

INSTITUTO NACIONAL DE TRAUMATO-ORTOPEDIA

Estudo Técnico Preliminar 131/2026

1. Informações Básicas

Número do processo: 25057.007469/2026-92

2. Descrição da necessidade

A presente necessidade da Administração do Instituto Nacional de Traumatologia e Ortopedia (INTO) consiste na contratação de solução tecnológica unificada e automatizada para o mapeamento, inventário, governança e monitoramento contínuo de seu parque tecnológico, estimado em 2000 (dois mil) ativos de rede, incluindo servidores e estações de trabalho.

A demanda visa substituir o atual modelo de levantamento manual e descentralizado, que gera opacidade informacional, ineficiência orçamentária (risco de licenças ociosas e obsolescência não mapeada) e impossibilita a auditoria de conformidade de licenciamento (*compliance*) em tempo real. Sem uma plataforma de automação, a capacidade técnica de identificar dispositivos não homologados e softwares legados torna-se severamente comprometida.

Sob a ótica da Segurança da Informação, a atual carência de controle sobre os *endpoints* expõe a infraestrutura crítica do INTO a vulnerabilidades cibernéticas, ameaçando a integridade e a confidencialidade dos dados clínicos e administrativos processados, bem como a continuidade dos serviços de saúde prestados aos pacientes.

Dessa forma, a contratação é medida imperativa para resguardar a capacidade operacional do Instituto, mitigar riscos cibernéticos e assegurar o estrito cumprimento do Programa de Privacidade e Segurança da Informação (PPSI) do Governo Federal (MGI). A solução alinhará a governança de TIC do INTO às melhores práticas internacionais de segurança, a exemplo do *CIS Critical Security Controls*, garantindo o nível de maturidade regulatória exigido pelos órgãos de controle.

3. Área requisitante

Área Requisitante	Responsável
Divisão de Tecnologia da Informação e Comunicação - DITEC	André Luiz Silva Ferreira

4. Necessidades de Negócio

O INTO necessita aprimorar sua capacidade institucional de gerenciar, monitorar e proteger os recursos tecnológicos sob sua responsabilidade, de forma centralizada, automatizada e alinhada às melhores práticas de governança de TIC e aos requisitos regulatórios da Administração Pública Federal.

4.1 Objetivos Específicos de Negócio

a) Ampliar a eficiência operacional da gestão de TIC Eliminar a dependência de processos manuais, fragmentados e propensos a erros humanos nas atividades de inventário, controle e manutenção dos ativos tecnológicos, liberando a equipe técnica para atividades de maior valor estratégico.

b) Garantir conformidade regulatória plena Assegurar o atendimento às exigências do Programa de Privacidade e Segurança da Informação (PPSI), aos controles dos CIS Critical Security Controls e às determinações da Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente no que diz respeito à gestão de ativos que processam dados pessoais e sensíveis.

c) Elevar o nível de rastreabilidade e governança dos ativos Estabelecer mecanismos que assegurem visibilidade permanente, precisa e auditável sobre todo o parque tecnológico institucional, incluindo hardware, software e configurações dos ativos, fornecendo base confiável para prestação de contas a órgãos de controle.

d) Reduzir a exposição a riscos de segurança da informação Aprimorar a capacidade institucional de identificar, priorizar e mitigar riscos e vulnerabilidades no ambiente tecnológico, reduzindo a probabilidade de ocorrência de incidentes de segurança e seus impactos sobre a continuidade dos serviços assistenciais e administrativos do INTO.

- e) Otimizar a gestão de custos com recursos tecnológicos** Identificar e eliminar gastos desnecessários com licenças de software não utilizadas, equipamentos obsoletos e recursos duplicados, fundamentando as decisões de investimento em dados precisos e atualizados sobre o parque tecnológico.
- f) Fortalecer a capacidade de resposta a incidentes** Reduzir o tempo médio de identificação, contenção e recuperação de incidentes de segurança ou falhas operacionais que afetem os ativos tecnológicos e os serviços por eles suportados.
- g) Subsidiar a tomada de decisão estratégica em TIC** Prover à gestão institucional informações confiáveis, atualizadas e estruturadas sobre o parque tecnológico, que fundamentem o planejamento estratégico, a elaboração e revisão do PDTIC e as decisões de alocação de recursos em TIC.
- h) Mensurar a qualidade da experiência digital dos usuários** Estabelecer mecanismos objetivos para avaliar o desempenho dos ativos tecnológicos sob a perspectiva do usuário final, identificando gargalos que impactam a produtividade e a qualidade do atendimento prestado pelo Instituto.

5. Necessidades Tecnológicas

5.1 Capacidades Tecnológicas Requeridas

Em correspondência direta com os objetivos de negócio identificados na seção 4, a solução a ser adotada pelo INTO deverá possuir as seguintes capacidades tecnológicas:

5.1.1 Descoberta e Inventário Automatizado de Ativos: Capacidade de identificação automática e contínua de todos os dispositivos conectados à rede institucional, incluindo aqueles sem componente de gerenciamento instalado, com coleta de informações detalhadas de hardware e software em tempo real ou em intervalos programáveis. A coleta deve abranger, no mínimo: hardware (fabricante, modelo, processador, memória, armazenamento), software (nome, versão, fornecedor, uso), configurações de sistema, usuários conectados e conexões de rede ativas.

5.1.2 Gerenciamento Centralizado de Atualizações e Correções: Capacidade de distribuir, aplicar e monitorar a instalação de atualizações de sistemas operacionais e aplicativos de forma automatizada, a partir de repositório centralizado, com suporte a janelas de manutenção programadas, rollback em caso de falha e rastreabilidade do status de aplicação por ativo.

5.1.3 Análise Contínua de Vulnerabilidades e Conformidade: Capacidade de identificar, catalogar e priorizar vulnerabilidades conhecidas presentes nos ativos gerenciados, com base em parâmetros de criticidade padronizados, e de avaliar a conformidade das configurações dos ativos em relação a padrões de segurança de referência da indústria. Deve incluir a capacidade de quantificação e evolução temporal do risco do ambiente.

5.1.4 Gestão Centralizada de Configuração: Capacidade de definir, distribuir, monitorar e enforcing políticas de configuração segura nos ativos gerenciados, incluindo restrições de aplicações, controle de dispositivos de armazenamento externo e padronização de parâmetros de segurança.

5.1.5 Automação de Respostas a Incidentes: Capacidade de executar ações automatizadas de resposta a eventos de segurança ou desvios de conformidade, incluindo isolamento de ativos comprometidos, execução de scripts de remediação e notificação de responsáveis, sem necessidade de intervenção manual imediata.

5.1.6 Distribuição e Gestão de Software: Capacidade de distribuir, instalar, atualizar e remover aplicações nos ativos gerenciados de forma centralizada, automatizada e rastreável, com suporte a distribuição condicional baseada em atributos dos ativos e com mecanismos de otimização de consumo de banda de rede.

5.1.7 Controle de Acesso Baseado em Perfis e Integração com Gerenciamento de Identidades: Capacidade de implementar controle de acesso à plataforma de gerenciamento com segregação de funções por perfis de permissão, com suporte à integração com provedores de identidade corporativos para autenticação centralizada e gerenciamento de usuários.

5.1.8 Integração com Sistemas Corporativos de Segurança e Gestão: Capacidade de integração nativa ou por meio de interfaces programáticas com sistemas de monitoramento de segurança (SIEM), plataformas de gestão de serviços de TI (ITSM) e outros componentes do ecossistema tecnológico institucional, garantindo a interoperabilidade da solução com o ambiente existente.

5.1.9 Trilhas de Auditoria e Relatórios de Conformidade: Capacidade de registrar, armazenar e exportar logs detalhados de todas as operações realizadas na plataforma e nos ativos gerenciados, com suporte à geração de relatórios customizáveis e à exportação em múltiplos formatos para atendimento a auditorias e exigências regulatórias.

5.1.10 Gestão de Certificados Digitais: Capacidade de identificar, monitorar e alertar sobre o status dos certificados digitais instalados nos ativos gerenciados, incluindo a identificação de certificados expirados ou próximos à data de expiração.

5.1.11 Mensuração da Experiência Digital do Usuário: Capacidade de coletar, agregar e apresentar métricas sobre o desempenho dos ativos e das aplicações sob a perspectiva do usuário final, com suporte à realização de pesquisas de satisfação diretamente nos dispositivos gerenciados e ao cálculo automatizado de indicadores de experiência.

