ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

DOCUMENTO DE OFICIALIZAÇÃO DE DEMANDA – DOD

AQSETIN2023010 - Segurança de Endpoint
PAC: TJCESETIN_2024_0011

1. INTRODUÇÃO

1.1. Este documento tem como finalidade formalizar o início do processo de planejamento da contratação de **Solução de segurança de Endpoint**, 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: Solução de proteção de segurança da informação de Endpoint.

Responsável pela Demanda: Cristiano Henrique Lima de Carvalho

Matrícula: 5198

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

Telefone: (85) 3207-7756

3. IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE DEMANDANTE

Nome	Heldir Sampaio Silva	**Matrícula**	*9630*
Cargo	Técnico Judiciário	**Lotação**	Coordenadoria de Segurança da Informação
E-mail	heldir.sampaio@tjce.jus.br	**Telefone**	(85)3207-6850
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			
Fortaleza			

4. IDENTIFICAÇÃO DA DEMANDA

4.1. Aquisição ou atualização da solução de segurança de Endpoint, para prever, prevenir, detectar e responder a ciberataques de maneira holística, otimizada, integrada e simplificada, no âmbito do Tribunal de Justiça do Estado do Ceará (TJCE).

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 2023-2024

ID	INICIATIVA ELENCADA NO PDTIC 2023-2024
01	N23121 Aquisição de antivírus (endpoint).

7. METAS DO DESDOBRAMENTO ESTRATÉGICO DE TI A SEREM ALCANÇADAS

INDICADOR	META
Índice de conformidade com as políticas de segurança de TIC.	Atender 90% de itens das normas até 2026.
Grau de disponibilidade de sistemas judiciais.	Manter os sistemas disponíveis e em pleno funcionamento 98% do tempo até 2026.
Grau de disponibilidade de sistemas administrativos.	Manter os sistemas disponíveis e em pleno funcionamento 99% do tempo até 2026.

8. ALINHAMENTO AO PLANO ANUAL DE CONTRATAÇÕES 2024

ITEM	DESCRIÇÃO
01	TJCESETIN_2024_0011

9. MOTIVAÇÃO/JUSTIFICATIVA

9.1. **Situação Atual**

9.1.1. A história de 150 anos do Tribunal de Justiça do Ceará (TJCE) é marcada por constantes avanços tecnológicos e inovações. Ao longo do tempo, o Judiciário tem acompanhado a evolução da tecnologia para melhorar os serviços oferecidos aos cidadãos.

9.1.1.1. Um dos marcos mais significativos foi a implementação do Sistema de Automação da Justiça (SAJ) em 2009. Essa iniciativa foi crucial para modernizar os processos judiciais e tornar o acesso à justiça mais ágil e eficiente.

9.1.1.2. Em 2019, foi concluída a digitalização de todos os processos, permitindo que os cidadãos pudessem acessar seus processos de qualquer lugar, enquanto os magistrados podiam realizar seus procedimentos judiciais remotamente.

9.1.1.3. Um exemplo disso é o Processo Judicial Eletrônico (PJe), introduzido em 2014, que foi projetado para otimizar o fluxo de trabalho no Judiciário e facilitar a vida dos profissionais do Direito.

9.1.1.4. Durante a pandemia de Covid-19, o TJCE implementou o regime obrigatório de teletrabalho até meados de 2021, como medida para garantir a segurança dos servidores e jurisdicionados e cumprir as restrições de locomoção recomendadas pelas autoridades de saúde.

9.1.1.5. Em 2021, ainda enfrentando os desafios da pandemia, o TJCE lançou o "Balcão

Virtual", um serviço permanente de atendimento digital no Judiciário, seguindo as diretrizes do Conselho Nacional de Justiça (CNJ). O Balcão Virtual oferece uma ampla gama de serviços, incluindo informações processuais e funcionamento das unidades judiciárias, e permite o contato imediato por meio de videoconferência.

