ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

DOCUMENTO DE OFICIALIZAÇÃO DE DEMANDA – DOD

AQSETIN2019002 – Solução de gestão e auditoria dos controladores de domínio, dos servidores de arquivos e dos serviços de *e-mail* de forma centralizada.

PAC: TJCESETIN_2025_0007

1 INTRODUÇÃO

O presente documento tem por finalidade formalizar o início do processo de planejamento para a provisão de solução de gestão e auditoria dos controladores de domínio, dos servidores de arquivos e do serviço de e-mail de forma centralizada para o Tribunal de Justiça do Estado do Ceará, vincular as necessidades, provenientes da solução, aos objetivos estratégicos e às necessidades corporativas da instituição, garantindo alinhamento ao Plano Estratégico Institucional e ao Painel de Contribuição da TI, indicar a fonte de recursos e indicar os integrantes da Equipe de Planejamento da Contratação.

PREENCHIMENTO PELA ÁREA DEMANDANTE

2 IDENTIFICAÇÃO DA ÁREA DEMANDANTE

Área Demandante: Diretoria de Infraestrutura de TI

Nome do/da Projeto/Aquisição: Solução de gestão e auditoria dos controladores de domínio, dos servidores de arquivos e dos serviços de e-mail de forma centralizada.

Responsável pela Demanda: Cristiano Henrique Lima de Carvalho

Matrícula: 9630

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

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

3 IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE DEMANDANTE

Nome	Cristiano Henrique Lima de Carvalho	**Matrícula**	5198
Cargo	Diretor de Infraestrutura de TI	**Lotação**	Diretoria de Infraestrutura de TI
E-mail	cristiano.carvalho@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.			
Cristiano Henrique Lima de Carvalho – 5198 Integrante demandante			

4 IDENTIFICAÇÃO DA DEMANDA

4.1 Provimento de **solução de gestão e auditoria dos controladores de domínio, dos servidores de arquivos e dos serviços de e-mail de forma centralizada**, com o fito de atender as necessidades de gestão dos ativos de TIC do TJCE.

5 ALINHAMENTO AOS PLANOS ESTRATÉGICOS

5.1A proposição de uma **solução de gestão e auditoria dos controladores de domínio, dos servidores de arquivos e dos serviços de e-mail de forma centralizada**, está alinhada e presente no mapa do Planejamento Estratégico do TJCE 2030 com os objetivos de:

ID	Objetivo Estratégico Institucional	ID	Objetivos de Contribuição da SETIN
02	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 2025 – 2026

ID	Iniciativa Elencada no PDTIC 2025 – 2026
01	N25048 – Aquisição de Auditoria AD

7 METAS DO DESDOBRAMENTO ESTRATÉGICO DE TI A SEREM ALCANÇADAS

INDICADOR	META
Indicador 2: Índice de conformidade com as políticas de segurança de TIC	Atender 90% de itens das normas até 2026

8 ALINHAMENTO AO PLANO ANUAL DE CONTRATAÇÕES 2025

ITEM	DESCRIÇÃO
TJCESETIN_2025_0007	Solução para análise e auditoria dos usuários do TJCE

9 MOTIVAÇÃO E JUSTIFICATIVA

9.1 Situação Atual

9.1.1 Atualmente o TJCE utiliza o ambiente ***Microsoft Active Directory (On-Premise) – MSAD*** como plataforma de gerenciamento de objetos e recursos da sua rede, composta pelos seguintes componentes:

9.1.1.1 Controlador de Domínio *(Domain Controller)*

9.1.1.1.1 Servidores que armazenam a base de dados do *Active Directory* e gerenciam a autenticação e a autorização de usuários e dispositivos dentro de um domínio.

9.1.1.2 Servidor *Global Catalog (Global Catalog Server)*

9.1.1.2.1 O *Global Catalog* é um serviço que armazena uma cópia parcial de todos os objetos em todos os domínios na floresta do *Active Directory*.

