



CONSELHO DA JUSTIÇA FEDERAL

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA - DOD Nº 0576012/2024

INTRODUÇÃO

Em conformidade com o Guia de Contratações de Soluções de TIC, previsto no art. 3º da Resolução CNJ n. 468, de 15 de julho de 2022, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda – DOD pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução.

De maneira complementar, devem ser observadas as disposições contidas na Seção I, artigos do 4º ao 7º, da Portaria CJF n. 232, de 30 de maio de 2023, que tratam da elaboração e tramitação do DOD até a nomeação da Equipe de Planejamento e Apoio à Contratação – EPAC.

PREENCHIMENTO PELA ÁREA REQUISITANTE

1 – IDENTIFICAÇÃO DA ÁREA REQUISITANTE

Área Requisitante (Unidade/Diretoria/Coordenação/Divisão/Seção): Secretaria de Tecnologia da Informação	Matrícula: 1091
Responsável pela demanda: Charles Fernando Alves	
E-mail: charles.alves@cjf.jus.br	Telefone: 3022-7401

2 – IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE TITULAR (Portaria CJF n. 232/2023, art. 4º, inciso IV)

Nome: Jefferson Colombo Barbosa Xavier	Matrícula: 740
Cargo: Subsecretário de Infraestrutura e Suporte Técnico	Lotação: STI/SUTEC
E-mail: colombo@cjf.jus.br	Telefone: 3022-7420

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas no Guia de Contratações de Soluções de TIC, previsto no art. 3º da Resolução CNJ n. 468, de 15 de julho de 2022, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

3 – IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE SUPLENTE (Portaria CJF n. 232/2023, art. 4º, inciso IV)

Nome: Matheus Souza Fonseca	Matrícula: 958
Cargo: Diretor de Divisão	Lotação: STI/DIDIA
E-mail: matheus.fonseca@cjf.jus.br	Telefone: 7413

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE definidas no Guia de Contratações de Soluções de TIC, previsto no art. 3º da Resolução CNJ n. 468, de 15 de julho de 2022, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

4 – IDENTIFICAÇÃO DA DEMANDA

Contratação de solução em modelo SaaS (*Software* como Serviço) para auditoria, monitoramento, proteção de dados, detecção e resposta a ameaças a metadados e dados não estruturados, além de análise de dados em repositórios corporativos internos (*on-premises*) ou em ambiente *cloud* (nuvem) em plataformas de colaboração.

5 – ALINHAMENTO AO PLANO ESTRATÉGICO DE TI – PETI 2021-2026 (Resolução CJF n. 685/2020 – Anexo I)

ID	Objetivos Estratégicos
1	Aperfeiçoar e assegurar a efetividade dos serviços de TI para a Justiça Federal.
2	Promover e fortalecer a segurança da informação digital na Justiça Federal.

6 – ALINHAMENTO AO PLANO DIRETOR DE TI – PDTI 2024-2026

ID	Iniciativa do PDTI
INIC-2024-008	Implantar política de gestão de dados e inteligência artificial

7 – ALINHAMENTO COM O PLANO DE CONTRATAÇÕES ANUAL – PCA 2024 (Portaria CJF n. 232/2023, art. 4º, inciso II)

Item	Descrição
96	Aquisição de solução de governança/auditoria de dados

8 – JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO (Portaria CJF n. 232/2023, art. 4º, inciso I)

Este Conselho lida diariamente com uma grande diversidade de informações, das quais algumas são protegidas por lei. A presente contratação tem por objetivo atender demandas relacionadas a proteção dessas informações somados aos esforços já empregados em outras frentes, como as práticas procedimentais para a Gestão da Segurança da Informação (eletrônica ou física), bem como antivírus e bloqueio de acessos indevidos aos ativos de TI.

Segundo o instituto de pesquisas técnicas e análises de tendências de TI - o GARTNER GROUP, cerca de 80% dos dados estratégicos estão armazenados em "base de dados não estruturadas" que se traduz em pastas, arquivos, vídeos, imagens, e-mails dentre outros, que tem como responsáveis (donos): departamentos, setores e pessoas. As informações do Conselho da Justiça Federal se encontram espalhadas em diversos locais, e a utilização de plataformas em nuvem, ao mesmo tempo em que entregam uma velocidade e disponibilidade ímpares para otimizar os trabalhos da nobre atividade jurisdicional, também aumentam a dificuldade em monitorar todos os acessos aos dados do CJF. Por conseguinte, a probabilidade de ocorrerem acessos não autorizados cresce exponencialmente, e a viabilidade de auditar tamanha infinidade de repositórios de informações de forma não automatizada é absolutamente inviável.

