ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
COORDENADORIA DE SEGURANÇA DA INFORMAÇAO

DOCUMENTO DE FORMALIZAÇÃO DE DEMANDA – DFD
DOCUMENTO DE OFICIALIZAÇÃO DE DEMANDA – DOD
(DFD/DOD)

Código da contratação - PAC 2025: TJCESETIN_2025_0008

Síntese do Tipo de Demanda: AQSETIN2025002 - Solução de para proteção do ambiente de dados (vazamento de informações) para usuários privilegiados do TJCE.

1. IDENTIFICAÇÃO DA ORIGEM DA DEMANDA

Área da Demanda: Gerência de Segurança da Informação e Ambientes Tecnológicos

Solicitante: Heldir Sampaio Silva

Matrícula: 9630

E-mail: heldir.sampaio@tjce.jus.br

2 OBJETIVO DESTE DOCUMENTO

2.1 Este documento tem como finalidade registrar específica necessidade detectada e os elementos característicos, para identificação de melhor forma de atendimento e, se for o caso, elaboração dos demais artefatos necessários à contratação.

3 IDENTIFICAÇÃO DA NECESSIDADE

3.1 Considerando a crescente complexidade dos ambientes de Tecnologia da Informação no âmbito do Poder Judiciário Cearense, bem como a necessidade premente de estabelecer mecanismos rigorosos de controle sobre o acesso a credenciais privilegiadas, revela-se imprescindível o uso de uma solução de gerenciamento de acesso para usuários que utilizam sistemas com contas privilegiadas.

3.2 A inexistência de uma ferramenta específica para essa finalidade impõe à instituição riscos significativos, tais como acessos indevidos, movimentação lateral de ameaças cibernéticas e

comprometimento de contas críticas, circunstâncias que podem comprometer a segurança institucional e a conformidade com as diretrizes estabelecidas na Resolução nº 396/2021 do CNJ – Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) – bem como com a PORTARIA nº 162, de 10 de junho de 2021.

4 DESCRIÇÃO SUSCINTA DA SOLUÇÃO

4.1 Trata-se de uma solução tecnológica que efetue o controle rigoroso e a supervisão das ações realizadas por usuários com privilégios elevados nos sistemas, garantindo que somente profissionais autorizados possam acessar áreas sensíveis e realizar operações críticas.

4.2 Em termos práticos, a solução deve verificar a identidade dos usuários, registrar todas as atividades efetuadas e impor restrições quando os acessos não se encontram em conformidade com as normas de segurança, protegendo, assim, os dados e os sistemas que sustentam o funcionamento do tribunal.

5 MOTIVAÇÃO E RESULTADOS ESPERADOS

5.1 Considerando o cenário de crescente sofisticação das ameaças cibernéticas e a notória vulnerabilidade decorrente do uso de contas privilegiadas, revela-se imperiosa a adoção de medidas que assegurem o controle rigoroso de acessos e a proteção dos ativos tecnológicos críticos do Poder Judiciário. A inexistência de mecanismos específicos para gerenciar tais acessos expõe a instituição a riscos substanciais, como a ocorrência de fraudes, a movimentação lateral de ameaças e o comprometimento de informações sensíveis, circunstâncias que podem, de forma decisiva, comprometer a continuidade dos serviços jurisdicionais e a confiança da sociedade.

5.2 A contratação de uma solução de gerenciamento de acesso para usuários que operam com contas privilegiadas configura medida indispensável à prevenção de incidentes que aconteceram em outro Tribunal de Justiça, no qual um servidor explorou fragilidades sistêmicas para comercializar decisões judiciais.

5.3 No âmbito do Poder Judiciário, a solução demandada reveste-se de especial importância para a manutenção da integridade e da confiabilidade dos sistemas administrativos e judiciais. Ao promover a auditoria constante e a identificação precoce de atividades suspeitas, a ferramenta de gerenciamento de acesso privilegiado não só previne incidentes de segurança como também assegura a conformidade com os padrões normativos exigidos (Resolução nº 396/2021 do CNJ e a PORTARIA nº 162, de 10 de junho de 2021 do CNJ), preservando os ativos essenciais à prestação jurisdicional e fortalecendo a governança da tecnologia empregada na atividade judicial.

