

Estudos Preliminares
Tribunal Regional Eleitoral de São Paulo
Estudos Preliminares - v. 2.2

1 – Identificação do Estudo Preliminar

Este estudo visa atender à Estratégia de Cibersegurança da Justiça Eleitoral com a contratação de ferramenta de Gestão de Ativos de Tecnologia da Informação e Patches de Segurança, de acordo com a definição dos requisitos deste EP, incluindo serviços de implantação da solução, repasse de conhecimento, atualizações das licenças e suporte.

A contratação será feita em conjunto com os Tribunais Regionais Eleitorais que tiverem interesse na participação, sendo que a licitação deverá ser realizada pelo TRE-SP.

2 – Análise de Viabilidade da Contratação

2.1 – Definição e a especificação dos requisitos

A contratação visa atender às necessidades de vários Tribunais Regionais Eleitorais, bem como do Tribunal Superior Eleitoral. Foi realizada—consulta inicial com cada Tribunal, objetivando o entendimento das necessidades e particularidades de cada um, sendo identificado o seguinte cenário:

- a) Tribunais que já possuem solução de Gestão de Ativos e gostariam de adquirir somente a solução de Gestão de Patches;
- b) Tribunais que já possuem solução de Gestão de Patches e gostariam de adquirir somente a solução de Gestão de Ativos;
- c) Tribunais que não possuem a solução de Gestão de Ativos e de Patches;
- d) Tribunais que necessitam da Solução de gerenciamento de ativos e patches com suporte a VPRO.

Ademais, constatou-se ainda que algumas soluções serão contratadas com instalação local e outras em nuvem (*Cloud Computing*)

Desta forma, propõe-se a aquisição em 5 formatos de licenciamento, onde se prevê contratação de serviço em *Cloud Computing* (nuvem), licenças permanentes e a possibilidade de aquisição por módulos.

Obs.: *Cloud Computing* (computação em nuvem): onde os serviços e recursos de TI são fornecidos remotamente, mantidos em um Data Center externo, sob a responsabilidade da equipe técnica do provedor da nuvem.

2.1.1 - Objeto da Gestão de Ativos de Tecnologia da Informação e Patches de Segurança

a) Ativos a serem gerenciados:

Microcomputador (estações e servidores localizados nas Secretarias dos Tribunais, Cartórios Eleitorais, em teletrabalho e trabalho remoto com acesso por VPN), usuários (contas), impressoras, Switches, Access Point Wireless e qualquer outro software e equipamento (ou Itens de Configuração – ICs) de TI possível ser conectado à rede de dados e acessado via protocolo SNMP, SSH ou IPMI, homologados pelo fabricante da solução.

b) Versões mínimas de Sistemas Operacionais a serem inventariados e gerenciados pela Solução de Gestão de Ativos:

Windows 8.1,—Windows 10, Windows 11, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Embedded Standard/Enterprise 7, Windows Embedded POSReady 7, Windows Embedded 8.1, Windows 10 IoT Enterprise y Mac OS X 10.15.x, 11.0.1, 11+ M1 CPU ,12.0.1, LINUX SuSE, Red Hat, Centos, Ubuntu, Solaris 10, Solaris 11, OracleLinux, Raspbian 10 e versões superiores de todos os listados.

c) Versões mínimas de Sistemas Operacionais gerenciados pela Solução de Gestão de Patch:

Sistemas operacionais Windows 10 e 11; Windows Server, 2012, 2012 R2, 2016, 2019.

Deve oferecer suporte à aplicação de patches em pelo menos três das distribuições Linux, a seguir: Ubuntu, Debian, Cent OS, Red Hat, Suse Linux, Oracle Linux e Amazon Linux

2.1.2 Requisitos Gerais – para todas as Soluções (Gestão de Ativos e Patches e Gestão de Patches):

1 – O licenciamento dos softwares deverá ser por equipamento gerenciado;

2 – Recomenda-se a adoção das boas práticas, funções e processos definidos no framework (estrutura de processos) do ITIL Versão 3 (ITIL v3) para gerenciamento de Serviços de TI.

3 – Segurança:

O acesso ao console de gerenciamento das soluções, por todos os usuários, deverá ocorrer por duplo fator de autenticação (2FA), com o registro de acessos para fins de auditoria.

Toda e qualquer informação coletada ou trafegada nas soluções não poderão ser fornecidas a agentes externos e/ou divulgadas na internet, sem o consentimento dos Tribunais.

Caso possua agente instalado nos ativos de TI, não pode utilizar o compartilhamento administrativo do Windows (C\$, D\$, etc).

Deverá ter a capacidade de atribuir diferentes níveis de privilégios aos usuários, ou grupo de usuários, para acesso às funções e recursos das soluções.

Deve permitir um controle de acesso diferenciado para os usuários, incluindo: visões, acessos, privilégios e permissões. Além de permitir a configuração do perfil dos usuários, como administrador e operador

Deverá permitir a integração com o *Active Directory* do Tribunal.

A comunicação do agente (se houver), deve ocorrer por meio de protocolos seguros como HTTPS, SSH ou equivalentes.

4 – As soluções, caso desenvolvidas para plataforma web, devem possuir compatibilidade com navegadores de mercado, incluindo Chrome e Firefox.

5 – As soluções devem ser distribuídas em português e/ou inglês (inclusive manuais e help on-line).

6 – Deverá ofertar documentação do software que inclua detalhamento do processo de instalação, manual de usuário, ajuda online integrada, tutoriais, etc.

2.1.3 Solução de Gerenciamento de Ativos e Patches – requisitos específicos:

Além dos requisitos gerais, listados acima, os requisitos específicos mínimos que a solução de Gestão de Ativos e Patches deverá atender são:

	Requisito	Descrição
1	Realizar inventário de Hardware.	A solução deve inventariar os ativos de Hardware, coletando informações sobre computadores e seus componentes, impressoras e demais equipamentos. Exemplo de informações que devem constar no inventário: fabricante, nome do modelo, número de série, processador, placa-mãe, disco rígido, placa de vídeo, de rede, memória RAM, etc.
2	Realizar inventário de Software.	A solução deve inventariar os softwares instalados em dispositivos Windows e Linux da rede, possibilitando seu registro e controle de licenciamento.

