TRT-24ª REGIÃO
Mato Grosso do Sul

GESLAINE PEREZ MAQUERTE
PEDRO VILLEGAS ARAUJO
ALEXANDRE ROSA CAMY
CAMILO GAMA DA SILVA
ERICK TAKA HASHI
PAULO SERGIO PETRI
FÁBIO NOGUEIRA DA SILVA
GLEISON AMARAL DOS SANTOS

ESTUDO TÉCNICO PRELIMINAR

PROAD N° 19874/2022

AQUISIÇÃO DE SOLUÇÕES DE SEGURANÇA, AUDITORIA E PREVENÇÃO DE AMEAÇAS À BASE DE DADOS NÃO ESTRUTURADOS

PARA CUMPRIMENTO DA RESOLUÇÃO CNJ 182/2013 E PORTARIA TRT/GP/DG 74/2017
* ARTIGOS REFERENCIADOS NO TEXTO SERÃO REFERENTES À RESOLUÇÃO CNJ
** ESTÃO IDENTIFICADOS OS ITENS DO PLANO DE TRABALHO CONFORME PORTARIA TRT24

I. IDENTIFICAÇÃO DA DEMANDA

(Art. 12, § 1º, 'I' e Art. 14, I e IV)

1 DEMANDANTE

Área demandante: Secretaria de Tecnologia da Informação e Comunicações

Responsável: Alexandre Rosa Camy

E-mail: acamy@trt24.jus.br

Telefone/ramal: (67) 3316-1720

2 OBJETIVOS DA CONTRATAÇÃO

(** Plano de Trabalho – item 1)

Objetivo geral:

Garantir um ambiente mais seguro para a plataforma de serviços de TI, através da aquisição, implantação e uso de ferramentas avançadas de segurança da informação.

Objetivos específicos:

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

Obter suporte técnico, atualização e monitoramento necessários para os softwares da solução evitando aumento de demanda para a equipe da SETIC que possui defasagem de quantitativos na equipe técnica, o que dificulta inclusive na aquisição de conhecimentos para soluções pertencentes a um mercado abrangente, volátil, e no presente tema ainda bastante recente.

3 OBJETO DA CONTRATAÇÃO

O objeto a ser contratado será composto de:

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

4 PROCESSO DE TRABALHO PARA O ESTUDO DA SOLUÇÃO

Este documento consiste de estudos preliminares necessários para assegurar a viabilidade da contratação, mensurar os riscos, determinar uma estratégia para a contratação, fornecer subsídios para a elaboração do Termo de Referência, bem como definir um plano de sustentação para a solução contratada.

Para o presente estudo foram realizadas as seguintes atividades:

a) Definição de demanda no Comitê de Governança de TIC;

b) Envio de solicitação de orçamento ao CSJT (Documento de Demanda Orçamentária);

c) Elaboração inicial de Estudo Técnico Preliminar pela equipe da SETIC;

d) Validação da adesão com a empresa ganhadora da Ata de Registro de Preços TST PE – 058/2021;

e) Confirmação do recebimento de crédito orçamentário;

f) Elaboração de planilha de preços e finalização dos estudos preliminares com indicação da contratação;

g) Validação dos Riscos Contratuais (para ver se há algo mais além dos riscos apontados no projeto "20220501 - Implantar Solução de Segurança e PAM", com o andamento lançado no PROAD 20235/2022);

h) Encaminhamento para providências da administração.

5 NECESSIDADE DA CONTRATAÇÃO E IDENTIFICAÇÃO DOS BENEFÍCIOS

(Art. 14,IV,"c")
(** Plano de Trabalho – item 4)

O cenário nos órgãos do Poder Judiciário com o aumento de Incidentes Cibernéticos direcionados ao Governo criou uma série de recomendações para que eventos análogos não ocorressem em outros Órgãos. O CNJ também encaminhou recomendações similares a todos os Tribunais por meio da Portaria 162/2021.

A continuidade de negócio do TRT24, como de qualquer organização, requer o investimento em ativos e serviços de TI sob pena de inviabilizar a execução da missão do órgão em caso de falha técnica.

Garantir um ambiente seguro no atual cenário tecnológico é essencial.

Para atender às recomendações do CNJ e da norma ABNT NBR ISO/IEC 27001:2013, faz-se necessário a ampliação das ferramentas hoje disponibilizadas à equipe de TI do Tribunal, especialmente nos campos de auditoria comportamental de usuários para prevenção e mitigação de ataques danosos com *ransomwares,* que em geral são ataques que envolvem a criptografia de dados estruturados, e solicitações de resgate para a liberação das informações.

Os resgates apontados não garantem a recuperação dos dados. Desse modo, estamos falando de uma perda de informações sem possibilidade recuperação.

Como esses ataques muitas vezes conseguem, antes que haja tempo de perceber a ocorrência dentro da organização, criptografar arquivos que seguem para o backup, pode representar a perda definitiva dos dados.

No atual ambiente de trabalho envolvendo o Sistema PJe, estamos falando em uma instituição que presta serviços à sociedade e cuja atividade fim, o processo judicial trabalhista, está internalizado dentro do ambiente tecnológico. Assim, o prejuízo é incalculável, pois envolve os processos de fato, por serem eletrônicos, ou seja, não haver correspondente físico para recuperação.

Para promover um ambiente minimamente seguro e que, em caso de ataque cibernético, ofereça garantias de recuperação é necessário investir em uma infraestrutura de soluções tecnológicas de apoio. As ferramentas abrangem desde soluções de proteção (como, por exemplo, soluções de firewall) que evitam o ataque, soluções de backup (quente ou frio) que permitam a recuperação das atividades após um incidente de segurança, até soluções de monitoramento para detecção mais rápida de intrusos no ambiente cibernético.

Essa contratação envolve duas (2) frentes de proteção. Na primeira frente de proteção as ferramentas devem abranger a proteção de dados não estruturados, a partir dos sistemas de arquivos, e-mails em conjunto com os controladores de domínio e das estações de trabalho (*endpoints*). A segunda deve abranger proteção de usuários administradores, que são os que possuem acessos mais amplos, chamados de usuários privilegiados.

Conforme parecer técnico emitido pelo CTINFRA/CTSEG (PARECER CTINFRA/CTSEG N. 1/2022, documento 2 do processo original juntado no documento 4) a solução recomendada para contratação por meio da Ata de Registro de Preços PE 58/2021 do Tribunal Superior do Trabalho (TST), apresenta as seguintes vantagens:

a) Proteção de Infraestruturas Críticas de TIC recomendada pela Portaria CNJ 162/2021;

b) Cria condições para gestão, monitoramento, proteção e controle das contas de acesso privilegiado (em especial as contas de administradores técnicos da SETIC), que apresentam mais risco, e que são alvos pela possibilidade de domínio do ambiente tecnológico, agravando a amplitude do ataque cibernético;

c) Monitoramento para detecção de problemas nas senhas privilegiadas (contas antigas, sem trocas de senha, contas inativas sem uso, dentre outros);

d) Monitoramento de estações de trabalho, demarcando estações com alto risco de ser uma janela de invasão cibernética, por terem softwares defasados, desativados, ou sem itens de segurança da informação (antivírus e firewall);

e) Monitoramento de dados não estruturados, com detecção imediata de arquivos criptografados e usuários comprometidos (senhas vazadas), permitindo que o ataque seja barrado antes da disseminação (os casos mais recentes indicam que o atacante ficou dentro da rede de dados por meses).

6 ALINHAMENTO ESTRATÉGICO DA CONTRATAÇÃO

(Art. 14, IV, "b")

6.1 Planejamento diretor de TIC do TRT24 2021-2022

Planejamento: PDTIC 2021-2022

Categoria: iGovTic JUD

Objetivo: Aumentar o nível de maturidade em relação ao índice nacional apurado pelo CNJ.

Indicador: Índice de Governança de TIC (iGovTIC-JUD)

Iniciativa: Disponibilizar Soluções de Segurança que atendam a Portaria CNJ 162/2021.

Resultados: Monitoramento centralizado do comportamento de rede de dados, inclusive estações, no que tange aos dados não estruturados que trafegam na rede. Gestão segura das senhas de acesso privilegiado.

II. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

(Art. 12, § 1º, 'I' e Art. 14, I)

1. MOTIVAÇÃO DA CONTRATAÇÃO

Em nove de novembro de 2020 o Superior Tribunal de Justiça foi alvo do maior ataque cibernético já realizado a um órgão do Governo Brasileiro. Foram mais de sete (7) dias com todos os sistemas indisponíveis. O foco do ataque foi a infraestrutura do Datacenter do STJ. Ataque com consequência semelhante foi realizado no Tribunal de Justiça do Rio Grande do Sul, TJ/RS, no final de abril de 2021, mas o foco, dessa vez, foi nas mais de 12.000 estações de trabalho do TJ/RS, conhecidos como "*endpoints*". Focos diferentes, estragos semelhantes, modo de operação similar: ataques do tipo *ransomware* que exploram vulnerabilidades existentes.

Ataques similares ocorrem em todo o mundo também em empresas privadas, como visto em algumas chamadas na imprensa, para citar alguns:

- Ataque de *ransomware* leva ao fechamento do maior oleoduto dos EUA - 7 de maio de 2021;
- JBS sofre ataque *hacker* e suspende operações em vários países – 31 de maior de 2021;
- Lojas Renner reestabelece *site* e sistema de pagamentos após ataque de *ransomware* – 19 de agosto de 2021.

O cenário é tão crítico que o CTIR GOV, Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, criou uma série de recomendações para que eventos análogos não ocorressem em outros Órgãos. O CNJ também encaminhou recomendações similares a todos os Tribunais.

Durante a ataque ocorrido ao STJ, foram realizadas, no âmbito do Tribunal, ações que reduzissem as eventuais vulnerabilidades do seu ambiente computacional. No entanto, o questionamento mais crítico que ainda permanecia sem resposta pelas atuais ferramentas de monitoramento era a identificação da existência de contas de usuários comprometidas no ambiente.

A identificação de usuários comprometidos, sejam eles comuns ou privilegiados, requer o uso de ferramentas capazes de avaliar o comportamento do usuário, normalmente através de *Machine Learning*. Um usuário comprometido é, normalmente, a porta de entrada para ataques como os citados. Por essa razão a capacidade de conhecer o comportamento de cada usuário da rede e de verificar se esses estão ou não comprometidos, é recurso essencial atualmente, onde há um crescente ataque às instituições e empresas.

Os ataques como os de *ransomware*, onde dados são sequestrados e há um pedido de resgate para sua recuperação, ocorrem em dados não estruturados ou semiestruturados. Assim, a capacidade de análise comportamental do usuário deve estar em linha com a análise do uso de dados estruturados ou semiestruturados, requerendo, assim que o uso de ferramentas e soluções adequadas que ofereçam segurança e eficiência a partir de um ambiente adequado à sua destinação.

Um problema recorrente e que acarreta brechas que podem ser exploradas em ataques cibernéticos são usuários que deveriam deixar de ter acesso a determinado conteúdo, seja por mudança de unidade, de atribuição ou mesmo por questões administrativas e, pelo fato de o gestor não solicitar a

remoção desse acesso (por equívoco ou esquecimento), esse usuário continua com o acesso e pode ser explorado por hackers.

São desafios que hoje são enfrentados pela equipe técnica de TI do Tribunal:

- Identificar/classificar conteúdo sensível;
- Identificar os proprietários dos dados;
- Controle e auditoria dos eventos (quem acessou o que e como);
- Excesso de demanda com falta de mão de obra para executar as tarefas;
- Assegurar que as autorizações são baseadas em necessidades de negócios e seguem o princípio do privilégio mínimo e segregação de funções.

Segundo o instituto de pesquisas técnicas e análises de tendências de TI – o Gartner Group, cerca de 80% dos dados estratégicos está armazenado em base de dados não estruturadas ou semiestruturadas. Toda essa informação está distribuída em pastas (departamentais, setoriais e individuais) acessadas pelos diversos usuários da rede e gerenciadas por sistemas operacionais que proporcionam registro de eventos (logs) custoso e pouquíssimo informativo e que não proporcionam a devida granularidade para pesquisas de auditorias referentes a quem, quando, onde e como um dado é utilizado.

Desta forma, na situação atual, quando necessário o monitoramento de acessos aos dados armazenados, gerenciamento e auditoria do repositório de usuários e ações proativas em casos de incidentes de segurança cibernética, ataques de *malwares* ou até identificação de acessos indevidos de usuários internos mal intencionados, a equipe técnica do Tribunal não dispõem de ferramental que possa avaliar todo o clico de uso dos recursos computacionais e se esse ciclo, ou comportamento, é adequado ou anormal.

Esse ciclo não se restringe ao acesso ao controlador de domínio e aos servidores de arquivos, mas também às estações de trabalho que são a principal porta de entrada para ataques. Por muitas vezes são exploradas vulnerabilidades nas estações (*endpoints*), se aproveitando de usuários locais para fazer ataques do tipo Leste-Oeste, onde o comprometimento de um *endpoint* pode afetar todos os demais que possuem, normalmente, as mesmas configurações.

Com o avanço da ousadia e das técnicas utilizadas pelos hackers para causarem prejuízos às instituições, há a necessidade de aprimorar os processos e ampliar as medidas preventivas e proativas de segurança da informação. Nesse sentido, o CNJ publicou a Resolução nº 396, de 7 de junho de 2021, que Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Em prosseguimento, publicou a Portaria nº 162, de 10 de junho de 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).

Entre os documentos aprovados pela Resolução 396, está o Manual de Referência de Proteção de Infraestruturas Críticas de TIC. Nele são definidos 3 (três) grupos de organizações conforme:

Grupo	Sugestão de ordem de implantação
Grupo 1	Organizações com nível limitado de recursos disponíveis e pouca experiência em segurança cibernética.
Grupo 2	Organizações com nível moderado de recursos disponíveis e experiência média em segurança cibernética.
Grupo 3	Organizações com nível elevado de recursos disponíveis e alta experiência em segurança cibernética.

O manual é baseado em um conjunto de boas práticas denominado CIS Controls, versão 7.1. Conforme o manual, por meio da adoção dos controles propostos por ele, estima-se que cerca de 85% (oitenta e cinco por cento) dos principais ataques praticados quando do lançamento do CIS versão 7.1 poderiam ser evitados (item 7.3 da portaria CNJ 162/2020.

Entre as recomendações propostas, existem aquelas que já estão implantadas, as que necessitam de alteração em processos ou ativos para serem implantadas, além daquelas que necessitam da aquisição de algum tipo de ferramenta especializada para dar suporte à sua implementação.

