TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO

ESTUDOS PRELIMINARES DE CONTRATAÇÃO DE SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

PROAD:5132/2022

1. Capítulo I - ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1. Objeto

Aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), abrangendo garantia, serviço de instalação e treinamento.

1.2. Justificativa

A Secretaria de Tecnologia da Informação possui a incumbência de assegurar que os serviços de TIC sejam prestados de forma satisfatória, com a finalidade de garantir o Princípio da Eficiência. Neste sentido possui o dever de planejar adequadamente suas aquisições e contratações, com vistas a buscar a melhor solução para o total atendimento do interesse que se busca satisfazer.

Neste contexto, a Secretaria de Tecnologia da Informação adota, dentre outros, o método de proteção em camadas. Este método consiste em criar várias camadas de proteção distintas e complementares, sendo cada camada atuando de forma especializada em algum componente de segurança.

Esta contratação de Solução de Gerenciamento de Acessos Privilegiados tem como objetivo criar mais uma camada, visando proteger o ambiente de servidores da Justiça do Trabalho da 12 Região. Este Tribunal possui um parque de servidores diversificado, extremamente numeroso e que necessita de proteção constante. O cerne da celeridade de suas atividades, sejam elas meio ou fim, baseia-se nos recursos de tecnologia da informação. Apesar de facilitadora, a tecnologia da informação inclui novos riscos às informações recebidas, armazenadas ou transmitidas, o que requer métodos adequados de proteção das informações.

Esta solução proverá ao contratante o gerenciamento de acessos privilegiados, o gerenciamento de privilégios mínimos, proteção às credenciais privilegiadas, autenticação transparente, múltiplos fatores de autenticação e adoção

de provisionamento de acessos; geração de relatórios sobre eventos, otimização nas rotinas de identificação, detecção e análise de eventos e incidentes, armazenamento de registros de ativos de rede unificado, com auxílio à respostas e remediações de incidentes de segurança.

Devido a constante busca por melhoria dos controles internos, as instituições necessitam de um controle mais efetivo do acesso lógico ao Datacenter, incluindo o controle de atividades executadas por terceiros e a identificação proativa de segurança de possíveis ameaças internas (alvo de constantes casos de ataques cibernéticos atuais).

Além da justificativa de eficiência operacional das atividades e mudanças realizadas no datacenter, acrescenta-se uma maior inteligência de segurança no rastreamento das atividades e possível identificação de anormalidades. Não há uma forma eficaz para auditar o uso de tais credenciais. Manter as senhas dessas credenciais de forma segura é um desafio enorme pois existe uma rotatividade de pessoas (servidores, estagiários e terceirizados). Quando as pessoas deixam as seções, nada impede que elas levem consigo as senhas das credenciais privilegiadas. Mudar as senhas periodicamente é algo extremamente complexo e, em alguns casos, impossível de se fazer, pois alterar as senhas implicaria em modificações em sistemas/serviços, o que poderia impactar na sua disponibilidade. Alguns sistemas possuem as mesmas senhas há diversos anos. Um dos principais objetivos dos hackers é ter acesso a contas privilegiadas uma vez que, tendo acesso a tais credenciais, podem assumir o controle total de um sistema, roubando informações, alterando configurações, indisponibilizando serviços ou, até mesmo, destruindo de forma permanente informações importantes. Ataque (roubo) a credenciais privilegiadas é uma prática bem-sucedida no meio hacker e um dos principais alvos de ataque. Proteger de forma eficaz as credenciais privilegiadas é crítico para as instituições protegerem seus ambientes e informações.

Uma credencial é considerada como acesso privilegiado quando possui direitos para administrar outras contas; alterar, remover arquivos e programas; gerenciar contatos; conceder ou revogar o acesso de outros usuários a sistemas.

As credenciais privilegiadas são os principais alvos de invasão dos cibercriminosos. Uma conta privilegiada comprometida pode, por exemplo, conceder acesso irrestrito à infraestrutura de TI da Companhia, possibilitando ao atacante ter o controle administrativo das demais contas e obter dados internos sensíveis. Toda esta facilidade de acesso, fará com que os danos sejam irreparáveis para a empresa afetada. Desta forma, busca-se uma solução que garanta a segurança operacional por meio de trilha de auditoria dos indivíduos que têm acesso a dados sensíveis ou processos críticos de TI. A aquisição da solução de segurança visa assegurar a gestão permanente do ambiente, independentemente da marca ou do produto que estará sendo utilizado como ferramenta.

O Tribunal Superior do Trabalho conduziu processo licitatório para aquisição das ferramentas, o que culminou na Ata de Registro de Preços 58/2021 daquele órgão. O Conselho Superior da Justiça do Trabalho encaminhou a este Tribunal o Ofício Circular CSJT.SG.SETIC.NUGOV Nº 42 2022, Proad 5573/2022, em que o Excelentíssimo Ministro Emmanoel Pereira, Presidente daquele Conselho, inclui, para ciência, o parecer técnico produzido pelo Comitê Técnico de Segurança – CTSeg juntamente com o Comitê Técnico de Infraestrutura – CTInfra, que recomenda a aquisição dos itens da Ata de Registro de Preços PE nº 58/2021 do Tribunal Superior do Trabalho, tendo em vista a crescente exposição da Justiça do Trabalho a riscos de segurança da informação, e sob à luz da Resolução CNJ nº 396/2021, e ainda, informou que os recursos orçamentários para a ação serão disponibilizados por aquele Conselho aos Tribunais Regionais do Trabalho.

1.3. Quantidade

Esta contratação se destina, fundamentalmente, a prover segurança para os servidores físicos, virtuais e às estações de trabalho, no gerenciamento, monitoramento e auditoria do acesso privilegiado às informações e ativos do Tribunal.

E ainda ampliar a segurança das informações produzidas no ambiente do Tribunal e otimizar o tempo de operações realizadas no gerenciamento de acesso privilegiado.

As soluções de mercado possuem seu licenciamento baseados em usuários que acessam o ambiente e em ativos protegidos, do tipo:

- Quantidade de usuários administradores (privilegiados);
- Quantidade de estações de trabalho;
- Quantidade de máquinas servidores;
- Quantidade equipamentos de rede;
- Quantidade de aplicações em container;
- Quantidade de aplicações fora de container;
- Quantidade de instâncias de banco de dados.

