DOCUMENTO DE OFICIALIZAÇÃO DE DEMANDA – DOD

Demanda n.º 10/2025
Controle SETIC

1. IDENTIFICAÇÃO

Demanda (descrição resumida)		**Solução de monitoramento de segurança para Active Directory**
Data de proposição		01/09/2025
Requisitante / Proponente	**Unidade Administrativa**	SETIC / Divisão de Segurança da Informação e Proteção de Dados - DSIPD
	Servidor (a) responsável	Leonardo Albuquerque de Rezende
	Ramal	6280
	E-mail	leonardo.rezende@trt19.jus.br
Autorização superior	**Unidade Administrativa**	COMITÊ DE GOVERNANÇA DE TIC (RA Nº 166/2019)
	Gestor(a) responsável	MANOEL MESSIAS FEITOZA
	Data aprovação	29/09/2025

2. NECESSIDADE E/OU OPORTUNIDADE DE MELHORIA

DESCRIÇÃO DA DEMANDA

Necessidade ou oportunidade de melhoria identificada:

A modernização das formas de trabalho proporcionada, em grande parte, pela adoção do trabalho remoto trouxe consigo muitos desafios do ponto de vista de segurança da informação e proteção de dados.

Um dos principais foi a adaptação das medidas de controle e monitoramento que anteriormente estavam centradas na proteção da rede corporativa, mas passaram, então, a serem direcionadas com mais atenção também para a proteção das identidades, visto que elas se tornaram um grande vetor de ataques.

Por identidade entende-se qualquer tipo de conta capaz de proporcionar acesso a recursos de Tecnologia da Informação, como sistemas, bancos de dados, arquivos, e-mails, estações de trabalho, etc. É importante ressaltar que as identidades não precisam necessariamente estar vinculadas a indivíduos, elas podem representar recursos computacionais, como servidores de rede e aplicações.

Com o intuito de facilitar o gerenciamento, existem ferramentas para realizar o armazenamento centralizado das identidades, permitindo a utilização de uma base única para acesso aos diversos recursos computacionais. Nesse sentido, o Active Directory, desenvolvido no início dos anos

2000, é um sistema amplamente utilizado no mercado. Nele é possível armazenar objetos associados a usuários, estações de trabalho, servidores de rede, contas de serviço, grupos, entre outros.

Embora a ferramenta tenha recebido atualizações no decorrer dos anos, o Active Directory não é essencialmente um produto adaptado para comunicação com aplicações mais modernas pois não possui nativo para protocolos de autenticação e autorização usados amplamente em APIs e serviços web, como o OpenID Connect e o OAuth2.

Uma das formas de suprir essa deficiência e ao mesmo tempo permitir a coexistência de aplicações modernas e legadas é a integração das contas do Active Directory com provedores de identidade externos. Na prática isso consiste na criação de contas na nuvem com informações sincronizadas a partir do diretório local. Esse sincronismo ocorre periodicamente, permitindo que informações alteradas localmente, como senhas ou pertencimento a grupos, por exemplo, sejam replicadas para o provedor de identidade em nuvem.

Contudo, apesar de garantir o uso de login único para as diversas aplicações, essa abordagem também aumenta consideravelmente a complexidade do ambiente, assim como os riscos de segurança da informação, possibilitando que vetores de ataque na nuvem sejam utilizados para acesso a recursos on-premises e vice-versa.

Considerando que os incidentes de segurança têm como origem mais comum o comprometimento de credenciais e que o Active Directory desempenha papel fundamental no processo de gerenciamento de identidades, a proteção adequada dessa ferramenta é um tema de extrema relevância.

Assim, com base nesses fatores, visando atingir o objetivo de melhorar a prevenção, detecção e resposta de incidentes de segurança direcionados às identidades do TRT19, torna-se premente a implementação de ferramentas apropriadas para o monitoramento do Active Directory em tempo real.

Solução proposta pelo demandante (escopo):

Instruir processo administrativo para analisar a necessidade e oportunidade de se contratar e implantar uma Solução de monitoramento de segurança de Active Directory no âmbito do TRT19.