5.1.12 Escalabilidade e Disponibilidade: A solução deverá ser capaz de gerenciar o volume total de ativos identificados no Instituto sem degradação de desempenho, com disponibilidade compatível com as necessidades operacionais de um ambiente de saúde em funcionamento contínuo.

5.1.13 Segurança das Comunicações: A comunicação entre os componentes de gerenciamento instalados nos ativos e a plataforma central deverá ser protegida por criptografia de ponta a ponta, garantindo a confidencialidade e a integridade dos dados transmitidos.

5.1.14 Agente Único Unificado: A plataforma deverá ser capaz de exercer todas as capacidades tecnológicas requeridas por meio de um único componente instalado nos ativos gerenciados, evitando a multiplicidade de agentes que aumenta a complexidade operacional, o consumo de recursos dos endpoints e os riscos de conflitos de software.

5.1.15 Suporte a Múltiplos Sistemas Operacionais A solução deverá suportar o gerenciamento de ativos que executam os sistemas operacionais presentes no parque tecnológico do INTO, incluindo diferentes versões de sistemas operacionais do tipo Windows, Linux e macOS, além de sistemas operacionais legados eventualmente presentes no ambiente.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Além dos requisitos tecnológicos descritos, a solução contratada deverá atender, cumulativamente, aos seguintes requisitos adicionais:

6.1 Requisitos Legais

A solução e o processo de sua contratação deverão estar em plena conformidade com os seguintes instrumentos normativos:

- **Lei nº 14.133/2021** — Lei de Licitações e Contratos Administrativos;
- **Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022** — Disciplina o processo de contratação de soluções de TIC pela Administração Pública Federal direta, autárquica e fundacional;
- **Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021** — Estabelece procedimentos para realização de pesquisa de preços para aquisições de bens e contratação de serviços em geral;
- **Lei nº 13.709, de 14 de agosto de 2018 (LGPD)** — Lei Geral de Proteção de Dados Pessoais;
- **Decreto nº 10.947/2022** — Regulamenta a Lei nº 14.133/2021;
- **Portaria nº 586/ INTO, de 22 de maio de 2023** — Plano de Logística Sustentável do INTO (PLS);
- **Constituição Federal, art. 37** — Princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.

6.2 Requisitos Regulatórios e de Conformidade

- Plena aderência ao **Programa de Privacidade e Segurança da Informação (PPSI)** do Governo Federal, instituído pelo Ministério da Gestão e da Inovação em Serviços Públicos (MGI);
- Conformidade com os **CIS Critical Security Controls (CIS Controls)**, adotados como framework de referência pelo PPSI, em especial os controles: CIS 1 (Inventário de Ativos Empresariais), CIS 2 (Inventário de Ativos de Software), CIS 4 (Configuração Segura), CIS 5 (Gestão de Contas), CIS 7 (Gestão de Vulnerabilidades Contínua) e CIS 11 (Recuperação de Dados);
- Observância às diretrizes da **Estratégia de Governo Digital (EGD) 2024–2027**, especialmente no que concerne à segurança e privacidade digital dos serviços governamentais;
- Aderência à **Política de Segurança da Informação do INTO**.

6.3 Requisitos de Proteção de Dados Pessoais (LGPD)

- A solução e seus processos de operação deverão respeitar os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, previstos no art. 6º da LGPD;
- Os dados coletados e processados pela solução deverão ser tratados exclusivamente para as finalidades declaradas, sendo vedado o uso para finalidades incompatíveis;
- A solução deverá dispor de mecanismos que assegurem a rastreabilidade do tratamento de dados pessoais eventualmente coletados, em cumprimento ao art. 37 da LGPD.

6.4 Requisitos de Segurança da Informação

- A solução deverá manter comunicações criptografadas entre todos os seus componentes, com protocolo de segurança que atenda aos padrões de mercado vigentes à época da contratação;
- Toda operação realizada na plataforma deverá ser registrada em trilha de auditoria não manipulável;
- A solução deverá implementar controle de acesso com segregação de funções, impedindo que um único usuário concentre permissões incompatíveis;
- A solução deverá suportar autenticação multifator para acesso à console de administração;
- Os dados coletados e armazenados pela solução deverão permanecer sob controle do INTO, sendo vedada sua utilização para fins comerciais por parte do fornecedor.

6.5 Requisitos de Suporte Técnico e Garantia

- **Regime de Suporte Técnico:** Atendimento especializado em caráter 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano), englobando modalidades remota e presencial (*on-site*), dimensionadas de acordo com a complexidade do chamado.
- **Vigência da Garantia:** Cobertura técnica mínima de 24 (vinte e quatro) meses, com marco inicial a partir do recebimento definitivo do objeto.
- **Qualificação da Força de Trabalho:** Atendimento, suporte ou sustentação executados por profissionais com comprovado domínio técnico, treinamento especializado ou expertise na arquitetura da solução adotada, de modo a garantir a continuidade, a segurança e a qualidade dos serviços.
- **Canais de Atendimento:** Disponibilidade de plataforma eletrônica dedicada (24x7) para abertura e rastreamento de chamados, além de suporte telefônico complementar durante o horário comercial padrão (8h por dia, 5 dias por semana).
- **Janelas de Manutenção Crítica:** Planejamento prévio e execução de intervenções estruturais no ambiente de produção do INTO obrigatoriamente fora dos horários de pico operacional, ressalvadas as excepcionalidades de emergência.

6.6 Requisitos Temporais

- A entrega e disponibilização da solução deverá ocorrer no prazo máximo de **90 (noventa) dias corridos**, contados do recebimento da Ordem de Serviços (OS), prorrogáveis por até 30 dias mediante justificativa prévia aprovada pela Contratante;
- A instalação deverá ser iniciada em, no máximo, **7 (sete) dias** após a emissão da Ordem de Início dos Serviços (OIS);
- A documentação técnica (*as-built*) deverá ser entregue em até **15 (quinze) dias úteis** após a conclusão da implantação.

6.7 Requisitos de Capacitação

- **Serviços de Capacitação:** Previsão de repasse de conhecimento prático (*hands-on*) sobre a solução tecnológica a ser adotada.
- **Dimensionamento:** Estimativa de uma turma com até 10 (dez) participantes e carga horária mínima de 16 (dezesesseis) horas cada.
- **Conteúdo Programático:** Abordagem mínima necessária englobando: visão geral e arquitetura da solução; instalação e configuração; gestão de acessos e perfis; configuração de varreduras e descoberta de ativos; gestão e aplicação de patches; análise de vulnerabilidades e conformidade; automação e resposta a incidentes; auditoria e segurança; e resolução de problemas (*troubleshooting*).
- **Insumos Didáticos:** Necessidade de fornecimento de todo o material didático correspondente, integrado ao escopo da solução.
- **Certificação:** Emissão de certificado individual com registro de carga horária e conteúdo programático.

6.8 Requisitos de Implantação e Implementação

- **Planejamento de Implantação:** Necessidade de elaboração prévia de um Plano de Instalação e Configuração, contemplando o detalhamento de etapas, cronograma, matriz de responsabilidades e análise de impactos operacionais.
- **Janelas de Execução:** Requisito de que as intervenções de implantação ocorram sem interrupção dos serviços em ambiente de produção, priorizando janelas de menor impacto para as atividades assistenciais do Instituto.
- **Qualificação Técnica:** Exigência de que os serviços sejam conduzidos por profissionais com comprovada expertise e domínio técnico sobre a arquitetura da solução adotada.

- **Diretriz de Execução Direta:** Previsão de vedação à subcontratação do objeto, visando mitigar riscos e assegurar a centralização da responsabilidade técnica e de segurança da informação.

6.9 Requisitos de Qualificação Técnica

- Previsão de atestado(s) de capacidade técnica compatível com o objeto, comprovando o gerenciamento prévio de, no mínimo, 50% do quantitativo estimado de ativos, nos termos do art. 67, § 2º, da Lei nº 14.133/2021.

