



Educação, Pesquisa
e Inovação em Rede.

Solução de UEM e Suporte Remoto

Termo de Referência
DATI/GTI • Julho/26



SUMÁRIO

1. INTRODUÇÃO	3
2. ESCOPO DA SOLUÇÃO	3
3. REQUISITOS.....	4
3.1. Requisitos Técnicos	4
3.2. Requisitos de privacidade e proteção de dados	6
3.3. Documentação comprobatória relacionada aos requisitos.....	6
4. MATRIZ DE ADERÊNCIA AOS REQUISITOS E VALORES	6
5. RESPOSTA AO TERMO DE REFERÊNCIA.....	8
6. CRITÉRIOS DE SELEÇÃO DA CONTRATAÇÃO.....	8

1. INTRODUÇÃO

Este documento constitui o Termo de Referência para contratação de solução de Gerenciamento Unificado de Endpoints (UEM) e Suporte Remoto, estabelecendo o escopo, os requisitos técnicos, de segurança da informação e de privacidade e proteção de dados a serem atendidos pela solução destinada à RNP.

2. ESCOPO DA SOLUÇÃO

A solução deverá apoiar a gestão operacional e a governança dos ativos computacionais da RNP, abrangendo estações de trabalho, notebooks, dispositivos móveis, servidores e demais equipamentos corporativos.

O escopo contempla uma plataforma corporativa capaz de centralizar a administração dos ativos de TI da organização.

A solução deverá ser disponibilizada obrigatoriamente em modelo SaaS, com console administrativa hospedada em ambiente de nuvem do fornecedor ou fabricante, acessível de forma segura pela RNP, com atualizações, correções e manutenção da plataforma sob responsabilidade do fornecedor ou fabricante.

Serão admitidos agentes, conectores, gateways, repositórios, servidores auxiliares ou demais componentes locais apenas quando tecnicamente indispensáveis para o funcionamento de funcionalidades específicas da solução, tais como comunicação com endpoints, distribuição de agentes, cache de pacotes, integração com ambiente corporativo, execução de rotinas locais ou implantação de sistemas operacionais. Nesses casos, o fornecedor deverá detalhar a finalidade de cada componente, requisitos de infraestrutura, requisitos de rede, responsabilidades de manutenção, requisitos de segurança, dependências técnicas e impacto operacional para a RNP.

A solução deve contemplar as seguintes funcionalidades:

- Suporte remoto seguro para estações de trabalho e servidores;
- Inventário automatizado de hardware e software;
- Distribuição e atualização de aplicações;
- Gerenciamento de patches e correções de segurança;
- Aplicação e monitoramento de políticas de configuração;
- Gestão de dispositivos móveis (MDM);
- Controle de conformidade e auditoria;
- Geração de relatórios gerenciais e operacionais;
- Integração com mecanismos corporativos de autenticação e segurança;
- Registro e rastreabilidade das atividades administrativas.
- Controle de aplicações, incluindo bloqueio, permissão e identificação de softwares não autorizados;
- Gerenciamento de privilégios administrativos locais, incluindo remoção de privilégios e elevação temporária controlada;
- Provisionamento, reinstalação ou implantação automatizada de sistemas operacionais (OS Deployment).

Com base nesse conjunto de funcionalidades, foram definidos os requisitos que servirão como critério para a avaliação das soluções propostas pelos fornecedores.

3. REQUISITOS

3.1. Requisitos Técnicos

Os requisitos técnicos apresentados nesta seção representam as capacidades mínimas esperadas para a solução, considerando as necessidades operacionais da área de Infraestrutura da RNP, os requisitos de administração dos ambientes computacionais e a necessidade de escalabilidade para atendimento da organização.