	Requisito	Descrição
3	Realizar medição de uso do Software	A solução deve realizar a medição do uso do software, informando a quantidade e duração de uso de um determinado software por um usuário e/ou estação de trabalho.
4	Controlar as licenças de Software	A solução deve permitir o registro das licenças existentes para cada software, a data de expiração das mesmas e o controle de quantas licenças estão sendo utilizadas e quantas estão ociosas. Deve identificar quais são os computadores que estão utilizando cada licença, gerar avisos quando há mais licenças do software em uso do que o número de licenças disponíveis.
5	Realizar a distribuição de softwares e aplicativos	Deve ser possível, através da solução, distribuir e reinstalar softwares e aplicativos para um ativo específico, assim como para um grupo ou para a totalidade de equipamentos da rede corporativa. Deve ser possível agendar (dia/semana/mês) a instalação ou mesmo fazê-la em tempo real.
6	Realizar a desinstalação de softwares e aplicativos	A solução deve implementar a funcionalidade de realizara desinstalação de softwares e aplicativos em um equipamento específico, assim como para um grupo ou para a totalidade de equipamentos da rede corporativa. Deve ser possível agendar a desinstalação ou mesmo fazê-la em tempo real.
7	Permitir a realização de configuração/manutenção remota dos ativos.	A solução deve permitir, através de sua interface administrativa, que os técnicos acessem remotamente computadores em manutenção para realizar tarefas como: iniciar ou parar um serviço, alterar o registro, apagar ou criar um arquivo e/ou pasta, renomear um computador ou parar um processo em execução.
8	A solução pode ser instalada localmente ou em nuvem.	Atender as especificidades de cada Tribunal participante quanto à forma de instalação.
9	Identificar ativos de diferentes Sistemas Operacionais (Windows e Linux).	Visa ampliar a portabilidade da solução, permitindo reconhecer e coletar informações de dispositivos Windows e Linux.
10	Interface Web ou padrão Windows	A solução deve permitir que o acesso às suas funcionalidades seja realizado via interface web ou padrão Windows, com autenticação de duplo fator.
11	Gerenciamento de Bitlocker	A solução deve permitir ativar e desativar o Bitlocker em estações de trabalho, assim como armazenar a chave de recuperação de cada disco criptografado.
12	Implantação de Sistema Operacional	A solução deve permitir a captura e implantação de imagens de sistema operacional remotamente.
13	Possibilitar autogerenciamento de aplicativos pelos usuários	A solução deve possibilitar que o usuário instale/desinstale aplicativos pré-definidos através de um portal de autoatendimento.

	Requisito	Descrição
14	Gerenciamento de Patches	A solução deve realizar o gerenciamento de patches de Sistema Operacional e de aplicativos de terceiros. Ainda, a solução deve permitir a automatização na implantação de patches de segurança e de melhoria.
15	Suporte à tecnologia VPRO (somente para o grupo 5)	Gerenciamento do setup dos computadores e atividades correlatas, como ligar, desligar, reiniciar os computadores remotamente, via console, sem necessidade de acesso direto com usuário administrador em cada computador.
16	Recurso para inclusão de campos adicionais no cadastro de ativos para hardware e software	O campo deve permitir incluir as informações: N° do contrato, objeto do contrato, fiscais do contrato, tipo, marca/modelo, valor, fornecedor, responsáveis pelos equipamentos (demandante, técnico e administrativo), garantia, status (ativo/inativo), classificação de criticidade e identificador.
17	Deve permitir o registro de informações dos bancos de dados corporativos	Controle de licença dos bancos de dados utilizados nos servidores corporativos.
18	Possuir Banco de Dados	Centralizado para armazenamento automático das informações referentes aos ativos e itens de configuração, estar de acordo com o definido no ITIL v3. Deverá fazer integração entre os ativos, seus atributos e a relação entre eles, de forma automática.
19	Integração	As soluções de gestão de Ativos e Patches deverão estar integradas entre si, através de uma base de dados, fazendo parte de uma mesma solução, podendo ser ofertadas por módulos.
20	Consultas, relatórios e dashboards	Consultas e relatórios acessíveis pela console Web ou padrão Windows, com pesquisas parametrizáveis, permitindo exibição por gráficos e exportação para vários formatos de arquivos do mercado, como por exemplo, .csv e .pdf.

2.1.4 Requisitos da Solução de Gerenciamento de Patches – requisitos específicos:

	Requisito	Descrição
1	Gestão dos Patches	A solução deve realizar o gerenciamento de patches de Sistema Operacional e de aplicativos de terceiros, de forma automática. Ainda, a solução deve permitir a automatização na implantação de patches de segurança e de melhoria. Gerenciamento de patch deve controlar multi-dependências de patches, ou seja, se há múltiplos pacotes sendo instalados, requerendo múltiplos reboots, o agente suprime os reboots até que tudo esteja completo. Deve apontar todas as versões da aplicação que são afetadas e precisam de correção.
2	Banco de Dados	Centralizado para armazenamento automático das informações referentes aos ativos e itens de configuração,

	Requisito	Descrição
		estar de acordo com o definido no ITIL v3. Possuir banco de dados de patches de correção que seja atualizado de forma contínua, a partir do site dos fabricantes. O catálogo de patches a serem aplicados deve filtrar de forma simples quais são os patches que precisam ser instalados e exibir somente as últimas versões disponíveis de cada um deles, considerando a obsolescência de versões antigas
3	Consultas, relatórios e dashboards	Consultas e relatórios acessíveis pela console Web ou padrão Windows, com pesquisas parametrizáveis, permitindo exibição por gráficos e exportação para vários formatos de arquivos do mercado, como por exemplo, .csv e .pdf. O status individual de cada tarefa de patch deve mostrar quais patches foram instalados com sucesso, quais falharam e quais não foram instalados por não serem necessários
4	Políticas	A solução deve permitir políticas impositivas de aplicações nos endpoints
5	Realizar a distribuição dos patches e agentes	A solução deve prover a instalação remota, automática e silenciosa do agente, quando houver. Deve permitir o download de patches antes do início da tarefa, de forma a otimizar o processo de instalação
6	Console Web ou interface padrão Windows	A solução deve permitir que o acesso às suas funcionalidades seja realizado via interface web ou padrão Windows, com autenticação de duplo fator.
7	Administração	Baseada em regras, permitindo segmentar níveis de acesso por perfis de usuários, como por exemplo, administradores, operadores
8	Integração	A solução deve prover integração com o <i>LDAP</i> ou Microsoft <i>Active Directory</i> .
9	Monitoramento	Escanear os endpoints em busca de informações sobre os patches não instalados e confrontá-los contra o banco de dados de patches disponíveis.
10	Sincronização	Possuir recurso para configuração da periodicidade de sincronização do banco de dados de patches. Possuir recurso para testar e aprovar os patches antes do processo de deploy.
11	Seleção	A solução deve conter a inteligência de filtrar automaticamente, sem intervenção, quais ativos receberão os patches selecionados na tarefa de patch considerando a arquitetura do sistema operacional e também a pré-existência de determinada aplicação, evitando assim instalações indesejadas;

2.1.5. Definição da licença/aquisição:

Como os Tribunais participantes possuem interesse em formatos diferentes da solução, foram definidos 5 grupos. Além disso, a divisão em grupos poderá possibilitar que vários fabricantes participem do certame, não sendo necessário que uma única solução vença.

