ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ

DOCUMENTO DE FORMALIZAÇÃO DE DEMANDA – DFD

Síntese do Tipo de Demanda: Promoção de ações de conscientização em segurança e defesa cibernética, a fim de garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD). No TJCE, essa iniciativa é especialmente relevante, onde a segurança digital é indispensável à proteção de dados sensíveis, ao funcionamento de sistemas críticos e à preservação da confiança pública.

1. IDENTIFICAÇÃO DA ORIGEM DA DEMANDA

Área da Demanda: SETIN/Diretoria de Infraestrutura de TI/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 uma necessidade específica detectada e os seus 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. Durante implementação das atividades no âmbito do Programa de Modernização do Poder Judiciário do Estado do Ceará – PROMOJUD, foi identificada a necessidade de realizar capacitações ligadas ao Programa de Desenvolvimento de Pessoas, conforme Produto 2.5 Capital humano aprimorado, Componente II Transformação Digital para Fortalecer a Governança e a Gestão da Carta Consulta à Comissão de Financiamentos Externos – COFIEX.

3.2. Atualmente, as pessoas são reconhecidas como o elo mais vulnerável na cadeia de segurança

da informação das organizações. Segundo reportagem em mídia especializada (https://www.cisoadvisor.com.br/hackers-adotam-novas-taticas-em-ataques-de-phishing), grupos de cibercriminosos estão utilizando ferramentas cada vez mais avançadas para obter sucesso em ataques que exploram técnicas de engenharia social, como *phishing* e *spear phishing*. Tais ataques são a porta de entrada para invasão do ambiente tecnológico, roubo/evasão de dados valiosos e realização de fraudes e golpes.

3.2.1. *Phishing* é um termo amplo para ataques cibernéticos que visam induzir uma vítima a compartilhar informações confidenciais, como logins, senhas e informações bancárias. Geralmente, esses ataques são realizados por meio de e-mails, SMS ou chamadas telefônicas.

3.2.2. *Spear Phishing* é um tipo de ataque de *phishing* que tem como alvo um indivíduo ou grupo específico dentro de uma organização. Diferentemente dos ataques de *phishing* em larga escala, o *spear phishing* é altamente personalizado e visa enganar a vítima para divulgar informações confidenciais, fazer o download de malware ou realizar ações não autorizadas.

3.3. Tais ataques são a porta de entrada para invasão do ambiente tecnológico, roubo/evasão de dadosvaliosos e realização de fraudes e golpes.

3.4. Segundo o relatório Custo de uma violação de dados em 2022, da IBM (https://www.ibm.com/br-pt/reports/data-breach), as violações tiveram um custo médio global de 4,35 milhões de dólares nas organizações estudadas. Dentre as descobertas na pesquisa realizada, chama a atenção que o *phishing* foi a causa de violação de maior impacto financeiro e que o comprometimento de credenciais de acesso foi a causa mais comum.

3.5. Para reduzir esses riscos, não basta a implementação de controles e de soluções tecnológicas de segurança. Uma das principais normativas na área de segurança da informação, a ISO 27002, possui um controle chamado "Conscientização, educação e treinamento em segurança da informação", que estabelece o seguinte:

> *Convém que todos os funcionários da organização e, onde pertinente, partes externas recebam treinamento, educação conscientização*

> *apropriados, e as atualizações regulares das políticas procedimentos organizacionais relevantes para as suas funções.*

3.6. Outro framework bastante conhecido na área de segurança da informação, o *CIS Controls* v8, estabelece, no controle 14, a necessidade de:

> *Estabelecer e manter um programa de conscientização de segurança para influenciar o comportamento da força de trabalho para ser consciente em segurança e devidamente qualificada para reduzir os riscos de segurança cibernética para a empresa.*

3.7. Ademais, a Estratégia Nacional de Segurança Cibernética do Poder Judiciário, instituída pela Resolução CNJ nº 396/2021, contempla, dentre diversos itens, "ações de comunicação, de conscientização, de formação de cultura e de direcionamento institucional com vistas à segurança cibernética."

3.8. Diante desse cenário, há uma necessidade clara de desenvolver um programa contínuo de capacitação em segurança da informação para todos os colaboradores, a fim de reduzir lacunas no conhecimento e fortalecer o ambiente tecnológico do Tribunal, por meio de métodos que aumentam o engajamento e a facilidade de entendimento dos assuntos por parte do público-alvo. Outro fator importante que deve ser considerado é que, no formato atual, a enxuta equipe da Coordenadoria de Segurança da Informação é responsável por atualizar periodicamente o material existente e até mesmo criar novos conteúdos, fazendo com que atividades críticas sejam colocadas em segundo plano.

3.9. Portanto, é imprescindível que se busque uma forma de proporcionar ao Tribunal treinamento contínuo em segurança da informação, contribuindo para a difusão de práticas seguras e mitigação de riscos cibernéticos, por meio da execução de um Programa de conscientização e capacitação os usuários dos equipamentos e sistemas de T.I.C do TJCE em segurança da informação, conforme programado na linha 6,46 do Plano de Aquisições do Promojud.

