A2B TECNOLOGIA

CARTA PROPOSTA

DINAMISMO E INOVAÇÃO

os melhores caminhos para a proteção do seu negócio

A A2B é uma empresa de renome no mercado, pois oferta aos seus clientes a qualidade e confiança imprescindíveis para atender além de suas expectativas.

Contamos com um portfólio, que foi totalmente desenhado para transformar o conceito de cibersegurança e segurança da informação, com soluções customizadas e metodologia exclusiva.

Conheça as 3 razões do porquê nos escolher

Profissionais Capacitados

Certificamos a nossa equipe junto aos mais conceituados fornecedores de Segurança da Informação. Aliamos preparo e conhecimento em prol do seu negócio.

Eficiência

Um processo eficiente alcança seus objetivos com a quantidade mínima necessária de tempo, dinheiro, pessoas ou outros recursos.

Confiabilidade

A política de segurança da informação é fundamental para que o ambiente de TI corporativo seja bem-sucedido. As rotinas de proteção que adotamos em nossos clientes trazem a confiança necessária para que trabalhem com alto desempenho.

CARTA PROPOSTA

Brasília, 11 de agosto de 2022

À PRODAM- PROCESSAMNTOS DE DADOS DO AMAZONAS
A/C: TI
Assunto: Referência Edital de Licitação por Pregão Eletrônico SRP n°. 06/2022

Prezados Senhores:

É com satisfação que passamos às mãos de V.Sª, a nossa proposta para execução, com preço unitário, de acordo com Edital de Licitação por Pregão Eletrônico n.° 06/2022 e seus anexos.

LOTE ÚNICO

Objeto: Aquisição de licenças de uso perpétuo de solução de hiperautomação cognitiva, incluindo treinamento e serviços técnicos especializados, para suportar o ambiente de produção e operação da infraestrutura de TIC da PROCESSAMENTO DE DADOS AMAZONAS S/A – PRODAM utilizando Inteligência Artificial para Operações de TI – AIOPS, fornecendo gerenciamento autônomo das aplicações, além de orquestrar e fornecer Application Programming Interface – APIs algorítmicas para implantação de barramento de "machine learning" e inteligência artificial.

SUBITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Plataforma de AIOPS	Licença por Item de Configuração - IC	1.000	R$ 3.087,00	R$ 3.087.000,00
2	Suporte técnico á plataforma	Assinatura Anual	1	R$ 51.448,00	R$ 51.448,00
3	Serviço de operação assistida	TURMA	1.000	R$ 1.482,00	R$ 1.482.000,00
			TOTAL EM R$		**R$ 4.620.448,00**

VALOR TOTAL R$ 4.620.448,00(Quatro Milhões, seiscentos e vinte mil, quatrocentos e quarenta e oito reais.)

O prazo para execução dos serviços é de 12 [doze] meses, a contar da data de assinatura do contrato.

Declaramos expressamente, que nos preços propostos, estão inclusas todas as despesas concernentes ao fornecimento de equipamentos, ferramental, mão de obra necessária, encargos sociais, benefícios e despesas indiretas, licenças inerentes à especialidade e tributos.

Declara ainda qual a solução que irá fornecer, devendo comprovar conformidade da ferramenta de gerenciamento, automação e orquestração da infraestrutura de TI utilizando AIOPS, com as exigências constantes neste Termo de Referência (check list) detalhados no Termo de Referência e seus anexos, por meio de entrega de documentação comprobatória (CDs, link públicos, manuais, guias de instalação, documentos homologados pelo fabricante.

Acompanham a presente proposta, os documentos requeridos, e aproveitamos para confirmar nosso endereço para eventual correspondência e o banco com o qual mantemos relações comercias.

Razão Social- A2B SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA
Telefone- (61) 3326-1948
Endereço- SHN QUADRA 02 BLOCO F, SALA 1410/1414-EDF EXECUTIVE OFFICE TOWER-ASA NORTE
Estado-BRASILIA
CEP-70.702-906
Banco- Banco do Brasil
Agencia:53108-1
C/Corrente- 1004-9
E-mail-CONTATO@A2BTECNOLOGIA.COM.BR

Validade da Proposta: 90 (noventa) dias.

CLEIDIANE DE MORAIS BORGES:02330674180

Assinado de forma digital por CLEIDIANE DE MORAIS BORGES:02330674180
Dados: 2022.08.11 15:43:29 -03'00'

A2B Serviços em Tecnologia da Informação Ltda
Cleidiane de Morais Borges
RG 2.526.053 SSP-DF
CPF 023.306.741-80
Representante Legal
Administradora