6.10 Requisitos Socioambientais e de Sustentabilidade

- A contratação deverá observar o **Plano de Logística Sustentável do INTO (Portaria nº 586/2023)** e o **Guia Nacional de Contratações Sustentáveis**;
- Por tratar-se de licenças e serviços digitais, a contratação não implica geração de resíduos sólidos significativos, sendo os impactos ambientais considerados irrelevantes para fins do art. 11 da IN SGD/ME nº 94/2022

6.11 Requisitos de Interoperabilidade

- A solução deverá possuir interface programática (API) documentada que permita a exportação de dados de inventário, telemetria e atributos dos ativos gerenciados para outros sistemas institucionais;
- A solução deverá suportar integração com sistemas de monitoramento de segurança (SIEM) amplamente utilizados no mercado;
- A solução deverá suportar integração com plataformas de gestão de serviços de TI (ITSM) para sincronização da base de ativos gerenciados com a base de itens de configuração do ITSM;
- A solução deverá suportar integração com provedores de identidade corporativos para autenticação centralizada dos administradores da plataforma, por meio de protocolos de mercado padronizados.

7. Estimativa da demanda - quantidade de bens e serviços

A demanda foi estimada com base no levantamento físico e lógico do parque tecnológico atual do Instituto Nacional de Traumatologia e Ortopedia (INTO) e nas projeções de crescimento da infraestrutura estipuladas para o período de vigência contratual. Os quantitativos consolidados e os respectivos códigos do catálogo de serviços (CATSER) estão dispostos na tabela abaixo:

Grupo	Item	Descrição	CATSER	Quantidade	Unidade
1	1	Subscrição da solução de gerenciamento unificado de ativos <i>endpoints</i> , com suporte e garantia técnica por 24 meses	27502	2000	UN
	2	Serviços técnicos especializados de instalação, configuração e repasse de conhecimento	26972	1	UN

7.1. Memória de Cálculo

A) Subscrição da Solução (Item 1):

O quantitativo de 2000 endpoints consolida os ativos que requerem monitoramento e governança, distribuídos da seguinte forma:

- **Estações de Trabalho (Desktops e Notebooks): 1600** unidades ativas utilizadas pelas áreas assistenciais e administrativas.
- **Servidores (Físicos e Virtuais): 300** unidades que compõem o datacenter local e sustentam os serviços críticos.
- **Margem de Expansão (Reserva Técnica): 100** licenças para cobrir novas aquisições previstas no PDTIC.

- **Total Nominal:** 2000 endpoints.

B) Serviços Técnicos e Repasse de Conhecimento (Item 2):

- **Instalação e Configuração:** 1 (um) serviço para a ativação da console gerencial e parametrização do ambiente para os 2000 endpoints.
- **Repasse de Conhecimento:** 1 (uma) turma para capacitação técnica, dimensionada para até 10 (dez) colaboradores da DITEC. Este quantitativo é o suficiente para compor a equipe de administradores e operadores da ferramenta.

8. Levantamento de soluções

O levantamento de soluções foi conduzido a partir das capacidades tecnológicas identificadas na seção 5 e dos requisitos estabelecidos na seção 6. Foram pesquisadas alternativas que, individualmente ou em conjunto, pudessem atender, total ou parcialmente, às necessidades identificadas. O levantamento não considerou marcas, fabricantes ou produtos específicos nesta etapa, mas sim categorias e modelos de fornecimento disponíveis no mercado.

8.1 Alternativas Identificadas

Alternativa A — Desenvolvimento de Solução Própria (Interno)

Consiste no desenvolvimento, pela própria equipe da DITEC/INTO ou mediante contratação de fábrica de software, de uma plataforma proprietária de gerenciamento de ativos, customizada para as necessidades específicas do Instituto. Nessa modalidade, o INTO seria responsável pelo desenvolvimento, implantação, manutenção e evolução da solução ao longo do tempo.

Alternativa B — Adoção de Software Livre (Open Source)

Consiste na implantação de ferramentas disponíveis sob licença de código aberto, sem custo de aquisição, que ofereçam, nativamente ou mediante customização, funcionalidades de gerenciamento de ativos. Exemplos disponíveis no ecossistema incluem soluções de inventário e gerenciamento de TIC amplamente utilizadas em ambientes corporativos e governamentais.

Alternativa C — Solução Comercial em Modelo On-Premises

Consiste na aquisição de licenças perpétuas ou por subscrição de plataforma de gerenciamento de ativos comercial, com implantação e operação em servidores instalados no próprio datacenter do INTO. Nesse modelo, toda a infraestrutura necessária ao funcionamento da plataforma é provisionada e gerenciada pelo próprio Instituto.

Alternativa D — Solução Comercial em Modelo SaaS (Software as a Service)

Consiste na contratação de plataforma de gerenciamento de ativos disponibilizada integralmente em nuvem, no modelo de software como serviço, com acesso via console web. Nesse modelo, toda a infraestrutura da plataforma é operada pelo fornecedor, sem necessidade de provisionamento de servidores ou componentes de infraestrutura no datacenter do INTO.

Alternativa E — Expansão ou Adaptação de Ferramentas Existentes

Consiste no aproveitamento, expansão ou combinação de ferramentas de TIC já eventualmente em uso no INTO para cobrir, ao menos parcialmente, as capacidades tecnológicas identificadas na seção 5, sem a aquisição de nova plataforma.

Alternativa F — Contratação de Serviço Gerenciado de TIC (Managed Services)

Consiste na contratação de empresa especializada para prestar, de forma terceirizada, todos os serviços de gerenciamento de ativos de TI, incluindo a utilização das ferramentas necessárias. Nessa modalidade, o fornecedor é responsável pela plataforma, pela operação e pelos resultados contratados.

9. Análise comparativa de soluções

A comparação entre as alternativas foi conduzida com base nos seguintes critérios:

Critério	Descrição
Aderência aos requisitos	Capacidade de atender às necessidades tecnológicas (seção 5) e demais requisitos (seção 6)
Viabilidade técnica	Compatibilidade com o ambiente tecnológico do INTO
Viabilidade operacional	Capacidade da equipe interna de operar e sustentar a solução
Prazo de implantação	Tempo estimado para disponibilização plena da solução
Escalabilidade	Capacidade de suportar crescimento do parque tecnológico
Continuidade e suporte	Garantias de continuidade do serviço e acesso a suporte especializado
Riscos associados	Riscos técnicos, operacionais, de segurança e regulatórios

9.1. Comparação das Alternativas

Alternativa A — Desenvolvimento Interno

Benefícios: Solução totalmente customizada às necessidades do INTO; total autonomia sobre o código-fonte e a roadmap tecnológica; sem dependência de fornecedor externo para continuidade.

Limitações: Exige equipe interna com alto grau de especialização em segurança, desenvolvimento de software e gestão de ativos — perfil não disponível na DITEC na quantidade e qualidade necessárias; tempo de desenvolvimento longo, estimado em 18 a 36 meses para uma plataforma com o nível de maturidade requerido; necessidade de investimento contínuo em evolução da plataforma.

Riscos: Alto risco de entrega fora do prazo e do escopo planejado; risco de obsolescência tecnológica caso a equipe não mantenha o ritmo de atualização do mercado; risco de não conformidade com requisitos do PPSI e CIS Controls, caso as implementações de segurança não acompanhem as atualizações dos frameworks de referência; dependência de pessoas-chave da equipe de desenvolvimento.

Aderência aos requisitos: Potencialmente plena, porém condicionada a recursos e prazo não compatíveis com a urgência da demanda.

Alternativa B — Software Livre (Open Source)

Benefícios: Ausência de custo de licenciamento; transparência do código-fonte; possibilidade de customização; ecossistema comunitário ativo.

Limitações: Ausência de suporte técnico garantido em SLA contratual; necessidade de esforço técnico intensivo de customização, integração e manutenção; funcionalidades de segurança avançada — como análise de vulnerabilidades em tempo real, DEX, automação de resposta a incidentes e integrações nativas com SIEM/ITSM — geralmente não disponíveis nativamente, demandando desenvolvimento adicional; interface de gerenciamento e experiência de uso geralmente inferiores às soluções comerciais.

Riscos: Risco de não conformidade com o PPSI e com os CIS Controls, dado que as ferramentas open source frequentemente não cobrem todos os controles requeridos sem customização extensiva; risco operacional decorrente da dependência de comunidades externas para correção de vulnerabilidades na própria ferramenta de segurança; risco de dificuldade em atender aos requisitos de auditoria e de prestação de contas a órgãos de controle.

Aderência aos requisitos: Parcial; as capacidades requeridas nas seções 5.1.3, 5.1.5, 5.1.11 e 5.1.8 dificilmente são cobertas nativamente por soluções open source disponíveis, exigindo desenvolvimento complementar.