9.1.2. Com a digitalização dos processos judiciais e a implementação de iniciativas como o teletrabalho e o Balcão Virtual, a segurança da informação tornou-se elementos crítico na manutenção da operacionalidade do tribunal e na proteção das informações confidenciais e sensíveis.

9.1.3. O escopo da análise do ambiente de segurança de TI consiste em uma abordagem abrangente e detalhada dos custos e do gerenciamento de todas as medidas de segurança relacionadas à tecnologia da informação dentro de uma organização.

9.1.4. Isso engloba o gerenciamento de identidade e acesso, proteção da rede, segurança dos dispositivos terminais, proteção dos dados, segurança dos aplicativos, gerenciamento de vulnerabilidades e análise de segurança, bem como governança, gestão de riscos e conformidade com as regulamentações.

9.1.5. Uma solução completa de segurança de Tecnologia da Informação (TI) é como um escudo de proteção digital para uma organização, integrando uma série de sistemas e tecnologias que trabalham em conjunto para salvaguardar contra uma ampla gama de ameaças cibernéticas. Aqui estão alguns dos principais sistemas que compõem essa defesa digital do Tribunal de Justiça do Ceará (TJCE):

9.1.5.1. Firewalls de Próxima Geração -Palo Alto Networks-: Estes são os guardiões virtuais que monitoram e filtram o tráfego de rede, vasculhando profundamente cada pacote de dados em busca de sinais de perigo. Eles são especialmente projetados para detectar e deter ataques maliciosos, protegendo a rede contra invasões indesejadas.

9.1.5.2. Firewall de Aplicativos Web (WAF) -Citrix NetScaler-: Este tipo específico de firewall é como um guarda de fronteira para aplicativos e sites da Web, filtrando e bloqueando o tráfego HTTP suspeito que possa representar ameaças para essas plataformas digitais.

9.1.5.3. Proxy Reverso -Citrix NetScaler-: Agindo como uma espécie de intermediário entre a internet e os servidores da organização, o proxy reverso ajuda a balancear a carga de tráfego e, cada vez mais, aprimora a segurança de aplicativos da Web, funcionando em conjunto com o WAF.

9.1.5.4. Soluções de Segurança de Endpoint -Kaspersky Endpoint Security-: Estas são como os guardiões dos dispositivos finais, como computadores e smartphones,

protegendo-os contra ameaças cibernéticas. Elas identificam e removem malware, como vírus e cavalos de Troia.

9.1.5.5. Soluções de Segurança de Email -Microsoft 365-: Estas são como os guardiões dos portões digitais, protegendo contra ameaças cibernéticas que chegam por meio de e-mails, como phishing e malware. Elas examinam, filtram e bloqueiam e-mails suspeitos, mantendo as caixas de entrada seguras.

9.1.5.6. Soluções de Gerenciamento de Vulnerabilidades -Tenable-: Este sistema detecta e prioriza vulnerabilidades nos sistemas e aplicativos da organização, permitindo que os administradores apliquem correções de segurança de maneira eficaz, reduzindo assim o risco de exploração por parte de invasores.

9.1.5.7. Soluções de Backup e Recuperação de Dados -Veeam-: Essas soluções garantem que os dados cruciais da organização sejam copiados e armazenados de forma segura, permitindo uma rápida recuperação em caso de perda de dados devido a falhas de hardware, ataques cibernéticos ou desastres naturais.

9.1.6. Juntos, esses sistemas formam uma defesa digital, garantindo que o TJCE esteja bem protegido contra as ameaças cibernéticas em constante evolução.

9.1.7. Endpoint, em termos de segurança da informação e tecnologia, refere-se a qualquer dispositivo terminal ou ponto de extremidade que esteja conectado a uma rede corporativa ou de internet. Esses dispositivos podem incluir computadores desktop, laptops, smartphones, tablets, servidores e outros dispositivos conectados à rede.

