

		Descrição
1	Pergunta	Prazo da contratação / licenciamento O Termo de Referência solicita a apresentação de preço anual, porém não identificamos de forma clara o período total previsto para a contratação. • Solicitamos confirmar qual será a vigência contratual e o período pelo qual deverão ser considerados os licenciamentos, subscrições, suporte e demais serviços associados à solução.
	RESPOSTA	A contratação e o licenciamento serão considerados pelo período inicial de 12 meses, contemplando licenças/subscrições, suporte técnico, atualizações, treinamento ou repasse técnico inicial e demais serviços previstos na proposta. Eventuais renovações serão avaliadas pela RNP conforme necessidade, disponibilidade orçamentária e condições contratuais.
2	Pergunta	Perfil dos 1.200 dispositivos Para o correto dimensionamento da solução, solicitamos informar a distribuição aproximada dos 1.200 dispositivos por sistema operacional e categoria. • Windows; • Linux; • macOS; • servidores; • Android; • iOS/iPadOS. Essa informação é especialmente relevante porque determinadas funcionalidades podem variar conforme o sistema operacional utilizado.
	RESPOSTA	Para fins de dimensionamento comercial, deverá ser considerada a seguinte estimativa: 1.000 estações de trabalho e notebooks; 150 servidores; 50 dispositivos móveis; total estimado: 1.200 endpoints/dispositivos. O parque é heterogêneo e contempla Windows, Linux, macOS, Android e iOS/iPadOS. A distribuição detalhada por sistema operacional ainda não está consolidada, razão pela qual os fornecedores deverão informar claramente as premissas adotadas na proposta, as plataformas suportadas, eventuais diferenças funcionais e impactos no licenciamento
3	Pergunta	Licenciamento e perfil dos 10 operadores/técnicos Solicitamos esclarecer se os 10 operadores/técnicos previstos correspondem a usuários nomeados da solução ou à quantidade máxima de acessos simultâneos. • Confirmar também se todos os operadores deverão possuir acesso a todas as funcionalidades previstas, incluindo gerenciamento e suporte remoto, ou se existirão diferentes perfis de operadores e privilégios.
	RESPOSTA	Para dimensionamento, deverão ser considerados até 10 operadores/técnicos autorizados a utilizar a solução. O fornecedor deverá informar se seu modelo de licenciamento considera usuários nomeados, usuários simultâneos, sessões concorrentes ou outra métrica. A solução deverá permitir criação de diferentes perfis administrativos e segregação de privilégios, de forma que nem todos os operadores precisem necessariamente possuir acesso irrestrito a todas as funcionalidades.
4	Pergunta	Acesso remoto assistido e não assistido Solicitamos esclarecer se o consentimento do usuário deverá obrigatoriamente ser solicitado em todas as sessões de suporte remoto. • Para servidores, equipamentos de infraestrutura ou dispositivos sem usuário presente, será permitido acesso remoto não assistido, desde que previamente autorizado por política administrativa da RNP e devidamente registrado e auditado?
	RESPOSTA	O consentimento do usuário deverá ser exigido nas sessões realizadas em estações de trabalho e dispositivos associados a usuários, salvo exceções previamente autorizadas pela RNP. Para servidores, equipamentos de infraestrutura, dispositivos sem usuário presente ou cenários administrativos previamente autorizados, será admitido acesso remoto não assistido, desde que controlado por política administrativa, restrito a operadores autorizados e devidamente registrado e auditado.
5	Pergunta	Requisito R1 - Suporte remoto Como alternativa à redação atual, sugerimos considerar: “A solução deve prover acesso remoto seguro e intermediado aos ativos corporativos, por meio de protocolos como RDP, SSH, VNC ou acesso Web, para atividades de suporte técnico, troubleshooting e operação assistida. Deve permitir autenticação forte, controle de acesso baseado em políticas, fluxo de aprovação prévia quando requerido, registro e gravação das sessões, monitoramento em tempo real e encerramento administrativo da sessão.”
	RESPOSTA	A redação sugerida não será adotada integralmente. Não é requisito que a solução utilize especificamente RDP, SSH ou VNC, pois serão aceitos mecanismos próprios e seguros de acesso remoto oferecidos pela solução. Permanece obrigatório que o acesso remoto contemple autenticação, controle de acesso, consentimento quando aplicável, registro de acesso e controle de sessão. Recursos adicionais como fluxo de aprovação, gravação, monitoramento em tempo real e encerramento administrativo serão avaliados conforme os requisitos de segurança, privacidade e auditoria do TR.
