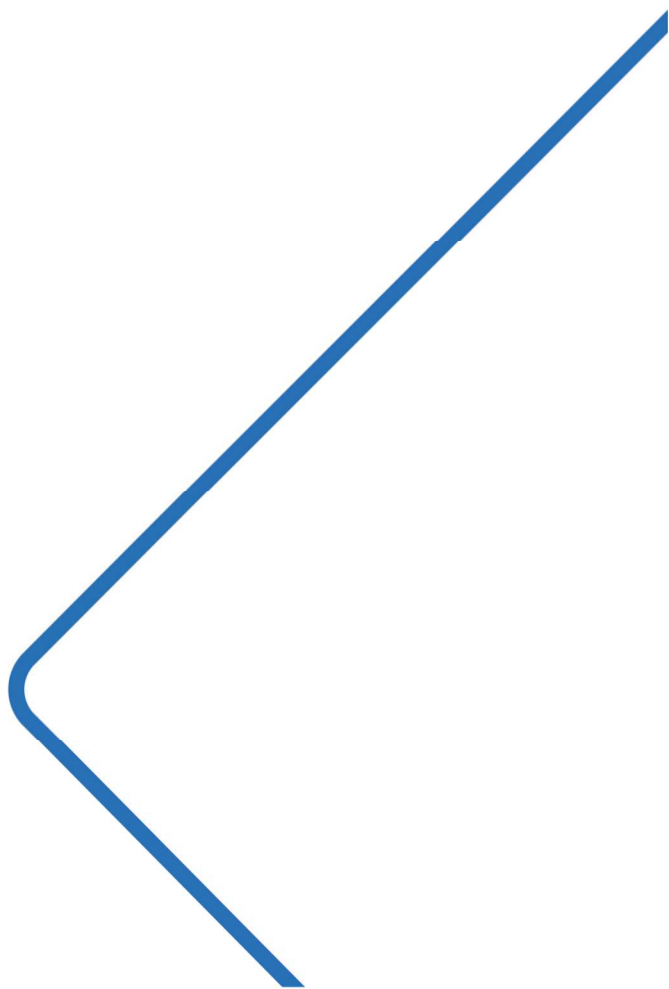
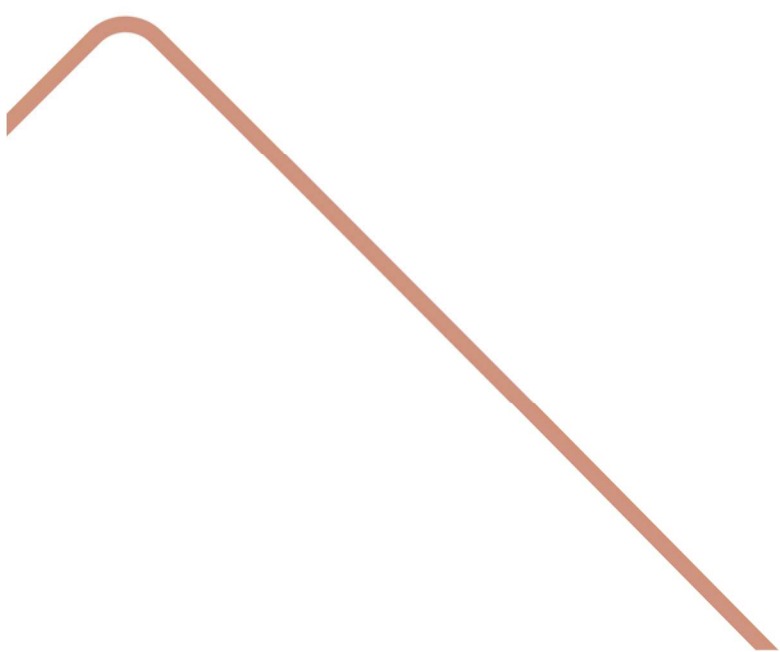


## ESPECIFICAÇÃO TÉCNICA



## ESPECIFICAÇÃO TÉCNICA

### 1. OBJETO

Contratação de empresa especializada, em lote único, para fornecimento de Solução integrada de Gerenciamento de Tecnologia da Informação (TI), incluindo ferramentas **Information Technology Service Management (ITSM)**, **Configuration Management Database (CMDB)**, **Information Technology Asset Management (ITAM)**, **Information Technology Operations Management (ITOM)**, e **Gerenciamento de Capacidade**, instalação, migração, configuração, parametrização, atualização, operação assistida, transferência de conhecimento técnico e suporte técnico, pelo período de 36 (trinta e seis) meses, conforme especificações descritas neste documento.

Uma solução integrada de Tecnologia da Informação é uma solução tecnológica que reúne diferentes ferramentas que se comunicam com o objetivo de otimizar processos, simplificar gestão e melhorar tomadas de decisões. Para isso, é necessário integrar todas as ferramentas de gerenciamento de TI que fazem parte desta contratação, incluindo as ferramentas já existentes na Prodeb, usando um único CMDB totalmente integrado na solução.

### 2. JUSTIFICATIVA DA CONTRATAÇÃO

A PRODEB possui o propósito de assegurar ao Governo do Estado o domínio na aplicação de soluções de Tecnologia da Informação e Comunicação. Para tanto, possui um grande datacenter, com cerca de 3000 servidores, que suportam operações críticas de negócios dos Órgãos e Entidades da Administração Pública Estadual.

Em decorrência de suas atribuições institucionais, a PRODEB busca alinhar sua estrutura, processos e atividades às melhores práticas, frameworks e modelos adotados pelo mercado e que melhor se aderem às necessidades do propósito da instituição. Desta forma, implantou vários de seus processos à luz do ITIL (Information Technology Infrastructure Library), promovendo maior eficiência e transparência aos serviços prestados pela instituição, como também realizar uma melhor gestão e continuidade dos serviços de TI.

Para garantir a disponibilidade, desempenho e segurança dos sistemas e serviços disponibilizados, torna-se necessária a contratação de uma solução integrada de gerenciamento de incidentes, problemas, mudanças, ativos e configurações de TI, bem como monitoramento contínuo. Essa solução deve integrar as melhores funcionalidades das soluções de ITSM, CMDB, ITAM e Monitoramento para garantir uma gestão eficiente e eficaz.

As ferramentas supracitadas são referentes a áreas distintas de gerenciamento de TI, devendo ser integradas a fim de fornecer uma visão completa e precisa do ambiente de TI da Prodeb. A integração dessas ferramentas é imprescindível no aprimoramento da eficiência e eficácia do gerenciamento de TI.

Cabe ressaltar que a ferramenta de CMDB deve ser usado para armazenar informações dos ativos de TI da Prodeb, enquanto a ferramenta de ITAM fará o gerenciamento dos ativos de microinformática ao longo do ciclo de vida. Cabe ao ITOM monitorar e gerenciar o desempenho dos sistemas e aplicativos de TI e ao ITSM gerenciar incidentes e solicitações de serviços.

A integração das ferramentas ITOM, ITAM, ITSM e Gerenciamento de Capacidade permitirá a abertura automática de chamados (Incidentes, Problemas e/ou Solicitações), tornando a operação mais ágil e eficiente.

#### **INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM)**

A implementação de uma ferramenta de ITSM (Information Technology Service Management) é de extrema importância para as organizações atualmente. Com o rápido avanço da tecnologia e a crescente dependência de sistemas e serviços de TI, tornou-se essencial ter uma estrutura eficiente para gerenciar e fornecer suporte aos processos relacionados à tecnologia da informação.

A referida ferramenta fornece uma abordagem estruturada para o gerenciamento de serviços de TI, permitindo a padronização e automatização de processos, promovendo maior eficiência operacional, reduzindo o tempo gasto em tarefas manuais e repetitivas, incluindo a definição de acordos de nível de serviço (SLAs), a priorização de solicitações e a implementação de processos de mudança controlados. Além do exposto, a solução de ITSM fornece uma ampla gama de recursos de relatórios e análises possibilitando informações valiosas sobre o desempenho dos serviços de TI para tomadas de decisão.

### **INFORMATION TECHNOLOGY ASSET MANAGEMENT (ITAM)**

Para garantir o cumprimento dos requisitos de boas práticas de Incidentes de Segurança, é importante contar com uma ferramenta que permita atender diversos requisitos de gerenciamento de dispositivos, tais como, desktops, notebooks, smartphones, tanto no critério hardware, quanto software, restringindo a comunicação quando necessário e aumentando a segurança, caso possua alguma vulnerabilidade a ser corrigida.

A contratação de uma ferramenta de gerenciamento e segurança de ativos de TI proporciona aumentar a segurança, melhorar a gestão de ativos, garantir suporte técnico eficiente, além de cumprir com requisitos de conformidade e auditoria. Essa contratação trará benefícios significativos, proporcionando um ambiente de TI mais seguro, eficiente e controlado.

### **INFORMATION TECHNOLOGY OPERATIONS MANAGEMENT (ITOM)**

A contratação de uma solução de monitoramento possibilitará a monitoração em tempo integral, sendo capaz de apoiar de forma efetiva a orquestração automática da operação dos ativos tecnológicos no ambiente do Data Center da PRODEB.

Atualmente, temos ferramentas de monitoramento que promovem ações reativas, resultando em um modelo de gerenciamento de TI que se concentra em “apagar incêndios”, ou seja, solucionar problemas à medida que eles surgem. A contratação de uma nova solução viabilizará o monitoramento proativo, modelo que se concentra em prevenir os problemas, antes que eles ocorram através da utilização de Inteligência Artificial (IA).

As soluções de ITOM mais recentes incorporam inteligência artificial para aprimorar o monitoramento e o desempenho de aplicativos. Estas ferramentas combinam analítica avançada e IA para, de maneira proativa, identificar problemas emergentes, diagnosticar problemas em diversos ambientes de TI e designar incidentes de forma adequada, entre outros.

O gerenciamento de operações de TI (ITOM) é responsável por gerenciar os requisitos de tecnologia da informação dentro de uma organização, supervisionando o fornecimento, a capacidade, o desempenho e a disponibilidade da infraestrutura e dos recursos de TI, tais como recursos de computação, rede e aplicativo. Seu papel é executar tarefas de rotina que promovam a qualidade, a eficiência e uma experiência positiva do usuário final durante toda a entrega do recurso de TI.

### **GERENCIAMENTO DE CAPACIDADE**

A contratação de uma solução de Gerenciamento de Capacidade possibilitará gerir o planejamento de capacidade futura com base nas análises de desempenho, fornecendo previsões de crescimento, estimativas de recursos necessários e recomendações para dimensionamento adequado dos servidores virtualizados. Este planejamento irá prover alocação eficiente de recursos, garantindo uma distribuição equilibrada e eficiente de CPU, memória, armazenamento e largura de banda entre as máquinas virtuais.

Com o Gerenciamento poderemos obter análise de tendências do ambiente virtualizado, bem como de serviços, onde será possível de analisar tendências de uso ao longo do tempo, permitindo a identificação de padrões sazonais, crescimento gradual ou mudanças repentinas na demanda de recursos.

A solução além de realizar visões de serviço e uso de capacidade computacional, poderá apresentar relatórios e apresentação para suportar a gerência de orçamento e custos de serviços.

### **3. RESULTADOS ESPERADOS**

- 3.1.** Aumentar a capacidade de respostas às dúvidas, solicitações, incidentes, eventos, mudanças, problemas e acessos aos serviços disponibilizados aos usuários.
- 3.2.** Assegurar que sejam efetivas as interfaces (entradas e saídas), processos, subprocessos, papéis, responsabilidades, e indicadores, descritos pelas melhores práticas de mercado.
- 3.3.** Facilitar a restauração da operação normal dos serviços com o mínimo de impacto nos processos de negócios, dentro dos acordos de níveis de serviços e prioridades estabelecidos.
- 3.4.** Gerar relatórios detalhados e gerenciais para identificar possíveis pontos de estrangulamento e problemas de infraestrutura, de modo a reduzir o número de incidentes.
- 3.5.** Comunicar e promover a disseminação adequada de informações para as unidades e áreas afetadas pelos eventos relacionados aos incidentes registrados.
- 3.6.** Manutenção do conhecimento acumulado, atualizando e mantendo Bases de Conhecimento.
- 3.7.** Melhorar a capacidade da organização de atingir os objetivos relacionados às mudanças de TI, maximizar o número de mudanças bem-sucedidas de produtos e serviços, garantindo que os riscos sejam avaliados adequadamente, autorizando mudanças e gerenciando um cronograma das alterações sem obstruir o fluxo, promovendo apenas alterações estáveis que contribuam para a geração de valor.
- 3.8.** Controlar as implantações no âmbito de mover hardware, software, documentação, processos novos ou alterados ou qualquer outro componente para ambientes ativos. Direcionado por políticas internas para a definição do tamanho, escopo, conteúdo e frequência de cada lançamento.
- 3.9.** Estabelecer o gerenciamento das interrupções não planejadas ou redução na qualidade dos serviços com o objetivo de minimizar o impacto negativo dos incidentes, restaurando a operação normal o mais rápido possível. Tendo o apoio de ferramenta que armazene as informações sobre incidentes fornecendo links para itens de configuração (IC) relacionados, registro de problemas e erros conhecidos permitindo uma recuperação rápida.
- 3.10.** Planejar e gerenciar o ciclo de vida completo de todos os ativos de TI, inclui todos os softwares, hardwares, redes, e serviços em nuvem. Assim permitirá a otimização do uso de recursos, facilitará a auditoria de uso das licenças de softwares, cruzará as solicitações de serviço para estabelecer previsões de demandas.
- 3.11.** Na Gestão de Conhecimento deve fornecer uma abordagem estruturada para definir, construir, reutilizar e compartilhar conhecimento, ou seja, informações, habilidades, práticas, soluções e problemas. Permitindo o uso de informações em um determinado contexto de forma adequada para o propósito, proporcionando ao analista encontrar o conteúdo relevante rapidamente.
- 3.12.** Observar sistematicamente os serviços e seus componentes, registrando e relatando mudanças selecionadas de estado identificadas como eventos. Estabelecendo resposta apropriada a esses eventos, incluindo condições que poderiam levar a possíveis falhas ou incidentes, garantindo minimizar ou eliminar seu impacto negativo nos serviços fornecidos.
- 3.13.** Reduzir a probabilidade e o impacto dos incidentes, identificando as causas reais e potenciais dos incidentes e gerenciando soluções alternativas e erros conhecidos. Possibilitar investigação e análise para identificar as causas, desenvolver soluções alternativas e recomendar soluções de longo prazo, reduzindo o número e o impacto de incidentes futuros.
- 3.14.** Disponibilizar para uso serviços e/ou recursos novos e/ou alterados por meio do Gerenciamento de Liberação, integrado às novas tendências como DevOps, permitindo alto desempenho reduzindo o tempo de espera para mudanças e maior frequência de implantações.
- 3.15.** Fornecer uma fonte única de informações consistentes sobre todos os serviços e ofertas de serviços e garantir que estejam disponíveis para o público relevante. O catálogo de serviços deve representar os serviços atualmente disponíveis, garantindo que as descrições dos produtos e serviços sejam expressas claramente para o público-alvo,

a fim de apoiar o envolvimento das partes interessadas e a entrega de serviços.

- 3.16. Garantir que informações precisas e confiáveis sobre a configuração de serviços e os ICs que os suportam estejam disponíveis quando e onde for necessário. Coletar, manter e fornecer informações sobre os ICs que contribuem para cada serviço e seus relacionamentos. Equilibrar o volume das informações necessárias com o valor que as informações criam para o negócio.
- 3.17. Apoiar a qualidade acordada de um serviço, tratando todas as solicitações de serviço predefinidas e iniciadas pelo usuário de uma maneira eficaz e amigável. É por meio da Solicitação de Serviço que um usuário (ou representante autorizado de um usuário) inicia uma ação de serviço que foi acordada como parte normal da entrega do serviço.
- 3.18. Implementar a estratégia omnichannel, que se baseia no uso simultâneo e interligado dos diferentes canais de atendimento/comunicação, aprimorando a experiência do usuário de TI. O usuário poderá iniciar o atendimento por um canal (chatbot, telefone, email, portal web, app mobile) e continuar/concluir o atendimento através de quaisquer outros canais, mantendo, sempre que possível, um número de chamado único independente do canal de atendimento.
- 3.19. Deverá gerar logs de auditoria e logs de registro de atividades diversos, tais como: acesso dos usuários, tentativas de acesso autorizadas e não autorizadas, criações, alterações, exclusões, exceções do sistema e eventos de segurança da informação.
- 3.20. Deverá ser capaz de exportar todos os tipos de log.
- 3.21. Deverá se capaz de integrar todas as ferramentas de gerenciamento de TI que fazem parte desta contratação, incluindo as ferramentas já existentes na Prodeb (por exemplo, Forescout, FortADC, Fort SIEM, Trend Micro Network Security, entre outras)

#### 4. DETALHAMENTO DO OBJETO

ITEM	DESCRIÇÃO / PRODUTO	QUANTIDADE A SER REGISTRADA	UNIDADE SUGERIDA*
4.	INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM), com garantia e atualização por 36 meses.	633	Usuário
	SOLUÇÃO DE INFORMATION TECHNOLOGY ASSET MANAGEMENT (ITAM), com garantia e atualização por 36 meses.	800	Ativos
	SOLUÇÃO DE INFORMATION TECHNOLOGY OPERATIONS MANAGEMENT (ITOM), com garantia e atualização por 36 meses.	4076	Ativos
	SOLUÇÃO DE GERENCIAMENTO DE CAPACIDADE, com garantia e atualização por 36 meses.	4076	Ativos
	Serviço de Instalação com migração de dados e configurações necessárias para as soluções(Evento Único).	1	Unidade
	Consultoria Técnica.	2.000	UST

\* Caso a unidade sugerida não seja a única adota, favor especificar.

#### 4.1. INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM)

4.1.1 Contempla o fornecimento de uma solução ITSM, instalação, migração, configuração, parametrização, atualização, capacitação, transferência de tecnologia e suporte técnico.

