1. Objeto:

1.1. A Companhia de Tecnologia da Informação do Estado de Minas Gerais – PRODEMGE, CNPJ nº 16.636.540/0001-04, doravante denominada CONSULENTE comunica aos interessados, doravante denominados PROPONENTES, que tenham interesse em participar da consulta de prospecção de **Software de Gestão de Ativos de Tecnologia da Informação - ITAM,** para utilização no ambiente computacional da CONSULENTE

1.2. O objetivo é conhecer as soluções de mercado relativas à **Gestão de Ativos de Tecnologia da Informação** que atendam aos requisitos técnicos definidos no **Anexo II** desse **Termo de Consulta.**

1.3. Durante a consulta a CONSULENTE irá avaliar o conjunto de funcionalidades do software proposto, o potencial de integração com as bases de dados de sistemas de informações hospedados no data center da CONSULENTE, o atendimento aos requisitos técnicos que atendam a gestão de ativos, as facilidades e os recursos do software.

1.4. A Proponente deverá comprovar ser o fabricante ou representante autorizado do software de Gestão de Ativos proposta.

1.5. Esse Termo de Consulta e seus anexos serão publicados no sitio eletrônico da CONSULENTE https://www.prodemge.gov.br/licitacoes/consultas-publicas-old

1.6. A documentação deverá ser encaminhada para compras@prodemge.gov.br

1.7. A CONSULENTE não aceitará propostas que não forem enviadas para o e-mail supracitado assim como as enviadas fora do prazo.

2. Das Condições de Participação

2.1. Poderá participar dessa consulta qualquer pessoa jurídica que atenda as exigências contidas neste Termo de Consulta e seus anexos.

2.2. A participação na consulta implica na aceitação de todas as condições estabelecidas neste Termo de Consulta e seus anexos.

2.3. As PROPONENTES permitirão a CONSULENTE utilizar os dados resultantes desta avaliação para confecção de Termo de Referência, Editais de Licitação e eventuais documentos públicos, com ou sem indicação de autoria.

2.4. A PROPONENTE arcará integralmente com todos os custos decorrentes de sua participação nesta consulta.

2.4.1. Não haverá qualquer forma de remuneração aos PROPONENTES que participarem da consulta.

2.4.2. Todos custos decorrentes serão de responsabilidade exclusiva da PROPONENTE.

2.5. Ao encaminhar a documentação a PROPONENTE deverá informar os dados da abaixo:

- Nome da empresa PROPONENTE
- CNPJ
- Endereço
- Telefone
- e-mail

2.6. A PROPONENTE deverá fornecer uma declaração informando que é fabricante ou representante autorizado do software de Gestão de Ativos de Tecnologia da Informação.

3. Prazos

3.1. A consulta pública estará aberta nos **5 (cinco) dias úteis** seguintes a publicação desse **Termo de Consulta** para inscrição dos PROPONENTES interessados e eventuais esclarecimentos técnicos.

3.2. Findado o prazo acima os PROPONENTES **terão mais 5 (cinco) dias úteis**, exclusivamente para encaminhamento da Planilha de Requisitos (**Anexo II**) e da Proposta Comercial (**Anexo I**) devidamente preenchidos, não sendo possível nesse segundo prazo nenhum esclarecimento técnico.

4. Da documentação

4.1. Planilha de Requisitos (Anexo II)

4.1.1. Deverá ser preenchida a coluna **Observações sobre o atendimento ao Requisito**, onde a PROPONENTE deverá informar:

4.1.1 **SIM** se atende totalmente

4.1.2 **PARCIALMENTE** se atende de forma parcial e informar como atende ao requisito técnico solicitado.

4.1.4 **NÃO** caso não atenda e informar possível solução de contorno para avaliação pela CONSULENTE.

4.2 Proposta Comercial (Anexo I)

4.2.1 Deverá ser preenchida as colunas **Valor Unitário** e **Valor Total** do **Software de Gestão de Ativos proposto** e a PROPONENTE deverá informar a solução proposta.

4.3 A documentação encaminhada deverá estar assinada, via certificado digital, pelo representante legal ou assinatura eletrônica com valor legal.