PONTO A PONTO PE 06/2022- PRODAM

DESCRIÇÃO DOS ITENS	SITE OFICIAL
7. ESPECIFICAÇÕES TÉCNICAS DA PLATAFORMA DE AIOPS	https://docs.simonops.com/
7.1. Requisitos Funcionais da plataforma	https://docs.simonops.com/
7.1.1. A solução deverá prover acesso e suporte a no mínimo 100 (cem) usuários finais (*end users*) e 20 (vinte) profissionais resolvedores / administradores, sendo que as licenças não deverão ser nominais (isto é, vinculadas a uma pessoa sem a possibilidade de remanejá-la);	https://docs.simonops.com/
7.1.2. A solução deverá prover acesso e suporte a no mínimo 10 (dez) usuários com privilégios de extração de dados analíticos, assim como desenvolvimento, modelagem e construção de relatórios, indicadores e painéis de controle;	https://docs.simonops.com/
7.1.3. A solução deverá suportar os requisitos de escalabilidade, ou seja, a habilidade de manter e implementar estrutura modular, possibilitando acrescentar recursos, nós de processamento, armazenamento e memória, sem impactar o funcionamento da solução no ambiente de produção da CONTRATANTE.	https://docs.simonops.com/simon-zone#DA3yu
7.1.4. Qualquer módulo ou ferramenta necessária para atender os requisitos da especificação deverão estar contemplados na proposta técnica-financeira.	https://docs.simonops.com/
7.1.5. **Descoberta de itens de configuração (*Discovery*)**	https://docs.simonops.com/
7.1.5.1. A descoberta de itens de configuração deverá suportar o escaneamento multiprotocolo tais como HTTP, SSH, SNMP, ou APIs RESTful, dos itens de configuração conectados à rede;	https://docs.simonops.com/topologiahttps://docs.simonops.com/simon-zone#XOj66
7.1.5.2. O processo de descoberta de itens de configuração primário deverá ser preferencialmente com uso de agentes (agentfull) e oferecer a opção sem uso de agente (agentless);	https://docs.simonops.com/topologiahttps://docs.simonops.com/simon-zone#XOj66
7.1.5.3. Possuir repositório ou banco de dados único para os itens de configuração descobertos;	https://docs.simonops.com/topologiahttps://docs.simonops.com/simon-zone#XOj66
7.1.5.4. Identificar o relacionamento e dependências hierárquicas entre os itens de configuração descobertos;	https://docs.simonops.com/topologiahttps://docs.simonops.com/simon-zone#XOj66
7.1.5.5. A solução deverá ser capaz de descobrir serviços em nuvem utilizados pela CONTRATANTE;	https://docs.simonops.com/topologiahttps://docs.simonops.com/simon-zone#XOj66
7.1.5.6. A solução deverá permitir a realização de descoberta de itens de configuração programada por sub-redes e faixas de IP;	https://docs.simonops.com/topologiahttps://docs.simonops.com/simon-zone#XOj66
7.1.5.7. Prover recurso de descoberta de item de configuração para apenas um IP se assim for configurado;	https://docs.simonops.com/topologiahttps://docs.simonops.com/simon-zone#XOj66
7.1.5.8. Realizar o processo de descoberta de itens de configuração por meio de protocolo seguro criptografando os dados dos itens de configuração descobertos;	https://docs.simonops.com/topologiahttps://docs.simonops.com/simon-zone#XOj66
7.1.5.9. Utilizar credenciais criptografadas para acesso aos itens de configuração e realização da coleta de dados;	https://docs.simonops.com/topologiahttps://docs.simonops.com/simon-zone#XOj66
7.1.5.10. Suportar a descoberta de qualquer item de configuração conectado à rede;	https://docs.simonops.com/simon-zone#X_3ul
7.1.5.11. A plataforma deverá permitir customizações nas tabelas registro de itens de configuração para complementar informações pertinentes ao negócio da CONTRATANTE; A solução deverá permitir a programação agendamentos para realização do processo de descoberta a partir da parametrização feita pelo usuário;	https://docs.simonops.com/simon-zone#XOj66
7.1.5.12. A solução deverá permitir o cadastramento de itens de configuração novos e atualização de qualquer item de configuração previamente cadastrado;	https://docs.simonops.com/infraestrutura
7.1.5.13. Prover interface para operação e administração da solução via browser;	https://docs.simonops.com/#0dOUR
7.1.5.14. A solução deverá disponibilizar visualização gráfica dos itens de configuração e suas relações;	https://docs.simonops.com/infraestrutura#lAnIl
7.1.5.15. O agente não deverá utilizar mais de 5% de CPU, em média;	https://docs.simonops.com/sphere-agent#Gh4t-
7.1.5.16. Possibilitar a instalação dos agentes de forma manual e automática;	https://docs.simonops.com/sphere-agent#pA1aehttps://docs.simonops.com/sphere-agent#tAfPp
7.1.5.17. Permitir cadastro e atualização de itens de configuração;	https://docs.simonops.com/infraestrutura#XB6i-
7.1.5.18. Possuir Discovery troubleshooting para identificar os problemas de descoberta e coleta de dados dos ativos;	https://docs.simonops.com/hosts#af2k8
7.1.6. **Gerenciamento de eventos**	https://docs.simonops.com/
7.1.6.1. A solução deverá correlacionar os eventos coletados de diferentes fontes utilizando técnicas de *machine learning* e os mapas de serviços cadastrados, entre outros recursos;	https://docs.simonops.com/correlacao-de-eventos
7.1.6.2. A solução deverá categorizar os eventos conforme sua severidade com base na importância que um determinado item de configuração tem para o serviço que está em operação;	https://docs.simonops.com/correlacao-de-eventos#kjnfH
7.1.6.3. A categorização de severidade dos eventos poderá ser realizada manualmente ou automaticamente através de técnicas de aprendizagem de máquina supervisionada, semi-supervisionada ou não supervisionada;	https://docs.simonops.com/correlacao-de-eventos#kjnfH
7.1.6.4. O gerenciamento de eventos deverá estar integrado com a funcionalidade de Service Mapping;	https://docs.simonops.com/eventos-e-incidentes#jj7kZ
7.1.6.5. A solução deverá implementar a criação de identificador único para cada correlação implementando o padrão de identificação do tipo “Season ID”, representando o ID no padrão ID/mês, suportando o ID com padrão numérico de até 6 algarismos decimais e mês com até 2 algarismos decimais.	https://docs.simonops.com/correlacao-de-eventos#kjnfH
7.1.6.6. Na gestão de eventos deverá ser implementados filtros de busca utilizando parâmetros de filtros por Status, Ordenação, Prioridade e por Tipo de cada correlação. Deverá ser possível, ainda, a busca por filtro de tempo, disponibilizando opções mais utilizadas, como: Hoje, últimos 7, 15 e 30 dias, além de período customizado de cada correlação.	https://docs.simonops.com/listagem-de-incidentes
7.1.6.7. A solução deverá suportar a análise de causa raiz dos eventos coletados das diferentes fontes e itens de configuração;	https://docs.simonops.com/atuacao-em-incidentes#TDrpA
7.1.6.8. A solução deverá agrupar os alertas baseado na análise de causa raiz sugerida automaticamente;	https://docs.simonops.com/atuacao-em-incidentes#TDrpA
7.1.6.9. A solução deverá prover visualização gráfica e tabulada das métricas operacionais cadastradas;	https://docs.simonops.com/metricas
7.1.6.10. A solução deverá prover mecanismos de integração e consolidação de eventos com as ferramentas de monitoramento (Solar Winds, Zabbix, AppDynamics, etc) para coleta de eventos e/ ou alertas;	https://docs.simonops.com/integracoes#LRnPg
7.1.6.11. A solução deverá suportar integrações com ferramentas de monitoramento por meio de API REST, SNMP, conectores nativos ou desenvolvidos;	https://docs.simonops.com/integracoes#LRnPg

