5.1 Permitir a definição de prioridade a partir de uma matriz de cálculo de impacto em função da urgência.

5.2 Permitir a associação entre os incidentes, requisições, problemas, mudanças e liberações relacionados através da interface de gerenciamento de incidentes.

5.3 Permitir a associação de Item de Configuração afetado através da interface de gerenciamento de incidentes.

5.4 Permitir estimar o impacto dos Itens de Configuração afetados para auxiliar a equipe de suporte de Gerenciamento de Incidentes a classificar adequadamente os registros de incidentes.

5.5 Permitir o acompanhamento gráfico e gerar alarmes automáticos e proativos (*e-mail* e gráficos) do envelhecimento dos incidentes.

5.6 Permitir a abertura de incidentes a partir de e-mail para qualquer usuário (interno ou externo).

5.7 Ser integrada na mesma plataforma que a Plataforma de Banco de Dados de Gerenciamento de Configuração (*CMDB*).

5.8 Facilitar a automação dos procedimentos de escalonamento de Incidentes para Problemas.

5.9 Permitir que o usuário final e analistas utilizem um corretor ortográfico na abertura de incidentes.

5.10 Permitir a abertura de incidentes através de *e-mail* e *web services*, para integração com outras soluções.

5.11 Possuir a funcionalidade de criação de incidentes a partir de modelos pré-definidos (*templates*).

5.12 Permitir o fechamento de todos os incidentes filhos relacionados a um incidente pai.

5.13 Possuir funcionalidade de fechamento automático do chamado quando o status for Resolvido. (Ex. Após 48 horas sem interação com o usuário final, o chamado será fechado automaticamente).

5.14 Permitir a criação de documentos de conhecimento a partir da solução de um registro de um incidente.

5.15 Permitir configurar tipos de tratamento especial associado ao contato, isto é, permite identificar contatos (usuários finais afetados) que exigem alguma forma de atenção especial. Ex. Usuário *VIP*, Deficiente visual.

5.16 Permitir controlar como os usuários selecionam os status disponíveis no formulário do chamado, ou seja, permitir a criação de fluxo de transição do chamado, o qual deve seguir um caminho pré-determinado configurado na ferramenta. (Ex., um *ticket* está em um *status* Aberto, e o fluxo de transição permite apenas que o analista atualize o *status* para Fechado).

5.17 Permitir controlar como os atributos são designados como necessários (devem ser fornecidos) ou bloqueados (não podem ser atualizados) dependendo do status do chamado, ou seja, permitir configurar quais campos no formulário precisam ser preenchidos e quais não podem ser alterados.

5.18 Prover um painel de controle automático ("*dashboard*") informando o quadro geral dos incidentes (por exemplo, informar os incidentes com status aberto, fechado, resolvido, pendente com usuário/fornecedor, próximo de romper o SLA).

6 **Em relação ao Gerenciamento de Problemas, a ferramenta deve:**

6.1 Possuir mecanismos para o controle de problemas, de acordo com as definições da *ITIL V4*, permitindo a identificação, classificação, designação, investigação e identificação da causa raiz.

6.2 Permitir a definição de prioridade em função do impacto e da urgência.

6.3 Permitir, através da interface de gerenciamento de problemas, a associação com os incidentes, requisições, problemas, mudanças e IC's relacionados.

6.4 Fechar automaticamente os incidentes em aberto quando houver o fechamento do problema relacionado àqueles incidentes.

6.5 Permitir o acompanhamento gráfico gerando alarmes pró-ativos (e-mail e gráficos) em relação ao envelhecimento dos chamados de problema (Por exemplo, permitir que ações de envio de e-mail sejam disparadas no caso de alertas para possíveis violações de SLA's).

6.6 Diferenciar a criticidade dos Itens de Configuração para auxiliar a equipe de Gerenciamento de Problemas a classificar os registros de Problemas.

6.7 Ser integrada na mesma plataforma que a Plataforma de Banco de Dados de Gerenciamento de Configuração (*CMDB*).

6.8 Permitir que a equipe de Gerenciamento de Problema comunique à Central de Serviços (*Service Desk*) o status e relatórios de progressos, assim como, soluções temporárias e soluções de contornos.

6.9 Permitir a alteração da classificação da severidade ou do impacto de um Problema.

6.10 Permitir que analistas utilizem um corretor ortográfico na abertura de problemas.

6.11 Permitir a abertura de problemas através de e-mail e *web services*.

6.12 Possuir a funcionalidade de criação de problemas a partir de modelos pré-definidos (*templates*).

6.13 Permitir a criação de documentos de conhecimento a partir da solução de um registro de um problema.

6.14 Permitir o fechamento de todos os problemas filhos relacionados a um problema pai.

6.15 Permitir controlar como os usuários selecionam os status disponíveis no formulário do chamado, ou seja, permitir a criação de fluxo de transição do chamado, o qual deve seguir um caminho pré-determinado configurado na ferramenta. (Ex., um *ticket* está em um status Aberto, e o fluxo de transição permite apenas que o analista atualize o status para Fechado).

6.16 Permitir controlar como os atributos dos chamados são designados como necessários (devem ser fornecidos) ou bloqueados (não podem ser atualizados) dependendo do status do chamado, ou seja, permitir configurar quais campos no formulário precisam ser preenchidos e quais não podem ser alterados.

6.17 Prover um painel de controle automático ("*dashboard*") informando o quadro geral dos problemas (por exemplo, informar os problemas com status aberto, fechado, resolvido, pendente com usuário/fornecedor, próximo de romper o SLA).

7 **Em relação ao Gerenciamento de Conhecimento, a ferramenta deve:**

7.1 Possuir uma base de conhecimento onde serão registrados erros conhecidos e soluções para os problemas. Deverá ser possível relacionar os problemas e suas respectivas soluções a mudanças e a incidentes específicos.

7.2 Permitir a adição de registros na base de conhecimento a partir dos registros de soluções de incidentes e de problemas.

7.3 Permitir o acesso à base de conhecimento via *Web*, assim como disponibilizar pesquisas por palavras-chave obtidas em um chamado, incidente, problema ou erro conhecido e possibilitar a navegação hierárquica de tópicos ou assuntos.

7.4 Possuir a capacidade de gerenciar os erros conhecidos, tornando-os disponíveis para consultas dos usuários e publicação na *Web*.

7.5 Possibilitar a usuários administradores, ou a outros usuários com nível de autorização suficiente, o gerenciamento (inclusão, alteração, consulta e exclusão) das informações armazenadas na base de conhecimento, bem como o gerenciamento das informações a serem armazenadas.

7.6 Possuir listas de perguntas frequentes (*FAQ's*) para cadastrar informações sobre problemas conhecidos, erros comuns, rotinas e procedimentos (*scripts*), além de permitir a categorização das informações inseridas.

7.7 Possuir em sua tela inicial um quadro de avisos onde serão informadas indisponibilidades de serviços (correntes ou programadas), mudanças relevantes ou outras mensagens genéricas cadastradas por um usuário administrador, e deverá permitir o direcionamento das informações para todos os usuários ou apenas para grupos de usuários.