4.4 Os documentos (**Anexo I e Anexo II**) deverão ser encaminhados no prazo definido no item 3.0 (Prazos), para a COMPANHIA DE TECNOLOGIA DA INFORMAÇÃO DO ESTADO DE MINAS GERAIS – PRODEMGE, via e-mail **compras@prodemge.gov.br**

4.5 Poderá também ser incluída documentação técnica sobre o software proposto (arquivos PDF, catálogos, vídeos, etc.) visando subsidiar a avaliação do software ofertado, enviando também para o mesmo e-mail já citado compras@prodemge.gov.br

5. Da Avaliação Técnica das Propostas

5.1. Estar em conformidade com os requisitos técnicos definidos no **Anexo II**, desse **Termo de Consulta**.

5.2. Uma vez que o objetivo principal desta consulta é avaliar as soluções disponíveis no mercado, visando elaboração de Termo de Referência, Edital de Licitação e eventuais documentos públicos, com ou sem indicação de autoria.

5.3. Não será feita nenhuma publicação de avaliação técnica, sendo a avalição utilizada para subsidiar a confecção do Termo de Referência futuro.

6. Das Disposições Gerais

6.1 O presente Termo de Consulta poderá ser revogado por razões de interesse público, decorrente de fato superveniente devidamente comprovado, ou

anulado, no todo ou em parte, por ilegalidade de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente comprovado.

6.2 Os pedidos de esclarecimentos, referentes a presente consulta, deverão ser realizados por meio de e-mail, por escrito, a serem enviados à CONSULENTE, aos cuidados da Gerência de Compras. Endereço de e-mail: compras@prodemge.gov.br citando o número do Termo de Consulta. **Os pedidos de esclarecimentos deverão ser encaminhados dentro do período da Consulta**.

6.2.1 Nos pedidos de esclarecimentos os interessados deverão se identificar (CNPJ, Razão Social e nome do representante e número do Termo de Consulta) e disponibilizar as informações para contato (endereço completo, telefone e e-mail). Tais informações serão disponibilizadas junto aos questionamentos.

6.2.2 Os esclarecimentos serão respondidos pela CONSULENTE e publicados em https://www.prodemge.gov.br/licitacoes/consultas-publicas-old.

6.3 Qualquer PROPONENTE poderá, em qualquer momento da consulta, desistir de participar sem ônus para qualquer uma das partes.

6.4 Considerando que o objetivo do Termo de Consulta não é apontar um vencedor, toda a informação produzida será utilizada internamente pela CONSULENTE para subsidiar uma análise de possíveis alternativas.

7 Dos Anexos

7.1 São partes integrantes deste Termo de Consulta os anexos abaixo relacionados:

7.1.1 Anexo I – Proposta Comercial

7.1.2 Anexo II – Planilha de Requisitos

I. A proponente deverá preencher o formulário abaixo e informar o valor unitário e o valor total proposto considerando o quantitativo total de ativos solicitado.
II. Os preços devem ser apresentados em Reais (R$), com todos os impostos, taxas e despesas inclusas.

Subscrição – usuários nomeados

Item	Produtos e Serviços	Unidade	Quantidade Consolidado	Valor Unitário	Valor Total
1	Subscrição do SOFTWARE DE GESTÃO de Ativos de Tecnologia da Informação – ITAM	Item de Configuração	5.000		
				Total	

Local e data:

Número do Requisito	Detalhamento técnico do requisito	Observações sobre o atendimento do requisito técnico
1	**Administração**	
1.1	A solução deve permitir criar diferentes níveis de acesso a usuários em sua organização, de modo a segregar permissões entre diferentes usuários. As funções podem ser personalizadas diretamente pela organização.	
1.2	A solução deve permitir resolver a autenticação com o Active Directory, Azure Active Directory, Google, Office365, OKTA, nativamente e integrando-se com qualquer provedor de identidade compatível com SAML 2.0 ou posterior.	
1.3	A solução deve permitir que a organização seja totalmente independente na administração e configurações, podendo defini-las e redefini-las quantas vezes julgar necessárias para se ajustar à operação, sem implicar custos adicionais.	
1.4	A solução deve permitir o acesso unificado a todas as suas funcionalidades, limitando o número de módulos necessários para prover as funcionalidades a no máximo dois, garantindo assim baixa complexidade em sua operação e manutenção.	
1.5	A solução deve ser uma plataforma no-code, que permita que todas as configurações sejam feitas de forma visual e através da interface do usuário.	
1.6	O fabricante da solução deve assegurar as melhores práticas de mercado para a proteção e segurança da plataforma em nuvem, minimamente adotando as seguintes ações e mecanismos de controle em camadas:	
1.7	No âmbito da Governança:	
1.7.1	a) Adotar rotinas de análise e gestão de riscos	
1.7.2	b) Efetuar periodicamente Testes de penetração e avaliações de vulnerabilidade.	