9.1.1.3 *Active Directory Domain Services (AD DS)*

9.1.1.3.1 Este é o serviço principal do *Active Directory*. O *AD DS* fornece autenticação, autorização e um repositório centralizado para informações sobre objetos na rede, como usuários, grupos e dispositivos. Ele também gerencia a estrutura hierárquica de domínios, árvores e florestas.

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

9.1.1.4Active Directory Users and Computers (ADUC)

9.1.1.4.1 O *ADUC* é uma ferramenta de administração que permite aos administradores gerenciar objetos de diretório, como usuários, grupos e computadores. Ele fornece uma interface gráfica para criar, modificar e excluir objetos no *Active Directory*.

9.1.1.5Política de Grupo (Group Policy)

9.1.1.5.1 O *Group Policy* é uma tecnologia que permite a administração centralizada de configurações e políticas de segurança para usuários e computadores em uma rede. Com o *Group Policy Management Console (GPMC)*, os administradores criam e aplicam políticas de grupo para configurar e controlar o ambiente dos usuários e dispositivos.

9.1.1.6Unidade Organizacional (*OU*)

9.1.1.6.1 Unidades Organizacionais são contêineres dentro de um domínio que permitem a organização hierárquica de objetos como usuários, grupos e computadores. Elas ajudam a aplicar políticas e permissões de forma granular e simplificam o gerenciamento de recursos e configurações.

9.1.2 Microsoft Azure Active Directory (Online) - Azure AD:

9.1.2.1O *Microsoft Azure Active Directory (Azure AD)* se trata de um serviço de identidade baseado na nuvem, oferecido pela *Microsoft*, atualmente responsável pelo gerenciamento, autenticação e autorização de usuários, aplicativos e dispositivos do ambiente de colaboração *Microsoft 365 (online)* do TJCE. É um diretório de identidade que viabiliza o controle de acessos e a implementação de políticas de segurança do *Microsoft 365*, sendo fundamental para a governança de TI;

9.1.2.2O *Azure AD* opera como um *Identity as a Service* (IDaaS), garantindo a autenticação segura dos usuários e dispositivos em redes corporativas, aplicativos SaaS e infraestrutura híbrida. Suas principais funcionalidades incluem:

9.1.2.2.1 Autenticação e gerenciamento de identidade, por meio do suporte ao *Single Sign-On (SSO)*, permitindo que usuários acessem múltiplos sistemas com uma única autenticação; *Multi-Factor Authentication (MFA)* para aumentar a segurança do acesso, exclusivo ao ambiente *Microsoft 365 (online)* e o *Conditional Access*, que impõe regras para permitir ou negar login com base em fatores como local, dispositivo e risco;

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

9.1.2.3 Além dos recursos acima, o *Microsoft Azure Active Directory* (Azure AD) provê o gerenciamento de usuários e grupos, por meio da integração com *Microsoft 365*, a sincronização com o *Active Directory On-Premise* (citado no **item 9.1.1**), permitindo o uso do *Hybrid Identity*;

9.1.2.4 Logo, o *Microsoft Azure Active Directory (Azure AD)* desempenha um papel essencial na gestão de identidade e acesso (*IAM – Identity and Access Management*) do ambiente MS365 do TJCE, cuja funcionalidade garante a segurança, proteção contra ameaças e o gerenciamento centralizado de identidades.

9.1.3 O TJCE, ainda por meio da solução de colaboração *Microsoft 365 (online),* é usuário da plataforma ***Microsoft OneDrive**,* que suporta o serviço de armazenamento e compartilhamento de arquivos na nuvem, permitindo o gerenciamento de dados, colaboração em tempo real e a sincronização de informações entre dispositivos.

9.1.3.1O *MS-OneDrive* opera com o compartilhamento seguro de arquivos, com controle granular sobre permissões de acesso (edição, leitura, expiração de links, etc.) provendo a integração com *Microsoft Teams, Outlook, SharePoint* e *Office Online*, viabilizando a colaboração em tempo real.