Estimativa Orçamentária

A ação será incluída no Plano de Contratações 2026 sob o item **9324 - SUPORTE PARA SOLUÇÃO DE MONITORAMENTO DE SEGURANÇA PARA ACTIVE DIRECTORY**

3. ALINHAMENTO COM O PLANEJAMENTO

3.1 ALINHAMENTO COM O PLANO ESTRATÉGICO DO TRT DA 19ª REGIÃO.

PERSPECTIVA	OBJETIVO ESTRATÉGICO	INDICADOR	IMPACTO NO INDICADOR
Aprendizado e Crescimento	Aprimorar a governança de TIC e a	Índice de processos	Modernização de equipamentos e tecnologias, garantindo o aprimoramento, a integridade e a

	proteção de dados.	judiciais eletrônicos	disponibilidade dos sistemas de informação e dos bancos de dados mantidos pelo TRT19

3.2 ALINHAMENTO COM A ESTRATÉGIA NACIONAL DE TIC DO PODER JUDICIÁRIO (ENTIC-JUD)

CÓDIGO	OBJETIVO ESTRATÉGICO
OE8	Prover Serviços de Infraestrutura e Soluções Corporativas

3.3 ALINHAMENTO COM O PLANO DIRETOR DE TIC 2025-2026 (PDTIC)

CÓDIGO	AÇÃO
9324	SUPORTE PARA SOLUÇÃO DE MONITORAMENTO DE SEGURANÇA PARA ACTIVE DIRECTORY

4. PREVISÃO ORÇAMENTÁRIA – PLANO DE AQUISIÇÃO

Previsão Orçamentária	Data prevista para entrega o ETP / TR	Data prevista para a entrega do objeto
PAC 2026 - Código: 9315	30/03/2026	30/06/2026

5. RESULTADOS ESPERADOS

TIPO DE RESULTADO	Sim	Não	Detalhamento
Ganho de produtividade	X		Com a solução, a equipe de segurança pode realizar um monitoramento de AD mais efetivo com menor esforço.
Redução de esforço	X		A solução permite a realização de monitoramento de AD de forma mais ampla e detalhada se comparada a procedimentos não automatizados.
Redução de custo		X	
Redução do uso de recursos		X	
Melhoria de controle	X		Uma solução de monitoramento permite realizar um maior número de controles de forma mais rápida e efetiva.

Redução de riscos	X		Há efetiva redução de riscos de comprometimento de identidades e vazamento de informações por meio de ataques cibernéticos.
Determinação legal		X	
Determinação administrativa		X	
Outra (Especificar)		X	

6. PROCESSOS DE TRABALHO IMPACTADOS

PROCESSO DE TRABALHO	ATIVIDADE IMPACTADA	MELHORIA ESPERADA	UNIDADES IMPACTADAS
Gestão de Segurança da Informação	Monitoramento de AD	Redução do esforço de monitoramento e de riscos de ataques cibernéticos.	SETIC

7. RISCOS DE NÃO IMPLEMENTAÇÃO DA DEMANDA

Risco	Impacto do risco ao negócio
Eventual comprometimento de identidades de usuários.	Acesso indevido ou vazamento de informações institucionais críticas, com consequente prejuízos às partes e à imagem do TRT.

8. RESTRIÇÕES PARA ATENDIMENTO DA DEMANDA

TIPO DE RESTRIÇÃO	Sim	Não	Detalhamento
Limitação de Prazo		X	
Limitação de Custo	X		O orçamento está limitado ao disponível no PCA 2026 para esta ação.
Limitação de Equipe da Área Demandante	X		Disponibilidade de um servidor com tempo compartilhado com outras ações, para acompanhamento da contratação.
Outra (Especificar)		X	

9. PARTES INTERESSADAS

PARTE INTERESSADA	POR QUE É INTERESSADA
COMITÊ GESTOR DE TIC	Demandante da ação e responsável pelos projetos em execução na SETIC.
SETIC	Responsável pela implantação e manutenção da solução.
Todas as unidades do TRT	O serviço afeta todas as atividades judicantes e administrativas de todas as unidades organizacionais do Tribunal.

10.EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO (SUGESTÃO)

ÁREA INTEGRANTE	NOME DO SERVIDOR
Unidade Requisitante	LEONARDO ALBUQUERQUE DE REZENDE – DSIPD / SETIC
Unidade Técnica	CARLOS RAFAEL ARAÚJO DA SILVA – DSIPD / SETIC
Unidade Administrativa	A ser indicado pela Secretaria de Administração