Estes dados são acessados diuturnamente pela rede do CJF e gerenciados por Sistemas Operacionais - SO que proporcionam os registros (logs) dos eventos (alteração, inclusão, exclusão e outros). Uma vez registrados tais eventos, que tem uma ordem de volume na casa de milhões, o SO não fornece forma eficiente de busca de informação para efeito por exemplo de auditoria; a interface é ineficiente para consultas e pesquisas, além de não fazer monitoramento e análise crítica de eventos visando detecção antecipada de situações indevidas, tornando inviável qualquer tipo de gerenciamento e auditoria de acesso a dados de forma real e imediata. Ou seja, com as ferramentas básicas que um analista de sistema operacional ou administrador de rede possui é praticamente inviável auditar quem acessou, modificou, apagou, renomeou ou enviou qualquer arquivo da referida "base não estruturada". Assim, o volume de usuários na rede interna multiplicados pelos eventos que cada um realiza diariamente, torna a atividade de auditoria, monitoramento e gerenciamento como uma "missão inexecutável", especialmente para a visão e gestão integrada dos serviços de AD (Microsoft Active Directory), servidor de Arquivos (Microsoft File Server) e sistema de correio eletrônico (Microsoft Exchange Server).

Neste ponto, importante reforçar a necessidade de aderência de regulamentações associadas a privacidade e proteção de dados, como a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD); a Resolução CNJ nº 396, de 7 de junho de 2021 - institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ); as Normas Internacionais de Segurança da Informação (ISO 27001/27002/27005/22301) e CIS Control V.8 (Critical Security Controls), dentre outras.

A contratação de uma solução de auditoria de dados ajudar a mitigar e solucionar uma série de problemas relacionados à segurança e gerenciamento de dados. Aqui estão alguns exemplos:

1. Identificação de ameaças internas: pode ajudar a identificar atividades suspeitas de usuários internos, como acesso não autorizado a dados sensíveis, compartilhamento indevido de informações confidenciais, entre outros.
2. Proteção contra vazamento de dados: pode detectar e alertar sobre tentativas de vazamento de dados, ajudando a prevenir incidentes de segurança que possam resultar na perda ou exposição de informações sensíveis.
3. Cumprimento de normas e regulamentações: oferece recursos para ajudar as empresas a cumprir normas como GDPR, LGPD e outras regulamentações de proteção de dados, fornecendo relatórios e auditorias detalhadas sobre o uso e acesso aos dados.
4. Melhoria na visibilidade e controle dos dados: fornece uma visão abrangente das atividades de dados em toda a rede, permitindo que as empresas identifiquem áreas de risco, monitorem o acesso aos dados e implementem políticas de segurança mais eficazes.

5. Detecção de ransomware e malware: pode ajudar a identificar atividades suspeitas associadas a ransomware e malware, permitindo uma resposta rápida para mitigar os danos causados por essas ameaças.
6. Aprimoramento da segurança do Active Directory: pode ajudar a proteger o Active Directory contra ameaças internas e externas, identificando e corrigindo configurações inadequadas que possam colocar em risco a segurança da rede.

A implementação de uma solução de auditoria de dados deve ser parte de uma estratégia abrangente de segurança da informação, que inclua políticas claras, treinamento sobre segurança cibernética dos servidores e prestadores e outras medidas de proteção de dados.

9 – PREVISÃO DA DATA DE INÍCIO DA PRESTAÇÃO DOS SERVIÇOS (Portaria CJF n. 232/2023, art. 4º, inciso III)

Setembro de 2024.