7.8 Prover dados do processo de Gerenciamento do Conhecimento para os processos de Incidentes e Problemas nativamente.

7.9 Suportar o cadastro, a alteração, a revisão, a desativação, a publicação, a definição de público-alvo, a definição de área responsável, a alteração de status e a categorização de documentos de conhecimento.

7.10 Suportar o recebimento de propostas de documento de conhecimento, sua posterior análise e sua aceitação ou rejeição. O recebimento de propostas de documentos de conhecimento deve ter origem no gerenciamento de incidentes, no gerenciamento de problemas ou em uma solicitação direta de um usuário.

7.11 Suportar revisões para cada documento de conhecimento e a emissão de alertas configuráveis.

7.12 Deve permitir anexar documentos, além de figuras e *link's*.

7.13 Prover resultados de pesquisas na base de conhecimento que incluam a relevância do documento através de pontuação e a qualificação do documento realizada por usuários e analistas.

7.14 A solução deverá permitir que o usuário final possa pesquisar na base de conhecimento antes da abertura de um incidente ou requisição.

7.15 Possibilitar a criação do documento através da escolha de um modelo padrão.

7.16 Permitir a seleção dos campos para pesquisa como título, sumário do documento, problema ou solução encontrada.

7.17 Permitir associar ao *log* do incidente ou problema o *link* para o documento de conhecimento utilizado.

7.18 Controlar o processo de aprovação de um documento, antes do mesmo ser publicado na base de conhecimento.

7.19 Permitir avaliar a qualidade de documentos da base através de pesquisas com o usuário final ou analista.

7.20 Permitir aos usuários e analistas enviar comentários sobre o documento de conhecimento.

7.21 Permitir o cadastro de palavras e símbolos que devem ser ignoradas nas pesquisas (Ex: “e”, “a”, “ou”, “sempre”, “já”, “tudo”, entre outras).

7.22 Permitir a utilização de corretor ortográfico em Português na criação de documentos de conhecimento.

7.23 Permitir configurar o controle de acesso para escrita e/ou leitura do documento levando em consideração o perfil do usuário.

7.24 Disponibilizar a funcionalidade de pesquisa de documentos similares, na criação de um novo documento.

8 **Em relação ao Gerenciamento de Nível de Serviço, a ferramenta deve:**

8.1 Suportar a definição de níveis de serviço para os processos de Incidentes, Problemas, Mudanças e Requisições de Serviços.

8.2 Permitir a definição dos níveis de serviço de tempo para início do atendimento e tempo de solução, no mínimo.

8.3 Permitir a identificação dos níveis de serviço estabelecidos para um chamado de acordo com seu tipo, classificação, prioridade, área-fim, IC's envolvidos e usuários envolvidos.

8.4 Possibilitar a definição de paradas programadas e janelas de manutenção para os serviços de TI, de modo que interrupções durante esses intervalos não influenciem o cálculo dos níveis de serviço correspondentes.

8.5 Emitir alerta automático (*e-mail*), quando um nível de serviço estiver próximo de seu limite de acordo com valores limites preestabelecidos.

8.6 Prover às gerências de incidentes, problemas e requisições de serviços, o acesso a informações de SLA's.

8.7 Permitir a associação automática de incidentes, problemas e mudanças a serviços e SLA's, possibilitando a visualização dos incidentes que impactaram serviços e SLA's.

8.8 Permitir a emissão de relatórios comparativos entre os níveis de serviço acordados e os níveis de serviço efetivamente realizado para requisições, incidentes, problemas e mudanças.

8.9 Permitir a emissão de gráficos gerenciais consolidados por período, contendo os indicadores de desempenho.

8.10 Redundante com o item 8.15. Acredito que as duas situações podem ser explicadas num item só. Permitir o cadastro de horário de atendimento por dia da semana e de acordo com uma tabela de feriados pré-configurada.Possibilitar o cadastro dos SLA’s com base em calendários de cálculo e calendários de trabalho, onde esses calendários definirão quando o SLA pode ser aplicado e qual será o cálculo de horas para esse SLA.

8.11 Possuir a funcionalidade de *STOP* SLA, para que possa ser calculado atrasos no serviço por motivo de terceiros, esse cálculo deverá ser apresentado em tempo real nas aplicações de Solicitações de Serviço e Incidentes com objetivo dos gestores dos processos poderem gerenciar de forma mais dinâmica o não cumprimento dos SLA’s.

8.12 Permitir configurações de alertas para Gestão de Níveis de Serviço via e-mail.

8.13 Se a palavra "escalação" se refere a atribuição do chamado, o assyst não faz isso de forma automática nessa situação (quando um SLA está estourado ou próximo a vencer)Possibilitar a criação de eventos e macros associados a SLA's que serão utilizados para notificação e para escalar o chamado (por exemplo, permitir que ações de envio de e-mail sejam disparadas no caso de violações de SLA's, permitir que ações de envio de e-mail sejam disparadas no caso de alertas para possíveis violações de SLA's, permitir que os chamados sejam escalados no caso de violações de SLA's, permitir que os chamados sejam escalados no caso de alertas para possíveis violações de SLA's).

8.14 Registrar os alarmes e violações de SLA através de cores e símbolos.

8.15 Permitir a associação e a configuração de calendários de horas de trabalho (por exemplo, para horário de expediente de 8h00 – 18h00, será contabilizado o prazo corrido de 10 horas úteis) aos SLA's para que sejam calculados corretamente.

8.16 Permitir o gerenciamento do ciclo de vida de um Acordo de Nível Operacional (*OLA - Operational Level Agreement*).

8.17 Permitir o registro dos custos das violações para cada SLA.

9 **Em relação ao Gerenciamento de Mudanças, a ferramenta deve:**

9.1 Permitir o registro e a classificação das mudanças.

9.2 Permitir a associação de uma mudança a um IC através da interface de gerenciamento de mudanças.

9.3 Permitir a avaliação de impacto de uma mudança através de interface gráfica e por relatório relacionando todos os IC's que podem ser afetados.

9.4 Permitir a execução da análise de impacto da mudança de forma automática. A funcionalidade terá que varrer o *CMDB* retornando de forma gráfica para o analista de mudanças quais impactos a mesma terá.

9.5 Permitir o acompanhamento do processo de mudança fim a fim (desde o registro até a implantação e revisão da mudança).

9.6 Permitir o cadastro de mudanças pré-aprovadas.

9.7 Permitir a definição de níveis de acesso aos registros em função do perfil do usuário.

9.8 Permitir que um participante do Comitê de Mudanças possa delegar a sua aprovação para outro usuário.

9.9 Permitir que determinados tipos de mudança tenham a sua aprovação delegada para outro usuário.

9.10 Registrar a hora e o responsável por toda e qualquer alteração no registro de uma mudança.

9.11 Implantar *workflow* automatizado para a aprovação de mudanças programadas, emergenciais e padrão.

9.12 Obter do CMDB a lista de todos os IC's afetados pela mudança.

9.13 Armazenar e fornecer *templates* de planejamento das mudanças.

9.14 Possuir integração nativa com o módulo de gerenciamento de nível de serviço.

9.15 Gerar notificações através da interface gráfica e e-mail para o início e final das mudanças.

9.16 Disponibilizar para o *Service Des*k (Central de Serviços) quadro de avisos com as principais mudanças em andamento e o impacto no ambiente.