9.1.8. Os endpoints são os pontos onde os usuários interagem diretamente com a rede e acessam os recursos e dados necessários para realizar suas atividades. No contexto da segurança da informação, os endpoints são frequentemente alvos de ataques cibernéticos, pois representam pontos de entrada potenciais para invasores.

9.1.9. Portanto, a proteção dos endpoints é uma preocupação fundamental para garantir a segurança de uma rede corporativa ou de internet. Isso geralmente envolve a implementação de medidas de segurança, como antivírus, firewalls, soluções de detecção e resposta e outras tecnologias destinadas a proteger esses dispositivos contra ameaças cibernéticas, como malware, ransomware, ataques de phishing e outras formas de ataques.

9.1.10. Atualmente estão em uso dois pacotes de licenças Kaspersky Endpoint Security for Business SELECT: uma com 6500 licenças, válida até dezembro de 2023 (CT Nº 28-2020). E a outra com 2500 licenças, válida até abril de 2024 (CT Nº 09-2021). Totalizando 9000 licenças para uso.

9.2. **Descrição da Oportunidade ou do Problema**

9.2.1. **Problema**

9.2.1.1. A opção de licenciamento atual para a proteção representa o nível mais básico oferecido pelo fabricante para garantir a segurança dos endpoints corporativos. Esse nível de segurança já não é mais suficiente para atender às demandas dos dispositivos conectados à rede de dados do TJCE, isso pode trazer várias implicações na segurança e o funcionamento adequado dos sistemas do TJCE, como:

9.2.1.1.1. Vulnerabilidades de segurança: O nível básico de proteção pode não ser capaz de defender efetivamente os endpoints contra as ameaças cibernéticas atuais, aumentando o risco de ataques, infecções por malware e violações de dados.

9.2.1.1.2. Conformidade regulatória: Desconformidade das regulamentações da resolução CNJ Nº 363 de 12/01/2021, que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. E da resolução CNJ Nº 396 de 07/06/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário.

9.2.1.1.3. Impacto nas operações: Falhas de segurança e ataques cibernéticos podem interromper as operações normais da organização, causando tempo de inatividade, perda de produtividade e danos à reputação.

9.2.1.1.4. Prejuízos financeiros: Incidentes de segurança podem resultar em custos significativos, incluindo gastos com recuperação de dados, reparos de sistemas comprometidos e custos legais.

9.2.1.2. A quantidade atual de licenças não é mais capaz de abranger todos os dispositivos que estão atualmente em uso na rede de dados do TJCE. Assim, torna-se imprescindível adquirir licenças adicionais para garantir a cobertura atual e futura.

9.2.1.3. O fim do suporte aos softwares que compõem a solução atual de antivírus, em abril de 2024, pode ter diversas implicações negativas para a segurança e o funcionamento dos sistemas e dispositivos do TJCE, como:

9.2.1.3.1. Vulnerabilidades de segurança: Sem atualizações de segurança regulares, os softwares desatualizados podem se tornar vulneráveis a novas ameaças cibernéticas, como vírus, malware e ataques de hackers.

9.2.1.3.2. Falhas de desempenho: O software desatualizado pode apresentar falhas de desempenho, incluindo lentidão, travamentos e incompatibilidades com outros programas e sistemas operacionais.

9.2.1.3.3. Conformidade: Em muitos setores, existem requisitos regulatórios que exigem a utilização de software atualizado e suportado para proteger dados

sensíveis e informações confidenciais.

9.2.1.3.4. Perda de suporte técnico: Sem o suporte do fabricante, o TJCE não pode obter assistência técnica para resolver problemas e realizar manutenções necessárias.

9.2.2. **Oportunidade**

9.2.2.1. A evolução das soluções de antivírus e proteção de endpoint tem sido constante ao longo das últimas décadas, com novas tecnologias e técnicas sendo desenvolvidas para lidar com as ameaças cada vez mais sofisticadas que surgem no cenário de segurança cibernética.