1.7.3	c) Efetuar periodicamente Treinamento de conscientização de segurança.	
1.8	Quanto ao Acesso Físico:	
1.8.1	a) Hospedagem em datacenters certificados com padrões de controle de acesso em território nacional.	
1.8.2	b) Acesso seguro a todas as instalações que requeiram acesso autenticação de dois fatores.	
1.9	Quanto à Proteção de Perímetro:	
1.9.1	a) Adoção de Firewall Corporativos, totalmente redundantes.	
1.9.2	b) Adoção de Sistema de prevenção de intrusão (IPS) que monitora e bloqueia proativamente a atividade de tráfego malicioso na rede.	
1.9.3	c) Utilização de conexões HTTPS SSL de 256 bits.	
1.9.4	d) Utilização da camada de segurança de transporte (TLS) garante a transmissão segura de e-mails e arquivos de dados.	
1.9.5	e) Utilização de Certificados SSL (2048 bits).	
1.9.6	f) Utilização de Filtragem do conteúdo da web.	
1.9.7	g) Uso interno de Proteção antivírus e anti-malware empresarial.	
1.9.8	h) Fazer uso de solução de gerenciamento automatizado de patches e vulnerabilidades oferecendo resposta rápida a ameaças, ataques e outras atividades não autorizadas.	
1.9.9	i) Realização de Testes estáticos de segurança de aplicações, para detectar proativamente problemas relacionados à segurança no código e bibliotecas de terceiros.	
1.9.10	j) Testes de segurança de aplicações.	
1.9.11	k) Oferecer opções de criptografia de banco de dados em repouso, mediante solicitação.	

1.9.12	l) Backup seguro dos dados para armazenamento a curto e longo prazo utilizando a criptografia AES 256-bit.	
1.9.13	m) Dados em trânsito na Internet pública utilizando tecnologias de criptografia como HTTPS/SSL, TLS, AES e IPSec.	
1.9.14	n) Deve permitir a conexão segura entre o datacenter do contratante e a nuvem da solução através de uma conexão VPN site-to-site.	
1.9.15	o) Para o Gateway entre a infraestrutura do cliente e a nuvem SaaS da solução, utilizar técnicas de criptografia HTTPS, incluindo suporte para TLS 1.2, cifras criptográficas FIPS 140-2, e chave de 2048 bits de comprimento.	
1.9.16	p) Assegurar operação em modo 24x7 com 99,5% de disponibilidade.	
1.9.17	q) Operar em conformidade com as normas ISO 9001, ISO 27001, SOC 1, SOC2 e SOC3 , FISMA, DIACAP and FedRAMP , DOD CSM Levels 1-5 PCI DSS Level 1 , ITAR , FIPS 140-2 , MTCS Level 3.	
1.9.18	r) Existência de um Plano de Recuperação de Desastre e Continuidade dos Negócios.	
1.9.19	s) Deve adotar os procedimentos do ISCP (Information Systems Contingency Plan) projetados para recuperar s) Deve adotar os procedimentos do ISCP (Information Systems Contingency Plan) projetados para recuperar os serviços RTO (Recovery Time Objective) e RPO (Recovery Point Objective).	
2	**Interface**	
2.1	A solução deve ter um design responsivo, que permita o acesso de qualquer dispositivo (smartphones, tablets e computadores) e forneça uma interface que se adapte à tela dos mesmos.	

2.2	A solução deve ser web, exigindo apenas um navegador compatível e uma conexão com a internet. No mínimo, ele deve ser compatível para usuários finais com navegadores como Internet Explorer versão x ou superior, Microsoft Edge, Mozilla Firefox versão x ou superior, Google Chrome versão x ou superior.	
3	**Infraestrutura**	
3.1	A solução deve incluir um mecanismo de atualização automática e não assistida, e implementada na modalidade de Software como Serviço (SaaS), em nuvem pública de um dentre os principais provedores de nuvem pública (Amazon AWS, Microsoft Azure, Oracle Cloud ou Google Cloud) em território nacional.	
3.2	A solução deve permitir configurar certificados SSL, a fim de manipular uma conexão segura pelo protocolo HTTPS com os usuários.	
3.3	A solução deve permitir a personalização do domínio do mesmo, para se adequar ao domínio da organização.	
3.4	A solução deve ser implementada em um esquema de nuvem (nuvem pública em esquema SaaS).	
4	**Relatórios**	
4.1	A solução deve permitir que listas e relatórios sejam extraídos nativamente em formatos .csv e .xlsx padrão.	
4.2	A solução deve permitir a criação de relatórios e dashboards customizados pela organização, de forma visual através da interface, com total independência do provedor.	
5	**Suporte**	
5.1	O suporte deve fornecer acesso a uma base de conhecimento que contenha pelo menos documentação de configuração, práticas recomendadas e solução de problemas.	
5.2	A solução deve ter documentação oficial em português do Brasil ou inglês	