9.17 Prover integração das Requisições de mudança com as atividades de liberações.

9.18 Prover um relatório integrando as mudanças com as liberações.

9.19 Prover um relatório possibilitando a visão de mudanças com sucesso: por área usuária, por área de TI, por área de negócio.

9.20 Prover um painel de controle automático ("*dashboard*") possibilitando a visão da eficiência operacional e dos impactos dos processos de negócio.

9.21 Prover um ciclo de vida da Requisição de Mudança em conformidade com o *ITIL V4*.

9.22 Prover uma visão de detecção de colisão, de forma automática, com outras mudanças planejadas.

9.23 Realizar o fechamento de problemas e incidentes automaticamente quando uma mudança relacionada for implementada com sucesso.

9.24 Possuir calendário de visualização para facilitar o planejamento das mudanças.

9.25 Possibilitar o relacionamento das solicitações de mudanças com outros incidentes, problemas, mudanças ou requisições.

9.26 Permitir a abertura de solicitações de mudança através de e-mail e *web services*.

9.27 Disponibilizar a criação de listas de atividades para serem executadas no registro de uma solicitação de mudanças.

9.28 Disponibilizar ferramenta de *workflow* para fluxos de mudanças que envolvam integrações com outras soluções.

9.29 Permitir a criação de solicitações de mudanças a partir de modelos pré-definidos. (*templates*).

9.30 Permitir o fechamento de todas as solicitações de mudanças filhas relacionadas a uma solicitação de mudança pai.

9.31 Oferecer Calendário de Mudanças gráfico, permitindo a visualização e o controle da agenda de mudanças.

9.32 Permitir visualizar todos os itens de configuração de uma mudança e seus relacionamentos, possibilitando incluir itens de configuração relacionados que não tenham sido originalmente vinculados à mudança.

9.33 Permitir controlar como os usuários selecionam os status disponíveis no formulário, ou seja, permitir a criação de fluxo de transição, o qual deve seguir um caminho pré-determinado configurado na ferramenta. (Ex., um *ticket* está em um *status* Aberto, e o fluxo de transição permite apenas que o analista atualize o *status* para Fechado).

9.34 Permitir controlar como os atributos são designados como necessários (devem ser fornecidos) ou bloqueados (não podem ser atualizados) dependendo do status do chamado, ou seja, permitir configurar quais campos no formulário precisam ser preenchidos e quais não podem ser alterados.

9.35 Verificar se é necessário solicitar muitos relatórios genéricos ou se é mais interessante definir quantitativo de relatórios e solicitar implementação de acordo com a necessidade dos indicadores do TJCE, como já citado.Prover no mínimo os seguintes Indicadores de desempenho e relatórios:

9.35.1 Índice de incidentes e problemas ocorridos devido a liberações realizadas.

9.35.2 Índice de atualização dos IC's.

9.35.3 Índice de liberações realizadas dentro do prazo.

9.35.4 Índice de solicitações de mudança implementadas.

9.35.5 Índice de mudanças não planejadas com impactos em processos críticos.

9.35.6 Quantidade de mudanças solicitadas e que foram consideradas inviáveis/negadas pelo comitê gestor de mudanças.

9.35.7 Informações sobre o status de cada mudança, principalmente quanto ao prazo de implementação, incluindo justificativas das mudanças atrasadas.

9.35.8 Relatório de status de todos os problemas e incidentes pendentes relacionados a mudanças e/ou liberações.

9.35.9 Relatório de quantidade de liberações realizadas.

9.35.10 Relatório de distribuição das liberações por departamento/localidade.

9.35.11 Relatório de distribuições de liberação por tipo.

9.35.12 Relatório de crescimento da demanda.

9.35.13 Relatório de liberações por fornecedor.

9.35.14 Relatório de desempenho das liberações por fornecedor.

9.35.15 Relatório de indicadores de desempenho.

10 **Em relação ao Gerenciamento de Liberação e Implementação, a ferramenta deve:**

10.1 Permitir o acompanhamento do ciclo de vida completo do Gerenciamento de Liberações e Distribuição para as fases de, mas não limitado a, planejamento, construção, testes, garantia da qualidade, agendamento e distribuição;

10.2 Permitir o estabelecimento dos critérios de conclusão de uma liberação, por exemplo, mas não limitado a, ter a capacidade de estabelecer tarefas ou marcos auditáveis que suportam o processo decisório para determinar se todos os requisitos da liberação foram cumpridos para a aprovação da distribuição;

10.3 Ser integrada a uma Biblioteca Definitiva de Software / Mídias;

10.4 Permitir o agendamento das atividades de distribuição e entrega de liberações;

10.5 Permitir a construção, empacotamento e o agendamento de diferentes tipos de pacotes de liberação;

10.6 Facilitar a identificação e o controle sobre aspectos do pacote de liberação, tais como *software*, *hardware*, documentação, requisitos de treinamento, etc.;

10.7 Facilitar o processo de autorização e agendamento de liberação de pacotes de forma integrada ao processo de Gerenciamento de Mudanças;

10.8 Permitir definir e tornar obrigatório, caso necessário, o processo de validação da Liberação e as atividades de teste;

10.9 Permitir o versionamento de pacotes de Liberação;

10.10 Possuir funcionalidades para o gerenciamento da reversão de Liberações (*rollback*) para versões anteriores da configuração;

10.11 Garantir que o processo de Liberação terá disponível todas as informações requeridas contidas no *CMDB* para a distribuição dos pacotes, através de integração com o processo de Gerenciamento de Ativos e Configuração;

10.12 Permitir a atualização automática do *CMDB* com as novas informações do item de configuração atualizado pela liberação;

10.13 Garantir que uma Liberação passe por processos de agendamento da distribuição e todas as aprovações requeridas pelo processo de Gerenciamento de Mudanças.

11 **Em relação ao Gerenciamento de Configuração e Repositório de Dados de Configuração (*CMDB*), a Plataforma deve:**

11.1 Permitir o acesso ao *CMDB* e disponibilizar *queries* (coletas) para visualização dos Itens de Configuração.

11.2 Possibilitar, através da identificação de um determinado *IC*, todos os relacionamentos e eventos ligados aos incidentes, problemas, mudanças, liberações, acordo de nível de serviço, contratos de garantia, licenças disponíveis, hardware que estão ligados a este IC (árvore horizontal e vertical).

11.3 Permitir a gestão de todo o ciclo de vida do ativo (planejamento de aquisição, aquisição, provisão, suporte, manutenção e descarte).

11.4 Atualizar e manter os *IC's* no *CMDB*.

11.5 Permitir o ajuste e adaptação (personalização) das informações do Item de Configuração.

11.6 Permitir que os dados sejam exportados em um dos seguintes formatos: *CSV*, *HTML* e *TXT*.

11.7 Permitir a criação e atualização de um modelo de serviço e seus respectivos relacionamentos no *CMDB*.

11.8 Disponibilizar graficamente um mapa com a dependência lógica das aplicações e dispositivos de infra.

11.9 Permitir a identificação dos dispositivos de infra que disponibilizam um serviço ou aplicação.

11.10 Permitir o mapeamento dos relacionamentos dos Itens de Configuração e classificar em: dependência, componentes e membros de um grupo.