Baseado neste cenário e na infraestrutura atual do Tribunal, a quantidade de cada um dos ativos a serem protegidos que o Tribunal possui hoje é:

- Quantidade de usuários administradores (privilegiados): 30 usuários;
- Quantidade de estações de trabalho: 2700;
- Quantidade de máquinas servidores: 500;
- Quantidade equipamentos de rede: 10;
- Quantidade de aplicações em container: 50;
- Quantidade de aplicações fora de container: 100;

- Quantidade de instâncias de banco de dados: 8;

Dados levantados com a equipe do Serviço de Infraestrutura - SEINFRA, que auxiliou neste ponto, visando garantir um ambiente de alta disponibilidade, escalável e seguro a fim de uma completa cobertura do ambiente computacional.

1.4 Definição e Especificação dos Requisitos.

1.4.1.1. O licenciamento da solução deve permitir a instalação de instância da solução no ambiente de contingência do Tribunal, o qual pode ser composto de serviços de computação em nuvem em ambiente contratado pelo Tribunal.

1.4.1.2. A solução não deve depender de qualquer ativo de infraestrutura que ela mesmo garante o acesso. Pretende-se evitar que os usuários privilegiados administrados pela solução, como por exemplo os do ambiente virtual, fiquem inacessíveis no caso de uma falha no ambiente de virtualização, pois, nesse cenário, a solução de controle dependeria da solução de virtualização.

1.4.1.3. A solução deve garantir a retenção dos registros de acesso por, pelo menos, 5 anos.

1.4.1.4. A solução deve gravar em vídeo os acessos privilegiados.

1.4.1.5. A solução deve possibilitar a configuração de duplo fator de autenticação para acesso aos ativos.

1.4.1.6. A solução deve permitir a inclusão de ativos na solução além do quantitativo licenciado, podendo gerar um alerta para o administrador nesta situação, mas não podendo, em hipótese alguma, impedir o acréscimo e limitar o uso.

1.4.1.7. A solução deve possuir ampla capacidade de gerar relatórios e dashboards.

1.4.1.8. A solução deve possuir mecanismos avançados de proteção dos usuários privilegiados, usando certificados digitais e criptografia, quando aplicável.

1.4.1.9. A solução deve possibilitar a realização de descoberta automática de ativos.

1.4.1.10. A solução deve atender usuários privilegiados do tipo administradores, root e admin de equipamentos e sistemas operacionais.

1.4.1.11. A solução deve permitir acesso de contas para acesso privilegiados simultâneos (admin segurança/rede/Root/Domain Admin/DBadmin/SysDBA, VMadmin, helpdesk)

1.4.1.12. A solução deve proteger usuários em:

1.4.1.12.1. Servidores Linux;

1.4.1.12.2. Servidores Windows;

1.4.1.12.3. *Storages*;

1.4.1.12.4. Estações de Trabalho Windows;

1.4.1.12.5. Equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP);

1.4.1.12.6. Aplicações conteinerizadas com *secrets*;

1.4.1.12.7. Instâncias de Banco de Dados (Oracle, PostgreSQL, MS-SQL e MySQL)

1.4.1.12.8. Aplicações não-conteinerizadas com senha embutida (*hard coded*)

1.4.1.13. A solução deve atender usuários privilegiados do tipo administradores de banco de dados Oracle, MS SQL, MySQL e PostgreSQL.

1.4.1.14. A solução deve possuir funcionalidades de gestão de usuários e perfis.

1.4.1.15. A solução deve possuir recursos de descoberta e cadastro automático de ativos.

1.4.1.16. A solução deve implementar mecanismos de proteção de credencias através de criptografia

1.4.1.17. A solução deve proteger informações privilegiadas, tais como certificados digitais e senhas.

1.4.1.18. A solução deve possuir mecanismos para bloquear comandos indesejados.

1.4.1.19. A solução deve possuir mecanismos para controlar privilégios.

1.4.1.20. A solução deve implementar rotações de senhas de fora automatizada em todos os ativos protegidos

1.4.1.21. A solução deve realizar análise comportamental do acesso dos usuários privilegiados.

Capacitação

O treinamento teórico e prático, destinado aos analistas responsáveis pela execução de atividades de administração e auditoria, para utilização de todos os softwares que compõem a solução.

1.5. Levantamento das alternativas existentes

Conforme estudo técnico, identificou-se os seguintes possíveis cenários para o objeto deste documento:

1.5.1. Cenário 1 - Desenvolvimento interno de solução PAM.

Tal alternativa necessita que a equipe de tecnologia da informação deste Tribunal desenvolva uma solução de hardware e software que realize auditoria e prevenção de ameaças à base de dados não estruturados, além de controle de acesso de usuários privilegiados, com relatórios, análise de riscos e compliance. Demandando bastante tempo, recursos humanos e investimento em qualificação da equipe em segurança da informação.