7.1.6.12. A solução deverá distinguir a severidade dos status dos serviços por esquemas de cores;	https://docs.simonops.com/correlacao-de-eventos#kjnfH
7.1.6.13. A solução deverá gerar incidentes automaticamente para ferramenta de ITSM da PRODAM (SGTI) a partir dos critérios definidos para os itens de configuração;	https://docs.simonops.com/integracoes#PzzHx
7.1.6.14. A solução deverá permitir o cadastro de ações de remediação automáticas disparadas por eventos ou alertas deflagrados na solução;	https://docs.simonops.com/atuacao-em-incidentes#8gUU5
7.1.6.15. A solução deverá disponibilizar um painel central de operações intuitivo que permita a visualização da saúde dos serviços e dos eventos relacionados a eles, permitir a navegação e drill down até as informações dos itens de configuração;	https://docs.simonops.com/servicos-de-ti
7.1.6.16. A solução deverá ter a capacidade de identificação da causa raiz do serviço de TI ou de negócio alarmado no painel central da solução através dos eventos originados das diversas ferramentas de monitoramento legadas da PRODAM.	https://docs.simonops.com/atuacao-em-incidentes#TDrpA
7.1.6.17. A tela de gestão dos eventos deverá suportar parametrização do tempo de atualização das informações com, no mínimo, 5/10/15/30 segundos, 1/2/10/15 minutos.	https://docs.simonops.com/listagem-de-incidentes
7.1.6.18. A solução deverá apresentar interface de análise preditiva do ambiente de infraestrutura, na qual deverá informar a previsão para os próximos 5/10/15 minutos de incidentes em cada dispositivo monitorado. Deverá ainda informar qual o serviço que poderá ser afetado em razão do possível incidente previsto.	https://docs.simonops.com/listagem-de-incidentes
7.1.6.19. A plataforma deverá ser capaz de se comunicar com as ferramentas da suíte de banco de dados ADABAS e Natural possibilitando a coleta de métricas para análises.	https://docs.simonops.com/simon-zone#XOj66
7.1.7. **Inteligência Operacional (AIOps)**	https://docs.simonops.com/
7.1.7.1. A solução deverá prover funcionalidades de aprendizagem de máquina para utilizar qualquer informação, massa de dados ou funcionalidade disponível na plataforma para desenvolver a inteligência operacional;	https://docs.simonops.com/simon-zone#XOj66https://docs.simonops.com/incidentes
7.1.7.2. A solução deverá realizar de-duplicação dos eventos coletados de diversas fontes com a finalidade de identificar com mais precisão a causa raiz e eliminar duplicidades que venham gerar desvios nas análises de dados e tirar o foco do operador;	https://docs.simonops.com/correlacao-de-eventos
7.1.7.3. A solução deverá ter capacidade de realizar filtragem dos eventos possibilitando análises mais limpas, ricas e focadas;	https://docs.simonops.com/listagem-de-incidentes
7.1.7.4. A solução deverá normalizar os eventos oriundos de diversas ferramentas e fontes de dados consolidando sua nomenclatura;	https://docs.simonops.com/incidentes
7.1.7.5. A solução deverá realizar o agrupamento automático de alertas relacionados entre si facilitando o gerenciamento, a tomada de decisão e operação;	https://docs.simonops.com/correlacao-de-eventos
7.1.7.6. A solução deverá ter a capacidade de identificar automaticamente padrões de eventos e alertas	https://docs.simonops.com/atuacao-em-incidentes
7.1.7.7. A solução deverá ter capacidade de, com base no comportamento das operações, atribuir “thresholds” automaticamente. Estes limites poderão ser reajustados manualmente;	https://docs.simonops.com/alertas-triggers
7.1.7.8. A solução deverá permitir a construção de “datasets” a partir de dados históricos das operações e das ações e atividades executadas pelos usuários e operadores da solução;	https://docs.simonops.com/atuacao-em-incidentes#dKvzF
7.1.7.9. A solução deverá possuir recursos de análise dos alertas com base em padrões temporais identificando comportamentos recorrentes e sazonalidades das operações podendo inclusive inibir alertas para comportamentos corriqueiros;	https://docs.simonops.com/atuacao-em-incidentes#dKvzF
7.1.7.10. A solução deverá priorizar automaticamente alertas baseado na recorrência de eventos com o passar do tempo;	https://docs.simonops.com/atuacao-em-incidentes#dKvzF
7.1.7.11. A solução baseada na inteligência operacional e na análise de dados históricos ter a capacidade de predizer alertas através de análises de padrões parciais, ou seja, gerar estimativas de probabilidade de ocorrência;	https://docs.simonops.com/listagem-de-incidentes
7.1.7.12. A solução deverá suportar a correlação topológica de alertas baseado em CMDB - Configuration Management data Base, ou seja, em seus itens de configuração e relacionamentos, além do uso dos mapas de serviços com a finalidade de identificar o evento de origem e a propagação de sua consequência nos serviços mapeados em que há dependência direta ou indireta do item de configuração alertado;	https://docs.simonops.com/#o4XI6
7.1.7.13. A solução deverá suportar o feedback dos usuários para otimizar o modelo de correlação de alertas e eventos, ou seja, aprendizado semi-supervisionado;	https://docs.simonops.com/correlacao-de-eventos
7.1.7.14. Ajustar automaticamente os “thresholds” dos alertas conforme o comportamento dos dados e eventos coletados	https://docs.simonops.com/atuacao-em-incidentes
7.1.7.15. A solução deverá permitir a atribuição de pesos aos itens de configuração, manualmente ou automaticamente, para que em um potencial ocorrência de interrupção de serviço seja aplicada com mais precisão as estimativas de probabilidades de ocorrência e indicando o nível de criticidade de seu impacto	https://docs.simonops.com/correlacao-de-eventos#kjnfH
7.1.7.16. A solução deverá ter capacidade de analisar grande volume de dados para identificar e resolver incidentes e realizar melhoria operacional	https://docs.simonops.com/listagem-de-incidentes
7.1.8. **Orquestração e sincronização de tarefas (Orchestration)**	https://docs.simonops.com/
7.1.8.1. A solução deverá automatizar e sincronizar tarefas e fluxos de trabalho das mais simples às mais complexas;	https://docs.simonops.com/pipes-e-automacao
7.1.8.2. A funcionalidade de orquestração deverá integrar aos demais processos e funcionalidades da plataforma;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.8.3. A solução deverá prover conectores para os elementos de infraestrutura e plataforma da PRODAM permitindo que as tarefas e workflows desenhados no módulo de orquestração sejam executadas por todo o ambiente de TI da CONTRATANTE;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.8.4. A solução deverá suportar o desenvolvimento de fluxos de trabalhos conectados a qualquer elemento de infraestrutura da PRODAM;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.8.5. A solução deverá permitir a criação de componentes reutilizáveis para outros fluxos;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.8.6. A solução deverá disponibilizar painel de controle específico para consulta, edição e execução dos fluxos;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.8.7. A solução deverá suportar a programação de execução dos fluxos pelo menos das seguintes formas:	https://docs.simonops.com/pipes-e-automacao
7.1.8.8. Programada a partir de definições de schedule;	https://docs.simonops.com/pipes-e-automacao
7.1.8.9. Manual a partir de interação do usuário	https://docs.simonops.com/pipes-e-automacao
7.1.8.10. Automática sendo disparada por ações de outros sistemas e fluxos ou eventos e ações da própria plataforma;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.8.11. A solução deverá permitir que os componentes dos fluxos desenvolvidos façam chamadas externas à plataforma;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.8.12. A solução deverá persistir os dados das execuções dos fluxos de trabalho;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.8.13. A solução deverá suportar integração com webservices;	https://docs.simonops.com/testes-web
7.1.8.14. A solução deverá suportar integração via linha de comando;	https://docs.simonops.com/pipes-e-automacao