Alternativa C — Solução Comercial On-Premises

Benefícios: Controle total sobre a infraestrutura; dados mantidos no ambiente interno do INTO; possibilidade de personalização avançada; maturidade tecnológica e suporte técnico comercial garantido por SLA; aderência plena aos requisitos funcionais das seções 5 e 6.

Limitações: Exige provisionamento de infraestrutura dedicada (servidores de alta disponibilidade, banco de dados, servidores de backup, componentes de rede); requer equipe interna para administração da plataforma de gerenciamento; custos de CAPEX elevados para aquisição do hardware necessário; ciclos de atualização dependem de intervenção manual da equipe; tempo de implantação geralmente superior ao modelo SaaS.

Riscos: Risco de subutilização da infraestrutura provisionada; risco de obsolescência do hardware antes do fim do ciclo útil esperado; risco operacional caso a equipe interna não tenha capacidade suficiente para absorver a administração da plataforma em paralelo às demais responsabilidades.

Aderência aos requisitos: Plena para os requisitos funcionais; restrições nos requisitos de disponibilidade e escalabilidade caso a infraestrutura não seja provisionada adequadamente.

Alternativa D — Solução Comercial SaaS

Benefícios: Disponibilização sem necessidade de infraestrutura local dedicada; atualizações automáticas realizadas pelo fornecedor; alta disponibilidade gerenciada; escalabilidade sob demanda; menor tempo de implantação; acesso via console web sem necessidade de VPN; suporte técnico comercial garantido por SLA.

Limitações: Dependência da conectividade com a internet para acesso à console de gerenciamento; dados armazenados em infraestrutura do fornecedor, exigindo cláusulas contratuais adequadas sobre soberania e proteção dos dados; menor grau de personalização de infraestrutura em relação ao modelo on-premises.

Riscos: Risco de descontinuidade do serviço pelo fornecedor (mitigável por cláusulas contratuais); risco de variação cambial em contratos internacionais; risco de conformidade com a LGPD relativo ao armazenamento de dados em servidores externos (mitigável por contratação de fornecedores com data centers em território nacional ou por cláusulas de proteção de dados adequadas).

Aderência aos requisitos: Plena para todos os requisitos das seções 5 e 6.

Alternativa E — Expansão de Ferramentas Existentes

Benefícios: Potencial reaproveitamento de licenças e investimentos já realizados; menor curva de aprendizado para a equipe.

Limitações: O INTO não dispõe, na configuração atual, de ferramentas que cubram as capacidades tecnológicas requeridas nas seções 5.1.1 a 5.1.15 em escopo e profundidade suficientes; eventual expansão de ferramentas pontuais resultaria em múltiplos agentes instalados nos endpoints, consoles de gerenciamento fragmentados e ausência de visão unificada — contrariando os requisitos identificados.

Riscos: Risco de lacunas funcionais permanentes; risco de não conformidade com o PPSI por cobertura incompleta dos controles requeridos.

Aderência aos requisitos: Baixa; não há ferramentas existentes no INTO passíveis de expansão para cobrir o escopo total das necessidades identificadas.

Alternativa F — Serviço Gerenciado (Managed Services)

Benefícios: Transferência da responsabilidade operacional para empresa especializada; SLA sobre resultados; sem necessidade de especialistas internos dedicados.

Limitações: Menor visibilidade e controle direto sobre as operações de TIC; dependência elevada do fornecedor para informações sobre o próprio parque tecnológico; dificuldade de internalização de conhecimento pela equipe do INTO; custos recorrentes tipicamente superiores às demais alternativas.

Riscos: Risco de lock-in operacional com o fornecedor; risco de descontinuidade do serviço; risco de conflito de interesses caso o fornecedor gerencie informações sensíveis sobre a infraestrutura crítica do Instituto; riscos regulatórios relacionados ao acesso de terceiros a sistemas que processam dados sensíveis de saúde.

Aderência aos requisitos: Potencialmente plena para os requisitos funcionais, porém com restrições nos requisitos de segurança da informação, LGPD e governança, dada a natureza crítica dos dados gerenciados.

10. Registro de soluções consideradas inviáveis

10.1 Critérios de Inviabilidade

Uma alternativa é classificada como inviável quando apresenta, isoladamente ou em combinação, os seguintes elementos: incapacidade de atender aos requisitos mínimos estabelecidos nas seções 5 e 6; inviabilidade operacional decorrente de insuficiência de recursos humanos especializados no INTO; inviabilidade econômica demonstrada por relação custo-benefício desfavorável; ou inviabilidade jurídica decorrente de incompatibilidade com as normas aplicáveis à contratação pública.

10.2 Alternativa A — Desenvolvimento Interno: INVIÁVEL

Justificativa técnica: O desenvolvimento de uma plataforma com o nível de maturidade e a cobertura funcional requeridas nas seções 5 e 6 demanda competências técnicas altamente especializadas em segurança de endpoints, desenvolvimento de software de infraestrutura, gerenciamento de

vulnerabilidades e integração com sistemas SIEM/ITSM. A DITEC/INTO não dispõe, em seu quadro atual, de profissionais com o perfil e a quantidade necessários para absorver tal demanda sem comprometimento das atividades operacionais regulares.

Justificativa operacional: O prazo estimado para desenvolvimento, testes, homologação e implantação de uma solução com as capacidades requeridas é incompatível com a urgência da necessidade identificada e com os riscos operacionais e regulatórios em curso. A equipe técnica da DITEC está plenamente alocada na operação e manutenção da infraestrutura existente, sem capacidade ociosa para absorver um projeto de desenvolvimento de tal porte.

Justificativa econômica: Os custos de desenvolvimento — incluindo contratação de profissionais especializados ou fábrica de software, infraestrutura de desenvolvimento e testes, e manutenção evolutiva — superariam, em estimativas preliminares, os custos de uma solução comercial madura, sem apresentar benefícios compensatórios. Adicionalmente, os custos de manutenção contínua seriam permanentes e crescentes.

Justificativa regulatória: O desenvolvimento e a manutenção de uma plataforma própria para atender às exigências do PPSI e dos CIS Controls demandaria acompanhamento contínuo das atualizações desses frameworks, com implementação tempestiva das novas exigências — esforço que não é compatível com a capacidade técnica e operacional disponível no INTO.

10.3 Alternativa B — Software Livre (Open Source): INVIÁVEL

Justificativa técnica: As soluções open source disponíveis no ecossistema de gerenciamento de ativos de TIC não cobrem, nativamente, as capacidades tecnológicas requeridas nas seções 5.1.3 (análise contínua de vulnerabilidades com pontuação de risco), 5.1.5 (automação de respostas a incidentes), 5.1.11 (mensuração da experiência digital do usuário com scores automatizados) e 5.1.8 (integração nativa com SIEM e ITSM). A cobertura dessas lacunas exigiria desenvolvimento adicional de componentes proprietários, redirecionando o modelo para uma variante da Alternativa A.

Justificativa operacional: A implantação, customização, integração, atualização e manutenção de solução open source requer equipe técnica dedicada com perfil de desenvolvedor de software e especialista em segurança — recurso não disponível na DITEC/INTO em quantidade e especialização suficientes.

Justificativa regulatória: A ausência de SLA contratual garantido e de responsabilidade jurídica formalmente atribuída a um fornecedor pela conformidade da solução com o PPSI, a LGPD e os CIS Controls representa risco regulatório incompatível com as exigências do ambiente da Administração Pública Federal. Em caso de incidente de segurança ou de apontamento por órgão de controle, o INTO não teria contrato ou responsável técnico formalmente habilitado para responder pelas falhas da plataforma.

10.4 Alternativa E — Expansão de Ferramentas Existentes: INVIÁVEL

Justificativa técnica: O INTO não dispõe, em sua infraestrutura atual, de ferramentas passíveis de expansão que cobririam, individualmente ou em conjunto, as capacidades tecnológicas requeridas nas seções 5.1.1 a 5.1.15, com o nível de integração, automação e rastreabilidade exigidos. Qualquer combinação de ferramentas pontuais resultaria em múltiplos agentes instalados nos endpoints, consoles fragmentados e ausência de visão unificada — contrariando diretamente o requisito 5.1.14 (agente único) e inviabilizando o atendimento ao requisito 5.1.9 (trilhas de auditoria centralizadas).