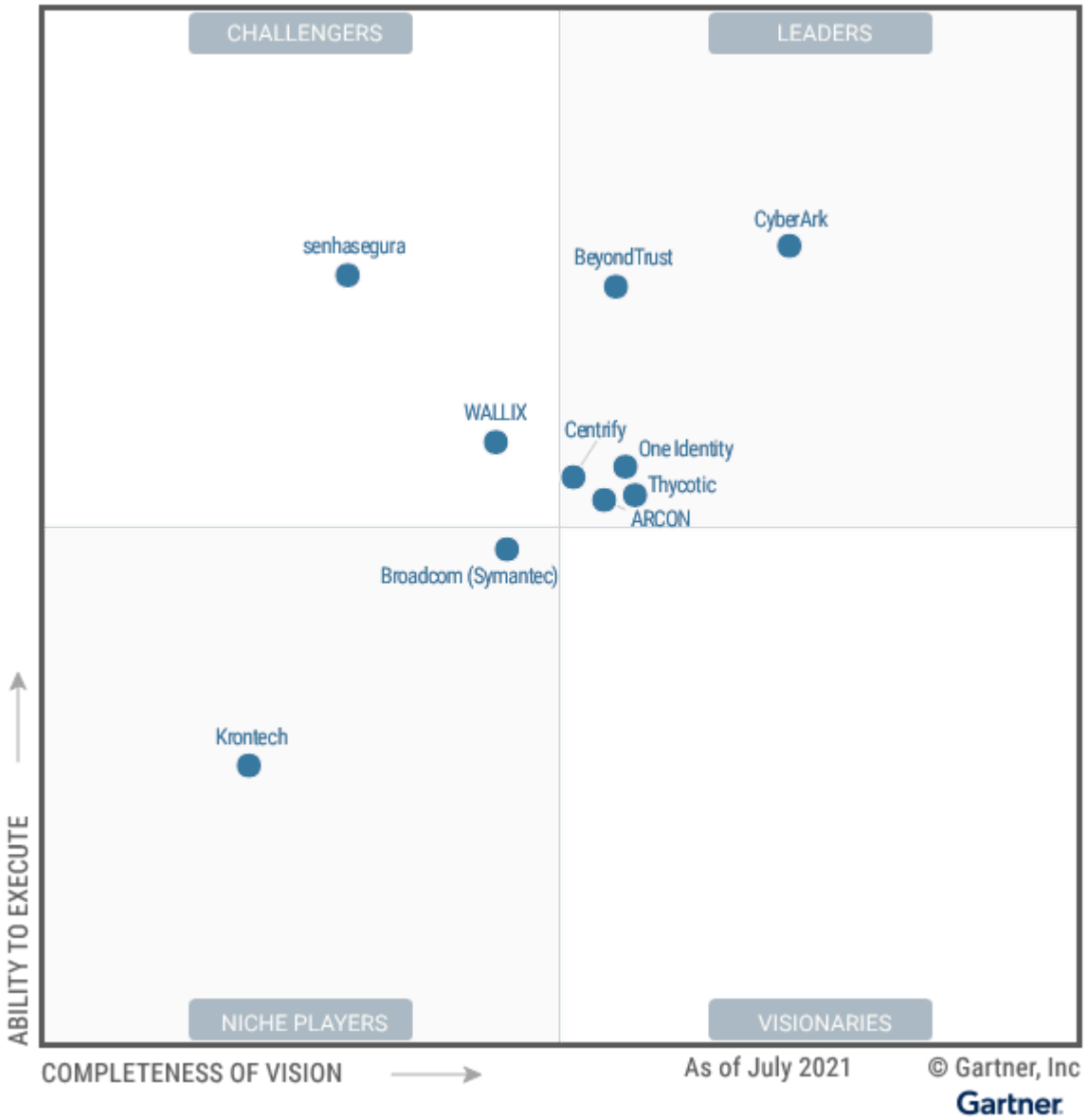
1.5.2. Cenário 2 - Adoção de ferramentas PAM de código aberto.

Não foi encontrada solução que atenda aos requisitos presentes neste documento, no Portal do Software Público Brasileiro (http://softwarepublico.gov.br).

As ferramentas gratuitas disponíveis para download e utilização são limitadas em funcionalidades, relatórios gerados, tipos de ativos suportados e não possuem suporte técnico adequado, além disso, os relatórios fornecidos pelas ferramentas não apresentam rastreabilidade das atividades já realizadas pelos usuários privilegiados nos ativos e sistemas, tornando-as incompatíveis com as necessidades do Tribunal Regional do Trabalho da 12ª Região.

1.5.3. Cenário 3 - Solução consolidada de mercado que garanta segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados.

Pesquisando no site da empresa de consultoria Gartner para encontrar soluções que atendam essa demanda encontramos a seguinte figura:



Assim podemos listar os seguintes fornecedores para efetuar uma pesquisa de preços: CyberArk, SenhaSegura, BeyondTrust, estas ferramentas estão no mesmo nível de habilidade de execução e portanto podem ser consideradas. Um contraponto entre o PAM e outros tipos de tecnologias de segurança é que o PAM abrange vários pontos da cadeia de ataques cibernéticos, fornecendo proteção contra ataques externos e ameaças internas.

O PAM confere vários benefícios principais, incluindo:

- Redução na Infecção e propagação de malwares: muitas variedades de malware precisam de privilégios elevados para sua instalação ou execução. A remoção de privilégios excessivos, como a aplicação de privilégios mínimos em toda a empresa, pode impedir que o malware se estabeleça ou reduza sua disseminação, se isso acontecer.

- Desempenho operacional: restringir privilégios ao intervalo mínimo de processos para executar uma atividade autorizada reduz a chance de problemas de incompatibilidade entre aplicativos ou sistemas, além de ajudar a reduzir o risco de tempo de inatividade.
- Conformidade: ao restringir as atividades privilegiadas que podem ser realizadas, o PAM ajuda a criar um ambiente menos complexo e, portanto, mais amigável para as auditorias.

Além disso, muitos regulamentos de conformidade (incluindo HIPAA, PCI DSS, FDDC, Government Connect, FISMA e SOX) e legislações de proteção de dados (como GDPR, LGPD e CCPA) exigem que as organizações apliquem políticas de acesso com privilégios mínimos para garantir a administração de dados e segurança de sistemas adequadas.

	Característica	**Cenário 1**	**Cenário 2**	**Cenário 3**
01	Fabricante/Fornecedor	TRT12	Software Livres	Diversos/ SAAS
02	Nome solução (modelo)	N/A	Variadas	Variadas
03	Custo efetivo total (CET)	0	Não foram estimados os custos dessa alternativa, uma vez que a mesma se mostra extremamente ineficaz para os propósitos estabelecidos na demanda e de alto custo operacional para o Tribunal	R$ 2.845.589,04
04	Forma de entrega	Construção Própria	Software/ Serviço	Hardware/ Software/ Serviço
05	A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	N/A	N/A	Sim
06	A Solução está disponível no Portal do Software Público Brasileiro?	N/A	N/A	N/A

07	A Solução é um software livre ou software público?	Não	Sim	Não
08	A Solução é aderente às políticas, premissas e especificações técnicas definidas no MNI do Poder Judiciário? (quando houver intercâmbio de informações de processos judiciais)	N/A	N/A	N/A
09	A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	N/A	N/A	N/A
10	A Solução é aderente a orientações, premissas e especificações técnicas e funcionais do Moreq-Jus? (quando houver documentos digitais produzidos pelo Judiciário)	N/A	N/A	N/A

1.6. Justificativa da escolha da solução

Desta forma o cenário 1 fica prejudicado por não termos quadro de pessoal suficiente para este desenvolvimento, o cenário 2 como descrito acima não contempla todas as necessidades de verificação e proteção para garantir um mínimo de segurança além de demandarem uma maior sobrecarga de trabalho das equipes internas.

