ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

DOCUMENTO DE OFICIALIZAÇÃO DE DEMANDA – DOD

CÓDIGO PAC 2024: TJCESETIN_2024_031
AQSETIN2022020 - Soluções de Segurança – Firewall grande porte

1. INTRODUÇÃO

Este documento tem como finalidade formalizar o início do processo de planejamento da contratação de uma **solução de Segurança da Informação para proteção do perímetro de rede (Firewall de grande porte)**, vincular as necessidades da contratação desejada aos objetivos estratégicos de TI e às necessidades corporativas da instituição, garantindo alinhamento ao Plano Estratégico Institucional e ao Painel de Contribuição da TI, indicar a fonte de recursos para a contratação e indicar os integrantes da Equipe de Planejamento da Contratação.

PREENCHIMENTO PELA ÁREA DEMANDANTE

2. IDENTIFICAÇÃO DA ÁREA DEMANDANTE

Área Demandante (Unidade/Setor/Gerência/Coordenação/Seção): SETIN/Gerência de Infraestrutura de TI

Nome do/da Projeto/Aquisição: Soluções de Segurança – Firewall grande porte: ampliação/renovação

Responsáveis pela Demanda: Cristiano Henrique Lima de Carvalho

Matrícula: 5198

E-mail: cristiano.carvalho@tjce.jus.br

Telefone:

3. IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE DEMANDANTE

Nome	Heldir Sampaio Silva	**Matrícula**	9630
Cargo	Coordenador de Segurança da Informação	**Lotação**	Coordenadoria de Segurança da Informação

E-mail	heldir.sampaio@tjce.jus.br	**Telefone**	-
Por este instrumento declaro ter ciência das competências do INTEGRANTE DEMANDANTE definidas na Resolução CNJ n° 468, de 15 de julho de 2022 - capítulo 2, item 2.1, subitem 1 do Guia de Contratações do Poder Judiciário, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.			
Heldir Sampaio Silva – 9630 Integrante Demandante			
Fortaleza, 30 de março de 2023.			

4. IDENTIFICAÇÃO DA DEMANDA

4.1. Aumento da demanda por cibersegurança em um ambiente complexo de prestação de serviços ao público, juntamente com a crescente complexidade e diversidade das ameaças digitais, representam um grande desafio para o Tribunal de Justiça do Estado do Ceará (TJCE) em garantir a segurança de seus sistemas de informação.

4.2. Para atender à necessidade de uma solução mais avançada de monitoramento e detecção de ameaças, capaz de garantir a integridade dos dados e sistemas e responder rapidamente a incidentes de segurança, o Tribunal busca por uma solução de alta disponibilidade de Next Generation Firewall com gerenciamento centralizado e integrado, garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local ou remoto, no modelo 24x7, pelo prazo de 60 (sessenta) meses, incluindo serviços de instalação e treinamento.

5. ALINHAMENTO AOS PLANOS ESTRATÉGICOS

ID	Objetivo Estratégico Institucional	ID	Objetivos de Contribuição da Setin
01	Fortalecer a inteligência de dados e a segurança da informação	01	Proporcionar segurança, disponibilidade e confiabilidade às informações dos sistemas, plataformas e ferramentas institucionais

6. ALINHAMENTO AO PDTIC – PLANO DIRETOR DE TIC 2021-2022

ID	INICIATIVA ELENCADA NO PDTIC (2021-2022)

N5	Soluções de Segurança – Firewall grande porte

7. METAS DO DESDOBRAMENTO ESTRATÉGICO DE TI A SEREM ALCANÇADAS

INDICADOR	META
Índice de Serviços Críticos com Gestão de Risco.	Mede o percentual de serviços críticos que possuem a gestão de risco implementada ao(s) seu(s) processo(s) - 40% em 2023.
Índice de conformidade com as políticas de segurança de TIC.	Mede o grau de atendimento às políticas de segurança de TIC com base no percentual de cumprimento de itens das normas - 60% em 2023.
Índice de integração de soluções de TIC.	Mede o percentual de atendimento ao Plano de integração de soluções de TIC - 80% em 2023.
Percentual de execução do Plano de soluções inovadoras e integradas de TIC.	Mede o percentual de execução do Plano de soluções inovadoras e integradas de TIC- 60% em 2023.