O levantamento do ETP do TST foi feito antes do lançamento da versão 8 do CIS, motivo pelo qual ainda se encontra com a redação da versão anterior do CIS (versão 7). A análise de riscos realizada pelo TRT24 - PROAD 21261/2022 – já foi feita considerando-se os controles da mais nova versão do CIS (versão 8). Sendo assim, a tabela abaixo foi extraída a partir do levantamento e tratamento de riscos do TRT24 e reflete a situação atual dos controles CIS v8, demonstrando a necessidade ou não de aquisição de ferramentas especializadas, onde "NI" significa Não Implantada e "I" significa Implantado:

ID	Requisito	Controle	Situação atual*	Necessário aquisição?
Inventário e controle de ativos organizacionais				
1.1	Estabelecer e manter um inventário detalhado de ativos corporativos;	Identificar	I	Não
1.2	Endereçar ativos não autorizados;	Responder	NI	Sim
1.3	Usar uma ferramenta de descoberta ativa;	Detectar	I	Sim
1.4	Usar o Dynamic Host Configuration Protocol (DHCP) para atualizar o inventário de ativos corporativos;	Identificar	NI	Sim
1.5	Usar uma ferramenta de descoberta passiva;	Detectar	I	Sim
Inventário e controle de ativos de software				
2.1	Estabelecer e manter um inventário de software	Identificar	NI	Não
2.2	Assegurar que o software autorizado seja atualmente suportado	Identificar	NI	Sim
2.3	Endereçar o software não autorizado	Responder	NI	Sim
2.4	Utilizar ferramentas automatizadas de inventário de software	Detectar	I	Sim
2.5	Lista de permissões de Software autorizado	Proteger	NI	Não
2.6	Lista de permissões de bibliotecas autorizadas	Proteger	NI	Não
2.7	Lista de permissões de Scripts autorizados	Proteger	NI	Não
Proteção de dados				
3.1	Estabelecer e manter um processo de gestão de dados	Identificar	NI	Não
3.2	Estabelecer e manter um inventário de dados	Identificar	NI	Não
3.3	Configurar listas de controle de acesso a dados	Proteger	NI	Não
3.4	Aplicar retenção de dados	Proteger	NI	Sim
3.5	Descartar dados com segurança	Proteger	NI	Não
3.6	Criptografar dados em dispositivos de usuário final	Proteger	NI	Não
3.7	Estabelecer e manter um esquema de classificação de dados	Identificar	NI	Sim
3.8	Documentar Fluxos de Dados	Identificar	NI	Sim
3.9	Criptografar dados em mídia removível	Proteger	NI	Não

ID	Requisito	Controle	Situação atual*	Necessário aquisição?
3.10	Criptografar dados sensíveis em trânsito	Proteger	I	Não
3.11	Criptografar dados sensíveis em repouso	Proteger	NI	Não
3.12	Segmentar o processamento e o armazenamento de dados com base na sensibilidade	Proteger	NI	Não
3.13	Implantar uma solução de prevenção contra perda de dados	Proteger	NI	Sim
3.14	Registrar o acesso a dados sensíveis	Detectar	NI	Não
Configuração segura de ativos corporativos e softwares				
4.1	Estabelecer e manter um processo de configuração segura	Proteger	NI	Não
4.2	Estabelecer e Manter um Processo de Configuração Segura para a Infraestrutura de Rede	Proteger	NI	Não
4.3	Configurar o bloqueio automático de sessão nos ativos corporativos	Proteger	NI	Não
4.4	Implementar e gerenciar um firewall nos servidores	Proteger		Não
4.5	Implementar e gerenciar um firewall nos dispositivos de usuário final	Proteger	I	Não
4.6	Gerenciar com segurança os ativos e softwares corporativos	Proteger	I	Não
4.7	Gerenciar contas padrão nos ativos e softwares corporativos	Proteger	NI	Não
4.8	Desinstalar ou desativar serviços desnecessários nos ativos e softwares corporativos	Proteger	NI	Não
4.9	Configurar servidores DNS confiáveis nos ativos corporativos	Proteger	I	Não
4.10	Impor o bloqueio automático de dispositivos nos dispositivos portáteis do usuário final	Responder	NI	Não
4.11	Impor a capacidade de limpeza remota nos dispositivos portáteis do usuário final	Proteger	NI	Sim
4.12	Separar os Espaços de Trabalho Corporativos nos dispositivos móveis	Proteger	NI	Não
Gestão de contas				
5.1	Estabelecer e manter um inventário de contas	Identificar	NI	Não
5.2	Usar senhas exclusivas	Proteger	NI	Não
5.3	Desabilitar contas inativas	Responder	NI	Não
5.4	Restringir privilégios de administrador a contas de Administrador dedicadas	Proteger	NI	Não
5.5	Estabelecer e manter um inventário de contas de serviço	Identificar	NI	Sim
5.6	Centralizar a gestão de contas	Proteger	NI	Sim
Gestão de controle de acessos				
6.1	Estabelecer um Processo de Concessão de Acesso		NI	Não
6.2	Estabelecer um Processo de Revogação de Acesso		NI	Não
6.3	Exigir MFA para aplicações expostas externamente		NI	Não
6.4	Exigir MFA para acesso remoto à rede		I	Não
6.5	Exigir MFA para acesso administrativo		NI	Não
6.6	Estabelecer e manter um inventário de sistemas de autenticação e autorização		NI	Não
6.7	Centralizar o controle de acesso		NI	Sim

ID	Requisito	Controle	Situação atual*	Necessário aquisição?
6.8	Definir e manter o controle de acesso baseado em funções		NI	Não
Gestão contínua de vulnerabilidades				
7.1	Estabelecer e manter um processo de gestão de vulnerabilidade	Proteger		Não
7.2	Estabelecer e manter um processo de remediação	Responder		Não
7.3	Executar a gestão automatizada de patches do sistema operacional	Proteger	NI	Sim
7.4	Executar a gestão automatizada de patches de aplicações	Proteger	NI	Sim
7.5	Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos internos	Identificar	NI	Sim
7.6	Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos expostos externamente	Identificar	NI	Sim
7.7	Corrigir vulnerabilidades detectadas	Responder	I	Não
Gestão de registros de auditoria				
8.1	Estabelecer e manter um processo de gestão de log de auditoria	Proteger	NI	Não
8.2	Coletar logs de auditoria	Detectar	I	Não
8.3	Garantir o armazenamento adequado do registro de auditoria	Proteger	NI	Sim
8.4	Padronizar a sincronização de tempo	Proteger	I	Não
8.5	Coletar logs de auditoria detalhados	Detectar	NI	Não
8.6	Coletar logs de auditoria de consulta DNS	Detectar	NI	Não
8.7	Coletar logs de auditoria de requisição de URL	Detectar	NI	Não
8.8	Coletar logs de auditoria de linha de comando	Detectar	NI	Não
8.9	Centralizar os logs de auditoria	Detectar	NI	Não
8.10	Reter os logs de auditoria	Proteger	NI	Não
8.11	Conduzir revisões de log de auditoria	Detectar	NI	Sim
8.12	Colete logs do provedor de serviços	Detectar	NI	Não
Proteção de e-mail e navegador web				
9.1	Garantir o uso apenas de navegadores e clientes de e-mail suportados plenamente	Proteger	NI	Não
9.2	Usar serviços de filtragem de DNS	Proteger	I	Sim
9.3	Manter e impor filtros de URL baseados em rede	Proteger	I	Sim
9.4	Restringir extensões de cliente de e-mail e navegador desnecessárias ou não autorizadas	Proteger	NI	Sim
9.5	Implementar o DMARC	Proteger	I	Não
9.6	Bloquear tipos de arquivo desnecessários	Proteger	I	Sim
9.7	Implantar e manter proteções *antimalware* de servidor de e-mail	Proteger	I	Sim
Defesas contra *malware*				
10.1	Instalar e manter um software *antimalware*	Proteger	NI	Sim
10.2	Configurar atualizações automáticas de assinatura *antimalware*	Proteger	I	Sim
10.3	Desabilitar a execução e reprodução automática para mídias removíveis	Proteger	NI	Não
10.4	Configurar a varredura *antimalware* automática de mídia removivel	Detectar	I	Sim
10.5	Habilitar recursos anti-exploração	Proteger	I	Sim
10.6	Gerenciar o software *antimalware* de maneira centralizada	Proteger	I	Sim
10.7	Usar software *antimalware* baseado em comportamento	Detectar	I	Sim
Recuperação de dados				
11.1	Estabelecer e manter um processo de recuperação de dados	Recuperar	I	Não
11.2	Executar backups automatizados	Recuperar	I	Sim

ID	Requisito	Controle	Situação atual*	Necessário aquisição?
11.3	Proteger os dados de recuperação	Proteger	NI	Sim
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	Recuperar	NI	Não
11.5	Testar os dados de recuperação	Recuperar	NI	Não

Parte das recomendações que constam no Manual de Referência de Proteção de Infraestruturas Críticas de TIC necessitam de aquisição de ferramentas para serem atendidas.

No mesmo contexto de segurança da informação, a norma ABNT NBR ISO/IEC 27001:2013 trata de recomendações práticas para a gestão da segurança da informação, onde destacamos:

> A NBR ISO/IEC 27002:2013, item 10.10, assim determina:
> "10.10 - Monitoramento"
> Objetivo: Detectar atividades não autorizadas de processamento de informação.
> Convém que os sistemas sejam monitorados e eventos de segurança da informação sejam registrados.
> Convém que registros (log) de operador e registros (log) de falhas sejam utilizados para assegurar que os problemas de sistemas de informação sejam identificados.
> Convém que as organizações estejam de acordo com todos os requisitos legais relevantes aplicáveis para suas atividades de registro e monitoramento.
> Convém que o monitoramento do sistema seja utilizado para checar a eficácia dos controles adotados e para verificar a conformidade com o modelo de política de acesso."
> Ainda com relação à preservação dos logs, continua a referida norma técnica:
> "10.10.1 - Registros de auditoria
> Controle: Convém que registro (log) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.
> Diretrizes para implementação:
> Convém que os registros (log) de auditoria incluam, quando relevante:
> a) Identificação dos usuários;
> b) Datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (log-on) e saída (log-off) no sistema;
> c) Identificação do terminal ou, quando possível, a sua localização;
> d) Registro das tentativas de acesso ao sistema aceitas e rejeitadas;
> e) Registros das tentativas de acesso a outros recursos e dados aceitos e rejeitados;
> f) Alterações na configuração do sistema;
> g) Uso de privilégios;
> h) Uso de aplicações e utilitários do sistema;
> i) Arquivos acessados e tipo de acesso;
> j) Endereços e protocolos de rede;
> k) Alarmes provocados pelo sistema de controle de acesso;
> l) Ativação e desativação dos sistemas de proteção, tais como sistema de antivírus e sistema de detecção de intrusos."
> Quanto ao monitoramento do uso do sistema (controle de acesso), a Norma recomenda:
> "10.10.2 - Monitoramento do uso do sistema:
> Controle: Convém que sejam estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento sejam analisados criticamente, de forma regular.
> Controle: Convém que a organização esteja de acordo com todos os requisitos legais relevantes, aplicáveis para suas atividades de monitoramento. Convém que as seguintes áreas sejam consideradas;
> a) Acessos autorizados, incluindo detalhes do tipo;
> 1. Identificador do usuário (ID de usuário);
> 2. A data e o horário dos eventos-chave;

3. Tipo do evento;
4. Os arquivos acessados;
5. Os programas ou utilitários utilizados;

b) Todas as operações privilegiadas, tais como:
1. Uso de contas privilegiadas, por exemplo: supervisor, root, administrador;
2. Inicialização e finalização do sistema;
3. A conexão e a desconexão de dispositivos de entrada e saída;

c) Tentativas de acesso não autorizadas, tais como:
1. Ações de usuários com falhas ou rejeitados;
2. Ações envolvendo dados ou outros recursos com falhas rejeitadas;
3. Violação de políticas de acesso e notificações para gateways de rede e firewalls, dentre outros."

E prossegue abordando a proteção e registro de logs:

"10.10.3 - Proteção das informações dos registros (logs):

Controle: Convém que os recursos e informações de registros (log) sejam protegidos contra falsificação e acesso não autorizado.

Convém que os controle implementados objetivem a proteção contra modificações não autorizadas e problemas operacionais com os recursos dos registros (log). Registros de sistema precisam ser protegidos, pois os dados podem ser modificados e excluídos e suas ocorrências podem causar falsa impressão de segurança.

10.10.4 - Registros (log) de administrador e operador.

Controle: Convém que as atividades dos administradores e operadores do sistema sejam registradas.

Convém que esses registros (log) incluam:

a) A hora em que o evento ocorreu (sucesso ou falha);
b) Informações sobre o evento (exemplo: arquivos manuseados) ou falhas (exemplo: erros ocorridos e ações corretivas adotadas);
c) Que conta e que administrador ou operador estava envolvido;
d) Que processo estavam envolvidos."

Para atender às recomendações do CNJ e da norma ABNT NBR ISO/IEC 27001:2013, faz-se necessário a ampliação das ferramentas hoje disponibilizadas à equipe de TI do Tribunal, especialmente nos campos de auditoria comportamental de usuários para prevenção e mitigação de ataques danosos com *ransomwares*. Essas ferramentas devem abranger a proteção dos sistemas de arquivos e e-mails em conjunto com os controladores de domínio, das estações de trabalho (*endpoints*) e dos usuários administradores, que são os que possuem maiores privilégios, chamados de usuários privilegiados.

2. OBJETIVOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

O objetivo principal é aprimorar a segurança da informação, através da aquisição, implantação e uso de ferramentas avançadas de segurança da informação.

Com a contratação de tais ferramentas, pretende-se colocar o Tribunal em acordo com às recomendações constates no Manual de Referência de Proteção de Infraestruturas Críticas de TIC, aprovado através da Portaria CNJ nº 162, de 10 de junho de 2021, e às recomendações constantes na norma ABNT NBR ISO/IEC 27001:2013, item 10.10.

3. BENEFÍCIOS DIRETOS E INDIRETOS RESULTANTES DA CONTRATAÇÃO

Ao atingir o objetivo principal, é esperado que os seguintes benefícios, diretos e indiretos, sejam alcançados:

- Permitir a automação de controle de privilégios aos curadores dos dados e informações;
- Aprimorar a governança de TI quanto aos dados não estruturados;
- Aprimorar a gestão de segurança da informação e comunicações.
- Aproveitamento eficiente do espaço de armazenamento dos eventos de auditoria;
- Mitigar o risco de ataques de *ransomware* e, caso ele ocorra, limitar seu efeito e consequente impacto.

4. REQUISITOS E NECESSIDADES TÉCNICAS

Requisitos que a solução CONTRATADA/adquirida deverá atender, incluindo os requisitos mínimos de qualidade, de modo a possibilitar a seleção da proposta mais vantajosa mediante competição. Incluem requisitos internos funcionais, requisitos internos não funcionais e requisitos externos.

Requisitos gerais de Negócios	
ID	**Descrição**
R.N01	Atendimento aos padrões definidos no item 10.10 da norma ABNT NBR ISO/IEC 27002:2013 - Código de Prática para a Gestão da Segurança da Informação.
R.N02	Analisar, proteger, monitorar e gerenciar a integridade das informações armazenadas e disponibilizadas no ambiente de arquivos.
R.N03	Atender ao Manual de Referência de Proteção de Infraestruturas Críticas de TIC, aprovado através da PORTARIA CNJ No 162, DE 10 DE JUNHO DE 2021.
R.N04	Classificação dos arquivos armazenados em repositórios não estruturados, mapeando onde e para quem os dados estão expostos.
R.N05	Análise comportamental dos usuários internos no ambiente computacional para rápida identificação de anomalias advindas de ataques, perda de informações e má gestão dos repositórios dos dados não estruturados.
R.N06	Aprimorar governança de dados e informação.
R.N07	Disponibilização de segurança, auditoria ininterrupta dos serviços de correio eletrônico, compartilhamento de arquivos, e de sistemas de TI.
R.N08	Pesquisas de auditoria referente a quem, quando, onde e como um dado é utilizado.
R.N09	Ações proativas em casos de incidentes de segurança cibernética e ataque de *malwares*.
R.N10	Identificação de acessos indevidos de usuários mal-intencionados.
R.N11	Garantir que usuários privilegiados sejam controlados e não acessem os ativos de TIC de forma direta.
R.N12	Verificação de comportamento de usuários nos *endpoints* para identificação de comportamento anômalo que possa representar um ataque.
R.N13	Proteção nos *endpoints* além do que é oferecido pelos antivírus.

