1.2 **Quantidade:** R\$ 3.645.894,65

2.1.1.3 **Disponibilidade:** Contínua

2.1.1.4 **Ação para Obtenção do Recurso:** Priorizar a contratação da solução e prever o recurso orçamentário para continuidade da execução contratual dos serviços de suporte técnico.

2.1.1.5 **Responsável:** Secretário de TI.

2.1.2 Equipe de fiscalização:

2.1.2.1 **Gestor do contrato:** dedicação estimada em aproximadamente 30min/dia.

2.1.2.2 **Fiscal técnico da STI:** dedicação estimada em aproximadamente 30min/dia.

2.1.2.3 **Fiscal administrativo da SAD:** dedicação estimada em aproximadamente 30min/mês.

2.2 Continuidade do fornecimento da solução de TIC em eventual interrupção contratual

2.2.1 Indisponibilidade orçamentária

2.2.1.1 **Ação de Contingência:** Remanejar o orçamento para atender a manutenção de atividade continuada.

2.2.1.2 **Responsável:** STI, SAD e SPO

2.2.2 Empresa impedida de prosseguir com a prestação do serviço

2.2.2.1 Ação de Contingência: Atualizar o termo de referência; Contratação emergencial; Realização de nova licitação.

2.2.2.2 Responsável: Gestor do contrato, Fiscal Técnico, STI e SAD

2.2.3 Fracasso do processo licitatório

2.2.3.1 Ação de Contingência: Análise do resultado e execução de nova licitação.

2.2.3.2 Responsável: STI e SAD.

2.2.4 Evento 4: Falência da contratada:

2.2.4.1 Ação de Contingência: Iniciar a contratação de nova prestadora de serviços de forma emergencial, até a finalização de novo processo de contratação e licitação dos serviços.

2.2.4.2 Responsável: STI e SAD.

2.3 Atividades de transição contratual e de encerramento do contrato

2.3.1 Atividade: documentar e armazenar, no CJF, todos os trabalhos/serviços produzidos pelos profissionais da CONTRATADA.

2.3.1.1 Responsável: Equipe de fiscalização do contrato

2.3.1.2 Período: mensal

2.3.2 Atividade: contratar nova empresa para a continuidade do serviço.

2.3.2.1 Responsável: Equipe de planejamento da contratação

2.3.2.2 Período: 1 ano antes do encerramento do contrato

2.4 Estratégia de independência do órgão

2.4.1 Transferência de Conhecimento:

2.4.1.1 Item 1: Manutenção de base de conhecimento.

2.4.1.2 Forma de Transferência do Conhecimento: Realizar a documentação dos procedimentos realizados durante a implantação da solução em base de conhecimento do CONTRATANTE.

2.4.2 Competência técnica:

2.4.2.1 Item 2: Atualização tecnológica continuada da equipe técnica.

2.4.2.2 Forma de Gestão do Conhecimento: Participação regular em eventos e ações de capacitação relacionadas às tecnologias de segurança cibernética, permitindo que a equipe técnica consiga criticar as entregas e configurações das soluções bem como acompanhar a evolução tecnológica do mercado e acompanhar a necessidade de modernização das proteções.

2.5 Justificativa para o parcelamento ou não do objeto (Art. 18, § 1º, VIII, da Lei n. 14.133/2021)

O objeto do certame não será parcelado, uma vez que os serviços técnicos especializados que compõe o objeto formam um conjunto indissociável, composto pela interligação dos serviços que funcionam harmonicamente.

As melhores práticas de implementação da solução se baseiam na integração dos serviços, que são indissociáveis e apresentam inter-relação entre si, de forma que assegurem o alinhamento e a coerência em termos de qualidade técnica, resultando assim, no perfeito atendimento dos princípios da celeridade, economicidade e eficiência.

Somente a execução de forma integrada dos serviços garante a qualidade das entregas, evitando transferência de responsabilidades, nos casos de eventuais problemas causados por serviços prestados por mais de uma empresa contratada.

É importante, também, se observar o posicionamento do Egrégio Tribunal de Contas da União, nos autos

do Acórdão n. 1916/2009 – Plenário, sobre a matéria: “15. Acerca da alegada possibilidade de fragmentação do objeto, vale notar que nos termos do art. 23, § 1º, da Lei n. 8.666/1993, exige-se o parcelamento do objeto licitado sempre que isso se mostre técnica e economicamente viável. A respeito da matéria, esta Corte de Contas já editou a Súmula n. 247/2004, in verbis: “É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes...” (grifos não constam do original).

Nesse toar, mencionamos o Acórdão TCU n. 5134/2014 – 2ª Câmara, de modo que a interpretação da Súmula 247 TCU e do art. 23, §1º da Lei n. 8.666/1993 não deve ser feita de modo literal, já que itens de mesma natureza devem compor um único lote, não havendo restrição ao caráter competitivo do certame.