8. ALINHAMENTO AO PLANO ANUAL DE CONTRATAÇÕES 2023

ITEM	DESCRIÇÃO
TJCESETIN_2024_0016	Aquisição Firewall Grande Porte

9. MOTIVAÇÃO/JUSTIFICATIVA

9.1. Situação Atual

9.1.1. O TJCE possui dados e informações que necessitam de proteção constante e sem interrupções. Os possíveis danos causados por ataques cibernéticos podem comprometer a confidencialidade, integridade, disponibilidade, autenticidade e privacidade dos dados institucionais, bem como, os serviços e a rede corporativa, o que pode causar prejuízos para a prestação jurisdicional. Os prejuízos podem ser tangíveis ou intangíveis, e comprometer a imagem da instituição perante a sociedade. Por estas razões, reconhecemos que soluções robustas, performáticas e estáveis sejam utilizadas para defesa, controle e mitigação de ameaças digitais, auxiliando na manutenção da disponibilidade das atividades institucionais e reduzindo riscos que podem impactar diretamente nas estratégias do negócio.

9.1.2. O TJCE utiliza estratégia de proteção em camadas de segurança. Esta estratégia consiste em criar várias camadas de proteções distintas e complementares, sendo cada camada atuando de forma especializada em algum componente de segurança. Uma das principais

camadas de proteção é a solução composta de Firewall de próxima geração, cujo nome Firewall é o nome dado ao dispositivo de uma rede de computadores que tem por função regular, analisar e determinar quais operações de transmissão ou recepção de dados podem ser executadas a partir de um conjunto de regras ou instruções, inspecionando, controlando e bloqueando o tráfego proveniente da Internet para os sistemas e serviços do TJCE, e também aplicar políticas e restrições de acessos inter-redes e controlar os acessos dos usuários internos para a Internet. Sua finalidade consiste em bloquear o tráfego de dados indesejado e liberar acessos impedindo a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.

9.1.3. Atualmente o TJCE dispõe de uma solução de Firewall de próxima geração de alta disponibilidade que atua simultaneamente na proteção do ambiente de servidores (perímetros) e na proteção borda de acesso à Internet.

9.1.4. O Poder Judiciário Cearense com o intuito de prover a segurança de rede e controlar os acessos à internet, protegendo contra possíveis tentativas de acesso indevido adquiriu através do contrato CT Nº 17/2018, celebrado com a empresa Teltec Solutions Ltda, uma solução segurança de rede (Firewall) composta por:

9.1.4.1. 01 (uma)Solução de Plataforma de Segurança em cluster Palo Alto Networks PA-5220 composta por 02 (dois) Firewalls de Próxima Geração;

9.1.4.2. 01 (uma) Garantia da Solução de Plataforma de Segurança em cluster Palo Alto Networks PA-5220 com Suporte Oficial Palo Alto Networks 24x7 fornecido no Brasil em português por ASC (Authorized Support Center) e com serviço de suporte técnico remoto por 60 meses;

9.1.4.3. 02 (duas Assinatura Threat prevention para Solução de Plataforma de Segurança em cluster Palo Alto Networks PA-5220;

9.1.4.4. 02 (duas) Assinatura URL filtering para Solução de Plataforma de Segurança em cluster Palo Alto Networks PA-5220;

9.1.4.5. 02 (duas) Assinatura WildFire para Solução de Plataforma de Segurança em cluster Palo Alto Networks PA-5220;

9.1.4.6. 02 (dois) Módulos de Interface 1000BASE-T;

9.1.4.7. 14 (quatorze) Módulos de interface 10GBASE-SR;

9.1.4.8. 01 (um) Software Panorama para Gerenciamento Palo Alto Networks Panorama para Solução de Plataforma de Segurança em cluster Palo Alto Networks PA-5220; e

9.1.4.9. 01 (uma) Garantia do Software para Gerenciamento Palo Alto Networks Panorama com Suporte Oficial Palo Alto Networks 24x7 fornecido no Brasil em português por ASC (Authorized Support Center) por 60 meses.