5.4 **Situação atual**

5.4.1 O TJCE não conta atualmente com uma solução específica para o gerenciamento de acessos destinada a usuários que operam com contas privilegiadas em seus sistemas. O TJCE dispõe de ferramentas tecnológicas que utilizam contas privilegiadas, no entanto, não as gerencia

de forma adequada. Como exemplo, podem ser citados os seguintes casos:

5.4.1.1 O *Zero Trust Network Access* (ZTNA) foca em fornecer acesso seguro baseado em confiança zero para aplicativos e redes, mas não gerencia ou monitora contas privilegiadas, nem controla credenciais críticas ou registra atividades específicas de usuários privilegiados.

5.4.1.2 Embora o *Windows Server* possua recursos básicos de gerenciamento de usuários e permissões, ele não oferece uma solução para monitorar, auditar e proteger acessos privilegiados em sistemas heterogêneos ou complexos.

5.4.1.3 O *Endpoint Detection and Response* (EDR) é voltado para detecção e resposta a ameaças em dispositivos de usuários, concentrando-se em comportamentos maliciosos e incidentes de segurança, sem fornecer controle granular sobre acessos privilegiados ou gestão de credenciais críticas.

5.4.1.4 O *Web Application Firewall* (WAF) e o *Load Balancer* (LB) protegem aplicações web contra ataques externos e distribuem tráfego, mas não possuem capacidade de gerenciar ou monitorar acessos privilegiados a sistemas internos ou críticos.

5.5 **Resultados Esperados**

5.5.1 **Controle Centralizado de Acessos Privilegiados**: A solução proporcionará um ambiente centralizado para o gerenciamento de credenciais privilegiadas, permitindo a administração eficiente de senhas e permissões.

5.5.2 **Monitoramento e Auditoria das Atividades de Usuários Privilegiados**: A implementação da solução possibilitará o monitoramento contínuo e a auditoria detalhada de todas as atividades realizadas por usuários com privilégios elevados.

5.5.3 **Redução do Risco de Fraudes Internas**: A solução atuará como um mecanismo preventivo contra fraudes internas, uma vez que limitará o uso indiscriminado de contas privilegiadas. Ao restringir o acesso apenas ao estritamente necessário e registrar todas as operações realizadas, será possível identificar rapidamente qualquer comportamento suspeito ou irregular.

5.5.4 **Mitigação de Vulnerabilidades Relacionadas a Senha**s: A gestão automatizada de senhas privilegiadas eliminará práticas inseguras, como o armazenamento manual de credenciais em documentos não protegidos ou a utilização de senhas fracas e repetidas.

5.5.5 **Conformidade com Normativas de Segurança da Informação do CNJ**: A adoção da solução permitirá ao Tribunal alinhar-se às exigências de normativas de segurança da informação, como a Resolução nº 396/2021 do CNJ e a PORTARIA nº 162, de 10 de junho de

2021 do CNJ.

5.5.6 **Conformidade com Normativas Internacionais de Segurança da Informação**

5.5.6.1 ISO 27001 - Seção A.9.4.1 (Controle de Acesso Privilegiado).

5.5.6.2 ISO 27002 - Seção 9.4 (Gerenciamento de Acesso Privilegiado).

5.5.6.3 CIS Controls - Controle 4 (Controle de Contas Privilegiadas).

5.5.6.4 COBIT 2019 - Domínio APO01 (Alinhar, Planejar e Organizar) e Domínio BAI06 (Construir, Adquirir e Implementar).

5.5.6.5 SANS Critical Security Controls - Controle 12 (Gerenciamento de Contas Privilegiadas).

5.5.6.6 NIST SP 800-53 - Controle AC-2 (Gestão de Contas).

ENCAMINHAMENTO
Encaminha-se a autoridade competente da Área Administrativa para: a. Decidir motivadamente sobre o prosseguimento da contratação; b. Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e c. Instituir a Equipe de Planejamento da Contratação conforme exposto no art. 7º, da Resolução CNJ n° 468, de 15 de julho de 2022.
Heldir Sampaio Silva – 9630 **Gerente de Segurança da Informação e Ambientes Tecnológicos** **Solicitante**
Fortaleza, data da assinatura eletrônica.

6 ALINHAMENTO ENTRE A DEMANDA E O PLANEJAMENTO ESTRATÉGICO INSTITUCIONAL E DESDOBRAMENTO ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO

6.1 Esta demanda se relaciona ao planejamento estratégico com o intuito de prover soluções de TI inovadoras para a transformação digital, de modo que se mostra aderente ao Planejamento Estratégico do Tribunal de Justiça do Ceará TJCE 2030.