Grupo	Item	Descrição	Unidade de medida
1	1	Solução de gerenciamento de ativos e patches, instalação local, com manutenção e suporte por 60 meses - estações	Licenças para Estações
	2	Solução de gerenciamento de ativos e patches, instalação local, com manutenção e suporte por 60 meses - servidores	Licenças para Servidores
	3	Serviço de implantação e configuração solução na infraestrutura do TRE	Unidade
	4	Serviço de repasse de conhecimento com mínimo de 20 horas	Pessoas
2	1	Solução de gerenciamento de ativos e patches, em nuvem (<i>Cloud Computing</i>), com suporte por 24 meses - estações	Licenças para Estações
	2	Solução de gerenciamento de ativos e patches, em nuvem (<i>Cloud Computing</i>), com suporte por 24 meses - servidores	Licenças para Servidores
	3	Serviço de implantação e configuração	Unidade
	4	Serviço de repasse de conhecimento com mínimo de 20 horas	Pessoas
3	1	Solução de gerenciamento de patches, instalação local - estações	Licenças para Estações
	2	Solução de gerenciamento de patches, instalação local - servidores	Licenças para Servidores
	3	Serviço de implantação e configuração	Unidade
	4	Serviço de repasse de conhecimento com mínimo de 20 horas	Pessoas
4	1	Solução de gerenciamento de patches, em nuvem (<i>Cloud Computing</i>), com suporte por 24 meses - estações	Licenças para Estações
	2	Solução de gerenciamento de patches, em nuvem (<i>Cloud Computing</i>), com suporte por 24 meses - servidores	Licenças para Servidores
	3	Serviço de implantação e configuração	Unidade
	4	Serviço de repasse de conhecimento com mínimo de 20 horas	Pessoas
5	1	Solução de gerenciamento de ativos e patches com suporte a VPRO - instalação local, com manutenção e suporte por 60 meses - estações	Licenças para Estações
	2	Solução de gerenciamento de ativos e patches com suporte a VPRO - instalação local, com manutenção e suporte por 60 meses - servidores	Licenças para Servidores
	3	Serviço de implantação e configuração	Unidade
	4	Serviço de repasse de conhecimento com mínimo de 20 horas	Pessoas

2.1.5.1. Solução com licenciamento perpétuo:

As licenças de software fornecidas deverão ser de uso definitivo. Após o final do contrato, o Tribunal reserva-se o direito de manter em uso todas as licenças de software aqui especificadas, e recebidas, por tempo indeterminado.

A solução deverá suportar a instalação em servidores físicos ou virtuais da contratada e deverá poder operar em servidor compartilhado com outras aplicações dos Tribunais.

Se as soluções exigirem Banco de Dados específico, proprietário, que exija licenciamento, a empresa deverá prover a licença, sem ônus para o Tribunal, e realizar a instalação e sua respectiva configuração.

– Grupo 1:

Solução de gerenciamento de ativos e patches, com fornecimento de licenças perpétuas, com manutenção e suporte por 60 meses

A contratação visa à disponibilização, implantação, fornecimento de licenças perpétuas e suporte à solução de **Gestão de Ativos de Tecnologia da Informação e Patches**, devendo atender integralmente a todos os requisitos mínimos descritos no presente EP.

– Grupo 3:

Solução de gerenciamento de patches, com fornecimento de licenças perpétuas, com manutenção e suporte por 60 meses

A contratação visa a disponibilização, implantação, fornecimento de licenças perpétuas e suporte à solução de **Gestão de Patches**, devendo atender integralmente a todos os requisitos mínimos descritos no presente EP.

– Grupo 5:

Solução de gerenciamento de ativos e patches, com suporte à tecnologia VPRO, da Intel. Fornecimento de licenças perpétuas ou Serviço em nuvem (Cloud Computing), com manutenção e suporte por 60 meses

A contratação visa a disponibilização, implantação, fornecimento de licenças perpétuas e suporte à solução de **Gestão de Ativos e Patches, com suporte à Tecnologia VPRO da Intel**, via console de gerenciamento, devendo atender integralmente a todos os requisitos mínimos descritos no presente EP.

2.1.5.2.Licenças de Software como Serviço (SaaS): Após o término do contrato, o Tribunal que não fizer a renovação não terá mais direito de utilizar a solução:

– Grupo 2:

Serviço de solução de gerenciamento de ativos de TIC e patches, em nuvem (Cloud Computing), com suporte por 24 meses, prorrogáveis pelo prazo legal

A solução visa a contratação de serviço em nuvem, com a disponibilização da solução, implantação, configuração e suporte à solução de **Gestão de Ativos de TI e Patches**, devendo atender integralmente a todos os requisitos mínimos descritos no presente EP.

- Grupo 4:

Serviço de solução de gerenciamento de patches, em nuvem (Cloud Computing), com suporte por 24 meses, prorrogáveis pelo prazo legal

A solução visa a contratação de serviço em nuvem, com a disponibilização da solução, implantação, configuração e suporte à solução de **Gestão de Patches**, devendo atender integralmente a todos os requisitos mínimos descritos no presente EP.

Os requisitos exigidos deverão constar das 2 modalidades de solução: licenças em caráter perpétuo e serviço em *Cloud Computing* (nuvem). Ou seja, a modalidade de licenciamento, perpétuo ou licença como serviço, não pode ser um restritivo para alguma funcionalidade/requisito exigida neste EP e no TR.

2.1.6.Todas as soluções dos 5 grupos deverão prover também:

- Capacitação da equipe técnica nas ferramentas e configurações dos processos implantados;

- O direito de atualização das licenças e ao suporte, contados do aceite da fase em produção;
- Garantir todas as configurações necessárias para o pleno funcionamento da solução.

2.1.7 Serviço de implantação e configuração:

2.1.7.1. Para as soluções dos grupos 1, 3 e 5:

Levantamento e estudo da infraestrutura de cada Tribunal, para a instalação e configuração de todos os componentes das soluções: softwares, aplicativos, bancos de dados e clientes.

Diagnóstico e proposta para solução de problema de desempenho das soluções.

2.1.7.2. Para as soluções dos grupos 2 e 4:

Instalação e configuração dos clientes, caso existam, nos ativos de cada Tribunal.

Diagnóstico e proposta para solução de problema de desempenho das soluções.