O cenário 3 atende aos requisitos da contratação, desta forma foram pesquisadas soluções no mercado.

É possível contratar por licitação própria, ou utilizando a Ata de Registro de Preços. O Tribunal Superior do Trabalho realizou Pregão Eletrônico para contratação de Solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), que culminou na Ata de Registro de Preços Nº 058/2021, gerenciada pelo TST.

Como já colocado anteriormente, reforçamos que o Exmo. Ministro Emmanoel Pereira, Presidente do Conselho Superior da Justiça do Trabalho, enviou em 01/06/2022 o Ofício Circular CSJT.SG.SETIC.NUGOV Nº 42/2022 ao Tribunal

Regional do Trabalho da 12ª Região, em que encaminhou, para ciência, o parecer técnico produzido pelo Comitê Técnico de Segurança – CTSeg juntamente com o Comitê Técnico de Infraestrutura – CTInfra, que **recomenda a aquisição dos itens da Ata de Registro de Preços (ARP) PE nº 58/2021 do Tribunal Superior do Trabalho**, marcador 10, tendo em vista a crescente exposição da Justiça do Trabalho a riscos de segurança da informação, e sob à luz da Resolução CNJ nº 396/2021. A referida Ata de Registro de Preços possui, dentre os objetos listados, item que corresponde à demanda que se propõe contratar, objeto deste estudo, os itens 5 a 23, do grupo 2.

Considerando a economia e as vantagens de uma solução para todos os Tribunais, que gera sinergia e favorece a troca de informações, nivelando o conhecimento. Com a utilização desta ata teremos todas as vantagens do Cenário 3, apresentando ainda menor preço. Estando os preços da Ata de Registro de Preços do TST dentro dos valores praticados pelo mercado, esta equipe recomenda a adesão como carona.

1.7. Especificação completa da solução escolhida

A especificação completa da solução escolhida encontra-se nos itens 5 a 23, do grupo 2, conforme Edital do Pregão Nacional PG 058/2021 do TST.

1.8. Relação entre a demanda prevista e a quantidade adquirida

O quantitativo planejado para esta contratação consta no item 1.3 deste documento, que atende as necessidades pretendidas pelo período de 1 ano, pois o ambiente sofre muitas mutações e um levantamento com previsões maiores de 1 ano ocasionaram, via de regra, desperdício de licenciamento. Além do que, os valores para este licenciamento são facilmente absorvíveis pelo orçamento da SETIC, pelo seu baixo custo.

1.9. Considerações sobre os preços.

A busca por processos de aquisição de soluções de proteção de acesso privilegiado se concentrou no Portal de Compras do Governo Federal, onde se identificou os seguintes processos como relevantes, dadas as especificações da

solução pretendida por este Tribunal, as características dos serviços solicitados, as caraterísticas do órgão contratante e o momento da realização do certame.

- PE 99/2021 do Tribunal de Justiça do Poder Judiciário do Estado de Rondônia (TJRO), ocorrido em 13/10/2021, cujo objeto é o Registro de preços, pelo prazo de 12 (doze) meses, para eventual fornecimento de Solução de Segurança para Sistemas Críticos – Monitoramento e Repositório Seguro, visando atender as necessidades do Poder Judiciário do Estado de Rondônia – PJRO;
- PE 37/2021 do Conselho de Justiça Federal (CJF), ocorrido em 20/12/2021, cujo objeto é a Contratação de solução para gerenciamento de acesso privilegiado (privileged access management - PAM) para proteção dos ambientes computacionais do Conselho da Justiça Federal - CJF, contemplando licenciamento perpétuo, serviços de instalação e configuração, transferência de conhecimento, suporte técnico mensal e garantia para 48 (quarenta e oito) meses;
- PE 85/2021 do Tribunal Superior Eleitoral (TSE), ocorrido em 17/12/2021, cujo objeto é Registro de preços para eventual aquisição de Solução de Gerenciamento de Acessos Privilegiados para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos), com capacidade para armazenar, proteger, controlar, gerenciar, auditar e monitorar o acesso privilegiado incluindo serviço de instalação e transferência de conhecimento;
- PE 34/2020 do Tribunal Regional do Trabalho da 8ª Região (TRT8), ocorrido em 01/12/2020, cujo objeto é o Registro de preço para Solução de Proteção e Auditoria do Uso de Credenciais Monitoramento Comportamental e Repositório Seguro, com possibilidade de proteção, monitoramento e alerta baseado em análise comportamental, detecção e resposta a atividade de conta privilegiada, armazenamento de senhas e mitigação de riscos.

Cada processo possui particularidades inerentes da necessidade específica do órgão contratante. Contudo, ressalta-se que **todos visam a aquisição de solução de proteção de acessos privilegiados**, abrangendo garantia, suporte e treinamento. Apesar de o PE 34/2020 do TRT da 8ª Região não estar dentro do prazo estabelecido no Artigo 8º da Portaria PRESI nº 339/2022, por ser esta uma solução bastante específica e recente, consideramos que o preço deverá ser utilizado.

Passa-se abaixo a comparar características das soluções adquiridas em cada certame, considerando **funcionalidades relevantes para a aquisição pretendida** por este Tribunal. Incluiu-se, na última coluna, as características da solução registrada na ARP do TST, para fins de comparação com base nestes parâmetros.