Requisitos Tecnológicos para soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	
ID	**Descrição**
R.HS01	Auditoria e prevenção de ameaças em base de armazenamento de informação sobre usuários, dispositivos e sistemas, Microsoft Active Directory.
R.HS02	Auditoria e prevenção de ameaças em base de armazenamento de informação sobre usuários, dispositivos e sistemas, OpenLDAP. Esta base é utilizada por alguns sistemas legados.
R.HS03	Auditoria e prevenção de ameaças em correio eletrônico em nuvem, como Google Gmail (Suíte Google

	Workspace) e Microsoft 365.
R.HS04	Auditoria e prevenção de ameaças em servidores de sistemas de arquivos Windows Server 2012 e superiores.
R.HS05	Auditoria e prevenção de ameaças em samba 4.0 e superiores instalados em Oracle Enterprise Linux (ou equivalente) 7.0 e superior.
R.HS06	Auditoria e prevenção de ameaças em servidores de arquivos NAS DELL/EMC ISILON com OneFS na versão 8 em diante.
R.HS07	Auditoria e prevenção de ameaças em servidores Windows Server 2019 e superiores.
R.HS08	Auditoria e prevenção de ameaças em estações de trabalho com os seguintes sistemas operacionais: • Windows 10 32bits e 64 bits; • Windows 11 32bits e 64 bits; • Windows Server 2012 e superior.
R.HS09	Analisar o ambiente, coletar informações sobre objetos, arquivos e caixas de correio.
R.HS10	Gerar relatórios que permitam garantir a efetividade de controles de segurança, assim como uma visão do estado atual e histórico de usuários e acessos.
R.HS11	Ser capaz de rastrear os eventos que antecederam um evento de falha de segurança.
R.HS12	Permitir responder quem, quando, onde e como um determinado objeto foi acessado, editado ou excluído.
R.HS13	Permitir a identificação de tentativas ou acessos, aceitos ou rejeitados, de usuários, computadores ou sistemas.
R.HS14	Permitir identificar a frequência de utilização e o último acesso aos objetos e arquivos auditados.
R.HS15	Permitir identificar permissões de acesso ou de modificação não necessárias aos recursos, arquivos ou caixas de correio.
R.HS16	Permitir identificar a origem dos acessos a arquivos e objetos.
R.HS17	Permitir o acesso às informações de auditoria em tempo real ou em histórico de, no mínimo, 5 anos.
R.HS18	Permitir automatizar a identificação, a remoção de permissões, a desativação e a remoção de objetos e arquivos com base em informações de auditoria.
R.HS19	Detectar atividades não autorizadas de processamento de informações.
R.HS20	Permitir a configuração de alertas com base nas informações auditadas.
R.HS21	Permitir a auditoria de informações de acessos tanto de administradores quanto dos usuários dos serviços.
R.HS22	Utilizar de forma eficiente o espaço em disco necessário para armazenamento dos eventos de auditoria.
R.HS23	Utilizar as informações auditadas para sugerir melhorias no uso dos recursos.
R.HS24	Permitir a gestão eficiente dos recursos auditados.
R.HS25	Permitir a identificação e classificação de conteúdos sensíveis em servidores de arquivos
R.HS26	Permitir a identificação dos proprietários dos dados, listas de distribuição e caixas de correio individuais ou corporativas.
R.HS27	Monitorar os eventos das caixas postais dos usuários.
R.HS28	A coleta de informações de auditoria não deve onerar o processamento nos servidores alvo.
R.HS29	Permitir o ajuste os diretórios com herança quebrada de permissões
R.HS30	Assegurar que as autorizações são baseadas em necessidades de negócio
R.HS31	Permitir auditar aproximadamente 1300 usuários do Tribunal
R.HS32	Permitir auditar aproximadamente 1300 contas de usuários/sistemas nos controladores de domínio.
R.HS33	Permitir auditar aproximadamente 500 grupos nos controladores de domínio.
R.HS34	Permitir auditar aproximadamente 1500 objetos de computadores nos controladores de domínio.
R.HS35	Permitir auditar aproximadamente 20000 objetos diversos nos controladores de domínio.
R.HS36	Permitir auditar aproximadamente 100 TeraBytes de dados não estruturados.
R.HS37	Permitir auditar aproximadamente 1500 caixas de correio eletrônico.
R.HS38	Suportar a utilização de servidores virtualizados para todos os seus componentes.
R.HS39	Gerar relatórios de todas as consultas e ações feitas pelos usuários através da interface gráfica da solução, de modo que também seja possível realizar auditoria.
R.HS40	Ser capaz de analisar o comportamento do usuário para descobrir uso anômalo e, assim, identificar possíveis invasões.
R.HS41	A solução não poderá limitar
R.HS42	A inclusão de ativos na solução além do quantitativo licenciado deverá gerar um alerta para o administrador, mas não poderá, em hipótese alguma, impedir o acréscimo e limitar o uso da solução.
R.HS43	Realizar descoberta automática de ativos.
R.HS44	A solução poderá ser licenciada no modelo de direito de uso, desde que não perca suas funcionalidades

	quando da expiração da licença.
R.HS45	Deverá monitorar e proteger todos os processos existentes nos *endpoints*.
R.HS46	Deverá realizar detecção de vulnerabilidades e ameaças de *zero-day*
R.HS47	No caso de uso de agentes instalados nos *endpoints*, deverá implementar mecanismos para sua proteção.

Requisitos Tecnológicos para solução de proteção controle de acesso de usuários privilegiados (software e hardware)	
ID	**Descrição**
R.HS48	Ser instalado em equipamento físico dedicado, em cluster e sem ponto único de falha.
R.HS49	O cluster deverá permitir ser instalado de forma distribuída, ou seja, com os nós em locais físicos diferentes conectados por uma LAN.
R.HS50	Deverá ser garantido que a solução não dependa 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.
R.HS51	Garantir a retenção dos registros de acesso por, pelo menos, 5 anos.
R.HS52	Gravar em vídeo os acessos privilegiados
R.HS53	Possuir duplo fator de autenticação para acesso aos ativos
R.HS54	A inclusão de ativos na solução além do quantitativo licenciado deverá gerar um alerta para o administrador, mas não poderá, em hipótese alguma, impedir o acréscimo e limitar o uso da solução.
R.HS55	Possuir ampla capacidade de gerar relatórios e *dashboards*.
R.HS56	Possuir mecanismos avançados de proteção dos usuários privilegiados, usando certificados digitais e criptografia, quando aplicável.
R.HS57	Realizar descoberta automática de ativos.
R.HS58	Atender usuários privilegiados do tipo administradores, root e admin de equipamentos e sistemas operacionais.
R.HS59	Permitir acesso de contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, *helpdesk*)
R.HS60	Proteger usuários em: • Servidores Linux; • Servidores Windows; • Storages; • Estações de Trabalho Windows; • Equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP); • Aplicações conteinerizadas com *secrets*; • Instancias de Banco de Dados (Oracle, PostgreSQL, MS-SQL e MySQL) • Aplicações não-conteinerizadas com senha embutida (*hard coded*)
R.HS61	Atender usuários privilegiados do tipo administradores de banco de dados Oracle, MS SQL, MySQL e PostgreSQL.
R.HS62	Deverá possuir funcionalidades de gestão de usuários e perfis
R.HS63	Deverá possuir recursos de descoberta e cadastro automático de ativos.
R.HS64	Deverá implementar mecanismos de proteção de credencias através de criptografia
R.HS65	Deverá proteger informações privilegiadas, tais como certificados digitais e senhas.
R.HS66	Deverá possuir mecanismos para bloquear comandos indesejados
R.HS67	Deverá possuir mecanismos para controlar privilégios
R.HS68	Deverá implementar rotações de senhas de fora automatizada em todos os ativos protegidos
R.HS69	Deverá realizar análise comportamental do acesso dos usuários privilegiados
R.HS70	Deverá ser gerenciada através uma central única.

Requisitos de Treinamento (Capacitação)	
ID	**Descrição**
R.T01	O treinamento contemplará todos os softwares que compõem a solução.
R.T02	Deverá abordar de forma teórica e prática todas as funcionalidades solicitadas.

R.T03	Possuir carga horária adequada e compatível com o conteúdo a ser ministrado.
R.T04	O público-alvo deste treinamento são os analistas responsáveis pela execução de atividades de administração e auditoria dos ambientes monitorados pela solução.
R.T05	O treinamento deverá ser realizado utilizando-se solução idêntica à adquirida, inclusive quanto à versão dos sistemas.
R.T06	A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 6 (seis) horas de instrução diária.
R.T07	Deverá ser ministrada uma turma de treinamento que terá até 10 participantes.
R.T08	Deverá ser fornecido material em formato digital ou impresso do conteúdo do treinamento.
R.T09	O(s) instrutor(es) deverá(ão) ser comprovadamente certificado(s) nos sistemas e/ou ferramentas fornecidos no escopo da solução.
R.T10	A avaliação do sucesso do treinamento deverá ser mensurada pela turma através de mecanismos objetivos.
R.T11	A turma deverá ter até 10 alunos

Requisitos Legais, Sociais e Ambientais	
ID	**Descrição**
R.LSA01	A empresa deverá estar habilitada juridicamente (art. 28 da Lei n.º 8.666/93) e em regularidade fiscal e trabalhista (art. 29 da Lei n.º 8.666/93).
R.LSA02	Resolução CNJ nº 182/2013, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça.
R.LSA03	Decreto-lei N.º 5.452, de 1º de Maio de 1943, que define a Consolidação das Lei do Trabalho.
R.LSA04	Súmula nº 269 do TCU que estabelece que nas contratações para a prestação de serviços de Tecnologia da Informação, a remuneração deve estar vinculada a resultados ou ao atendimento de níveis mínimos de serviço.
R.LSA05	Cumprir o disposto no inciso XXXIII do art. 7.º da Constituição Federal de 1988, quanto ao emprego de menores.
R.LSA06	Promover a correta destinação dos resíduos resultantes da prestação do serviço, tais como peças substituídas, embalagens, entre outros, observando a legislação e princípios de responsabilidade socioambiental como a Política Nacional de Resíduos Sólidos (Lei n.º 12.305/2010) e o Guia de Contratações Sustentáveis da Justiça do Trabalho (Resolução n.º 103/2012 do Conselho Superior da Justiça do Trabalho).
R.LSA07	Prever a destinação ambiental adequada das pilhas e baterias usadas ou inservíveis, segundo disposto na Resolução CONAMA nº 257, de 30 de junho de 1999

Requisitos de Manutenção	
ID	**Descrição**
R.M01	O suporte deverá ser prestado na modalidade 24x7.
R.M02	A garantia deverá ser de, pelo menos, 12 meses
R.M03	O SLA para cada solução deverá ser adequado à criticidade do serviço e o impacto nos demais sistemas do Tribunal em caso de falha.
R.M04	Caberá a CONTRATADA, no momento da instalação, realizar as parametrizações necessárias para adequação da solução ao ambiente do Tribunal.
R.M05	Deverá ser possível abrir chamado na CONTRATADA e no Fabricante.

Requisitos de Prazo	
ID	**Descrição**
R.P01	Os prazos de entregada deverão ser: • Grupo 01, itens 01 e 02 – em até 5 (cinco) dias úteis após a assinatura do contrato; • Grupo 01, item 03 – em até 45 (quarenta e cinco) dias após a reunião de planejamento da instalação; • Grupo 01, item 04 – em até 45 (quarenta e cinco) dias após a reunião de planejamento do treinamento; • Grupo 02, itens 05 a 20 e item 23 – em até 45 (quarenta e cinco) dias após a assinatura do contrato; • Grupo 02, item 21 – em até 45 (quarenta e cinco) dias após a reunião de planejamento da instalação; • Grupo 02, item 22 – em até 45 (quarenta e cinco) dias após a reunião de planejamento do treinamento; As reuniões de planejamento da instalação e de treinamento previstas para os itens 03 e 04 do Grupo 01 e itens 21 e 22 do Grupo 02, deverão ser realizadas em até 10 dias após a assinatura do contrato, a critério da CONTRATANTE**.**

Requisitos de Segurança da Informação	
ID	**Descrição**
R.SI01	O acesso às instalações do CONTRATANTE onde serão realizados os serviços deverá ser controlado e permitido somente às pessoas autorizadas.
R.SI02	A CONTRATADA deverá substituir imediatamente aquele profissional que seja considerado inconveniente à boa ordem ou que venha a transgredir as normas disciplinares do Tribunal.
R.SI03	Os profissionais disponibilizados pela CONTRATADA para a prestação dos serviços deverão estar identificados com crachá de identificação da empresa, estando sujeitos às normas internas de segurança do Tribunal, inclusive àqueles referentes à identificação, trajes, trânsito e permanência em suas dependências.
R.SI04	A CONTRATADA deverá acatar e obedecer às normas de utilização e segurança das instalações do Tribunal.
R.SI05	Os profissionais deverão utilizar a conta que lhe for atribuída, de forma controlada e intransferível, mantendo secreta a sua respectiva senha, pois todas as ações efetuadas através desta, serão de responsabilidade do profissional da CONTRATADA.
R.SI06	A CONTRATADA deverá manter os seus profissionais informados quanto às normas disciplinares do Tribunal, exigindo sua fiel observância, especialmente quanto à utilização e segurança das instalações.
R.SI07	A CONTRATADA deverá garantir a segurança das informações do Tribunal e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido do Tribunal no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.
R.SI08	A CONTRATADA e seus profissionais devem manter sigilo absoluto sobre documentos elaborados e informações obtidas dentro do Tribunal.

5. DESCRIÇÃO DE CENÁRIO E NECESSIDADES DO TRT24

As soluções propostas para aquisição possuem seu licenciamento baseados em usuários que acessam o ambiente, caixas postais em ativos protegidos, do tipo:

- Quantidade de usuários que fazem uso dos sistemas de arquivos e controladores de domínio;
- Quantidade de usuários administradores;
- Quantidade de estações de trabalho;

- Quantidade de máquinas servidores;
- Quantidade de equipamentos de armazenamento;
- Quantidade de caixas postais de e-mail;
- Quantidade de usuários privilegiados que acessam o ambiente;
- Quantidade equipamentos de rede;
- Quantidade de aplicações em container;
- Quantidade de aplicações fora de container;
- Quantidade de instâncias de banco de dados.

Uma das infraestruturas mais frequentemente utilizadas para sistemas web é a utilização de aplicações e armazenamento de dados em nuvem. Essa escolha de implementação para plataformas de infraestrutura oferece a redução de custos para a instituição, não somente em equipamentos, como em quantidade de pessoal técnico necessário para a manutenção da plataforma necessária para sediar os sistemas.

Nessa proposta o TRT24 tem 2 projetos em instalação entre o final do exercício de 2022 e o início do exercício de 2023:

- Projeto local em andamento, que visa contratação de solução de e-mail e de servidor de arquivos, em nuvem; e,

- PJe em nuvem: O CSJT selecionou o TRT24, em conjunto com o TRT17, para participação como Tribunal piloto, no projeto de migração do Sistema PJe para a nuvem.