Justificativa operacional: A gestão de múltiplas ferramentas heterogêneas aumentaria, e não reduziria, a complexidade operacional da DITEC, contrariando o objetivo de negócio 4.2.a (ampliar a eficiência operacional).

10.5 Alternativa F — Serviço Gerenciado (Managed Services): INVIÁVEL

Justificativa de segurança e regulatória: O acesso de terceiros às operações de gerenciamento de ativos que incluem dados de configuração de sistemas críticos de saúde, dados de usuários e credenciais de acesso representa risco de segurança e de conformidade com a LGPD incompatível com o perfil de risco aceitável pelo INTO. A natureza dos dados processados pelos sistemas gerenciados — incluindo informações de pacientes e dados governamentais sensíveis — exige que o controle operacional permaneça sob responsabilidade direta da equipe do Instituto.

Justificativa de governança: O modelo de managed services implica dependência elevada do fornecedor para obtenção de informações sobre a própria infraestrutura tecnológica do Instituto, reduzindo a capacidade de governança interna e dificultando o cumprimento dos objetivos estratégicos de rastreabilidade e prestação de contas do PDTIC 2025–2026.

11. Análise comparativa de custos (TCO)

11.1 Alternativas Viáveis para Análise de TCO

Com base na análise comparativa da seção 9 e no registro de inviabilidades da seção 10, as alternativas que permanecem viáveis para análise de TCO são:

- **Alternativa C:** Solução Comercial On-Premises
- **Alternativa D:** Solução Comercial SaaS

11.2 Metodologia e Componentes do TCO

O TCO foi calculado para o horizonte de **24 meses**, correspondente ao período de cobertura planejado, considerando os seguintes componentes de custo:

Componente de Custo	Definição
Aquisição/Licenciamento	Custos de compra de licenças ou subscrição da plataforma
Infraestrutura	Custos de hardware, sistemas operacionais e rede dedicados à plataforma
Implantação	Custos de instalação, configuração e integração com o ambiente existente
Capacitação	Custos de treinamento da equipe técnica do INTO
Suporte e Garantia	Custos de suporte técnico e manutenção corretiva pelo período contratual
Atualizações	Custos de atualização de versões da plataforma e do ambiente de suporte
Operação	Custos de mão de obra interna para administração da plataforma
Riscos e Contingências	Estimativa de custos decorrentes de falhas, indisponibilidade e retrabalho

11.3 TCO — Alternativa C: Solução Comercial On-Premises (24 meses)

Componente	Estimativa Qualitativa	Observações
Licenciamento	Alto	Licenças perpétuas ou anuais com custo de renovação
Infraestrutura	Alto	Necessidade de 2 servidores físicos em HA + storage dedicado + SO
Implantação	Médio	Serviços de implantação pelo fornecedor
Capacitação	Médio	Treinamento sobre a plataforma
Suporte e Garantia	Médio	Contratos de suporte anual com o fabricante
Atualizações	Médio	Requer intervenção da equipe técnica e janelas de manutenção
Operação	Alto	Necessidade de administrador dedicado à plataforma no quadro do INTO
Riscos/Contingências	Alto	Risco de falha de hardware, obsolescência e subutilização
TCO 24 meses	Alto	Predominância de CAPEX com impacto orçamentário concentrado

Características relevantes para o TCO On-Premises:

Os custos de infraestrutura representam componente significativo do TCO total, dado que a alternativa exige, no mínimo: 2 servidores físicos configurados em alta disponibilidade (HA); licenciamento de sistema operacional de servidor; solução de backup dedicada; adequação de racks e cabeamento no datacenter do INTO; e provisionamento de equipe interna para administração da plataforma.

O modelo CAPEX intensivo implica concentração do desembolso orçamentário nos primeiros meses, com impacto relevante no planejamento financeiro do exercício.

A obsolescência do hardware adquirido representa custo de reposição ao final do ciclo de vida, que pode ocorrer dentro ou logo após o período de vigência contratual de 24 meses.

A necessidade de um administrador interno dedicado à plataforma representa custo de oportunidade relevante — capacidade de mão de obra especializada que deixa de estar disponível para outras atividades da DITEC.

11.4 TCO — Alternativa D: Solução Comercial SaaS (24 meses)

Componente	Estimativa Qualitativa	Observações
Subscrição	Médio	Custos previsíveis distribuídos ao longo da vigência contratual
Infraestrutura	Nulo	Não requer hardware ou SO dedicados no datacenter do INTO
Implantação	Médio	Serviços de implantação e configuração pelo fornecedor
Capacitação	Médio	Treinamento sobre a plataforma
Suporte e Garantia	Incluído	Geralmente incorporado ao valor da subscrição
Atualizações	Nulo	Realizadas automaticamente pelo fornecedor
Operação	Baixo	Menor necessidade de administração de infraestrutura interna
Riscos/Contingências	Baixo	Responsabilidade de disponibilidade e continuidade do fornecedor
TCO 24 meses	Médio-Baixo	Modelo OPEX com desembolso distribuído e previsível

Características relevantes para o TCO SaaS:

O modelo de subscrição distribui os custos ao longo do período contratual, facilitando o planejamento orçamentário anual e o controle de execução financeira.

A eliminação dos custos de infraestrutura local representa economia direta e mensurável, pois dispensa investimentos em hardware de servidor, licenciamento de SO, backup dedicado e adequação de datacenter.

A realização automática de atualizações pelo fornecedor elimina os custos operacionais e os riscos associados ao gerenciamento manual de versões, bem como os custos de janelas de manutenção para aplicação de patches na própria plataforma de gerenciamento.

O menor esforço de administração interna da plataforma, comparativamente ao modelo on-premises, representa redução do custo de oportunidade da equipe da DITEC.

11.5 Síntese Comparativa de TCO

Componente de Custo	On-Premises	SaaS
Licenciamento/Subscrição	Alto (CAPEX)	Médio (OPEX distribuído)
Infraestrutura dedicada	Alto	Nulo
Implantação	Médio	Médio
Capacitação	Médio	Médio
Suporte/Garantia	Médio	Incluído na subscrição
Atualizações	Médio (esforço interno)	Nulo (automático)
Operação/Administração interna	Alto	Baixo
Riscos e contingências	Alto	Baixo
TCO Total Estimado — 24 meses	Alto	Médio-Baixo
Modelo financeiro	CAPEX intensivo	OPEX previsível

12. Descrição da solução de TIC a ser contratada

12.1 Solução Escolhida

Plataforma comercial de Gerenciamento Unificado de Ativos de TI, disponibilizada na modalidade *Software as a Service* (SaaS), consolidada no mercado tecnológico por sua maturidade e alta disponibilidade técnica. A solução abrangerá o fornecimento continuado da plataforma de software, atrelado a suporte e garantia técnica por 24 (vinte e quatro) meses e serviços especializados de implantação, parametrização e repasse de conhecimento.

12.2 Escopo da Contratação

A contratação está organizada em um único Grupo (Grupo 01), composto por dois itens tecnicamente interdependentes:

Item 1 — Subscrição da plataforma SaaS para gerenciamento de até 2000 endpoints (24 meses)

Compreende o direito de acesso e uso pleno da plataforma, incluindo suporte técnico e garantia pelo período de vigência contratual, abrangendo as capacidades relacionadas abaixo.

Item 2 — Serviços técnicos especializados de instalação, configuração e repasse de conhecimento

Compreende todos os serviços necessários à implantação da plataforma no ambiente do INTO e à capacitação da equipe técnica para operação autônoma.

12.3 Modelo de Fornecimento e Licenciamento

- **Modelo:** Software as a Service (SaaS), sem necessidade de instalação de servidores, componentes de infraestrutura ou VPN no ambiente do INTO;
- **Acesso:** Console web unificada, acessível de qualquer navegador, com todas as funcionalidades da plataforma disponíveis em uma única interface;
- **Cobertura:** de 2000 **endpoints**, incluindo estações de trabalho, notebooks, servidores físicos, máquinas virtuais e thin clients;
- **Prazo de subscrição:** 24 (vinte e quatro) meses, contados da emissão do Termo de Recebimento Definitivo;
- **Agente:** Único agente unificado e oculto ao usuário final, responsável por todas as funcionalidades da plataforma.

12.4 Sistemas Operacionais Suportados

A plataforma deverá suportar o gerenciamento de endpoints com os seguintes sistemas operacionais: Windows (versões 10, 11, Server 2016, 2019, 2022); Linux (Red Hat Enterprise Linux, CentOS, Ubuntu, Debian, Oracle Linux, SUSE Linux); macOS (versões suportadas pelo fabricante); IBM AIX; e Solaris.