4.1.2 O cenário atual da solução ITSM consiste em:

a) Processos ITIL:

- Gerenciamento de Solicitações de Serviço
- Gerenciamento de Incidentes
- Gerenciamento de Mudanças
- Gerenciamento de Configuração
- Gerenciamento de Eventos
- Gerenciamento do Catálogo de Serviços
- Gerenciamento de Capacidade

b) Itens gerenciados conforme as quantidades da tabela a seguir:

QUANTITATIVOS	
Tenants específicos de clientes/serviços	5
Usuários ativos	5223
Analistas ativos	633
Clientes	122
Grupos de atendimento (Analistas)	133
Catálogo (quantidade de Categorias de Serviço)	1257
Catálogo de mudanças (quantidade de categorias)	54
Eventos por mês (média últimos 6 meses)	489
Solicitações e incidentes por mês (média últimos 6 meses)	16704
Mudanças por mês (média últimos 6 meses)	367
CMDB	
ICs	14501
Famílias de ICs	25
Classes de ICs	34

4.1.3 ITENS PARA ELABORAÇÃO DO CATÁLOGO DE SERVIÇOS

a) Os itens estão relacionados no ANEXO III

4.1.4 O conjunto de todos os requisitos, constam no ANEXO I da Especificação Técnica.

#### 4.2. SOLUÇÃO DE INFORMATION TECHNOLOGY ASSET MANAGEMENT (ITAM)

4.2.1 MÓDULO GESTÃO DO CICLO DE VIDA DO ATIVO DE TI

- Contemplar o fornecimento de uma solução de gestão do ciclo de vida dos ativos de TIC, abrangendo desde a aquisição até o descarte dos dispositivos.
- Permitir o controle e o monitoramento de todos os ativos de TIC da empresa CONTRATANTE, incluindo informações de inventário, configurações, atualizações de software, histórico de manutenção, entre outros.
- Oferecer recursos de gestão de garantia, controle de versões, gerenciamento de contratos e políticas de segurança.

4.2.2 MÓDULO DE CONTROLE REMOTO

- Contemplar o fornecer suporte remoto instantâneo e confiável a usuários finais e clientes dentro e fora

de sua rede suporte remoto instantâneo e confiável a usuários finais e clientes dentro e fora de sua rede software de controle remoto que permita aos técnicos de TI acessarem e controlarem remotamente os dispositivos da empresa CONTRATANTE.

- O software deve ser seguro, confiável e fornecer recursos de compartilhamento de tela, transferência de arquivos e controle total dos dispositivos.
- Deve ser compatível com os principais sistemas operacionais e dispositivos utilizados pela empresa CONTRATANTE.

#### 4.2.3 QUADRO INFORMAÇÕES DA SOLUÇÃO DE GESTÃO DE ENDPOINT

EQUIPAMENTO	QUANTIDADE
<b>Gestão do Ciclo de Vida do Ativo de TIC</b>	
<b>Desktop</b>	551
<b>Notebook</b>	145
<b>Software</b>	A confirmar
<b>Monitor</b>	+ 551
<b>Dispositivos reservas</b>	100
<b>Controle Remoto</b>	
<b>Software de Controle Remoto</b>	8 postos de trabalho

#### 4.2.4 ITENS PARA ELABORAÇÃO DO CATÁLOGO DE SERVIÇOS

- a) Os itens estão relacionados no ANEXO III

4.2.5 O conjunto de todos os requisitos, constam no ANEXO I da Especificação Técnica.

### 4.3. SOLUÇÃO DE INFORMATION TECHNOLOGY OPERATIONS MANAGEMENT (ITOM)

4.3.1 Contemplar o fornecimento de Instalação, migração, configuração, parametrização, atualização, capacitação, transferência de tecnologia e suporte técnico das seguintes soluções:

Devendo ser configurado inicialmente:

- Processos Itil
- Gerenciamento de Eventos e Alertas

ESTIMATIVA MONITORAMENTO		
<b>Equipamentos Redes</b>	570	
<b>Servidores</b>	2750	
<b>Banco</b>	121	
<b>Storage</b>	5	
<b>URL</b>	630	
<b>Total estimado</b>	4076	

#### 4.3.2 ITENS PARA ELABORAÇÃO DO CATÁLOGO DE SERVIÇOS

- a) Os itens estão relacionados no ANEXO III

4.3.3 O conjunto de todos os requisitos, constam no ANEXO I da Especificação Técnica.

### 4.4. SOLUÇÃO DE GERENCIAMENTO DE CAPACIDADE

#### 4.4.1 Ativos para Monitoramento

ESTIMATIVA DE ATIVOS		
Equipamentos Redes	570	
Servidores	2750	
Banco	121	
Storage	5	
URL	630	
<b>Total estimado</b>	<b>4076</b>	

#### 4.4.2 ITENS PARA ELABORAÇÃO DO CATÁLOGO DE SERVIÇOS

- a) Os itens estão relacionados no ANEXO III

4.4.3 O conjunto de todos os requisitos, constam no ANEXO I da Especificação Técnica.

### 5. ENTREGA DO OBJETO

5.1. Os componentes de software que integram a solução definida no ANEXO I – ESPECIFICAÇÃO TÉCNICA, deverão ser disponibilizados ao Gestor do contrato, no prazo máximo de 10 (dez) dias úteis, a contar do dia seguinte à assinatura do Contrato, no endereço a seguir por meio de:

5.1.1. Data Center PRODEB.

5.1.2. Após disponibilizar A SOLUÇÃO IMPLANTADA, a CONTRATADA deverá notificar formalmente ao Gestor do contrato.

5.1.3. Junto aos produtos fornecidos, a CONTRATADA deverá entregar ao Gestor do contrato, as documentações descritas abaixo:

a) Documentação de Registro de Entrega / Nota Fiscal;

b) Documentação relacionando os itens discriminados na documentação de Registro de Entrega / Nota Fiscal com os produtos de que compõem a solução e estão descritos na proposta técnica comercial validada pela PRODEB, de forma que seja possível verificar a correlação entre os itens que compõem as Soluções e demais módulos da solução, conforme definido no ANEXO I – ESPECIFICAÇÃO TÉCNICA, e aqueles representados na documentação de Registro de Entrega / Nota Fiscal. Esta correlação não poderá ser feita por códigos e sim pela descrição de cada solução com a respectiva quantidade;

c) Documentação técnica, original do fabricante, em língua portuguesa, que abranja configuração, instalação e gerenciamento dos produtos adquiridos;

5.1.4. A PRODEB validará os produtos recebidos em até 05 (cinco) dias úteis, contados a partir do recebimento da formalização de entrega dos itens pela CONTRATADA. Constatada a ocorrência de divergência entre os componentes entregues e o descrito na documentação das alíneas “a”, “b” e “c” do subitem 5.1.3, fica a CONTRATADA obrigada a providenciar a sua correção ou sua substituição, a critério da PRODEB. Os produtos não serão considerados entregues até que todas as pendências sejam sanadas.

### 6. SERVIÇO DE INSTALAÇÃO

6.1. A CONTRATADA deverá realizar a instalação “assistida” de toda a solução, incluindo sua configuração, que será acompanhada por analistas da PRODEB. Todo processo de instalação deverá atender ao especificado no Plano de Instalação a ser apresentado e aprovado pela PRODEB, conforme descrito no subitem 6.2 desta Especificação Técnica.

- 6.2. O prazo para conclusão da instalação das soluções será de 30 (trinta) dias úteis, contados a partir do dia seguinte à ocorrência dos fatos abaixo:
- Aprovação da versão definitiva do Plano de Instalação;
  - Emissão do Termo de Recebimento;
  - Elaboração da Documentação de Implantação;
- 6.3. A CONTRATADA deverá providenciar a aplicação de todas as correções e atualizações da solução liberadas até a data da instalação, salvo solicitação da PRODEB por outra versão. A CONTRATADA deverá encaminhar documento, em meio eletrônico, que comprove a aplicação das atualizações em todos os produtos instalados.
- 6.4. A CONTRATADA deverá considerar para a migração de dados as informações contidas desta Especificação Técnica, conforme o item 4 desta Especificação Técnica;
- 6.5. É de responsabilidade da CONTRATADA toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação aqui mencionados.
- 6.6. Concluídas a instalação, migração e a configuração dos produtos adquiridos, a CONTRATADA deverá comunicar formalmente à PRODEB sobre a conclusão dos serviços. A PRODEB terá o prazo de até 05 (cinco) dias úteis para verificar a conformidade da instalação, migração e das configurações realizadas com as condições constantes desta Especificação Técnica.
- 6.7. Caso sejam constatadas anormalidades ou sejam detectados problemas durante a verificação de conformidade realizada pela PRODEB, esta comunicará formalmente os problemas detectados e que a instalação não foi concluída. A CONTRATADA terá um novo prazo de 5 (cinco) dias úteis, contados a partir do dia seguinte à confirmação de recebimento da comunicação, para sanar os problemas/anormalidades detectados, sem prejuízo do prazo descrito no anexo I desta Especificação Técnica, sujeitando-se a CONTRATADA às penalidades previstas.
- 6.8. Os serviços de instalação, configuração e migração deverão ocorrer em dias úteis, no horário compreendido entre 9:00h e 17:00h, salvo definição contrária, realizada em comum acordo entre a PRODEB e a CONTRATADA e deverão ser agendados previamente com a PRODEB.
- 6.9. Caso o fornecedor opte pelo fornecimento na modalidade *ON Premise*, será de responsabilidade da PRODEB a disponibilização de ambientes físicos, acesso a redes e servidores, configurações de segurança, acessos ao ambiente legado e demais informações sobre configurações e condições que possibilitem a CONTRATADA realizar a instalação com migração de dados de conhecimento e configuração, respeitando as normas e restrições de segurança estabelecidas na PRODEB;
- 6.10. Os produtos adquiridos serão considerados instalados e o Termo de Aceite será emitido pela PRODEB em até 10 (dez) dias úteis, contados a partir da ocorrência dos fatos a seguir:
- a) As atualizações serem aplicadas e a documentação comprobatória ser entregue à prodeb pela CONTRATADA, conforme descrito no anexo I desta Especificação Técnica.
  - b) A PRODEB receber o comunicado da CONTRATADA informando a conclusão dos serviços de instalação, migração e configuração, conforme descrito no anexo I desta Especificação Técnica.
  - c) A PRODEB concluir a verificação da conformidade da instalação, migração e das configurações realizadas com as condições constantes desta Especificação Técnica e que não existem anormalidades ou foram sanados todos os problemas detectados.

## **7. CONSULTORIA TÉCNICA**

- 7.1. As atividades de consultoria técnica objetivam otimizar a utilização dos produtos adquiridos e o desenvolvimento ou aperfeiçoamento de competências e melhorias nas soluções, por meio do repasse de conhecimento de forma ordenada, esta consultoria tem como escopo itens que não fazem parte dos catálogos de serviços que estão descritos no Anexo III, e seu escopo compreende:

- Apoiar as equipes da PRODEB a definir a melhor metodologia para o uso adequado da solução;
  - Apoiar as equipes de desenvolvimento na exploração de recursos avançados da solução;
  - Apoiar as equipes de infraestrutura na investigação e resolução de incidentes e problemas no ambiente da solução;
  - Diagnóstico / orientação quanto à análise do desempenho da solução;
  - Diagnóstico / orientação quanto à customização e execução de melhorias da solução;
  - Auxiliar no levantamento e análise de processos e integrações;
  - Auxiliar na definição de métricas e indicadores dos processos de negócio;
  - Auxiliar na documentação de metodologia de uso da solução
  - Planejamento e apoio em integrações com outras soluções em uso na PRODEB;
  - Auxiliar e implementar melhorias proposta pela PRODEB em todo o ambiente da solução;
- 7.2. As atividades de consultoria técnica serão realizadas de forma presencial ou remota em comum acordo entre a PRODEB e CONTRATADA, a partir da assinatura do Contrato durante toda a vigência contratual. A critério da PRODEB, as atividades poderão ser realizadas nas dependências da CONTRATADA.
- 7.3. Estas atividades devem ter produtos definidos (planos, procedimentos, laudos, pareceres técnicos, guias, padrões, etc), escopo, prazo de entrega e as respectivas UST alocadas para a execução, previamente aprovadas pela PRODEB, para fins de contabilização e posterior faturamento. Estas informações devem estar devidamente registradas nas respectivas Ordens de Serviço, autorizadas pelo Gestor do contrato.
- 7.4. A CONTRATADA deverá disponibilizar 2.000 (duas mil) UST de consultoria técnica, a serem realizadas por profissionais especializados na solução fornecida. Essas UST serão utilizadas, sob demanda, de acordo com as necessidades da PRODEB.
- 7.5. O serviço de consultoria técnica deverá ser executado por profissionais que comprovem qualificação para atuar na solução que será objeto da contratação, através de certificado de participação e conclusão em curso oficial do Fabricante, com o mínimo de 1 ano comprovado de atuação com a mesma solução.
- 7.6. Os serviços de Consultoria Técnica serão prestados em conformidade com as Ordens de Serviços (OS) a serem emitidas para sua execução, conforme modelo constante no ANEXO II – MODELO DE ORDEM DE SERVIÇO. As Ordens de Serviço deverão ser executadas de acordo com planejamento realizado pela equipe da PRODEB em conjunto com a equipe da CONTRATADA, obedecendo cronograma estabelecido.
- 7.7. A CONTRATADA deverá disponibilizar os seguintes canais de atendimento para abertura das Ordens de Serviço:
- Website e telefone (preferencialmente, 0800).
- 7.8. Cada solicitação de consultoria técnica deverá conter, no mínimo, o registro das informações abaixo:
- Número do chamado (na abertura da OS; a ser fornecido pela CONTRATADA);
  - Número da Ordem de Serviço (a ser fornecido pela PRODEB);
  - Identificação do atendente;
  - Identificação do solicitante;
  - Data e hora da solicitação;
  - Descrição da demanda.
- 7.9. As informações sobre os canais de atendimento para abertura das Ordens de Serviço deverão ser apresentadas à

PRODEB no prazo máximo de 10 (dez) dias, contados a partir do dia seguinte à assinatura do Contrato.

- 7.10. As solicitações de serviço deverão ser retornadas no prazo máximo de 4 (quatro) horas após o seu respectivo registro, entendido este retorno como um contato inicial para fins de definição do escopo e forma de tratamento da demanda apresentada. Neste retorno, deverá ser agendada uma reunião presencial ou uma audioconferência para definição do número de horas necessárias e cronograma de execução da respectiva Ordem de Serviço.
- 7.11. A CONTRATADA terá o prazo máximo de 3 (três) dias, contados a partir do dia seguinte ao registro da solicitação de abertura da Ordens de Serviço (OS) pela PRODEB, para se reunir com o solicitante, presencialmente ou por meio de audioconferência, com a finalidade de definir o escopo e a forma de tratamento da demanda apresentada. Nesta reunião a CONTRATADA obterá os insumos necessários para realizar a definição do número de horas e do cronograma de execução da respectiva Ordem de Serviço (OS). A data da reunião deverá ser agendada em comum acordo com a PRODEB.
- 7.12. A CONTRATADA terá o prazo máximo de 3 (três) dias, contados a partir do dia seguinte à realização da reunião descrita no subitem 7.10 para encaminhar ao solicitante, por meio eletrônico, o número de horas e o cronograma de execução da respectiva Ordem de Serviço (OS). Após alinhamentos entre a CONTRATADA e a PRODEB, possíveis negociações e aprovação do número final de horas e cronograma de execução da respectiva Ordem de Serviço (OS), a PRODEB emitirá o documento de abertura da Ordem de Serviço (OS), que deverá ser assinado por responsáveis da CONTRATADA e pelo gestor técnico da PRODEB.
- 7.13. Todas as funções e atividades desempenhadas pela CONTRATADA deverão ter como preocupação primária a transferência do conhecimento à equipe técnica da PRODEB designada a acompanhar cada atividade. Caso a PRODEB entenda ser necessário, poderá solicitar, mediante Ordem de Serviço específica, a realização de workshops, que não se caracterizam como capacitação, mas como apresentação e debate sobre as atividades planejadas ou executadas abrangendo tópicos específicos da tecnologia envolvida.
- 7.14. Entende-se por transferência de conhecimento, a passagem de conhecimento para os técnicos da PRODEB, de todas as atividades desenvolvidas, relativas a cada Ordem de Serviço executada, visando aprimorar os conhecimentos da tecnologia utilizada e maximizar a utilização das funcionalidades.
- 7.15. Os registros de solicitação de serviços poderão ser realizados em horário comercial (9:00 às 17:00 horas), de segunda a sexta-feira, excluídos os feriados nacionais.
- 7.16. Os serviços solicitados serão realizados em horário comercial (8:00 às 17:30 horas), de segunda a sexta-feira, excluídos os feriados nacionais, salvo definição contrária, realizada em comum acordo entre a PRODEB e a CONTRATADA.
- 7.17. Concluída a realização dos serviços solicitados na OS (Ordem de Serviço), a CONTRATADA deverá comunicar este fato formalmente à CONTRATANTE. A PRODEB terá o prazo de 10 (dez) dias, contados a partir da formalização da conclusão, para realizar a avaliação das entregas e validar o consumo de horas, de acordo com:
  - A documentação técnica entregue, conforme padrões previamente acordados entre as partes;
  - O atingimento dos resultados já estipulados;
  - A disponibilização dos entregáveis.
- 7.18. Após a prodeb finalizar a avaliação das entregas e a validação do consumo de horas, atestando que o serviço foi realizado em conformidade com o solicitado, emitirá o documento de aceite da respectiva OS (Ordem de Serviço), que deverá conter as informações relacionadas à sua execução e ser assinado por responsáveis da CONTRATADA e pelo Gestor Técnico da PRODEB.
- 7.19. As Ordens de Serviço aprovadas para execução e formalizadas, não poderão sofrer acréscimos em seu conteúdo previamente negociado sem a anuência do Gestor Técnico.
- 7.20. Em casos excepcionais, as Ordens de Serviço poderão sofrer redução no conteúdo, previamente negociado, desde que a atividade específica ainda não tenha sido iniciada.

## **8. SUPORTE TÉCNICO**

- 8.1. Durante o período de garantia, a CONTRATADA deverá prover o serviço de suporte técnico para os produtos adquiridos, que deverá ser prestado na modalidade presencial e/ou Remoto, conforme descrito no anexo I desta Especificação Técnica.
- 8.2. Entende-se por SUPORTE TÉCNICO REMOTO as seguintes atividades para tratamento de problemas relacionados à solução:
- a) Orientações sobre uso, configuração e instalação dos produtos contratados;
  - b) Questões sobre compatibilidade e interoperabilidade dos produtos adquiridos e integração com outras soluções;
  - c) Interpretação da documentação dos produtos contratados;
  - d) Orientações para identificar a causa de uma falha de software;
  - e) Para os casos de defeitos de software conhecidos, devem ser fornecidas as informações sobre a correção ou a própria correção.
  - f) No caso de defeitos de software não conhecidos, quando a CONTRATADA tiver optado por utilizar centro de suporte e assistência técnica próprio, deverá enviar as informações sobre a falha ao fabricante do produto para que este forneça a solução. A CONTRATADA deverá informar o número do chamado aberto junto ao fabricante, bem como uma estimativa de prazo para solução da falha;
  - g) Orientação para solução de problemas de “performance” e para a execução de melhorias nas configurações dos produtos contratados;
  - h) Orientação quanto às melhores práticas para implementação dos produtos;
  - i) Recuperação de ambientes em caso de panes ou perda de dados (disaster recovery), recuperação de configurações e reinstalação;
  - j) Execução de procedimentos de atualização para novas versões dos produtos de software instalados;
  - k) Reconfiguração da solução em função de alteração/melhoria da arquitetura da infraestrutura.
- 8.3. As atividades relacionadas ao SUPORTE TÉCNICO REMOTO devem ser realizadas por meio de contato telefônico, troca de mensagens eletrônicas e audioconferência por meio de ferramenta homologada pela PRODEB, sendo vedada a utilização de acesso remoto. Caso a CONTRATADA opte por solucionar o problema reportado pela PRODEB por meio de atendimento on site (presencial), isso não deve imputar qualquer ônus adicional à PRODEB. Em caráter excepcional, a área de Segurança da Informação da PRODEB poderá autorizar a utilização de acesso remoto por meio de ferramenta homologada pela PRODEB após avaliar sua necessidade devido a situações emergenciais que representem grande impacto para PRODEB.
- 8.4. O fato de qualquer um dos produtos adquiridos não utilizar a última versão disponibilizada de quaisquer dos softwares instalados originalmente, não poderá ser utilizado pela CONTRATADA como argumento para postergar eventual suporte técnico, a menos que tenha sido objeto de notificação e que seja apresentada documentação correlacionando a falha detectada com a versão de software disponibilizada.