9.1.4 Enquanto o *MS-OneDrive* trata de um servidor de armazenamento em nuvem (*online*) o ***Microsoft File Server*** provê a gestão de arquivos e pastas pelos usuários da rede do TJCE, de forma local (*On-premise*). Cujas diferenças de arquiteturas, finalidades e modos de operação seguem dispostas abaixo:

CRITÉRIO	***MICROSOFT ONEDRIVE***	***MICROSOFT FILE SERVER***
Modelo de Armazenamento	Armazenamento em nuvem *(Azure).*	Armazenamento local *(On-Premise).*
Infraestrutura	Baseado na nuvem, sem necessidade de servidores físicos locais.	Requer servidores locais e infraestrutura própria.
Acesso	Disponível via internet em qualquer dispositivo.	Disponível apenas na rede interna da empresa (salvo uso de *VPN* ou acesso remoto).
Sincronização	Permite sincronização automática entre dispositivos.	Não há sincronização automática com dispositivos externos.
Colaboração	Compartilhamento e edição simultânea com *Microsoft 365* (*Word, Excel, Teams*, etc.).	Colaboração limitada a usuários na mesma rede.

Controle de Acesso	Controle de permissões via *Azure AD* e políticas de compartilhamento.	Controle de permissões via *Active Directory* e *NTFS*.
Segurança	Criptografia em trânsito e repouso, autenticação multifator (*MFA*), auditoria na nuvem.	Segurança definida pelo administrador local (ex.: *backups, firewalls*, criptografia local).
Gerenciamento de Versões	Permite restauração de versões anteriores de arquivos.	Pode exigir configuração manual para manter versões anteriores.
Backup e Recuperação	Backup na nuvem gerenciado pela Microsoft.	Backup depende da infraestrutura e política de TI da empresa.
Custo	Assinatura Microsoft 365 ou licenciamento separado.	Custo elevado com hardware, manutenção e licenciamento de software.
Escalabilidade	Escalável automaticamente sem necessidade de aquisição de hardware.	Expansão exige compra de novos servidores e armazenamento físico.

9.1.5 Por meio da solução *Microsoft 365*, objeto do Contrato CT N.º 15/2021, o TJCE é usuário da plataforma web denominada ***Microsoft SharePoint*** que provê a gestão de conteúdos, colaboração corporativa e automação de processos e que possibilita a criação de *intranets*, repositórios documentais, portais institucionais e fluxos de trabalho automatizados, o que se revela como sendo uma ferramenta essencial para governança da informação do Judiciário Cearense;

9.1.6 Não menos importante, cabe citar que o TJCE utiliza **Serviços de *E-Mail*** hospedados em infraestruturas *On-Premise*, no caso do *Microsoft Exchange* e, *Online*, provida por meio do *Microsoft 365*, cujas diferenças de arquiteturas, finalidades e modos de operação seguem dispostas na tabela abaixo:

CRITÉRIO	*EXCHANGE SERVER* (*ON-PREMISE*)	*EXCHANGE* NUVEM (*ONLINE*)
Infraestrutura	Requer servidores próprios da empresa.	Hospedado nos *datacenters* da *Microsoft*.
Gerenciamento	Administração interna pela equipe de TI da empresa.	Gerenciado pela *Microsoft*, com menos necessidade de manutenção interna.
Escalabilidade	Limitado pela capacidade dos servidores locais.	Expansível sob demanda, sem necessidade de novos servidores.
Atualizações	Dependem da equipe interna para	Atualizações automáticas feitas pela

	implementação.	*Microsoft.*
Segurança e Backup	Controle total sobre segurança e backups.	Segurança gerenciada pela *Microsoft*, com backup automatizado.
Conformidade Regulatória	Maior controle sobre dados, permitindo adequação a normas específicas.	Certificações de conformidade com LGPD, GDPR, HIPAA, ISO, entre outras.
Acesso Remoto	Requer *VPN* ou configurações específicas.	Acesso direto pela internet, via *Outlook Web App* ou dispositivos móveis.
Recursos de Segurança	Personalizável, depende da infraestrutura local.	Proteção avançada com Microsoft Defender for *Office 365*, autenticação *multifator (MFA)* e políticas de DLP.
Armazenamento	Limitado pela capacidade dos servidores locais.	Planos do *Microsoft 365* oferecem de 50*GB* a caixas ilimitadas.
Custo Inicial	Alto investimento em hardware, licenciamento e manutenção.	Modelo de assinatura mensal ou anual sem necessidade de infraestrutura local.