6	Pergunta	Gravação das sessões e retenção O requisito prevê registro/gravação das sessões de acesso remoto. Solicitamos esclarecer: • Todas as sessões deverão obrigatoriamente ser gravadas? • Qual deverá ser o período mínimo de retenção das gravações? • A retenção deverá ocorrer na própria solução ou poderá ser realizada em repositório externo da RNP? • Existe estimativa da quantidade/duração média das sessões mensais? Como alternativa de redação: “A solução deve gerar logs e gravações das sessões de acesso remoto, contendo no mínimo identificação do colaborador RNP, dispositivo acessado, data/hora de início e término e registro das ações executadas, com mecanismos de verificação de integridade e possibilidade de envio dos logs para repositório externo da RNP.”
	RESPOSTA	A solução deverá possuir capacidade de gravação das sessões de acesso remoto, permitindo à RNP definir, por meio de políticas administrativas, quais tipos de sessão deverão ser obrigatoriamente gravados. A solução deverá permitir retenção na própria plataforma ou exportação para repositório externo controlado pela RNP, desde que sejam preservadas integridade, segurança, rastreabilidade e possibilidade de consulta. A política e o período definitivo de retenção serão definidos pela RNP durante a implantação, considerando requisitos internos, capacidade de armazenamento, segurança e privacidade. Não há, neste momento, estimativa consolidada da quantidade ou duração média mensal das sessões.
7	Pergunta	Inventário de ativos - ITAM/SAM Solicitamos confirmar se o objetivo deste requisito é manter um inventário operacional dos endpoints gerenciados ou se é requerida uma plataforma completa de IT Asset Management/Software Asset Management, contemplando também gestão de contratos, licenças, garantias e ciclo de vida patrimonial. Caso o objetivo seja o inventário dos endpoints, sugerimos: “A solução deve manter inventário centralizado dos endpoints gerenciados, contemplando informações do sistema operacional e inventário dos softwares instalados, incluindo nome, fabricante e versão, permitindo consulta e acompanhamento dessas informações a partir da console central.”

	RESPOSTA	O objetivo principal é manter inventário operacional e centralizado dos endpoints gerenciados, contemplando hardware, sistema operacional, softwares instalados, fabricante, versão, alterações e informações relevantes para administração e conformidade. Recursos adicionais de gestão de contratos, garantias, licenças e ciclo de vida patrimonial serão considerados positivos, porém não caracterizam, isoladamente, requisito obrigatório para uma plataforma completa de ITAM/SAM patrimonial.
8	Pergunta	Gerenciamento de privilégios administrativos Solicitamos esclarecer se o requisito busca especificamente gerenciamento de privilégios administrativos locais dos endpoints (Endpoint Privilege Management - EPM) ou gerenciamento de acessos e credenciais privilegiadas (PAM). Caso o objetivo seja PAM, sugerimos: "A solução deve permitir gerenciamento de acessos privilegiados, contemplando descoberta e gerenciamento de contas e credenciais privilegiadas, armazenamento seguro de credenciais, rotação de senhas, controle de acesso baseado em papéis, concessão de acesso mediante políticas e fluxo de aprovação, rastreabilidade e gravação das sessões privilegiadas."
	RESPOSTA	O requisito busca especificamente o gerenciamento de privilégios administrativos locais nos endpoints, caracterizado como Endpoint Privilege Management, e não a contratação de uma solução corporativa completa de PAM ou cofre de credenciais. A solução deverá permitir identificar usuários com privilégios locais, remover direitos administrativos, realizar elevação temporária e controlada, permitir execução autorizada de aplicações com privilégio elevado, aplicar segregação de funções e manter rastreabilidade das ações.
9	Pergunta	Patch Management / atualização do sistema operacional Solicitamos confirmar se é obrigatório que a própria plataforma distribua diretamente os patches e atualizações ou se será aceito o acionamento e gerenciamento dos mecanismos nativos dos sistemas operacionais. Como alternativa: "A solução deve permitir identificar vulnerabilidades e atualizações de segurança do sistema operacional e possibilitar a execução das atualizações utilizando os mecanismos nativos do sistema operacional, disponibilizando à administração centralizada informações sobre as vulnerabilidades identificadas nos endpoints."