## **9. ACORDO DE NÍVEL DE SERVIÇOS**

- 9.1. Deverão ser considerados os seguintes prazos e níveis de severidade para os chamados de Suporte Técnico.

<b>PRAZOS PARA SOLUÇÃO DAS OCORRÊNCIAS REGISTRADAS (a partir do registro da ocorrência)</b>	
<b>SEVERIDADE INFORMADA</b>	<b>TEMPO PARA SOLUÇÃO</b>
<b>1</b>	<b>4 horas corridas</b>
<b>2</b>	<b>24 horas corridas</b>
<b>3</b>	<b>72 horas corridas</b>
<b>4</b>	<b>48 horas corridas</b>

9.2. Os níveis de severidade são descritos abaixo:

- a) Severidade 1 – quando ocorre a perda ou paralisação de atividades exercidas ou de serviços relevantes prestados pela PRODEB, configurando-se como situação de emergência. Uma solicitação de serviço de Severidade 1 pode possuir uma ou mais das seguintes características:
- Dados corrompidos;
  - Uma função crítica não está disponível;
  - O sistema se desliga repentinamente causando demoras excessivas e intermitências para utilização de recursos;
  - O sistema falha repetidamente após tentativas de reinicialização;
  - O sistema continua em execução permanente (congelado) necessitando ser reiniciado.
- b) Severidade 2 – quando se verifica uma grave perda de funcionalidades em programas ou sistemas da PRODEB, inexistindo alternativas de contorno, sem, no entanto, interromper em sua totalidade a prestação do serviço.
- c) Severidade 3 – quando se verifica uma perda de menor relevância de funcionalidades em programas ou sistemas da PRODEB, causando apenas inconveniências para a devida prestação dos serviços pela PRODEB.
- d) Severidade 4 – quando se verifica como necessária a prestação de informações, aperfeiçoamentos ou esclarecimentos sobre documentação ou funcionalidades de programas, porém sem prejudicar diretamente a operação dos programas ou sistemas da PRODEB.

9.3. O nível de severidade será atribuído pela PRODEB no momento da abertura do chamado.

9.4. No atendimento dos chamados, para efeitos de apuração do tempo gasto pela CONTRATADA para a disponibilização da solução, serão desconsiderados os períodos em que a PRODEB estiver responsável por executar ações necessárias para a análise e solução da ocorrência.

9.5. Considerando que as soluções das ocorrências de software, pela sua natureza, podem envolver atividades relacionadas ao desenvolvimento de patches específicos, admite-se, para todos os casos, a adoção de solução de contorno (workaround), respeitados os prazos definidos para cada severidade informada, sem prejuízo da disponibilização da solução definitiva cabível. Neste caso, a partir do encerramento do chamado original, com a disponibilização da solução de contorno, a CONTRATADA deverá abrir uma nova ocorrência para provimento da solução definitiva imediatamente, na qual deverá constar, obrigatoriamente, um novo campo contendo o número do chamado original (encerrado com a solução de contorno).

9.6. O prazo máximo para disponibilização da solução definitiva será:

<b>PRAZOS PARA SOLUÇÃO DEFINITIVA</b> <b>(a partir do encerramento do chamado original, com a disponibilização da solução de contorno)</b>	
<b>SEVERIDADE INFORMADA</b>	<b>TEMPO PARA SOLUÇÃO</b>
<b>1</b>	<b>15 dias corridos</b>
<b>2</b>	<b>30 dias corridos</b>
<b>3</b>	<b>45 dias corridos</b>

- 9.7. Para fins de cálculo do período decorrido para solução da ocorrência de software, será contabilizado o prazo entre a formalização e o fechamento efetivo da ocorrência – seja essa solução de caráter definitivo ou provisório com a disponibilização de solução de contorno (workaround).
- 9.8. Em caso de impossibilidade da disponibilização de solução de contorno ou definitiva das ocorrências de software, dentro dos prazos estabelecidos, a CONTRATADA deverá, ainda dentro destes prazos, emitir um parecer com previsão de novo prazo, contendo o histórico de maior abrangência possível das atividades desenvolvidas desde a abertura do respectivo chamado.
- 9.9. Após avaliação deste parecer inicial, a PRODEB decidirá sobre a periodicidade da emissão de pareceres ou laudos posteriores, até o fechamento do atendimento, sem prejuízo da aplicação das penalidades previstas pelo descumprimento dos prazos estabelecidos nos subitens 9.1 e 9.5 desta Especificação Técnica.

## **10. DESCONTO POR DESCUMPRIMENTO DE NÍVEL DE SERVIÇO**

- 10.1. Será aplicada multa pelo descumprimento dos prazos relacionados no item 6.2 – Serviço de Instalação/Planejamento desta Especificação Técnica, causado pela CONTRATADA. O descumprimento de cada prazo implicará em uma nova multa, aplicadas cumulativamente conforme o caso.
- 10.2. O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:
- Para atrasos de até 10 (dez) dias corridos → multa de 0,1% (um décimo por cento) ao dia do valor mensal do respectivo Contrato;
  - Para atrasos superiores a 10 (dez) dias corridos → a multa descrita na alínea “a” será substituída por multa de 0,25% (vinte e cinco centésimos por cento) ao dia, até o limite máximo de 5% (cinco por cento) do valor mensal do respectivo Contrato.
- 10.3. Será aplicada multa pelo atraso causado pela CONTRATADA na Entrega, conforme descrito no subitem 5.1 desta Especificação Técnica.
- 10.4. O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:
- Para atrasos de até 15 (quinze) dias corridos → multa de 0,2% (dois décimos por cento) ao dia do valor mensal dos produtos adquiridos;
  - Para atrasos superiores a 15 (quinze) dias corridos → a multa descrita na alínea “a” será substituída por multa de 0,5% (cinco décimos por cento) ao dia, até o limite máximo de 10% (dez por cento) do valor mensal do contrato.
- 10.5. Será aplicada multa pelo atraso causado pela CONTRATADA na Instalação, conforme descrito no subitem 6.2 desta Especificação Técnica. O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:
- Para atrasos de até 10 (dez) dias corridos → multa de 0,2% (dois décimos por cento) ao dia do valor mensal, quanto ao item instalação;
  - Para atrasos superiores a 10 (dez) dias corridos → a multa descrita na alínea “a” será substituída por multa de

0,5% (cinco décimos por cento) ao dia, até o limite máximo de 10% (dez por cento) do valor na fatura mensal, quanto ao item Instalação.

10.6. Caso a CONTRATADA descumpra os prazos descritos nos itens 5 e 6 desta Especificação Técnica, simultaneamente, a multa descrita no subitem 10.5, alíneas “a” e “b”, será substituída por multa de 2% (dois por cento) ao dia, até o limite máximo de 20% (vinte por cento) do valor total do item Instalação, pelo atraso, causado pela CONTRATADA, na instalação dos produtos adquiridos.

a) Para atrasos de até 10 (dez) dias corridos → multa de 0,1% (um décimo por cento) ao dia do valor total dos produtos contratados;

b) Para atrasos superiores a 10 (dez) dias corridos → a multa descrita na alínea “a” será substituída por multa de 0,25% (vinte e cinco centésimos por cento) ao dia, até o limite máximo de 5% (cinco por cento) do valor total dos produtos contratados.

## ANEXO I

### ESPECIFICAÇÕES TÉCNICAS

#### SOLUÇÃO GERENCIAMENTO DE TECNOLOGIA DE INFORMAÇÃO

#### 1.1. REQUISITO OBRIGATÓRIO

1.1.1. As ferramentas devem ser apresentadas em Português (PT-BR)

1.1.2. Informações do ambiente atual:

Itens	Descrição	Unidade	Qtd.
01	<b>Information Technology Service Management (ITSM) - instalação, migração, configuração, parametrização, atualização, capacitação, transferência de tecnologia e suporte técnico das seguintes soluções</b> <b>Deve ser considerado inicialmente:</b>		
	PROCESSOS ITIL •GERENCIAMENTO DE SOLICITAÇÕES DE SERVIÇO •GERENCIAMENTO DE INCIDENTES •GERENCIAMENTO DE MUDANÇAS •GERENCIAMENTO DE CONFIGURAÇÃO •GERENCIAMENTO DE EVENTOS •GERENCIAMENTO DO CATÁLOGO DE SERVIÇOS •GERENCIAMENTO DE CAPACIDADE		
	TENANTS ESPECÍFICOS DE CLIENTES/SERVIÇOS	Unidade	5
	USUÁRIOS ATIVOS	Unidade	5223
	ANALISTAS ATIVOS	Unidade	633
	CLIENTES	Unidade	122
	GRUPOS DE ATENDIMENTO	Unidade	133
	CATÁLOGO (QUANTIDADE DE CATEGORIAS DE SERVIÇO)	Unidade	1257
	Eventos por mês	Média	489
	Solicitações e incidentes por mês		
	Tenant PRODEB	Média	10522
	Demais Tenants	Média	6182
	Solicitações de Mudanças por mês	Média	367
	Possíveis Integrações com ferramentas já existentes na Prodeb: Forescout, FortADC, Fort SIEM, Trend Micro Network Security		
02	<b>Configuration Management Database (CMDB) - instalação, migração, configuração, parametrização, atualização, capacitação, transferência de tecnologia e suporte técnico das seguintes soluções</b> <b>Deve ser considerado inicialmente:</b>		
	ICs	Unidade	14501
	famílias de ICs	Unidade	25
	classes de ICs	Unidade	345
03	<b>Information Technology Operations Management (ITOM) - instalação, migração, configuração, parametrização, atualização, capacitação, transferência de tecnologia e suporte técnico das seguintes soluções</b> <b>Deve ser considerado inicialmente:</b>		
	PROCESSOS ITIL • GERENCIAMENTO DE EVENTOS E ALERTAS		
	Equipamentos Redes	Unidade	570
	SERVIDORES	Unidade	2750
	BANCO DE DADOS	Unidade	121



funcionalidades que atendam todos os requisitos técnicos da contratação, em especial:

- PJM – Project Management - Gerenciamento de Projetos, Portfólio e Demandas.
- SD – Service Desk - Central de Serviço
- REL – Release Management - Gerenciamento de Implantação
- SPM – Service Portfolio Management – Serviço de Gerenciamento de Portfólio

1.1.3.4. Deverá possibilitar transacionar dados com soluções de terceiros através de protocolos compatíveis com padrões abertos indispensavelmente:

- XML (Extensible Markup Language) como definido pelo W3C.
- JSON (Javascript Object Notation) como definido pela IETC.
- Protocolos SOAP e REST.

1.1.3.5. Deverá ser disponibilizado para acesso plataforma WEB, acessadas via navegador compatível com, Microsoft Edge, Brave, Opera, Mozilla Firefox, Google Chrome e/ou Safari.

1.1.3.6. Deverá ser solução responsiva que funcione em diferentes dispositivos, tais como: PC's com sistemas operacionais Windows, Unix, Linux e MacOS, além de Smartphones e tablets com sistemas operacionais IOS e Android.

1.1.3.7. Além das características técnicas e funcionais mínimas, a solução deve possuir o conjunto mínimo de fluxos/módulos/funcionalidades nativo(a)s integradas e de mesmo fabricante desenvolvedor.

1.1.3.8. Será admitida a utilização de ferramentas complementares à solução principal citada no item anterior para implementação/entrega das funcionalidades de gerador de relatórios, conectores para aplicações externas (APM, Jira, Azure Devops, etc.), sistemas de mensageria e telefonia (SMS, WhatsApp, Telegram, Centrais telefônicas, etc.), rotinas e conectores para fontes externas de dados (AD, sistemas de RH, etc.) e mecanismo de inteligência artificial do chatbot, desde que sejam fornecidas pelo mesmo fabricante da plataforma principal ofertada e possam ser integradas a ela.

1.1.3.9. Administração geral e administração segmentada por tenant

1.1.3.10. Administração de usuários e serviços do cliente pelos gestores locais (do cliente)

1.1.3.11. Central de serviços com equipes N1, N2 e N3

1.1.3.12. Processos podem ser disponibilizados por: tenant, serviço, cliente, grupo, função ou tipo de usuário.

1.1.3.13. Possibilitar usuários multi tenant (com atuação em mais de um tenant)

1.1.3.14. Relacionamento entre diferentes tipos de chamados (incidentes, solicitações, eventos, problemas e mudanças)

1.1.3.15. Permitir criação e configuração de novos status e transições de status

1.1.3.16. Filas de atendimento e acompanhamento de chamados configuráveis por: tenant, grupo, perfil, função ou cliente

1.1.3.17. Repositórios de anexo por tenant e cliente

1.1.3.18. Possibilitar realização de inserções, alterações ou exclusões por meio de cargas ou integrações para input de grandes volumes de dados

1.1.3.19. Possibilidade de acesso às aplicações com Single Sign-On

#### **1.1.4. Política de upgrade e atualização**

- 1.1.4.1. As atualizações da solução devem ser realizadas pelo fabricante desenvolvedor.
- 1.1.4.2. As atualizações devem ser feitas em duas fases, sendo a fase 1 uma atualização para os ambientes de Homologação, seguida pela fase 2, em caso de sucesso, replicando no ambiente de Produção.
- 1.1.4.3. Deverá ser capaz de exportar os logs de auditoria com registro de atividades de acesso dos usuários, tentativas de acesso autorizadas e não autorizadas, exceções do sistema e eventos de segurança da informação.
- 1.1.4.4. Deverá disponibilizar os ambientes de homologação e produção.
- 1.1.4.5. A ferramenta deverá permanecer atualizada de acordo com a ultima versão estável do fabricante desenvolvedor.

### **1.2. Information Technology Service Management (ITSM)**

#### **1.2.1. Gerenciamento de configurações**

- 1.2.1.1. O banco de dados de gerenciamento de configuração (CMDB) deve oferecer suporte a vários conjuntos de dados com recursos de federação e reconciliação para obter dados de várias ferramentas de descoberta e por meio do processo de importação manual.
- 1.2.1.2. A federação de fontes de dados externas deve ser possível com a capacidade de armazenar atributos comuns no CMDB e obter outros atributos de fontes de dados externas em tempo real.
- 1.2.1.3. A reconciliação de dados deve ser possível com vários provedores de dados com base em atributos comuns e na capacidade de definir regras de precedência sobre atributos.
- 1.2.1.4. Deve fornecer normalização e reconciliação em nível de atributo para aproveitar os dados existentes de ativos de terceiros ou ferramentas de descoberta para atingir o objetivo de ter uma fonte confiável de dados de configuração.
- 1.2.1.5. Deve ter alguns meios nos quais seja possível rastrear as notificações relacionadas a um elemento.
- 1.2.1.6. Deve permitir visualizar graficamente as relações entre os itens de configuração.
- 1.2.1.7. Deve permitir uma navegação simples e ágil na visualização gráfica das relações entre os componentes.
- 1.2.1.8. Deve oferecer facilidades como zoom in, zoom out, pesquisas, filtros, agrupamentos, etc. dentro do console de navegação da visualização gráfica dos relacionamentos entre os itens de configuração.
- 1.2.1.9. Deve permitir o acesso à visão gráfica das relações entre os itens de configuração, a partir de registros de incidentes, mudanças etc.
- 1.2.1.10. Deve fornecer a facilidade de criar cronogramas de indisponibilidade para um item e indicar o motivo, a data e os dados adicionais.
- 1.2.1.11. Deve permitir armazenar contratos, identificando seus tipos, de forma configurável, como aluguel, suporte, garantia, compra, manutenção etc., bem como sua relação com outros contratos.
- 1.2.1.12. Deve ser possível vincular os contratos entre si para fornecer uma estrutura de contrato principal.
- 1.2.1.13. Deve permitir o envio de notificações em datas próximas às datas de vencimento e revisão dos contratos.

- 1.2.1.14. Deve permitir associar ICs a contratos, tenants e serviços para identificar quais ICs são cobertos por quais contratos, tenants e serviços.
- 1.2.1.15. Deve ter a capacidade de acessar dados federados (acesso a dados em bancos de dados externos sem a necessidade de replicação) de forma que sua visualização seja semelhante aos dados armazenados localmente.
- 1.2.1.16. Deve ter a capacidade de representar as áreas de negócios impactadas pelos ICs.
- 1.2.1.17. Deve ter a capacidade de normalizar dados de diferentes fontes, configurando regras para se adequar a um formato padrão.
- 1.2.1.18. Deve ter a capacidade de ter uma interface visual para mapear o impacto existente derivado das relações existentes entre ICs, processos e serviços.
- 1.2.1.19. Deve ter capacidade de interface visual para simulação de impactos e identificação direta dos serviços impactados por um IC, ou por um grupo específico de ICs.
- 1.2.1.20. Deve ter a capacidade de segregar dados por operação (tenant) e grupos, garantindo acesso aos ICs apenas para entidades ou grupos predefinidos.
- 1.2.1.21. Deve ter a capacidade de segregar dados por empresa e grupos, garantindo mudanças de IC apenas para empresas ou grupos predefinidos.
- 1.2.1.22. Deve ter a capacidade de representar ICs lógicos no CMDB, como processos de negócios, serviços técnicos, serviços de negócios, produtos, áreas, locais físicos, etc.
- 1.2.1.23. Deve ter a capacidade de renderizar relacionamentos de cardinalidade entre classes de CI, um para um, um para muitos e muitos para muitos.
- 1.2.1.24. A estrutura de dados da ferramenta CMDB deve ser construída sob padrões internacionais, como o DMTF. O referido modelo de dados CMDB deve ser flexível e personalizável de acordo com os requisitos da Instituição, com uma interface gráfica onde possa:
  - Adicionar ou modificar tipos de itens de configuração.
  - Adicionar ou modificar atributos de CI.
  - Adicionar ou modificar permissões para tipos e atributos de IC.
- 1.2.1.25. Deve gerenciar um conceito de partição CMDB em que pode gerenciar um espaço para os ICs a serem importados e analisados, uma partição de produção e uma partição de arquivo para itens de configuração obsoletos.
- 1.2.1.26. Deve permitir plena integração ao conjunto de ferramentas do fabricante desenvolvedor.
- 1.2.1.27. Deve permitir integração com ferramentas de terceiros.