	TJRO	**CJF**	**TSE**	**TRT8**	**TST**

Inclui fornecimento de equipamento?	Não	Sim (1)	Não	Não	Sim (2)
Hardware dedicado ou virtual?	Virtual + Virtual	Dedicado + Virtual	Virtual + Virtual	Virtual + Virtual	Dedicado + Dedicado
Tipo de garantia e suporte	Fornecido pela contratada	Fornecido pela contratada	Fornecido pela contratada	Fornecido pela contratada	Garantia: Fornecido pelo fabricante Suporte: Fornecido pela contratada
Prazo de garantia e suporte	36 meses	48 meses	60 meses	60 meses	12 meses
Quantidade de ativos	4799	1410	14.267	5.099	26.516
Licenciamento de aplicações conteinerizadas	Por *secret*	N/A	N/A	Por cluster	Por aplicação
Quantidade de usuários	150	40	N/A	79	60
Treinamento	Gerenciamento 12 pessoas 40 horas Operação 15 pessoas 24 horas	6 pessoas 20 horas	20 pessoas 20 horas	10 pessoas 40 horas	10 pessoas 30 horas
Solução ofertada	Senha Segura	Senha Segura	BeyondTrust	CyberArk	Senha segura
Empresa contratada	ARVVO Tecnologia, Consultoria e Serviços Ltda	ARVVO Tecnologia, Consultoria e Serviços Ltda	SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA	IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA EIRELI	JAMC Consultoria e Representação de Software LTDA
Valor total (dos pregões)	R$ 1.188.441,66	R$ 900.010,00	R$ 21.860.450,00	R$ 7.199.487,02	R$ 13.116.300,29

O primeiro ponto considerado é a entrega de equipamento pela empresa contratada, o que está de certa forma vinculado ao segundo item, que indica se a proposta vencedora do certame empregava uma solução em máquinas dedicadas ou virtuais (ou ambas).

Considerando que, uma vez instalado, a solução de controle de acesso privilegiado intermediará todo e qualquer acesso a ativo de TIC do Tribunal (inclusive aos sistemas gerenciadores de máquinas virtuais), ela se torna um ativo crítico para a operação de TIC. Desta forma, apesar de apresentar um custo mais elevado, a opção por hardware dedicado para a solução a torna independente dos ativos protegidos. Por exemplo, em uma eventual indisponibilidade do ambiente virtual, caso se tenha uma solução empregando somente nós virtuais, perde-se também o acesso a solução e, por consequência, o acesso a todos os outros ativos fica bastante dificultado (necessário proceder com recuperação emergencial das credenciais a partir das cópias de segurança). Com o exposto, e considerando a experiência da equipe técnica do Tribunal, estabelece-se como requisito a necessidade da solução ser entregue em um cluster de máquinas físicas.

Outro ponto bastante interessante observado na análise dos processos acima listados é quanto ao tipo de garantia e suporte ofertado, e o prazo inicial considerado. Embora não usual, a possibilidade de se obter acesso diretamente ao fabricante da solução para a prestação de serviços de garantia é bastante vantajosa, tendo em vista a independência que se obtém da contratada em eventual dificuldade ou impossibilidade desta na realização dos serviços. Contudo, este tipo de acesso possui um custo maior associado, uma vez que o licitante necessita negociar tal serviço junto ao fabricante e incluí-lo em sua proposta.

A garantia, em geral, é paga de forma integral, juntamente com a aquisição das licenças, enquanto o serviço de suporte é pago mensalmente. Prever um período maior de garantia e suporte na contratação inicial proporciona maior previsibilidade para os licitantes, de maneira que os valores mensais para os serviços de suporte ofertados tendem a se tornarem mais baratos. Por outro lado, a garantia, estendida para grandes períodos, ocasiona um incremento do custo inicial, pois é paga integralmente na aquisição da solução.

Outra variável considerada pelos licitantes na precificação de propostas é a complexidade do escopo de contratação, o que nesta análise se traduz para a quantidade de ativos considerados e a quantidade de usuários. Levando em conta que a empresa contratada apoia e/ou realiza a configuração e manutenção das integrações entre ativos e solução, quanto maior a quantidade e a variedade de ativos, maior tende a ser o preço do serviço de suporte.

Por fim, a proteção e controle de *secrets* em aplicações conteinerizadas. Em geral, este é um item relativamente custoso das propostas, e tende a variar conforme a especificação realizada. Os tipos de cotações encontrados para este item variam desde a precificação individual de cada *secret*, até a proteção do cluster por completo, independentemente do número de aplicações e *secrets*. A forma intermediária se encontra na precificação de cada aplicação coberta, independentemente do número de *secrets*. Cabe mencionar que uma aplicação

pode possuir uma quantidade bastante significativa de *secrets*, o que pode encarecer bastante o custo total, a depender do tipo de cotação adotado.

1.9.1. **Comparação dos processos licitatórios com a Ata do TST**

A comparação item a item dos certames listados acima não é factível, uma vez que a grande maioria dos processos licitatórios para aquisição de solução de controle de acesso privilegiado opta por não individualizar cada item envolvido na solução. Considerando ainda, que cada órgão possui uma realidade e, a abordagem de pacote dificulta ainda mais, uma vez que os quantitativos de ativos, usuários da solução e os prazos de suporte e garantia escolhidos variam consideravelmente de órgão para órgão.

Considerando também que a ARP do TST procurou individualizar cada licença envolvida na solução, e também separou os itens de licença dos itens de garantia, uma abordagem que se identificou para estabelecer comparativos de preços é o de “cotar” os quantitativos estipulados nos processos licitatórios de outros órgãos com os preços registrados na Ata do TST. Contudo, há de se considerar as diversas peculiaridades de cada processo licitatório, em termos de tempo e formato de garantia e suporte, fornecimento de equipamentos, e formato de licenciamento.

1.9.1.1. **Processo TJRO x ARP do TST**

O marcador 12 apresenta a precificação dos itens e quantidades do certame do TJRO considerando os preços praticados na ARP do TST. As principais diferenças entre estes processos estão no fornecimento de equipamentos, no formato de licenciamento de aplicações containerizadas e no formato da garantia, além do prazo de garantia e suporte. No processo do TJRO, não há fornecimento de equipamentos, então os itens referentes ao cluster foram zerados para a comparação. O licenciamento de aplicações containerizadas é feito por *secret* no processo do TJRO, enquanto na ARP do TST é por aplicação. Para fins de comparação, de forma a trazer razoabilidade, tomou-se a razão de 5 *secrets* para cada aplicação.