Depreende-se, portanto, que a divisão do objeto deverá ser implementada sempre que houver viabilidade técnica e econômica para a sua adoção.

Nesse ponto, calha trazer à baila o escólio de Marçal Justen Filho: “O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. Não é possível desnaturar um certo objeto, fragmentando-o em contratações diversas e que importam o risco de impossibilidade de execução satisfatória.” (Comentários à Lei de Licitações e Contratos Administrativos. 10. ed. São Paulo: Dialética, 2004. p. 209).

Ainda, de acordo com a Lei 14.133/2021 em seu art. 47, inciso II, as licitações de serviços atenderão ao princípio do parcelamento, quando for tecnicamente viável e economicamente vantajoso. Portanto, em virtude da especificidade do objeto, pode-se afirmar ser tecnicamente inadequado o seu desmembramento, sob pena de não se atender o objetivo buscado, que é proporcionar maior celeridade e qualidade na implementação da solução de segurança da informação. Sob o ponto de vista econômico, não há elementos nos autos que permitam concluir que a adoção do parcelamento do objeto, seria, no caso concreto, mais vantajosa para o CJF.

Tendo em vista que uma das necessidades de negócio definida para esta contratação consiste na interoperabilidade da solução de detecção e resposta avançada de incidentes e automação de respostas decorrente do correlacionamento dos dados recebidos pelos demais itens que compõem o objeto, não é possível contratar tais itens em separado. Neste caso, o parcelamento provocaria restrições de funcionalidade na interoperabilidade pretendida.

2.6 Margem de Preferência

- **Lei 8.248/1991 e Decreto 7.174/2010:**

o Não se aplica a Lei 8.248/1991, pois não há previsão em seu art. 16-A de serviços relacionados à contratação de solução de segurança de TI para proteção de servidores de rede, estações de trabalho, serviço de *e-mail* e Microsoft 365. Consequentemente, afasta-se a aplicação do Decreto 7.174/2010, o qual regulamenta a lei supracitada.

- **Decreto 8.538/2015:**

o Não se aplica o referido decreto pois o tratamento diferenciado e simplificado para as microempresas e as empresas de pequeno porte não é vantajoso para a Administração Pública e pode representar prejuízo ao conjunto ou ao complexo do objeto a ser contratado, conforme mencionado no item 2.5 (Justificativa para o parcelamento ou não do objeto), uma vez que os serviços técnicos especializados que compõem o objeto formam um conjunto indissociável, composto pela interligação dos serviços que funcionam harmonicamente. Assim preconizado no Art. 10, inciso II, do normativo mencionado.

3 Posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina (Art. 18, § 1º, XIII, da Lei n. 14.133/2021)

Declara-se a viabilidade da contratação considerando a necessidade do manter a proteção dos *endpoints*, servidores de rede, serviço de *e-mail* corporativo e serviços colaborativos do Microsoft 365 utilizados pelo CJF.

4 Equipe de Planejamento e Apoio a Contratação - EPAC

O presente Estudo Técnico Preliminar foi elaborado pela Equipe de Planejamento e Apoio a Contratação, designada pela Portaria CJF n. 547/2023 (id. 0490449), consoante ao processo SEI n. 0001703-88.2023.4.90.8000, identificada adiante:

Integrante	Nome	Matrícula	Situação
Demandante	Renato Solimar Alves	673	Titular
Técnico	Nélio Alves da Silva	999	Titular
	Renato Solimar Alves	673	Suplente
Administrativo	Michael da Silva Placido	1102	Titular
	Rafael Veloso Mizuno	1059	Suplente



Autenticado eletronicamente por **Nélio Alves da Silva**, Chefe - Seção de Segurança de Rede , em 14/09/2023, às 16:26, conforme art. 1º, §2º, III, b, da [Lei 11.419/2006](#).



Autenticado eletronicamente por **Renato Solimar Alves**, Subsecretário(a) - Subsecretaria de Segurança da Tecnologia da Informação, em 14/09/2023, às 17:28, conforme art. 1º, §2º, III, b, da [Lei 11.419/2006](#).



Autenticado eletronicamente por **Michael da Silva Placido**, Diretor(a) da Divisão de Apoio ao Planejamento e à Fiscalização, em exercício, em 14/09/2023, às 18:25, conforme art. 1º, §2º, III, b, da [Lei 11.419/2006](#).



A autenticidade do documento pode ser conferida no site https://sei.cjf.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0497062** e o código CRC **7C098BEF**.

Setor de Clubes Esportivos Sul - Lote 09 - Trecho III - Polo 8 - Bairro Asa Sul - CEP 70200-003 - Brasília - DF - www.cjf.jus.br

Processo nº0001703-88.2023.4.90.8000

SEI
nº0497062