9.1.6.1 Os referidos serviços oferecem as seguintes funcionalidades, utilizadas pelos usuários do Judiciário Cearense:

9.1.6.1.1 Caixas de Correio – funcionalidades de envio, recebimento e organização de *e-mails* com suporte para múltiplos dispositivos e plataformas;

9.1.6.2 Calendário – ferramentas integradas para agendamento de compromissos, reuniões e eventos, com suporte para compartilhamento e sincronização;

9.1.6.3 Contatos – gerenciamento e sincronização de contatos com funcionalidades para criar, organizar e compartilhar listas de contatos.

9.1.7 O *Microsoft Active Directory* (On-Premise) é destinado à gerência de identidades, autenticação e autorização dos usuários; computadores e demais ativos e serviços cujas informações transigem em ambientes locais – *On-Premise* – como é o caso do *Microsoft File Server* e do *Exchange Server;*

9.1.8 Enquanto o *Microsoft Azure Active Directory* é destinado à gerência de identidades, autenticação e autorização dos usuários; computadores e demais ativos e serviços cujas informações transigem em ambientes em nuvem – *Online* – como é o caso do *Microsoft OneDrive, Microsoft SharePoint, Exchange Online (Nuvem)* e demais ferramentas, ambiente e serviços providos pela plataforma *Microsoft 365;*

9.2 Descrição da Oportunidade ou do Problema

9.2.1 Consta no chamado **R1649794**, que a SETIN exerce a gestão sobre a seguinte quantidade de itens, distribuídos entre ativos e domínios:

CONTROLADORES DE DOMÍNIO	**6**
SERVIDORES DE ARQUIVOS	**3**
TENANT AD AZURE	**1**
CAIXAS DE *E-MAIL*	**11.494**
CONTAS DE USUÁRIOS	**9.879**
OBJETOS DO *AD*	**323.860**

9.2.2 Subsiste, frente a essa vasta quantidade de informações, as seguintes necessidades:

9.2.2.1 Identificação e classificação de conteúdo sensível;

9.2.2.2 Identificação de proprietários de dados;

9.2.2.3 Controle e auditoria de eventos (quem acessou o quê, e como acessou);

9.2.2.4 Assegurar autorizações baseadas em necessidades de negócio.

9.2.3 As informações, arquivos e logs gerados e hospedados pelos ambientes anteriormente expostos, são acessados por diversos usuários na rede do TJCE, demandam a necessidade de aprimorar relatórios de acesso para fins de auditoria no que se refere a quem, quando, onde e como um dado foi utilizado;

9.2.4 Algumas pastas armazenam arquivos com informações de cunho crítico ao funcionamento do TJCE e que são acessadas rotineiramente por usuários que não possuem vínculo permanente com a Corte e/ou usuários que mudam frequentemente de cargo internamente. Tais

mudanças, quando não registradas ou atualizadas, expõem os ambientes a vulnerabilidades, decorrentes dos acessos por parte de usuários que não deveriam ter permissão para tal;

9.2.5 Diante da complexidade, da massividade de ativos e domínios e da profusão de arquivos e pastas geradas e que devem ser geridas e auditadas, é ponderoso garantir soluções especializadas e eficientes que possibilitem automatizar as atividades de auditar, controlar, gerenciar e monitorar as ações dos usuários quanto aos ambientes citados no item **9.1**, prevenindo ações e comportamentos suspeitos em tempo real, protegendo dados sensíveis e controlando permissões dos usuários de forma segura. Demanda-se, desta forma, a adequação contínua do controle e monitoramento dos acessos e informações;

9.2.6 A Resolução nº 396, de 07 de junho de 2021, do Conselho Nacional de Justiça preconiza a necessidade dos Tribunais terem fortes controles sobre seus ambientes, o que inclui controle de acessos aos ambientes já citados.