Nesse cenário, foram avaliadas as licenças de softwares de monitoramento de dados não estruturados que abrangesse a nova complexidade do ambiente.

Como essa instalação em nuvem é iminente, com o PJe previsto para estar armazenado em nuvem ainda em 2022, e a migração dos serviços de e-mail logo no início de 2023, a contagem de licenças para contratação foi feita com informações reunidas entre a Divisão de Proteção de Dados e Segurança da Informação com a Divisão de Infraestrutura de TI.

Também foi analisada a questão de utilização atual dos serviços de autenticação em dois domínios - OpenLDAP e Microsoft AD, definido no requisito R.HS01. A autenticação de domínio com o AD nas estações está 90% migrada, porém, aplicações antigas autenticam ainda no OpenLDAP, o que desfavorece a previsão de data para desativação. Por isso foi considerado o ambiente misto na utilização das licenças para contratação.

Além disso, no citado cenário de defasagem de recursos humanos disponíveis para manutenção de serviços de TI, a escolha de contratação de soluções de software especializadas pode oferecer condições de evoluir a proteção da instituição, sem onerar a equipe existente, minimizando o impacto da demanda atual, represada e reprimida pela falta de pessoal. Além de considerar ainda a importância de contratação de serviços de monitoramento, suporte e garantia para as soluções. O treinamento também é essencial e parte do escopo, mesmo no cenário de serviços incluídos na contratação, pois a fiscalização dos serviços exige um conhecimento mínimo.

Dentro da solução de senha segura, foi feita a contagem de senhas privilegiadas a partir dos números de integrantes de toda a equipe da SETIC, incluindo equipes terceirizadas. Isso porque há diferentes plataformas e diferentes acessos para cada unidade especializada da SETIC, que configuram

acesso privilegiado comparado ao público de usuários da organização, ainda que havendo diferenças no nível de acesso.

A contagem de *endpoints* (estações de trabalho) atualmente em produção foi feita com apoio do Núcleo de Microinformática, e para a totalização já foi considerada os projetos de aquisição de notebooks e o descarte de antigos.

A parceria da Divisão de Proteção de Dados e Segurança da Informação com a Divisão de Infraestrutura de TI também foi necessária para definir a quantidade de servidores de rede, de armazenamento, equipamentos de rede, aplicações em container e fora de container e instâncias de bancos de dados.

6. MAPEAMENTO DA DEMANDA DO TRT24

A seguir, estão computados os ativos a serem protegidos na solução, quantificados por tipo para os itens de licenciamento.

A) Quantidade de usuários que fazem uso dos sistemas de arquivos e controladores de domínio:

Magistrados	64
Servidores	580
Estagiários	120
Prestadores	130
Inativos	300
Usuários institucionais	206
Total	**1300**

Em vista da variação de estagiários e prestadores ao longo de um ano e do acréscimo de servidores convocados ou através de concurso, foi considerado o quantitativo máximo de cargos e de colaboradores utilizados pelos contratos e convênios assinados. Assim, foram computadas as vagas em aberto de magistrados, servidores (inclusive cedidos de outros órgãos), o limite máximo de estagiários, e terceirizados, para não permitir risco de usuários a descoberto. Ainda foram computados os números de usuários inativos, pois, apesar de não acessarem a rede computacional, acessam sistemas internos para comunicação com seus dados (Sistema de Processo Administrativo Eletrônico – PROAD, para requisições e Sistema de Gestão de Pessoas – SIGEP-OnLine e MeuPortal, para acesso a holerites Declaração de Rendimentos e históricos da vida ativa). Foram incluídos usuários institucionais, em razão da necessidade de utilização de estações com conexão dedicada (estações utilizadas nas áreas de segurança predial, memorial e outros, onde há uso de login para uso exclusivo em estações dedicadas).

B) Quantidade de estações de trabalho (incluindo Desktops e Notebooks):

Desktops	1120
Notebook	380
Total	**1500**

Nessa contagem foram incluídas as estações/notebooks em fase de contratação ainda em 2022 (no total de 180).

C) Quantidade de máquinas do tipo servidores:

Servidores físicos	72
Servidores virtuais	340
Total	**412**

A quantidade de servidores físicos só varia através de processo de aquisição, o que nos permite afirmar que não há variação prevista para os próximos 12 meses. Por outro lado, a variação de máquinas virtuais é intensa e não diretamente relacionada ao acréscimo de novas aplicações, mas com o simples aumento de recurso necessário para executar os sistemas atuais através de processo chamado de escalabilidade horizontal, onde mais máquinas são acrescidas a um sistema para melhor distribuir seu processamento. Soma-se a previsão de acréscimo de servidores virtuais a serem implementados nos próximos 12 meses.

D) Quantidade de equipamentos de armazenamento:

Storage 1	4
Storage 2	4
Total	**8**

E) Quantidade de caixas postais de e-mail:

Total de contas atuais	1500
Quantidade a contratar considerando a migração para a nuvem	**1500**

A quantidade de caixas postais atuais não tem sido suficiente para atender a demanda do Tribunal, estando próximo do limite de esgotamento. O projeto de migração do serviço de e-mail para a nuvem será assinado até novembro. Por isso o quantitativo do item a ser contratado deverá ser de 1300.

F) Quantidade de usuários privilegiados que acessam o ambiente:

Usuários privilegiados na Secretaria de TIC	01
Usuários privilegiados na Divisão de Governança e Gestão de TIC	06
Usuários privilegiados na Divisão de Infraestrutura de TIC	07
Usuários privilegiados na Divisão de Proteção de Dados e Segurança da Informação	03
Usuários privilegiados no Núcleo de Sistemas da Informação	16
Usuários privilegiados no Núcleo de Microinformática e Suporte ao Usuário	9
Total	**42**

São considerados usuários privilegiados aqueles que precisa ter acesso a sistemas ou equipamentos com privilégio avançados. Todos os servidores lotados na Divisão de Infraestrutura de TIC e na Divisão de Proteção de Dados e Segurança da Informação possuem acesso privilegiado a sistemas e/ou equipamentos. No Núcleo de Microinformática e Suporte ao Usuário, os usuários possuem acesso a estações de trabalho como administradores e alguns sistemas críticos para incluir/configurar acesso de usuários do TRT24. No Núcleo de Sistemas da Informação, há servidores que possuem acesso de administrador nas estruturas de plataforma como serviço baseado em container. Na Secretaria de TIC e na Divisão de Governança e Gestão de TIC, os usuários possuem acesso de leitura para governança, gestão e fiscalização, assim como acesso a alguns sistemas críticos. Na divisão de governança os servidores também trabalham com programação e acesso a banco de dados, em virtude do desenvolvimento em LifeRay de suas próprias aplicações e do portal de acesso externo.

G) Quantidade equipamentos de rede:

Switch de rede (ACESSO)	76
Switch (DATACENTER)	32
Controladoras Wifi Virtual	2
NAS	22
Firewall (MARCA)	4
Roteador	4
(OUTROS EQUIPAMENTOS)	30
Total	**170**

H) Quantidade de aplicações em container:

Quantidade de aplicações em containers	25
Total	**25**

São as principais aplicações que já estão em containers:

- PJe + 12 sistemas satélites;
- Proad;
- Sigep;
- Folhaweb;
- Gest;
- Ponto.

Há também um fator que influencia no licenciamento para esse desse tipo de aplicação, são as variáveis de ambiente de cluster de containers que serão protegidas. Os fabricantes chamam essa proteção de *secrets*. As aplicações do Tribunal precisam de proteção de, ao menos, duas variáveis de ambiente, são elas:

- URL de acesso ao banco de dados com o usuário e senha;
- Chave da API para troca de informações entre o micro serviços através de estrutura de API.

Portanto, cada licença de aplicação deverá licenciar também, ao menos, 2 (dois) *secrets*.

As aplicações do Tribunal estão passando por processo de modernização da arquitetura, indo da tradicional aplicação em máquina virtual para aplicações em containers. Somando o PJe e seus atuais 12 sistemas satélites com os 5 sistemas administrativos, temos demanda imediata de 18 licenças. Porém, temos que somar mais 7 licenças para suportar as aplicações que serão migradas para arquitetura de containers. Assim, a demanda total é de 25 licenças.

I) Quantidade de aplicações fora de container:

Quantidade de aplicações em infraestrutura tradicional	45
Total	**45**

Em vista da migração dos sistemas legados para infraestrutura mais moderna, como a de containers, não há previsão de crescimento de novas aplicações em infraestrutura tradicional nos próximos 12 meses.

J) Quantidade de instâncias de banco de dados:

Banco de dados Oracle	2
Banco de dados MS SQL	2
Banco de dados PostgreSQL	13
Banco de dados MySQL/MariaDB	5
Elastic Search	8
Total	**30**

A quantidade de instâncias de banco de dados pode variar conforme a demanda, sem que necessariamente sejam acrescidos licenciamento. Entre os bancos acima estão os de produção, homologação, desenvolvimento e treinamento.

Há ainda, como citado acima, a migração do Sistema PJe para a nuvem. No entanto, mesmo com essa migração será mantida a base atual como "backup quente" das aplicações. Não havendo previsão de crescimento, mas será mantida a estrutura de produção atual como site redundante.

K) Instalação

O serviço de instalação necessário pode ser dividido em duas soluções: solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoints* e solução de controle de acesso de usuários privilegiados. Para cada um, um serviço diferente de instalação.

L) Treinamento

Para o treinamento da solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint* é necessário o envolvimento das seguintes unidades da TI:

Usuários privilegiados na Divisão de Infraestrutura de TIC	07
Usuários privilegiados na Divisão de Proteção de Dados e Segurança da Informação	02
Usuários privilegiados no Núcleo de Microinformática e Suporte ao Usuário	01
Total de turmas de 10 alunos	**01**

Para o treinamento da solução de controle de acesso de usuários privilegiados, considerando a dificuldade de separação de todas as unidades envolvidas para o treinamento completo, treinaremos o público de acesso mais restrito e crítico e faremos disseminação interna. A necessidade de disseminação interna é ainda mais necessária em decorrência dos usuários específicos que o Tribunal não tem abrangência jurídica para custear o treinamento, pessoal terceirizado da Central, mas que fazem o atendimento em nível 2.

Usuários privilegiados na Divisão de Infraestrutura de TIC	04
Usuários privilegiados na Divisão de Proteção de Dados e Segurança da Informação	02
Usuários privilegiados no Núcleo de Sistemas da Informação	02
Usuários privilegiados no Núcleo de Microinformática e Suporte ao Usuário	02
Total de turmas de 10 alunos	**1**

M) Licenças e Garantia para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados

A garantia para as duas soluções será de 12 meses. A solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*, conforme será apresentado adiante, deverá ser adquirida pelo modelo de subscrição, onde o direito de uso das licenças e a sua garantia e suporte são adquiridos como serviço por período, no caso, 12 meses. Assim, é seu quadro de quantitativo para contratação:

O quadro de quantitativo para a solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint* precisa ser: **Especificação**	**Unidade**	**Quantidade a contratar**
Licença de uso de *software* e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint.*	Usuários	1300
Licença de uso de *software* e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados.	Usuários	1300
Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*.	Serviço	1
Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint.*	Turma	1

Na solução de proteção e controle de usuários privilegiados (PAM), não encontramos evidências de que a aquisição da garantia e suporte por período maior que 12 meses representa economicidade. Também cabe a separação entre a garantia do software, oferecida pelo fabricante, e o serviço de suporte técnico especializado que pode ser fornecido por empresas especializadas em segurança da informação. Dessa maneira cabe a separação da garantia fornecida pelo fabricante, vinculada individualmente para cada licença/hardware, e o suporte técnico especializado. O primeiro, como está vinculado à licença, o pagamento é realizado da mesma foram que a licença: de uma única vez e com por período de 12 meses. O segundo, por ser tratar de serviço de suporte, ainda que vinculado à solução, mas não vinculado às licenças, pois não é fornecido pelo fabricante, o pagamento deve ser mensal.

Assim, é seu quadro de quantitativo para contratação:

Item	**Especificação**	**Unidade**	**Quantidade a contratar**
01	Cluster para prover recursos para solução de acesso a usuários privilegiados	*Cluster	1
02	Garantia do fabricante por período de 12 meses para cluster para prover recursos para solução de acesso a usuários privilegiados	*Cluster	1
03	Licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, *helpdesk*)	Usuários	42
04	Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, *helpdesk*)	Usuários	42
05	Licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores	420
06	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores	420
07	Licença para estações de trabalho Windows	Estações	1500

Item	Especificação	Unidade	Quantidade a contratar
08	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows	Estações	1500
09	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos	170
10	Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos	170
11	Licença para aplicações conteinerizadas com *secrets*	Aplicações	25
12	Garantia do fabricante por período de 12 meses para licença para aplicações conteinerizadas com *secrets*	Aplicações	25
13	Licença para aplicações não-conteinerizadas com senha embutida (*hard coded*)	Aplicações	45
14	Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (*hard coded*)	Aplicações	45
15	Licença para instancias de Banco de Dados (Oracle, Postgres, MS-SQL e MySQL)	Instâncias	30
16	Garantia do fabricante por período de 12 meses para licença para instancias de Banco de Dados (Oracle, Postgres, MS-SQL e MySQL)	Instâncias	30
17	Serviço de instalação para solução de controle de acesso de usuários privilegiados.	Serviço	1
18	Treinamento para solução de controle de acesso de usuários privilegiados.	Turma	1
19	Serviço e suporte técnico especializado	Meses	12

**Cluster deve ser entendido como dois ou mais equipamentos funcionando em conjunto para prover alta disponibilidade*

7. CONTRATAÇÕES SIMILARES EM OUTROS ÓRGÃOS E NO PORTAL DE SOFTWARE PÚBLICO BRASILEIRO

(art. 14, I, "b" e art. 14, II, "a" e "c")

A contratação pretendida foi realizada pelo TST, resultando em uma ARP com possibilidade de adesão. Contratações similares, com escopos um pouco diferentes, foram realizadas pela ANA e ANAC.

Em consulta ao portal do software público brasileiro (https://softwarepublico.gov.br/social/), realizada em 30/07/2021, não foram identificadas soluções de auditoria para ambientes de datacenter, *endpoint* e gestão de usuários privilegiados que atendam a demanda em tela.

8. ADERÊNCIA A PROJETOS NACIONAIS E DO CNJ

(art. 14, II, "d", "e", "f")

Não se aplicam as diretrizes do Modelo Nacional de Interoperabilidade (MNI).

Não se aplica o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do PJ (Moreq-Jus).

Não se aplica o padrão de aderência à ICP-Brasil.

9. LEVANTAMENTO DE MERCADO

(art. 14, II, "d", "e", "f")
(** Plano de Trabalho – item 6)

A demanda objeto desse estudo pode ser dividida em dois tipos: solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*; e soluções de segurança e controle de acesso de usuários privilegiados.

O tipo de solução de segurança e controle de acesso de usuários privilegiados é chamado de PAM, que é a sigla em inglês para Gerenciamento de Acesso Privilegiado (Privilege Access Management). Essas soluções são softwares fechados que possuem todas as funcionalidades para atender a esse tipo de necessidade, que é o controle de acesso e proteção à usuários privilegiados.