5.3	A aquisição da solução dá à organização acesso aos canais oficiais de suporte, sem limite e sem incorrer em custos adicionais.	
5.4	O suporte oficial da solução deve estar disponível em português do Brasil ou inglês.	
5	**Administração da Gestão de Ativos**	
5.1	A solução deve permitir definir campos estruturados personalizados associados a qualquer tipo de ativo e item de configuração. Esses campos e seus valores devem poder ser consultados e extraídos através de relatórios, nativamente na solução.	
5.2	O módulo de gerenciamento de ativos e configuração deve permitir a criação de regras de negócios personalizadas que acionam ações automáticas quando as condições estabelecidas são atendidas. Essas ações devem incluir, no mínimo, o envio de e-mails, atualizações automáticas de ativos e itens de configuração ou a execução de chamadas para serviços Web.	
5.3	A solução deve permitir organizar os ativos e itens de configuração por grupos, empresas e locais, a fim de executar diferentes regras de negócios e relatórios baseados neles.	
5.4	Sua solução deve permitir que organizar ativos e itens de configuração por grupos, empresas e locais automaticamente com base em critérios definidos por sua organização.	
5.5	A solução deverá permitir a importação de ativos de modo a facilitar a transferência e o Carregamento de ativos.	
5.6	A solução deve permitir definir tipos de ativos e elementos de configuração personalizados para a organização, podendo modelar suas características de acordo com seus critérios.	

5.7	A solução deve permitir modificar o local atribuído a um ativo e elementos de configuração com base em suas próprias características, como informações relacionadas ao seu domínio ou IP.	
6	**Operação**	
6.1	A solução deve permitir anexar arquivos quando necessário, sem que isso implique em custos adicionais.	
6.2	A solução deve permitir a atualização das informações dos ativos e itens de configuração em massa através da interface.	
6.3	A solução deve armazenar informações sobre todas as alterações aplicadas a um ativo ou item de configuração, identificando pelo menos a data, hora e usuário ou mecanismo que aplicou essa alteração. Essas informações de auditoria devem ser acessíveis a partir da interface, incluir a capacidade de filtrar por data, tipo de evento e exportar relatórios em formatos .xlsx e .csv. As informações devem permanecer disponíveis sem limite de validade e sem incorrer em custos adicionais.	
6.4	A solução deve permitir definir a disponibilidade, integridade e confidencialidade de um ativo ou elemento de configuração, e avaliar seu nível de criticidade de acordo com uma matriz baseada nessas características e definida pela organização.	
6.5	A solução deve permitir a criação de documentos relacionados a um ou mais ativos e itens de configuração. Esses documentos devem funcionar como material de apoio antes da movimentação e entregas, podem ser gerados de forma simples, duplicada ou triplicada e devem ser automaticamente relacionados aos elementos desde o seu momento de criação. Eles também devem ser personalizáveis para o uso da organização.	

6.6	A solução deve permitir identificar geograficamente o local a partir do qual a última atualização de informações para um ativo e item de configuração foi recebida. As informações devem ser entregues em latitude e longitude, bem como apresentadas em um mapa. No mínimo, deve ser capaz de obter essas informações em dispositivos Microsoft Windows 10 em diante.	
6.7	A solução deve permitir que o valor monetário expresso em moeda local seja exibido.	
6.8	A solução deve permitir a normalização automática de todos os softwares detectados em ativos e itens de configuração. Essa padronização deve incluir pelo menos o desenvolvedor de software, o tipo de software, o tipo de licenciamento e sua versão, e essas informações podem ser usadas para a configuração de relatórios e regras de negócios.	
6.9	A solução deve permitir a criação de códigos QR para a rotulagem física dos ativos, contendo algum identificador legível do ativo, como seu ID de inventário, e contendo informações sobre as características desse ativo.	
6.10	Estes códigos QR devem poder ser impressos em impressoras de etiquetas ou exportados em .csv para impressão com software especializado de terceiros.	
6.11	A solução deve permitir a leitura de códigos QR a partir de um dispositivo móvel, a fim de acessar os detalhes do ativo de qualquer lugar, e como um mecanismo para visualizar as atividades de inventário físico.	
6.12	A solução deve permitir definir e controlar grupos de regras de conformidade personalizadas, a fim de identificar o status de integridade de um ativo com base em políticas estabelecidas. Os recursos a serem monitorados devem incluir, no mínimo, status do firewall, status do antivírus, espaço em disco disponível, número de tíquetes pendentes e status da garantia.	
6.13	A solução deve habilitar automaticamente um inventário de IDs de conexão para provedores de área de trabalho remoto.	