## **1.2.2. Gerenciamento de Incidentes**

- 1.2.2.1. Deve ser capaz de registrar, classificar, priorizar e diagnosticar os incidentes.
- 1.2.2.2. Deve permitir identificar rápida e concisamente incidentes e relações com o mesmo solicitante, proporcionando a facilidade de identificar incidentes duplicados e evitar a captura de incidentes já reportados.
- 1.2.2.3. Deve permitir a visualização e relacionamento fácil dos itens de configuração (CI) associados ao solicitante.
- 1.2.2.4. Deve permitir a criação de relações de incidentes diretamente com outros Incidentes, Itens de

Configuração (CIs), Soluções/Erros conhecidos, Mudanças, Ordens de Trabalho, Artigos de Conhecimento

- 1.2.2.5. Deve permitir a criação de problemas, erros conhecidos, artigos de conhecimento, ordens de trabalho e pedidos de mudança diretamente associados com o incidente, a partir do mesmo registro de incidentes.
- 1.2.2.6. Deve ser capaz de sugerir artigos de conhecimento facilmente acessíveis ao usuário, a fim de realizar diagnósticos baseados neles.
- 1.2.2.7. Deve permitir um acesso rápido e simples a um CMDB a partir do registro do incidente para apoiar a identificação da solução do incidente.
- 1.2.2.8. Deve permitir a criação de artigos de conhecimento diretamente do registro de incidentes.
- 1.2.2.9. Deve salvar automaticamente o tempo e a hora de registro do incidente de acordo com o fuso horário e horário de trabalho definido para cada usuário e prestador de serviço bem como tempos por grupos e por cada status do chamado e, se necessário, calcular automaticamente a diferenciação do tempo entre os diferentes fusos horários.
- 1.2.2.10. Deve permitir que o tempo de restauração seja pausado devido a um evento específico, e depois continue a registrar esse tempo, sem afetar o nível de serviço comprometido.
- 1.2.2.11. Deve permitir a Integração bidirecional com DevOps, das demais ferramentas do mercado.
- 1.2.2.12. Deve permitir a vinculação automática de incidentes a um grupo solucionador responsável pelo serviço afetado ou Item de configuração associado ao chamado.
- 1.2.2.13. Deve possibilitar a vinculação de incidente a artigo da base de conhecimento.
- 1.2.2.14. Deve permitir que usuários com as devidas permissões de acesso abram um incidente em nome de terceiro, ajustando automaticamente os níveis de serviço de atendimento ao terceiro.
- 1.2.2.15. Deve possuir mecanismos de escalonamento hierárquico e funcional dos incidentes, de acordo com critérios estabelecidos e registrados na ferramenta.
- 1.2.2.16. Deve possuir mecanismos de vinculação de um ou mais incidentes a um registro de problema.
- 1.2.2.17. Deve ser capaz de integrar-se com ferramentas de monitoramento para geração de alertas e registros de incidentes.
- 1.2.2.18. Deve realizar a sugestão de categorização e opção de categorização automática do Incidente através do uso de Aprendizado de Máquina.
- 1.2.2.19. Deve suportar a abertura automática de Incidentes enviados por e-mail, com uso de Inteligência Artificial e/ou automatização para identificação de Padrões/Templates.
- 1.2.2.20. Deve fazer uso de algoritmos de análise de NLP (Natural Language Processing) e agrupamento por Inteligência Artificial para correlacionar incidentes em tempo real.
- 1.2.2.21. Deve relacionar ou sugerir relacionamento de múltiplos incidentes como duplicatas.
- 1.2.2.22. Deve suportar registros de Incidentes Críticos ou de Crise (Major Incident) com a facilidade de estabelecimento e colaboração do time escalado dentro do mesmo registro de incidente bem como, o acompanhamento das áreas (Grupos) correlacionadas.

### **1.2.3. Gerenciamento de Problemas**

- 1.2.3.1. Deve permitir o registro de problema a partir de um incidente ou vinculação de um incidente a um incidente pai, de forma que os próximos incidentes já estejam vinculados ao problema ou incidente pai.
- 1.2.3.2. Deve permitir a definição de prioridade em função do impacto, risco e da severidade do problema.
- 1.2.3.3. Deve permitir a associação automática com incidentes, mudanças, liberações, ICs relacionados e base de conhecimento.
- 1.2.3.4. Deve possuir mecanismo de fechamento automático dos incidentes em aberto, quando houver o fechamento do problema ao qual estejam vinculados.
- 1.2.3.5. Deve permitir o acompanhamento gráfico e gerar notificações em relação ao andamento dos chamados de problema. Deve permitir alterar a classificação da severidade ou do impacto de um problema.
- 1.2.3.6. Deve possibilitar o roteamento e a atribuição automática dos registros de problemas.
- 1.2.3.7. Deve possibilitar o monitoramento e o acompanhamento dos problemas.
- 1.2.3.8. Deve possibilitar a entrada de texto livre para registrar as descrições dos problemas e atividades de resolução.
- 1.2.3.9. Deve permitir que cada problema possa ser tratado e acompanhado de várias tarefas, que poderão ser encaminhadas para vários grupos solucionadores.
- 1.2.3.10. Deve permitir a associação de problemas diretamente com Incidentes, com Itens de Configuração (ICs) ou com Soluções/Erros conhecidos e Mudanças a partir do mesmo Registro de Problemas.
- 1.2.3.11. Deve permitir a criação de Incidentes ou solicitações de Mudança diretamente associados ao problema, de dentro do Registro de Problemas.
- 1.2.3.12. Deve conter uma área onde os erros conhecidos, a causa raiz e as soluções de trabalho podem ser documentados.
- 1.2.3.13. Deve permitir a criação de artigos de conhecimento documentando as soluções aplicadas, diretamente a partir do registro do problema.
- 1.2.3.14. Deve conter funcionalidade de bate-papo, permitindo que outros profissionais sejam adicionados a uma conversa sobre um determinado problema e salvar a conversa no registro.
- 1.2.3.15. Deve permitir sugerir a categorização automática do Problema através do uso de Aprendizado de Máquina.
- 1.2.3.16. Deve permitir sugerir a Causa Raiz do Problema através do uso de Aprendizado de Máquina.
- 1.2.3.17. Deve fazer uso de algoritmos de análise de NLP (Natural Language Processing) e agrupamento de incidentes, por Inteligência Artificial, para iniciar a gestão proativa de problemas.
- 1.2.3.18. Deve detectar clusters de incidentes recorrentes, de acordo com a criticidade, e efetuar automaticamente registros de problema, para iniciar a investigação proativa.

#### **1.2.4. Gerenciamento de Mudanças**

- 1.2.4.1. Deve permitir o registro e classificação das mudanças, atribuindo um identificador único para cada mudança criada e as eventuais tarefas existentes.
- 1.2.4.2. Deve permitir a associação de uma mudança a um ou mais processos (Solicitação, Incidente ou

Problema) ou ICs.

- 1.2.4.3. Deve suportar diferentes processos de mudança para diferentes tipos de mudanças, tais como emergencial, padrão e normal, podendo-se criar e configurar outros tipos de mudança conforme a necessidade.
- 1.2.4.4. Deve permitir modificações necessárias e realizar o controle do nível de acesso para leitura, escrita e modificação das RDMs para Usuários e/ou Grupos.
- 1.2.4.5. Deve possibilitar a revisão das mudanças implementadas e o processo de aprovação possibilitando aprovação automática e aprovação com perfis ou funções específicas.
- 1.2.4.6. Deve permitir limitar o número de revisores ou aprovadores com base em regras de negócio.
- 1.2.4.7. Deve possibilitar a configuração das janelas de mudanças (programação de períodos de mudanças).
- 1.2.4.8. Deve permitir que o requisitante justifique a mudança solicitada em campo textual ou lista pré-definida.
- 1.2.4.9. Deve permitir fechar requisições, incidentes, problemas e erros conhecidos quando uma mudança relacionada é implementada com sucesso.
- 1.2.4.10. Deve facilitar a comunicação da mudança e de agendamentos ao Service Desk e grupos de analistas.
- 1.2.4.11. Deve manter uma associação lógica entre erros conhecidos e mudanças.
- 1.2.4.12. Deve possibilitar a definição de várias tarefas para uma mudança, atribuindo responsáveis e os respectivos prazos. As tarefas devem ser controladas concorrente e sequencialmente, conforme a necessidade.
- 1.2.4.13. Deve permitir obter automaticamente do CMDB a lista de todos os IC's afetados pela mudança.
- 1.2.4.14. Deve permitir o cadastro de mudanças pré-aprovadas. Nesse caso, deve aprovar automaticamente a mudança e iniciar a próxima ação ou não possuir o estado de aprovação.
- 1.2.4.15. Deve permitir aos usuários incluírem anexos nas requisições de mudanças.
- 1.2.4.16. Deve registrar a hora e o responsável por toda e qualquer alteração no registro de uma mudança.
- 1.2.4.17. Deve permitir o uso de modelos para ajudá-lo a preencher dados específicos, bem como para lidar com tarefas pré-definidas com um processo de execução sequencial e/ou paralelo.
- 1.2.4.18. Permitir a associação de múltiplos ICs nas mudanças e nas tarefas de mudança.
- 1.2.4.19. Deve permitir a documentação e avaliação do risco e do impacto da mudança, com funcionalidades específicas para este fim.
- 1.2.4.20. Deve conter um calendário de mudanças no qual as mudanças programadas possam ser observadas em uma visão geral.
- 1.2.4.21. Deve ser capaz de realizar simulações de impacto de mudanças programadas com base no CMDB, de modo que se uma mudança for planejada em um determinado item de configuração, ela possa simular quais outros itens de configuração ou serviços serão afetados pela possível interrupção da operação desse item de configuração.
- 1.2.4.22. Deve detectar a colisão de mudança, ou seja, ser capaz de identificar se uma mudança programada

em um item de configuração está em colisão porque o mesmo item de configuração já faz parte de uma mudança previamente programada.

- 1.2.4.23. Deve ter a capacidade de criar fluxos de trabalho de pedidos de mudança simples a complexos, através de tarefas sequenciais e paralelas.
- 1.2.4.24. Deve possibilitar a gestão de reuniões de CAB:
  - com visibilidade das mudanças inclusas em cada reunião, prevista, planejada, em andamento ou realizada.
  - com visibilidade das atividades/tarefas previstas para o período sob a forma de KanBan
  - com campos específicos para documentar as decisões deliberadas durante cada sessão de CAB.
  - com campos específicos para registro de comentários, aprovações e interações entre os participantes.
  - Suportando assim a realização da reunião de forma remota.
- 1.2.4.25. A solução deve ser capaz de se integrar com o CMDB nativamente para facilitar o acesso aos atributos e relações dos ICs para permitir a avaliação e autorização de mudanças.
- 1.2.4.26. Deve permitir integração com soluções de descoberta de ativos para que alterações realizadas nos ICs sejam identificadas para tratamento através de registro de Incidente ou Problema.
- 1.2.4.27. Deve ter funcionalidade de bate-papo, permitindo adicionar outros usuários a uma conversa sobre uma determinada mudança e salvar a conversa no registro.
- 1.2.4.28. Deve permitir relacionar diversas mudanças existentes e ser capaz de definir sua ordem de execução, com respeito ao plano de liberação.
- 1.2.4.29. Deve permitir a programação de liberações de acordo com um cronograma de diversas mudanças.
- 1.2.4.30. Deve permitir sugerir a categorização e opção de categorização automática da Mudança através do uso de Aprendizado de Máquina.
- 1.2.4.31. Deve ser capaz de efetuar a aplicação automática de template às Mudanças abertas via e-mail.
- 1.2.4.32. Deve permitir sugerir o nível de risco da Mudança, e opção de cálculo automático, através do uso de Aprendizado de Máquina.
- 1.2.4.33. Deve permitir a integração bidirecional com DevOps - sincronismo entre Issue, registros de Mudanças e as demais ferramentas do mercado.

#### **1.2.5. Gerenciamento de Nível de Serviços**

- 1.2.5.1. Deve fornecer uma maneira de rever, aplicar e informar sobre o nível de serviço prestado para garantir que níveis adequados de serviço sejam fornecidos em alinhamento com as necessidades comerciais a um custo aceitável.
- 1.2.5.2. Deve fornecer informações sobre o cumprimento de SLAs para a gestão dos contratos de prestação de serviços.
- 1.2.5.3. Deve permitir documentar e acompanhar o histórico dos indicadores e métricas de avaliação dos serviços de TI.
- 1.2.5.4. Deve permitir definição de múltiplos SLAs e OLAs.
- 1.2.5.5. Deve permitir a configuração de contabilização de SLA apenas em horários definidos pelo

CONTRATANTE (definição de turnos de trabalho).

- 1.2.5.6. A medição de prazos deverá ser insumo para a composição de indicadores gráficos de performance, exibidos em painéis do tipo dashboard.
- 1.2.5.7. Deve permitir alertas às equipes técnicas e à gestão caso um evento exceda um número específico de atribuições e escalações ou caso exceda um tempo limite especificado.
- 1.2.5.8. Deve permitir a criação de SLAs, OLAs e KPIs definidos pelo administrador.
- 1.2.5.9. Deve permitir o acompanhamento do atingimento de metas dos acordos de nível de serviço.
- 1.2.5.10. Deve permitir a geração e customização de dashboards e relatórios de medição dos SLAs.
- 1.2.5.11. Deve apoiar o monitoramento e a gestão das métricas operacionais e de SLA dos fornecedores.
- 1.2.5.12. Deve permitir a gestão e automação de metas de nível de serviço em termos de regras de negócio automatizadas, alertas, escalonamentos e notificações.
- 1.2.5.13. Deve permitir a configuração de metas de nível de serviço, de forma que se um critério configurado na meta de nível de serviço for cumprido (por exemplo, um certo tempo decorrido, ou uma certa porcentagem de tempo em relação a um limite), atividades como notificações ou escalas (por exemplo, o envio de um e-mail para uma pessoa específica, ou a reatribuição do bilhete para outro grupo ou pessoa de suporte) são executadas.
- 1.2.5.14. Deve permitir configuração de matriz de prioridade por tenant, por serviço ou por categoria de serviço.
- 1.2.5.15. As matrizes de prioridade devem permitir relacionamento entre impacto, urgência, risco e localidade do usuário.

#### **1.2.6. Gerenciamento de Liberações**

- 1.2.6.1. Deve ter uma abordagem unificada e uniforme para o gerenciamento de negócios de mudanças e lançamentos em toda a infraestrutura, permitindo automatizar as melhores práticas para gerenciar mudanças e lançamentos juntos.
- 1.2.6.2. Deve permitir relacionar as mudanças existentes e poder definir sua ordem de execução, no que diz respeito ao plano de liberação.
- 1.2.6.3. Deve permitir a criação de tarefas manuais ou modelo em cada etapa do plano de liberação.
- 1.2.6.4. Deve permitir agendar lançamentos de acordo com um cronograma de mudanças.

#### **1.2.7. Gerenciamento de Conhecimento**

- 1.2.7.1. Deve ter um processo de gerenciamento do ciclo de vida do artigo de conhecimento.
- 1.2.7.2. A base de conhecimento deve permitir feedback dos usuários dos documentos da solução.
- 1.2.7.3. A base de conhecimento deve permitir, através de fluxo de autorização, que os usuários personalizem seus dados gerais, bem como os tópicos de seu interesse.
- 1.2.7.4. Deve ser capaz de usar formatos personalizáveis que funcionarão para a criação de artigos de conhecimento.
- 1.2.7.5. Deve gerar documentos de solução providos de segurança em nível de campo e em nível de documento, de forma a segregar as informações e que só possam ser consultadas por pessoal

autorizado.

- 1.2.7.6. Deve usar um editor para criar, modificar e rastrear artigos de conhecimento.
- 1.2.7.7. Deve ter a capacidade de pesquisar várias bases de conhecimento para artigos de conhecimento relevantes durante a criação de registros (incidente, solicitação, problema, mudança) por meio de auto-atendimento ou de outra forma.
- 1.2.7.8. Deve ter a capacidade de solicitar aprovações para publicação de artigos de conhecimento de acordo com perfis de usuário pré-definidos.
- 1.2.7.9. Deve permitir a criação e o uso obrigatório de regras de entrada de dados para criar registros de conhecimento.
- 1.2.7.10. Deve permitir a entrada de texto em formato livre, imagens, multimídia, anexos etc.
- 1.2.7.11. Deve automatizar o preenchimento de registros de conhecimento com dados de autor e proprietário, data de criação, bem como qualquer outro atributo exigido pela organização.
- 1.2.7.12. Deve facilitar a identificação de informações redundantes ou duplicadas, seja em um único registro ou em múltiplos registros.
- 1.2.7.13. Deve permitir a notificação automática às partes interessadas sobre a apresentação de novos conhecimentos / soluções que lhes sejam aplicáveis.
- 1.2.7.14. Deve permitir que você exiba as perguntas mais frequentes e destaque o conteúdo de conhecimento recém-adicionado.
- 1.2.7.15. Deve permitir a integração com todos os processos de gerenciamento de serviço para permitir a criação rápida de registros de conhecimento a partir de registros com links associados.
- 1.2.7.16. Deve permitir avaliar a utilidade do conhecimento utilizado pelo usuário final.

#### **1.2.8. Gerenciamento das Requisições de Serviços**

- 1.2.8.1. Deve fornecer ao solicitante a capacidade de interromper o processo ou cancelar sua solicitação de serviço.
- 1.2.8.2. Deve ter uma área de trabalho onde o usuário possa inserir as informações necessárias para a solicitação de serviço.
- 1.2.8.3. Deve oferecer a possibilidade de anexar informações ou arquivos externos como parte das informações fornecidas.
- 1.2.8.4. Um usuário que envia uma solicitação de serviço pode adicionar outros usuários como colaboradores da solicitação, para que os colaboradores possam visualizar e comentar sobre a solicitação inicial.
- 1.2.8.5. Os usuários finais podem atribuir permissão a um ou mais usuários na sua solicitação para inserir comentários, anexar arquivos ou reabrir o chamado.
- 1.2.8.6. Deve conter relatórios prontos para uso que fornecem informações em tempo real sobre os serviços mais populares, o custo total e as métricas de desempenho do provedor de acordo com o acordo de nível de serviço (SLA).
- 1.2.8.7. Deve mostrar o dia e a hora em que se espera que a solicitação seja resolvida.
- 1.2.8.8. Deve oferecer a possibilidade de adicionar informação ao pedido de serviço depois de o mesmo

ter sido enviado.