Esse tipo de solução possui produtos consolidados no mercado com diversos fabricantes. Corrobora com essa afirmação a existência de um quadrante mágico criado pelo Gartner Group especificamente para esse tipo de solução, onde o de 2021 pode ser visto abaixo:

Magic Quadrant

Figure 1: Magic Quadrant for Privileged Access Management

Source: Gartner (July 2021)

Do quadrante, observamos que há 10 fabricantes diferentes que possuem representatividade no mercado. Entre os fabricantes no quadrante de líderes, vimos apresentações dos produtos da CyberArk, BeyondTrust e Thycotic. Também vimos apresentação do produto "senhasegura", desenvolvido pela empresa Brasileira MT4 Tecnologia e está posicionada no quadrante como "Challenger".

As principais diferenças entre as soluções estudadas estão na interface de gerenciamento e nas funcionalidades oferecidas. Apesar das diferenças, a necessidade do Tribunal pode ser atendida por qualquer uma delas, não sendo necessário a solução mais completa em termos de funcionalidade que, no caso, é a líder CyberArk.

O licenciamento desse tipo de solução é baseado na quantidade de ativos que são protegidos e possui o modelo de licenças perpétuas. Há fabricantes que oferecem como alternativa modelo de licenciamento como serviço prestado em nuvem, mas todos os principais fabricantes possuem o modelo de licenças perpétuas.

Uma necessidade que não é oferecida como padrão por essas soluções é a exigência de instalação em máquinas físicas que formam cluster de alta disponibilidade. No entanto, essa demanda é facilmente atendida por qualquer licitante capaz de ofertar máquinas servidores x86.

Para a solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*, não encontramos no mercado um único software que abrange toda a demanda. Existem softwares que atendem partes dos requisitos, alguns mais do que outros. No entanto, a demanda pode ser atendida se a contratação não focar em um produto único, mas em uma solução formada por mais de um software e fornecida ao Tribunal através de empresas integradoras, ou seja, por empresas que integram produtos de TIC e a entregam como uma solução.

Há, pelo menos, 34 fabricantes que possuem produtos de softwares que podem atender a parte dos requisitos necessários, são eles:

Active Navigation	Varonis
Adlib	Veritas Technologies
Condrey	ZL Technologies
Druva	Dell
Egnyte	NetAdmin
Everteam	OREV
Formpipe	Carbon Black
FTI Technology	Cisco
Ground Labs	CrowdStrike
IBM	Cylance
Index Engines	Kaspersky Lab
Micro Focus	McAfee
Netwrix	Microsoft
SailPoint	SentinelOne
Spirion	Sophos
STEALTHbits Technologies	Symantec
Titus	Tanium

Esses fabricantes foram encontrados com o auxílio de documentos publicados pelo Gartner Group e através de reuniões realizadas com em especializadas em segurança da informação e que são integradoras de solução de TIC.

Entre as soluções ofertadas, a forma de licenciamento mais abrangente é o de direito de uso por período determinado. Esse tipo de licenciamento é o mais utilizado por soluções de segurança da informação, pois são softwares que envolvem constante atualização de suas bases de ameaças para manter o ambiente protegido. É o mesmo modelo oferecido pelo mercado para softwares de antivírus, onde a atualização da sua base é mandatória para a efetiva proteção. O cliente paga pelo uso, por período específico.

Esses softwares não deixam de funcionar quando a licença expira, ou seja, é possível manter o seu uso, no entanto, a atualização das bases utilizadas para proteção dos dados (base de dados com assinaturas de ataques, vírus, *malwares* etc.) deixam de ser atualizadas, fazendo com que a solução rapidamente perca sua eficácia.

Conforme o modelo de comercialização de cada fabricante, há produtos que são ofertadas com instalação local no ambiente do cliente (*on-premisses*), ofertados apenas em nuvem publica, ofertados de forma hibrida (com instalação local e na nuvem) e, para alguns fabricantes, ofertados o mesmo produto localmente ou na nuvem.

Considerando que os dados não sairão da infraestrutura do Tribunal, não há qualquer óbice no uso de serviços em nuvem para esse tipo de produto, pois trata apenas de análise dos dados e de medidas protetivas. Inclusive, normalmente os produtos oferecidos em nuvem possuem maior capacidade de análise de eventuais ameaças e medidas protetivas mais eficazes.

10.JUSTIFICATIVAS DA ESCOLHA DO TIPO DE SOLUÇÃO A CONTRATAR

Como visto no estudo de mercado, não há um único produto de software que atenta sozinho todos os requisitos para a solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoints*. Sendo assim, a melhor forma de aquisição é a contratação de uma solução e não um produto específico. Essa solução será formada por dois ou mais produtos de software e caberá a uma empresa integradora de TIC, especializada em segurança da informação, ofertar, em processo licitatório, o melhor conjunto de produtos de softwares que estejam em acordo com o especificado no Termo de Referência.

Em vista da vasta quantidade de fabricantes que podem atender partes da demanda e a inexistência de um único fabricante que atenda a 100% dela, a escolha prévia de produtos de softwares pode limitar a concorrência para determinado nicho de mercado e prejudicar a ampla concorrência. Assim, é preferível especificar a necessidade do Tribunal e deixar para o mercado, no momento da licitação, apresentar sua oferta com a escolha dos softwares que irão compor a solução pretendida.

Quanto ao tipo de licenciamento, os fabricantes realizaram nos últimos dois anos movimento de troca do tipo de oferta, de licenças perpétuas para licença de uso por período determinado. Esse movimento decorre também da adoção cada vez maior de serviços em nuvem, onde o software passa a ser tratado como um serviço e não mais como uma licença permanente.

Em decorrência da mudança de oferta no modelo de licenciamento oferecido pelo mercado, a licença de uso por período determinado (ou subscrição) é o modelo mais abrangente, favorecendo a concorrência em um pregão. No entanto, cabe avaliar se esse modelo de subscrição possui valor análogo ao modelo anterior, onde as licenças eram perpétuas. Considerando a quantidade de fabricantes que possuem produtos possíveis de atender a demanda do Tribunal, é inviável a análise comparativa de cada um dos produtos de software capazes de atender a demanda. Apensar disso, encontramos um desses

produtos de softwares que foram contratados pela administração pública, através de pregão eletrônico, que possuem diferentes modelos de licenciamento, onde é possível realizar a comparação, conforme:

Órgão	UASG	Pregão	Modelo de Licenciamento	Data do Pregão	Fabricante
ANAC	113214	28/2019	Perpétua	11/12/2019	Varonis
ANA	443001	24/2020	Subscrição	23/11/2020	Varonis

O produto ofertado pelo fabricante Varonis é um dos mais abrangentes dentre os que podem atender, como parte de um conjunto de softwares, as necessidades do Tribunal. Também é um dos mais contratados, possuindo vários contratos com o Governo nas três esferas. Assim, a comparação entre dois preços públicos de órgãos da esfera federal para o mesmo software com modelo de licenciamento distintos, nos fornece insumos para avaliar se o modelo de licenciamento por subscrição, ainda que mais abrangente no mercado e, assim, melhorando a concorrência, é economicamente equivalente ao modelo anterior de licenças perpétuas.

É o conjunto de itens do pregão 24/2020 realizado pela ANA, referente ao licenciamento no modelo de subscrição com suporte por 12 meses, com o preço unitário após pregão:

Item	Descrição	Quantidade	Valor
1	Licença de subscrição, por 12 meses, de solução de auditoria para Microsoft Active Directory.	1000	R$ 332,00
2	Licença de subscrição, por 12 meses, de solução de auditoria para Microsoft Windows File Server e Microsoft OneDrive.	1000	R$ 315,00
3	Licença de subscrição, por 12 meses, de solução de auditoria para Microsoft Exchange.	1000	R$ 332,00
4	Licença de subscrição, por 12 meses, de solução de mapeamento e detecção de dados em risco.	1000	R$ 244,00
5	Licença de subscrição, por 12 meses, de solução de análise em tempo real e prevenção de comportamentos suspeitos.	1000	R$ 332,00

É o conjunto de itens do pregão 28/2019 realizado pela ANAC, referente ao licenciamento no modelo perpétuo com suporte por 36 meses, com o preço unitário após pregão:

Item	Descrição	Quantidade	Valor
1	Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de serviço de diretório (Microsoft Active Directory).	2400	R$ 415,00
2	Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de servidores de arquivos.	2400	R$ 513,00
3	Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de correio eletrônico (Microsoft Exchange).	2400	R$ 535,00
4	Licença perpétua de software de Solução de Tecnologia da Informação para identificação e classificação de conteúdos sensíveis.	2400	R$ 444,50
5	Serviços de suporte técnico e garantia.	36	R$ 74.000,00

A licitação da ANA possui uma licença a mais que a da ANAC e em seus preços já constam o suporte e a garantia por 12 meses juntamente com a licença de uso. Na licitação da ANAC, os itens 1 ao 4 tratam de licença perpétua e o item 5 do suporte para essas licenças, com valor mensal.

Para comparar o modelo de licenciamento entre as contratações, é preciso avaliar o custo das subscrições anuais no mesmo período de suporte das licenças perpétuas, equiparar as licenças e, considerando que são produtos dolarizados, o valor do dólar nas datas do pregão.

A equivalência estre as licenças é:

Pregão ANAC		Pregão ANA	
Item	**Preço por usuário**	**Item**	**Preço por usuário**
1	R$ 415,00	1	R$ 332,00
2	R$ 513,00	2	R$ 315,00
3	R$ 535,00	3	R$ 332,00
4	R$ 444,50	4	R$ 224,00
Total	R$ 1.907,50	Total	R$ 1.223,00

Considerando o valor do dólar na data da licitação de cada órgão, conforme o site do BACEN (https://www.bcb.gov.br/estabilidadefinanceira/historicocotacoes), o valor convertido foi de:

Órgão	**Preço**
ANAC	R$ 4,1147
ANA	R$ 5,3822

Para equiparar os valores em decorrência da variação do dólar é preciso acrescer cerca de 30,8% no preço praticado na ANAC (5,3822 ÷ 4,1147 ≈ 1,308 = 30,8%).

As licenças perpétuas foram adquirias por 36 meses e as subscrições com 12 meses. Assim, o valor de comparação precisa ser 3 vezes o preço da subscrição do pregão da ANA comparado com o preço total praticado pela ANAC, ambos com a quantidade de usuários igualada (2400 para ambos, que é o total da ANAC).

O valor total da subscrição na licitação da ANA, considerando 3 anos e 2400, é de R$ 8.805.600,00.

Memória de cálculo:

R$ 1.223,00 (valor das licenças por usuário) × 2400 (usuários) × 3 (anos) = R$ 8.805.600,00

O valor total da subscrição na licitação da ANAC considerando 3 anos, 2400 e a diferença do valor do dólar a época do pregão da ANA é de R$ 9.472.839,43.

Memória de cálculo:

R$ 1.907,50 (valor das licenças por usuário) × 2400 (usuários) + R$ 2.664.000 (3 anos de suporte) = R$ 7.242.000,00

R$ 7.242.000,00 * (5,3822 ÷ 4,1147 ≈ 1,308 = 30,8%) (diferença da cotação do dólar) = R$ 9.472.839,43.

Considerando o apresentado, o preço comparativo entre a licença por tempo de uso (subscrição) por 36 meses e licença perpétua com garantia e suporte por 36 meses é:

Órgão	Preço (36 meses)
ANA	R$ 8.805.600,00.
ANAC	R$ 9.472.839,43
Diferença (%)	-7,04%

A análise de preços entre os dois modelos de licenciamento demostra que o preço por subscrição é ligeiramente menor que por licenças perpétuas no mesmo período.

Destacamos que, por não sermos especialistas na solução Varonis, não é possível a equipe da contratação realizar análise minuciosa dos requisitos dos dois editais para saber, em detalhes, as equivalências entre as licenças. Para essa análise, contamos com as informações que nos foram repassadas por representantes da Varonis, onde nos foi dito a equivalência supracitada.

No entanto, mesmo que toda a especificação da contratação realizada pela ANA esteja contida na contratação realizada pela ANAC é possível observar que os valores são equivalentes, pois nesse caso, mesmo não parecendo ser o correto, os valores totais, considerando os mesmos cálculos, seriam:

Órgão	Preço total
ANA	R$ 11.196.000,00.
ANAC	R$ 9.472.839,43
Diferença (%)	18,19%

Na tabela acima, o preço por usuário/ano no pregão da ANA foi considerado como R$ 1.555,00 (a soma dos 5 itens).

Há outros fatores que influenciam no preço de uma licitação, como o volume a ser adquirido. No pregão da ANAC o montante é 2,4 vezes maior que no pregão da ANA, o que pode representar um maior desconto no preço praticado na ANAC.

A análise de preço entre esses dois pregões mostra que a diferença de custo entre subscrições e licenças perpetuas não é elevada ou desproporcional, indicando que a escolha do licenciamento por subscrição não representa desvantagem econômica significativa e, por favorecer a concorrência no certame ao ser o modelo mais comum entre os fabricantes, é a melhor escolha.

Associados ao modelo de licença de uso por período determinado estão a garantia de atualização e o suporte da solução junto ao fabricante. O modelo de venda, em todos os fabricantes listados, é a subscrição com pagamento em uma única parcela por período mínimo de 12 meses.

A escolha do conjunto de softwares como uma solução ofertada por uma única CONTRATADA em detrimento da aquisição individual de cada produto de softwares deve-se, principalmente, pela complexidade das opções possíveis para atender às necessidades postas.

Para cada ativo protegido, monitorado e auditado, como o Microsoft Active Directory (AD), servidores de arquivos e *endpoints*, há produtos de softwares que são especializados em cada um desses ativos. Há produtos que conseguem proteger, monitorar e auditar vários, mas não todos, esses ativos em conjunto.

Dentro das funcionalidades de proteção, auditoria e monitoramento há produtos de software que oferecem apenas uma dessas funcionalidades para um mesmo ativo.

Há softwares mais completos para proteção, monitoramento e auditoria de ativos como AD e servidores de arquivos, incluindo ativos de nuvem como o Google Workspace, mas eles ignoram proteção

análoga no *endpoints*. Há softwares de proteção para o mercado de *endpoints*, como os antivírus, mas eles tratam apenas a proteção, com poucas funcionalidades de autoria e monitoramento.

Em conversas com diversos fornecedores de soluções de segurança da informação, não encontramos um único produto de software capaz de atender a demanda de maneira completa.

Ademais, por se tratar de segurança da informação, a consistência na informação fornecida por ferramentas distintas e a capacidade de correlacionar essas informações é primordial para identificar uma falha de segurança e evitar que ele cause prejuízos à instituição.

É até possível administrar diversas ferramentas onde cada uma é responsável por um "pedaço" do ambiente, apensar da óbvia dificuldade, mas se cada uma dessa ferramenta for resultado de um contrato distinto, onde fornecedores diferentes realizaram a instalação e fornecem o suporte sem conhecer as demais ferramentas e os outros "pedaços" do ambiente de TIC, a eficaz administração torna-se inviável.

A divisão da necessidade em nichos acarretaria a limitação da concorrência a fabricantes especializados em cada nicho, e o resultado seria uma ferramenta e um contrato para cada "pedaço" do ambiente.

Dividir a necessidade em nichos, mas realizar a adjudicação por grupo, resolve o problema de um contrato para cada produto de software, mas limita as empresas integradoras de TIC, especializadas em segurança da informação, que eventualmente poderiam participar do certame, pois as possibilidades de composição de produtos de software seriam limitadas a cada nicho.