9.2.2.2. As soluções de proteção de endpoint se tornaram cada vez mais integradas, com muitas soluções combinando recursos de antivírus, segurança de rede e gerenciamento de dispositivos em uma única plataforma. A inteligência artificial e a aprendizagem de máquina também se tornaram cada vez mais comuns na detecção de ameaças e na proteção contra ataques cibernéticos sofisticados.

9.2.2.3. Em resumo, as soluções de antivírus e proteção de endpoint evoluíram de soluções simples de detecção de vírus para plataformas avançadas de segurança cibernética que protegem contra uma ampla variedade de ameaças em constante evolução.

9.2.2.4. Atualizar um antivírus para uma plataforma de segurança de endpoint avançada oferece diversas oportunidades para melhorar a postura de segurança. Aqui estão algumas das oportunidades que essa transição pode proporcionar:

9.2.2.4.1. Detecção Avançada de Ameaças: As plataformas de segurança de endpoint avançadas oferecem recursos de detecção avançada de ameaças, como análise comportamental, detecção de anomalias e inteligência artificial, que podem identificar e responder a ameaças de forma mais eficaz do que os antivírus tradicionais.

9.2.2.4.2. Prevenção de Ameaças Avançadas: Essas plataformas fornecem camadas adicionais de proteção, como prevenção de intrusões, sandboxing e aprendizado de máquina, que ajudam a impedir ataques cibernéticos avançados, como ransomware, ataques de dia zero e malware avançado.

9.2.2.4.3. Resposta Automatizada a Incidentes: Uma plataforma de segurança de endpoint avançada pode oferecer recursos de resposta automatizada a incidentes, que ajudam a identificar, isolar e remediar ameaças de forma rápida e eficiente, reduzindo o tempo de inatividade e o impacto nos negócios.

9.2.2.4.4. Visibilidade Aprimorada: Essas plataformas geralmente incluem recursos de monitoramento e relatórios avançados, que oferecem uma visão mais detalhada e em tempo real da atividade do endpoint, permitindo uma melhor compreensão das ameaças e vulnerabilidades em toda a organização.

9.2.2.4.5. Gerenciamento Centralizado: Uma plataforma de segurança de endpoint avançada geralmente oferece um console centralizado para gerenciamento e monitoramento de todos os endpoints da organização, facilitando a implementação de políticas de segurança consistentes e a aplicação de patches e atualizações de forma eficiente.

9.2.2.4.6. Conformidade Regulatória: Ao adotar uma plataforma de segurança de endpoint avançada, as organizações podem melhorar sua conformidade com regulamentações de segurança cibernética, demonstrando uma abordagem proativa para proteger os dados confidenciais dos clientes e funcionários.

9.3. Motivação da Demanda

9.3.1. O término do suporte aos softwares de antivírus requer uma abordagem cuidadosa e proativa para manter a segurança dos sistemas e dados da organização. É importante entender que o nível atual de proteção de endpoints pode não ser mais suficiente diante das ameaças cibernéticas em constante evolução. Portanto, é crucial tomar medidas proativas para fortalecer a segurança da organização.

9.3.2. Para isso, é necessário reconhecer a necessidade de atualizar e adquirir licenças adicionais para garantir a cobertura adequada de segurança dos dispositivos na rede de dados do TJCE. Isso ajudará a mitigar os riscos de segurança e a garantir a conformidade regulatória, além de proteger os ativos e dados da organização contra ameaças cibernéticas em constante evolução.

9.3.3. É necessário explorar opções para atualizar ou melhorar o software de segurança de endpoints, escolhendo uma solução mais robusta e adequada às necessidades atuais do TJCE.

9.3.4. A atualização de um antivírus para uma plataforma de segurança de endpoint avançada oferece uma série de oportunidades para fortalecer a solução completa de segurança de TI do TJCE.