- 1.2.8.9. Deve permitir uma gestão e acompanhamento completo dos pedidos de serviço desde o início até ao fim.
- 1.2.8.10. Deve permitir a distinção e gerenciamento de papéis funcionais para diferenciar as atividades realizadas pelo pessoal da contratante e disponibilizar a visualização em forma de dashboards .
- 1.2.8.11. Deve permitir o relacionamento de duas ou mais solicitações de serviço.
- 1.2.8.12. Deve permitir cancelar solicitações, bem como modificar suas informações.
- 1.2.8.13. Deve mostrar e notificar quando uma solicitação de serviço requer informações adicionais do solicitante na tela de abertura e edição.
- 1.2.8.14. Deve ter flexibilidade para permitir que os usuários façam solicitações em nome de outros usuários.
- 1.2.8.15. Deve fazer uso de um catálogo de serviços padrão para as diferentes áreas, contratos e tenants.

#### **1.2.9. Gerenciamento de Catálogo**

- 1.2.9.1. Deve permitir a criação de um Catálogo de Serviços capaz de gerir os diversos serviços de TI e de áreas de negócios, integrada nativamente à solução de chatbot, sem a necessidade de conhecimento de programação para a gestão do catálogo e do chatbot.
- 1.2.9.2. Deve ser possível publicar um Catálogo de Serviços contendo serviços de diversas naturezas (TI, RH, Finanças etc.), incluindo a centralização de serviços provenientes de diferentes origens.
- 1.2.9.3. Deve organizar os serviços em grupos lógicos ou estruturas hierárquicas que podem ser utilizadas para reunir os serviços aos clientes em pacotes.
- 1.2.9.4. Deve permitir a expansão do catálogo apresentando serviços de várias unidades, em um único catálogo.
- 1.2.9.5. Deve permitir configurar uma exibição no catálogo para fornecer informações sobre o status de funcionamento dos serviços que são fornecidos em sua organização.
- 1.2.9.6. Deve facilitar o gerenciamento distribuído de Catálogo de Serviços baseado em funções, tenant, grupo, serviços, tipos de usuário e cliente. Incluindo diferentes aspectos de configuração e manutenção do catálogo por diferentes funções, por exemplo: Função de administrador de correio etc.
- 1.2.9.7. Ao administrador de catálogo, deve ser permitido projetar pesquisas de satisfação personalizadas ou definir uma pesquisa padrão para todas as solicitações de serviços concluídas.

#### **1.2.10. Portal de Serviços**

- 1.2.10.1. Deve permitir a criação de um Portal de serviços unificado para todos os serviços de TI e de áreas de negócios, acessível de forma Omni-Channel, permitindo a busca cognitiva com uso através de linguagem natural e em idioma local.
- 1.2.10.2. O portal deve oferecer a facilidade de configuração através do uso de ações de arrastar e soltar, personalização dos fluxos de trabalho e configurações customizáveis para entregar a capacidade de resolução mais rápida de incidentes e problemas assim como oferecer uma melhor experiência do usuário
- 1.2.10.3. Deve entregar um portal de auto-atendimento para que os usuários tenham acesso ao catálogo de

serviços unificado da organização, podendo ser segmentado em vários portais e subportais para cada linha de negócio ou segmentação de atendimento.

- 1.2.10.4. Deve permitir aos usuários enviar solicitações e encontrar recursos de autoajuda, reservar salas de reuniões, visualizar mapas de localização e agendar compromissos com a equipe de suporte.
- 1.2.10.5. Deve permitir iniciar um processo de solicitação imediatamente em um serviço ou adicionar serviços a um "carrinho de compras" para fazer várias solicitações ou solicitá-los posteriormente.
- 1.2.10.6. Deve apoiar a criação e publicação de ofertas de serviços com:
- 1.2.10.7. Descrição das características da oferta de serviço, funções e vantagens em termos de negócio.
- 1.2.10.8. Opções de nível de serviço de suporte e níveis de disponibilidade comprometidos.
- 1.2.10.9. Preços e níveis de custo associados aos níveis de serviço selecionados.
- 1.2.10.10. Deve organizar os serviços em grupos lógicos ou estruturas hierárquicas que podem ser utilizadas para reunir os serviços aos clientes em pacotes/ofertas relevantes para o negócio.
- 1.2.10.11. Deve permitir a expansão do catálogo apresentando serviços de várias unidades de negócios, incluindo TI, RH e instalações, em um único catálogo.
- 1.2.10.12. Deve permitir criar um portal e expor um catálogo de serviços para usuários externos, ou seja, para usuários que não pertencem à organização.
- 1.2.10.13. Deve se integrar com sistemas de atendimento de solicitação externa por meio de conectores de serviço que passam informações de uma solicitação de serviço para um sistema externo.
- 1.2.10.14. Deve permitir experiências amigáveis com um design modular altamente configurável por meio do mecanismo de "arrastar e soltar".
- 1.2.10.15. Deve ter a capacidade de fornecer uma visão de serviços associados a funções de negócios específicas com base em seu uso ou assinatura. Por exemplo, a capacidade de construir e fornecer uma visão "Meu Catálogo de Serviços".
- 1.2.10.16. Deve permitir a configuração de fluxos de trabalho para reduzir os tíquetes de nível um, desviando as chamadas de rotina para o help desk.
- 1.2.10.17. Deve permitir que os usuários interajam com mais de um idioma em suas estações de trabalho.
- 1.2.10.18. Deve permitir promover aplicativos, serviços e / ou anúncios com banners de vários tamanhos na interface do usuário de forma intuitiva, bem como permitir um direcionamento personalizado, baseado em direitos, para possibilitar campanhas programadas específicas.
- 1.2.10.19. Deve ser integrada com o módulo de gerenciamento de incidentes nativa e bidireccionalmente. Os incidentes podem estar associados aos serviços contidos no catálogo de serviços.
- 1.2.10.20. Deve ser integrado ao módulo de gerenciamento de solicitação de serviço proposto de maneira bidireccional. As solicitações de serviço podem ser associadas aos serviços contidos no catálogo de serviços.
- 1.2.10.21. Deve ser integrado ao módulo de gerenciamento de nível de serviço proposto de maneira bidireccional. Os serviços podem estar associados a acordos de nível de serviço, operacionais e de fornecedores.
- 1.2.10.22. Deve conter Interface de usuário totalmente responsiva para funcionar em qualquer dispositivo, onde o usuário pode consumir serviços digitais com base em sua função.

- 1.2.10.23. Deve ter a funcionalidade de construção de pesquisas de satisfação com base nos serviços publicados.
- 1.2.10.24. Deve possuir métodos padronizados de integração com terceiros para fortalecer o preenchimento dos questionários associados aos serviços.
- 1.2.10.25. Deve ter uma busca nativa por fontes de conhecimento interno e externo, bem como processamento de linguagem natural nas consultas.
- 1.2.10.26. Deve se integrar ao módulo de Chatbot para interação por meio de conversa entre os usuários e o catálogo de serviços.
- 1.2.10.27. Deve ter a funcionalidade de apresentar mapas interativos que permitam visualizar os bens ou serviços dos mesmos e poder fazer reservas, selecionando o dia e a hora, bem como visualizar outros subserviços associados à localização.

#### **1.2.11. Módulo de Atendimento por Chatbot com Inteligência Artificial**

- 1.2.11.1. Deverá conter mecanismos de inteligência artificial e utilização da conversação em linguagem Natural no idioma português do Brasil.
- 1.2.11.2. Deve suportar a busca cognitiva em dados não estruturados e estruturados e em múltiplas bases de conhecimento.
- 1.2.11.3. Dever permitir configurar múltiplos “motores” de chatbot adaptados para cada linha de negócio possibilitando um bate-papo contextualizado e adaptado à cada necessidade.
- 1.2.11.4. Deve conter a integração nativa com o Catálogo de Serviços, Portal de Solicitações, e Base de Conhecimento.
- 1.2.11.5. Deverá permitir registrar incidentes e requisições por meio de um portal de autoatendimento de chatbot ou chat online.
- 1.2.11.6. Deverá permitir redirecionar o atendimento de clientes para o agente humano.
- 1.2.11.7. Deve permitir a realização de bate-papo ao vivo entre usuários e agentes (ou usuários e profissionais das equipes de service desk)
- 1.2.11.8. Deverá permitir o fluxo de conversação com controle de acesso para diferentes perfis de usuários com privilégios distintos.
- 1.2.11.9. Deverá permitir na modalidade de atendimento humano, o atendente conversar com os usuários dentro de um ambiente separado e com autenticação de acesso.
- 1.2.11.10. Deverá permitir, além do perfil de atendente, a inclusão de um outro perfil, o de supervisor.
- 1.2.11.11. Deverá permitir, no perfil de administrador, a possibilidade de gerar relatórios e configurar/customizar a plataforma.
- 1.2.11.12. Deverá possibilitar a visualização de painéis estatísticos aos usuários administradores e supervisores, contendo informações sobre os atendimentos em tempo real e série histórica e sobre o desempenho de cada atendente.
- 1.2.11.13. Deverá possibilitar a leitura de painéis de informações com TMA (Tempo Médio de Atendimento), Tempo Médio de Espera e quantidade de atendimentos total e por atendente.
- 1.2.11.14. Deverá possibilitar a configuração e separação de grupos de atendentes, com habilitação de recursos e informações específicas para cada grupo, canal de atendimento, filas e roteamentos.

- 1.2.11.15. Deverá possibilitar visualizar o histórico das conversações (chats) realizadas e a quantidade de atendimentos realizados por tempo, com período de análise ajustável em mês, dias, horas e minutos.
- 1.2.11.16. Deverá permitir a exportação de relatórios e estatísticas gerados sobre chat, utilizando-se de formatos diversos, tais como pdf, xls, xlsx e csv.
- 1.2.11.17. Deverá possibilitar a integração nativa com serviços de Processamento de Linguagem Natural (do inglês "Natural Language Processing" ou NLP) em português (Brasil), para inteligência artificial.
- 1.2.11.18. Deverá possibilitar entrada de dados em formato de texto.
- 1.2.11.19. Deverá possibilitar integração nativa para atendimento com canais popularizados, tais como: Whatsapp, SMS, MS Teams, Slack, Twilio etc.
- 1.2.11.20. Deverá possibilitar o consumo de Web Services e Application Programming Interfaces - API's, com a finalidade de integrá-los aos fluxos de conversação que vierem a ser configurados dentro da plataforma, independentemente da modalidade de atendimento (humano ou automatizado).
- 1.2.11.21. Deverá disponibilizar código necessário para integrar o componente de conversação - popular "balão de chat" - em ambiente web próprio da contratante, quando da utilização do canal de atendimento web.
- 1.2.11.22. Deverá possuir componente de conversação customizável, de modo que seja adaptado à identidade visual da contratante.
- 1.2.11.23. Deverá possibilitar a coleta de informações do cliente antes de iniciar o atendimento.
- 1.2.11.24. Deverá possibilitar sugestão de entradas de texto, opções pré-configuradas e texto livre durante a conversação.
- 1.2.11.25. O componente de conversação, no lado do cliente, deverá funcionar sem a necessidade de instalação de plug-ins e componentes adicionais.
- 1.2.11.26. Deverá fornecer interface de configuração de fluxos de conversação de forma gráfica (árvores de decisão ou fluxogramas) ou textual (listas encadeadas ou lista de frases de treinamento).
- 1.2.11.27. Deverá possibilitar, na configuração dos fluxos de conversação, o controle do horário de atendimento, de modo a especificar formas de atendimento distintas aos clientes, nas modalidades de atendimento humano ou automatizado (chatbot ou assistente virtual) a depender do horário em que for realizado o contato.

#### **1.2.12. Desenvolvimento de aplicações No Code / Low Code**

- 1.2.12.1. Deverá permitir a automação de processos e fluxos de trabalho de forma interativa, prática e de fácil implementação.
- 1.2.12.2. Deverá possibilitar a configuração pelo administrador e suportar modelos e designs.
- 1.2.12.3. Deverá suportar a criação de soluções, automações de fluxos de trabalho e suportar a implementação de rotinas e processamento de funcionalidades com uma programação mínima e básica (Low Code/ No Code), usando componentes integrados e nativos da própria plataforma.
- 1.2.12.4. Deverá possibilitar configuração simples de atividades em fluxos de trabalho, com recursos interativos de workflow, do tipo de arrastar e soltar, providos pela própria solução.
- 1.2.12.5. Deverá possibilitar configuração simples de aprovações em fluxos de trabalho utilizando os

próprios recursos da solução para configuração de aprovações.

- 1.2.12.6. Deverá possibilitar configuração de formulário simples com a inclusão de campos sem a necessidade de criação de scripts para preenchimento dinâmico.
- 1.2.12.7. Deverá possibilitar configuração de notificações simples em fluxos de trabalho, com recursos da própria solução.
- 1.2.12.8. Deverá permitir configuração de formulário com possibilidade de ações como: ocultar campo, exibir como executar regras de negócio configuradas na ferramenta sem a necessidade de escrita de código fonte.
- 1.2.12.9. Deverá permitir criação de fluxos de aprovação automática com formulário detalhado de acordo com as regras de negócio em vigor na contratante, com possibilidade de atualização, vários níveis de aprovação, em diferentes departamentos, com aprovadores definidos por função e por organograma e instâncias em plataformas web e/ou mobile.
- 1.2.12.10. Deverá apresentar componente próprio para a modelagem gráfica e a automação de processos e fluxos de trabalho da solução.
- 1.2.12.11. Deverá permitir a criação e automação de processos e fluxos de trabalho de forma segregada e independente.
- 1.2.12.12. Deverá possuir recursos gráficos de workflow interativos (editor gráfico integrado) para criação de processos e rotinas operacionais, que permita operações como arrastar-e-soltar para o desenho dos fluxos de trabalho.
- 1.2.12.13. Deverá permitir que os processos sejam desdobrados em níveis inferiores, tais como subprocessos, atividades e tarefas.
- 1.2.12.14. Deverá permitir associação de documentos e hyperlinks a processos e atividades.
- 1.2.12.15. Deverá permitir a automação de fluxos de automação de forma gráfica, incluindo estágios, tarefas paralelas ou sequenciais, regras de decisão e aprovação, sem a necessidade de programação ou alteração de código-fonte.
- 1.2.12.16. Deverá permitir a customização de menus, formulários, labels, automatizações de fluxos de trabalho e processos, desenvolvidos na solução, permitindo a adequação às necessidades de uso de cada usuário, sem a necessidade de programação ou alteração do código-fonte.
- 1.2.12.17. Deverá suportar o versionamento dos fluxos e processos nela modelados, permitindo consultar o histórico das revisões realizadas.
- 1.2.12.18. Quando da publicação de alterações em processos existentes, essas devem ser transparentes para o usuário final sem a necessidade de aplicação de release na solução ou alteração em seu código-fonte.
- 1.2.12.19. Deverá permitir a substituição de um processo em produção sem que isso afete as requisições que já foram iniciadas, mantendo as já iniciadas pelo caminho previsto em seu início.
- 1.2.12.20. Deverá prover modelos predefinidos e configuráveis de fluxo de trabalho para os processos de gerenciamento de serviços de TIC, baseados no ITIL - Information Technology Infrastructure Library e nas melhores práticas de mercado.
- 1.2.12.21. Deverá permitir a adequação de qualquer um dos processos de gerenciamento de serviços de TIC, de operações de TIC, de negócio de TIC e demais, implementados nativamente na solução, para o contexto operacional da contratante, de forma a se adaptar ao processo em operação ou já

implantado.

### **1.2.13. Módulo de Descoberta de Itens de Configuração e Serviços de TI**

- 1.2.13.1. A solução deve descobrir automaticamente dispositivos de hardware e software da contratante instalados em nuvem privada ou pública, identificando a sua configuração e os dados de relacionamento entre os componentes descobertos, bem como entre os aplicativos e a infraestrutura que os suporta.
- 1.2.13.2. Deve permitir a modelagem de relacionamentos e impactos de infraestrutura e de serviços e negócios de forma unificada, sem a necessidade de replicação e gestão de diversos modelos e bases de dados entre módulos das soluções. Ou seja, o CMDB deve ser único, com informações provenientes de diversas origens de dados e utilizado diretamente pelos diversos módulos ou disciplinas da solução
- 1.2.13.3. Para a coleta de dados locais, deve conter ferramenta de outpost que será instalada no data center da contratante (em uma ou mais localidades), e que permitirá, de forma segura, a alimentação dos dados coletadas na nuvem da solução.
- 1.2.13.4. O CMDB Discovery deverá fazer o relacionamento com os itens descobertos e já mapear automaticamente o desenho das aplicações.
- 1.2.13.5. Deve conter uma biblioteca de padrões para identificação dos softwares líderes de mercado e fornecer a atualização periódica destes padrões para permitir que novos softwares e/ou suas novas versões possam ser descobertos automaticamente.
- 1.2.13.6. A solução deve permitir operar com ou sem a instalação de agentes nos equipamentos a serem descobertos.
- 1.2.13.7. Para minimizar o tráfego na rede, deve permitir a instalação de múltiplos pontos de coleta cada rede e consolidá-la num servidor central, bem como permitir adaptar configurações relacionadas com a quantidade de dados a descobrir.
- 1.2.13.8. Deve suportar redes IPV6 e redes IPV4 / IPV6 duplas.
- 1.2.13.9. A comunicação entre os itens descobertos e Deve ser criptografada.
- 1.2.13.10. Deve utilizar o mecanismo de "shadow credentials", permitindo gerar credenciais marcadas que se referem às credenciais reais, de forma que nunca saiam das instalações do cliente.
- 1.2.13.11. As credenciais devem ser mantidas em um cofre de credenciais seguro. Enquanto a solução está em uso, as credenciais nunca devem sair das instalações do cliente.
- 1.2.13.12. Deve ser possível verificar quem está conectado e ver os detalhes de cada sessão ativa na solução.
- 1.2.13.13. Deve conter função de auditoria que permita rastrear as alterações na configuração do sistema. Todos os eventos iniciados pelo usuário que mudam o estado ou comportamento do sistema devem ser registrados.
- 1.2.13.14. Deve oferecer opção de fazer backup de seu cofre de credenciais usando funções de exportação e importação.
- 1.2.13.15. Deve permitir a descoberta de ativos em toda a infraestrutura da contratante identificando estações de trabalho Windows, MacOs e Linux, equipamentos de rede, dispositivos de armazenamento, sistemas operacionais de servidores Windows, Linux, e Unix, servidores físicos, virtuais e containers, Instâncias OpenShift, Docker, Kubernetes, Web Servers, Application Servers,

Bancos de Dados, Microserviços, Servidores Hiperconvergentes, Clusters de Servidores e Aplicações, etc.), estejam eles na infraestrutura interna ou em nuvens públicas (Microsoft Azure, Google Cloud, Amazon Web Service – AWS, Oracle OCI dentre outras).