7.1.8.15. A solução deverá suportar integração com banco de dados;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.8.16. A solução deverá suportar nativamente design de fluxos de trabalho de forma gráfica;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.8.17. A solução deverá disponibilizar dashboard com métricas e gráficos do histórico das execuções dos fluxos de trabalho	https://docs.simonops.com/pipes-e-automacao
7.1.8.18. A solução deverá prover design gráfico dos workflows inclusive em tempos de execução;	https://docs.simonops.com/pipes-e-automacao
7.1.8.19. A solução deverá prover recursos para automatização de tarefas do Service Desk baseado em seus processos e catálogo de serviços;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.8.20. Os desenvolvimentos de fluxos deverão seguir o processo de Gerenciamento de Mudanças;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.8.21. A solução deverá prover ambientes segregados para realização dos desenvolvimentos e testes do ambiente de produção;	https://docs.simonops.com/pipes-e-automacaohttps://docs.simonops.com/pipes-e-automacao#c5bfo
7.1.9. **Mapeamento de Serviços (Service Mapping)**	https://docs.simonops.com/
7.1.9.1. A solução deve ser capaz relacionar os ativos de TI com Serviços em um mapa de relacionamento de forma automatizada pelo processo de descoberta;	https://docs.simonops.com/topologia
7.1.9.2. A solução deverá ter capacidade de construir mapas de serviço baseado em dependências identificando automaticamente os relacionamentos dos itens de configuração;	https://docs.simonops.com/topologiahttps://docs.simonops.com/monitor-de-network
7.1.9.3. A solução deverá exibir os itens de configuração e os relacionamentos entre eles de forma gráfica e interativa;	https://docs.simonops.com/topologiahttps://docs.simonops.com/monitor-de-network
7.1.9.4. A solução deverá permitir construção ou adequação automático dos mapas de serviços;	https://docs.simonops.com/topologia
7.1.9.5. Os mapas de serviços construídos deverão ser disponibilizados via API para possível integração a partir de informações úteis ao CMDB utilizado pela PRODAM.	https://docs.simonops.com/topologia
7.1.9.6. A solução deverá se integrar com Gerenciamento de Eventos em tempo real;	https://docs.simonops.com/monitor-de-network
7.1.9.7. A solução deverá sinalizar nos itens de configuração no mapa de serviço a relação com os eventos em qualquer criticidade apontada pelo gerenciamento de eventos;	https://docs.simonops.com/monitor-de-network
7.1.9.8. Assim como no Gerenciamento de Eventos, a solução deverá diferenciar os eventos nos itens de configuração do mapa de serviços através de esquema de cores;	https://docs.simonops.com/alertas-triggers#0sSqC
7.1.9.9. A interatividade dos mapas de serviço deverá permitir opções para ações de correção diretamente do mapa do serviço se integrando a ações automatizadas no módulo de orquestração;	https://docs.simonops.com/correlacao-de-eventos
7.1.9.10. A solução deverá permitir ao usuário o ajuste e a visualização do mapa permitindo desta forma o aumento ou redução do tamanho do mapa e a focalização nos itens de configuração do mapa mantendo boa resolução para leitura das informações;	https://docs.simonops.com/monitor-de-network
7.1.9.11. A solução deverá ter recursos para mapear Cloud Services (Serviços em Nuvem) durante o processo de mapeamento dos serviços;	https://docs.simonops.com/servicos-de-ti
7.1.9.12. A solução deverá estar integrada ao processo de Gerenciamento de Mudanças de forma a atualizar automaticamente os mapas de serviços ou pelo menos identificar e notificar os administradores da solução que existe uma pendência de atualização;	https://docs.simonops.com/servicos-de-ti
7.1.9.13. A solução deverá se integrar com o processo de Gerenciamento de Níveis de Serviço para que os acordos de nível de serviços cadastradas nos Catálogos de Serviços sejam refletidos nos mapas de serviço;	https://docs.simonops.com/servicos-de-ti
7.1.9.14. A solução deverá permitir categorizar os mapas de serviços construídos em pelo menos Serviços Técnicos ou de Suporte e Serviços de Negócio, porém primando pelo foco na visão de Serviços de Negócio;	https://docs.simonops.com/servicos-de-ti
7.1.9.15. A solução deverá manter arquivado o histórico de informações, alterações e atualizações dos mapas de serviço permitindo rastreabilidade das mudanças com pelo menos as seguintes informações: Autor, data e hora da mudança;	https://docs.simonops.com/servicos-de-ti
7.1.9.16. A solução deverá ter capacidade de efetuar correções automáticas dos mapas de serviço utilizando diversas técnicas inclusive a aprendizagem de máquina (machine learning) do módulo AIOps;	https://docs.simonops.com/pipes-e-automacao
7.1.9.17. A solução deverá mapear estruturas complexas como cluster e barramentos corporativos	https://docs.simonops.com/servicos-de-ti
7.1.9.18. A solução deverá oferecer recursos para mapeamento de estruturas virtualizadas (Vmware, Citrix, KVM, Hyper-V)	https://docs.simonops.com/servicos-de-ti
7.1.9.19. A solução deverá permitir drill down do mapa de serviço até as informações dos itens de configuração do serviço;	https://docs.simonops.com/servicos-de-ti
7.1.10. **Monitoramento de Serviços de Negócios com APM**	https://docs.simonops.com/
7.1.10.1. Monitoramento autônomo inteligente de aplicações e sistemas com o intuito de disponibilizar o mapeamento constante e automático de todas as interdependências entre aplicações, serviços, processos e hosts. Correlacionando os componentes e alertando quando existe um problema acontecendo.	https://docs.simonops.com/application-performance-management
7.1.10.2. A plataforma deverá ser capaz de monitorar transações de aplicações em tempo real	https://docs.simonops.com/application-performance-management
7.1.10.3. A plataforma deverá possuir funcionalidade de que possibilitará a análise de todas as transações de serviços que compõem as aplicações, permitindo filtros compostos por status, serviços, tipo da transação, método http e query.	https://docs.simonops.com/application-performance-management
7.1.10.4. A plataforma deverá permitir o detalhamento dos serviços que compõem as aplicações, podendo demonstrar através de gráficos as seguintes informações: Total de requisições, Erros, Latência máxima, Latência p90, Latência p50, distribuição de latência pelo total de requisições e listagem dos recursos acionados, como queries e endpoints.	https://docs.simonops.com/application-performance-management
7.1.10.5. A plataforma deverá permitir a listagens dos serviços que são utilizados pelas aplicações da PRODAM.	https://docs.simonops.com/application-performance-management
7.1.10.6. A plataforma deverá permitir a listagens de todas as transações que pertencentes às execuções nos serviços que compõem as aplicações, em forma de flamegraph podendo ser capaz de demonstrar rapidamente o tempo de execução de cada uma das aplicações.	https://docs.simonops.com/application-performance-management
7.1.10.7. A plataforma deverá ser capaz de exibir dados referentes a contêineres que suportam os serviços das aplicações.	https://docs.simonops.com/application-performance-management
7.1.10.8. A plataforma deverá ser capaz de ao detalhar uma execução, exibir o agrupamento das transações realizadas por serviço, a fim de facilitar e dar visibilidade ao fluxo de execução.	https://docs.simonops.com/application-performance-management
7.1.10.9. A plataforma deverá suportar a painéis visuais com dados para monitoramento dos usuários de uma aplicação.	https://docs.simonops.com/application-performance-management
7.1.10.10. A plataforma deverá ser capaz de identificar erros ocorridos nas aplicações.	https://docs.simonops.com/application-performance-management
7.1.10.11. A plataforma deverá ser capaz de identificar erros de javascript que podem acontecer ao usuário utilizar às aplicações.	https://docs.simonops.com/application-performance-management
7.1.10.12. A plataforma deverá ser capaz de identificar as ações realizadas por um usuário no decorrer de uma sessão de uso.	https://docs.simonops.com/real-user-monitoring
7.1.10.13. A plataforma deverá ser capaz de listar os recursos carregados através da utilização das aplicações via navegador web.	https://docs.simonops.com/application-performance-management