11.11 Permitir a criação de filtros no momento da reconciliação do *CMDB* para que só sejam populados no *CMDB* dados de *IC´s* que são permitidos pelo gestor da configuração.

11.12 Permitir a representação de diversos componentes de infraestrutura por meio de Itens de Configuração dentro do *CMDB*.

11.13 Permitir a representação como *IC's* de, no mínimo, os seguintes componentes: servidores, sistemas, ativos de rede, topologia da rede, aplicações e informações de usuários.

11.14 Disponibilizar um modelo padrão para a representação gráfica dos *IC's*.

11.15 Permitir o relacionamento e identificação das dependências entre os *IC's*.

11.16 Possuir a capacidade de criar Itens de Configuração (*IC's*) e manter as configurações de acordo com a necessidade da Contratante.

11.17 Disponibilizar a visualização dos *IC's* por meio de serviço do catálogo de serviços atrelados com todos os Itens de Configuração referente ao serviço.

11.18 Disponibilizar uma interface gráfica *Web* para visualização dos *IC's* e seus relacionamentos.

11.19 Possuir um mecanismo para incluir e relacionar itens configuráveis (físico) dentro de um processo de TI e aplicação (lógico).

11.20 Prover funcionalidade de pesquisa por *IC's* para qualquer processo de TI relacionado ao mesmo.

11.21 Permitir o relacionamento entre pessoas, processos e tecnologia de dados dentro do *CMDB*. As informações podem ser provenientes de várias fontes, como: ferramentas de descobrimento (*discovery*), banco de dados de ativos de TI, ferramentas de rede e processos de negócio.

11.22 Permitir a população do *CMDB* e mantê-lo atualizado por meio de troca de dados com a solução de inventário contida no processo.

11.23 Possuir um mecanismo para popular manualmente os *IC's* no *CMDB*.

11.24 Permitir o armazenamento dos dados manipulados no *CMDB*.

11.25 Prover mecanismo de Federação que permita o acesso ao *CMDB* e a seus objetos, como documentos e arquivos, por meio de um *link* ou referência para que o *CMDB* não armazene localmente todos estes objetos.

11.26 Prover mecanismo de Reconciliação que permita consolidar as informações e visões de um elemento ou instância a partir da obtenção de dados de mais de uma fonte de origem, a fim de evitar a duplicidade das informações e agrupar os itens automaticamente.

11.27 Permitir a definição de perfis de usuários, como: administradores de sistema, analistas de *service desk*, especialistas de rede, atribuindo a cada perfil um nível de autorização específico.

11.28 Permitir a definição de permissões para cada campo do *IC* com, no mínimo, as seguintes opções: nenhum acesso, somente visualização e alteração.

11.29 Prover um acesso seguro e controlado para o *CMDB*.

11.30 Prover uma interface gráfica que permita navegar, modificar e extrair informações relacionadas aos Itens de Configuração, como indicadores de criticidade e classificação de falha de um *IC*.

11.31 Apresentar graficamente o relacionamento entre pai e filho dos *IC's*, como os mapas gerados com a estrutura dos serviços de TI.

11.32 Suportar a configuração em *cluster* de Sistema Operacional (SO) e banco de dados, bem como a utilização de múltiplos servidores de aplicação.

11.33 Permitir a definição de uma estrutura de categorização dos *IC's*, com a categoria principal e subcategoria, no mínimo.

11.34 Permitir a associação dos *IC's* aos Serviços de Negócio, estabelecendo quais são os *IC's* que participam da infraestrutura de um determinado serviço.

11.35 Permitir a associação dos *IC's* aos serviços de terceiros envolvendo Contratos de Apoio – Cas (*Underpinning Contracts - UC*). Estabelecendo quais *IC's* são suportados por um determinado serviço externo.

11.36 Disponibilizar funcionalidade para registro de períodos de bloqueio com a possibilidade de emissão de alertas.

11.37 Disponibilizar aplicação de uma linha base dos Itens de Configuração (*Snapshot*) autorizados pelo *CMDB* versus a linha base (*Snapshot*) dos Itens de Configuração descobertos pela ferramenta de Inventário (*Discovery*).

11.38 Ser capaz de dentro da interface gráfica de visualização dos relacionamentos e dos itens de configuração filtrar os componentes por relacionamentos e por tipos de *IC's*, refletindo, imediatamente, a nova visualização dos *IC's* na interface gráfica.

11.39 Permitir o filtro de profundidade e abrangência nas consultas dentro do *CMDB*, possibilitando ao analista de *CMDB* ter mais ou menos visibilidade das camadas do *CMDB*.

11.40 Possuir a capacidade de gerar relatórios gerenciais baseados nos dados cadastrados.

11.41 Prover relatórios gerenciais e auditoria relacionada ao inventário dos *IC's*.

11.42 Disponibilizar relatórios gerenciais, via *Web*, personalizáveis de acordo com as necessidades e informações relacionadas à Central de Serviços.

11.43 Relacionar aos *IC's* específicos seus contratos para controle de garantia, de aluguel, de compra ou manutenção.

11.44 Dispor de uma funcionalidade que permita informar ao analista utilizar quais relacionamentos dos *IC's* serão levados em consideração no momento da análise de impacto.

11.45 Possuir descobrimento (*Discovery*) de servidores (*Linux Red Hat*, *Linux Debian*, *Linux Suse*, *Linux CentOs*, AIX, *Windows* 2000, 2003 e 2008) com ou sem agente (SSH).

11.46 Possuir descobrimento (*Discovery*) de aplicações de mercado (ex: *BEA*, *HP*, *CA*, *IBM*, *JBOSS*, *McAfee*, *Microsoft*, *Oracle*, *SAP*, *Siebel*, *Sybase*, *Symantec*, *TIBCO*, *VMware*, dentre outros) com ou sem agente (*SSH*).

11.47 Possuir relacionamento automático dos servidores e das aplicações que rodam nos Servidores.

11.48 Permitir o descobrimento (*Discovery*) de ambiente em *cluster* ou virtualizado.

11.49 Detecção de mudanças dos Servidores, Serviços, *Software*, Parâmetros, Arquivos Gerenciados, dados gerenciados e Dados de Configuração que estão sendo gerenciados.

11.50 Permitir criar *baselines* de Configuração.

11.51 Permitir criar Padrões de Configuração.

11.52 Permitir a comparação entre Servidores e mostrar as diferenças existente entre os mesmos.

11.53 Permitir configurar Regras de Conformidade para detectar violação das políticas configuradas.

11.54 Possuir interface gráfica para demonstrar o relacionamento entre os itens de configuração.

11.55 Permitir pelo menos cinco níveis de relacionamentos na interface gráfica.

11.56 Permitir visualizar somente os itens afetados por um item de configuração (Análise de Impacto).

11.57 Permitir visualizar somente os itens que afetam um item de configuração (Análise de Causa Raiz).

11.58 Permitir filtrar os tipos de itens de configuração a se visualizar (por exemplo, visualizar somente itens de configuração do tipo Serviço ou SLA).