6.14	A solução deve permitir medir o uso do software em ativos e itens de configuração, de forma a identificar o tempo de uso de um software específico em horas. Essas informações devem ter pelo menos uma atualização diária e devem poder ser visualizadas em relatórios.	
6.15	A solução deve permitir definir software e categorias de software observadas pela organização, e identifique automaticamente qualquer dispositivo que tenha esse software instalado	
6.16	A solução deve permitir a gestão do ciclo de vida completo dos ativos, sendo capaz de identificar e personalizar o estado em que se encontram.	
6.17	Deverá conter minimamente módulos para o cumprimento das ações de suporte remoto, distribuição de software na plataforma Windows, compliance, além de inventário de hardware e software.	
6.18	A solução deve permitir a conciliação de dispositivos detectados como duplicados com base em critérios, como números de série duplicados. Essa conciliação pode ser definida como manual ou automática, a critério da organização.	
6.19	A solução deve permitir a criação de IDs de inventário únicos e irrepetíveis, automaticamente, respeitando o formato personalizado pela organização.	
6.20	A solução deve permitir gerenciar as informações financeiras dos ativos, incluindo dados como data de garantia, fornecedor, pedido de compra, depreciação e centro de custo, entre outros.	
6.21	A solução deve permitir manter um inventário de ativos móveis, como smartphones e tablets.	
6.22	A solução deve permitir criar regras de cálculo de obsolescência, que identificam fácil e automaticamente dispositivos obsoletos no inventário com base em regras de negócios personalizadas	

7	**Gestão de Contratos**	
7.1	A solução deve permitir visualizar o custo anual estimado em licenças de software para cada estação de trabalho do usuário.	
7.2	A solução deve permitir gerenciar os contratos de serviço relacionados aos diferentes itens e ativos de configuração.	
7.3	A solução deve permitir gerenciar os contratos de licenciamento de software relacionados aos diferentes itens e ativos de configuração.	
8	**CMDB**	
8.1	Caso a solução necessite da instalação de clientes para a coleta de informações, elas devem ter a capacidade de serem atualizadas de forma totalmente automática e autônoma.	
8.2	A solução deve permitir recuperar informações de conformidade de computadores, incluindo pelo menos o antivírus, seu status, status de firewall e criptografia de disco.	
8.3	A solução deve permitir que varreduras de rede sejam realizadas para obter informações dos dispositivos conectados e a capacidade de incorporá-las ao CMDB. Essa descoberta deve funcionar com protocolos diferentes, incluindo pelo menos DNS, ICMP, mDNS, NetBIOS, SNMPv1, SNMPv2c, SNMPv3, TCP e UPnP.	
8.4	A solução deve permitir projetar e implementar mapas de relacionamento entre os componentes do CMDB, para que a organização possa identificar a composição de aplicativos, serviços, processos de negócios ou qualquer outro relacionamento que considere relevante e em um nível personalizado de detalhes.	