- 1.2.13.16. As descobertas devem ser executadas através dos protocolos dos componentes que serão mapeados.
- 1.2.13.17. Deve permitir criar relacionamentos upstream e downstream entre os componentes interdependentes.
- 1.2.13.18. Deve descobrir e mapear relacionamentos do tipo virtual-virtual e virtual-físico.
- 1.2.13.19. Deve descobrir e mapear relacionamentos em ambientes virtualizados e de containers.
- 1.2.13.20. Descobrir e mapear relacionamentos onde os componentes estão dentro de um único host virtual ou espalhados por vários hosts virtuais.
- 1.2.13.21. Descobrir e mapear todos os componentes e relacionamentos de TI que suportam um serviço, incluindo aplicativos, middleware, servidores, storage e equipamentos de rede.
- 1.2.13.22. Descobrir os componentes de TI individualmente, bem como todas as conexões diretas entre componentes adjacentes.
- 1.2.13.23. Descobrir, documentar e mapear dependências de aplicações instaladas em Docker e Kubernetes, suportando as API's dessas tecnologias.
- 1.2.13.24. Ser capaz de realizar a descoberta preservando informações de descobertas anteriores, permitindo mostrar as diferenças entre os atributos reconhecidos entre uma tarefa de descoberta e outra.
- 1.2.13.25. Deve relatar as características físicas e térmicas do hardware de acordo com as informações publicadas pelo fabricante, incluindo capacidade térmica (BTU) ou energia (Volt Amps ou Watts).
- 1.2.13.26. Deve permitir a exclusão de desktops da descoberta.
- 1.2.13.27. Deve permitir que determinados IP's ou intervalos específicos de IP's possam ser excluídos das descobertas.
- 1.2.13.28. Deve possuir um mecanismo para a criação automática do modelo de relacionamento entre os itens de configuração permitindo a associação entre os itens e geração do mapa de serviços.
- 1.2.13.29. Deve identificar automaticamente os nós de software que provavelmente serão compartilhados por vários aplicativos, por exemplo, servidores de banco de dados compartilhados e filas de mensagens.
- 1.2.13.30. Deve possuir um mecanismo que permita modificar ou criar padrões de modelagem para se alinhar às necessidades da organização.
- 1.2.13.31. Deve incluir relatórios de tudo o que foi descoberto e deve permitir a definição de novos relatórios.
- 1.2.13.32. Deve fornecer painéis de controle com indicadores configuráveis (Dashboards) para cada perfil de usuário.
- 1.2.13.33. Deve possuir uma linguagem de consulta semelhante ao SQL que permita consultar todos os dados armazenados no banco de dados.
- 1.2.13.34. Deve se integrar com "cofres de senha" para sua gestão, minimamente para os seguintes fabricantes/produtos: BeyondTrust Password Safe, Centrify Identity Platform, CyberArk Enterprise e Thycotic.

- 1.2.13.35. Deve ter uma API REST para acionar a descoberta, gerenciar credenciais, consultar dados e fazer upload de atualizações.
- 1.2.13.36. Deve possuir API's de exportação de dados, que permitam aos usuários efetuar buscas usando um script ou programa e receber dados como um fluxo de texto, uma string vazia ou um código de retorno.
- 1.2.13.37. Deve permitir a integração com o CMDB permitindo selecionar quais dados serão sincronizados no CMDB.
- 1.2.13.38. Deve permitir pesquisas globais por textos ou palavras chave para a busca de todos os itens relacionados a ela.
- 1.2.13.39. Disponibilizar filtros para cadastros manuais de componentes que devem ser ignorados nos processos de descoberta.
- 1.2.13.40. Disponibilizar graficamente mapas com toda topologia dos serviços identificados.
- 1.2.13.41. Disponibilizar interface para cadastro manual de serviços, componentes e transações.
- 1.2.13.42. Fornecer filtros para seleção das informações que serão coletadas durante as ações de descoberta.
- 1.2.13.43. Fornecer templates customizáveis para realização de descobertas pelos seguintes critérios:
- Gerar mapas atualizados com a identificação dos componentes e os relacionamentos que suportam os serviços.
  - Identificar graficamente nos mapas os componentes que impactam na qualidade e disponibilidade dos serviços.
  - Identificar portas de entrada e processos utilizados em servidores e que tenham relação com os serviços mapeados.
  - Identificação de forma proativa de componentes e relacionamentos que não fazem parte do serviço.
- 1.2.13.44. Manter os mapas de serviços atualizados periodicamente, bem como as informações das aplicações e de todos os componentes de rede. O período de atualização pode ser customizável.
- 1.2.13.45. Validar periodicamente as relações de dependência das aplicações com componentes de rede e de infraestrutura.
- 1.2.13.46. Montar mapas de dependências e de topologia automaticamente a partir do cadastro de pontos de entrada como URL's, componentes, serviços e transações.
- 1.2.13.47. Permitir a descoberta e obtenção de informações sobre softwares ou outros componentes não suportados nativamente através da customização e extensão de sensores.
- 1.2.13.48. Permitir o mapeamento manual de componentes e serviços.
- 1.2.13.49. Permitir o uso de tags personalizadas para os componentes descobertos.
- 1.2.13.50. Registrar informações de IP e subnets associados aos componentes descobertos e mapeados.
- 1.2.13.51. Usar aprendizado de máquina para detectar automaticamente os componentes e detectar anomalias nos serviços mapeados.

### **1.3. Information Technology Operations Management (ITOM)**

#### **1.3.1. Módulo de Monitoração e Gerenciamento de Infraestrutura de TI**

#### 1.3.1.1. Arquitetura

- Os módulos que compõem a solução devem suportar a instalação de agentes em ambientes Windows e Linux:
  - Windows 2000, 2003, 2008, 2012, 2016, 2019, 2022 ou superior
  - Windows 7, 10, 11 ou superior
  - CentOS 5.x, 6.x, 7.x, 8.x ou superior
  - Oracle Linux 7.x, 8.x ou superior
  - Linux - Debian 6.x, 7.x, 8.x, 9.x, 10.x ou superior
  - Linux - RedHat 5.x, 6.x, 7.x, 8.x ou superior
  - Fedora 8
  - OpenBSD
  - FreeBSD
  - Solaris 10.x, 11.x ou superior
  - Ubuntu 16.04, 18.04, 20.04, 22.04 ou superior
  - Linux SUSE
- A solução proposta deve possuir agente para banco de dados Microsoft
  - MySQL 5.0 a 5.7, 8 ou superior
  - SQL Server 2000, 2005, 2008, 2012, 2014, 2017, 2019, 2022 ou superior
- A solução proposta deve possuir agente para banco de dados PostgreSQL
  - PostgreSQL 8.x a 14x ou superior
- A solução proposta deve possuir agente para banco de dados MongoDB
  - MongoDB 4.2, 4.4 ou superior
- A solução proposta deve possuir agente para banco de dados Oracle
  - Oracle 10, 11, 12, 19, 21c ou superior
- A solução deverá suportar o gerenciamento de ambientes virtuais, como o Vmware 6.5 e 6.7 ou superior
- Deve prover suporte para monitoramento das soluções de backup corporativo.

1.3.1.2. Deverá permitir a visão centralizada do estado de saúde (desempenho e disponibilidade) dos serviços de negócios suportados pela TI.

1.3.1.3. A solução deverá ser multitenancy

1.3.1.4. Permitir a criação de controles de acesso baseado em papéis multitenancy

1.3.1.5. Deve prover suporte para monitoramento das soluções de backup corporativo.

1.3.1.6. Permitir a monitoração em diferentes ambientes, incluindo físicos, virtuais, nuvem pública, nuvem privada, contêineres e microsserviços;

1.3.1.7. Possuir uma interface centralizada para configuração de todos os coletores externos;

1.3.1.8. Ter solução compatível para dispositivos móveis, que seja responsiva.

1.3.1.9. Capacidade de automonitoramento de todos os componentes da solução para identificação precoce de falhas e incidentes quanto ao uso de funcionalidades contratadas e respectivos níveis de serviço contratualmente exigidos.

1.3.1.10. A plataforma de gerenciamento de eventos deverá coletar os dados diretamente no dispositivo monitorado, com ou sem agente.

1.3.1.11. Dever suportar a análise inteligente detectando tendências, padrões e anomalias e enviando alertas preditivos antes que as baselines sejam violadas.

1.3.1.12. Deve realizar a correlação de eventos com AI e ML, gerenciamento de situação e isolamento da causa raiz para redução do MTTR

- 1.3.1.13. Deve permitir consolidar, correlacionar e analisar eventos de todas as ferramentas de monitoração para apresentar em tempo real informações sobre a saúde dos serviços de negócio e sua infraestrutura.
- 1.3.1.14. Deve permitir a criação de mapa de calor para a monitoração dos serviços, fornecendo uma visualização fácil e rápida do “status” dos serviços monitorados.
- 1.3.1.15. Deve possuir capacidade de consolidação de eventos e falhas (redução de ruído) para evitar a proliferação de múltiplos alertas para uma mesma origem.
- 1.3.1.16. Deve possuir mecanismo de inteligência artificial para geração de análise preditiva de falhas.
- 1.3.1.17. Possuir separação entre eventos e alertas. Eventos serão as notificações informadas por uma ou mais fonte externa/ferramentas de monitoração (Zabbix, Nagios, vCenter, Traps SNMP, e-mail, etc.) as quais indicam algo que ocorreu no ambiente que necessita ser registrado, como logs, warning ou erro. Alertas serão um ou mais eventos que serão destacados que possuem relevância para ser tratados e gerenciados, pois requerem mais atenção.
- 1.3.1.18. Deverá oferecer gerenciamento de eventos abrangente que permite descobrir, analisar, correlacionar e resolver problemas em aplicativos e dispositivos a partir de um único console.
- 1.3.1.19. Deve integrar com as ferramentas padrões de Mercado de monitoração nativamente utilizando os seguintes tipos de conexão, REST API, SNMP, ou JavaScript customizado.
- 1.3.1.20. Deve permitir usar a ingestão de evento via Rest API para enviar eventos de aplicações de terceiros para a solução de monitoramento, permitindo:
  - Gerenciar classes de eventos:
    - Criar uma classe de evento
    - Atualizar uma classe de evento
    - Eliminar uma única classe de evento por ID
    - Obter detalhes de todas as classes de eventos e detalhes de seus inquilinos
    - Obtenha detalhes de uma única classe de evento
  - Gerenciar dados de eventos:
    - Enviar eventos de terceiros para a solução de monitoramento
    - Atualizar um evento
    - Busca de eventos
  - Gerenciar operações de eventos:
    - Atribuir/designar eventos
    - Estabelecer prioridade para os eventos
    - Tomar responsabilidade dos eventos
    - Declinar a propriedade dos eventos
  - Adicionar notas aos eventos
    - Reconhecer (acknowledge) os eventos
    - Desconhecer (unacknowledge) um evento
- 1.3.1.21. Permitir a integração através de conectores prontos com: Microsoft SCOM, Nagios, vCenter, vRealize e Zabbix).
  - Permitir integração aberta com ferramentas de terceiros, inclusive para abertura automática de chamados.
- 1.3.1.22. Possuir uma arquitetura que permita separar os eventos recebidos, classificar e identificar quais dos eventos serão criados dos alertas que realmente necessitam de atenção do time de operação. evitando excesso de trabalho no volume de eventos das diversas fontes de informação.

- 1.3.1.23. Permitir que o evento original deve ser mantido, para revisão ou remediação.
- 1.3.1.24. Possuir mecanismos para ver todos os eventos que estão vindo de fontes de monitoração ou de outras fontes como Traps SNMP e email.
- 1.3.1.25. Permitir criar regras de eventos para gerar alertas.
- 1.3.1.26. A solução deverá emitir alertas preditivos, antes que as linhas base sejam alcançadas;
- 1.3.1.27. Permitir a criação de políticas de blackout, ou seja, para que eventos sejam ignorados em um período específico.
- 1.3.1.28. Deverá permitir copiar uma regra de evento existente, trazendo as informações da regra original.
- 1.3.1.29. Por padrão deverá associar um evento a um IC, porém deve permitir ajustar a regra para sobrepor esse padrão para associar um evento a um alerta de um tipo de IC diferente.
- 1.3.1.30. Quando um evento passar por uma regra de evento que deverá gerar um alerta, um alerta deverá ser criado. Cada alerta deverá possuir um número identificador único e um workflow específico para seu ciclo de vida.
- 1.3.1.31. Deverá oferecer gerenciamento de eventos abrangente que permite descobrir, analisar, correlacionar e resolver problemas em aplicativos e dispositivos a partir de um único console.
- 1.3.1.32. A criação de políticas de correlação de eventos deverá ser baseada em regras definidas pelo administrador e também podendo ser de acordo o aprendizado de máquina e o uso de inteligência artificial;
- 1.3.1.33. Deverá oferecer integrações nativas com soluções de monitoramento de mercado (para receber eventos e / ou métricas), bem como permitir a criação de novos intervalos.
- 1.3.1.34. Deverá oferecer recursos para monitorar os diferentes elementos da infraestrutura de TI, minimamente: servidores físicos e virtuais, sistemas operacionais Windows e Linux, containers, storage, banco de dados, aplicações, web servers, Application Servers, sistemas operacionais e aplicações clusterizadas, bases de dados não estruturados, etc., instalados em nuvens privadas ou públicas (Amazon AWS, Google Cloud, MS Azure ou Oracle OCI).
- 1.3.1.35. Deverá oferecer suporte para criação de visões, Dashboards e relatórios sem que os usuários necessitem de conhecimento de programação.
- 1.3.1.36. Deverá oferecer Dashboards e relatórios de acesso Web, com visibilidade de todos os elementos monitorados desde diferentes perspectivas (serviço, infraestrutura etc.), além de oferecer relatórios e Dashboards prontos para uso (OOTB) e permitir criar, exportar e compartilhar relatórios e painéis interativos com usuários dentro ou fora do mesmo ambiente.
- 1.3.1.37. Deverá permitir o agrupamento de Dispositivos e / ou Eventos, seja manualmente ou por meio de regras. Esses grupos serão usados na Operação e Administração da solução.
- 1.3.1.38. Deve ser capaz de apresentar os Serviços / Aplicativos existentes, sua topologia e os incidentes e mudanças que os afetam.
- 1.3.1.39. Permitir a configuração de visualizações por eventos, dispositivos e grupos de entidades específicos para monitorar a saúde da infraestrutura e responder a eventos críticos com mais rapidez.
- 1.3.1.40. Deverá permitir baixar, configurar e executar a sincronização de grupos e usuários de um LDAP com a solução,

- 1.3.1.41. Deverá realizar a Autenticação e Autorização de Usuários, por meio de uma solução SSO (Single Sign On), oferecendo definição de funções, perfis e acessos e suportando os seguintes métodos: SAML 2.0, LDAP, Kerberos, baseada em certificado, OAuth 2.0 e OpenID Connect.
- 1.3.1.42. Deverá ter capacidade de monitorar as seguintes métricas de servidor físico e virtual: Consumo(s) de CPU, Consumo de memória (física, swap, etc.), Disponibilidade de PING, Espaço em disco e suas partições (discos físicos, lógicos e externos), Paginação e uso de swap, Uso e status da (s) interface (s) de rede, Processos específicos, Serviços específicos, Portas específicas (80, 8080, 21, 22, etc.), serviço DNS, DHCP (valida se o serviço DHCP está ativo, monitorando e status dos pools), estatísticas e histórico de desempenho.
- 1.3.1.43. Deverá suportar o monitoramento de : Banco de dados: PostgreSQL, SQL Server, Oracle, MySQL e MongoDB. Cluster: Disponibilidade, discos e processos. URL's: Disponibilidade e tempo de resposta. Ambiente virtual Oracle VM: Desempenho, Recursos e disponibilidade. Supercluster Oracle: Desempenho, Recursos e disponibilidade.
- 1.3.1.44. Deverá suportar o monitoramento dos seguintes ambientes virtuais: VMware vSphere (Datacenters, Clusters, Hosts, máquinas virtuais (VMs), pools de recursos, VMware vApps, Datastores), Microsoft System Center (grupos de hosts, clusters, hosts, máquinas virtuais), Red Hat, Oracle VM e Citrix XenServer.
- 1.3.1.45. Deverá permitir realizar testes remotos com base em um dos seguintes protocolos: Monitores SNMP, Monitor ICMP- Ping, Monitor de porta, monitor DNS.
- 1.3.1.46. Suporte para monitoramento de sistemas de storage corporativo e dispositivos de rede SAN. Performance, Utilização e Disponibilidade de disco.
- 1.3.1.47. Suporte para monitoramento de redes. A solução deve utilizar as informações disponíveis para ajudar na descoberta da rede. A solução deve suportar uma ampla amostra de dispositivos dos principais fabricantes. Possibilitar a criação de dashboards de redes, possibilitando visualização de dados de disponibilidade, performance, compliance e risco dos dispositivos de rede. Permitir a monitoração de desempenho e falhas de interfaces de rede, além de suas conexões. A solução deve descobrir VLANs definidas no ambiente, bem como a quantidade de dispositivos/interfaces associados. A solução deve descobrir e associar todos os endereços L2 e L3 com cada interface ou portas descobertas. A solução deve ser capaz de fornecer uma visão de fluxo de tráfego de rede. A ferramenta deve ter a capacidade de descoberta e identificação de todos os dispositivos e seus componentes na rede. Capacidade de pesquisar topologia de rede para o endereço IP .A solução deve fornecer mapas de topologia com capacidade de zoom-in / zoom-out. A solução deve ser capaz de se comunicar com tecnologias de redes utilizando os seguintes protocolos: SNMPv1, SNMPv2, SNMPv3, TCP/IP, UDP, ICMP. Representar a topologia descoberta graficamente. A solução deve ser capaz de suportar MIBs para auxiliar na monitoração de dispositivos. Deve permitir a importação de definições a partir de arquivos (MIB files), em extensão ou reposição aos previamente armazenados. A solução deve inclusive ser capaz de monitorar MPLS, VPN, IPT, e Multi Cast. A solução deve ser capaz de monitorar tráfego de rede. A solução deve ser capaz de fazer coleta de dados de diagnóstico. Suportar dispositivos no padrão Ipv6. A solução deve fornecer a capacidade de descobrir e monitorar protocolos padrão da indústria tais como EtherChannel, MLT, SMLT .A solução deve fornecer a capacidade de descobrir e monitorar protocolos padrão da indústria tais HSRP, VRRP. Protocolos devem incluir ARP, DNS, SNMP, BGP, EIGRP, OSPF e LLDP (link em nível de protocolo de descoberta).
- 1.3.1.48. Deverá suportar o monitoramento de containeres: Kubernetes e Docker (hosts Docker, containers Docker, swarm Docker).
- 1.3.1.49. Deverá permitir monitorar e gerenciar a disponibilidade e o desempenho de um ambiente

OpenShift, emitir avisos visuais e alarmes quando os limites são excedidos, permitindo fácil identificação de áreas problemáticas. As seguintes entidades podem ser monitoradas no OpenShift: Nós, Projetos, Operadores de cluster, Controladores e Pods.