9.1.5. A infraestrutura mencionada é utilizada pelo Judiciário Cearense sendo formada por equipamentos, subscrições de softwares e software de gerência, que compõem a solução de perímetro de segurança da informação que provê, além da segurança, a integridade dos dados trafegados entre os serviços Judiciais e Administrativos, através de uma rede de dados.

9.2. Descrição da Oportunidade ou do Problema

9.2.1. A aquisição da solução acima mencionada foi contemplada através da celebração do contrato CT Nº 17/2018, celebrado com a empresa Teltec Solutions Ltda. Devido a dilação temporal do fornecimento dos mesmos, a atual infraestrutura de conectividade da solução acima encontra-se com os serviços de garantia e suporte a vencer no dia 28 de julho de 2023, o que pode implicar em riscos de segurança no que diz respeito à trafegabilidade e a integridade dos dados. Em caso de falha, por não estarem cobertos pela política de suporte de seus respectivos fabricantes/fornecedores, os componentes da solução podem vir a gerar a indisponibilidade dos Sistemas Judiciais e Administrativos, bem como, não atualização das subscrições para controle de ameaças conhecidas e desconhecidas, e impactos na filtragem de URL.

9.2.2. Ao longo do período do contrato, destaque para o ano de 2020, ano em que a COVID-19 foi caracterizada pela OMS como uma pandemia, levou o Tribunal de Justiça do Estado do Ceará a adotar o Teletrabalho para todos os magistrados, servidores e colaboradores. Desta forma, ao longo do período surgiram novas necessidades que precisam, além das já atendidas pela solução atual, ser atendidas por uma Solução de Proteção de Redes (Firewall de Grande Porte), por exemplo: no entanto, ao longo da pandemia foi detectado outras necessidades que a solução atual não vem atendendo, tais como: falta de mapeamento e/ou bloqueio assertivo dos equipamentos que forem identificados realizando ações maliciosas; bloquear o acesso de um determinado dispositivo a rede, seja de forma automática ou manual; verificação de novas ameaças em tempo real, uso da Inteligência artificial para prevenção de ameaças e ameaças avançadas, análise de um maior fluxo de informações devido ao aumento de banda dos links de internet das Comarcas do interior, prevenção, detecção e resposta a incidentes baseadas nos eventos gerados pelo firewall, localização de anomalias dentro do ambiente com o uso de inteligência artificial, necessidade de integração com tecnologias de proteção de endpoints e servidores.

9.2.3. O Poder Judiciário do Estado do Ceará usa o Cinturão Digital do Governo do Ceará para o fornecimento de Internet e dos Serviços de Sistemas para as comarcas do interior, tal utilização necessita constantemente de controles centralizados para controlar o tráfego

de rede entre o cinturão, as comarcas e os ambientes computacionais do Tribunal de Justiça do Estado do Ceará (TJCE) e dos Fóruns.

9.2.4. Para manter o nível adequado de segurança da informação, há a necessidade de manter e expandir o controle de acesso de usuários e de outros aplicativos a sites, além de garantir que as informações existentes neste Poder estejam protegidas contra-ataques maliciosos, no que tange às ameaças provenientes de ataques internos e externos.

9.2.5. A Secretaria de Tecnologia da Informação (Setin), através da aquisição desta solução, direciona os seus esforços para perseguir uma abordagem moderna de segurança, chamada de Zero Trust.

9.2.6. Avançando para o caminho do Zero Trust, esta aquisição deverá contemplar atualização e expansão da solução de segurança de perímetro para incrementar a função de proteção do Data center do TJCE.