2.1.8. Serviços de Manutenção e Suporte:

O serviço de suporte será prestado durante o período de vigência contratual, em dias úteis (de segunda-feira a sexta-feira), em horário comercial (das 9h às 18h), por profissionais especializados, instruídos e controlados pela Contratada, incluindo, ajustes, reparos e correções necessárias para o perfeito funcionamento da solução contratada, e ainda mediante suporte técnico telefônico, sem ônus adicional para a CONTRATANTE;

2.1.8.1. O início do prazo de manutenção e suporte operacional se dará com o aceite definitivo da solução contratada.

2.1.8.2. A abertura de chamados junto à CONTRATADA consistirá em esclarecimentos de dúvidas, orientação no uso da console e outras solicitações afetas ao uso e configuração da solução contratada, cujos serviços serão prestados pelos técnicos da CONTRATADA.

2.1.8.3. Classificação dos eventos:

Nível de Severidade	Descrição
1	Serviço totalmente indisponível
2	Serviço com funcionamento degradado
3	Serviço com funcionamento intermitente
4	Solicitação de informações, configurações, atividades que não afetem o funcionamento do equipamento ou rede como um todo

2.1.8.4. Prazos de atendimento

Nível de Severidade	de	Prazo de conclusão
1		8 horas, considerando o expediente entre 8h e 20h
2		12 horas
3		24 horas
4		24 oras

2.1.8.5. Os chamados somente podem ser encerrados após a validação da solução apresentada.

2.1.8.6. É vedado o encerramento do chamado pela contratada sem a autorização prévia da CONTRATANTE.

2.1.8.7. É vedado o cancelamento de chamados pela contratada sem a autorização prévia da CONTRATANTE.

2.1.8.8. Os atendimentos dos chamados técnicos serão definidos a seguir:

2.1.8.8.1. O atendimento dos chamados técnicos de nível de severidade 1 deverá ser iniciado em até 15 (quinze) minutos e o chamado solucionado em até 8 (oito) horas corridas em A critério da CONTRATANTE, quando da abertura de chamado ocorrer após às 18h, poderá ser interrompida a contagem de tempo e a retomada das atividades se dará a partir das 8h do dia seguinte.

2.1.8.8.2. O atendimento dos chamados técnicos de nível de severidade 2 deverá ser iniciado em até 2 (duas) horas e solucionado em até 12 (doze) horas corridas em período não eleitoral A critério da CONTRATANTE, quando da abertura de chamado ocorrer após às 18h, poderá ser interrompida a contagem de tempo e a retomada das atividades se dará a partir das 8h do dia seguinte.

2.1.8.8.3. O atendimento dos chamados técnicos de nível de severidade 3 deverá ser iniciado em até 4 (quatro) horas e solucionados em até 24 (vinte e quatro) horas corridas. A critério da CONTRATANTE, quando da abertura de chamado ocorrer após às 18h, poderá ser interrompida a contagem de tempo e a retomada das atividades se dará a partir das 8h do dia seguinte.

2.1.8.8.4. O atendimento dos chamados técnicos de nível de severidade 4 deverá ser iniciado em até 6 (seis) horas e solucionados em até 24 (vinte e quatro) horas, considerando o horário comercial, de segunda à sexta.

2.1.8.9. Por início de atendimento entende-se a alocação de técnico para efetuar a correção do problema ou o diagnóstico preciso, com interlocução telefônica direta com a equipe da CONTRATANTE.

2.1.8.10. Em caso de necessidade de coleta de logs e demais informações que permitam o adequado diagnóstico, a contratada deve fazê-lo remota ou localmente, com acompanhamento da equipe do CONTRATANTE ou terceiro por ela autorizado.

2.1.8.11. O atendimento dos chamados deve ser em língua portuguesa, incluindo o atendimento telefônico, o e-mail e o portal de atendimento.

2.1.8.12. A interrupção do atendimento, assim como o não cumprimento dos chamados técnicos, poderá ensejar na aplicação das penalidades previstas no contrato.

2.1.8.13. Deverá haver uma descrição da solução, imediatamente após fechamento dos chamados, acerca das soluções aplicadas para definitivamente retornar à solução ao pleno estado de funcionamento.

2.1.8.14. Essa descrição deverá fornecer em detalhes, por e-mail ou portal de atendimento, a solução para o problema detectado. Deverá cobrir todo e qualquer defeito apresentado no serviço, incluindo todos os componentes da solução, equipamentos de comunicação, peças e esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias.

2.1.8.15. A contratada deverá entregar documentação comprobatória da contratação da Garantia técnica, pelo período especificado neste documento, junto ao fabricante da solução ofertada; A contratação da garantia técnica junto ao fabricante não exime a contratada da mesma responsabilidade; os serviços deverão ser prestados pelo fabricante do equipamento ou pela rede de assistência técnica autorizada, sempre sob responsabilidade da contratada.

2.1.8.16. Todas as despesas decorrentes da necessidade de substituição de equipamento, infraestrutura, transporte, deslocamento, embalagem, peças, partes, manuais do fabricante, serão de inteira responsabilidade da contratada, não devendo gerar qualquer ônus adicional para o CONTRATANTE.

2.1.9. Soluções disponíveis no mercado de Tecnologia da Informação e Comunicação e seus respectivos fornecedores (nome da empresa, site e telefone);

- Manage Engine Desktop Central: <https://www.manageengine.com/products/desktop-central/>
- Ivanti Unified Endpoint Management: <https://www.ivanti.com/solutions/unified-endpoint-management>
- Microsoft Endpoint Manager: <https://www.microsoft.com/pt-br/security/business/microsoft-endpoint-manager>

- Qualys Asset Management: <https://www.qualys.com/apps/cybersecurity-asset-management/>

2.1.10. Contratação similar já realizada pelo TRE-SP:

PREGÃO ELETRÔNICO FEDERAL 75/2013: Solução para Gerenciamento de Serviços e componentes de TI: a ferramenta adquirida possuía um módulo de inventário de software e hardware, similar ao software de gestão de ativos, porém não possui todos os requisitos deste EP.

2.1.11. Contratações similares realizadas por outros órgãos:

- ESTADO DE MINAS GERAIS - SECRETARIA DE ESTADO DE FAZENDA: PREGÃO ELETRÔNICO Nº 111/2021: Aquisição de solução para gestão de vulnerabilidades e auditoria de configuração de ativos de rede, disponível em <https://www.google.com/url?sa=t&rct=j&q=&>
- Tribunal Superior do Trabalho - 18ª Região, Pregão: 44/2020; UASG: 80020
Item 1 - Direito de atualização (upgrade) para a versão atual Ivanti EndPoint Manager. (Quantidade = 2.234; Valor = 92.755,68)
Item 2 - Suporte, garantia e direito de atualização por 12 meses Ivanti EndPoint Manager.
- Ministério da Fazenda - Superintendência de Seguros Privados/RJ. Pregão: 31/2015; UASG: 177039, Solução de gerenciamento de Endpoints, incluindo: aquisição das licenças perpétuas de software; atualização de versão das licenças; serviço de suporte técnico; serviço de instalação e configuração da solução no ambiente da Susep; e treinamento da equipe da Susep;

2.2 –Identificação das diferentes Soluções de Tecnologia da Informação e Comunicação

No Portal de Software Público Brasileiro (<http://www.softwarepublico.gov.br>), o software Cacic, Configurador Automático e Coletor de Informações Computacionais, possui as funcionalidades de suporte a inventário em plataformas Windows e GNU/Linux; obtenção automatizada de dados e hardware e software; controle de patrimônio; alertas relativos às alterações de hardware e inserção de dispositivos USB; suporte ao controle de licenças; controle de softwares adquiridos versus inventariados, não contempla distribuição de aplicações, gerenciamento de Patches, Bitlocker e vulnerabilidades

Snipe-IT , Solução open-source, que embora implemente requisitos como inventário de ativos de TI e controle de licença, não contempla outras funcionalidades como distribuição de aplicações, gerenciamento de Patches, Bitlocker e vulnerabilidades.