4. DESCRIÇÃO SUSCINTA DA SOLUÇÃO

4.1. Para atender a essa necessidade, a contratação de empresa especializada em capacitação da segurança da informação, apresenta-se, em princípio, como a alternativa mais adequada para atender à demanda identificada.

4.2. Desta forma, e considerando a necessidade de garantir que os servidores e colaboradores do TJCE adquiram conhecimentos e habilidades para proteger dados, sistemas e infraestrutura contra ameaças cibernéticas, esta demandante entende ser pertinente a contratação de empresa especializada para a implementação de um programa em segurança da informação.

4.3. É necessário que as pessoas sejam capacitadas e treinadas no assunto, de forma a serem capazes de identificar tentativas de golpes e de fraudes, reduzindo as chances de consumação de ataques que visam à obtenção de algum meio para transpor os mecanismos de segurança tecnológica

4.4. Essa contratação será necessária para treinar os servidores e colaboradores do TJCE em diferentes níveis de conhecimento, realizar simulações e testes práticos de ataques, realizar avaliações de maturidade em segurança das informações, bem como sensibilizar os servidores e colaboradores sobre as boas práticas no uso dos sistemas e equipamentos do TJCE, por meio da implementação de um programa de capacitação em segurança da informação, com o objetivo de promover maior adesão e engajamento dos usuários, através da realização de campanhas de conscientização direcionadas ao público interno do TJCE, abordando tópicos essenciais para fortalecer a cultura de segurança, assegurando que todos estejam preparados para enfrentar os desafios relacionados à segurança da informação.

4.5. Público-alvo:

4.5.1. Todos os usuários e usuárias de equipamentos de T.I do TJCE.

5. ALINHAMENTO ENTRE A DEMANDA E O PLANEJAMENTO ESTRATÉGICO INSTITUCIONAL E/OU PLANEJAMENTO ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO ÓRGÃO

6.1 Esta demanda se relaciona ao objetivo estratégico “Fortalecer a inteligência de dados e a segurança da informação”, de modo que se mostra aderente ao Planejamento Estratégico do

Tribunal de Justiça do Ceará 2030.

6. ALINHAMENTO AO PLANO ANUAL DE CONTRATAÇÕES 2025

6.1. O objeto da contratação está previsto no Plano de Contratações Anual 2025, especificamente no Código da Contratação TJCESGP_UGP_2025_0003.

7. FONTE DE RECURSOS

7.1. Para a demanda ora posta, no caso desta contratação os recursos financeiros serão provenientes do Projeto de Modernização do Poder Judiciário do Estado do Ceará - PROMOJUD.

7.2. O custo da contratação será financiado com recursos do Contrato de Empréstimo nº 5248/OC-BR, conforme programado no Plano de Execução Plurianual (PEP), Plano Operacional Anual e Plano de Aquisição (Componente II, Produto 2.5, Projeto 2.5.3) com resultado previsto na Matriz de Resultado do Programa, conforme programado na linha 6,46, por Sistema Nacional (SN) - Pregão Eletrônico/SRP, do Plano de Aquisições do Promojud, atualizado pelo TJCE e aprovado pelo BID.

8. COMPLEMENTO DE INFORMAÇÕES

8.1. O desenvolvimento de cada um dos produtos do PROMOJUD depende da realização de contratações previstas no Plano de Aquisições do Programa. Essas contratações devem seguir as Políticas de Aquisição do BID, especificamente a GN-2349-15 (Políticas para aquisição de bens e contratação de obras financiadas pelo BID) e a GN-2350-15 (Políticas para a seleção e contratação de consultores financiados pelo BID), e as modalidades de contratação do Sistema Nacional aceitas pelo Banco.

ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ

ENCAMINHAMENTO
Encaminho a Secretária da Secretaria da Tecnologia da informação, Denise Maria Norões Ólsen, para análise e providências, especialmente para definir a pertinência e forma de atendimento e, caso decidido pela contratação, encaminhamento à equipe de planejamento para providências seguintes.
HELDIR SAMPAIO SILVA:99576848334 Assinado de forma digital por HELDIR SAMPAIO SILVA:99576848334 Dados: 2025.03.18 14:14:39 -03'00' Heldir Sampaio Silva **Gerência de Segurança da Informação e Ambientes Tecnológicos** Solicitante
Fortaleza, de março de 2025.

Ciente da demanda apresentada, passo a complementar a avaliação da mesma e indicação de providências.

9. DECISÃO DE ANDAMENTO

9.1. Em vista das constatações deste documento, aprovo o prosseguimento do atendimento da demanda, com a análise das alternativas para a implementação de um programa de conscientização em segurança da informação.

9.2. Após conclusão do Estudo Técnico Preliminar (ETP), submeta-se ao Centro de Formação de Servidores/Coordenadoria Pedagógica para deliberação, que indica formulação de artefato de contratação (Termo de Referência).

DENISE MARIA NOROES OLSEN:28381610320

Assinado de forma digital por DENISE MARIA NOROES OLSEN:28381610320
Dados: 2025.03.18 15:35:37 -03'00'

Denise Maria Norões Ólsen
Secretária da Secretaria da Tecnologia da Informação

Fortaleza, de março de 2025