		7.1.10.14. A plataforma deverá ser capaz de acionar um fluxo de automação a partir de algum problema que possa ter ocorrido em um dos serviços das aplicações.	https://docs.simonops.com/application-performance-managementhttps://docs.simonops.com/pipes-e-automacao
		7.1.10.15. A plataforma deverá ser capaz de identificar as transações do tipo SQL que possam ocorrer e quais os serviços acionados durante essas transações.	https://docs.simonops.com/application-performance-management
		7.1.10.16. A plataforma deverá ser capaz de listar as aplicações de monitoramento do usuário final contemplando o número de sessões, tempo de carregamento e percentual de erros ocorridos.	https://docs.simonops.com/real-user-monitoring
		7.1.10.17. A plataforma deverá suportar o gerenciamento de performance das aplicações da PRODAM para, no mínimo, as seguintes tecnologias de desenvolvimento e versões:	https://docs.simonops.com/application-performance-management
Biblioteca	**Tecnologia**	**Compatibilidade de Versão**	https://docs.simonops.com/apm-staging/Tsst-net
.NET	.NET Core	.NET Core 2.1, 3.1, e .NET 5.	https://docs.simonops.com/apm-staging/Tsst-net
	.NET Framework	.NET Framework 4.5 ou maior.	https://docs.simonops.com/apm-staging/Tsst-net
NodeJS	connect	>=2	https://docs.simonops.com/apm-staging/Q9bM-nodejs
	express	>=4	https://docs.simonops.com/apm-staging/Q9bM-nodejs
	fastify	>=1	https://docs.simonops.com/apm-staging/Q9bM-nodejs
	graphql	>=0.10	https://docs.simonops.com/apm-staging/Q9bM-nodejs
	gRPC	>=1.13	https://docs.simonops.com/apm-staging/Q9bM-nodejs
	hapi	>=2	https://docs.simonops.com/apm-staging/Q9bM-nodejs
	koa	>=2	https://docs.simonops.com/apm-staging/Q9bM-nodejs
	microgateway-core	>=2.1	https://docs.simonops.com/apm-staging/Q9bM-nodejs
	next	>=9.5	https://docs.simonops.com/apm-staging/Q9bM-nodejs
	paperplane	>=2.3	https://docs.simonops.com/apm-staging/Q9bM-nodejs
	restify	>=3	https://docs.simonops.com/apm-staging/Q9bM-nodejs
Ruby	MRI	2.1 +	https://docs.simonops.com/apm-staging/ruby
	Jruby	9.2 +	https://docs.simonops.com/apm-staging/ruby
PHP	Linguagem	5.4.x a 8.0.x	https://docs.simonops.com/apm-staging/dPer-php
Java	Linguagem	JRE 1.7 e versões superiores	https://docs.simonops.com/apm-staging/java
Python	Linguagem	versões 2.7+ e 3.5+	https://docs.simonops.com/apm-staging/j92n-python
		Tabela 1: Listagem de tecnologias de desenvolvimento suportadas pela plataforma de AIOPS	https://docs.simonops.com/
		7.1.11. **Integrações**	https://docs.simonops.com/
		7.1.11.1. A plataforma deverá oferecer recurso de autenticação dos usuários do tipo SSO (Single Sign-On), sincronizável com a console de administração de domínio da plataforma Windows – Active Directory; para os diversos perfis existentes (requisitantes, aprovadores, resolvedores, gestores de aplicação, etc.);	https://docs.simonops.com/integracoes#FLBJo
		7.1.11.2. Todos os custos com a integração serão de responsabilidade da CONTRATADA. A PRODAM fornecerá acesso às soluções através de usuário e senha, API ou Webservice.	https://docs.simonops.com/integracoes
		7.1.11.3. A plataforma deverá ser capaz de se integrar com a plataforma de gerenciamento de serviços (ITSM – IT Service Management) implantado na PRODAM, conforme:	https://docs.simonops.com/integracoes#PzzHx
		7.1.11.4. Integração com soluções de autosserviço e de automações de processos de negócio. Exemplo: Integração com o Portal de Serviços de TI da plataforma de ITSM e outras plataformas da PRODAM permitindo a automação de serviços end-to-end;	https://docs.simonops.com/integracoes#PzzHx
		7.1.11.5. A plataforma deverá suportar a integração com os sistemas de e-mail da CONTRATANTE.	https://docs.simonops.com/integracoes#hCg4B
		7.1.11.6. A plataforma deverá permitir a integração de sistemas de terceiros tais como OTRS, 4Biz, ServiceNow, CITSmart, Zabbix, Nagios, Splunk, CloudWatch, AppDynamics, SolarWinds, Sensu, Pingdom, DataDog, New Relic, OpsView, Slack, Twilio, Centreon.	https://docs.simonops.com/integracoes#LRnPg
		7.1.11.7. Deve ser capaz de analisar e correlacionar diversos de sensores, eventos e processos distintos, dos sistemas de monitoramento e de segurança do ambiente do cliente na qual listamos alguns, mas não limitando a:	https://docs.simonops.com/integracoes#LRnPg
		7.1.11.8. Zabbix, Nagios, Splunk, CloudWatch, AppDynamics, SolarWinds, Sensu, Pingdom, DataDog, New Relic, OpsView, Slack, Twilio, Centreon.	https://docs.simonops.com/integracoes#LRnPg
		7.1.11.9. Deve permitir que os eventos correlacionados sejam automaticamente direcionados às filhas solucionadoras de cara área da infraestrutura de TI provendo informações de possíveis causas raiz, das áreas afetadas e o tempo de vida do evento apontando as alterações de status dos eventos ocorridas por período.	https://docs.simonops.com/incidentes
		7.1.11.10. Apresentar flexibilidade na personalização e integração de interfaces, fluxos de trabalho e ações de automação;	https://docs.simonops.com/pipes-e-automacao
		7.2. **Requisitos auxiliares da plataforma**	https://docs.simonops.com/
		7.2.1. Geral	https://docs.simonops.com/
		7.2.1.1. Todas as informações armazenadas no banco de dados da solução contratada são pertencentes à PRODAM e poderão ser acessadas a qualquer momento, mesmo após o encerramento do contrato de prestação de serviços;	https://docs.simonops.com/
		7.2.1.2. As informações armazenadas no banco de dados da solução contratada pertencentes à PRODAM deverão ser disponibilizadas em sua integralidade após o encerramento do contrato, por um período mínimo de 120 (cento e vinte) dias;	https://docs.simonops.com/
		7.2.1.3. O licenciamento será realizado através da contratação de licenças na modalidade de aquisição perpétua da solução;	https://docs.simonops.com/
		7.2.1.4. A entrega das licenças deverá ocorrer em até 10 (dez) dias após assinatura do contrato.	https://docs.simonops.com/