GLPi , Software de código aberto que implementa controle de inventário de software, distribuição de aplicações e controle de licenciamento de software. Não contempla, porém, outros requisitos como a possibilidade de acesso remoto para manutenção em tempo real na configuração de estações de trabalho.

OPSI , Ferramenta open source para inventário de hardware e software, além de distribuição de aplicações em ambiente Windows / Linux. Através do documento de funcionalidades (features) disponibilizado no site do projeto, se constata que é possível que a solução implemente também controle de licenças e possibilidade de alterar as configurações de uma estação de trabalho em tempo real (registro, por exemplo). Não existe, porém, um parceiro no Brasil que possa fornecer maiores detalhes e oferecer suporte técnico. Além disso, em seu rol

de features, não menciona implementar requisitos como gerenciamento de patches e vulnerabilidades.

SpiceWorks , Software sem custo, que implementa inventário de hardware e software, além de suporte remoto. No entanto, não implementa uma série de outros requisitos como distribuição de aplicações e gerenciamento de BitLocker.

Citsmart: esta solução está em uso, atualmente, pelo TRE-SP, e atende somente parte dos requisitos deste EP. A solução só permite inventariar os ativos, trazendo uma relação dos softwares e hardware.

Não se aplicam a observância às políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário, visto que a solução que se pretende adquirir não trata com tramitação de processos, a aderência às regulamentações da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), por não exigir uso de certificado digital e a observância às orientações, premissas e especificações técnicas e funcionais definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus) pela solução ser destinada a finalidade diversa.

Foram obtidos orçamentos preliminares para as soluções comercializadas pela Ivanti e Qualys, para auxiliar a fundamentação dos estudos para a contratação.

2.3 –Análise e a comparação entre os custos totais das Soluções de Tecnologia da Informação e Comunicação identificadas.

Pesquisa inicial para estimativas de valores:

Gestão de Ativos e Patches, Fornecedor Qualys, referência para os grupos 2 e 5

Item	DESCRIÇÃO DOS PRODUTOS E SERVIÇOS	Período	QTD	VALOR UNIT. R\$	VALOR TOTAL R\$
1	Solução de gerenciamento e controle de patches	60 meses	21280	305	6.490.400,00
2	Solução de inventário de ativos	60 meses	21280	155	3.298.400,00
3	Instalação, Configuração e documentação – por localidade.	N/A	11	14.000,00	154.000,00
4	Serviços de Suporte Técnico	60 meses	11	600.000,00	6.600.000,00
5	Treinamento Oficial 20 horas - por profissional	20 horas	22	6.500,00	143.000,00
				TOTAL	16.685.800,00

Gestão de ativos, fornecedor Ivanti, referência para o grupo 1

Item	DESCRIÇÃO DOS PRODUTOS E SERVIÇOS	QTD	VALOR UNIT. R\$	VALOR TOTAL R\$
1	Solução de Gerenciamento Ivanti EndPoint Manager com suporte e garantia por 12 meses	12000	186,19	2.234.296,88
2	Serviços de Instalação e Configuração	600 horas	330,00	198.000,00
3	Operação Assistida mensal	12	45.000,00	540.000,00
			Total	2.972.296,88

Gestão de patches, fornecedor HCL Big Fix, subscrição, referência para o grupo 4

Item	DESCRIÇÃO DOS PRODUTOS E SERVIÇOS	QTD	VALOR UNIT. R\$	VALOR TOTAL R\$
1	Licenciamento por subscrição para 60 meses HCL BigFix Patch, Perpetual License & 60 Month S&S, Client Device	1200	R\$ 325,45	390.540,00
2	HCL BigFix Patch, Perpetual License & 60 Month S&S, Managed Virtual Server	300	R\$ 2051,99	615.597,00

3	Repasse de conhecimento para até 5 participantes remotos durante a instalação	1	R\$ 84.857,84	84857,84
4	Suporte técnico 60 meses	1	R\$ 81.295,31	81295,31
			Total	1.172.285,47

Gestão de patches, fornecedor HCL Big Fix, licença perpétua, referência para o grupo 3

Item	DESCRIÇÃO DOS PRODUTOS E SERVIÇOS	QTD	VALOR UNIT. R\$	VALOR TOTAL R\$
1	Licenciamento por subscrição para 60 meses HCL BigFix Patch, Perpetual License & 60 Month S&S, Client Device	1200	254,62	305.544,00
2	HCL BigFix Patch, Perpetual License & 60 Month S&S, Managed Virtual Server	300	1.777,30	533.190,00
3	Repasse de conhecimento para até 5 participantes remotos durante a instalação	1	84.857,84	84.857,84
4	Suporte técnico 60 meses	1	81.295,31	81.295,31
			Total	1.004.889,37

2.4 – Escolha da Solução de Tecnologia da Informação e Comunicação e justificativa

A segurança da informação depende do conhecimento de informações detalhadas do parque computacional da organização que se pretende proteger. Deve-se conhecer, por exemplo, quantos dispositivos estão conectados à rede, se o dispositivo é conhecido e aprovado pela organização, quais softwares estão instalados nos dispositivos e em que versões são utilizados, entre outras.

No entanto, a obtenção deste grande conjunto de informações é um desafio, visto que há grande heterogeneidade de dispositivos e softwares, grande volume de informações a serem coletadas e, por se tratarem de informações que estão em constante evolução e alteração. Desta forma, a obtenção e organização destas informações necessita do apoio de soluções computacionais para sua automação. Estas soluções são chamadas de Gestão de Ativos, cuja aquisição é um dos objetivos desta contratação.

As soluções de Gestão de Ativos são capazes de atender alguns controles previstos no framework *CIS Controls* versão 8, que é utilizado pelo TCU para avaliar o nível de maturidade de segurança da informação dos órgãos jurisdicionados.