	RESPOSTA	A solução deverá permitir gerenciamento centralizado do ciclo de atualizações, contemplando identificação das correções aplicáveis, definição de políticas, programação, acionamento da instalação, acompanhamento e relatórios de conformidade. Será aceito o uso dos mecanismos nativos dos sistemas operacionais quando essa for a arquitetura da solução, desde que todo o processo possa ser administrado, acionado e acompanhado pela console central. A mera identificação de vulnerabilidades, sem capacidade de gerenciar ou acionar a aplicação das atualizações, não atende integralmente ao requisito.
10	Pergunta	Auditoria de alterações / Change Tracking Solicitamos esclarecer se é necessária auditoria histórica detalhada de cada alteração realizada em hardware, software, drivers e configurações ou se o requisito poderá ser atendido por inventário atualizado associado à identificação de dispositivos fora da postura de segurança estabelecida pela RNP.
	RESPOSTA	O requisito busca identificar e acompanhar alterações relevantes em hardware, software, drivers, configurações, políticas e componentes instalados nos endpoints. Será aceito inventário atualizado com comparação de estado, histórico de modificações, alertas ou identificação de dispositivos fora da postura estabelecida, desde que a solução permita identificar o ativo, o elemento alterado e o momento ou período da alteração. Não é obrigatória a reprodução detalhada de cada operação interna executada pelo sistema operacional.
11	Pergunta	Relatórios operacionais e executivos Será aceita a exportação ou integração dos dados e registros da solução com ferramentas externas da RNP para elaboração de relatórios executivos? Caso positivo, sugerimos: "A solução deve disponibilizar painéis e informações operacionais referentes aos endpoints gerenciados, inventário, postura de segurança, vulnerabilidades e acessos privilegiados, possibilitando a exportação ou integração dos registros para tratamento e elaboração de relatórios em ferramentas externas da RNP."
	RESPOSTA	Sim. Será aceita a exportação ou integração de dados com ferramentas externas da RNP para elaboração de relatórios executivos, desde que a solução disponibilize nativamente informações operacionais suficientes sobre endpoints, inventário, postura de segurança, vulnerabilidades, conformidade, suporte remoto e demais funcionalidades contratadas.
12	Pergunta	Instalação inicial dos agentes Solicitamos confirmar se a instalação inicial do agente poderá ser realizada utilizando mecanismos corporativos existentes, tais como GPO, SCCM, MDM, pacote customizado ou convite/link disponibilizado ao usuário, permanecendo atualização e remoção sob gerenciamento centralizado da solução.
	RESPOSTA	Sim. A instalação inicial poderá utilizar mecanismos corporativos existentes. Após a implantação, a solução deverá permitir gerenciamento centralizado do ciclo de vida dos agentes, incluindo atualização, reinstalação, monitoramento e remoção, quando tecnicamente suportado.
13	Pergunta	Windows, Linux e macOS Solicitamos confirmar se todas as funcionalidades especificadas deverão estar disponíveis de forma idêntica nos sistemas Windows, Linux e macOS ou se serão aceitas diferenças funcionais decorrentes das características e limitações de cada sistema operacional.
	RESPOSTA	Serão aceitas diferenças funcionais decorrentes das características e limitações técnicas de cada sistema operacional. O fornecedor deverá declarar claramente, para cada requisito, quais funcionalidades estão disponíveis em Windows, Linux e macOS, eventuais limitações, dependências e módulos adicionais. As diferenças serão avaliadas pela RNP quanto ao impacto operacional e à aderência ao parque de dispositivos.
14	Pergunta	Gestão de dispositivos móveis - MDM Para atendimento aos requisitos de gerenciamento de Android e iOS/iPadOS, será permitida composição com solução complementar de MDM, desde que integrada/compatível com o ambiente e administrada pela CONTRATADA? Sugestão de complemento: "Será permitida a composição de soluções, desde que sejam compatíveis com o ambiente da RNP e administradas pela CONTRATADA."
	RESPOSTA	A RNP busca uma solução integrada, fornecida e suportada por uma única CONTRATADA. Será aceita a utilização de módulo complementar de MDM, desde que faça parte da solução ofertada pelo mesmo fornecedor/fabricante ou seja integralmente fornecido, administrado e suportado pela CONTRATADA, sem transferência de responsabilidades para a RNP ou necessidade de contratação separada. Todos os componentes, licenciamentos, integrações, custos, suporte e responsabilidades necessários ao atendimento do requisito deverão estar contemplados na proposta.
