ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

DOCUMENTO DE OFICIALIZAÇÃO DE DEMANDA – DOD

Código PAC 2023: TJCESETIN_UGP_2023_09

AQSETIN2022010 – Serviços Gerenciados de Segurança da Informação

1. INTRODUÇÃO

Este documento tem como finalidade formalizar o início do processo de planejamento da ***Contratação de Serviços Gerenciados de Segurança da Informação***, 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): Gerência de Infraestrutura de TI.

Nome do/da Projeto/Aquisição: Serviços Gerenciados de Segurança da Informação.

Responsável 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, 02 de junho de 2023.			

4. IDENTIFICAÇÃO DA DEMANDA

Com o crescimento da demanda por serviços de informática do TJCE, tanto na área judiciária quanto na área administrativa, a Secretaria de Tecnologia da Informação-SETIN tem a necessidade contínua de analisar a sua demanda e adequar a sua infraestrutura de tecnologia da informação e segurança da informação, garantindo assim, a satisfação de seus usuários, mantendo a integridade, confidencialidade e disponibilidade dos dados institucionais do Tribunal.

A crescente complexidade e sofisticação das ameaças cibernéticas representam um grande desafio para o Tribunal de Justiça do Ceará (TJCE) na garantia da segurança de seus sistemas de informação. Ainda que medidas preventivas, como a instalação de antivírus e firewalls, sejam adotadas, o TJCE identificou a 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, usando ferramentas de detecção e bloqueio de ataques por meio da correlação de eventos e incidentes que possam surgir nos ativos de rede do 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>

ID	INICIATIVA ELENCADA NO PDTIC 2023
N23003	Aquisição e Implantação de SOC (“Security Operations Center” - Centro de Operações de Segurança).

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.

8. ALINHAMENTO AO PLANO ANUAL DE CONTRATAÇÕES 2023

ITEM	DESCRIÇÃO
TJCESETIN UGP 2023 09	Contratar serviços para implantação do SOC (Centro de operações de segurança).

9. MOTIVAÇÃO/JUSTIFICATIVA

9.1. Situação Atual

O Tribunal de Justiça do Estado do Ceará (TJCE) tem como objetivo garantir a segurança das informações que circulam em sua rede, bem como proteger seus sistemas contra ameaças cibernéticas. Atualmente, a equipe de segurança da informação do TJCE possui uma série de desafios para identificar e responder a incidentes de segurança em tempo hábil, além de gerenciar informações de diversos sistemas, dificultando a análise e a tomada de decisões.

O TJCE possui uma infraestrutura de segurança da informação implantada e consolidada, incluindo Firewall, antivírus e alguns outros mecanismos de segurança adquiridos.

Atualmente temos as seguintes soluções de segurança da informação e monitoramento em operação nos Data Centers:

Id	Solução	Qtde.	Funcionalidade
1	NGFW Palo Alto	02	Next Generation Firewall para a segurança de perímetro de rede.
2	Antivírus Kaspersky	9000	Licenças de antivírus com agentes em clientes e central de monitoramento.
3	WAF NetScaller	02	Firewall de aplicação web para a segurança de tráfego na camada de aplicação do modelo TCP/IP no perímetro de rede.
4	Zabbix	04	Software de monitoramento de desempenho e disponibilidade de ativos de rede, servidores e aplicativos.
5	Grafana	01	Plataforma de visualização e análise de dados que

			coleta, visualiza e analisa dados de ativos de rede, servidores e aplicativos.
6	Tenable	01	Plataforma de gerenciamento de vulnerabilidades de segurança de rede.

9.2. Descrição da Oportunidade ou do Problema

O Brasil segue, pelo segundo ano consecutivo, no topo do pódio de países mais atacados por Ransomware (programa malicioso de extorsão) na América Latina. É o que revelam os dados mais recentes da Palo Alto Networks, empresa especializada em segurança cibernética:

- **Brasil**: 59 ataques;
- **Japão**: 32 ataques;
- **China**: 29 ataques;
- **México**: 26 ataques;
- **Argentina**: 23 ataques.