8.5	A solução deve ter um mecanismo automático de coleta de informações. Precisa ser capaz de fazer isso em qualquer dispositivo executando os sistemas operacionais Windows (7 ou posterior / 2003 Server ou posterior), Linux (Ubuntu 12.04 ou posterior / Debian 8 ou posterior / CentOS 7 ou posterior / Red Hat Enterprise Linux 7 ou posterior / Oracle Linux 6 ou posterior), macOS (macOS X 10.13 ou posterior) e Android (5 ou posterior).	
8.6	As informações devem poder ser coletadas de forma completamente independente do domínio e da rede em que os dispositivos estão localizados, mesmo que não estejam dentro da organização.	
8.7	A solução deve ter a capacidade de identificar relações entre diferentes itens de configuração e ativos. Essa relação deve descrever não apenas seu tipo, mas também a criticidade dele	
8.8	Caso a solução necessite da instalação de clientes para a coleta de informações, ela também deve fornecer mecanismos que permitam canalizar as informações através de proxies locais (on premise).	
9	**Integração**	
9.1	A solução deve permitir a integração nativa com um ou mais Active Directory´s locais. As informações armazenadas no Active Directory devem ser sincronizadas com o perfil do usuário na solução, incorporando pelo menos seu nome, e-mail e informações de contato.	
9.2	A solução deve ter uma API disponível e documentada que permita que as consultas REST sejam usadas a critério da organização nas integrações que julgarem apropriadas.	
9.3	A solução deve permitir a integração com outras soluções que estejam dentro da infraestrutura da organização, com total independência da infraestrutura da solução proposta.	

9.4	A solução deve permitir a integração nativa com os serviços da Amazon Web Services (AWS), a fim de manter as informações de todas as instâncias do EC2 implantadas com o CMDB sincronizadas. Essas informações devem incluir, no mínimo, nomes de instância, sistema operacional, capacidade de memória, processamento, armazenamento, tipo de instância, região e dados de custo financeiro.	
9.5	A solução deve permitir se integrar nativamente, para que possa iniciar uma conexão remota com um ativo ou item de configuração com esse serviço a partir dele.	
9.6	A solução deve permitir a integração nativa com os serviços do Azure, a fim de manter as informações de todas as instâncias do AzureVM implantadas com o CMDB sincronizadas. Essas informações devem incluir, no mínimo, nome da instância, sistema operacional, capacidade de memória, processamento, armazenamento, tipo de instância, região e dados de custo financeiro.	
9.7	A solução deve permitir a integração nativa com os serviços do Google, a fim de manter as informações de todos os Chromebooks sincronizadas com o CMDB.	
9.8	A solução deve permitir a integração nativa com os serviços JAMF, a fim de manter as informações de todos os dispositivos disponíveis sincronizadas com o CMDB.	
9.9	A solução deve permitir se integrar nativamente com o Microsoft RDP, para que possa iniciar uma conexão remota com um ativo ou item de configuração com esse serviço a partir dele.	
10	**Gestão do Ciclo de Vida do Ativo**	
10.1	Deverá conter minimamente módulos para o cumprimento das ações de suporte remoto, distribuição de software, compliance, gerenciamento de patches além de inventário de hardware e software.	

10.2	Deverá conter um banco de dados integrado ao servidor mestre, uma interface gráfica com o usuário para acessar os dados do banco de dados e agentes instalados nos clientes, fornecendo os dados para o banco de dados.	
10.3	Deverá permitir automatiza o rastreamento de inventário para ajudar a orientar as decisões de investimento, reduzir os processos manuais e manter a conformidade para dispositivos físicos e virtuais.	
10.4	Deverá permitir a implantação de sistema operacional e aplicativos de forma centralizada e automatizada permitindo a implantação ou migração de sistema operacional com a mínima interrupção.	
10.5	Deverá permitir o gerenciamento de licenças de software entendendo o uso da licença de software e os passivos financeiros associados.	
10.6	Deverá permitir o gerenciamento de patches, avaliando, implantando e gerando relatórios sobre patches de maneira centralizada para garantir que os sistemas sejam seguros e que a integridade de seus negócios nunca seja comprometida.	
10.7	Deverá permitir o gerenciamento de eventos rastreando e automatizando a correção de forma proativa quando eventos importantes de infraestrutura ocorrerem.	
10.8	Deverá permitir a aplicação de políticas de conformidade através do monitoramento centralizado de ativos de TI baseado nos modelos SCAP certificados pelo National Institute of Standards and Technology (NIST).	
10.9	Deverá permitir visualizar, controlar, monitorar e atualizar todos os principais softwares antivírus eanti spyware de uma única fonte.	
10.10	Deverá permitir o gerenciamento remoto da área de trabalho dos usuários para que os administradores detectem, diagnostiquem e resolvam problemas do PC sem sair de suas mesas.	
10.11	Deverá permitir o gerenciamento do consumo de energia do PC.	