6.2 Adicionalmente, se mostra também aderente ao PLANO ESTRATÉGICO 2030, pois está alinhada com os indicadores: *Indicador 20: Índice de conformidade com as políticas de segurança de TIC e Indicador 19: Percentual de execução do Programa de Modernização do Poder Judiciário*, do Plano Estratégico TJCE 2030 (Portaria n. 846/2024).

7 ALINHAMENTO AO PLANO ANUAL DE CONTRATAÇÕES

7.1 Trata-se de demanda prevista no PAC 2025, conforme abaixo identificado:

ITEM	DESCRIÇÃO
TJCESETIN_2025_0008	Aquisição de solução de para proteção do ambiente de dados (vazamento de informações).

8. FONTE DE RECURSOS

8.1 Para a demanda ora posta, foi identificada a seguinte previsão de fonte de recursos, o que admite seguimento para contratação:

Órgão: 04000000 - TRIBUNAL DE JUSTIÇA;
Unid. Orçamentaria: 04100021 SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO;
Ação: 20511 – Apoio ao desenvolvimento da prestação - Jurisdicional na área de TI – FERMOJU (1° Grau) e 20512 – Apoio ao desenvolvimento da prestação - Jurisdicional na área de TI – FERMOJU (2° Grau).

9. DECISÃO DE ANDAMENTO

9.1 Em vista das constatações deste documento, aprovo o prosseguimento do atendimento da demanda na forma de planejamento de eventual contratação.

9.2 Para tanto, encaminhamos às respectivas áreas competentes para ciência do(s) integrante(s) técnico(s), administrativo(s) e demandante(s).

Denise Maria Norões Olsen – 24667

Autoridade Competente da Área Tecnologia da Informação

Fortaleza, data da assinatura eletrônica.

FORMAÇÃO DA EQUIPE DE PLANEJAMENTO PARA CONTRATAÇÃO

IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO

Nome	Francisco José Pessoa Furtado	**Matrícula**	8284
Cargo	Técnico Judiciário	**Lotação**	Coordenadoria de Contratos e Aquisições de TIC

E-mail	francisco.furtado@tjce.jus.br	**Telefone**	(85) 3207-7878
Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na Resolução CNJ n° 468, de 15 de julho de 2022 e no Guia de Contratações do Poder Judiciário, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.			
Francisco José Pessoa Furtado – 8284			
Fortaleza, data da assinatura eletrônica.			

IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE DEMANDANTE

Nome	Heldir Sampaio Silva	**Matrícula**	9630
Cargo	Gerente	**Lotação**	Gerência de Segurança da Informação e Ambientes Tecnológicos
E-mail	heldir.sampaio@tjce.jus.br	**Telefone**	(85) 3207-7878
Por este instrumento declaro ter ciência das competências do INTEGRANTE DEMANDANTE definidas na Resolução CNJ n° 468, de 15 de julho de 2022 e no 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, data da assinatura eletrônica.			

IDENTIFICAÇÃO E CIÊNCIA DOS INTEGRANTES TÉCNICOS

Nome	Max Eduardo Vizcarra Melgar	**Matrícula**	48994
Cargo	Coordenador	**Lotação**	Coordenadoria de Segurança da Informação
E-mail	max.melgar@tjce.jus.br	**Telefone**	(85) 3207-7878

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas na Resolução CNJ n° 468, de 15 de julho de 2022 e no Guia de Contratações do Poder Judiciário, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.
Max Eduardo Vizcarra Melgar - 48994
Fortaleza, data da assinatura eletrônica.

Fica instituída a Equipe de Planejamento da Contratação e será automaticamente destituída quando da assinatura do contrato.

_____

Denise Maria Norões Olsen – 24667

Autoridade Competente da Área Tecnologia da Informação

Fortaleza, data da assinatura eletrônica.

Documento assinado eletronicamente por **HELDIR SAMPAIO SILVA**, **Gestor de Unidade**, em 10/04/2025, às 08:43, conforme horário oficial de Brasília, com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **MAX EDUARDO VIZCARRA MELGAR**, **Gestor de Unidade**, em 10/04/2025, às 09:44, conforme horário oficial de Brasília, com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015 .

Documento assinado eletronicamente por **FRANCISCO JOSÉ PESSOA FURTADO**, **Servidor**, em 10/04/2025, às 09:51, conforme horário oficial de Brasília, com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **DENISE MARIA NORÕES OLSEN**, **Gestor de Unidade**, em 10/04/2025, às 13:52, conforme horário oficial de Brasília, com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei-adm.tjce.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0079222** e o código CRC **ECC236EF**.