11.59 Permitir a seleção de 02 (dois) itens de configuração para a visualização do caminho completo entre estes dois itens quando houver relacionamento entre eles.

11.60 Permitir pesquisar os itens de configuração diretamente na interface de visualização dos relacionamentos.

11.61 Possuir funcionalidade de mostrar/esconder os itens de configuração em exibição.

11.62 Permitir o controle de aproximação da imagem (*zoom*) para facilitar a visualização dos itens de configuração.

11.63 Permitir alterar níveis hierárquicos a serem visualizados dinamicamente.

11.64 Permitir que a visualização seja salva em um modelo para futuras consultas.

11.65 Possuir funcionalidade de pesquisa no gráfico para facilitar o encontro de informações.

11.66 Permitir a criação de um item de configuração diretamente na interface gráfica de visualização.

11.67 Permitir a criação de relacionamentos diretamente na interface gráfica de visualização.

11.68 Mostrar o status do item de configuração na interface gráfica (Ex. Ativo, Indisponível, em manutenção, etc).

11.69 Permitir, através de diferentes visões, a visualização dos itens de configuração.

11.70 Permitir a criação de novos filtros definidos pelo usuário para facilitar a visualização dos relacionamentos entre os itens de configuração.

11.71 Permitir a listagem dos itens de configuração que sofreram mudanças no último dia, última semana ou último mês.

11.72 Permitir visualizar facilmente quantas requisições, incidentes, problemas e solicitações de mudanças estão relacionados ao item de configuração.

11.73 Executar o versionamento dos itens de configuração de forma automática.

11.74 Permitir a associação de SLA's aos itens de configuração para a contabilização do tempo de atendimento a estes itens.

11.75 Possuir mecanismo de reconciliação de itens de configuração para evitar duplicação de itens durante as importações.

12 **Em relação ao Gerenciamento do Catálogo de Serviços de TI, a ferramenta deve:**

12.1 Permitir a definição do catálogo de serviços e o cadastro e manutenção de descrição de serviços, assim como de seus atributos;

12.2 Prover a personalização da estrutura do catálogo de serviços, devendo esta parametrização ser realizada através da própria interface da solução pelos administradores da ferramenta;

12.3 Permitir o relacionamento dos serviços de TI disponíveis com seus respectivos usuários;

12.4 Permitir que, para cada serviço e/ou item de configuração, seja possível informar o seu grau de prioridade (importância) para o negócio de forma a estabelecer a priorização no atendimento;

12.5 Prover a disponibilização do catálogo de serviços aos usuários;

12.6 Permitir a criação de uma hierarquia (por exemplo, categoria e subcategoria) de serviços por meio da criação de dependências com relacionamento do tipo pai/filho.

13 **Em relação ao Gerenciamento de Ativos de TI e Controle de Ativos de TI, a ferramenta deve:**

13.1 Descobrir e identificar estações de trabalho, notebooks ou servidores não-gerenciados para oferecer suporte automático às instalações do agente ou localizar estações de trabalho,

*notebooks* e servidores que não pertencem à rede organizacional. Para tanto, esta funcionalidade deve:

13.1.1 Fornecer um processo de descoberta descentralizada minimizando o impacto sobre o tráfego de rede ou de segurança.

13.1.2 Ser capaz de designar "*scan points*" dentro de cada sub-rede do console. Este "*scan point*" deve ser qualquer máquina não dedicada que está sendo gerenciado pelo produto.

13.1.3 Ser capaz de identificar novas estações de trabalho, *notebook's* e servidores conectados à rede *IP* e as informações descobertas devem incluir (mas não limitado a) *hostname*, OS, endereço *IP* e endereço *MAC*.

13.1.4 Oferecer um método para instalar o agente, quando aplicável.

13.1.5 Permitir que o administrador configure e agende os *scan's*.

13.1.6 A coleta de dados de inventário só deve carregar as diferenças a partir da última verificação.

13.2 Permitir a coleta e gerenciamento de informações dos componentes de estações de trabalho, *notebooks* ou servidores sob demanda. Para tanto, esta funcionalidade deve:

13.2.1 Ser capaz de detectar informações de ativos de hardware dos sistemas que têm os agentes instalados sem a necessidade de configuração ou agendamento de um processo de inventário.

13.2.2 Permitir que as alterações de inventário que são processados automaticamente no agente sejam enviadas para o servidor sem intervenção do operador.

13.2.3 Registrar todas as informações sobre estações de trabalho, notebooks ou servidores no servidor de gerenciamento sendo que algumas das informações básicas devem incluir, no mínimo:

13.2.3.1 Informações do *BIOS*;

13.2.3.2 Velocidade e tipo de *CPU*;

13.2.3.3 Espaço em disco rígido;

13.2.3.4 Quantidade de memória disponível;

13.2.3.5 Nome do computador;

13.2.3.6 Modelo de computador;

13.2.3.7 Endereço *IP*;

13.2.3.8 Sistema operacional;

13.2.3.9 Periféricos conectados;

13.2.4 Permitir que os usuários do console criem consultas personalizadas sobre informações de estações de trabalho, *notebooks* ou servidores para serem recuperadas pelos agentes.

13.2.5 Ser capaz de agrupar clientes dinamicamente com base nas informações de estações de trabalho, *notebooks* ou servidores.

13.2.6 Ser capaz de listar todos os *softwares* e aplicativos, incluindo números de versão, que estão instalados na máquina do agente.

13.2.7 Ser capaz de listar todos os *softwares* e aplicativos instalados para um grupo de clientes, incluindo o número de instalação para cada *software* ou aplicação.

13.2.8 Permitir que os usuários do console criem consultas personalizadas em informações de inventário de *software* a serem recuperada pelos agentes.

13.3 Ser capaz de reunir, armazenar e analisar informações de aplicações de *softwares* instalados em estações de trabalho, *notebooks* ou servidores, possibilitando assim o controle efetivo do uso das licenças existentes.

13.4 Possuir uma arquitetura de implementação contemplando os seguintes aspectos:

13.4.1 A solução deve permitir indicar o máximo de banda permitido.

13.4.2 A solução deve suportar estações de trabalho, *notebooks* ou servidores conectados via rede corporativa (*LAN*) e *VPN* para os equipamentos que estejam dentro do range de *IP's* da rede do TJCE.

13.4.3 A solução deve suportar inventário em ambientes multi-plataforma (*Windows*, *Unix*, *Linux* e *MacOS*).

13.4.4 A solução deve permitir integração com outro *software* de gerência através de APIs ou *WebServices*.

13.4.5 A solução deve possibilitar que os dados trafegados sejam criptografados através do uso de algoritmos como *3DES* ou *AES*.

14 **Em relação ao Gerenciamento de Configuração de *Desktops*, a ferramenta deve:**

14.1 Possuir mecanismo de automação com no mínimo Inventário (*Discovery*), Distribuição de *Software* e Conexão Remota.

14.2 Possuir mecanismo de inventário para plataformas *Windows* e *Linux*.

14.3 Possuir mecanismo de "*discovery*" que permite identificar os equipamentos (estações de trabalho e *notebooks*) conectados à rede e que não possuem os *plug-ins* de agente da solução (inventário, controle remoto e distribuição de *softwares*) instalados.