- 1.3.1.50. Deverá oferecer suporte ao monitoramento de dispositivos de armazenamento da CONTRATANTE.
- 1.3.1.51. A solução deve permitir a coleta e análise do fluxo de tráfego das interfaces dos equipamentos de rede através de NetFlow

### **1.3.2. Módulo de Inteligência artificial para Operações de TI – AIOps**

- 1.3.2.1. Deve agregar uma camada de inteligência artificial e aprendizado de máquina ao módulo de Monitoração de infraestrutura e serviços.
- 1.3.2.2. Deve oferecer a capacidade de integração com diversas tecnologias de mercado, de forma gráfica e de configuração de mapas “de-para” entre os campos das soluções integradas.
- 1.3.2.3. Deverá conter minimamente a capacidade de ingestão de dados, reconciliação e updates dinâmicos
- 1.3.2.4. Deve permitir a modelagem dinâmica de serviço criando um modelo de infraestrutura de serviço que se mantém atualizado em tempo real.
- 1.3.2.5. Deve permitir encontrar a causa raiz de um problema utilizando mecanismos de inteligência artificial
- 1.3.2.6. Deve conter algoritmos pré-treinados para a identificação e recuperação de falhas no ambiente corporativo.
- 1.3.2.7. Deve sincronizar automaticamente com o CMDB para melhorar o gerenciamento de serviços, funções e atividades.
- 1.3.2.8. O modelo de serviço dinâmico deve alimentar painéis específicos de funções, que permitem que diferentes tipos de usuários vejam rapidamente a integridade dos serviços de negócios, aplicativos e infraestrutura específicos nos quais estão interessados.
- 1.3.2.9. Deve oferecer suporte a alertas de interrupção proativos para envio de alertas oportunos sobre possíveis problemas de desempenho, permitindo a atuação das equipes de TI antes que eles causem problemas
- 1.3.2.10. Deve conter recurso de reconciliação de topologia permitindo mesclar todos os seus dados ingeridos em um único modelo unificado de seu ambiente de serviço.
- 1.3.2.11. Deve permitir resolver conflitos de forma inteligente na representação de nomes e relacionamentos, criando uma fonte verdadeiramente abrangente e consistente.
- 1.3.2.12. Deve permitir que o modelo de serviços dinâmico se mantenha atualizado com os dados mais recentes de suas ferramentas. Qualquer alteração do ambiente deve acionar uma atualização imediata no modelo.
- 1.3.2.13. O modelo de serviço dinâmico deve estar sempre ativo e disponível podendo ser usado para alimentar painéis de integridade de serviço personalizados.
- 1.3.2.14. A modelagem de serviço dinâmico deve permitir ingerir dados de múltiplas fontes em seu ambiente conectando a fontes de dados baseadas em nuvem, locais, híbridas e de terceiros.
- 1.3.2.15. Construção automática de baselines a partir de inferência de padrões de uso de recursos

computacionais, mediante análise corrente e histórica de dados e informações provenientes de coleta de métricas e dados dos elementos monitorados, com a finalidade de detecção de anomalias e situações de alarme.

1.3.2.16. Geração de alarmes de forma automática, de acordo com baselines e sazonalidade dos recursos computacionais monitorados que, ainda, poderão, se o caso, ser ajustados ou reconfigurados manualmente pelo usuário ou pelas observações/inferências da ferramenta de AIOps (seasonal anomaly detection).

1.3.2.17. A ferramenta de observabilidade/AIOps deve ser capaz de identificar padrões anômalos de comportamento relacionados à ocorrência de incidentes na infraestrutura de rede que ocasionem lentidão no tráfego ou problemas de acesso a serviços ou à ocorrência de incidentes, problemas de acesso, lentidão ou negação de serviço na infraestrutura de banco de dados e aplicações, dentre outras possibilidades e casos de uso que possam ser definidos com base nos dados e informações.

#### 1.4. Módulo de Gestão de Capacidade

1.4.1. A solução deverá conter módulo de Análise de consumo dos servidores, utilizando inteligência e análise preditiva para gerenciar recursos e aplicações de TI, incluindo aquelas baseadas em Kubernetes e pods, microserviços, containeres e serviços multi-nuvem.

1.4.2. Deve permitir obter uma visão geral da utilização de recursos tecnológicos para seus serviços comerciais a fim de analisar a capacidade no nível do pool de serviços ou de implantação.

1.4.3. Deve criar e utilizar KPI's de negócios e simulações de "e se" para determinar com precisão as necessidades de recursos para mudanças futuras na demanda de negócios.

1.4.4. Deve fornecer informações para que a contratante possa fazer o melhor uso dos recursos locais e multi-nuvem.

1.4.5. Deve fornecer recomendações proativas baseadas em algoritmos de AI & ML para otimizar recursos e gerenciar riscos

1.4.6. Deve permitir simular cenários de uso para migração para a nuvem fornecendo as recomendações de tamanho correto que lhe permitam rever estimativas de custos futuros e tendências de custos da migração de servidores no local para a nuvem pública.

1.4.7. Deve permitir calcular e programar a quantidade de recursos necessários para a execução de novos serviços e aplicações de negócio.

1.4.8. Deve fornecer a visibilidade da capacidade de recursos, da utilização e das tendências de utilização.

1.4.9. Deve, a partir dos dados de infraestrutura coletados pelo módulo de monitoração, entender o uso e o desempenho de seus elementos de infraestrutura, determinar se os elementos de infraestrutura são usados de forma otimizada e eficiente ou estão em risco, e permitir planejar as necessidades futuras de capacidade.

1.4.10. Deve permitir a visibilidade do uso e da disponibilidade de todos os recursos de infraestrutura, onde quer que estejam, localmente e/ou na nuvem pública.

- Deve permitir gerar / criar as seguintes visões:

- **Visão por serviços:**

- Gerar a visão de Serviços para obter um resumo consolidado dos serviços de negócio em sua infraestrutura e para compreender a saúde geral e a situação dos serviços.
- Permitir pesquisar por serviços específicos e visualizar os aplicativos associados, os pools de serviços (para nuvem e no local), ou os detalhes de implantação (para Kubernetes).
- Permitir analisar a capacidade no nível do pool de serviços ou da implantação.

- Produzir indicadores de Risco, Utilização e Dias de saturação para cada pool de serviços ou implantação definida com base nos valores dos indicadores dos servidores ou pods contidos respectivamente.
- **Visibilidade de recursos em Nuvem:**
  - Devem permitir visualizar e gerenciar a capacidade de entidades, instâncias, volumes, máquinas virtuais na infraestrutura de nuvem, fornecendo uma visão geral da capacidade disponível, utilização, tendências e capacidade residual em termos de CPU, memória e utilização de datastore para cada entidade.
- **Visibilidade de Kubernetes**
  - Deve identificar e compreender os gargalos de recursos e a capacidade residual agregada dos grupos Kubernetes, bem como os nós individuais
  - Detectar condições atuais ou iminentes de saturação de recursos e dias antes que o recurso esteja saturado para cada recurso Kubernetes importante (por exemplo: agrupamento, nós, implantações, cápsulas)
  - Deve permitir avaliar o nível de eficiência da infraestrutura, comparando os recursos alocados com os recursos reais, e identificar a maioria das implantações ou vagens de desperdício
  - Identificar a aplicação em padrões de uso de recursos e detectar condições de escassez de recursos
  - Deve compreender a utilização de recursos de namespaces, incluindo o nível de utilização das quotas de recursos
  - Resolver questões que são identificadas para seu ambiente Kubernetes, fornecendo um conjunto de ações recomendadas
- **OEM - Oracle Database Cluster e seus anfitriões**
  - Deve obter uma visão geral da utilização dos clusters e de seus servidores de banco de dados
  - Deve permitir acessar métricas detalhadas para clusters de bancos de dados, instâncias, servidores e grupos de discos
  - Identificar espaços em tabelas de banco de dados e status de grupos de discos e detectar condições de escassez de recursos
  - Deve entender as tendências e utilizações atuais dos Real Application Clusters (RAC) da Oracle
- **Visibilidade de Servidores**
  - Deve permitir gerenciar a capacidade e o desempenho dos seguintes sistemas:
  - Máquinas UNIX ou Windows rodando diretamente no hardware com coleta de dados do agente.
  - Máquinas virtuais Windows ou Linux com coleta de dados de agentes de dentro das máquinas virtuais. Estes sistemas devem aparecer como tipo de nó virtual
    - Hyper-V
    - KVM
    - VMware
    - Xen
- **Visibilidade do Explorador de dados**
  - Deve fornecer uma visão chamada de “Servers Data Explorer” mostrando o comportamento de métricas de desempenho específicas da entidade sob períodos de tempo fixos e personalizados.
  - Devem mostrar a utilização de recursos das principais métricas, tais como, Número de núcleos de CPU, % de utilização de CPU, % de utilização de memória, % de utilização de memória real, % de utilização de sistemas de arquivo, Taxa de E/S do disco, entre outros.
  - Deve permitir filtrar os dados.
  - Deve gerar métricas categorizadas com base em diferentes perfis e agrupadas em abas separadas.
- **Visibilidade do Storage-Host**

- A visão Hosts permite verificar a capacidade inicialmente alocada aos hosts e determinar a capacidade que é realmente consumida por cada hosts.
- Hosts
- Hosts de sistemas
- Hosts dos Pools
- Hosts para Volumes
- Tabela de Mapeamento de Volumes.
- **Visibilidade de Storages Systems**
  - A visão Sistemas de Armazenamento permite realizar todas as operações básicas de gerenciamento graças às valiosas informações coletadas sobre os sistemas de armazenamento, arquivadores de armazenamento, pools de armazenamento, volumes de armazenamento e ações de armazenamento presentes em seu ambiente:
    - Storage Systems
    - Filers
    - Pools
    - Volumes
    - Shares

### **1.5. Automação de tarefas**

- 1.5.1. Permitir controle dos processos em tempo real, mostrando seu status e apresentando informações relativas ao tempo de execução realizado e previsto para finalização.
- 1.5.2. Possuir interfaces de relatórios gráficos com informações gerenciais e de auditoria.
- 1.5.3. Demonstrar de forma proativa a predição dos fluxos de processamento, permitindo assim uma análise profunda, e prevenindo resultados indesejáveis nos serviços.
- 1.5.4. Deverá proativamente detectar potenciais atrasos e erros em serviços críticos gerenciados.
- 1.5.5. Permitir ações corretivas antes de o serviço crítico causar impacto.
- 1.5.6. Deverá ser nativamente integrado com a solução de gestão de serviços de TI (ITSM) permitindo a adição de tarefas automatizadas no catálogo de serviços para que sejam executadas diretamente pelos próprios usuários finais.
- 1.5.7. Deverá permitir uso de filtros para mostrar uma visão detalhada com foco em serviços específicos.
- 1.5.8. Permitir criação de diversos perfis de utilização com permissões distintas e segmentadas por grupo, tenant e função.
- 1.5.9. Deve oferecer a visualização da interdependência entre jobs/tarefas em diferentes plataformas / sistemas.
- 1.5.10. Deve permitir a seleção múltipla de jobs para realizar ações em massa.
- 1.5.11. Deve permitir marcar os jobs mais acessados ou críticos para localizar e acessar rapidamente.
- 1.5.12. Deve ser capaz de reiniciar os jobs pela interface gráfica automaticamente através de uma ação corretiva definida no job ou através de ação manual efetuada por um usuário autorizado.
- 1.5.13. Deve permitir a classificação de jobs em hierarquia com base nas aplicações e processos.
- 1.5.14. Deve oferecer um console de alertas dedicado e um painel de status de SLA para operadores e usuários da interface web.
- 1.5.15. Permitir envio de alertas via e-mail e notificação.

- 1.5.16. Deve distinguir jobs críticos dos não críticos, especialmente aqueles vinculados a um processo de SLA.
- 1.5.17. Deve fornecer assistente de gerenciamento de calendário centralizado.
- 1.5.18. Deve fornecer a capacidade de clicar e conectar dois jobs para estabelecer dependência entre eles.
- 1.5.19. Deve permitir definir a janela de tempo dentro da qual o job deve ser enviado para execução, se a janela falhar, o job não poderá ser iniciado.
- 1.5.20. Deve ser capaz de configurar os jobs para iniciar a execução com base nas seguintes condições:
  - Ad-hoc (sob demanda por um usuário).
  - Data e hora (Data e hora específicas).
  - Time window (apenas enviar dentro de uma janela de tempo específica).
  - Job do Predecessor concluindo com sucesso.
  - Disponibilidade de recursos (física e lógica).
  - Evento externo (gatilho API da aplicação).
  - Visualização de arquivos (criação, exclusão, modificação de arquivos específicos).
  - Um outro job que termine com um código de retorno específico.
- 1.5.21. Deve suportar o parâmetro do fuso horário para indicar o tempo de início / término definidos nos jobs.
- 1.5.22. Deve oferecer a capacidade de configurar uma janela de período ativo para o job, onde o job específico estará ativo apenas por esse período e será desativado automaticamente após a passagem da janela ou executado de forma contínua por determinado período.
- 1.5.23. Deve permitir que os usuários definam os alertas em todos os jobs para as condições abaixo:
  - Se o job não for enviado ou não for concluído por um certo tempo.
  - Se o tempo de execução do job exceder uma duração definida ou o seu tempo médio de execução.
  - Se o job foi concluído com muita rapidez.
  - Se o job falhou ou foi reiniciado.
  - Se o job finalizou com sucesso ou com código de retorno específico.
  - Se o número de falhas do job exceder uma certa contagem.
  - Se a saída do job não for encontrada.
- 1.5.24. Deve permitir capturar os dados específicos da saída do job para serem armazenados em uma variável a ser passada como um parâmetro de entrada para outros jobs.
- 1.5.25. Deve determinar o status do final do job com base no Código de retorno do script ou código específico que aparece nos registros de saída do job.
- 1.5.26. Deve ter um mecanismo de SLA para amarrar o fluxo do processo de negócios em lote até um prazo específico para garantir que os jobs que são críticos concluam a tempo sem impacto para a empresa.
- 1.5.27. Deve permitir usar as variáveis do sistema como parâmetros de entrada dos jobs.
- 1.5.28. Deve ter capacidade de calcular datas e passá-la para os jobs.
- 1.5.29. Deve permitir que os usuários executem a definição do fluxo de job em qualquer um dos casos abaixo:
  - Crie o fluxo de job a partir do zero.
  - Carregue jobs existentes e faça as alterações conforme necessário.
  - Carregar os jobs do JSON exportado de outros ambientes.
- 1.5.30. Deve fornecer a capacidade de validar a programação definida nos jobs antes de sua execução em produção para garantir que o critério estabelecido no job seja atendido.
- 1.5.31. Deve identificar o caminho crítico mapeando todos os jobs responsáveis pelos níveis de serviço SLA e enviar uma notificação proativa após atraso ou falha.
- 1.5.32. Deve oferecer a simulação preditiva para os jobs que ainda não foram executados com o tempo estimado

de início e término exibindo na interface gráfica.

- 1.5.33. Deve fornecer o tempo de início e o tempo de término estimado para todos os jobs carregados para serem executados com base em suas informações estatísticas históricas.
- 1.5.34. Deve agrupar estatísticas do tempo de execução com base nas tendências e execuções separadas.
- 1.5.35. Deve oferecer a capacidade de tomar algumas das ações-chave nos jobs pelos usuários da aplicação, tais como: reexecutar jobs com falha e finalizar o job no status de execução, se autorizado.
- 1.5.36. Deve oferecer recursos de transferência segura de arquivos para as plataformas Linux, Windows e Unix, bem como suportar todos os protocolos compatíveis com o FIPS padrão da indústria, como FTP, SFTP, FTPS etc.,
- 1.5.37. Deve oferecer a autenticação e criptografia da chave SSH para transferências de arquivos protegidos.
- 1.5.38. Deve oferecer um painel de controle dedicado para monitorar o status da transferência de arquivos.
- 1.5.39. Deve alertar de forma proativa se houver qualquer latência de rede ou problemas em alguns dos principais sistemas que podem causar atrasos nas transferências de arquivos.
- 1.5.40. Deve permitir utilizar e gerenciar credenciais para todos os pontos finais de FTP a partir de um console de administrador centralizado.
- 1.5.41. Deve oferecer um console centralizado para os servidores de FTP e para as máquinas de destino onde os serviços do servidor FTP devem ser instalados.
- 1.5.42. Deve permitir reiniciar as transferências de arquivos a partir do ponto de falha.
- 1.5.43. Deve permitir confirmar que os arquivos estejam presentes antes de serem transferidos para o destino.
- 1.5.44. Deve permitir que os usuários definam a transferência de arquivos também como parte do processamento de lote de negócios com o monitoramento de prazo de SLA.
- 1.5.45. Deve se integrar com a gestão de mudanças para a aprovação ou não da execução de jobs.
- 1.5.46. Deve permitir a aplicação de padrões para o controle de qualidade na criação e definição de jobs.
- 1.5.47. Deve fornecer uma opção para acessar o registro do job, incluindo o resultado do job nas execuções passadas históricas da interface gráfica.
- 1.5.48. Deve ser capaz de simular as definições de jobs validando previamente à execução.
- 1.5.49. Deve fornecer o tempo estimado dinâmico de início e final para os jobs na simulação com base nas estatísticas anteriores do histórico de execução.
- 1.5.50. Deve oferecer uma capacidade para controlar a versão de todas as mudanças nas definições do job.
- 1.5.51. Deve permitir comparar duas versões e gerar relatório para fins de auditoria nas mudanças feitas.
- 1.5.52. Deve fornecer a opção de visualizar todas as alterações feitas nas definições do job dentro de um período e fornecer uma opção para restaurar em massa todas as alterações feitas nessa janela.
- 1.5.53. Deve permitir habilitar a auditoria para ações de usuário selecionadas.
- 1.5.54. Deve oferecer relatório de auditoria com campos e operações personalizáveis.
- 1.5.55. Deve fornecer a informação de quem fez alterações, quais os campos e as informações alteradas e por que as alterações foram realizadas no relatório completo de auditoria.
- 1.5.56. Deve fornecer a capacidade de criar perfis de usuários ou grupos de usuários para limitar os privilégios no

nível de membro do usuário ou grupo para poder programar / monitorar os jobs.