7.2.1.5. As atualizações das versões da solução ofertada deverão ser realizadas durante todo o período de vigência contratual;	https://docs.simonops.com/#0dOUR
7.2.1.6. A "atualização de versão" deve ser entendida como o fornecimento de novas versões corretivas ou evolutivas do software componente do serviço, mesmo em caso de mudança de designação do nome do software, devendo compreender a correção de falhas e implementação de melhorias no produto independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas à CONTRATADA;	https://docs.simonops.com/#0dOUR
7.2.1.7. A versão da solução ofertada deverá ser a mais recente e estável disponibilizada e seguir o roadmap de atualizações do fabricante durante a vigência do contrato;	https://docs.simonops.com/#0dOUR
7.2.1.8. Todos os custos necessários para viabilização do projeto devem estar previstos nas propostas incluindo, viagens, deslocamentos, hospedagens e alimentação. Nenhum valor poderá ser cobrado extraordinariamente da PRODAM por conta de despesas não planejadas pelo fornecedor.	https://docs.simonops.com/#0dOUR
7.2.2. **Infraestrutura e Plataforma**	https://docs.simonops.com/
7.2.2.1. Documentação técnica da solução, apresentando, no mínimo, o blueprint de arquitetura, com destaque para os seguintes pontos: interfaces entre módulos da aplicação, pontos de conexão com sistemas externos, bases de dados. Descrever quais outras documentações são disponibilizadas juntamente com a solução.	https://docs.simonops.com/simon-zone
7.2.2.2. As aplicações e demais recursos presentes no serviço contratado devem possuir o horário sincronizado de forma automática com a Hora Legal Brasileira no Observatório Nacional;	https://docs.simonops.com/#0dOUR
7.2.2.3. A solução ofertada deverá oferecer arquitetura de alta disponibilidade;	https://docs.simonops.com/requisitos-de-software#JoiLw
7.2.2.4. A solução ofertada deverá oferecer arquitetura de escalabilidade;	https://docs.simonops.com/requisitos-de-software#JoiLw
7.2.2.5. Banco de dados único, 100% exportável, pelo menos, para Oracle ou Microsoft SQL Server na versão utilizada pela PRODAM no momento da solicitação ou conforme requisitos especificados no ato da solicitação;	https://docs.simonops.com/requisitos-de-software#_Pgwh
7.2.2.6. Documentação de monitoramento da solução, descrevendo detalhadamente quais pontos precisam ser monitorados (processos, serviços, logs, etc.);	https://docs.simonops.com/simon-zone
7.2.2.7. O sistema deve possuir compatibilidade com versões atualizadas e suportadas pelos fabricantes de sistema operacional, banco de dados, plugins e outros serviços necessários para seu funcionamento.	https://docs.simonops.com/requisitos-de-software#aEjQx
7.2.2.8. Todo licenciamento, os serviços de manutenção e sustentação destes componentes para operação da solução deve fazer parte do pacote de suporte oferecido, não cabendo à CONTRATANTE quaisquer ônus para operacionalização da solução além dos descritos nestas especificações;	https://docs.simonops.com/
7.2.2.9. Possuir compatibilidade com protocolo IPV6;	https://docs.simonops.com/simon-zone
7.2.2.10. Utilizar portas específicas para coleta e execução de comandos nos dispositivos conectados à rede;	https://docs.simonops.com/simon-zone#vXeRS
7.2.3. **Disponibilidade**	https://docs.simonops.com/
7.2.3.1. A plataforma ofertada para Gerenciamento, Automação e Orquestração de Operações de TI utilizando AIOPS deverá estar disponível e acessível durante o regime 24x7 durante 365 dias por ano no ambiente da CONTRATANTE.	https://docs.simonops.com/#0dOUR
7.2.3.2. Manutenções e atualizações deverão negociadas previamente e só poderão ser executadas com aprovação da PRODAM, as Infrações a estes itens estão sujeitas as sanções definidas no ANS.	https://docs.simonops.com/#0dOUR
7.2.3.3. Os serviços deverão estar disponíveis, no mínimo, 99,8% (noventa e nove vírgula oito por cento) do tempo contratado. Infrações a estes itens estão sujeitas as sanções definidas no ANS.	https://docs.simonops.com/#0dOUR
7.2.3.4. A aferição do acordo de nível de serviço (SLA) para determinar o nível de disponibilidade da solução deverá ser calculado através da fórmula:	https://docs.simonops.com/slas
7.2.3.5. (Número total de minutos em um mês - Total de minutos de indisponibilidade da solução no mês em questão) / (Número total de minutos em um mês).	https://docs.simonops.com/slas
7.2.3.6. O "Tempo de Indisponibilidade" para aferição do acordo de nível de serviço (SLA) é definido como qualquer período em que qualquer quantidade de usuários não consiga utilizar efetivamente os serviços oferecidos pela CONTRATADA.	https://docs.simonops.com/slas
7.2.3.7. A contabilização do tempo de indisponibilidade deverá ser cumulativa dentro do mês, porém não será cumulativa entre os meses.	https://docs.simonops.com/slas
7.2.3.8. Serão considerados os intervalos de tempo decorridos entre a queda e o restabelecimento do serviço para contabilização do tempo de indisponibilidade, incluindo os tempos de paradas programadas que excederem ao limite estabelecido.	https://docs.simonops.com/slas
7.2.3.9. As interrupções previamente programadas deverão ser negociadas antecipadamente em busca do horário de menor impacto para operação dos serviços. Interrupções dentro do regime horário contratado sem que haja negociação prévia com a CONTRATANTE serão consideradas como INDISPONIBILIDADES. Infrações a estes itens estão sujeitas as sanções definidas no ANS.	https://docs.simonops.com/manutencoes
7.2.3.10. As interrupções previamente programadas pela CONTRATADA deverão ser comunicadas com antecedência mínima de 3 dias úteis.	https://docs.simonops.com/manutencoes
7.2.3.11. Não serão consideradas para fins de contabilização de indisponibilidades, interrupções de acesso aos serviços, cuja causa seja de responsabilidade da PRODAM ou de seus fornecedores terceiros.	https://docs.simonops.com/simon-zone#DA3yu
7.2.3.12. Será considerado como indisponibilidade a interrupção total ou parcial dos serviços que compõem a solução.	https://docs.simonops.com/simon-zone#DA3yu
7.2.3.13. A solução deverá possuir mecanismos que possibilitem, a qualquer tempo, a CONTRATANTE, visualizar o status de disponibilidade dos serviços contratados, incluindo o histórico de interrupções.	https://docs.simonops.com/simon-zone#DA3yu
7.2.4. **Ferramentas e integrações**	https://docs.simonops.com/
7.2.4.1. Compatibilidade com as versões mínimas dos navegadores desktop e móveis:	https://docs.simonops.com/#0dOUR
7.2.4.1.1. Google Chrome;	https://docs.simonops.com/#0dOUR
7.2.4.1.2. Mozilla Firefox Quantum;	https://docs.simonops.com/#0dOUR
7.2.4.1.3. Mozilla Firefox para dispositivos móveis;	https://docs.simonops.com/#0dOUR
7.2.4.1.4. Microsoft Edge;	https://docs.simonops.com/#0dOUR