15	Pergunta	Provisionamento de sistemas operacionais - OS Deployment Para funcionalidades de captura, distribuição ou implantação de imagens de sistemas operacionais, será permitida composição com ferramenta complementar compatível com o ambiente da RNP e administrada pela CONTRATADA?
	RESPOSTA	A RNP busca uma solução integrada, fornecida e suportada por uma única CONTRATADA. Será aceita a utilização de módulo ou componente complementar para OS Deployment, desde que faça parte da solução ofertada pelo mesmo fornecedor/fabricante ou seja integralmente fornecido, administrado e suportado pela CONTRATADA, sem transferência de responsabilidades para a RNP ou necessidade de contratação separada. Todos os componentes, licenciamentos, integrações, custos e serviços necessários deverão estar contemplados na proposta. O fornecedor deverá detalhar as dependências de infraestrutura, rede, imagens, drivers, repositórios e demais recursos necessários ao funcionamento do módulo.

16	Pergunta	Controle de aplicações Solicitamos esclarecer se o requisito exige obrigatoriamente controle da execução local de aplicações por hash/allowlist/blocklist ou se poderá ser atendido por políticas de controle de aplicações associadas ao tráfego dos endpoints, complementadas pelo inventário dos softwares instalados.
	RESPOSTA	O requisito exige controle da execução local de aplicações nos endpoints, por meio de allowlist, blocklist, hash, assinatura digital, aplicação, grupo de aplicações ou mecanismo técnico equivalente. Políticas aplicadas somente ao tráfego de rede, associadas apenas ao inventário de softwares instalados, não atendem integralmente ao requisito.
17	Pergunta	Modelo SaaS e componentes locais Considerando que determinadas funcionalidades de PAM, intermediação de acesso e gravação de sessões podem demandar componentes específicos, solicitamos confirmar se serão aceitos componentes adicionais físicos ou virtuais no ambiente da RNP ou em ambiente de nuvem suportado, mantendo-se a console principal de gerenciamento de endpoints em modalidade SaaS.
	RESPOSTA	Serão aceitos componentes virtuais adicionais no ambiente on-premises da RNP ou em ambiente de nuvem suportado, quando tecnicamente indispensáveis ao funcionamento de funcionalidades específicas da solução. Não está prevista a instalação ou o fornecimento de componentes físicos dedicados na infraestrutura da RNP. A console principal de gerenciamento deverá permanecer em modalidade SaaS. O fornecedor deverá detalhar a finalidade de cada componente virtual, arquitetura, requisitos de infraestrutura e rede, capacidade computacional, segurança, atualização, manutenção, suporte e responsabilidades operacionais.
18	Pergunta	LGPD - controle e retenção dos dados Solicitamos confirmar se será aceita arquitetura na qual a RNP detenha o controle sobre configuração, retenção e exclusão dos dados e logs, enquanto o fornecedor/fabricante atue como operador dos dados mediante acordo de tratamento de dados (DPA).
	RESPOSTA	Sim. Será aceita arquitetura na qual a RNP, na condição de controladora, defina e administre as configurações de retenção, acesso e exclusão disponíveis na solução, enquanto fornecedor e fabricante atuem como operadores ou suboperadores, conforme aplicável. A relação deverá ser formalizada contratualmente, incluindo finalidades, responsabilidades, medidas de segurança, suboperadores, transferência internacional, retenção, exclusão e atendimento aos direitos dos titulares.
19	Pergunta	Minimização da coleta de dados Será considerado aderente o atendimento ao princípio de minimização por meio da possibilidade de habilitar ou desabilitar individualmente funcionalidades de coleta, como inventário de software e gravação de sessões, conforme políticas definidas pela RNP?
	RESPOSTA	Sim. Será considerada aderente a solução que permita configurar e limitar individualmente funcionalidades de coleta e tratamento, de acordo com as políticas da RNP e com a finalidade operacional. Entretanto, a desativação de uma coleta não poderá inviabilizar requisitos obrigatórios contratados sem que a limitação seja explicitamente informada pelo fornecedor
20	Pergunta	Delimitação do escopo de acesso Solicitamos esclarecer se a restrição exigida deverá ocorrer obrigatoriamente no nível de diretórios e arquivos dentro do dispositivo ou se poderá ser implementada por ativo, protocolo e aplicação autorizada, restringindo o operador apenas aos recursos necessários ao atendimento.