- 1.5.57. Deve ser capaz de se integrar com o servidor Active Directory ou LDAP para a autenticação.
- 1.5.58. Deve permitir distribuição centralizada de correções/atualizações para os componentes do agendador.
- 1.5.59. Deve suportar as diferentes distribuições do Unix, Linux, Windows no ambiente virtual, físico e cloud.
- 1.5.60. Dever ter capacidade de integração com qualquer banco de dados que ofereça driver JDBC.
- 1.5.61. Deve ser capaz de ativar o job com base na criação, modificação ou exclusão de um arquivo.
- 1.5.62. Deve fornecer a capacidade de renomear, excluir ou mover o arquivo antes de disparar o job.
- 1.5.63. Deve suportar wildcards na busca de arquivos e/ou busca por data e hora no nome do arquivo.
- 1.5.64. Deve ser capaz de alertar quando o arquivo não for criado ou modificado dentro do horário estabelecido.
- 1.5.65. Deve fornecer a opção de reter os jobs que aguardam dependências durante a janela definida pelo usuário.
- 1.5.66. Deve permitir definir uma única agenda a ser usada para todos os jobs em todas as plataformas.
- 1.5.67. Deve ter a opção de escolher os dias úteis e os dias não úteis para o ano civil.
- 1.5.68. Deve permitir a personalização de relatórios no sistema de agendamento com a opção de escolher os campos a serem incluídos ou excluídos no relatório (inclusive via dispositivos móveis).
- 1.5.69. Deve suportar, pelo menos, os seguintes tipos de relatórios via dispositivos móveis:
  - 1.5.70. - Relatórios de horários de execução de tarefas de produção.
  - 1.5.71. - Relatório de tarefas em execução.
  - 1.5.72. - Relatório de análise de nível de serviço.
  - 1.5.73. - Relatório de análise de tendências e previsibilidade de execução de tarefas.
  - 1.5.74. - Relatório de distribuição da carga de job.
  - 1.5.75. - Relatório de falhas.
  - 1.5.76. - Relatório de auditoria e compliance.
- 1.5.77. Deve permitir gerar relatórios exportados para os vários formatos de arquivo, como PDF, CSV, XLS ou XLSX.
- 1.5.78. Deve possuir interface para dispositivos móveis intuitiva com usabilidade sem detalhes técnicos permitindo que áreas gerenciais possam utilizá-los de forma intuitiva.
- 1.5.79. Deve permitir ao usuário de forma remota e através de dispositivos móveis, ter controle geral sobre a execução da carga de job, podendo monitorar o andamento em tempo real, incluindo a capacidade de aprovar horários e alterá-los conforme necessário.

## **1.6. Solução Information Technology Asset Management (ITAM)**

- 1.6.1. Gestão do Ciclo de Vida do Ativo
  - 1.6.1.1. 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.

- 1.6.1.2. 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.
- 1.6.1.3. 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.
- 1.6.1.4. 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.
- 1.6.1.5. Deverá permitir o gerenciamento de licenças de software entendendo o uso da licença de software e os passivos financeiros associados.
- 1.6.1.6. 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.
- 1.6.1.7. Deverá permitir o gerenciamento de eventos rastreando e automatizando a correção de forma proativa quando eventos importantes de infraestrutura ocorrerem.
- 1.6.1.8. 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).
- 1.6.1.9. Deverá permitir visualizar, controlar, monitorar e atualizar todos os principais softwares antivírus e anti spyware de uma única fonte.
- 1.6.1.10. 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.
- 1.6.1.11. Deverá permitir o gerenciamento do consumo de energia do PC.
- 1.6.1.12. 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.
- 1.6.1.13. 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.
- 1.6.1.14. 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.
- 1.6.1.15. Deverá permitir a geração de inventário de seus ativos de TI identificando exatamente como esses ativos estão sendo usados.
- 1.6.1.16. Deverá permitir implantar, atualizar e corrigir facilmente sistemas operacionais e aplicativos através da instalação e distribuição remota de software.
- 1.6.1.17. 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.

- 1.6.1.18. Deverá permitir acessar remotamente todos os dispositivos, mesmo aqueles não conectados via VPN.
- 1.6.1.19. 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.
- 1.6.1.20. 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.
- 1.6.1.21. 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.
- 1.6.1.22. 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.
- 1.6.1.23. 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.
- 1.6.1.24. 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.
- 1.6.1.25. Deverá permitir integrar os dados do cliente à central de atendimento.
- 1.6.1.26. 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.
- 1.6.1.27. Deve permitir analisar automaticamente o ambiente de TI, identificando quais dispositivos estão faltando quais patches.
- 1.6.1.28. 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.
- 1.6.1.29. Deverá permitir atualizações automáticas de boletins de segurança através da configuração de
- 1.6.1.30. downloads e atualizações para o catálogo de boletins de vulnerabilidades e patches.
- 1.6.1.31. 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.
- 1.6.1.32. Deverá permitir visualizar uma lista de patches ausentes por dispositivo com seu nível de gravidade.
- 1.6.1.33. 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.

- 1.6.1.34. Deverá permitir a criação de grupos dinâmicos direcionando grupos de dispositivos para atualizações com base nos requisitos de patch e nos atributos do computador.
- 1.6.1.35. Deverá permitir monitorar o processo de correção em tempo real e fornecer informações detalhadas sobre quaisquer erros ou anomalias para que possam ser tomadas medidas corretivas imediatas.
- 1.6.1.36. 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.
- 1.6.1.37. Deverá prover a medição de software acompanhando o uso real de qualquer aplicativo e reimplementando licenças de software não utilizadas para outros usuários.
- 1.6.1.38. Deverá permitir a criação de grupos dinâmicos, identificando, agrupando e corrigindo os dispositivos que não seguem as políticas de conformidade definidas.
- 1.6.1.39. Deverá permitir a descoberta de ativos com agente e sem agente com informações detalhadas de configuração.

#### 1.6.2. Gestão do Controle Remoto do Ativo

- 1.6.2.1. 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.
- 1.6.2.2. 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.
- 1.6.2.3. 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.
- 1.6.2.4. Deve ser possível transferir arquivos entre os dispositivos locais e remotos, facilitando o compartilhamento de documentos, patches de software, atualizações e outros arquivos relevantes.
- 1.6.2.5. Deverá suportar mecanismos de Multicasting e gerenciamento de largura de banda de rede nos processos de atualização e gerenciamento remoto de dispositivos.
- 1.6.2.6. Deverá permitir a Implantação e atualizações do agente de forma automática para máquinas recém-descobertas.
- 1.6.2.7. Deverá suportar a instalação remota do sistema operacional Windows, incluindo formatação/particionamento de discos rígidos.
- 1.6.2.8. Deverá permitir a criação de um catálogo baseado na Web de software aprovado para instalações de auto-atendimento após a migração.
- 1.6.2.9. Deverá permitir a execução de linha de comando, transferências de arquivos, gerenciamento

da área de transferência e reinicialização do dispositivo de destino.

- 1.6.2.10. Deverá manter trilha de auditoria de sessões de controle remoto e reconhecimentos do usuário final.
- 1.6.2.11. 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.
- 1.6.2.12. 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.
- 1.6.2.13. 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.
- 1.6.2.14. 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.
- 1.6.2.15. 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.
- 1.6.2.16. 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.
- 1.6.2.17. 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.

## **1.7. Relatórios e Dashboards**

- 1.7.1. Deve incluir relatórios pré-definidos para a geração de informações para a gestão dos serviços.
- 1.7.2. Deve permitir a criação de relatórios e painéis por meio de consultas customizadas.
- 1.7.3. Deve permitir exportar, importar e/ou baixar painéis e relatórios, para que sejam customizados e personalizados de acordo com a necessidade dos usuários.
- 1.7.4. Deve permitir exportar relatórios gerados em ao menos dois dentre os formatos a seguir: PDF, CSV, XLS ou XLSX.
- 1.7.5. Deve permitir estabelecer um cronograma/agendamento para envio de relatórios para endereços de e-mail externos ou internos e repositórios.
- 1.7.6. Deve permitir adicionar o logotipo e a marca da empresa nos relatórios que serão gerados e enviados periodicamente por e-mail.
- 1.7.7. Deve permitir adicionar links de drill-down em painéis, para se obter mais informações sobre seus dados em painéis específicos ou mais detalhados.

- 1.7.8. Deve permitir a adição de links de acesso aos registros da gestão de serviços em meio aos painéis e relatórios.
- 1.7.9. Deve permitir acesso aos relatórios e painéis por tenant, grupo, perfil, função e/ou cliente.
- 1.7.10. Deve permitir confecção de painéis adicionais e relatórios.
- 1.7.11. Geração automática de relatórios executivos.
- 1.7.12. Deve permitir a gestão e administração de maneira amigável de usuários, grupos, configurações, funções e auditoria.
- 1.7.13. Os relatórios e dashboards não devem causar impacto nos recursos da solução de ITSM.

## **1.8. Opções de Gráficos e Visualizações**

- 1.8.1. Permite visualizar os dados como diagramas em painéis.
- 1.8.2. Permite visualizar os dados como uma combinação de diagramas e gráficos em painéis.
- 1.8.3. Permite visualizar os dados como gráfico de pizza.
- 1.8.4. Permitir visualizar os dados como gráfico de barras.
- 1.8.5. Permitir visualizar os dados como gráfico de linhas.
- 1.8.6. Permitir visualizar os dados como gráfico de áreas.
- 1.8.7. Permite visualizar os dados como tabelas em painéis.
- 1.8.8. Permite visualizar os dados como registros em painéis.
- 1.8.9. Permite visualização de séries cronológicas.
- 1.8.10. Permite visualização como medidor (ponteiro).
- 1.8.11. Permite visualização em tabela, suportando vários modos para séries cronológicas, tabelas e dados em JSON.
- 1.8.12. Permite a visualização do painel Heatmap para a visualização de histogramas ao longo do tempo.
- 1.8.13. Deve permitir exibir alertas nos painéis.
- 1.8.14. Deve possuir gráfico de nó para visualizar gráficos orientados ou redes, de modo que possa exibir mapas complexos de infraestrutura, hierarquias ou diagramas de execução.
- 1.8.15. Deve permitir visualizar os dados em Semáforos.

**ANEXO II – MODELO DE ORDEM DE SERVIÇOS**

<p><b>ORDEM DE SERVIÇO Nº XXX/202X</b></p> <p><b>ABERTURA</b></p>				
<b>1. DADOS DO CONTRATO</b>				
CONTRATO Nº				
CONTRATADA		GESTOR TÉCNICO		
OBJETO		VIGÊNCIA		
DESCRIÇÃO	QUANTIDADE	UNIDADE	VALOR UNITÁRIO	VALOR TOTAL
<b>2. REGISTRO DA ABERTURA DA ORDEM DE SERVIÇO</b>				
Nº DO CHAMADO	DATA DO CHAMADO	RESPONSÁVEL PRODEB ABERTURA DA OS / MATRÍCULA	ÓRGÃO	
<b>3. DEFINIÇÃO DE ESCOPO DA ORDEM DE SERVIÇO - OS</b>				
DATA DA REUNIÃO	RESPONSÁVEL PRODEB	RESPONSÁVEL CONTRATADA		
DESCRIÇÃO				
SERVIÇO A SER ENTREGUE COM A DEVIDA DOCUMENTAÇÃO COMPROBATÓRIA				
<b>4. PLANEJAMENTO DA EXECUÇÃO DA ORDEM DE SERVIÇO-OS</b>				
DATA DE ENVIO CRONOGRAMA E TOTAL DE HORAS ESTIMADO	CRONOGRAMA ESTIMADO		Nº TOTAL DE HORAS ESTIMADO	
	DATA DE INÍCIO	DATA DE CONCLUSÃO		
<b>5. APROVAÇÃO DO PLANEJAMENTO DA ORDEM DE SERVIÇO - OS</b>				
ASSINATURA / CARIMBO RESPONSÁVEL CONTRATADA	ASSINATURA / CARIMBO GESTOR TÉCNICO PRODEB		DATA DA APROVAÇÃO PRODEB	
OBSERVAÇÃO: OS NÍVEIS DE SERVIÇO EXIGIDOS ESTÃO DESCRITOS NO ITEM ORIENTAÇÃO TÉCNICA DO Especificação Técnica.				

**ANEXO III - ITENS SUGERIDOS PARA O CATÁLOGO DE SERVIÇOS**

ITSM

**Atendimento**

Criar/Desativar conta na solução ITSM

Gerenciar contas de usuários

Fornecer Informações/Orientações

Configurar/Alterar chamados

**Administração**

Configurar opções/campos

Criar/Alterar Catálogo de serviços

Criar/Alterar Categorias de incidente/solicitação/problema/evento/mudança

Criar/Alterar perfis de usuários

Criar/Alterar Clientes

Criar/Alterar Tenants

Criar/Alterar Repositórios de anexos

Criar/Alterar Contratos

Criar/Alterar Turnos de trabalho

Criar/Alterar SLAs/OLAs

Criar/Alterar fluxos de trabalho (workflow)

Criar/Alterar documentos de conhecimento

Criar/Alterar ICs/Classes/Famílias

Criar/Alterar notificações

Criar/Alterar Grupos de atendimento

Criar/Alterar Locais

Criar/Alterar status e transições de status

Criar/Alterar matrizes de prioridade/risco/impacto/urgência

Criar/Alterar Filas de atendimento

Criar/Alterar modelos (templates)

Criar/Alterar avisos/anúncios

Documentar instrução de trabalho/procedimento operacional/tutorial

**Relatórios e painéis**

Disponibilizar acesso a Relatórios

Disponibilizar acesso a Painéis

Administrar contas de usuários

Criar/Alterar dashboards

Criar/Alterar relatórios

Automatizar geração/envio de relatórios

Criar e realizar consultas em bancos de dados

Configurar métricas e KPIs

**Resolução de Incidentes e Problemas**

Incidente na solução ITSM

Incidente em Relatórios

Incidente em Painéis

Problema na solução ITSM

Problema em Relatórios

Problema em Painéis

	<b>Desenvolvimento</b>
	Implementar customizações na ferramenta ITSM
	Homologar nova funcionalidade/customização
	Alterar chamados em lote
	Executar Requisição de mudança (RDM)
	Realizar integrações da ferramenta ITSM
	Desenvolver/executar scripts
	Criar/Alterar campos e formulários
	Criar/Alterar automações na solução ITSM
	<b>Gestão de Ativos</b>
	Criar/Desativar/Modificar Ativos de TIC
	Gerenciar contas de usuários no módulo de Gerenciamento de Ativos
	Fornecer Informações/Orientações sobre Ativos
	Configurar/Alterar Painéis, Parâmetros e configurações de ativos de TIC
	<b>Gestão da Solução de Controle Remoto</b>
	Criar/Desativar/Modificar usuários
	Gerenciar contas de usuários no módulo de Controle remoto
	Fornecer Informações/Orientações sobre acessos e logs de segurança
	Configurar/Alterar método de notificação
	Criar/Alterar Softwares de Auto-serviço
	Criar/Alterar Softwares de Categorias de Auto-Serviços
	<b>Administração da Solução de Ativos</b>
	Configurar opções/campos/categorias e layout de telas
	Criar/Alterar Catálogo de Ativos
	Criar/Alterar perfis de usuários e analistas
	Criar/Alterar Clientes
	Criar/Alterar Softwares de Auto-serviço
	Criar/Alterar Softwares de Categorias de Auto-Serviços
	Criar/Alterar Repositórios de anexos
	Criar/Alterar Contratos
	Criar/Alterar Fornecedores
	Criar/Alterar Garantias
	Criar/Alterar Classe/Família de Ativos
	Criar/Alterar fluxos de trabalho (workflow)
	Criar/Alterar notificações de Ativos Críticos e Não críticos
	Criar/Alterar Grupos Solucionador/Usuário/Cliente do Ativos
	Criar/Alterar Cliente/Departamento/Setor dos Ativos
	Criar/Alterar Informações de Campos de Hardware
	Criar/Alterar Informações de Campos de Software
	Criar/Alterar Informações de Campos de Hardware
	Criar/Alterar Informações de Software Licenciados e Não Licenciados
	Criar/Alterar Informações de Contratos e Garantia de Hardware
	Criar/Alterar Informações de Contratos e Garantia de Software
	Criar/Alterar modelos (templates de ICs)
ITAM	

	Criar instrução de Trabalho/procedimento de Conformidade com Normas de Segurança CIS Framework
	Criar instrução de Trabalho/procedimento de Conformidade com Normas de Segurança Internas
	<b>Relatórios e painéis</b>
	Relatório de Inventário de Ativos: Visão geral dos ativos de endpoint gerenciados pela solução.
	Relatório de Inventário de Ativos: Inclui informações como nome do dispositivo, sistema operacional, versão do software, hardware e detalhes de configuração.
	Relatório de Conformidade de Segurança: Avaliar o nível de conformidade dos endpoints com as políticas de segurança estabelecidas na Prodeb;.
	Relatório de Vulnerabilidades: Identificar as vulnerabilidades existentes nos endpoints gerenciados.
	Relatório de Desempenho de Endpoint: Apresentar métricas de desempenho dos endpoints, como utilização da CPU, memória e disco.
	Relatório de Incidentes e Problemas: Registra e acompanha os incidentes e problemas relatados pelos usuários vinculados aos Ativos
	Relatório de Utilização de Software:
	Relatório de Atualizações e Patches
	Relatório de Disponibilidade e Tempo de Atividade
	Criar/Alterar dashboards
	Criar/Alterar relatórios
	Automatizar geração/envio de relatórios
	Criar e realizar consultas em bancos de dados
	Configurar novas métricas e KPIs
ITOM	<b>Monitoramento de Ambiente</b>
	Configurar ativo de monitoramento
	Criar / Alterar / Excluir Dashboards
	Emitir Relatórios de Monitoramento
	Fornecer Acesso as ferramentas de monitoramento
	Configurar ativo de monitoramento
	Alterar ativo de monitoramento
	Inserir ativo de monitoramento
	Remover ativo de monitoramento
	<b>Incidentes</b>
	Incidente em Monitoramento de Ambiente
	Falha de comunicação de agente
	Indisponibilidade de agente
	<b>Mudança</b>
	Colocar o ativo em modo manutenção
	Configurar Monitoramento
	Tirar o ativo do modo manutenção
	Inserir ativo no monitoramento
Alterar ativo no monitoramento	
Excluir ativo do monitoramento	

Gerenciamento de Capacidade	<b>Gestão</b>
	Análise de padrões de utilização histórica para prever demandas futuras.
	Capacidade de ajustar e adaptar a capacidade de acordo com as projeções de carga.
	Dimensionamento de recursos das VMs com base em requisitos de carga de trabalho.
	Geração de relatórios detalhados sobre a utilização de recursos, tendências e previsões.
	Análise do desempenho do data center e das VMs para a tomada de decisões estratégicas.
	Permitir a criação de cenários para a análise comparativa de demandas entrantes e em relação à disponibilidade de recursos financeiros e humanos.
	Sistema além de realizar visões de serviço e uso de capacidade computacional, apresente relatórios de cobrança e apresentação para suportar a gerência de orçamento e custos de serviços.
	<b>Configuração e Relatórios/Dashboard</b>
	Configuração de Pool de Equipamentos
	Configuração de Serviços
	Elaboração de Relatórios / Dashboards de Tendências
	Elaboração de Relatórios / Dashboards de Serviços
	Elaboração de Relatórios / Dashboards de Planejamento de Capacidade
Elaboração de Projeção de substituição / migração de equipamentos	