- **R1 - Suporte remoto a usuários em regime de teletrabalho:** A solução deve prover funcionalidades de Remote Support ou Remote Assistance, permitindo acesso remoto seguro aos ativos corporativos para suporte técnico, troubleshooting e operação assistida, incluindo autenticação, consentimento do usuário, registro de acesso e controle de sessão.
- **R2 - Inventário de ativos físicos e softwares:** A solução deve prover funcionalidades de IT Asset Management (ITAM) e Software Asset Management (SAM), permitindo descoberta automática, inventário, classificação e rastreamento de hardware, software, sistemas operacionais, versões instaladas e informações de ciclo de vida dos ativos.
- **R3 - Gerenciamento de privilégios administrativos locais e controle de acesso administrativo:** A solução deve permitir identificação, controle e gestão de usuários com privilégios administrativos locais nos endpoints, possibilitando remoção de direitos administrativos, elevação temporária de privilégio, execução controlada de aplicações com privilégio elevado, segregação de funções administrativas e rastreabilidade das ações executadas.
- **R4 - Deploy remoto de aplicações e atualizações:** A solução deve permitir Software Deployment e Application Management centralizado, incluindo distribuição remota de pacotes, instalação, atualização, rollback e remoção de aplicações em dispositivos gerenciados.
- **R5 - Atualização remota do sistema operacional:** A solução deve prover funcionalidades de Patch Management e OS Update Management, permitindo distribuição automatizada de atualizações de segurança, correções críticas e gerenciamento do ciclo de atualização dos sistemas operacionais.
- **R6 - Auditoria das sessões de acesso remoto:** A solução deve prover funcionalidades de Remote Session Auditing, incluindo registro detalhado de acessos, gravação de sessões, trilha de auditoria, rastreabilidade e armazenamento de logs para fins de compliance e segurança.
- **R7 - Auditoria e controle de alterações de software e hardware:** A solução deve permitir Change Tracking e Configuration Compliance, possibilitando auditoria de alterações em hardware, software, configurações, drivers, políticas e componentes instalados nos endpoints.
- **R8 - Relatórios operacionais e executivos:** A solução deve prover Operational Dashboards e Executive Reports, permitindo geração de relatórios gerenciais, indicadores operacionais, métricas de compliance, inventário, vulnerabilidades e status dos ativos gerenciados.
- **R9 - Instalação e remoção remota dos agentes:** A solução deve permitir Agent Lifecycle Management, incluindo instalação, atualização, reinstalação e remoção remota dos agentes utilizados para gerenciamento dos endpoints.

- **R10 – Aplicação de políticas para Windows, Linux e macOS:** A solução deve permitir Cross-platform Endpoint Configuration Management, suportando criação, distribuição e aplicação de políticas de configuração e segurança para dispositivos Windows, Linux e macOS.
- **R11 – Gestão de dispositivos móveis (MDM):** A solução deve prover funcionalidades de Mobile Device Management, incluindo registro e gerenciamento de dispositivos móveis, criação e aplicação de perfis corporativos, aplicação de políticas de segurança, controle de aplicativos, monitoramento de conformidade e wipe remoto total ou seletivo quando aplicável.
- **R12 – Provisionamento e implantação automatizada de sistemas operacionais (OS Deployment):** A solução deve permitir recursos de provisionamento, reinstalação ou implantação automatizada de sistemas operacionais, contemplando captura, distribuição ou implantação de imagens, suporte a drivers, execução de pacotes pós-instalação, automação do processo de instalação e documentação das dependências técnicas necessárias para uso da funcionalidade no ambiente da RNP.
- **R13 – Controle de aplicações:** A solução deve permitir controle da execução de aplicações nos endpoints, incluindo criação de listas de permissão e bloqueio, controle por aplicação, grupo de aplicações, hash ou mecanismo equivalente, identificação de softwares não autorizados e geração de relatórios de aplicações bloqueadas ou em desconformidade.
- **R14 – Disponibilização em modelo SaaS:** A solução deve ser disponibilizada em modelo SaaS, com console administrativa em nuvem, atualizações, correções e manutenção da plataforma sob responsabilidade do fornecedor ou fabricante. Componentes locais somente serão admitidos quando tecnicamente indispensáveis para funcionalidades específicas, devendo ser detalhados quanto à finalidade, requisitos de infraestrutura, requisitos de rede, segurança, manutenção, suporte e impacto operacional. Requisitos de segurança da informação

Requisitos obrigatórios:

- *Apresentação de uma política formal de segurança da informação vigente*
- *Apresentação de uma análise de gaps e conformidade com ISO/IEC 27001, e caso seja certificado, compartilhar o comprovante da certificação.*
- *Compartilhamento de um contato do responsável formal por segurança da informação.*
- *Apresentar comprovação de que adota práticas de desenvolvimento seguro (secure coding) e que aplica correções de segurança regularmente em suas soluções.*
- *Ssuporte à autenticação forte para os usuários, com MFA,*
- *Permitir integração com mecanismos de autenticação centralizado,*
- *Permitir definição de perfis de acesso e privilégios (RBAC),*
- *Garantir que toda comunicação entre usuário e operador seja protegida por criptografia forte,*
- *Permitir restrição de acesso por rede (VPN ou rede corporativa), e*
- *Registro de todas as sessões de acesso remoto, incluindo: identificação do operador, identificação do usuário/ativo acessado, data e hora da conexão e duração da sessão.*

Requisitos Desejáveis: permitir encerrar sessões remotamente pelo operador ou automaticamente por inatividade, impedir múltiplas sessões simultâneas não autorizadas, permitir restrição de funcionalidades durante a sessão (ex.: transferência de arquivos, execução de comandos), permitir restringir ou desabilitar recursos que possam expor dados (ex.: download, compartilhamento, gravação local).