12.5 Capacidades e Funcionalidades da Plataforma

A plataforma contratada deverá oferecer, no mínimo, as seguintes capacidades e funcionalidades integradas:

Gestão de Inventário (HWAM/SWAM): Coleta automatizada e em tempo real de inventário de hardware e software; descoberta de dispositivos não gerenciados na rede sem agente instalado; consultas de inventário em segundos; envio apenas de delta de alterações para minimizar consumo de banda; medição de uso de softwares com métricas de tempo e frequência; identificação de padrões de uso e software não utilizado.

Gerenciamento de Patches: Repositório centralizado de patches dos fabricantes de sistemas operacionais sem necessidade de empacotamento manual; aplicação automatizada com janelas de manutenção programáveis; histórico de patches por ativo; status de reinicialização pós-patch; suporte a distribuição *peer-to-peer* para otimização de banda.

Análise de Vulnerabilidades e Conformidade: Identificação e priorização de vulnerabilidades com base em parâmetros de criticidade padronizados (CVE/CVSS); cálculo de pontuação de risco de todo o ambiente com evolução temporal; avaliação de conformidade com padrões de segurança de referência.

Gestão de Configuração: Definição, distribuição e enforcement de políticas de configuração segura; automação de regras para eliminação de programas não autorizados e interrupção de funções ociosas.

Distribuição e Gestão de Software: Implantação, atualização e remoção de aplicações de forma centralizada e condicional; upload, download e remoção de arquivos nos endpoints; suporte a grupos de software com atualização dinâmica.

Automação de Respostas: Recursos de automação sem código (*no-code playbooks*) para configuração de respostas automáticas a eventos detectados; isolamento de endpoints comprometidos; execução de scripts de remediação.

Controle de Acesso (RBAC): Controle de acesso baseado em perfis com segregação de funções; perfis pré-configurados e customizáveis; integração com provedores de identidade via SAML 2.0 (iDP) para autenticação centralizada, sincronização e aplicação de políticas por grupos.

Integrações: Integração nativa com sistemas SIEM (Splunk, ArcSight, QRadar, LogRhythm) por socket TCP e HTTP customizável; integração com ServiceNow para sincronização de base de dispositivos gerenciados com itens de configuração do ITSM; exportação de dados via API documentada (JSON, CSV, HTML).

Experiência Digital do Usuário (DEX): Cálculo automático de *scores* de experiência do funcionário para Windows, Linux e macOS; identificação de anomalias e análise de causa raiz; pesquisas de satisfação customizáveis diretamente na área de trabalho do usuário; notificações configuráveis por grupos de dispositivos.

Gestão de Certificados Digitais: Identificação e monitoramento de certificados instalados nos endpoints; alertas para certificados expirados ou próximos à data de expiração.

Relatórios e Dashboards: Dashboards padrão e personalizáveis; relatórios pré-definidos com capacidade de clonagem e customização; exportação em múltiplos formatos (JSON, HTML, CSV); agendamento de relatórios recorrentes; criação de gráficos para visualização de dados.

12.6 Arquitetura e Segurança da Plataforma

- Arquitetura de distribuição de conteúdo descentralizada, utilizando ativos locais para otimização de entrega de pacotes;
- Comunicação criptografada ponta a ponta entre agente e plataforma com **TLS 1.3 ou superior**;
- Capacidade de operação sem necessidade de servidores secundários de distribuição/retransmissão na LAN ou WAN;
- Suporte a sobreposição de endereços IP e transição entre limites NAT e PAT;
- Rastreamento persistente de agente durante transição entre redes;
- Suporte a utilização de proxy para comunicação entre clientes e plataforma.

12.7 Serviços de Implantação e Capacitação (Item 2)

Serviços de implantação:

- Reunião de kickoff (presencial ou remota) para alinhamento de expectativas e apresentação do cronograma;
- Elaboração conjunta do Plano de Instalação antes do início dos serviços;
- Instalação e configuração completa da plataforma no ambiente do INTO;
- Configuração de RBAC, integração com Active Directory/LDAP, MFA, SIEM e ServiceNow;
- Configuração de políticas de patches, conformidade e alertas;
- Testes funcionais e validação da implantação;
- Entrega de documentação técnica *as-built* em até 15 dias úteis após a conclusão.

Serviços de capacitação:

- Mínimo de **16 horas por turma**, com até 10 participantes por turma;
- Conteúdo programático mínimo conforme seção 6.7 deste ETP;
- Fornecimento de material de apoio integrado na proposta de capacitação;
- Emissão de certificado individual para cada participante.

12.8 Suporte Técnico e Garantia

- Suporte técnico em regime **24x7x365**, nas modalidades remota e *on-site*;
- Período de garantia técnica: **24 (vinte e quatro) meses** a contar do Termo de Recebimento Definitivo;
- Execução por técnicos certificados pelo fabricante;
- Canal eletrônico de abertura de chamados 24x7 e telefônico em horário comercial.

12.9 Diretrizes Estratégicas e Alinhamento de Desempenho da Solução

A solução de TIC a ser contratada compreende a subscrição de uma plataforma unificada, baseada em nuvem (*Software as a Service* - SaaS), destinada ao mapeamento, inventário automatizado, governança e monitoramento contínuo de *endpoints*, servidores e dispositivos móveis corporativos do Instituto Nacional de Traumatologia e Ortopedia (INTO).

Para que a solução técnica atenda integralmente às necessidades de negócio e aos rigorosos requisitos de segurança da informação estipulados por esta Administração, a plataforma ofertada deverá possuir capacidades tecnológicas nativas que viabilizem a transição do atual cenário de gestão manual e fragmentada para um ambiente centralizado, ágil e auditável.

Nesse sentido, as funcionalidades da ferramenta a ser contratada deverão garantir não apenas a execução rotineira das atividades de governança de TI, mas também o fornecimento de painéis (*dashboards*) e relatórios que permitam à equipe técnica da DITEC aferir, monitorar e comprovar o alcance das

seguintes metas de desempenho, divididas em indicadores operacionais e de conformidade:

12.9.1 Indicadores Operacionais

Indicador	Situação Atual	Meta Pós-Implantação	Prazo
Tempo médio para inventário e análise de ativos	Alto (processo manual, estimado em horas /semana)	Redução de 80% (automatizado, em minutos)	90 dias pós-implantação
Tempo consumido com rotinas de controle de ativos	Alto (processo fragmentado e reativo)	Redução de 60% (automatizado e centralizado)	90 dias pós-implantação
Cobertura de endpoints com inventário atualizado	Parcial e desatualizada	100% do parque — atualização em segundos	30 dias pós-implantação
Tempo de aplicação de patches críticos	Semanas (processo manual)	Redução para poucas horas (automatizado)	90 dias pós-implantação
Endpoints com vulnerabilidades críticas conhecidas	Desconhecido	Identificação e priorização em 100% dos ativos	30 dias pós-implantação

12.9.2 Indicadores de Segurança e Conformidade

Indicador	Situação Atual	Meta Pós-Implantação	Prazo
Conformidade com controles PPSI/CIS (CIS 1, 2, 4, 5, 7, 11)	Não demonstrável (ausência de evidências automatizadas)	Conformidade documentada e auditável em 100% dos controles aplicáveis	180 dias pós-implantação
Dispositivos não gerenciados na rede	Desconhecido	0 (descoberta automática contínua)	60 dias pós-implantação
Tempo médio de recuperação de incidentes (MTTR)	Estimado em 48 horas ou mais	Redução para menos de 4 horas em incidentes de endpoint	180 dias pós-implantação
Cobertura de trilhas de auditoria exportáveis	Inexistente	100% das operações registradas e exportáveis ao SIEM	90 dias pós-implantação

13. Estimativa de custo total da contratação

[Conteúdo Sigiloso | Justificativa: A não divulgação do orçamento tem por objetivo evitar que as propostas/lances gravitem em torno do orçamento fixado pela administração de modo que os proponentes apresentem lances realmente competitivos e de acordo sua efetiva capacidade de honrá-los com lucratividade adequada. Nesse contexto de ponderação de princípios, entende-se estar justificada a ausência temporária da divulgação do orçamento, pois amparada no princípio da busca da melhor proposta pela administração. Deste modo, o processo foi classificado como restrito e obedecerá o previsto no artigo 24, da Lei 14.133/2021.]