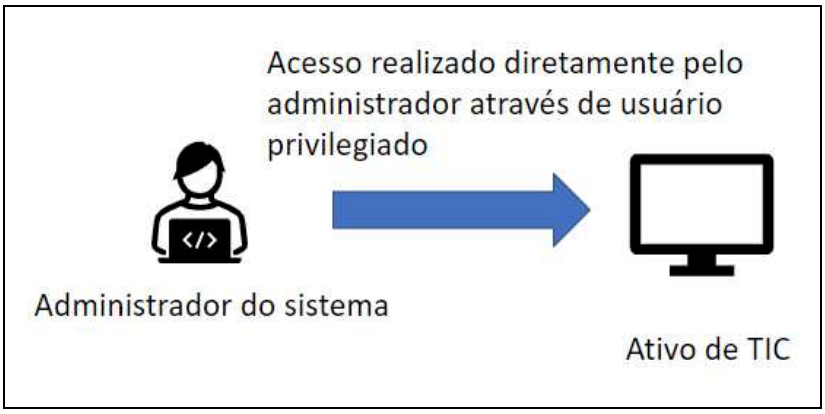
Portanto, apresentar a necessidade para o mercado através de especificações técnicas capazes de traduzir a demanda e permitir que qualquer empresa de TIC, devidamente qualificada, ofereça a sua proposta em atendimento à demanda do Tribunal com o preço mais vantajoso possível é, dentro do cenário que se apresenta, a melhor opção.

Essa estratégia irá propiciar a máxima concorrência através de diversas possibilidades de combinações de produtos de software, conforme a possibilidade de cada licitante, e reduzirá o risco de baixa eficácia e eficiência na administração dos softwares de segurança, pois todos serão responsabilidade de uma única CONTRATADA.

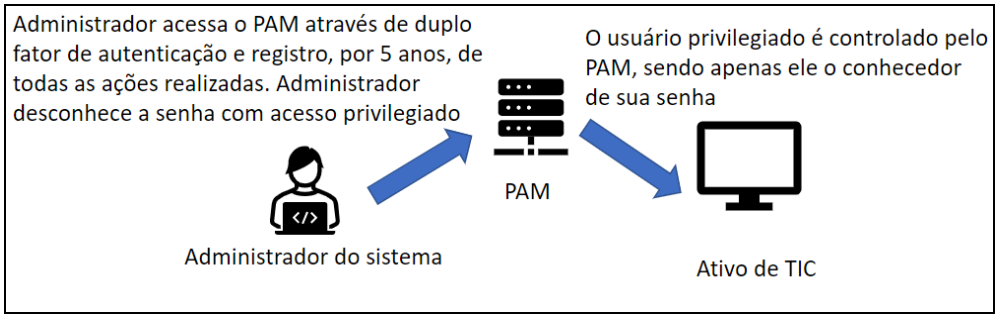
Para a solução de proteção e controle de usuários privilegiados, trata de produto de software bastante difundido no mercado e que possui nicho determinado. No entanto, há um requisito que não é ofertado pela maioria dos fabricantes: a entrega da solução em cluster de hardware.

Esse requisito da solução instalada em cluster de servidores físicos é entendido quando se compreende o funcionamento de uma solução de PAM. Uma vez instalado no ambiente de TI do Tribunal, os usuários administradores não mais terão acesso às senhas de acesso privilegiado nos dispositivos protegidos, sejam eles switches de rede ou estações de trabalho. Todo acesso será fornecido pela solução de PAM, pois ela passará a ser a conhecedora das senhas privilegiadas.

Para esclarecer, a figura abaixo mostra de forma simplificada a forma como o acesso é realizado sem um PAM:



Uma vez implementado uma solução de PAM na infraestrutura de TIC do Tribunal, muda-se a forma de acesso aos ativos conforme a figura abaixo:



Pelas descrições, percebe-se que uma vez instalado o PAM na infraestrutura de TI do Tribunal o acesso aos ativos de TIC para atividades de administração será inteiramente dependente do PAM, tornando ele um ativo crítico para o andamento das atividades realizadas em um datacenter.

Existem 4 formas costumeiras para a implementação de uma solução de PAM, são elas:

- Em *cluster* de máquinas físicas;
- Em *cluster* híbrido, com um nó físico e outro virtual;
- Em *cluster* de máquinas virtuais;
- Em nuvem pública.

Para cada implementação, foram elencadas as seguintes vantagens e desvantagens:

***Cluster* de máquinas físicas**	Vantagens: • Total independência dos ativos protegidos; • Equipamento dedicado tende a proporcionar maior desempenho.
	Desvantagens: • Maior custo entre as possíveis opções de implantação. • Tempo de implantação mais demorado.

***Cluster* híbrido, com um nó físico e outro virtual**	Vantagens: • Parte da infraestrutura, o nó físico, possui total independência dos ativos protegidos. • Há maior flexibilidade na implantação por possuir um nó virtual.
	Desvantagens: • Segundo maior custo entre as opções existentes; • Parte da solução depende de uma ativo que é protegido por ela, ou seja, ela permite o acesso de administração ao ambiente virtual, mas depende dele para garantir esse acesso. No caso de o ambiente virtual ficar inacessível, parte da solução também ficará.

***Cluster* de máquinas virtuais**	Vantagens: • Solução flexível e rápida na implantação; • Maior agilidade na evolução da solução; • Possibilidade de fazer backup da máquina inteira. • Menor custo de implantação e aquisição.
	Desvantagens: • Por ser inteiramente instalada no ambiente virtual, também é inteiramente dependente dele. Ainda que um evento raro (que já ocorreu em Tribunais da JT, como por exemplo o TST), uma falha generalizada no ambiente virtual deixaria a solução também indisponível, impossibilitando (ou criando barreira complexa) a atividades de administração para o restabelecimento da infraestrutura que se encontra em falha.

Em nuvem pública	Vantagens: • A solução mais rápida na implantação; • A que possuir a maior agilidade na evolução da solução; • Permite a proteção de ativos que se encontram fora do ambiente do Tribunal.
	Desvantagens: • É dependente do link de internet; • É dependente do firewall; • No caso de falha em qualquer um dos dois ativos citados, o acesso de administração a todos os ativos de TIC ficará prejudicado, como no caso do ambiente virtual.

Ainda que seja a opção de maior custo, considerando a experiência da equipe técnica do Tribunal com falhas graves que acarretaram a indisponibilidade de grande parte ou todo o ambiente de TIC, para uma solução onde todo o acesso a atividades de administração, que requeiram acesso privilegiado, irão depender dela, a independência de ativos de TIC é fundamental. Portanto, a opção mais segura é a mais conservadora: PAM instalado em cluster de máquinas físicas.

11. VIABILIDADE DA CONTRATAÇÃO

11.1. Descrição da solução de TI como um todo

A aquisição proposta trata de um conjunto de ferramentas de software e hardware que, em conjunto, irão elevar sobremaneira o grau de segurança do ambiente de TIC do Tribunal.

A solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*, será atendida por um conjunto de ferramentas de software que irão trabalhar juntas, sob a tutela de uma única CONTRATADA, para propiciar mecanismos de segurança, proteção, auditoria e prevenção a ameaças para todos os usuários do Tribunal e seus dados não estruturados, como arquivos em discos de rede, e-mails e arquivos em nuvem. O licenciamento proposto é no modelo de subscrição, o mais abrangente para esse tipo de solução, com vigência de 12 meses. Faz parte da solução o serviço de instalação, o suporte técnico fornecido pela CONTRATADA e fabricante por período de 12 meses, e o treinamento para uso das ferramentas.

Em complemento a solução supracitada, há a aquisição de solução de Gerenciamento de Usuários Privilegiados (PAM), que é composta por hardware dedicado com redundância, softwares especializados para a proteção de ativos de TIC e seus usuários administradores com privilégios elevados. Faz parte da solução o licenciamento no modelo perpétuo, com 12 meses de garantia e suporte especializado e o treinamento para uso da ferramenta.

11.2. Resultados pretendidos

São os resultados pretendidos:

- Aumentar o nível de atendimento e qualidade das operações de serviços de TI ao permitir aprimorar a gestão dos dados não estruturados;
- Analisar, proteger, monitorar e gerenciar a integridade das informações armazenadas e disponibilizadas no ambiente de arquivos;
- Automação de controle de privilégios aos curadores dos dados e informações;
- Classificação dos arquivos armazenados em repositórios não estruturados, mapeando onde e para quem os dados estão expostos;
- Análise comportamental dos usuários internos no ambiente computacional reduzindo os riscos de falhas de segurança, perda de informações e má gestão dos repositórios dos dados não estruturados;
- Ao permitir maior controle, visibilidade e segurança dos dados não estruturados e dos permissionamentos dos diversos usuários, é esperado um aprimoramento da governança de TI;
- Aprimorar governança de dados, informação e conhecimento;
- Aprimorar a gestão de segurança da informação e comunicações;
- Disponibilização de segurança e auditoria ininterrupta dos serviços de correio eletrônico, compartilhamento de arquivos, serviços de diretórios e *endpoints*;

- Aprimorar a gestão da informação para a tomada de decisão.

11.3. Parecer do CTINFRA – recomendação CSJT aos Tribunais

Em 2022 foi emitido parecer técnico produzido pelo Comitê Técnico de Segurança – CTSeg juntamente com o Comitê Técnico de Infraestrutura – CTInfra, comitês instituídos pelo CSJT, recomendando a aquisição dos itens da Ata de Registro de Preços PE nº 58/2021 do TST, 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.

O parecer foi encaminhado pelo Ministro Presidente do TST em 1º de junho de 2022, e informou a disponibilização de recursos orçamentários pelo CSJT para ação de adesão à ARP TST PE-058/2021, e solicitando o envio de Documento de Oficialização de Demanda Orçamentária – DDO, com os quantitativos necessários para o atendimento da demanda ao TRT24.

Esses documentos (Parecer Técnico, Ofício recebido do CSJT e DDO enviado) estão anexados no documento 4, "Processo 20549/2022 (Juntado)".

Cabe ressaltar dois pontos importantes que o parecer técnico foi explícito em seu conteúdo:

a) uma vez implementada as soluções contidas na ATA, a invasão no TRT17 poderia ter sido descoberta antes do comprometimento da infraestrutura com o monitor de comportamento dos usuários e, caso não tivesse sido, com a solução de PAM implementada o dano causado teria sido bem menor.

b) os benefícios apresentados pelo objeto da ARP conseguirão evitar crimes cibernéticos, ou reduzir grandemente suas consequências, estando corretamente implantado e operado.

No entanto, o parecer destaca que ainda persistirá a necessidade de mapear e eliminar vulnerabilidades dos sistemas - o que está fora do escopo do objeto da ARP, portanto, não fez parte dos levantamentos deste estudo, cujo foco foi validar requisitos abordados no ETP do TST, e verificar a manutenção dos preços em 2022, visto que a ARP é de 21/12/2021.

11.4. Demanda final para adesão à ARP do TST

(Art. 14, IV, "d")
(** Plano de Trabalho – item 5)

A seguir a tabela com a demanda do TRT24, resultante da análise dos quantitativos individuais e de suas respectivas justificativas.

Item	Especificação	Unidade	Qtde.
1	Licença de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	Usuários	1300
2	Licença de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados	Usuários	1300
3	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	Serviço	1
4	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	Turma	1

Item	Especificação	Unidade	Qtde.
5	Cluster para prover recursos para solução de acesso a usuários privilegiados	Cluster	1
6	Garantia do fabricante por período de 12 meses para cluster para prover recursos para solução de acesso a usuários privilegiados	Cluster	1
7	Licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, *helpdesk*)	Usuários	42
8	Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdm in/DBadmin/SysDBA, VMadmin, *helpdesk*)	Usuários	42
9	Licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores	420
10	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores	420
11	Licença para estações de trabalho Windows	Estações	1500
12	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows	Estações	1500
13	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos	170
14	Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos	170
15	Licença para aplicações conteinerizadas com *secrets*	Aplicações	25
16	Garantia do fabricante por período de 12 meses para licença para aplicações conteinerizadas com *secrets*	Aplicações	25
17	Licença para aplicações nãoconteinerizadas com senha embutida (hard coded)	Aplicações	45
18	Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (hard coded)	Aplicações	45
19	Licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	Instâncias	30
20	Garantia do fabricante por período de 12 meses para licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	Instâncias	30
21	Serviço de instalação para solução de controle de acesso de usuários privilegiados	Serviço	1
22	Treinamento para solução de controle de acesso de usuários privilegiados	Turma	1
23	Serviço e suporte técnico especializado	Mês	12

12.ANÁLISE DE CUSTOS

(Art. 14, III)

12.1. Levantamento de preços - justificativas

Para verificar os preços existentes na ARP TST PE-058/2021 e avaliar a adesão à ARP no quesito “preço de mercado”, foi enviado e-mail requisitando propostas para os principais fornecedores de soluções de segurança no mercado.

A média de preços foi obtida com a comparação de preços encontrados em ARPs, contratos de outros órgãos e de preços praticados pelo fornecedor/desenvolvedor e em contratações anteriores. Não

foram encontrados preços em sítios da internet por se tratar de produtos e serviços específicos para o ambiente corporativo.

Não existe nenhuma contratação anterior no TRT24 para comparação e precificação.

O Tratamento estatístico apresenta o resultado abaixo:

PLANILHA DE PREÇOS COM APLICAÇÃO DE TRATAMENTO ESTATÍSTICO

ITEM	QUANTIDADE	UNIDADE	ESPECIFICAÇÃO	FORNECEDOR 1	FORNECEDOR 2	FORNECEDOR 3	CONTRATO ÓRGÃO PÚBLICO 1	PREÇO MÉDIO UNITÁRIO	DESVPAD	CV	PREÇO MÉDIO TOTAL
1	1300	unid.	Licença de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.	2.153,00	*	2.091,87	*	**2.122,44**	43,23	0,020	**2.759.172,00**
2	1300	unid.	Licença de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados.	435,00	535,00	477,92	385,50	**458,36**	63,54	0,139	**595.868,00**
3	1	unid.	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.	120.000,00	110.000,00	117.599,00	95.000,00	**110.649,75**	11270,26	0,102	**110.649,75**
4	1	unid.	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.	42.000,00	*	35.335,90	*	**38.667,95**	4712,23	0,122	**38.667,95**
5	1	unid.	Cluster para prover recursos para solução de acesso a usuários privilegiados	324.200,00	372.000,00	300.098,00	249.500,00	**311.449,50**	50975,60	0,164	**311.449,50**
6	1	unid.	Garantia do fabricante por período de 12 meses para cluster para prover recursos para solução de acesso a usuários privilegiados	64.840,00	*	59.122,23	*	**61.981,12**	4043,07	0,065	**61.981,12**
7	42	unid.	Licença para contas para acesso privilegiados simultâneos (admin/segurança/rede/Root/DomainAdmin/DBadmin/ SysDBA, VMadmin, helpdesk)	1.625,00	2.150,00	1.694,31	1.405,00	**1.718,58**	312,94	0,182	**72.180,36**
8	42	unid.	Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiados simultâneos (admin/segurança/rede/Root/DomainAdmin/DBadmin/ SysDBA, VMadmin, helpdesk)	325,00	*	350,35	291,93	**322,43**	29,29	0,091	**13.542,06**
9	420	unid.	Licença para servidores físicos e virtuais (Linux, Windows e Storages)	57,45	*	54,98	*	**56,22**	1,75	0,031	**23.612,40**
10	420	unid.	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages)	11,49	*	12,22	*	**11,86**	0,52	0,044	**4.981,20**
11	1500	unid.	Licença para estações de trabalho Windows	17,85	*	17,99	*	**17,92**	0,10	0,006	**26.880,00**
12	1500	unid.	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows	*	*	5,01	4,18	**4,60**	0,59	0,128	**6.900,00**
13	170	unid.	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	27,50	*	28,04	*	**27,77**	0,38	0,014	**4.720,90**
14	170	unid.	Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	5,50	*	5,35	4,55	**5,13**	0,51	0,100	**872,10**
15	25	unid.	Licença para aplicações conteinerizadas com secrets	7.100,00	9.350,00	8.109,00	6.840,00	**7.849,75**	1140,13	0,145	**196.243,75**
16	25	unid.	Garantia do fabricante por período de 12 meses para licença para aplicações conteinerizadas com secrets	*	*	1.925,99	1.603,75	**1.764,87**	227,86	0,129	**44.121,75**
17	45	unid.	Licença para aplicações não-conteinerizadas com senha embutida (hard coded)	1.740,00	*	1.904,92	1.589,00	**1.744,64**	158,01	0,091	**78.508,80**
18	45	unid.	Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (hard coded)	348,00	*	389,04	332,05	**356,36**	29,40	0,083	**16.036,20**
19	30	unid.	Licença para instancias de Banco de Dados (Oracle, Postgres, MS-SQL e MySQL)	1.100,00	1.450,00	1.282,45	1.044,00	**1.219,11**	184,55	0,151	**36.573,30**
20	30	unid.	Garantia do fabricante por período de 12 meses para licença para instancias de Banco de Dados (Oracle, Postgres, MS-SQL e MySQL)	220,00	*	269,22	223,24	**237,49**	27,53	0,116	**7.124,70**
21	1	unid.	Serviço de instalação para solução de controle de acesso de usuários privilegiados.	74.200,00	*	53.599,00	*	**63.899,50**	14567,11	0,228	**63.899,50**
22	1	unid.	Treinamento para solução de controle de acesso de usuários privilegiados.	*	29.500,00	19.400,00	*	**24.450,00**	7141,78	0,292	**24.450,00**
23	12	unid.	Serviço e suporte técnico especializado	18.000,00	14.000,00	15.092,00	12.090,00	**14.795,50**	2470,44	0,167	**177.546,00**
DESPESA TOTAL ESTIMADA											**4.675.981,34**