14.4 Possibilitar a instalação de agentes via *GPO*, *Logon Script* ou ainda através de recurso de instalação remota de agentes da própria ferramenta.

14.5 Permitir criação de grupos estáticos e/ou dinâmicos de equipamentos gerenciados, sendo que os grupos dinâmicos serão baseados em resultados de pesquisas previamente definidas e seu conteúdo mantido de forma automática (inclusão e exclusão de equipamentos participantes do grupo) - e os grupos estáticos terão seu conteúdo mantido manualmente pelo administrador da solução.

14.6 Possuir mecanismo para definição de política de configuração dos componentes da solução (*manager* e agentes), sendo possível definir-se uma ou mais políticas para os agentes.

14.7 A distribuição de políticas de configuração pode ser efetuada imediatamente após a solicitação ou então através de agendamento para distribuição e ativação em data e hora mais convenientes.

14.8 Possuir a capacidade de, a partir de regra criada (política de gerenciamento baseada em informações inventariadas), executar abertura de chamados/incidentes/requisições de forma automática.

14.9 Executar o inventário de *softwares* a partir de lista de conhecimento atualizada periodicamente e de forma automática, provendo mecanismo de "assinatura" de softwares localizada nos agentes para otimização da coleta de informações e diminuição da carga de processamento nos componentes "*managers*" da Solução.

14.10 Executar o inventário de *softwares* a partir de lista de *softwares* cadastrada pelo administrador do ambiente, permitindo o reconhecimento de aplicações diversas (inclusive as desenvolvidas internamente), utilizando como possíveis critérios de reconhecimento: o nome do arquivo, as extensões de arquivo, os arquivos adicionais que devem ser localizados na mesma pasta do arquivo principal.

14.11 Implementar mecanismo de políticas de gerenciamento, a partir do qual pode-se identificar máquinas que estão violando uma política previamente definida (baseada em informações coletadas de inventário).

14.12 Adicionalmente, através do mecanismo de políticas de gerenciamento, deverá ser possível automatizar a execução de ações quando da detecção de uma violação de política, sendo possível enviar *e-mail*, executar um *job* na estação de trabalho que violou a política, enviar *traps SNMP*, alertar na console de administração do produto e incluir o equipamento em um determinado grupo.

14.13 Similar à violação de políticas de gerenciamento de inventário, também deverá ser possível tomar ações pré-definidas pelo administrador quando um determinado equipamento não mais violar a regra estabelecida.

14.14 Disponibilizar *WebServices*.

14.15 Prover suporte ao *FIPS* 140-2 (*Federal Information Processing Standard - Publication* 140-2).

14.16 Suportar a tecnologia *WOL* (*Wake-On-LAN*).

14.17 Suportar plataformas de virtualização *VMWARE*.

14.18 Prover suporte a capacidade de execução de comandos de "*power up*" e "*power down*" remotos em estações de trabalho.

14.19 Prover funcionalidades de *Discovery* e Inventário.

14.20 Possuir agentes que suportem execuções em plataformas *Windows XP Professional*, *Windows Vista Business* e *Windows* 7 (*Professional* e *Ultimate*).

14.21 Prover o inventário das informações de *hardware* de estações de trabalho e servidores tais como: processador(es), memória, placa-mãe, interface(s) de rede, protocolos de rede, *System BIOS*, *System Slots*, portas de I/O, Devices, Discos (físicos e lógicos), *file systems*, re-

cursos do sistema operacional, *settings* de região, controladoras (*IDE, SCSI, USB, Floppy*) e outros e também acessar e coletar informações em *Registry* (*Windows*).

14.22 Possibilitar a coleta, em plataforma *Windows*, dos serviços existentes e as informações associadas a estes (*Status*, descrição, etc).

14.23 Possibilitar a coleta, em plataforma *Windows*, das informações sobre usuários e grupos de usuários definidos nos equipamentos inventariados.

14.24 Possuir mecanismo (*template*) que permite a inclusão de informações externas à base de dados do inventário tais como: número de série do equipamento, número do ativo fixo/patrimônio, responsável, localização física, etc. Tais informações podem ser inseridas (baseado em customização específica) pelo administrador do ambiente ou pelo usuário do equipamento inventariado.

14.25 Permitir configurar o nível de detalhamento das informações a serem coletadas pelo agente de inventário.

14.26 Executar o inventário de *softwares* a partir de informações coletadas em *registry*, campos do *add*/*remove programs*, ícones presentes na barra iniciar e/ou no *desktop*.

14.27 Permitir a diferenciação entre aplicações e suítes de aplicações.

14.28 Permitir a categorização dos *softwares*.

14.29 Possibilitar a obtenção de imagem da estrutura de diretórios, até o nome do arquivo e seus dados (*timestamp*, tamanho e atributos).

14.30 Possuir componente de monitoração de utilização de *softwares* (*software metering/software usage*), a partir do qual pode-se acompanhar o uso efetivo de determinadas aplicações no ambiente inventariado.

14.31 Permitir que a medição do uso de *softwares* ocorra de forma passiva, onde serão coletados os dados estatísticos de utilização das aplicações monitoradas e enviados ao manager da solução para posterior uso em análises do ambiente.

14.32 Possibilitar definir o número limite de licenças disponíveis. Uma vez atingido tal número limite, bloquear automaticamente qualquer requisição de instalação daquele *software* por parte do usuário.

14.33 Permitir coleta de dados *WBEM* (via *WMI – Windows Management Instrumentation*).

14.34 Possibilitar execução de *scripts* diversos (*BAT*, *shell*, etc..) nas estações inventariadas via agente de inventário, independente das permissões do usuário que esteja logado na estação no momento da execução.

14.35 Permitir definição de agendamentos para a execução dos *scripts* nas estações inventariadas.

14.36 Possuir mecanismo de geração de relatórios próprio, possibilitando a execução de relatórios tanto pré-definidos como também customizados.

14.37 Possibilitar a utilização de *Queries* (pesquisas) na geração de relatórios, permitindo assim que os dados de determinado relatório sejam pertinentes somente ao grupo de equipamentos que atender ao critério definido na pesquisa.

14.38 Permitir que os relatórios sejam exportados nos formatos *PDF*, *HTML* e *CSV*.

14.39 Permitir criar tabelas específicas no banco de dados da Solução contendo o resultado de relatórios previamente configurados.

14.40 Permitir definir os campos que deverão compor o relatório, independente do tipo de informação (*hardware*, *software*, etc).

14.41 Permitir aplicar filtros para eliminar/manter informações específicas.

14.42 Permitir executar um relatório sob demanda ou então de forma agendada, sendo que neste caso será possível definir a periodicidade de geração do mesmo.

15 **Em relação ao Gerenciamento de Configuração de *Desktops*, na funcionalidade de distribuição de *softwares*, a ferramenta deve:**

15.1 Permitir a criação de política de reinstalação automática dos aplicativos previamente instalados pela solução, após uma nova instalação do agente em máquina existente no ambiente que passou por processo de recuperação (por exemplo, após um *crash* em disco).