9.2.7 Ademais, com a Lei nº 13,709, de 14 de Agosto de 2018 – Lei Geral de Proteção de Dados brasileira, depreende-se que o TJCE deve investir em segurança e implementar processos e tecnologias efetivos para prevenir, detectar e remediar violações de dados pessoais.

9.2.8 Vale ressaltar que a presente demanda prestigia o que estabelece o Conselho Nacional de Justiça por meio da Portaria Nº. 162/2021 que

> *Aprova Protocolos e Manuais criados pela Resolução CNJ no 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).*
>
> *Art. 5º Os protocolos e manuais aprovados por este ato deverão ser implementados por todos os órgãos do Poder Judiciário, com exceção do Supremo Tribunal Federal.*

Cujo conteúdo dispõe em certo trecho do **ANEXO VI – MANUAL DE REFERÊNCIA – GESTÃO DE IDENTIDADE E DE CONTROLE DE ACESSOS**, o seguinte:

> *1. Visão geral*
>
> *1.1 Este Manual estabelece as* ***diretrizes principais para a gestão de identidades e credenciais eletrônicas*** *bem como para o* ***controle de acessos aos sistemas, serviços e equipamentos de***

tecnologia da informação (TI)*.*

1.2 Orienta, também, quanto à ***criação de identidades e contas, formas de autenticação, gerenciamento de autorizações, remoção de contas e privilégios e registro das ações executadas para fins auditoria****.*

1.3 ***Este Manual é aplicável*** *aos titulares de contas individuais e define as responsabilidades deles quanto à proteção de suas contas e ao uso adequado de suas autorizações, bem como aos operadores* ***responsáveis pelo Gerenciamento de Identidade e Acesso para sistemas de informação****;*

3. Diretrizes gerais

*3.1.****Os órgãos do Poder Judiciário devem efetuar a gestão de identidade e o controle de acessos de seus usuários****, sejam magistrados ou magistradas, servidores ou servidoras, prestadores ou prestadoras de serviços, usuários ou usuárias dos serviços e equipe de TIC.*

3.2. Deve ser estabelecido, em normativo próprio, o regramento de cada órgão, considerando as boas práticas de segurança da informação e em observância às seguintes diretrizes:

3.2.1. Definição de padrão de identidade do órgão, que contemple, no mínimo, os critérios para padronização de nome de usuário e de conta de e-mail;

3.2.2. Consideração do princípio de privilégio mínimo e de segregação de funções, visando a evitar acessos indevidos e reduzir os riscos de vazamento de informações;

3.2.3. Estabelecimento de processo e de responsáveis por solicitação, gerenciamento e revogação de contas de acesso, preferencialmente de forma automática;

3.2.4. Utilização de login único para acesso a serviços de diretório corporativo e para acesso aos sistemas, com o objetivo de uniformizar e garantir a experiência única de interação e evitar a criação de contas e autorizações locais;

3.2.5. Adoção de modelo de controle de acesso, preferencialmente utilizando controle de acesso baseado em funções (RBAC) em que as credenciais recebam os privilégios de acesso conforme os papéis e as responsabilidades executadas pelos usuários;

3.2.6. Criação de processos de verificação de identidade nas interações entre sistemas, internos ou

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

externos, com vinculação das credenciais aos usuários e às suas autorizações;

3.2.7. Registro de trilhas de auditoria que vise ao registro dos acessos a sistema de informação, quais operações foram realizadas e em qual período;