12.2. Preços totais ARP PE-58/2021 do TST

Considerando os valores individuais registrados na ARP TST PE-058/2021, e a expectativa de aquisição por parte deste Regional, a estimativa de custo para o TRT24 é a seguinte:

Item	Especificação	Unidade	Qtde.	Valor Unitário	Valor para pagamento em 2022	Valor para pagamento em 2023
1	Licença de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	Usuários	1300	R$1.735,50	R$2.256.150,00	
2	Licença de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados	Usuários	1300	R$385,50	R$501.150,00	
3	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	Serviço	1	R$95.000,00	R$95.000,00	
4	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	Turma	1	R$29.000,00	R$29.000,00	
5	Cluster para prover recursos para solução de acesso a usuários privilegiados	Cluster	1	R$249.500,00	R$249.500,00	
6	Garantia do fabricante por período de 12 meses para cluster para prover recursos para solução de acesso a usuários privilegiados	Cluster	1	R$49.094,43	R$49.094,43	
7	Licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, *helpdesk*)	Usuários	42	R$1.405,00	R$59.010,00	
8	Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, *helpdesk*)	Usuários	42	R$291,93	R$12.261,06	
9	Licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores	420	R$45,73	R$19.206,60	
10	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores	420	R$9,57	R$4.019,40	
11	Licença para estações de trabalho Windows	Estações	1500	R$14,41	R$21.615,00	

12	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows	Estações	1500	R$4,18	R$6.270,00	
13	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos	170	R$23,30	R$3.961,00	
14	Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos	170	R$4,55	R$773,50	
15	Licença para aplicações conteinerizadas com *secrets*	Aplicações	25	R$6.840,00	R$171.000,00	
16	Garantia do fabricante por período de 12 meses para licença para aplicações conteinerizadas com *secrets*	Aplicações	25	R$1.603,75	R$40.093,75	
17	Licença para aplicações nãoconteinerizadas com senha embutida (hard coded)	Aplicações	45	R$1.589,00	R$71.505,00	
18	Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (hard coded)	Aplicações	45	R$332,05	R$14.942,25	
19	Licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	Instâncias	30	R$1.044,00	R$31.320,00	
20	Garantia do fabricante por período de 12 meses para licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	Instâncias	30	R$223,24	R$6.697,20	
21	Serviço de instalação para solução de controle de acesso de usuários privilegiados	Serviço	1	R$44.900,00	R$44.900,00	
22	Treinamento para solução de controle de acesso de usuários privilegiados	Turma	1	R$16.000,00	R$16.000,00	
23	Serviço e suporte técnico especializado	Mês	12	R$12.090,00	R$48.360,00	R$96.720,00
				Total anual	**R$3.751.829,19**	**R$96.720,00**

O valor final na ARP ficou abaixo da planilha com tratamento estatístico, em cerca de 18%, mostrando-se compatível com o mercado e adequado para contratação pelo TRT24.

13. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

(Art. 14, IV, 'a')
(** Plano de Trabalho – item 7)

A solução escolhida, motivada por recomendação do CSJT, com demonstração da vantajosidade financeira, é a contratação da empresa detentora da **ARP TST PE-058/2021**, para aquisição de licenças e subscrições de softwares e serviços de suporte, monitoramento, implantação e treinamento. A empresa detentora da ARP, JAMC Consultoria e Representação de Software Ltda., já manifestou interesse na contratação com o TRT24 (doc.15).

Juntado aos autos do processo da contratação, no documento de nº 11, encontra-se detalhado o atendimento dos produtos incluídos da ARP PE-58/2021 do TST para a Portaria 162.

A aquisição proposta trata de um conjunto de ferramentas de software e hardware que, em conjunto, irão elevar sobremaneira o grau de segurança do ambiente de TIC do Tribunal.

A solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoints*, será atendida por um conjunto de ferramentas de software que irão trabalhar juntas, sob a tutela de um único fornecedor, para propiciar mecanismos de segurança, proteção, auditoria e prevenção a ameaças para todos os usuários do Tribunal e seus dados não estruturados, como arquivos em discos de rede, e-mails e arquivos em nuvem. O licenciamento proposto é no modelo de subscrição, o mais abrangente para esse tipo de solução, com vigência de 12 meses. Faz parte da solução o serviço de instalação, o suporte técnico fornecido pela contratada e fabricante por período de 12 meses, e o treinamento para uso das ferramentas.

Em complemento à solução supracitada, há a aquisição de solução de Gerenciamento de Usuários Privilegiados (PAM), que é composta por hardware dedicado com redundância, softwares especializados para a proteção de ativos de TIC e seus usuários administradores com privilégios elevados. Faz parte da solução o licenciamento no modelo perpétuo, com 12 meses de garantia e suporte especializado e o treinamento para uso da ferramenta.

14.REQUISITOS DA CONTRATAÇÃO

Os requisitos da minuta de contrato do edital do TST atendem às necessidades técnicas, gerenciais e de fiscalização contratual pretendidas pela SETIC/TRT24.

III. SUSTENTAÇÃO DO CONTRATO

(Art. 12, § 1º, 'II' e Art. 15)

1. RECURSOS FINANCEIROS

(** Plano de Trabalho – item 3)

Os recursos financeiros serão disponibilizados pelo CSJT por nota de crédito, conforme valores já autorizados e informados à Secretaria de Orçamento e Finanças, relativos à fonte "02.122.0571.4256.0054 - Apreciação de Causas na Justiça do Trabalho - No Estado de Mato Grosso do Sul", do programa orçamentário "PO 0001 - Manutenção e Gestão dos Serviços e Sistemas de Tecnologia da Informação".

2. AMBIENTE DE INSTALAÇÃO

(Art. 15, I)

2.1. Adequação à Política de Segurança da Informação

A solução encontrada é compatível com o serviço atualmente prestado ao TRT24 e atende às normas definidas pela Política de Segurança da Informação.

2.2. Recursos materiais e humanos

Para essa contratação não serão alocados recursos materiais adicionais além dos já utilizados atualmente pela Seção de Infraestrutura de TI, Seção de Segurança da Informação do TRT24 e Central de Atendimento. As necessidades referentes à configuração do ambiente e repasse de conhecimentos já estão previstos nos requisitos técnicos desta contratação.

2.3. Providências para adequação do ambiente do órgão

Para a solução de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoints*, ela deverá ser compatível com a infraestrutura de TIC do Tribunal. Portanto, as especificações constantes no termo de referência deverão contemplar a compatibilidade com sua a infraestrutura.

Quanto a solução de controle de acesso privilegiado, será necessário realizar alterações na forma como os acessos privilegiados são concedidos aos diversos ativos de TIC. Considerando as diversas formas possíveis de implementar esse tipo de solução, caberá à CONTRATADA, no momento da instalação, realizar as parametrizações necessárias para adequação da solução ao ambiente do Tribunal.

Para garantir a desejada plena independência da solução quanto aos ativos de infraestrutura onde ela administra seus usuários privilegiados, o switch de rede onde o cluster será instalado não poderá ser administrado por ela.

2.4.Plano de implantação

O cronograma a ser seguido para a instalação da solução do Grupo 1 será conforme tabela abaixo:

Etapa	Descrição	Prazo Máximo	Marco Temporal
1	Entrega das licenças	5 dias úteis	Assinatura do contrato
2	Reunião de planejamento da instalação	10 dias	Assinatura do contrato
3	Entrega do plano de instalação	15 dias	Reunião de planejamento da instalação
4	Conclusão da instalação	45 dias	Entrega do plano de instalação

O cronograma a ser seguido para a execução do treinamento das soluções dos Grupos 1 e 2 será conforme tabela abaixo:

Etapa	Descrição	Prazo Máximo	Marco Temporal
1	Reunião de planejamento do treinamento	10 dias	Assinatura do contrato
2	Conclusão do treinamento	45 dias	Reunião de planejamento do treinamento

O cronograma a ser seguido para a instalação da solução do Grupo 2 será conforme tabela abaixo:

Etapa	Descrição	Prazo Máximo	Marco Temporal
1	Reunião de planejamento da instalação	10 dias	Assinatura do contrato
2	Entrega do plano de instalação	15 dias	Reunião de planejamento da instalação
3	Entrega do cluster e das licenças	45 dias	Assinatura do contrato
4	Conclusão da instalação	45 dias	Entrega do cluster e das licenças

A CONTRATADA deverá apresentar Plano de Instalação da Solução detalhando os aspectos da instalação e configuração dos componentes, migração do ambiente de produção, incluindo, no mínimo:

- Detalhamento do Escopo.
- Descrição de atividades em cada etapa do projeto.

- Cronograma de atividades.
- Definição de responsabilidades.
- Pontos de controle.
- Descrição detalhada dos componentes.
- No caso do Grupo 2: Documentação a ser entregue, incluindo todos os detalhes das instalações a serem realizadas, deverá apresentar informações para procedimentos, incluindo comandos e testes aplicáveis, procedimentos de inicialização e procedimentos de configuração.
- Requisitos necessários.

O cronograma deverá contar o prazo em dias corridos para a execução dos serviços e atividades projetadas.

O plano poderá ter propostas de alteração do CONTRATANTE, devendo ser executado somente após a aprovação deste.

3. CONTINUIDADE DO FORNECIMENTO

(Art. 15, II)

Durante a vigência do contrato as necessidades serão mantidas e preservadas pelas cláusulas contratuais.

Caso surjam problemas contratuais, devem ser tomadas as medidas legais previstas nos contratos assinados e na Lei 8.666/1990, conforme os casos.

3.1. Recursos necessários para continuidade de negócio durante e após a contratação

A solução prevista no Grupo 1 não acresce dependência a continuidade de negócio, ou seja, ainda que a descontinuidade da solução prejudique o nível de segurança alcançado após a sai implantação, nenhum serviço crítico ao negócio irá deixar de funcionar. No entanto, para preservar a continuidade dos processos de segurança da informação após a implantação da ferramenta, entre as especificações técnicas deverá ser exigido que os softwares envolvidos na solução não poderão perder suas funcionalidades caso as subscrições vençam.

Para a solução do Grupo 2, como ela irá gerar dependência na infraestrutura de TIC, é preciso definir mecanismos para continuidade do negócio caso o contrato seja suspenso. Para tanto, as especificações técnicas deverão, assim como o Grupo 1, exigir que a solução permaneça operando mesmo se um contrato de suporte vigente.

3.2. Elementos necessários à continuidade do fornecimento da solução

Deverá se requisito das soluções a serem contratadas que elas não poderão deixar de funcionar em eventual suspensão ou não continuidade dos serviços de subscrição.

4. TRANSIÇÃO CONTRATUAL E ENCERRAMENTO DO CONTRATO

(Art. 15, III)

Após todas as possibilidades legais de prorrogação contratual, será necessário realizar nova licitação. Se a CONTRATADA não sagrar vencedora do certame, em até 30 dias antes do vencimento do contrato vigente, a CONTRATADA deverá disponibilizar para download todo e qualquer dado armazenado, em formato padrão de mercado, para que seja realizado a migração destes para a nova solução. Na nova licitação será necessário considerar o custo de migração, que deverá ficar sob responsabilidade da nova CONTRATADA.

4.1. Entrega de produtos finais

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

4.2. Transferência de conhecimentos

Será realizado na implantação da solução, durante o treinamento.

4.3. Devolução de recursos materiais

Todo material adquirido será de propriedade do Tribunal. A devolução não se aplica nesse caso.

4.4. Revogação de perfis de acessos

Os acessos remotos relacionados ao suporte técnico serão revogados assim que as atividades sejam concluídas.

4.5. Direitos de propriedade intelectual

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

5. INDEPENDÊNCIA DA EMPRESA CONTRATADA

(Art. 15, IV)

A dependência da empresa se deve ao tipo de serviço fornecido no monitoramento, permanecendo durante todo o contrato, e cuja transferência segue os requisitos do item anterior.

IV. ESTRATÉGIA PARA A CONTRATAÇÃO

(Art. 12, § 1º, 'III' e Art. 16)

1. NATUREZA DO OBJETO

(Art. 16, I)

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

A contratação da empresa fornecedora de equipamentos e serviços se dará por meio de adesão à ARP TST PE-58/2021.

2. PARCELAMENTO DO OBJETO

(Art. 16, II)

2.1 Justificativas para o parcelamento ou não da solução

Em conjunto, as soluções irão atender as necessidades técnicas e de negócio para aprimorar o nível de segurança de TIC do Tribunal. Por se tratar de produtos com nicho de mercado distintos, o processo licitatório foi dividido em grupos distintos para que seja garantida a competividade da licitação para cada nicho de mercado. Cada nicho divido em grupos distintos, Grupo 1 e Grupo 2.

Conforme explanado no Estudo Técnico Preliminar do TST, a solução para o Grupo 1 envolve uma quantidade não conhecida de produtos de softwares, portanto, é preciso que a mesma licitante que oferte esses produtos como uma solução, os suporte, sob risco de impossibilidade de execução contratual. A divisão possível de itens é o licenciamento conforme tipo de necessidade, serviço de instalação e treinamento.