9.2.7. A estratégia de aquisição dos ativos de TI deve ser trabalhada de forma a implementar uma política de substituição e descarte, conforme, o guia com as Diretrizes para Contratação de Ativos de TIC vinculado à Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, conforme § 2º do Art. 8º. A última fase do clico de vida dos bens de TI têm baixa comercialização e alto custo de manutenção. São compostos normalmente pelos ativos que fazem parte do legado tecnológico da instituição. Necessário que se observe que para equipamentos Tecnologia da Informação, há ciclos de atualização padrão em que à medida que os equipamentos envelhecem, os riscos variados de falha aumentam, por exemplo, no que se referem a Firewall: para equipamentos com menos de 4 anos o risco é baixo, para equipamentos de uso entre 4 a 6 anos, o risco é moderado, e para equipamentos acima de 6 anos, o risco é alto, desta forma faz-se necessário a atualização tecnológica da solução atual para mitigar o risco de natureza moderada no ano de 2023, e alto, a partir de 2024.

9.2.8. Considerando que a solução referente ao CT nº 17/2018 foi implementada em 2018, e em 2023 completar-se-á 5 (cinco) anos, nos remete para em 2023, os riscos variados de falha, passam a ser moderados, e em 2024, os riscos variados de falha, passam a ser alto. Em situações em que os riscos de falha passam a ser moderados e estão na eminência de se tornarem altos, é recomendado adotar um "Tech refresh", conhecido como atualização tecnológica, *"é o ciclo de atualização regular dos principais elementos de infraestrutura de TI para maximizar o desempenho do sistema. Em vez de usar os sistemas até que não possam mais funcionar, muitas empresas optam por atualizar ou substituir determinadas infraestruturas regularmente. Esse processo costuma ser chamado de atualização tecnológica". A manutenção da infraestrutura legada pode se tornar cara. A tecnologia*

de data center desatualizada pode levar a atrasos no desempenho e na entrega de serviços, ineficiências no consumo de energia e espaço e sobrecarga administrativa excessiva. Enquanto isso, os custos de manutenção de ativos de TI obsoletos e os riscos de falha aumentam, aumentando as preocupações e os desafios orçamentários.

9.2.9. Além de manter as funções de proteções atuais, será necessária uma expansão nas ferramentas e mecanismos de segurança para fazer frente ao considerado aumento do número de ataques cibernéticos e atendimento das seguintes Resoluções e Portarias:

9.2.9.1. artigo 2° da Resolução 370/2021 do CNJ, onde estabelece como objetivos estratégicos o seguinte tema: "Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados";

9.2.9.2. atender o inciso V, Art. 11., da Resolução CNJ Nº 396 de 07/06/2021, que Instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), e determina que para elevar o nível de segurança das infraestruturas críticas, deve-se: utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da internet;

9.2.9.3. atender a alínea b), inciso VII, Art. 24., Resolução CNJ Nº 396, em que a Política de Segurança Cibernética do Poder Judiciário estabelece como objetivo o tema em orientar ações relacionadas à segurança da informação das infraestruturas críticas. Tema este reforçado no Manual de Referência – Proteção de Infraestruturas Críticas de TIC, Anexo IV da Portaria CNJ N° 162, de 10 de junho de 2021.

9.3. Motivação da Demanda

9.3.1. Como o prazo de garantia/suporte/subscrições dos hardware e software adquiridos por meio do CT Nº 17/2018 expirarão em 2023, e considerando o aumento dos riscos variados de falha, à medida que os equipamentos envelhecem, e as Resoluções e Portarias acima citadas, faz-se necessário uma solução de Next Generation Firewall para atender a atual demanda, continuar a oferecer os serviços já citados acima, bem como, as novas necessidades citadas no item 9.2.2 propiciando ganhos na segurança, estabilidade, disponibilidade e desempenho dos Sistemas Administrativos e Judiciais que utilizam a solução atual.

9.4. Ciclo de Vida da Demanda

9.4.1. A solução demandada será utilizada por um período de 60 (sessenta) meses.

9.5. Clientes que farão uso da solução (objeto da demanda) ou serão beneficiados

9.5.1. Todos os usuários que precisam usar os serviços disponibilizados pelo Poder Judiciário do Estado do Ceará através de recursos de Tecnologia da Informação e Comunicação.