15.2 Possibilitar agendamento da distribuição e da instalação de pacotes de *softwares*.

15.3 Possuir mecanismo próprio para empacotamento de *softwares* (*Packager*).

15.4 Oferecer instalação baseada em políticas e gerenciar a distribuição de *software* por múltiplas plataformas a partir de um único ponto de controle.

15.5 Permitir implementação e migração para os sistemas *Windows* usando controle centralizado e automação para simplificar lançamentos a novas estações de trabalho, *notebooks* e servidores por toda a rede.

15.6 Fornecer capacidade para a entrega de correções para diferentes sistemas operacionais e aplicações para estações de trabalho, *notebooks* ou servidores, diminuindo o tempo de implementação destas correções e atualizações sem a perda da funcionalidade destes ativos (excetuando-se aqui necessidades específicas das correções aplicadas, tais como, por exemplo, o processo de reinicialização obrigatória do equipamento após a aplicação da correção), mesmo sobre banda estreita ou redes globalmente distribuídas.

15.7 Oferecer suporte e controle de *desktops*, *notebooks* e servidores por todo o ambiente distribuído a partir de uma localização central com gerenciamento e soluções dos problemas de sistemas para simplificar as funções de TI e reduzir o volume de trabalho do suporte técnico.

15.8 Implementar mecanismo de *checkpoint/restart*, que garante controle de integridade no processo de transferência do pacote de software, permitindo assim a posterior retomada de uma distribuição a partir do último ponto de parada íntegro verificado pela solução – em caso de interrupção no processo de distribuição.

15.9 Permitir o gerenciamento de *patches* (*fixes*/correções) dos sistemas operacionais *Windows XP*, *Windows 2000*, *Windows Vista*, *Windows 7*, ao menos nos idiomas Inglês e Português (Brasil).

15.10 Permitir o gerenciamento de *patches* (fixes/correções) das aplicações *Adobe Reader*, *Adobe Acrobat* (edições *Professional* e *Standard*), *Adobe Flash Player*, *Apple Quicktime player*, *Microsoft Office XP*, 2003, 2007 e 2010, *Microsoft .NET*, *Microsoft SQL Server* 2005 e 2008 (32 e 64bit), *Mozilla Firefox Browser*, *RealPlayer*, *Sun JRE*, *VMWare Server*, *Workstation* e *Player*, *Winzip*.

15.11 Prover componente de arquitetura que permite a transferência de pacotes de *software* para um servidor pré-determinado em sites remotos (através da *WAN*) e então, a partir deste servidor, executar a distribuição do referido pacote de *software* para as demais estações deste site remoto.

15.12 Possibilitar a distribuição de um pacote de *software* para um grupo de estações a partir de informações de inventário (usando estas informações como pré-requisitos), tais como: quantidade de memória, espaço em disco, *software* instalado ou não instalado, etc.

15.13 Oferecer suporte aos formatos de empacotamento *Microsoft MSI* (*Windows*) e *RPM* (*Linux*).

15.14 Suportar todos os possíveis procedimentos associados a um *software*, tais como Instalação, Remoção, Manutenção, Reparação, Instalação Administrativa – bastando, para a criação de tais procedimentos, que sejam fornecidas as documentações pertinentes aos procedimentos.

15.15 Possuir mecanismo que possibilita o controle da largura de banda utilizada nas distribuições de pacotes de *software*.

15.16 Permitir a distribuição de imagem de sistema operacional para novos equipamentos, suportando a criação de imagens (para posterior distribuição) dos sistemas operacionais.

16 **O assyst não faz controle remoto nativamente. O que ele permite é chamar um app de acesso remoto através da sua interface.Em relação ao Gerenciamento de Configuração de *Desktops*, na funcionalidade de controle remoto, a ferramenta deve:**

16.1 Permitir controle remoto de um equipamento *Linux* a partir de uma estação *Windows*.

16.2 Permitir configuração de controle de acesso de forma que apenas usuários autorizados possam tomar o controle de uma determinada estação/servidor.

16.3 Possuir opção de gravação da sessão no momento da captura de estação, gerando um vídeo que poderá ser utilizado posteriormente como evidência.

16.4 Permitir visualização de uma sessão gravada.

16.5 Permitir configuração de confirmação por parte do usuário do equipamento a ser controlado para que a sessão de controle remoto possa ser efetivamente iniciada.

16.6 Permitir controle da largura de banda utilizada para sessões de controle remoto.

16.7 Permitir habilitar compressão de dados trafegados durante a sessão de controle remoto.

16.8 Permitir execução de chats entre os participantes da sessão de controle remoto.

16.9 Permitir transferência de arquivos entre os equipamentos participantes da sessão de controle remoto.

17 **Em relação ao Gerenciamento de Configuração de *Desktops*, na funcionalidade de gerenciamento de Atualizações (*Patches*), a ferramenta deve:**

17.1 Permitir a identificação automatizada da necessidade de se instalar um determinado *patch*. Também, após ativação do procedimento de distribuição do *patch*, os procedimentos de obtenção, empacotamento, distribuição e validação dos *patches* devem ser automatizados.

17.2 Permitir estabelecer políticas de aplicação de *patches* (fixes, correções), garantindo também a verificação de conformidade do ambiente em relação a tais políticas.

17.3 Permitir identificar quais *softwares* e respectivos *patches* estão instalados no ambiente.

17.4 Permitir implementar e manter melhores práticas para testes e distribuições de *patches*.

17.5 Permitir implementar uma fase formal de testes de *patches*, a partir de distribuição destes para estações de trabalho de testes, possibilitando assim a verificação do impacto da aplicação de um *patch* antes de distribuí-lo para todo o ambiente de produção.

17.6 Permitir acompanhar em tempo real a distribuição dos *patches*.

17.7 Prover serviço de pesquisas online sobre *patches*, monitorando a disponibilidade, coletando as informações disponíveis, validando e identificando as dependências relativas aos *patches*.

17.8 Prover sistema de relatórios do tipo "*web-based*" (acessível via *Web Browser*), com possibilidade de agendamento automático da geração de relatórios.

17.9 A arquitetura da solução deve ser escalável, possibilitando suporte a um volume de PC's superior a 15.000 (quinze mil) equipamentos.

17.10 Permitir gerenciamento centralizado de todo o parque de PC's a partir de uma única console.

17.11 Permitir gestão de tarefas programadas/agendadas para os PC's a partir da console central de gerenciamento.

**ANEXO 2 DO CONTRATO**

**TERMO DE RECEBIMENTO PROVISÓRIO - TRP**

# ANEXO II – TERMO DE RECEBIMENTO PROVISÓRIO

| ESTADO DO CEARÁ<br>PODER JUDICIÁRIO<br>TRIBUNAL DE JUSTIÇA | **TERMO DE RECEBIMENTO PROVISÓRIO - TRP** |
|---|---|

## 1. IDENTIFICAÇÃO

| **FINALIDADE** | |
|---|---|
| Este documento tem como finalidade declarar formalmente para a contratada que os bens e serviços foram recebidos para posterior análise de conformidade de qualidade, baseadas nos critérios de aceitação definidos no contrato. | |
| **Processo Administrativo:** | |
| **Contrato Nº** | |
| **Contratada** | |
| **Objeto** | |
| **N. da OFBS** | |

Por este instrumento, atestamos, para fins de cumprimento do disposto no artigo 18, inciso III, alínea a, item 6, da Resolução CNJ nº 182/2013, que os serviços e bens, relacionados na Ordem de Fornecimento de Bens e/ou Serviços - OFBS identificada, foram recebidos nesta data e serão objetos de avaliação quanto à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos pelo Contratante.

Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até XX dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência correspondente ao Contrato supracitado.

## 2. APROVAÇÃO

XXXXXXXXXXXXXXXX
Matrícula: 99999999
Fiscal Técnico do Contrato

XXXXXXXXXXXXXXXX
Preposto da Contratada

Fortaleza XX, de XXXXXXXX de 2021

**ANEXO 3 DO CONTRATO**

**TERMO DE RECEBIMENTO DEFINITIVO - TRD**

# ANEXO III – TERMO DE RECEBIMENTO DEFINITIVO

| ESTADO DO CEARÁ<br>PODER JUDICIÁRIO<br>TRIBUNAL DE JUSTIÇA | **TERMO DE RECEBIMENTO DEFINITIVO - TRD** |
|---|---|

## 1. IDENTIFICAÇÃO

| **FINALIDADE** | |
|---|---|
| Este documento tem como finalidade declarar formalmente para a contratada que os bens e serviços foram devidamente avaliados e atendem aos requisitos estabelecido em Contrato. | |
| **Processo Administrativo:** | |
| **Contrato Nº** | |
| **Objeto** | |
| **Contratada** | |
| **N. da OFBS** | |

Os fiscais do contrato signatários deste instrumento atestam, para fins de cumprimento do disposto no artigo 18, inciso III, alínea a, item 6, da Resolução CNJ nº 182/2013, que os serviços e bens integrantes da Ordem de Fornecimento de Bens e/ou Serviços – OFBS acima identificada possuem qualidade compatível com com os critérios de aceitação previamente definidos no Termo de Referência do Contrato supracitado.

## 2. ATESTO

XXXXXXXXXXXXXXXX
Matrícula: 99999999
Fiscal Técnico do Contrato

XXXXXXXXXXXXXXXX
Matrícula: 99999999
Fiscal Requisitante do Contrato

Fortaleza XX, de XXXXXXXX de 2021

## 3. CIÊNCIA

XXXXXXXXXXXXXXXX
Matrícula: 99999999
Gestor do Contrato

XXXXXXXXXXXXXXXX
Preposto da Contratada

Fortaleza XX, de XXXXXXXX de 2021

**ANEXO 4 DO CONTRATO**

**TERMO DE CONFIDENCIALIDADE**

**Estado do Ceará**
**Poder Judiciário**
**Tribunal de Justiça**

**ANEXO IV - TERMO DE CONFIDENCIALIDADE**

## AQSETIN2020008 – Solução de Gerenciamento de *Service Desk*

Eu, _____, portador (a) da Carteira de Identidade n._____, expedida pela _____ e do Cadastro de Pessoa Física, CPF/MF sob o n. _____ declaro que:

– Todos os dados e informações recebidos do Tribunal de Justiça do Estado do Ceará durante a visita técnica realizada dia _____, às _____, deverão ser mantidos em sigilo e serão utilizados exclusivamente para a formulação de preço para fornecimento do objeto descrito no termo de referência;

Local e data,

_____

Representante da Contratada

Carimbo e Assinatura

_____

Prestador de Serviço

Assinatura e CPF do Prestador de Serviço

**ANEXO 5 DO CONTRATO**

**TERMO DE COMPROMISSO**

**ESTADO DO CEARÁ**
**PODER JUDICIÁRIO**
**TRIBUNAL DE JUSTIÇA**

**ANEXO V – TERMO DE COMPROMISSO – TC**

# AQSETIN2020008 – Solução de Gerenciamento de *Service Desk*

O ***TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARA***, sediado no Centro Administrativo Governador Virgílio Távora com sede na Avenida General Afonso Albuquerque Lima, s/n, Bairro Cambeba, Fortaleza-CE, inscrito no CNPJ n° *09.444.530/0001-01*, doravante denominado CONTRATANTE, e, de outro lado, a ***[.....]***, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º [.....] doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

## Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

## Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

**INFORMAÇÃO:** dados, processados ou não, que podem ser utilizados para produção e

transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

**INFORMAÇÃO SIGILOSA:** aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

**CONTRATO PRINCIPAL:** contrato celebrado entre as partes, ao qual este TERMO se vincula.

## Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

## Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

**I** – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

**II** – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

**III** – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

## Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite

formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

## Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

## Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

**Cláusula Oitava – DISPOSIÇÕES GERAIS**

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

## Cláusula Nona – DO FORO

A CONTRATANTE elege o foro da **cidade de Fortaleza/Ce**, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

**DE ACORDO**

| CONTRATANTE | CONTRATADA |
|---|---|
| _____<br>*<Nome>*<br>*<Qualificação>* | _____<br>*<Nome>*<br>*<Qualificação>* |

| Testemunhas | |
|---|---|
| **Testemunha 1** | **Testemunha 2** |
| _____<br>*<Nome>*<br>*<Qualificação>* | _____<br>*<Nome>*<br>*<Qualificação>* |

_____, _____ de _____ de 20____

**ANEXO 6 DO CONTRATO**

**TERMO DE CIÊNCIA**

**ESTADO DO CEARÁ**
**PODER JUDICIÁRIO**
**TRIBUNAL DE JUSTIÇA**

## ANEXO VI - TERMO DE CIÊNCIA

**AQSETIN2020008 – Solução de Gerenciamento de *Service Desk***

| INTRODUÇÃO |
|---|
| Visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos no projeto sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição. |

| IDENTIFICAÇÃO | | | |
|---|---|---|---|
| Contrato N°: | | | |
| Objeto: | | | |
| Contratante: | Tribunal de Justiça do Estado do Ceará. | | |
| Gestor do Contrato: | | Matr.: | |
| Contratada: | | CNPJ: | |
| Preposto da Contratada: | | CPF: | |

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes na Contratante.

| CIÊNCIA |
|---|
| **CONTRATADA – Funcionários** |

| | |
|---|---|
| _____ | _____ |
| ***<Nome>*** | ***<Nome>*** |
| **Matrícula: *<Matr.>*** | **Matrícula: *<Matr.>*** |
| _____ | _____ |
| ***<Nome>*** | ***<Nome>*** |
| **Matrícula: *<Matr.>*** | **Matrícula: *<Matr.>*** |
| _____ | _____ |
| ***<Nome>*** | ***<Nome>*** |
| **Matrícula: *<Matr.>*** | **Matrícula: *<Matr.>*** |

_____,_____ de _____ de 20_____.

**ANEXO 7 DO CONTRATO**

**PROPOSTA DA CONTRATADA**

**(INSERIR PROSPOTA AJUSTADA AO VALOR HOMOLOGADO)**