3.2.8. Definição de requisitos de tamanho, reutilização, critérios de complexidade e período de expiração de senhas;

3.2.9. Empenho pela adoção de múltiplo fator de autenticação;

3.2.10. Busca pela unificação de plataformas de autenticação, autorização e autenticação (AAA);

3.2.11. Estabelecimento de regras quanto ao acesso remoto e forma de disponibilização de sistemas e serviços na internet;

3.2.12. Gestão de credenciais privilegiadas e restrição ao uso de credenciais genéricas e de uso compartilhado;

3.2.13. Rastreabilidade de acessos e ações executadas por administradores de TI;

3.2.14. Utilização de mecanismos seguros de criptografia para o armazenamento e trânsito de credenciais de acesso;

3.2.15. Segregação de redes conforme o grupo dos serviços, sistemas ou usuários;

3.2.16. Controle do acesso físico aos ativos de tecnologia da informação e comunicação (TIC);

3.2.17. Implementação de controles de acesso proporcionais à classificação da informação;

3.2.18. Monitoração dos acessos e tentativas de acesso para identificação de ataques.

9.3 Motivação da Demanda

9.3.1 De acordo com o enredo exposto, seguem, respectivamente aplicadas para cada ambiente a ser contemplado com a implementação da solução proposta, as seguintes motivações:

9.3.1.1 Ambientes ***Microsoft Active Directory (On-Premise) e Microsoft Azure Active Directory (Online)***

9.3.1.1.1 Provisão de visão completa das estruturas dos *AD's* de forma que torne mais eficiente a administração dos diretórios de usuários e grupos de segurança bem como a gestão dos servidores de arquivos;

9.3.1.1.2 Execução de auditorias eficientes dos *AD's*, uma vez que por meio dos *logs* a equipe de TI terá uma melhor visibilidade de todos os eventos ocorridos;

9.3.1.1.3 Gerenciamento das permissões e os *logs* de todas as plataformas monitoradas, otimizando assim o desempenho da equipe técnica;

9.3.1.1.4 Emissão de relatórios de maneira ágil, facilitando o controle sobre o que acontece em todos os ambientes;

9.3.1.1.5 Execução de *scripts* de consultas e pesquisas de eventos de forma rápida e eficaz;

9.3.1.1.6 Recuperação e saneamento dos ambientes em diferentes setores – investigação de ocorrências e a realização de diagnósticos e melhorias constantes com base nas melhores práticas;

9.3.1.2 Ambientes ***Microsoft File Server – Armazenamento local (On-Premise) Microsoft OneDrive – Armazenamento em nuvem***

9.3.1.2.1 Segurança e conformidade, centralizando a gestão e auditoria dos servidores de arquivos, considerando a essencialidade de garantir que o acesso e a manipulação de pastas e arquivos críticos estejam de acordo com as políticas e normas de segurança da informação e demais regulamentações aplicáveis.

9.3.1.2.2 Gerenciar e monitorar de forma precisa as permissões de acesso às pastas e arquivos, garantindo que apenas usuários autorizados possam acessar as informações. Possibilitando controles granulares e a revisão periódica de permissões.

9.3.1.2.3 Implementar e auditar políticas eficazes de backup e recuperação de dados, minimizando o risco de perda de informações críticas armazenadas no *fileserver*.

9.3.1.2.4 Proporcionar a capacidade de rastreabilidade detalhada das ações realizadas nos arquivos e pastas, como criação, modificação e exclusão, para responder rapidamente a incidentes de segurança e para auditorias internas e externas.