7.2.4.1.5. Apple Safari;	https://docs.simonops.com/#0dOUR
7.2.4.1.6. Samsung Internet versão 10 para o sistema operacional Android.	https://docs.simonops.com/#0dOUR
7.2.4.2. **Integrações**	https://docs.simonops.com/
7.2.4.2.1. Suportar o protocolo LDAP;	https://docs.simonops.com/integracoes#FLBJo
7.2.4.2.2. A solução deverá ser capaz de se integrar com a solução de gerenciamento de serviços (ITSM – *IT Service Management*) visando:	https://docs.simonops.com/integracoes#PzzHx
7.2.4.2.2.1. A integração com os processos de ITSM provendo uma visão holística da operação dos serviços e dos processos de gerenciamento dos serviços de TI;	https://docs.simonops.com/integracoes#PzzHx
7.2.4.2.2.2. Integração com soluções de autosserviço e de automações de processos de negócio. Exemplo: Integração com o Portal de Serviços de TI da solução de ITSM e outras plataformas da CONTRATANTE permitindo a automação de serviços “end-to-end”;	https://docs.simonops.com/integracoes#PzzHx
7.2.4.2.3. A solução deverá ter recursos de construção de interfaces e formulários de entrada e saída de dados, permitindo a integração com outras soluções utilizadas pela CONTRATANTE.	https://docs.simonops.com/integracoes
7.2.4.2.4. A solução deverá suportar a integração com os sistemas de e- mail da CONTRATANTE.	https://docs.simonops.com/integracoes#hCg4B
7.2.4.2.5. A solução deverá permitir a integração de sistemas de terceiros e recursos de migração de dados tais como webservices, JDBC, LDAP, Excel, CSV, e-mail;	https://docs.simonops.com/integracoes#hCg4B
7.2.4.2.6. A solução também deve usar tecnologias padrão da indústria, como SOAP, REST, JSON ou WSDL.	https://docs.simonops.com/integracoes#dPMGC
7.2.4.2.7. Deve possuir integração com sistemas de monitoramento padrão de mercado, incluindo ferramentas Open Source para a medição da disponibilidade e abertura automática de tickets;	https://docs.simonops.com/integracoes#LRnPg
7.2.4.2.8. Deve ser capaz de analisar e correlacionar diversos de sensores, eventos e processos distintos, dos sistemas de monitoramento e de segurança do ambiente do cliente na qual listamos alguns, mas não limitando a:	https://docs.simonops.com/integracoes#LRnPg
7.2.4.2.8.1. Zabbix, Nagios, CA OpsCenter, Splunk, CloudWatch, AppDynamics, SolarWinds, Sensu, PingDom, DataDog, New Relic, OpsView, Slack, Twilio, Centreon.	https://docs.simonops.com/integracoes#LRnPg
7.2.4.2.9. Deve permitir que os eventos correlacionados sejam automaticamente direcionados às filhas solucionadoras de cara área da infraestrutura de TI provendo informações de possíveis causas raiz, das áreas afetadas e o tempo de vida do evento apontando as alterações de status dos eventos ocorridas por período.	https://docs.simonops.com/incidentes
7.2.4.2.10. Apresentar flexibilidade na personalização e integração de interfaces, fluxos de trabalho e ações de automação;	https://docs.simonops.com/pipes-e-automacao
7.2.4.2.11. A solução deve possuir controles para assegurar a proteção contra as seguintes vulnerabilidades: Injeção de código, Quebra de autenticação e Gerenciamento de Sessão, Cross-Site Scripting (XSS), Referência Insegura e Direta a Objetos, Configuração Incorreta de Segurança, Exposição de Dados Sensíveis, Falta de Função para Controle do Nível de Acesso, Cross-Site Request Forgery (CSRF), Utilização de Componentes Vulneráveis Conhecidos, Redirecionamentos e Encaminhamentos Inválidos.	https://docs.simonops.com/simon-zone#4yTtO
7.2.5. **Data Analytics / Relatórios / Dashboards**	https://docs.simonops.com/
7.2.5.1. A solução deverá oferecer recursos de análise de informações para elaboração de relatórios, indicadores e painéis de controle para gerenciamento do processo e de data analytics, contemplando os seguintes requisitos:	https://docs.simonops.com/dashboards
7.2.5.2. Dashboards e conteúdos prontos para uso;	https://docs.simonops.com/dashboards
7.2.5.3. Análises de tendências, comportamentos e gargalos a partir da massa de dados da plataforma;	https://docs.simonops.com/hosts#IL9cU
7.2.5.4. Disponibilizar métricas padrões para os processos implementados nos módulos;	https://docs.simonops.com/hosts#g0nNu
7.2.5.5. Execução com dados em tempo real;	https://docs.simonops.com/hosts#g0nNu
7.2.5.6. Gestão de perfis de acesso a funcionalidades e dados;	https://docs.simonops.com/real-user-monitoring#8Eu-f
7.2.5.7. O sistema deverá ter visualização gráfica dos dados para dar suporte a decisão gerencial;	https://docs.simonops.com/paineis-dashboards
7.2.5.8. Permitir a criação de dashboards dinâmicos de forma simples (drag & drop);	https://docs.simonops.com/paineis-dashboards
7.2.5.9. Permitir a exportação dos relatórios para os formatos PDF;	https://docs.simonops.com/paineis-dashboards
7.2.5.10. Permitir agendar o tempo de atualização dos dashboards;	https://docs.simonops.com/paineis-dashboards
7.2.5.11. Permitir exportar ou agendar a exportação dos dashboards no formato PDF;	https://docs.simonops.com/paineis-dashboards
7.2.5.12. Permitir o drill down dos dados dos itens de configuração;	https://docs.simonops.com/paineis-dashboards
7.2.5.13. Permitir projetar tendências;	https://docs.simonops.com/hosts#IL9cU
7.2.5.14. Permitir que o agendamento envie os relatórios gerados por e-mail, FTP e servidor de arquivos;	https://docs.simonops.com/compartilhamento-automatico
7.2.5.15. Permitir que o usuário crie relatórios ou atalhos para relatórios pré- existentes nas pastas as quais tem acesso;	https://docs.simonops.com/paineis-dashboards
7.2.5.16. Permitir que os relatórios sejam enviados por FTP, e-mail, e servidor de arquivos durante a sua visualização;	https://docs.simonops.com/agendamentos
7.2.5.17. Permitir controle aos relatórios conforme perfis disponibilizados na solução;	https://docs.simonops.com/times
7.2.5.18. Possuir integração com dashboards de ferramentas de terceiros;	https://docs.simonops.com/paineis-dashboards
7.2.5.19. Possuir a capacidade de customização de dashboards gerenciais e técnicos e a funcionalidade de navegação drill-down nos dashboards;	https://docs.simonops.com/paineis-dashboards
7.2.5.20. Apresentar o estado atualizado dos itens monitorados, em tempo real, sem a necessidade de realizar atualizações manuais de telas (refresh);	https://docs.simonops.com/paineis-dashboards
7.2.5.21. Possibilitar a visualização dos dados de monitoramento de performance, históricos e tempo real, permitindo a seleção de um determinado ponto na linha do tempo, possibilitando a identificação do momento exato no qual um determinado problema ou comportamento anormal se iniciou;	https://docs.simonops.com/paineis-dashboards
7.2.5.22. Prover layouts pré-definidos com gráficos, calendários, grids e pivot tables;	https://docs.simonops.com/paineis-dashboards
7.2.5.23. Prover visão da central de serviços em tempo real;	https://docs.simonops.com/paineis-dashboards
7.2.5.24. Suportar representação matemática de gráficos;	https://docs.simonops.com/paineis-dashboards
7.2.5.25. Sem limites para análises históricas;	https://docs.simonops.com/paineis-dashboards