	RESPOSTA	A restrição poderá ser implementada por ativo, grupo de ativos, perfil administrativo, protocolo, aplicação, tipo de sessão ou funcionalidade autorizada. Não é obrigatório que toda restrição seja realizada individualmente no nível de diretórios e arquivos, desde que a solução permita aplicar o princípio do menor privilégio e limitar o operador aos recursos necessários ao atendimento.
21	Pergunta	Transferência de arquivos e impressão remota O requisito menciona bloqueio de funcionalidades específicas, incluindo transferência de arquivos e impressão remota. Solicitamos confirmar se o bloqueio de impressão remota é requisito obrigatório ou apenas exemplificativo. Caso seja exemplificativo, sugerimos: "A ferramenta deve possibilitar a configuração de bloqueio de transferência de arquivos durante as sessões de acesso remoto, de acordo com as políticas da RNP."
	RESPOSTA	Os exemplos de transferência de arquivos e impressão remota são exemplificativos das funcionalidades sensíveis que a RNP poderá restringir. A solução deverá, obrigatoriamente, permitir controlar ou bloquear transferência de arquivos. O bloqueio de impressão remota será exigido quando essa funcionalidade estiver disponível na solução.
22	Pergunta	Proteção de dados e configuração das sessões Solicitamos confirmar se os parâmetros de proteção poderão ser definidos pela própria RNP por meio de políticas administrativas, incluindo habilitação/desabilitação da gravação, aprovação prévia e limitação temporal do acesso. Como alternativa: "A ferramenta deve permitir configurar, conforme as políticas da RNP, parâmetros de proteção de dados, tais como habilitação ou desabilitação da gravação de sessão, aprovação prévia para acesso e restrição temporal do acesso."
	RESPOSTA	Sim. Os parâmetros de proteção deverão ser configuráveis pela própria RNP por meio de políticas administrativas, incluindo, quando suportado, habilitação ou desabilitação da gravação, exigência de consentimento ou aprovação prévia, limitação temporal, transferência de arquivos e demais funcionalidades sensíveis. Essas configurações deverão respeitar os requisitos obrigatórios de auditoria, segurança e proteção de dados previstos no TR.
23	Pergunta	O item 4 define o cenário de referência como 1.200 endpoints/dispositivos e 10 operadores, mas não informa como esse total se divide entre estações de trabalho, servidores e dispositivos móveis. Como o licenciamento varia conforme o tipo de ativo, solicitamos que a RNP informe a quantidade aproximada de estações de trabalho/notebooks, servidores e dispositivos móveis que compõem os 1.200 endpoints. Caso essa informação não esteja disponível, perguntamos se será aceito que o proponente declare na proposta a premissa de composição adotada.
	RESPOSTA	Para fins de dimensionamento comercial, deverá ser considerada a seguinte estimativa: 1.000 estações de trabalho e notebooks; 150 servidores; 50 dispositivos móveis; total estimado: 1.200 endpoints/dispositivos. O parque é heterogêneo e contempla Windows, Linux, macOS, Android e iOS/iPadOS. A distribuição detalhada por sistema operacional ainda não está consolidada, razão pela qual os fornecedores deverão informar claramente as premissas adotadas na proposta, as plataformas suportadas, eventuais diferenças funcionais e impactos no licenciamento
24	Pergunta	Vigência contratual: Qual será o prazo de vigência da contratação/licenciamento da solução? Não identificamos essa informação de forma explícita no convite e no Termo de Referência.
	RESPOSTA	A contratação e o licenciamento serão considerados pelo período inicial de 12 meses, contemplando licenças/subscrições, suporte técnico, atualizações, treinamento ou repasse técnico inicial e demais serviços previstos na proposta. Eventuais renovações serão avaliadas pela RNP conforme necessidade, disponibilidade orçamentária e condições contratuais.
25	Pergunta	Validade da proposta: O convite solicita que seja informada a validade da proposta, porém não identifica um prazo mínimo exigido pela RNP. Há alguma orientação ou prazo mínimo que deva ser considerado pelos fornecedores?
	RESPOSTA	A proposta deve ter, preferencialmente, 60 dias de validade.