9.3.1.2.5 Necessidade de garantir a segurança por meio do controle sobre o acesso a dados armazenados no *OneDrive*. Os usuários do TJCE armazenam informações de relevante confidencialidade neste repositório, o que se revela crucial garantir que apenas as pessoas certas tenham acesso a determinados arquivos. Isso implica não apenas em controlar quem pode acessar os dados, mas também em garantir que essas permissões estejam alinhadas com as funções e responsabilidades de cada usuário;

9.3.1.2.6 A auditoria de acessos permite que o TJCE registre e analise as atividades de todos os usuários dentro do ambiente, identificando quem acessou quais documentos e quando, além de monitorar alterações feitas. Já o gerenciamento de permissões assegura que as permissões de acesso sejam atribuídas corretamente, de forma granular, garantindo que cada usuário tenha acesso apenas às informações necessárias para suas atividades. A auditoria de acessos e permissões é um dos mecanismos essenciais para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD), fornecendo registros detalhados sobre como os dados estão sendo acessados e manipulados, o que implica a mitigação do risco de vazamentos de dados ou uso indevido de informações;

9.3.1.2.7 O *OneDrive*, como qualquer sistema de armazenamento em nuvem, pode ser alvo de acessos não autorizados caso as permissões não sejam corretamente configuradas ou monitoradas. A auditoria de acessos ajuda a detectar atividades suspeitas, como tentativas de acesso a arquivos ou pastas fora do padrão de comportamento dos usuários;

9.3.1.2.8 Residualmente a demanda pela auditoria e gerenciamento de acessos a este ambiente visa melhorar a eficiência operacional da equipe de TI, reduzindo o tempo gasto em tarefas manuais, como a revisão de permissões ou o monitoramento de acessos, possibilitar a automatização dessas atividades e a identificação de problemas, como permissões excessivas ou acesso a dados de forma inadequada.

9.3.1.3 Ambiente ***Microsoft SharePoint***

9.3.1.3.1 O *Microsoft SharePoint* é utilizado como repositório centralizado para gestão documental e colaboração institucional, armazenando informações sensíveis, processuais e estratégicas. A inexistência de uma solução dedicada a auditoria e extração de relatórios para o ambiente compromete a transparência, a rastreabilidade e a segurança da informação, podendo gerar riscos de acessos indevidos, vazamento de informações sensíveis e não conformidade com normas de

proteção de dados e auditoria.

9.3.1.4Serviços de *E-Mail*

9.3.1.4.1 Dada a criticidade das informações hospedadas pelos servidores de e-mail do TJCE – *EXCHANGE SERVER (ON-PREMISE)* e *EXCHANGE ONLINE (NUVEM)* tem se como necessário garantir a proteção contra ameaças internas e externas em tais ambientes, considerando correios eletrônicos são os principais vetores de ataques cibernéticos, como *phishing* e *malware*. Uma solução gestão e auditoria permitirá a detecção precoce e a resposta eficiente a essas ameaças, protegendo as comunicações, assim como a conformidade com políticas de retenção de dados, objetivando assegurar que as comunicações por e-mail sejam gerenciadas de acordo com as políticas de retenção de dados e os requisitos legais, garantindo que registros importantes sejam preservados e acessíveis conforme necessário, além de auditar o conteúdo e o fluxo das comunicações;

9.3.1.5 Importante citar que diante da complexidade da demanda apresentada, é intrínseco que a solução demande a capacitação da equipe técnica que realiza a gestão dos ambientes mencionados. A qualificação da equipe é ensejada pela provisão dos serviços pertinentes à instalação da solução no ambiente do TJCE, bem como no provimento de serviço de treinamento, ambos com o intuito de munir os técnicos e unidades gestoras do conhecimento necessário para operacionalização da solução e dos benefícios derivados.

10 CICLO DE VIDA DA DEMANDA

10.1 Tendo em vista a constante evolução das tecnologias para proteção, gestão e auditoria dos controladores de domínio, dos servidores de arquivos, repositório *OneDrive* e do serviço de *e-mail*, a expectativa de uso da solução (em garantia) deverá ser de, no mínimo, 36 (trinta e seis) meses.

11 CLIENTES QUE FARÃO USO DA SOLUÇÃO (OBJETO DA DEMANDA) OU SERÃO BENEFICIADOS

11.1 Toda a Secretaria de Tecnologia da Informação do TJCE é cliente desta solução, sendo o Poder Judiciário do Ceará e seus usuários como beneficiados por esta Solução de TI.