Ainda, considerando que a precificação da garantia e do suporte para um período de 12 meses difere da precificação para um período de 36 meses, adotou-se um desconto padronizado de 5% sobre o valor total para cada 12 meses considerados. No caso, como o processo do TJRO considera um prazo de garantia e suporte de 36 meses, aplicou-se um desconto de 15% sobre o valor total destes itens.

Explicadas as premissas aplicadas, apresenta-se a comparação do valor global obtido:

	Valores globais (itens comparáveis)	**Diferença**

Processo TJRO	R$ 1.188.441,66	16,83%
ARP TST	R$ 1.388.407,55	

Para este caso, a comparação parece indicar uma não vantajosidade da ARP do TST. Contudo, ainda que algumas premissas tenham sido aplicadas para tentar trazer proporcionalidade à comparação, existem diferenças de especificação que devem ser consideradas. A principal delas, deve-se ressaltar, diz respeito ao tipo de garantia. A ARP do TST possui requisito explícito para que o contratante possa interagir diretamente com o fabricante da solução, caso assim deseje. Tal requisito mitiga o risco de eventuais problemas com a empresa contratada, e considera-se este requisito desejável para a contratação pretendida por este Tribunal. Outro ponto a se argumentar é razão de 5 *secrets* por aplicação, que é razoável para aplicações comuns, mas não para aplicações complexas, como o PJe, onde a quantidade de *secrets* pode chegar a centenas. Na ARP do TST, tal quantitativo não seria relevante, pois o licenciamento é por aplicação, mas em uma abordagem granular, como a do TJRO, o custo para aplicações como o PJe se torna bastante elevado.

1.9.1.2. **Processo CJF x ARP do TST**

O marcador 14 traz a precificação da aquisição feita pelo CJF considerando os preços praticados na ARP do TST. Este processo já possui a aquisição de equipamento, embora seja somente uma unidade (a outra instância é virtual). Como a ARP do TST contempla 2 *appliances* em seu item de cluster, é preciso aplicar uma proporção, de forma a tornar os processos comparáveis. Outro ponto é quanto ao período de garantia e suporte, que neste caso é de 48 meses. Aplicou-se a mesma premissa de desconto de 5% sobre o valor total para cada ano, de forma a tentar compensar as diferenças de precificação de fornecedores nos dois cenários. O processo do CJF não contém previsão para licenciamento de aplicações conteinerizadas, então este item foi excluído da comparação.

	Valores globais (itens comparáveis)	**Diferença**
Processo CJF	R$ 900.010,00	8,96%
ARP TST	R$ 980.652,51	

Novamente, ressalta-se a diferença na garantia da ARP do TST, em que se prevê a interação com o próprio fabricante para execução de serviços específicos. Outro ponto a se ressaltar nesta comparação é que a quantidade de ativos e usuários é significativamente menor neste processo. Os fornecedores em geral consideram a complexidade da instalação pretendida no orçamento de itens de serviço. Logo, é de se esperar que o valor de serviço obtido no processo do CJF seja bem menor do que aquele obtido no certame do TST, em que a quantidade

registrada é significativamente maior e existe uma diversidade de clientes (em função das coparticipações).

1.9.1.3. **ARP do TSE x ARP do TST**

A ARP do TSE apresenta uma iniciativa centralizada de registro de preços para a aquisição de solução de gerenciamento de acessos privilegiados para o próprio órgão e para todos os seus regionais (TREs). A ata possui apenas 2 itens, sendo o primeiro relativo à solução, quantificado por número de ativos, e um segundo de instalação, configuração e transferência de conhecimento, quantificado por número de instalações.

A contratação prevista pela ARP do TSE é de uma solução puramente virtual, em que não se menciona o serviço mensal de suporte, mas somente a garantia sobre os itens entregues. A vigência da contratação e da garantia está estipulada para um período de 60 meses. Como mencionado, a quantificação é por número de ativos, e não há definição quanto ao número de usuários que farão acesso à solução, exceto pela menção de taxa de conversão de 10 usuários para cada 100 ativos, para os casos em que os proponentes ofertem soluções com um modelo de licenciamento baseado em usuários. Apesar da ARP identificar somente o quantitativo total de ativos solicitados, estão presentes no Edital do certame, mais especificamente em um anexo do Termo de Referência, os quantitativos de servidores (físicos e virtuais), instância de banco de dados, aplicações com senha *hardcoded* e ativos de rede para cada regional. Desta forma, é possível calcular os quantitativos totais de ativos de cada categoria e fazer uma cotação com os preços da Ata do TST, para comparação. Em linhas gerais, utilizou-se do desconto de 5% por ano de contrato no valor total calculado para cada item de garantia, considerando que a precificação do fornecedor é influenciada pela vigência estipulada para o contrato.

	Valores globais (itens comparáveis)	**Diferença**
ARP TSE	R$ 21.860.450,00	-36,29%
ARP TST	R$ 13.927.465,44	

Percebe-se que a ARP do TST possui grande vantajosidade financeira sobre o valor total da ARP do TSE. Além disso, é importante ressaltar que, além do preço, a ARP do TST também possui outras vantagens. Conforme já mencionado, o processo do TSE prevê um serviço de suporte simplificado, de forma integrada à garantia, fornecido pela própria contratada, em um regime 8x5 (oito horas por dia, cinco dias por semana), durante horário comercial, o que difere sobremaneira dos itens de garantia da ARP do TST, que prevêm inclusive o acionamento do contratante ao fabricante, e do item de serviço de suporte técnico especializado. Na ARP do TSE também não está prevista a instalação em *appliance* físico, somente

em virtual, o que impossibilita uma configuração físico x físico e físico x virtual para alta disponibilidade, como já indicado de interesse para este Tribunal.

1.9.1.4. **Processo do TRT8 x ARP do TST**

O processo do TRT8 considera um período de 60 meses de vigência para a aquisição de solução de proteção e auditoria de acessos privilegiados, sendo esta provida por meio de licenciamento perpétuo, e com *appliances* virtuais. Os itens estão divididos conforme o objeto coberto pelas licenças (usuários, servidores, cluster de aplicações e estações de trabalho). Também há item de treinamento e item de suporte técnico especializado. Um diferencial a ressaltar deste certame é a forma adotada para o licenciamento de aplicações conteinerizadas. Ao invés de apresentar uma abordagem individual (por aplicação ou por *secret*), o órgão optou por licenciar os clusters de aplicações, sem definir a quantidade de aplicações.