	7.2.5.26. Suportar a criação de filtros e agrupamentos nos dashboards;	https://docs.simonops.com/paineis-dashboards
	7.2.5.27. Suportar a customização do portal de relatórios, por usuário;	https://docs.simonops.com/paineis-dashboards
	7.2.5.28. Suportar a definição de indicadores-chave de desempenho (KPIs);	https://docs.simonops.com/paineis-dashboards
	7.2.5.29. Permitir a construção de relatórios e painéis de informação, sem nenhuma limitação de quantidades e funcionalidades, e sem necessitar de outros sistemas ou aplicativos externos ou auxiliares;	https://docs.simonops.com/paineis-dashboards
	7.2.5.30. Prover funcionalidades de análise de dados, viabilizando a análise de informações preexistentes e oferecendo alertas e soluções para possíveis problemas futuros (Data Analytics).	https://docs.simonops.com/hosts#IL9cU
	7.2.5.31. Disponibilizar dashboards para Performance Analytics, com métricas defaults e customizáveis	https://docs.simonops.com/paineis-dashboards
	7.2.5.32. Disponibilizar dashboard para Gerenciamento de Eventos contendo, no mínimo:	https://docs.simonops.com/eventos-e-incidentes
	7.2.5.33. Capacidade de aplicar filtros por área de evento monitorado. Tais como: banco de dados, redes de dados, virtualização, storage, servidores, segurança, aplicações, entre outros.	https://docs.simonops.com/eventos-e-incidentes
	7.2.5.34. Implementação de filtro por período contendo, no mínimo, os últimos 7 dias de eventos, os últimos 30 dias e campo personalizado de período do evento conforme necessidade dos usuários.	https://docs.simonops.com/eventos-e-incidentes
	7.2.5.35. Deverá apresentar gráficos gerenciais conforme período selecionado, mostrando as informações através de gráficos circulares e de barras, sendo que no modelo circular deverá ser mostrado os dados de eventos críticos e Avisos (Warning). No modelo em barras deverá ser apresentado por dia o volume de eventos por tipo de tratativa: Críticos, Avisos, Resolvidos e Volume Total.	https://docs.simonops.com/eventos-e-incidentes
	7.2.5.36. Visão centralizada dos eventos conforme período selecionado indicando através de gráficos: o total de eventos no período, o total de eventos atrasados e o total dos eventos concluídos dentro do acordo de nível de serviços definido pela CONTRATANTE.	https://docs.simonops.com/visao-geral
	7.2.5.37. Os eventos devem ser classificados por tipo de severidade utilizando uma escala de cor por prioridade (vermelho - crítico, amarelo - alerta, verde - ok e cinza – manutenção programa e preto – serviço desabilitado).	https://docs.simonops.com/visao-geral
	7.2.5.38. Deverá apresentar visão centralizada dos eventos por cada área de infraestrutura ou por equipe relacionado ao evento monitorado:	https://docs.simonops.com/visao-geral
	7.2.5.39. Cada evento deverá ser categorizado e agrupado por cada tipo de tópico e por host apresentando, no mínimo, as informações de: status do evento, severidade, causa raiz e timeline do evento.	https://docs.simonops.com/eventos-e-incidentes
	7.2.5.40. Caso um mesmo evento ocorra no período de 24 (vinte e quatro) horas do último evento correlacionado deverá ser agrupado como um mesmo evento baseando-se no conceito de problemas do modelo ITIL v3, onde um ou mais incidente ou evento correlacionados cuja causa é desconhecida podem se tornar um problema.	https://docs.simonops.com/correlacao-de-eventos
	7.2.5.41. A correlação de eventos em cada ambiente deve possibilitar a separação dos eventos por status de tratativa: ativos, encaminhados, suspensos e concluídos.	https://docs.simonops.com/correlacao-de-eventos
	7.2.5.42. Possibilitar a criação de novos dashboards gerenciais utilizando plataforma web e sem a necessidade de desenvolvimento utilizando de código fonte.	https://docs.simonops.com/paineis-dashboards
	7.2.5.43. Deve possibilitar a visibilidade dos eventos por tipo de ferramenta de monitoração do ambiente de TI.	https://docs.simonops.com/eventos-e-incidentes
	7.2.5.44. Deve permitir a atualização automática dos dados gerenciais por tempo pré-definido pelo sistema de 5 em 5 minutos e de modo manual por cada usuário da plataforma possibilitando atualizações por período configurados de minuto em minuto.	https://docs.simonops.com/paineis-dashboards
	7.2.6. **Acessibilidade**	https://docs.simonops.com/
	7.2.6.1. Permitir mais de um servidor de Interface WEB comunicando com o mesmo banco de dados, provendo balanceamento de carga e alta-disponibilidade;	https://docs.simonops.com/requisitos-de-software#7slG-
	7.2.6.2. Deverá possibilitar aos usuários a customização das interfaces através de funcionalidades de “arrasta e solta” das telas dos dashboards gerenciais pré-definidos ou criados por cada usuário.	https://docs.simonops.com/requisitos-de-software#7slG-
	7.2.7. **Segurança**	https://docs.simonops.com/
	7.2.7.1. A solução deverá ser capaz de trafegar dados da rede corporativa interna utilizando protocolo HTTPS (HTTP com criptografia e identificação segura);	https://docs.simonops.com/simon-zone#EJ40y
	7.2.7.2. Permitir autenticação corporativa via SAML 2.0;	https://docs.simonops.com/integracoes#FLBJo
	7.2.7.3. A solução deverá realizar a autenticação de usuários de forma centralizada, utilizando uma das seguintes tecnologias: Protocolo LDAP ou Microsoft Active Directory;	https://docs.simonops.com/integracoes#FLBJo
	7.2.7.4. A solução deverá permitir a implementação e utilização de certificados digitais;	https://docs.simonops.com/simon-zone
	7.2.7.5. A solução deverá prover comunicação criptografada. Deve ser utilizada criptografia com padrões TLSv1.2, com chave de 128 bits ou superiores para qualquer transmissão de informações. Estes padrões devem suportar [SHA-256 com RSA] ou superior;	https://docs.simonops.com/simon-zone#4yTtO
	7.2.7.6. Disponibilizar rotina automática de backup gerando arquivos da base de dados e configurações;	https://docs.simonops.com/simon-zone
	7.2.7.7. Possibilidade de criação de perfis de usuário para acesso as funcionalidades e dados da solução (Administrador, Operador, Consulta, etc);	https://docs.simonops.com/usuarios
	7.2.7.8. A solução deve suportar a leitura recursiva de grupos (grupos como membros de grupos) no processo de autorização;	https://docs.simonops.com/permissoes-por-roles
	7.2.7.9. Permitir criação de trilhas de auditoria para rastreabilidade de informações de usuários, eventos do sistema, alterações de dados e configurações;	https://docs.simonops.com/simon-zone
	7.2.7.10. Periodicamente, identificar, corrigir e comunicar as vulnerabilidades à CONTRATANTE de acordo com sua criticidade;	https://docs.simonops.com/#0dOUR
	7.2.7.11. A solução deve possuir controles para assegurar a proteção contra as seguintes vulnerabilidades: Injeção de código, Quebra de autenticação e Gerenciamento de Sessão, Cross-Site Scripting (XSS), Referência Insegura e Direta a Objetos, Configuração Incorreta de Segurança, Exposição de Dados Sensíveis, Falta de Função para Controle do Nível de Acesso, Cross-Site Request Forgery (CSRF), Utilização de Componentes Vulneráveis Conhecidos, Redirecionamentos e Encaminhamentos Inválidos.	https://docs.simonops.com/lgpd