12 EXPECTATIVA DE ENTREGA DA SOLUÇÃO

12.1 A disponibilização da solução deve ocorrer até junho de 2025.

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

13 RESULTADOS A SEREM ALCANÇADOS

13.1 A solução de gestão e auditoria permitirá um controle mais rigoroso e eficiente sobre os acessos aos controladores de domínio, servidores de arquivos, serviços de e-mail e ambiente de colaboração, tanto *On-Premise* quanto em nuvem (*online*), reduzindo significativamente o risco de acessos não autorizados e potenciais vazamentos de informações confidenciais facilitando a detecção precoce de atividades suspeitas e incidentes de segurança, permitindo uma resposta mais rápida e efetiva, minimizando impactos adversos à Administração;

13.2 Com a provisão, assegura-se que operações relacionadas aos ambientes supracitados estejam em conformidade com as regulamentações vigentes, além de facilitar a aderência a outras normativas e boas práticas de governança garantindo uma trilha de auditoria detalhada, permitindo o rastreamento completo de todas as ações realizadas, desde a criação até a modificação e exclusão de quaisquer arquivos, dados e e-mails, por meio da visualização e manipulação de acessos e *log's*.

13.3 A implementação de permissões, políticas de segurança e monitoramento de atividades, resulta em uma redução da sobrecarga administrativa e na otimização dos recursos de TI, tendo em vista que tal funcionalidade incrementa a capacidade de identificar e resolver problemas relacionados a acessos e segurança aprimorando uma visão da equipe gestora e promovendo diagnósticos mais rápidos e soluções eficazes, tais como:

13.3.1 Fornecimento de relatórios detalhados e em tempo real sobre o uso e a segurança dos recursos de TI, permitindo que a gestão tome decisões informadas e estratégicas com base em dados confiáveis;

13.3.2 Acesso rápido e preciso, em casos de investigações internas ou auditorias específicas, à informações necessárias, acelerando o processo de investigação e assegurando que todas as ações sejam devidamente documentadas e analisadas.

14 FONTE DE RECURSOS

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

15 COMPLEMENTO DE INFORMAÇÕES

15.1 Sem informações complementares para a aquisição dessa solução.

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

ENCAMINHAMENTO
Encaminhe-se ao **Gerente de Segurança da Informação e Ambientes Tecnológicos** para indicar o Integrante Técnico para composição da Equipe de Planejamento da Contratação, quando da continuidade dos expedientes necessários.
Cristiano Henrique Lima de Carvalho – 5198 Área Demandante

PREENCHIMENTO PELA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

16 IDENTIFICAÇÃO E CIÊNCIA DOS INTEGRANTES TÉCNICOS

Nome	Heldir Sampaio Silva	**Matrícula**	9630
Cargo	Gerente de Segurança da Informação e Ambientes Tecnológicos	**Lotação**	Gerência de Segurança da Informação e Ambientes Tecnológicos
E-mail	heldir.sampaio@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.			
Heldir Sampaio Silva – 9630 Integrante Técnico			
ENCAMINHAMENTO			
Encaminha-se a autoridade competente da Área Administrativa para: • Decidir motivadamente sobre o prosseguimento dos expedientes; • Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação; • 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			

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

PREENCHIMENTO PELA ÁREA ADMINISTRATIVA

17 DECISÃO DA AUTORIDADE COMPETENTE

17.1 Aprovo o prosseguimento dos expedientes, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Demandante;

17.2 Designo, o servidor identificado no item a seguir como Integrante Administrativo para composição da Equipe de Planejamento da Contratação.

18 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) 98866-3555
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 Integrante Administrativo			
Fica instituída a Equipe de Planejamento da Contratação, conforme dispõe o art. 7º, da Resolução CNJ n° 468, de 15 de julho de 2022. A Equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato.			
Caroline Moraes Maia Fiúza – 3051 Área Administrativa			