3.2. Requisitos de privacidade e proteção de dados

Requisitos obrigatórios:

- Conformidade com a **LGPD**.
- Nomeação de Encarregado de Dados (DPO).
- Gestão total de dados pessoais pelo controlador (RNP).
- A ferramenta deve permitir configuração para coleta e processamento apenas dos dados estritamente necessários à finalidade de suporte técnico remoto.
- Deve possibilitar delimitação de escopo de acesso, evitando exposição desnecessária de diretórios, arquivos e aplicações não relacionados ao atendimento.
- O fornecedor deve documentar de forma detalhada quais categorias de dados pessoais são tratadas pela solução.
- A ferramenta deve possibilitar configuração de bloqueio de funcionalidades específicas (ex.: transferência de arquivos, impressão remota) de acordo com políticas da RNP.
- A solução não pode utilizar dados coletados para finalidades diversas do suporte técnico, especialmente para treinamento de algoritmos, publicidade ou perfilamento.
- A solução deve gerar logs completos e inalteráveis de todas as sessões de acesso remoto, contendo no mínimo: identificação do colaborador RNP, identificação do dispositivo acessado, data/hora de início e término, ações executadas e arquivos acessados ou transferidos.
- A solução não deve compartilhar dados pessoais coletados durante as sessões com terceiros, exceto quando estritamente necessário à prestação do serviço e mediante previsão contratual expressa.
- A ferramenta deve implementar configurações padrão (default) que priorizem a proteção de dados, que podem incluir: gravação de tela desabilitada, transferência de arquivos mediante aprovação, acesso limitado temporalmente.

Após término do contrato, o fornecedor deve eliminar definitivamente todos os dados pessoais coletados durante a prestação do serviço e tal eliminação deve ser comprovada mediante declaração formal assinada por responsável técnico do fornecedor.

3.3. Documentação comprobatória relacionada aos requisitos

- Política de Privacidade e demais artefatos relacionados
- Declaração formal de conformidade com a LGPD assinada por representante legal
- Mapeamento de fluxo de dados (data flow) detalhando origem, processamento, armazenamento e destinação de dados pessoais (RoPA)
- Identificação do Encarregado de Proteção de Dados (DPO) do fornecedor com canais de contato
- Comprovação de conformidade com ISO/IEC 27701 ou roadmap de certificação
- Relatório de Avaliação de Impacto à Proteção de Dados (RIPD) quando o tratamento envolver alto risco aos direitos dos titulares

4. MATRIZ DE ADERÊNCIA AOS REQUISITOS E VALORES

Para permitir a avaliação das propostas recebidas, deverá ser preenchida pelo fornecedor uma matriz de aderência relacionando os requisitos definidos pela RNP às funcionalidades oferecidas pela solução proposta, bem como o respectivo valor anual.

O fornecedor deverá informar, para cada requisito, a aderência da solução, o módulo ou funcionalidade correspondente, eventual necessidade de licenciamento adicional e observações sobre limitações, dependências técnicas ou condições de atendimento.

Para fins de comparação comercial, o valor anual informado deverá considerar o cenário de referência de 1.200 endpoints/dispositivos gerenciados e até 10 operadores/técnicos, contemplando os módulos necessários ao atendimento dos requisitos obrigatórios deste Termo de Referência, suporte técnico e treinamento ou repasse técnico inicial para administradores da ferramenta.

Requisito	Atende / Atende parcialmente / Não atende	Módulo ou funcionalidade correspondente	Depende de licenciamento adicional?	Observações / limitações
R1				
R2				
R3				
R4				
R5				
R6				
R7				
R8				
R9				
R10				
R11				
R12				
R13				
R14				
Requisitos de segurança da informação				
Requisitos de privacidade e proteção de dados				
Valor anual				

5. RESPOSTA AO TERMO DE REFERÊNCIA

Como resposta a este Termo de Referência, deverão ser apresentadas, no mínimo, as seguintes informações:

- Proposta técnica e comercial, contendo os valores anuais, detalhamento do modelo de licenciamento, descrição do suporte técnico e treinamento para os administradores da ferramenta
- Matriz de aderência requisito a requisito, indicando atende, atende parcialmente ou não atende, e apresentando justificativa para os itens classificados como atende parcialmente. (descrito no item 4)
- Documentação comprobatória relacionada aos requisitos (descrito no item 3.4)
- Além do preenchimento da matriz de aderência, o fornecedor deverá informar, na proposta técnica e comercial, o modelo de disponibilização da solução, o modelo de licenciamento, os módulos incluídos, eventuais módulos adicionais necessários ao atendimento dos requisitos, as dependências técnicas da solução e componentes necessários

6. CRITÉRIOS DE SELEÇÃO DA CONTRATAÇÃO

Serão consideradas tecnicamente elegíveis as soluções que atenderem aos requisitos obrigatórios estabelecidos neste Termo de Referência. Os itens classificados como ATENDE PARCIALMENTE serão avaliados pela RNP quanto ao impacto da limitação informada pelo fornecedor. Entre as propostas consideradas tecnicamente aptas, caso mais de uma solução atenda aos requisitos estabelecidos, será selecionada aquela que apresentar o menor valor.