Como nos demais certames, há um anexo do Termo de Referência que discrimina os ativos do ambiente do órgão que devem ser cobertos pela solução. Logo, é possível também utilizar estes quantitativos para cotar sua aquisição por meio da ARP do TST, de forma a possibilitar uma comparação entre os valores globais. Sobre os quantitativos, cumpre informar que se considerou o número majorado em 50%, dado o requisito do Termo de Referência daquele órgão de que a solução deve ser capaz de cobrir um acréscimo de até 50% no número de ativos, em decorrência do longo tempo de vigência do contrato. Outro ponto a se mencionar é que, pela diferença no formato de licenciamento de aplicações, adotou-se como premissa um quantitativo de 60 aplicações por cluster licenciado, totalizando 120 aplicações, tal como o Termo de Referência daquele órgão indicou ser o quantitativo. Não há também, no certame, menção à proteção de instâncias de bancos de dados. Para fins de comparação, tomou-se o quantitativo de 120 instâncias (a quantidade de aplicações) para realizar a cotação e possibilitar a comparação. Menciona-se também que a solução vencedora do certame é puramente virtual, e portanto, foram zerados os itens referentes ao fornecimento de cluster por meio de *appliances* físicos.

Por fim, ressalta-se que não se localizou dentre os itens do processo do TRT8 aqueles referentes ao licenciamento de ativos de infraestrutura de rede, ainda que estes estejam indicados no anexo que descreve o ambiente a ser protegido. De qualquer forma, o quantitativo de ativos de infraestrutura de rede foi considerado na cotação com a ARP do TST, acrescido de 50%. Todo o descritivo do cálculo realizado está presente no Anexo IV deste estudo.

	Valores globais (itens comparáveis)	**Diferença**
Processo TRT-8	R$ 7.679.418,14	-63,83%
ARP TST	R$ 2.777.809,90	

1.10 Avaliação das necessidades de adequação do ambiente para viabilizar a execução contratual.

Item	Característica	O que precisa ser feito	Responsável
01	Infraestrutura tecnológica (equipamentos, redes, link, etc..)	Os equipamentos serão instalados no datacenter principal do TRT12	
02	Infraestrutura elétrica	Não há necessidade de adequação da infraestrutura elétrica	
03	Logística de implantação	Não haverá necessidade de deslocamento da equipe da SEGINFO.	Equipe da SEGINFO
04	Espaço Físico	Nenhum dos equipamentos previstos na demanda necessitarão de adequação do espaço físico para seu funcionamento.	
05	Mobiliário	Não há necessidade de adequação do mobiliário	
06	Impacto ambiental	Não haverá impacto ambiental.	
07	Liberação de acesso	Permissões de acesso a funcionários da contratada para fazer a instalação nas dependências do tribunal.	Equipe da SEGINFO
08	Outros	Não há conhecimento de outras necessidades de adequação além das já comentadas	

1.11. Disponibilidade Orçamentária

Demanda prevista nos itens 15904, 15905 e 15906 do PAC. Os recursos previstos para viabilizar a execução contratual serão descentralizados pelo CSJT.

Valor estimado para 2022 (que garantirá a sustentação das licenças até 2023) é de R$ 1.161.314,25, sendo:

- Custeio - GND3: R$ 109.260,00
- Investimento - GND4: R$ 1.052.054,25

2. Capítulo II - SUSTENTAÇÃO DO CONTRATO

2.1. Recursos Necessários à Continuidade do Negócio Durante e Após a Execução do Contrato

2.1.1. Recursos Materiais

2.1.1.1. Recurso 1: Espaço em datacenter climatizado para alocação dos servidores adquiridos;

- Ação para Obtenção do Recurso: Recurso já está disponível;

- Responsável: Responsável pela área de Infraestrutura de TIC.

2.1.2. Recursos Humanos

Os recursos humanos para viabilizar o gerenciamento e fiscalização da solução serão os servidores do quadro permanente do TRT12 lotados no Serviço de Infraestrutura de TIC (SEINFRA) e Divisão de Segurança da Informação e Proteção de Dados (SEGINFO). Já a equipe de técnicos especialistas necessários para instalação, suporte e treinamento da solução são de responsabilidade da contratada.

2.2. Estratégia de Continuidade Contratual

Evento 1: Interrupção contratual por problemas com fornecedores antes da entrega/instalação dos produtos.

Ação de Contingência 1: Informar à Administração do Tribunal para aplicação das sanções previstas.

Responsável: Gestor do contrato.

2.3. Ações de transição e encerramento contratual

2.3.1. Entrega das versões finais dos produtos

A CONTRATADA deverá entregar ao CONTRATANTE todos os relatórios e quaisquer produtos gerados ao longo da execução contratual.

2.3.2. Transferência final de conhecimentos

Será realizado na implantação da solução, durante o treinamento.

2.3.3. Devolução de recursos materiais

Não é aplicável.

2.3.4. Revogação de perfis de acesso

Todos os eventuais acessos criados para os colaboradores da contratada devem ser formalmente solicitados com descrição detalhada das funções que os trabalhadores executarão. Após o término das atividades, o Tribunal revogará todos os acessos utilizados durante o processo de implantação, exceto se mandatório para execução de procedimentos de manutenções preventivas durante a vigência do contrato, o que deve ser formalmente solicitado e detalhado.

2.4. Estratégia de independência

Existem várias soluções no mercado que atendem os requisitos. A solução a ser contratada é proprietária e não customizada. Pode ser fornecida por pelo menos 4 fornecedores diferentes, porém não há integração entre as soluções. Apenas relatórios, guias de implantação, informações do ambiente e os dados armazenados serão propriedade do Tribunal. Sendo assim, caso ao fim do contrato o Tribunal opte por mudar de solução, deverá analisar custos, funcionalidades e poderá fazê-lo.