10.12	Deverá permitir o gerenciamento de dispositivos definindo e aplicando de maneira centralizada as políticas de uso dos dispositivos, controlando a atividade de upload e download, e registrando eventos para uma resposta proativa e auditoria de qualquer atividade indesejada.	
10.13	Deverá permitir colocar softwares pré-aprovados e solicitações de acesso nas mãos do usuário final, sem acessar nenhum site ou enviar formulários de help desk.	
10.14	Deverá permitir o rastreamento do ciclo de vida de cada ativo de TIC, desde a aquisição até o descarte. Isso inclui informações como datas de compra, garantia, manutenções realizadas, atualizações de software, configurações e histórico de uso.	
10.15	Deverá permitir a geração de inventário de seus ativos de TI identificando exatamente como esses ativos estão sendo usados.	
10.16	Deverá permitir implantar, atualizar e corrigir facilmente sistemas operacionais e aplicativos através da instalação e distribuição remota de software.	
10.17	A solução deve ser capaz de monitorar a saúde e o desempenho dos ativos de TIC, fornecendo informações sobre utilização de recursos, status de conectividade, falhas de hardware, entre outros. Isso permite identificar problemas e tomar ações corretivas de forma proativa.	
10.18	Deverá permitir acessar remotamente todos os dispositivos, mesmo aqueles não conectados via VPN.	
10.19	Deverá ser possível compartilhar a tela do dispositivo remotamente, permitindo que os técnicos visualizem e interajam com o ambiente de trabalho dos usuários finais. Isso facilita o suporte técnico e a resolução de problemas.	
10.20	Deverá permitir que os técnicos assumam o controle total dos dispositivos remotamente, podendo executar ações como instalação de software, configuração de parâmetros, diagnóstico de problemas e correção de erros.	

10.21	Deverá ser compatível com os principais sistemas operacionais utilizados pela empresa CONTRATANTE, como Windows, macOS, Linux, Android e iOS. Além disso, deve suportar diferentes tipos de dispositivos, incluindo computadores, laptops, smartphones e tablets.	
10.22	Deverá fornecer recursos robustos de autenticação e controle de acesso, garantindo que apenas os técnicos autorizados possam estabelecer conexões remotas. Isso inclui autenticação multifator, políticas de acesso baseadas em funções e permissões granulares.	
10.23	Deverá registrar todas as atividades realizadas durante as sessões de acesso remoto, incluindo informações como data, hora, técnicos envolvidos e ações executadas. Esses registros podem ser utilizados para auditoria e fins de segurança.	
10.24	Deverá empregar criptografia robusta para proteger a transmissão de dados entre os dispositivos locais e remotos. Além disso, deve adotar medidas de segurança para evitar o acesso não autorizado aos dispositivos e garantir a proteção dos dados sensíveis.	
10.25	Deverá permitir integrar os dados do cliente à central de atendimento.	
10.26	Deve ser possível notificar os usuários finais quando uma sessão de acesso remoto está sendo iniciada, bem como permitir que eles visualizem e controlem a sessão em tempo real. Isso promove a transparência e o controle sobre o acesso remoto.	
10.27	Deve permitir analisar automaticamente o ambiente de TI, identificando quais dispositivos estão faltando quais patches.	

10.28	Deve ainda oferecer aos administradores opções para implantação rápida de correções críticas para garantir a conformidade e reduzir o risco de uma violação ou incidente de segurança, incluindo a opção de definir uma vez e automatizar a correção contínua para sistemas operacionais e aplicativos em todo o ambiente. Os administradores devem poder acompanhar facilmente o progresso das atualizações de patches em tempo real e poder utilizar assistentes integrados para definir rapidamente os parâmetros de pré e pós-instalação para controlar como a implantação ocorre.	
10.29	Deverá permitir atualizações automáticas de boletins de segurança através da configuração de downloads e atualizações para o catálogo de boletins de vulnerabilidades e patches.	
10.30	Deverá permitir determine as opções de implantação, critérios de patch e implantar atualizações de patch ao longo do tempo - automaticamente ou mediante revisão e aprovação - com o assistente integrado.	
10.31	Deverá permitir visualizar uma lista de patches ausentes por dispositivo com seu nível de gravidade.	
10.32	Deverá ter suporte à tecnologia Wake-on-LAN para a distribuição patches e outras tarefas de manutenção relacionadas automaticamente, fora do horário comercial, ativando PCs, implantando patches e desligando máquinas assim que as atualizações forem concluídas.	
10.33	Deverá permitir a criação de grupos dinâmicos direcionando grupos de dispositivos para atualizações com base nos requisitos de patch e nos atributos do computador.	
10.34	Deverá permitir monitore o processo de correção em tempo real e fornecer informações detalhadas sobre quaisquer erros ou anomalias para que possam ser tomadas medidas corretivas imediatas.	