Nos últimos 18 meses, 59 casos foram registrados. Esse total representa aumento de 51% no número de casos em um ano, segundo o levantamento realizado pela referida empresa.

Além de liderar o pódio de alvos da América Latina, o Brasil aparece entre os países mais atacados por Ransomware do mundo, conforme comparativo abaixo:

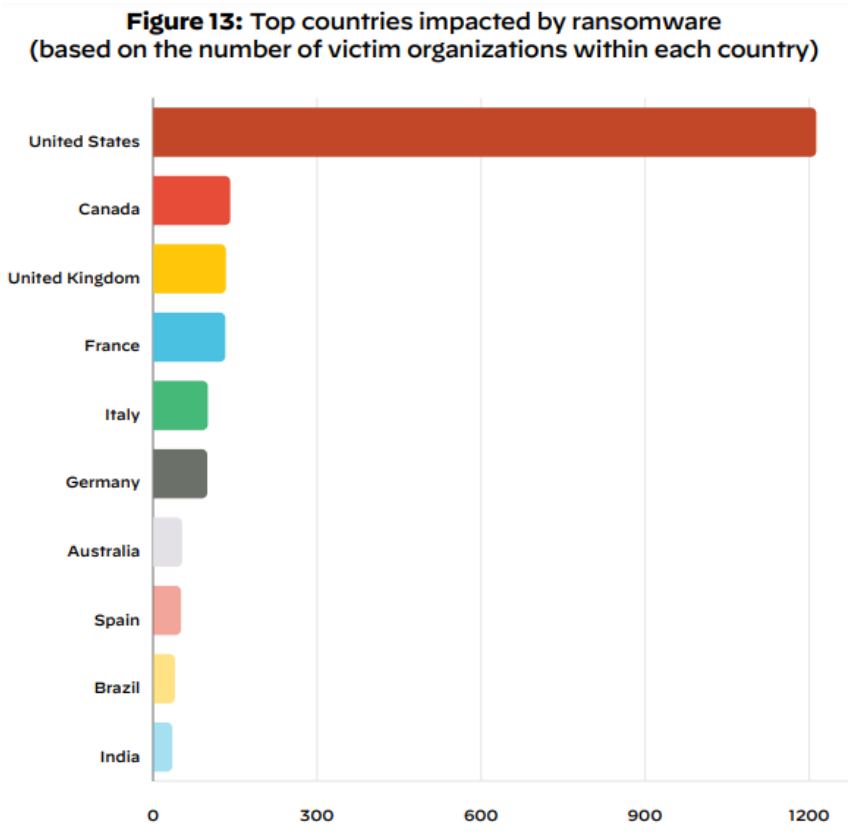

Figura 1 - https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2022-unit42-ransomware-threat-report-final.pdf

Além disso, um em cada cinco casos de Ransomware investigados revelou que os invasores coagem e perseguem suas vítimas, aproveitando informações do cliente que foram roubadas para forçar a organização a pagar pelo "resgate".

Conforme afirma Bert Milan, vice-presidente regional do Caribe e América Latina da Palo Alto Networks, "*Algumas das táticas de ataque incluem criptografia, roubo de dados, negação de serviço distribuída (DDoS) e assédio, com o objetivo final de aumentar as chances de receber o pagamento. O roubo de dados, frequentemente associado a sites de vazamento da Dark Web, foi a tática de extorsão mais comum, com 70% dos grupos criminosos utilizando no final de 2022 – um aumento de 30% em relação ao ano anterior.".*

Esses ataques podem acontecer por meio de links maliciosos, falta de backups e pouco investimento em cibersegurança. Além disso, sites de vazamento da Dark Web são associados com frequência ao roubo de dados.