Nomeadamente, este framework possui 2 controles diretamente relacionados à Gestão de Ativos: Controle 1 - Inventário e controle de ativos corporativos e Controle 2 - Inventário e controle de ativos de software. Portanto, a presente contratação é capaz de elevar a maturidade do TRE-SP, pelo menos, no tocante a estes 2 controles.

A segurança da informação também depende da manutenção de softwares e configurações de maneira a mantê-los seguros. Uma das atividades desta manutenção é a atualização frequente e constante dos softwares com o objetivo de mantê-los com suas correções de vulnerabilidades mais recentes, evitando que essas vulnerabilidades sejam exploradas por grupos hackers.

Embora tal atividade possa parecer trivial, porque basta atualizar os softwares dos dispositivos, em ambientes corporativos esta atividade é um grande desafio, visto que uma grande quantidade e variedade de softwares é utilizada e cada uma com mecanismos peculiares de atualização. Por exemplo, para atualização de correções dos sistemas operacionais Windows, costuma-se utilizar uma solução nativa chamada WSUS.

No entanto, esta solução é capaz de atualizar apenas os componentes do Windows. Navegadores como Firefox e Google Chrome possuem atualização automática, mas que normalmente é desabilitada em ambientes corporativos para garantir a compatibilidade com aplicações utilizadas na organização.

Demais categorias de softwares como suítes de escritório, leitores de PDF e softwares de terceiros também possuem peculiaridades. Desta forma, a atualização de softwares utilizados na organização também necessita do apoio de soluções computacionais para automação e uniformização da atividade.

Estas soluções são chamadas de Gestão de Patches, que durante os estudos foi identificado comumente como sendo um módulo que compõe as soluções de Gestão de Ativos.

A Gestão de Patches também é capaz de atender alguns controles previstos no CIS Controls, versão 8. Nomeadamente, ajuda a atender as medidas de segurança previstas no Controle 7 - Gestão contínua de vulnerabilidades. Portanto, a presente contratação é capaz de elevar a maturidade do TRE-SP, pelo menos, no tocante às medidas previstas neste controle.

São objetivos diretos desta contratação:

- Implantar e manter um inventário de ativos de hardware;
- Implantar e manter um inventário de ativos de software;
- Automatizar a instalação de correções (patches) para remediar vulnerabilidades;
- Automatizar a implantação de sistemas operacionais;
- Automatizar a implantação de softwares.

Os benefícios diretos e indiretos desta contratação são os seguintes:

- Elevação do nível de maturidade em segurança da informação;
- Otimização dos recursos humanos da TI pela automação e padronização de atividades rotineiras;
- Menor exposição a ataques cibernéticos pela utilização de softwares atualizados;
- Maior conhecimento e visibilidade do parque computacional.

As soluções que atendem às necessidades dos Tribunais são:

- Manage Engine Desktop Central:
- Ivanti Unified Endpoint Management
- Microsoft Endpoint Manager
- Qualys Asset Management

Como existem várias soluções que atendem aos requisitos, e vários representantes dos fornecedores, não optaremos por uma solução única, possibilitando a livre concorrência.

Poderá haver um fornecedor diferente para cada solução, de cada grupo. Não é obrigatório que somente um fornecedor ofereça todas as soluções de todos os grupos.

Com relação às soluções de software livre indicadas no item 2.2, elas não atendem a todos os requisitos solicitados. Assim, não é possível adotá-las.

Para o TRE-SP, é previsto que a solução contemple um parque de aproximadamente 8000 dispositivos, sendo registrada a contratação de 9000 licenças, para acompanhar eventual aumento de ativos durante a vigência da Ata de Registro de Preços.

2.4.1. Opção do TRE-SP por Solução de Gestão de Ativos e Patches com licença de caráter perpétuo e suporte à tecnologia VPRO da Intel:

O TRE-SP opta pelo Grupo 5, licenças de caráter perpétuo, com instalação na infraestrutura do TRE-SP, e não por solução em nuvem. A justificativa deve-se ao número de dispositivos a serem gerenciados, aproximadamente 8000, entre estações e servidores de rede, além do tráfego de informações, softwares e Patches de sistemas operacionais, que é muito elevado. Deve-se levar em conta também a distribuição de imagens de instalação dos sistemas operacionais, que chegam a ter cerca de 10 GB, podendo onerar o link de internet do Tribunal.

Tecnologia VPRO, da Intel: permite o controle dos ativos, através da tecnologia dos processadores Intel, presentes nos computadores do TRE-SP. Essa tecnologia permite realizar configurações no setup dos computadores, inserir ou alterar senhas, ligar, desligar e reiniciar os computadores.

2.4.2. Justificativa para vigência dos contratos

2.4.2.1. Grupos 1,3 e 5, contrato de 60 meses:

Por se tratar de serviço crítico, de segurança dos ativos de TIC, é mais vantajoso para o Órgão ter um contrato de 60 meses, não sendo necessário renovar a cada 12 meses, evitando-se o risco da não renovação. As consequências seriam:

Para os itens dos grupos 1, 3 e 5: desatualização das licenças e ativos, perda do suporte técnico, com conseqüente impacto na gestão dos ativos, pois a solução, após um determinado período, não conseguirá mais realizar o inventário e a distribuição de softwares mais recentes.

2.4.2.2. Grupos 2 e 4, contrato de 24 meses:

A vigência contratual para os serviços em nuvem será de 24 meses, prorrogáveis até o limite legal, dado que se trata de prazo adequado para a instalação e aplicação da solução aos controles de segurança da informação, recomendados pelos órgãos de auditoria. O contrário sensu, prazos inferiores não permitiriam amortização de investimento desta envergadura, além de representar lapso exíguo de efetivo uso em razão das providências preliminares de implantação

2.4.3. Participação de outros Tribunais - consulta:

Por se tratar de aquisição conjunta para a Justiça Eleitoral, os Tribunais responderão mediante convite, e questionário, enviados por ofício, sobre os quantitativos que necessitam e, para atender às demandas, foi definida a seguinte estrutura para a aquisição:

Grupo	Item	Descrição	Unidade de medida	Quantidade a ser registrada
1	1	Solução de gerenciamento de ativos e patches, instalação local, com manutenção, garantia e suporte por 60 meses - estações.	Licenças para Estações	
	2	Solução de gerenciamento de ativos e patches, instalação local, com manutenção, garantia e suporte por 60 meses - servidores.	Licenças para Servidores	
	3	Serviço de implantação e configuração da solução na infraestrutura do Tribunal.	Unidade	
	4	Serviço de repasse de conhecimento com mínimo de 20 horas	Pessoas	
2	5	Solução de gerenciamento de ativos e patches, em nuvem (<i>Cloud Computing</i>) por 24 meses, prorrogáveis até o limite legal, incluso suporte – estações.	Licenças para Estações	
	6	Solução de gerenciamento de ativos e patches, em nuvem (<i>Cloud Computing</i>), por 24 meses, prorrogáveis até o limite legal, incluso suporte – servidores	Licenças para Servidores	
	7	Serviço de implantação e configuração na infraestrutura do Tribunal.	Unidade	
	8	Serviço de repasse de conhecimento com mínimo de 20 horas	Pessoas	
3	9	Solução de gerenciamento de patches, instalação local, com manutenção, garantia e suporte por 60 meses - estações.	Licenças para Estações	
	10	Solução de gerenciamento de patches, instalação local, com manutenção, garantia e suporte por 60 meses - servidores.	Licenças para Servidores	
	11	Serviço de implantação e configuração da solução na infraestrutura do Tribunal.	Unidade	
	12	Serviço de repasse de conhecimento com mínimo de 20 horas	Pessoas	
4	13	Solução de gerenciamento de patches, em nuvem (<i>Cloud Computing</i>) - por 24 meses prorrogáveis até o limite legal, incluso suporte – estações	Licenças para Estações	

	14	Solução de gerenciamento de patches, em nuvem (<i>Cloud Computing</i>) - por 24 meses prorrogáveis até o limite legal, incluso suporte – servidores	Licenças para Servidores	
	15	Serviço de implantação e configuração na infraestrutura do Tribunal.	Unidade	
	16	Serviço de repasse de conhecimento com mínimo de 20 horas	Pessoas	
5	17	Solução de gerenciamento de ativos e patches com suporte a VPRO, com manutenção, garantia e suporte por 60 meses - estações	Licenças para Estações	
	18	Solução de gerenciamento de ativos e patches com suporte a VPRO, com manutenção, garantia e suporte por 60 meses - servidores	Licenças para Servidores	
	19	Serviço de implantação e configuração da solução na infraestrutura do Tribunal.	Unidade	
	20	Serviço de repasse de conhecimento com mínimo de 20 horas	Pessoas	

2.5 – Avaliação das necessidades de adequação do ambiente do órgão para viabilizar a execução contratual

2.5.1. Para as aquisições dos grupos 2 e 4:

Não haverá necessidade de adequação do ambiente, tendo em vista que a contratação não alterará em nada o ambiente atualmente em uso.

2.5.2. Para as aquisições dos grupos 1, 3 e 5:

Como envolvem instalação e configuração da solução na rede local, será necessário que o Tribunal disponibilize infraestrutura para que a empresa realize as instalações e configurações necessárias.

3 – Sustentação do Contrato

3.1 – Recursos materiais e humanos

Para a execução deste contrato, será necessária a participação de pessoal dos quadros das seções de Infraestrutura, Suporte a Aplicações e de Novas Tecnologias, além de funcionários da empresa vencedora da licitação.

Quanto aos recursos materiais, serão necessários: espaço de armazenamento em disco, servidores, rede de comunicação de dados, acesso à internet e computadores.

3.2 – Continuidade do fornecimento da Solução de Tecnologia da Informação e Comunicação

Caso ocorra interrupção contratual, será realizada nova licitação, para contratação e atualização da solução e suporte.

3.3 – Atividades de transição contratual e de encerramento do contrato:

3.3.1. Para as aquisições dos grupos 2 e 4:

As atividades de transição contratual e de encerramento do contrato, inclusive de acordo com a Instrução Normativa GSIPR Nº 5 DE 30/08/2021, consistem na eliminação de qualquer informação referente aos ativos de TIC do Órgão dos servidores, inclusive de mídias de backup da empresa. A empresa não poderá permanecer com nenhuma informação pertencente ao Órgão, após o encerramento do contrato. A empresa deverá informar ao Órgão que procedeu à eliminação das informações, através de termo assinado. Os logs deverão ser mantidos durante toda a vigência do contrato, devendo ser entregues quando solicitados e no encerramento do contrato.

3.3.1. Para as aquisições dos grupos 1, 3 e 5:

Quando do encerramento do contrato, a solução deverá estar atualizada em sua versão mais recente, não existindo devolução de materiais e licenças.

As licenças de Bancos de Dados proprietárias, cedidas pela Contratada e utilizadas na solução, serão de propriedade do Tribunal, sem ônus, e, no encerramento do contrato, não serão devolvidas e/ou desinstaladas da infraestrutura do Órgão.

3.4 – Regras para estratégia de independência do órgão com relação à empresa contratada

Haverá necessidade de treinamento ou repasse tecnológico, presencial ou à distância, no mínimo de 20 (vinte) horas, visando capacitar os servidores da Secretaria de Tecnologia da Informação no uso da ferramenta.

Além do repasse tecnológico para as equipes técnicas, deverão ser fornecidos documentos e tutoriais (em português) necessários à capacitação dos usuários finais da solução a respeito das funcionalidades que compõem as soluções.

O repasse de conhecimento poderá ser realizado de forma virtual, por ferramenta de videoconferência.

Deverá ser fornecido certificado para cada participante, contendo a respectiva data, carga horária e assinatura do técnico responsável/empresa fornecedora

4 Estratégia para a Contratação

4.1 Natureza do objeto:

Solução de gestão de ativos e patches e solução de gestão de Patches.

O objeto possui características comuns e é usualmente fornecido pelo mercado.

Considerando que as soluções descritas como instalação local, acompanha serviço de atualização das licenças perpétuas e serviço de suporte e manutenção, sendo um serviço continuado, a vigência será de 60 meses.

As soluções em nuvem, em atendimento às regras de contratação de softwares, terão vigência de 24 meses, prorrogáveis pelo prazo legal considerando se tratar de um serviço continuado e de extrema importância.

Alinhamento Estratégico

Planejamento Estratégico TRE-SP 2016-2021

Macrodesafio:

Melhorar a governança e infraestrutura de TIC

Indicador de Resultado 8.1: Índice de disponibilidade de serviços essenciais de TI

Planejamento Estratégico de TIC TRE-SP 2021-2022

Objetivos estratégicos:

Aprimorar a Segurança da Informação e a Gestão de Dados

Promover Serviços e Soluções de Infraestrutura e Soluções Corporativas

4.2 – Parcelamento do objeto com a demonstração da viabilidade ou não da divisão

O objeto foi dividido em grupos contendo características distintas, como instalação local ou serviço em nuvem e o suporte à tecnologia *VPro*.

Foi verificado que o fornecedor da solução de Gestão de Ativos normalmente oferece também a Solução de Gestão de Patches, sendo mais vantajoso o fornecimento conjunto das duas soluções, principalmente pela integração e operação mais eficientes. Para atender a Tribunais que já possuíam a Solução de Gestão de Ativos, mas demonstraram interesse na de Patches, foi acrescentado um grupo somente para este objeto.