14. Justificativa técnica da escolha da solução

14.1 Aderência aos Requisitos Tecnológicos (Seção 5)

A solução comercial SaaS escolhida atende integralmente a todas as capacidades tecnológicas identificadas na seção 5, conforme demonstrado na análise comparativa da seção 9. Em particular, destaca-se sua aderência aos requisitos mais críticos:

Requisito 5.1.14 (Agente único): A solução opera por meio de um único agente unificado responsável por todas as funcionalidades, eliminando a fragmentação operacional e o conflito entre componentes. Esta característica é exclusiva das soluções comerciais de mercado e inatingível pelas alternativas open source ou de desenvolvimento interno sem custo e prazo incompatíveis.

Requisito 5.1.3 (Análise de vulnerabilidades com pontuação de risco): A plataforma oferece cálculo contínuo de pontuação de risco para todo o ambiente, com evolução temporal, permitindo ao INTO demonstrar objetivamente sua postura de segurança aos órgãos de controle e evidenciar a conformidade com o PPSI.

Requisito 5.1.11 (DEX e pesquisas de satisfação): A capacidade de calcular automaticamente *scores* de experiência digital do usuário para Windows, Linux e macOS, e de realizar pesquisas de satisfação diretamente na área de trabalho, são funcionalidades não disponíveis nas alternativas open source e dependentes de infraestrutura adicional no modelo on-premises.

Requisito 5.1.8 (Integração nativa com SIEM e ITSM): A integração nativa com os principais SIEMs de mercado (Splunk, QRadar, ArcSight, LogRhythm) e com o ServiceNow garante a interoperabilidade imediata com o ecossistema tecnológico do INTO, sem necessidade de desenvolvimento de adaptadores ou integrações customizadas.

14.2 Aderência aos Requisitos Complementares (Seção 6)

Suporte 24x7x365 (Seção 6.5): Atendido por meio de contrato com o fornecedor, com SLA formalizado e responsabilidade técnica e jurídica definidas.

Garantia de 24 meses (Seção 6.5): Coberta integralmente pelo modelo de subscrição SaaS, que inclui suporte e atualizações automáticas durante todo o período contratual.

Conformidade com PPSI e CIS Controls (Seção 6.2): A plataforma foi desenvolvida para atender especificamente aos controles CIS 1, 2, 4, 5, 7 e 11, que constituem o núcleo do PPSI aplicável à gestão de ativos.

Criptografia ponta a ponta TLS 1.3 (Seção 6.4): Atendida nativamente pela arquitetura da plataforma, conforme especificado na seção 12.6.

Capacitação da equipe (Seção 6.7): Incluída no escopo dos serviços (Item 2), com cobertura de todos os temas mínimos requeridos.

14.3 Superioridade Técnica frente ao Modelo On-Premises (Alternativa C)

Em relação à única alternativa viável que não foi selecionada — a solução *on-premises* —, a solução SaaS apresenta vantagens técnicas diretas: eliminação dos riscos de obsolescência de infraestrutura local; atualização automática da plataforma sem necessidade de janelas de manutenção gerenciadas internamente; escalabilidade imediata sem provisionamento adicional de hardware; e disponibilidade gerenciada pelo fornecedor com SLA contratual, sem dependência da disponibilidade da infraestrutura local do datacenter do INTO.

15. Justificativa econômica da escolha da solução

15.1 Comparação de TCO com a Alternativa On-Premises

Conforme demonstrado na análise de TCO (seção 11), a solução SaaS apresenta TCO total para 24 meses significativamente inferior ao modelo on-premises, pelos seguintes motivos objetivos:

Eliminação de custos de infraestrutura: O modelo SaaS dispensa a aquisição de servidores físicos em configuração de alta disponibilidade, licenças de sistema operacional de servidor, solução de backup dedicada e adequações de datacenter — componentes com custo de aquisição e manutenção relevantes no modelo on-premises.

Modelo OPEX versus CAPEX: A conversão de investimentos de capital (CAPEX) em custos operacionais (OPEX) distribuídos e previsíveis ao longo dos 24 meses facilita a execução orçamentária, evita impactos concentrados no exercício de aquisição e reduz o risco de contingências orçamentárias.

Eliminação de custos de administração interna da plataforma: O modelo SaaS reduz a necessidade de administrador interno dedicado à infraestrutura da plataforma, representando custo de oportunidade significativo da equipe especializada da DITEC para outras atividades estratégicas.

Eliminação de custos de atualização: As atualizações automáticas do modelo SaaS eliminam os custos de planejamento, homologação e execução de atualizações manuais da plataforma on-premises.

15.2 Ganhos de Eficiência Operacional com Retorno Econômico

Além da comparação direta de TCO, a adoção da solução SaaS gera ganhos de eficiência operacional com retorno econômico mensurável:

- **Redução de 80% no tempo de inventário e análise de ativos:** A automatização do inventário libera horas de trabalho técnico qualificado atualmente consumidas com levantamento manual, representando valor econômico direto em termos de produtividade da equipe de TI;
- **Redução de 60% no tempo consumido com rotinas de controle:** Processos hoje executados manualmente — como verificação de conformidade de configurações, aplicação de patches e revisão de licenças — passam a ser automatizados, com monitoramento centralizado;
- **Redução do MTTR de incidentes:** A capacidade de resposta automatizada a incidentes e o isolamento imediato de endpoints comprometidos reduzem o tempo médio de recuperação, minimizando o impacto econômico de interrupções de serviços críticos de saúde.

15.3 Princípio da Economicidade

A escolha da solução SaaS atende ao princípio da economicidade estabelecido no art. 5º da Lei nº 14.133/2021, pois oferece, para o menor TCO entre as alternativas viáveis, a maior cobertura funcional dos requisitos identificados nas seções 5 e 6, com menor risco operacional, maior previsibilidade de custos e menores exigências de recursos internos do INTO para sua operação e manutenção.

16. Benefícios a serem alcançados com a contratação

16.1. Benefícios Operacionais

- **Automação e Otimização do Inventário de Ativos:** Substituição do modelo manual e descentralizado pela identificação automática e contínua do parque tecnológico. Essa automação libera a força de trabalho da DITEC da execução de rotinas operacionais repetitivas, permitindo o redirecionamento dos servidores para atividades de maior valor analítico e estratégico.
- **Fortalecimento da Capacidade de Resposta a Incidentes:** Redução substancial do tempo necessário para identificação, contenção e recuperação de incidentes e falhas, por meio da automação de respostas (isolamento de endpoints comprometidos), garantindo a continuidade imediata dos serviços assistenciais e clínicos prestados aos pacientes.

16.2. Benefícios Administrativos

- **Elevação da Transparência e Rastreabilidade Institucional:** A consolidação de um painel centralizado (*dashboard*) assegurará visibilidade permanente, precisa e auditável sobre hardware, software e configurações, fornecendo uma base probatória robusta e confiável para a prestação de contas aos órgãos de controle.
- **Garantia de Conformidade Regulatória Plena (Compliance):** O monitoramento contínuo permitirá auditar o licenciamento e as políticas de uso em tempo real, assegurando o estrito cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) em relação à gestão dos dispositivos que processam dados clínicos sensíveis, além de mitigar sanções ou apontamentos por não conformidade.

16.3. Benefícios Financeiros

- **Otimização da Execução Orçamentária de TIC:** Identificação precisa e eliminação de gastos desnecessários com licenças de softwares ociosos, subutilizados ou equipamentos precocemente classificados como obsoletos. Isso fundamenta e racionaliza as futuras decisões de investimento em renovações tecnológicas.

- **Maximização do Retorno sobre Investimento (ROI) via Eficiência:** O esforço de distribuição e gestão remota mitigará a necessidade de deslocamentos físicos das equipes de suporte pelo campus hospitalar, reduzindo os custos operacionais (HH - Homem/Hora) atrelados à manutenção técnica em campo.

16.4. Benefícios Tecnológicos

- **Mitigação Contínua de Vulnerabilidades Cibernéticas:** Por meio da análise sistemática e da aplicação automatizada de correções (*patches*), a solução reduzirá drasticamente a janela de exposição da infraestrutura crítica do INTO contra ameaças virtuais, impedindo vazamentos de dados hospitalares.
- **Padronização e Configuração Segura dos Endpoints:** A solução aplicará políticas de configuração segura (ex: controle de USB e parâmetros de antivírus), barrando dispositivos não homologados de se conectarem à rede do Instituto (aderência direta aos *CIS Critical Security Controls*).