Bert Milan, vice-presidente regional do Caribe e América Latina da Palo Alto Networks, destaca que "*Atualmente, empresas devem fazer investimentos maciços em segurança cibernética, além de treinar funcionários para que estejam a par das melhores práticas cibernéticas ao usarem equipamentos da empresa. É desaconselhado que um negócio continue fazendo poucos esforços pela sua cibersegurança, mesmo sabendo que isso não garante total imunidade aos ataques. Essa postura certamente impedirá que grupos de Ransomware atinjam o coração da empresa.".*

Fonte: https://olhardigital.com.br/2023/03/21/seguranca/de-novo-brasil-eh-o-pais-latino-mais-atacado-por-ransomware/

O Poder Judiciário Cearense não possui uma solução de gerenciamento de segurança da informação moderna, eficiente, única e centralizada. Atualmente o gerenciamento é feito de forma descentralizada em cada uma das soluções elencadas na tabela do item 9.1. Sem uma gestão única e centralizada esta Corte está com sérias restrições e capacidade extremamente reduzida de ter uma visão completa das atividades da rede, tornando difícil identificar comportamentos suspeitos ou anomalias. Sem uma equipe dedicada para monitorar, investigar e tratar incidentes de segurança. Não tem uma equipe pronta para lidar com incidentes de segurança o que torna a resposta a incidentes mais lenta e mais suscetível a erros, além das dificuldades para identificar e tratar vulnerabilidades em sua rede.

Sem uma solução de gerenciamento de segurança da informação, o monitoramento e análise de eventos de segurança do TJCE estão comprometidos, tornando mais difícil a identificação de ameaças em tempo hábil e a adoção de medidas para mitigá-las. Tal ausência dificulta a identificação de correlações entre eventos de segurança, bem como a centralização dos logs e eventos de segurança em um único local.

A falta de solução de gerenciamento de segurança da informação faz com que a atual equipe de segurança da informação do TJCE demore muito tempo para pode dar uma resposta de ação em caso de incidentes de segurança, aumentando o risco de perda de dados sensíveis. Torna o processo de resposta a incidentes de segurança do TJCE mais lento e menos eficiente, o que pode levar a uma maior exposição, perda e vazamento de dados. Torna mais difícil a identificação de vulnerabilidades em sistemas e aplicações, bem como a realização de testes de segurança regulares e a validação de medidas de segurança já implementadas.

Ao contratar serviços gerenciados de segurança da informação, o TJCE obterá diversos benefícios para a segurança do órgão. Esses serviços permitirão uma detecção mais eficiente de ameaças e uma resposta mais rápida a incidentes de segurança, resultando em uma maior proteção aos dados e sistemas do Tribunal. Além disso, a automação dos processos e a equipe especializada permitirão uma melhor gestão de riscos e redução de vulnerabilidades, aumentar a inteligência e a maturidade em segurança da informação, garantir a conformidade com as leis e regulamentações de segurança, aumentando a confiança dos usuários nos serviços prestados pelo TJCE. Além disso, tal investimento reforçará o compromisso desta Corte em manter a integridade, confidencialidade e disponibilidade dos dados institucionais do Tribunal.

9.3. Motivação da Demanda

9.3.1 Realizar coleta, análise e gerenciamento de informações de segurança em tempo real. Monitorar a rede do TJCE e detectar possíveis ameaças e vulnerabilidades de maneira centralizada, garantindo a segurança da informação e a integridade dos sistemas. Além disso, fornecer informações e recomendações para a tomada de decisões estratégicas relacionadas à segurança da informação.

9.3.2 Identificar e responder a ameaças em tempo real. Coletar, analisar e correlacionar informações de segurança de vários dispositivos e sistemas do TJCE, permitindo que a equipe de segurança possa responder prontamente a possíveis ataques ou vulnerabilidades.

9.3.3 Lidar com incidentes de segurança cibernética. Ter expertise para identificar, isolar e solucionar possíveis problemas de segurança, minimizando o impacto e os danos causados por um possível ataque. Sendo essencial para garantir a continuidade dos serviços do TJCE, mantendo a integridade da informação.

9.3.4 Automatizar processos e fluxos de trabalho relacionados à segurança da informação. Simplificar e agilizar a resposta a incidentes de segurança, permitindo que a equipe de segurança possa lidar com mais eficiência e rapidez com possíveis ameaças ou vulnerabilidades.