Será realizada prova de conceito POC para teste e aceite da solução, a ser realizado no prazo máximo de 7 dias úteis, contados da solicitação do pregoeiro, para as duas soluções: Gestão de Ativos e Patches, com suporte à VPRO e Gestão de Patches.

Realizando a POC para essas duas soluções já se consegue validar as soluções dos 5 grupos, podendo ser todas de solução em nuvem, desde que os requisitos sejam os mesmos para as soluções em nuvem e com instalação local.

A validação deverá ocorrer mediante prévio agendamento com os seguintes Tribunais:

Para o grupo 1 - Gestão de Ativos e Patches (On-premises):

TRE-TO: Seção de Redes e Segurança de Computadores, pelo e-mail: seres@tre-to.jus.br ou pelo telefone (63)3229-9716, de segunda a sexta-feira, das 13:00 às 19:00.

Para o grupo 2 - Gestão de Ativos e Patches (Nuvem):

TRE-MS: Seção de Gestão de Ativos pelo e-mail Seção de Gestão de Ativos ou pelo telefone (67) 2107-7120/7103, de segunda a sexta-feira, das 12 às 18hs.

Para o grupo 3 - Gestão Patches (On-premises):

TRE-PB: Seção de Segurança Cibernética, pelo e-mail: sesec@tre-pb.jus.br ou pelo telefone: (83)3512-1420, de segunda a sexta, das: 13h00 às 19h00.

Para o grupo 4 - Gestão Patches (Nuvem):

TRE-PR: Assessoria de Segurança Cibernética - ASC,), pelo e-mail asc@tre-pr.jus.br ou pelo telefone (41) 3330-8767, de segunda a sexta-feira, das 13:00 às 19:00.

Para o grupo 5 - Gestão de Ativos e Patches, com suporte à VPRO:

TRE-SP: Coordenadoria de Gestão e Segurança (COGS), pelo e-mail cogs@tre-sp.jus.br ou pelo telefone (11)3130-2117, de segunda a sexta-feira, das 13 às 19hs.

Caso o produto não cumpra os requisitos mínimos descritos neste tópico, a proposta da licitante será desclassificada

Recursos para a validação:

Os Tribunais participantes da POC deverão fornecer 10 (dez) microcomputadores, dentre eles: estações de trabalho e servidor, ambientes com e sem SIS, utilizados na rede do Tribunal (Secretaria e cartórios) e utilizados em trabalho remoto, 2 elementos de rede como, por exemplo, impressora, appliances, switches.

A validação corresponderá à execução das seguintes tarefas:

Para a gestão de ativos e patches, com suporte à VPRO:

Efetuar a instalação e execução do agente (se houver), em pelo menos 8 (oito) microcomputadores, de forma “silenciosa”.

Efetuar o inventário com a coleta dos seguintes atributos de hardware em, no mínimo 8 (oito) dos 10 (dez) computadores disponibilizados: Endereço IP, Hostname; tamanho da memória, processador, MAC Address e o campo “Asset Tag”, da BIOS.

Efetuar o inventário com a coleta dos seguintes atributos de softwares em, no mínimo 8 (oito) dos 10 (dez) computadores disponibilizados: “Nome Original do Arquivo”, “Nome do Software”, “Fabricante” e “Versão”.

Verificar se compartilhamento administrativo do Windows continua desativado: a solução não pode utilizar esse recurso, por se tratar de uma brecha de segurança.

Acessar a console de gerenciamento e analisar se solicita a autenticação por 2FA

Identificar as mudanças de hardware e/ou software que forem feitas em um dos computadores: proceder com desinstalação e instalação de softwares. Alterar algum item de hardware.

Aplicar patches sugeridos pela solução e acompanhar a instalação e resultados da instalação: se foi com sucesso, se houve erros, sugestões da ferramenta para correções.

Gerar um pacote de um software e efetuar a distribuição, de forma silenciosa, em pelo menos 8 (oito) microcomputadores

Emitir relatório de softwares e atributos inventariados nos microcomputadores

Acessar uma das estações utilizando a função controle remoto

Deverá ser configurada a função para que o usuário autorize o acesso

Através do recurso da VPRO: ligar, reiniciar e desligar os computadores

Para a gestão de patches:

Efetuar a instalação e execução do agente (se houver), em pelo menos 8 (oito) microcomputadores, de forma “silenciosa”.

Verificar se compartilhamento administrativo do Windows continua desativado: a solução não pode utilizar esse recurso, por ser uma brecha de segurança.

Acessar a console de gerenciamento e analisar se solicita a autenticação por 2FA

Analisar as informações coletadas pela solução.

Emitir relatórios.

Aplicar patches sugeridos pela solução e acompanhar a instalação e resultados da instalação: se foi com sucesso, se houve erros, sugestões da ferramenta para correções.

Utilizar os computadores durante o processo de atualização dos patches e observar se há lentidão, mensagens ou erros no computador.

4.3 – Adjudicação do objeto com a indicação e justificativa da forma escolhida

A adjudicação se dará por grupos contendo itens, podendo uma empresa ser a vencedora de mais de um grupo, visando à obtenção de proposta mais vantajosa através do aumento de competitividade.

4.4 – Modalidade e o tipo de licitação

Será adotada a modalidade de pregão eletrônico por menor preço, para formação de Ata de Registro de Preços, de modo que o serviço seja prestado conforme a demanda / necessidade de cada Tribunal participante desta aquisição conjunta.

4.5 – Classificação orçamentária e indicação da fonte de recurso

Recursos previstos no orçamento 2022, cuja classificação será oportunamente registrada quando da formalização dos contratos decorrentes das atas de de Registro de Preços.

4.6 – Vigência e a indicação do prazo de garantia dos bens e/ou prestação dos serviços contratados

Os contratos originados a partir desta aquisição terão vigência de 60 meses para os grupos 1,3 e 5 e de 24 meses, prorrogáveis pelo período legal.

4.7 – Equipe de Apoio à Contratação

<inciso VII do Art. 16 da Res. CNJ 182/2013:

Indicar os integrantes da Equipe de Apoio à Contratação, se necessário.>

4.8 – Equipe de Gestão da Contratação

<inciso VIII do Art. 16 da Res. CNJ 182/2013:

Indicar os integrantes da Equipe de Gestão da Contratação (fiscais).>

5 – Análise de Riscos

A Análise de Riscos segue em documento anexo.

6 – Declaração de Viabilidade da Contratação

São Paulo, em xx/xx/xx.

Diante dos estudos realizados opinamos pela viabilidade da Contratação.

<nome>	<nome>	<nome>
Equipe de Planejamento da Contratação		

Aprovo a viabilidade da Contratação.

<nome>
<Titular da área Demandante>