2.4.1. Formas de transferência do conhecimento.

A empresa contratada deverá fornecer toda documentação técnica do ambiente implantado, assim como das alterações efetuadas durante o período de garantia e suporte, de forma a possibilitar o repasse de conhecimento no caso de

transição contratual, sem perda de informações ou ônus adicional ao Tribunal. Toda e qualquer informação produzida no âmbito da execução do objeto do contrato pela empresa prestadora dos serviços será de propriedade do TRT12 e fica a empresa obrigada a documentar e registrar os produtos, serviços e eventos.

2.4.2. Direitos de Propriedade Intelectual (Lei nº 9.610, de 19 de fevereiro de 1998)

Não há previsão de desenvolvimento de qualquer novo conhecimento, código ou outro tipo de conhecimento que se converta em propriedade intelectual.

2.4.3. Outras formas de minimizar dependência

A equipe de fiscalização técnica se manterá atenta à qualidade das entregas para garantia da independência do fornecedor.

3. Capítulo III - ESTRATÉGIA DA CONTRATAÇÃO

3.1. Natureza do objeto

Trata-se de aquisição de serviço comum, cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado.

3.2. Parcelamento do objeto

Conforme concluído no presente estudo, o contrato prevê fornecedor único, portanto não haverá parcelamento do objeto.

3.3. Modalidade e tipo de licitação (justificativa)

Utilização como Carona da Ata de Registro de Preços PE – 058/2021 gerenciada pelo TST, cujo ETP e Projeto Básico (Termo de referência) constam nos documentos 10 e 11, respectivamente.

A autorização do Órgão Gerenciador consta no documento 18 e da empresa

JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA, vencedora do Registro de Preços consta no documento 19.

3.5. Classificação Orçamentária.

O objeto da contratação possui partes classificadas como GND3 e partes classificadas como GND4.

- Custeio - GND3:
  - Itens 6, 8, 10, 12, 14, 16, 18 e 20 - Garantia do fabricante por período de 12 meses - Valor Total para 2022 R$: 189.147,25;
  - Item 21 - Serviços técnicos profissionais de TIC - R$ 44.900,00;
  - Item 22 - Treinamento técnico da Solução de PAM - 1 unidade, Valor Total: R$ 16.000,00;
  - Item 23 - Servico de Suporte técnico - 6 unidades, Valor Total: R$ 48.360,00 ;
- Investimento - GND4: R$ 862.907,00 - Itens 5, 7, 9, 11, 13, 15, 17 e 19

3.6. Equipe de apoio à contratação

Este papel será desempenhado pela equipe de planejamento da contratação.

3.7. Equipe de gestão da contratação

a) Gestor do Contrato e Fiscal Demandante: Serão indicados nominalmente pelo Diretor da Secretaria demandante. A indicação será efetuada no despacho de aprovação dos Estudos Preliminares e Projeto Básico.

b) Fiscal Técnico: Será indicado nominalmente pelo Diretor da SEGINFO, no despacho de aprovação dos Estudos Preliminares e Projeto Básico.

c) Fiscal Administrativo: Será indicado nominalmente pelo Diretor da Secretaria Administrativa, por despacho ao determinar a abertura de procedimento administrativo.

4. Capítulo IV - ANÁLISE DE RISCOS

4.1. Riscos da Solução contratada não ter sucesso (riscos do produto/serviço)

RISCO 1	Problema físico na Solução de PAM
PROBABILIDADE	Baixa
DANOS E IMPACTO	Em caso de parada da Solução, o impacto será médio, pois todos os serviços e sistemas do TRT12 continuarão disponíveis, porém com maior demora no acesso administrativo.

AÇÕES A SEREM TOMADAS PARA REDUZIR OU ELIMINAR OS RISCOS	**RESPONSÁVEL**
Manter os Data Centers refrigerados, com nobreaks funcionando corretamente e com os demais requisitos de ambiente verificados e corretos.	Secretaria de Tecnologia da Informação
DEFINIÇÃO DAS AÇÕES DE CONTINGÊNCIA A SEREM TOMADAS CASO OS RISCOS DE CONCRETIZEM	**RESPONSÁVEL**
Garantir que o backup da Solução PAM esteja acessível e testado pela Secretaria de Tecnologia da Informação do TRT12.	Secretaria de Tecnologia da Informação

RISCO 2	Falha no software de PAM
PROBABILIDADE	Baixa
DANOS E IMPACTO	Em caso de falha no software de PAM, o impacto será médio, pois todos os serviços e sistemas do TRT12 continuarão disponíveis, porém com maior demora no acesso administrativo.

AÇÕES A SEREM TOMADAS PARA REDUZIR OU ELIMINAR OS RISCOS	**RESPONSÁVEL**
Não atualizar o software de PAM pouco tempo antes do término do contrato de suporte.	Secretaria de Tecnologia da Informação
DEFINIÇÃO DAS AÇÕES DE CONTINGÊNCIA A SEREM TOMADAS CASO OS RISCOS DE CONCRETIZEM	**RESPONSÁVEL**
Capacitar a equipe de Infraestrutura para ter conhecimentos técnicos avançados, de forma que possam sanar eventuais falhas no software de PAM.	Secretaria de Tecnologia da Informação

5. Capítulo V - ASSINATURAS

Florianópolis, 16 de setembro de 2022

Equipe de Planejamento da Contratação

Integrante Demandante:

Nome: Valdir Luiz da Cunha
Cargo: Diretor da Secretaria da Tecnologia da Informação e Comunicação - SETIC
E-mail: valdir.cunha@trt12.jus.br

Integrante técnico:

Nome: Arthur Fernando Dellagiustina Lago
Cargo: Diretor da Divisão de Segurança da Informação e Proteção de Dados - SEGINFO
E-mail: arthur.lago@trt12.jus.br

Substituto:

Nome: Marcus Vinicius Mattos
Cargo: Técnico Judiciário
Email: marcus.mattos@trt12.jus.br

Integrantes administrativos:

Nome: Sérgio Moritz
Cargo: Analista Judiciário
E-mail: sergio.moritz@trt12.jus.br

Substitutos:

Nome: Edson de Amorim
Cargo: Técnico Judiciário
Email: edson.amorim@trt12.jus.br