10.35	Deverá permitir o gerenciamento de conformidade definindo políticas com base nos contratos de licenciamento de seus fornecedores e outros padrões regulatórios com ferramentas, relatórios e modelos essenciais para guias de proteção PCI, ISO 27001, ISO 27002, NIST e Microsoft.	
10.36	Deverá prover a medição de software acompanhando o uso real de qualquer aplicativo e reimplementando licenças de software não utilizadas para outros usuários.	
10.37	Deverá permitir a criação de grupos dinâmicos, identificando, agrupando e corrigindo os dispositivos que não seguem as políticas de conformidade definidas.	
10.38	Deverá permitir a descoberta de ativos com agente e sem agente com informações detalhadas de configuração.	
11	**Gestão do Controle Remoto do Ativo**	
11.1	A solução deve fornecer uma conexão segura entre os dispositivos da empresa contratante e os técnicos de TI, estes estando em trabalho remoto ou presencial, garantindo a confidencialidade e integridade dos dados durante a transmissão.	
11.2	Deve ser possível compartilhar a tela do dispositivo remotamente, permitindo que os técnicos visualizem e interajam com o ambiente de trabalho dos usuários finais. Isso facilita o suporte técnico e a resolução de problemas.	
11.3	A solução deve permitir que os técnicos assumam o controle total dos dispositivos remotamente, podendo executar ações como instalação de software, configuração de parâmetros, diagnóstico de problemas e correção de erros.	
11.4	Deve ser possível transferir arquivos entre os dispositivos locais e remotos, facilitando o compartilhamento de documentos, patches de software, atualizações e outros arquivos relevantes.	

11.5	Deverá suportar mecanismos de Multicasting e gerenciamento de largura de banda de rede nos processos de atualização e gerenciamento remoto de dispositivos.	
11.6	Deverá permitir a Implantação e atualizações do agente de forma automática para máquinas recém-descobertas.	
11.7	Deverá suportar a instalação remota do sistema operacional Windows, incluindo formatação/particionamento de discos rígidos.	
11.8	Deverá permitir a criação de um catálogo baseado na Web de software aprovado para instalações de auto-atendimento após a migração.	
11.9	Deverá permitir a execução de linha de comando, transferências de arquivos, gerenciamento da área de transferência e reinicialização do dispositivo de destino.	
11.10	Deverá manter trilha de auditoria de sessões de controle remoto e reconhecimentos do usuário final.	
11.11	Deverá permitir acesso direto ao dispositivo para realização de ações comuns, como: ativação, verificação de conectividade, reinicialização, desligamento, resumo da configuração, transferência de arquivo, controle remoto, sistema de arquivos, registro, serviços, gerenciamento de processos e eventos do Windows, e permita que os administradores executem qualquer uma dessas opções para ajustes após o expediente ou solução de problemas.	
11.12	A solução deve ser compatível com os principais sistemas operacionais utilizados pela empresa CONTRATANTE, como Windows, macOS, Linux, Android e iOS. Além disso, deve suportar diferentes tipos de dispositivos, incluindo computadores, laptops, smartphones e tablets.	

11.13	A solução deve fornecer recursos robustos de autenticação e controle de acesso, garantindo que apenas os técnicos autorizados possam estabelecer conexões remotas. Isso inclui autenticação multifator, políticas de acesso baseadas em funções e permissões granulares.	
11.14	A solução deve registrar todas as atividades realizadas durante as sessões de acesso remoto, incluindo informações como data, hora, técnicos envolvidos e ações executadas. Esses registros podem ser utilizados para auditoria e fins de segurança.	
11.15	A solução deve empregar criptografia robusta para proteger a transmissão de dados entre os dispositivos locais e remotos. Além disso, deve adotar medidas de segurança para evitar o acesso não autorizado aos dispositivos e garantir a proteção dos dados sensíveis.	
11.16	Deve ser possível notificar os usuários finais quando uma sessão de acesso remoto está sendo iniciada, bem como permitir que eles visualizem e controlem a sessão em tempo real. Isso promove a transparência e o controle sobre o acesso remoto.	
11.17	A solução deve permitir o registro de problemas encontrados durante as sessões de acesso remoto, bem como as soluções aplicadas. Isso contribui para a criação de um banco de conhecimento e o aprimoramento contínuo do suporte técnico.	