9.3.5. Entendemos a importância da segurança da informação em todos os processos do TJCE. Isso se dá pelo fato de que a instituição lida com informações sensíveis e confidenciais, o que a torna um alvo potencial para ataques cibernéticos. E com o constante aumento das ameaças cibernéticas, é fundamental contar com uma solução que possa garantir a

proteção dos endpoints utilizados pelos colaboradores do tribunal.

9.4. Ciclo de Vida da Demanda

9.4.1. É difícil prever com precisão quando uma solução de nova geração se tornará obsoleta, pois isso dependerá de muitos fatores, incluindo avanços na tecnologia, evolução das ameaças cibernéticas e mudanças nas necessidades do TJCE.

9.4.2. No entanto, é possível dizer que a solução de proteção de segurança de endpoint de próxima geração continuará a ser uma parte essencial da estratégia de segurança cibernética nos próximos anos. Isso se deve ao fato de que, mesmo com os avanços na tecnologia de segurança cibernética, as ameaças cibernéticas continuarão a evoluir e se tornar cada vez mais sofisticadas.

9.4.3. A expectativa de uso deverá ser de, no mínimo, 60 (sessenta) meses, pelas características físicas e tecnológicas da rede do TJCE, que possui uma ampla capilaridade.

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

9.5.1. Todos os usuários de estações de trabalho, notebooks, dispositivos institucionais, computadores servidores e máquinas virtuais, bem como, todo o público jurisdicionado que utiliza, direta ou indiretamente, os serviços de informática do TJCE.

9.6. Expectativa de entrega da solução

9.6.1. A expectativa de entrega da solução é para o 2º semestre de 2024.

10. RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

10.1. Espera-se que a SETIN possa detectar e responder ameaças cibernéticas com mais rapidez e eficácia, reduzir o tempo de inatividade não planejado e minimizar o impacto de violações de segurança.

10.2. Como também, aprimorar a investigação de incidentes ao coletar informações mais detalhadas e obter *insights* valiosos para aprimorar a segurança de forma ampla e efetiva.

10.3. Com a possibilidade de utilizar a solução na nuvem, permite a escalabilidade da proteção para um número maior de endpoints, sem comprometer a eficácia da segurança.

11. FONTE DE RECURSOS

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

12. COMPLEMENTO DE INFORMAÇÕES

12.1. Não há informações complementares.

ENCAMINHAMENTO
Encaminhe-se à Área de Tecnologia da Informação de para providências.
Cristiano Henrique Lima de Carvalho - 5198
Fortaleza

PREENCHIMENTO PELA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

13. IDENTIFICAÇÃO E CIÊNCIA DOS INTEGRANTES TÉCNICOS

Nome	Diego Francisco de Mesquita Oliveira	**Matrícula**	48802
Cargo	Analista Judiciário	**Lotação**	Coordenadoria de Suporte Técnico-SETIN
E-mail	diego.oliveira@tjce.jus.br	**Telefone**	86999561176
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.			
Diego Francisco de Mesquita Oliveira - 48802			
Fortaleza			

JUSTIFICATIVA PARA ACUMULAÇÃO DE PAPÉIS

Não aplicável.

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.
Andrea Antunes de Carvalho - 3270 Área de Tecnologia da Informação
Fortaleza

PREENCHIMENTO PELA ÁREA ADMINISTRATIVA

14. DECISÃO DA AUTORIDADE COMPETENTE

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

14.2. Designo, o servidor identificado no item 15, como Integrante Administrativo, para composição da Equipe de Planejamento da Contratação.

15. IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO

Nome	Francisco José Pessoa Furtado	**Matrícula**	8284
Cargo	Técnico Judiciário	**Lotação**	Coordenadoria de gestão de contratos e orçamento de TI
E-mail	francisco.furtado@tjce.jus.br	**Telefone**	32077870

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.
Francisco José Pessoa Furtado – 8284
Fortaleza

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 15, 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.

Denise Maria Norões Olsen – 24667

Autoridade Competente da Área Administrativa

Fortaleza, 17 de maio de 2024.