9.6. Expectativa de entrega da solução

9.6.1. A Solução Integrada deverá ser entregue e instalada, até setembro de 2024.

10. RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

10.1.1. Manutenção e controle do tráfego de rede;

10.1.2. Filtrar o conteúdo da Web:

10.1.2.1. Garantir que apenas navegadores web e clientes de e-mail suportados possam ser executados na organização, idealmente utilizando apenas a versão mais recente disponibilizada pelo fabricante.

10.1.2.2. Desinstalar ou desabilitar plug-ins ou aplicações add-on não autorizados para navegadores web e clientes de e-mail.

10.1.2.3. Utilizar filtros de URL baseados em rede de forma a limitar a possibilidade de sistemas se conectarem a websites não aprovados pela organização. Tais filtros devem ser impostos a todos os sistemas da organização, quer se encontrem dentro do espaço físico da organização, quer não.

10.1.2.4. Subscrever serviços de categorização de URLs de forma a garantir que o filtro esteja atualizado com base nas mais recentes definições de categorias de sítios eletrônicos disponíveis. Sites não categorizados devem ser bloqueados por padrão.

10.1.2.5. Realizar registros de log de todas as requisições a URLs a partir de cada um dos sistemas da organização, quer nas dependências corporativas, quer em dispositivos móveis, de forma a identificar potenciais atividades maliciosas e auxiliar operadores de incidentes com a identificação de sistemas potencialmente comprometidos.

10.1.2.6. Utilizar serviços de filtragem de DNS para auxiliar no bloqueio de acessos a domínios maliciosos.

10.1.3. Prevenção da rede interna contra ameaças cibernéticas digitais;

10.1.4. Análise preventiva a incidentes de segurança: prevenção, detecção e resposta a incidentes baseadas nos eventos gerados pelo firewall;

10.1.5. Coleta e tratamento de dados relacionados a segurança;

10.1.6. Filtrar os dados;

10.1.7. Estabelecimento de canal de comunicação seguro através da VPN;

10.1.8. Aumento da confidencialidade, integridade e disponibilidade das informações do Poder

Judiciário do Estado do Ceará;

10.1.9. Aumento da proteção da rede interna contra possíveis tentativas de acesso indevido;

10.1.10. Implementação de mecanismos de proteção, prevenção de intrusão;

10.1.11. Implementação de regras de segurança, além de proteção específica em nível de aplicações como correio eletrônico, servidores WEB;

10.1.12. Melhoria da qualidade dos serviços, da proteção das informações da instituição e da produtividade dos usuários; e

10.1.13. Capacitação e qualificação da equipe de TIC do Poder Judiciário do Estado do Ceará.

10.1.14. Manter a estabilidade, confiabilidade e proteção do tráfego de perímetro e da borda de acesso à Internet, através da renovação da solução atual que está em pleno funcionado e das expansões de segurança pretendidas;

10.1.15. Introduzir o conceito de Zero Trust na arquitetura de segurança do TJCE, permitindo que o Tribunal esteja atualizado com as melhores práticas e referências do mercado no quesito segurança da informação.

10.1.16. Além disso, esta contratação oferece recursos para aperfeiçoar o monitoramento, controle, penalização e bloqueio de bots (robôs) que utilizam recursos em excesso da infraestrutura de TI e aplicações do TJCE na Internet, muitas vezes até causando depreciação da performance dos sistemas e causando indisponibilidade nos serviços;

10.1.17. Prevenir, detectar e responder a incidentes baseadas nos eventos gerados pelo firewall;

10.1.18. Localizar anomalias dentro do ambiente com o uso de inteligência artificial;

10.1.19. Dispor de equipamentos e soluções com novas tecnologias e recursos;

10.1.20. Prover alta disponibilidade nos equipamentos e mecanismos que são a base para proteção contra-ataques cibernéticos dentro da infraestrutura do TJCE;

10.1.21. Garantir o nível de suporte técnico necessário para atender um ambiente corporativo complexo e robusto;

10.1.22. Aperfeiçoar a detecção e respostas a ameaças cibernéticas no ambiente do TJCE;

10.1.23. Suporte a solução a ser adquirida;

10.1.24. Obter suporte adequado do fabricante quando da necessidade de aperfeiçoamento, melhores práticas, dúvidas de utilização e resolução de problemas.