10 – RESULTADOS A SEREM ALCANÇADOS

A adoção de uma solução de auditoria de dados proporcionará inúmeros benefícios ao CJF, dentre eles:

1. Auditar acessos nos mais variados repositórios de dados (file server, sharepoint, exchange, onedrive, etc);
2. Controlar dados não estruturados e estruturados;
3. Auditar ambiente Active Directory: alterações em GPOs do domínio, grupos do domínio, permissões de compartilhamentos, delegação de permissões, comportamento de usuário;
4. Auditar servidores de arquivos Microsoft;
5. Identificar compartilhamentos de arquivos não autorizados, que possam resultar em vazamento de informações;
6. Auditar as ações em credenciais do domínio, como criação, reset de senha, deleção, adição ou remoção em grupos;
7. Utilizar solução de inteligência artificial para identificar desvios de padrão, informação que será utilizada em análises forenses de incidentes cibernéticos, possibilitando uma ação proativa do SOC;
8. Monitorar atividades de usuários: monitoramento detalhado das atividades dos usuários em relação aos recursos tecnológicos;
9. Identificar e classificar dados sensíveis: possibilita a identificação de dados sensíveis e classificação de informações críticas;
10. Aplicar políticas de segurança que garantam que apenas usuários autorizados tenham acesso às informações;
11. Mitigar ameaças internas: dificulta o vazamento indevido de informações confidenciais ou sensíveis;
12. Proteger contra Ransomware e ataques cibernéticos: identifica padrões e comportamentos suspeitos, desvios de comportamentos, prevenindo e protegendo contra atores maliciosos;
13. Controle de acesso baseado em função: implementa políticas de controle de acesso baseados na função;
14. Resposta a incidentes: em casos de incidentes cibernéticos, viabiliza investigação forense com rastreabilidade detalhada, e ainda possibilita a realização de ações corretivas;
15. Auditar ambiente Exchange On-premises e Online;
16. Auditar ambiente Azure, Sharepoint e Teams.

11 – FONTE DE RECURSOS

Plano orçamentário (PO):

- SEG0 – Segurança da Informação

Natureza da despesa (NDD):

- 33.90.40.11 Suporte de Infraestrutura de TIC

12 – IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome:

André Conterato Brasileiro da Costa

Matrícula:

1103

Cargo: Chefe de Seção	Lotação: SUTEC/SESINF
E-mail: andre.costa@cjf.jus.br	Telefone: 3022-7419
Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas n o Guia de Contratações de Soluções de TIC, previsto no art. 3º da Resolução CNJ n. 468, de 15 de julho de 2022, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.	

13 – IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO (SUPLENTE)	
Nome: Adriana de Jesus Moraes	Matrícula: 382
Cargo: Chefe de Seção	Lotação: DIDIA/SESSER
E-mail: adriana@cjf.jus.br	Telefone: 3022-7401
Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO definidas n o Guia de Contratações de Soluções de TIC, previsto no art. 3º da Resolução CNJ n. 468, de 15 de julho de 2022, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.	

14 – ENCAMINHAMENTO
Encaminhe-se ao Secretário de Tecnologia da Informação para providências.

	Autenticado eletronicamente por Matheus Souza Fonseca, Diretor(a) - Divisão de Tratamento de Dados, Inovação e Inteligência Artificial , em 24/04/2024, às 19:33, conforme art. 1º, §2º, III, b, da Lei 11.419/2006 .
	Autenticado eletronicamente por André Conterato Brasiliano da Costa, Chefe - Seção de Suporte à Infraestrutura , em 25/04/2024, às 11:52, conforme art. 1º, §2º, III, b, da Lei 11.419/2006 .
	Autenticado eletronicamente por Adriana Jesus de Moraes, Chefe - Seção de Suporte a Serviços , em 25/04/2024, às 11:52, conforme art. 1º, §2º, III, b, da Lei 11.419/2006 .
	Autenticado eletronicamente por Jefferson Colombo Barbosa Xavier, Subsecretário(a) - Subsecretaria de Tecnologia e Suporte Técnico , em 26/04/2024, às 10:45, conforme art. 1º, §2º, III, b, da Lei 11.419/2006 .



A autenticidade do documento pode ser conferida no site
https://sei.cjf.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0
informando o código verificador **0576012** e o código CRC **9518E65B**.

Setor de Clubes Esportivos Sul - Lote 09 - Trecho III - Polo 8 - Bairro Asa Sul - CEP 70200-003 - Brasília - DF - www.cjf.jus.br

Processo nº0000921-59.2024.4.90.8000

SEI
nº0576012