9.3.5 Capacidade de testar a segurança do sistema simulando um ataque real. Defender a rede

e os sistemas, respondendo aos ataques simulados e implementando medidas de segurança para evitar possíveis violações de segurança.

9.4. Ciclo de Vida da Demanda

A expectativa de uso deverá ser de, no mínimo, 36 (trinta e seis) meses.

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

Todos os usuários de Tecnologia da Informação (TI) a serviço do Poder Judiciário do Estado do Ceará, bem como, todo o público jurisdicionado que utiliza, direta ou indiretamente, os serviços de informática deste Poder.

9.6. Expectativa de entrega da solução

Até outubro de 2023.

10. RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

10.1 Aumento de rapidez em detecção e respostas a ameaças e incidentes, trazendo ganho de eficiência operacional e gestão de risco.

10.2 Maior visibilidade, fortalecimento, inteligência e a maturidade em de segurança da informação.

10.3 Automação dos processos de tarefas repetitivas e rotineiras, permitindo que a equipe de segurança se concentre em atividades mais críticas e aumentando a confiança dos usuários nos serviços prestados pelo TJCE.

10.4 Melhoria da conformidade regulatória. Mantendo o TJCE em conformidade com as leis e regulamentações de segurança, minimizando o risco de penalidades ou multas.

10.5 Serviço técnico especializado de testes de invasão por meio da identificação, mapeamento e documentação de possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica, com o objetivo de avaliar a eficácia das medidas de segurança existentes, assim como analisar, remediar, conter e documentar os eventos de segurança da informação que podem ser transformados em incidentes de segurança para implementação de medidas de proteção.

10.6 Serviço técnico especializado ininterrupto (24h x 7d x 365d) de monitoramento, controle e visibilidade de ataques cibernéticos no tráfego de rede do TJCE (aplicações em nuvem ou *on-premise*, servidores *bare-metal* ou virtualizados, equipamentos de roteamento/switch de redes e equipamentos ou aplicações de segurança de redes), com processos de triagem e respostas/tratamento a incidentes de segurança.

10.7 Uso de ferramentas tecnológicas para coleta, análise, correlação e retenção de logs do tráfego de rede do TJCE, com o objetivo de gerenciar eventos de maneira automatizada para executar detecção de ameaças, respostas a incidentes, simplificar processos de contabilidade e auditoria, acelerar fluxos de trabalho e tornar o serviço técnico especializado mais eficiente.

10.8 Treinamento especializado para repasse de conhecimento do serviço técnico especializado.

11. FONTE DE RECURSOS

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, 02 de junho de 2023.

PREENCHIMENTO PELA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

13. IDENTIFICAÇÃO E CIÊNCIA DOS INTEGRANTES TÉCNICOS

Nome	Max Eduardo Vizcarra Melgar	**Matrícula**	48994
Cargo	Analista Judiciário	**Lotação**	Coordenadoria de Segurança da Informação
E-mail	max.melgar@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.			
Max Eduardo Vizcarra Melgar – 48994 Integrante Técnico			
Fortaleza, 02 de junho de 2023.			

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, 02 de junho de 2023.

PREENCHIMENTO PELA ÁREA ADMINISTRATIVA

14. DECISÃO DA AUTORIDADE COMPETENTE

14.1. 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;

14.2. 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 aquisição de serviços inovadores de tecnologia da informação para obter ganhos na segurança, estabilidade, disponibilidade e desempenho dos Sistemas Administrativos e Judiciais que utilizam a solução atual.

15. IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO

Nome	Fábio de Carvalho Leite	**Matrícula**	9594
Cargo	Técnico Judiciário	**Lotação**	Coordenadoria de Gestão Administrativa de T.I.
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 Integrante Administrativo			
Fortaleza, 02 de junho de 2023.			

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.

Caroline Moraes Maia Fiúza – 3051

Autoridade Competente da Área Administrativa

Fortaleza, 02 de junho de 2023.