11. FONTE DE RECURSOS

11.1. Fundo Especial de Reaparelhamento e Modernização do Poder Judiciário do Estado do Ceará – FERMOJU.

12. COMPLEMENTO DE INFORMAÇÕES

Sem informações complementares

ENCAMINHAMENTO
Encaminhe-se à Denise Maria Norões Olsen para providências.
Cristiano Henrique Lima de Carvalho – 5198 Titular da Área Demandante
Fortaleza, 20 de fevereiro de 2024

PREENCHIMENTO PELA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

13. IDENTIFICAÇÃO E CIÊNCIA DOS INTEGRANTES TÉCNICOS

Nome	Heldir Sampaio Silva	**Matrícula**	9630
Cargo	Técnico Judiciário	**Lotação**	Coordenadoria de Segurança da Informação
E-mail	heldir.sampaio@tjce.jus.br	**Telefone**	
Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na Resolução CNJ n° 468, de 15 de julho de 2022 - capítulo 2, item 2.1, subitem 2 do Guia de Contratações do Poder Judiciário, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.			
Heldir Sampaio Silva - 9630			
Fortaleza, 20 de fevereiro de 2024			

ENCAMINHAMENTO
Encaminha-se a autoridade competente da Área Administrativa para: 1. Decidir motivadamente sobre o prosseguimento da contratação; 2. Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e 3. Instituir a Equipe de Planejamento da Contratação conforme exposto no art. 7º, da Resolução CNJ n° 468, de 15 de julho de 2022.
Denise Maria Norões Olsen – 24667 Área de Tecnologia da Informação
Fortaleza, 20 de fevereiro de 2024

PREENCHIMENTO PELA ÁREA ADMINISTRATIVA

1. DECISÃO DA AUTORIDADE COMPETENTE

1.1. Atender o inciso V, Art. 11., da Resolução CNJ Nº 396 de 07/06/2021, que Instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), e determina que para elevar o nível de segurança das infraestruturas críticas, deve-se: utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da internet;

1.2. Com o prazo de garantia/suporte/subscrições dos hardware e software adquiridos por meio do CT Nº 17/2018 expirarão em 2023, e considerando o aumento dos riscos variados de falha, à medida que os equipamentos envelhecem, e as Resoluções e Portarias acima citadas, faz-se necessário uma Solução de Next Generation Firewall para atender a atual demanda, continuar a oferecer os serviços já citados acima, bem como, as novas necessidades citadas no item 5.2.2 propiciando ganhos na segurança, estabilidade, disponibilidade e desempenho dos Sistemas Administrativos e Judiciais que utilizam a solução atual.

2. IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO

Nome	Fábio de Carvalho Leite	**Matrícula**	9594
Cargo	Técnico Judiciário	**Lotação**	Coordenadoria de Gestão Administrativa de TI
E-mail	fabio.leite@tjce.jus.br	**Telefone**	
Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na Resolução CNJ n° 468, de 15 de julho de 2022 - capítulo 2, item 2.1, subitem 3 do Guia de Contratações do Poder Judiciário, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.			
Fábio de Carvalho Leite - 9594			
Fortaleza, 20 de fevereiro de 2024			

DECISÃO DA AUTORIDADE COMPETENTE

I. Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Demandante.

II. Designo, o servidor identificado no item 13, como Integrante Administrativo, para composição da Equipe de Planejamento da Contratação.

III. Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o art. 7º, da Resolução CNJ n° 468, de 15 de julho de 2022.

IV. A Equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato.

Caroline Moraes Maia Fiúza – 3051
Autoridade Competente da Área Administrativa

Fortaleza, 20 de fevereiro de 2024