Todos os itens foram vinculados na ARP, pois a empresa que vender a licença de uma solução cujos componentes de software não são previamente conhecidos pelo Tribunal, deverá ser a mais capacitada para instalar a solução e realizar treinamento. Não há possibilidade de se adquirir um conjunto de softwares com base em um conjunto de necessidades, sem conhecimento prévio de quais softwares são, e esperar que outra licitante suporte os softwares e realize o treinamento.

Quanto ao Grupo 2, o hardware, as licenças, a instalação, o treinamento e o serviço de suporte técnico são intrínsecos. Nem mesmo o hardware, que poderá ser adquirido em separado pela licitante, pode ser desvinculado da solução como um todo, pois cabe a licitante que ofertará as licenças para a solução dimensionar o hardware conforme os requisitos de desempenho para seu produto de software. Mesma lógica para o serviço de instalação, treinamento e suporte técnico.

3. ADJUDICAÇÃO DO OBJETO

(Art. 16, III)

A adjudicação do objeto será global para cada Grupo, de forma que os produtos formem um conjunto único, compatíveis em marca e modelo e projeto. Sendo sugerido neste ETP a contratação conforme os moldes da ARP PE-58/2021 do TST.

4. TIPO DE LICITAÇÃO OU MODALIDADE DE CONTRATAÇÃO

(Art. 16, IV)
(** Plano de Trabalho – item 2)

Contratação dos itens da ARP PE-58/2021 do Tribunal Superior do Trabalho, em regime de adesão, conforme itens da tabela abaixo:

Item	Especificação	Unidade	Qtd	Valor Unitário	Valor para pagamento em 2022	Valor para pagamento em 2023
1	Licença de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	Usuários – Pagamento único	1300	R$1.735,50	R$2.256.150,00	
2	Licença de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados	Usuários – Pagamento único	1300	R$385,50	R$501.150,00	
3	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	Serviço – Pagamento único	1	R$95.000,00	R$95.000,00	
4	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	Turma – Pagamento único	1	R$29.000,00	R$29.000,00	
5	Cluster para prover recursos para solução de acesso a usuários privilegiados	Cluster – Pagamento único	1	R$249.500,00	R$249.500,00	
6	Garantia do fabricante por período de 12 meses para cluster para prover recursos para solução de acesso a usuários privilegiados	Cluster – Pagamento único	1	R$49.094,43	R$49.094,43	
7	Licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, *helpdesk*)	Usuários – Pagamento único	42	R$1.405,00	R$59.010,00	

Item	Especificação	Unidade	Qtd	Valor Unitário	Valor para pagamento em 2022	Valor para pagamento em 2023
8	Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, *helpdesk*)	Usuários – Pagamento único	42	R$291,93	R$12.261,06	
9	Licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores – Pagamento único	420	R$45,73	R$19.206,60	
10	Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages)	Servidores – Pagamento único	420	R$9,57	R$4.019,40	
11	Licença para estações de trabalho Windows	Estações – Pagamento único	1500	R$14,41	R$21.615,00	
12	Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows	Estações – Pagamento único	1500	R$4,18	R$6.270,00	
13	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos – Pagamento único	170	R$23,30	R$3.961,00	
14	Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	Equipamentos – Pagamento único	170	R$4,55	R$773,50	
15	Licença para aplicações conteinerizadas com *secrets*	Aplicações – Pagamento único	25	R$6.840,00	R$171.000,00	
16	Garantia do fabricante por período de 12 meses para licença para aplicações conteinerizadas com *secrets*	Aplicações – Pagamento único	25	R$1.603,75	R$40.093,75	
17	Licença para aplicações nãoconteinerizadas com senha embutida (hard coded)	Aplicações – Pagamento único	45	R$1.589,00	R$71.505,00	
18	Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (hard coded)	Aplicações – Pagamento único	45	R$332,05	R$14.942,25	
19	Licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	Instâncias – Pagamento único	30	R$1.044,00	R$31.320,00	
20	Garantia do fabricante por período de 12 meses para licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	Instâncias – Pagamento único	30	R$223,24	R$6.697,20	
21	Serviço de instalação para solução de controle de acesso de usuários privilegiados	Serviço – Pagamento único	1	R$44.900,00	R$44.900,00	

Item	Especificação	Unidade	Qtd	Valor Unitário	Valor para pagamento em 2022	Valor para pagamento em 2023
22	Treinamento para solução de controle de acesso de usuários privilegiados	Turma – Pagamento único	1	R$16.000,00	R$16.000,00	
23	Serviço e suporte técnico especializado	Mês – Pagamento Mensal	12	R$12.090,00	R$48.360,00	R$96.720,00
				Total anual	**R$3.751.829,19**	**R$96.720,00**

5. CLASSIFICAÇÃO ORÇAMENTÁRIA

(Art. 16, V)
(** Plano de Trabalho – item 8)

Item ARP	Elemento de Despesa	Forma de Pagamento	Valor para pagamento em 2022	Valor para pagamento em 2023
1 - Licença de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	3.3.90.40.07	Parcela única	R$2.256.150,00	
2 - Licença de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados	3.3.90.40.07	Parcela única	R$501.150,00	
3 - Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	3.3.90.40.21	Parcela única	R$95.000,00	
4 - Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e *endpoint*	3.3.90.40.20	Parcela única	R$29.000,00	
5 - Cluster para prover recursos para solução de acesso a usuários privilegiados	4.4.90.40.05	Parcela única	R$249.500,00	
6 - Garantia do fabricante por período de 12 meses para cluster para prover recursos para solução de acesso a usuários privilegiados	3.3.90.40.07	Parcela única	R$49.094,43	
7 - Licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, *helpdesk*)	4.4.90.40.05	Parcela única	R$59.010,00	
8 - Garantia do fabricante por período de 12 meses para licença para contas para acesso privilegiados simultâneos (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, *helpdesk*)	3.3.90.40.07	Parcela única	R$12.261,06	
9 - Licença para servidores físicos e virtuais (Linux, Windows e Storages)	4.4.90.40.05	Parcela única	R$19.206,60	
10 - Garantia do fabricante por período de 12 meses para licença para servidores físicos e virtuais (Linux, Windows e Storages)	3.3.90.40.07	Parcela única	R$4.019,40	
11 - Licença para estações de trabalho Windows	4.4.90.40.05	Parcela única	R$21.615,00	

Item ARP	Elemento de Despesa	Forma de Pagamento	Valor para pagamento em 2022	Valor para pagamento em 2023
12 - Garantia do fabricante por período de 12 meses para licença para estações de trabalho Windows	3.3.90.40.07	Parcela única	R$6.270,00	
13 - Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	4.4.90.40.05	Parcela única	R$3.961,00	
14 - Garantia do fabricante por período de 12 meses para licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN (Switch, Roteadores, Firewall e Controladoras WIFI, VOIP)	3.3.90.40.07	Parcela única	R$773,50	
15 - Licença para aplicações conteinerizadas com *secrets*	4.4.90.40.05	Parcela única	R$171.000,00	
16 - Garantia do fabricante por período de 12 meses para licença para aplicações conteinerizadas com *secrets*	3.3.90.40.07	Parcela única	R$40.093,75	
17 - Licença para aplicações nãoconteinerizadas com senha embutida (hard coded)	4.4.90.40.05	Parcela única	R$71.505,00	
18 - Garantia do fabricante por período de 12 meses para licença para aplicações não-conteinerizadas com senha embutida (hard coded)	3.3.90.40.07	Parcela única	R$14.942,25	
19 - Licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	4.4.90.40.05	Parcela única	R$31.320,00	
20 - Garantia do fabricante por período de 12 meses para licença para instancias de Banco de Dados (Oracle, Postgres, MSSQL e MySQL)	3.3.90.40.07	Parcela única	R$6.697,20	
21 - Serviço de instalação para solução de controle de acesso de usuários privilegiados	3.3.90.40.21	Parcela única	R$44.900,00	
22 - Treinamento para solução de controle de acesso de usuários privilegiados	3.3.90.40.20	Parcela única	R$16.000,00	
23 - Serviço e suporte técnico especializado	3.3.90.40.07	Mensal	R$48.360,00	R$96.720,00
		Total anual	**R$3.751.829,19**	**R$96.720,00**

6. VIGÊNCIA

(Art. 16, VI)

O contrato terá vigência de 12 (doze) meses, contados a partir da data de sua assinatura, sem prejuízo das garantias contratuais previstas, na forma disposta no artigo 57, inciso IV, da Lei N° 8.666/1993.

7. EQUIPE DE APOIO À CONTRATAÇÃO

(Art. 16, VII)

Conforme Portaria TRT/GP/DGCA Nº 89/2021:

a) Representante do Integrante Demandante: Geslaine Perez Maquerte, e em sua ausência, Alexandre Rosa Camy;

b) Integrante Técnico: Erick Takahashi, e em sua ausência, Fabio Nogueira da Silva;

c) Integrante Administrativo: Paulo Sergio Petri, e em sua ausência Camilo Gama da Silva.

8. EQUIPE DE GESTÃO DA CONTRATAÇÃO

(Art. 16, VIII)

Conforme Resolução 182/2013, do CNJ:

Gestor do Contrato: Geslaine Perez Maquerte, e em suas ausências, Alexandre Rosa Camy;

Fiscal Demandante: Fabio Nogueira da Silva, e em suas ausências, Erick Takahashi;

Fiscal Técnico: Erick Takahashi e em suas ausências, Fábio Nogueira da Silva;

Fiscal Administrativo: Camilo Gama da Silva, e em suas ausências, Pedro Villegas Araújo.

Em caso de conflito de atribuições previstas na Resolução 182/2013 do CNJ, com as normas internas do TRT24, os nomes acima indicados devem ser adequados para realizar as atribuições previstas na primeira, ou de norma que vier a substituí-la, em especial quanto aos procedimentos de recebimento provisório e definitivo e preparo e autorização dos pagamentos dos serviços contratados.

V. ANÁLISE DE RISCOS

(Art. 12, § 1º, 'IV')

1. AÇÕES PREVISTAS PARA REDUZIR OU ELIMINAR OS RISCOS

(Art. 17, I a V)

O projeto de aquisição consta do portfólio de TIC, por essa razão, tem os riscos inerentes às ações geridas pela SETIC, e está sendo gerenciado com auxílio do escritório de projetos.

Durante a execução do contrato, é parte dos processos de trabalho da Segurança da Informação, com destaque para o processo de Gestão de Riscos.

Os riscos classificados como extremos tiveram ações para mitigação previstas neste Estudo Técnico Preliminar.

RISCO			ANÁLISE DO RISCO				CONTROLE						RESPOSTA AO RISCO		
Fase da Contratação	Risco	Consequência	Impacto	Probabilidade	Risco Inerente (Impacto X Probabilidade)	Nível de Risco	Medida de Controle	Responsável	Eficácia do Controle	Multiplicador do Risco Inerente	Risco Inerente	Nível de Risco	Resposta ao Risco	Ações de contingência	Responsável
Planejamento	Atraso na contratação da solução	Riscos de Crime Cibernético	4	4	16	Extremo	Acompanhamento da infraestrutura para bloqueios de atividades suspeitas	DITI e DPDSEG	Fraco	0,8	3,2	Alto	Reduzir	Ativação do SysPass, Aumento de controles de 2FA, Maior rigor na atualização de softwares, eliminação de softwares com vulnerabilidade	DPDSEG
Planejamento	Falta de recursos orçamentários	Encerramento ou adiamento da demanda	5	1	5	Médio	Solicitar liberação de recursos em caráter de urgência. Esse serviço é essencial para a Segurança	SETIC	Satisfatório	0,4	2	Médio	Evitar	Encaminhar para o CSJT para urgente liberação de recursos	SETIC

RISCO			ANÁLISE DO RISCO				CONTROLE						RESPOSTA AO RISCO		
Fase da Contratação	Risco	Consequência	Impacto	Probabilidade	Risco Inerente (Impacto X Probabilidade)	Nível de Risco	Medida de Controle	Responsável	Eficácia do Controle	Multiplicador do Risco Inerente	Risco Inerente	Nível de Risco	Resposta ao Risco	Ações de contingência	Responsável
Problemas na instrução do processo	Atraso na contratação da solução	Riscos de Crime Cibernético	5	3	15	Extremo	Acompanhamento da infraestrutura para bloqueios de atividades suspeitas	DITI e DPDSEG	Fraco	0,8	3,2	Alto	Reduzir	Ativação do SysPass, Aumento de controles de 2FA, Maior rigor na atualização de softwares, eliminação de softwares com vulnerabilidade	DPDSEG
Gestão do contrato	Atraso na entrega da solução	Não entrega do produto/serviço demandado;	4	2	8	Alto	1. Definir prazos em conjunto com fornecedores. 2.Definir penalidades que inibam atrasos	DPDSEG	Satisfatório	0,4	3,2	Médio	Compartilhar	1.Aguardar as justificativas apresentadas pela empresa e encaminhar para deliberação superior; 2. Sugerir a aplicação das penalidades contratuais.	SETIC, Secretaria administrativa e Diretoria Geral
Gestão do contrato	Instalação/configuração insatisfatória	Indisponibilidade ou ineficiência na execução do serviço	4	1	4	Médio	1. Definir penalidades para inibir instalação/configuração insatisfatória da solução. 2.Exigir configuração com equipe presencial, caso necessário.	SETIC	Mediano	0,6	2,4	Médio	Compartilhar	1.Aguardar as justificativas apresentadas pela empresa e encaminhar para deliberação superior; 2.Sugerir a aplicação das penalidades contratuais; 3.Rescindir o contrato em casos extremos.	SETIC, Secretaria administrativa e Diretoria Geral
Encerramento do contrato	Impossibilidade de renovação	Riscos de Crime Cibernético	4	4	16	Extremo	Acompanhamento da infraestrutura para bloqueios de atividades suspeitas	DITI e DPDSEG	Fraco	0,8	3,2	Alto	Reduzir	Manutenção do Senah Segura em Funcionamento, Aumento de controles de 2FA, Maior rigor na atualização de softwares, eliminação de softwares com vulnerabilidade	DPDSEG

VI. INTEGRANTES E APROVAÇÃO

1. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Geslaine Perez Maquerte Integrante técnico	Documento assinado digitalmente pelo PROAD
Erick Takahashi Integrante técnico	Documento assinado digitalmente pelo PROAD
Fábio Nogueira da Silva Integrante técnico	Documento assinado digitalmente pelo PROAD
Paulo Sergio Petri Integrante administrativo	Documento assinado digitalmente pelo PROAD

2. EQUIPE DE GESTÃO E FISCALIZAÇÃO

Geslaine Perez Maquerte Gestor	Documento assinado digitalmente pelo PROAD
Alexandre Rosa Camy Gestor Substituto	Documento assinado digitalmente pelo PROAD
Erick Takahashi Fiscal técnico Fiscal demandante substituto	Documento assinado digitalmente pelo PROAD
Fábio Nogueira da Silva Fiscal demandante Fiscal técnico substituto	Documento assinado digitalmente pelo PROAD
Camilo Gama da Silva Fiscal administrativo	Documento assinado digitalmente pelo PROAD
Pedro Villegas Araújo Fiscal administrativo substituto	Documento assinado digitalmente pelo PROAD

3. REVISÃO

Gleison Amaral dos Santos Setor de Apoio a Contratações de TIC	Documento assinado digitalmente pelo PROAD

4. APROVAÇÃO DA SETIC

Alexandre Rosa Camy Secretário de TIC	Documento assinado digitalmente pelo PROAD

Campo Grande, 27 de setembro de 2022.