16.5. Benefícios Estratégicos

- **Subsídio Qualificado ao Planejamento Estratégico (PDTIC):** A disponibilização de métricas precisas sobre o ciclo de vida e a saúde dos ativos servirá de insumo direto para a elaboração e revisão do Plano Diretor de Tecnologia da Informação e Comunicação do órgão.
- **Mensuração da Experiência Digital do Usuário (DEX):** A solução agregará métricas de desempenho sob a perspectiva do usuário final (médicos, enfermeiros e corpo administrativo), permitindo identificar gargalos tecnológicos que impactam negativamente o fluxo hospitalar e a produtividade da ponta.

16.6. Indicadores Recomendados para Mensuração de Resultados

Para atestar a efetividade dos benefícios arrolados ao longo da vigência contratual, propõe-se a medição dos seguintes indicadores de desempenho e resultado:

Categoria do Benefício	Benefício Vinculado	Indicador Recomendado para Mensuração
Operacional	Automação do Inventário	Taxa de Visibilidade de Ativos (%): Proporção de ativos reportados na solução <i>versus</i> base histórica estimada (meta de alcance de 100%).
Operacional	Resposta a Incidentes	Tempo Médio de Resolução (MTTR): Redução no tempo em horas para identificação e isolamento de um ativo infectado/vulnerável.
Administrativo	Rastreabilidade e Governança	Nível de Conformidade Regulamentar (%): Percentual de <i>endpoints</i> que cumprem 100% das políticas básicas de configuração e segurança.
Financeiro	Otimização Orçamentária	Taxa de Recuperação de Licenças (%): Número de licenças de software detectadas como inativas e reaproveitadas/canceladas no trimestre.
Tecnológico	Mitigação de Vulnerabilidades	Índice de Cobertura de Patches (%): Porcentagem de estações críticas atualizadas dentro do ciclo de 30 dias após lançamento do <i>patch</i> .

17. Providências a serem Adotadas

17.1 Providências para Viabilização da Contratação e Ritos Administrativos

- a) Aprovação do ETP e Autorização:** A DITEC deverá submeter o presente ETP à aprovação da autoridade competente do INTO, obtendo a autorização formal para o avanço da fase de planejamento, nos termos do art. 18 da Lei nº 14.133/2021.
- b) Elaboração do Mapa de Gerenciamento de Riscos (MGR):** A equipe de planejamento da contratação deverá confeccionar o mapa de riscos da solução de TIC, identificando e tratando os riscos inerentes à fase de planejamento, seleção de fornecedor e gestão do contrato, conforme a IN SGD/MGI nº 94/2022.
- c) Elaboração do Termo de Referência (TR):** Com base nos requisitos deste ETP, a equipe redigirá o TR detalhado, contemplando o modelo de execução, níveis de serviço (SLAs), critérios de aceitação e especificações técnicas de segurança da informação.
- d) Pesquisa de Preços e Adequação Orçamental:** Conduzir ampla pesquisa de mercado (IN SEGES/ME nº 65/2021) para definição do valor estimado e articular com o setor financeiro a confirmação de disponibilidade de dotação orçamental compatível.
- e) Inscrição no Plano de Contratações Anual (PCA):** Assegurar o alinhamento da contratação ao PCA do INTO (Decreto nº 10.947/2022) e ao Plano Diretor de TIC (PDTIC).
- f) Designação da Equipe de Fiscalização:** A autoridade competente deverá nomear formalmente o Gestor e os Fiscais (Técnico, Requisitante e Administrativo) do contrato, em cumprimento ao art. 117 da Lei nº 14.133/2021, para acompanhamento desde a fase preparatória até à implementação.

17.2 Providências Técnicas Prévias para Implementação da Solução

- g) Inventário Manual Complementar de Ativos:** Previamente à licitação, a DITEC realizará o mapeamento consolidado do parque para identificar ativos não catalogados, garantindo que o dimensionamento final no TR cubra todos os *endpoints* institucionais.
- h) Definição de Perfis (RBAC) e Diretrizes de Acesso:** Mapear previamente as matrizes de acesso, segmentando privilégios (operadores, administradores, auditores), para garantir a aplicação do princípio do menor privilégio (ISO 27001) logo no primeiro dia de implementação.
- i) Adequação da Infraestrutura Lógica (Firewall, Proxy e SSO):** A equipe de infraestrutura deverá auditar e prever os ajustes em regras de rede, bem como preparar o ambiente de Federação de Identidades (ex: SAML 2.0/Active Directory) e o ITSM (ServiceNow) para a integração fluida com a plataforma SaaS a ser contratada.
- j) Planejamento de Janelas de Manutenção:** Estabelecer, em conjunto com as áreas finalísticas, a matriz de horários de menor impacto operacional, assegurando a continuidade irrestrita dos serviços assistenciais e médicos do hospital durante a futura instalação dos agentes.
- k) Estruturação de Plano de Comunicação (Gestão de Mudança):** Desenvolver campanha de comunicação voltada aos utilizadores do INTO sobre a futura implementação da ferramenta, com foco no esclarecimento de impactos e na redução de requisições de suporte ao *help desk* (alinhamento ITIL).
- l) Avaliação de Impacto e LGPD:** Submeter os preceitos tecnológicos da solução ao Comitê de Segurança da Informação e/ou ao Encarregado pelo Tratamento de Dados Pessoais (DPO), assegurando a aderência às políticas de privacidade institucionais.

18. Alinhamento com Planos Estratégicos

A contratação proposta encontra embasamento no Plano Diretor de Tecnologia da Informação – PDTI para o biênio 2025-2026, possui lançamento no Planejamento e Gerenciamento de Contratações 2026 e atende às necessidades e aos Objetivos Estratégicos Institucionais que visam:

ALINHAMENTOS AOS PLANOS ESTRATÉGICOS	
ID	Objetivos Estratégicos
OE.03	Prover a estrutura de TIC apropriada para as atividades administrativas e assistenciais.
OE.04	Prover serviços de TIC com geração de valor para o usuário.
OE.05	Zelar pela segurança da informação no que tange dados governamentais e operacionais sob responsabilidade da DITEC.

OE.06	Prover a qualidade dos serviços de forma continuada através de soluções adequadas.
OE.09	Evoluir continuamente, inovando e aprimorando processos e recursos, para a melhor prestação de serviço de TIC aos usuários.

ALINHAMENTO AO PDTIC 2025-2026			
ID	Ação do PDTIC	ID	Meta do PDTIC associada
N16	Manter as soluções de infraestrutura de TIC atualizadas.	OE.03	Prover a estrutura de TIC apropriada para as atividades administrativas e assistenciais.
N02	Criar e implantar procedimentos das Normas de segurança.	OE.05	Zelar pela segurança da informação no que tange dados governamentais e operacionais sob responsabilidade da DITEC.
N18	Apoiar e estimular o ConstruINTO.	OE.03	Prover a estrutura de TIC apropriada para as atividades administrativas e assistenciais.
N14	Tornar os sistemas aderentes aos padrões governamentais, gerando qualidade aos usuários.	OE.04	Prover serviços de TIC com geração de valor para o usuário.
N20	Promover inovação através da iniciativa de novos processos e tecnologias.	OE.09	Evoluir continuamente, inovando e aprimorando processos e recursos, para a melhor prestação de serviço de TIC aos usuários.

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

A contratação da solução comercial em modalidade SaaS demonstra-se totalmente viável e vantajosa para o INTO, pois apresenta o menor custo total de propriedade (TCO), garante plena conformidade com a LGPD e as normas de segurança, e otimiza a eficiência operacional na gestão automatizada dos 2000 ativos da instituição.

20. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

Despacho: INTEGRANTE REQUISITANTE

CARLOS EDUARDO MARQUES CORDEIRO

Agente de contratação



Assinou eletronicamente em 20/08/2026 às 12:08:34.

Despacho: INTEGRANTE TÉCNICO

ANDRE LUIZ SILVA FERREIRA

Agente de contratação



Assinou eletronicamente em 20/08/2026 às 11:58:55.

Despacho: INTEGRANTE ADMINISTRATIVO / AUTORIDADE MÁXIMA DE TIC

OSNY PEREIRA FILHO

Agente de contratação



Assinou eletronicamente em 20/08/2026 às 13:26:07.