**ANEXO II DO TERMO DE REFERÊNCIA**

**ESPECIFICAÇÕES TÉCNICAS**

**item 1 - Jira Service Management Premium**

**Especificações:**

1. Disponibilizar portal web que possibilite:
   1. Usuários solicitarem serviços de TI através de catálogo de serviços.
   2. Autoatendimento, integrado à solução de gestão de conhecimento, onde seja possível acessar artigos da base de conhecimento, com base em problemas cadastrados, e FAQs.
   3. Consultar andamento dos serviços solicitados, atualizar informações e fechar solicitações.
   4. Acesso a funcionalidades de acordo com o perfil de acesso (usuários, agentes de atendimento, administradores, etc.)
   5. Customização do portal web, adaptação de design, campos e formulários.
2. Interface amigável e intu**i**tiva tanto para usuários quanto para agentes resolvedores, e administradores.
3. Interface de acesso, portal de atendimento e demais telas em idioma português (brasileiro), inclusive relatórios e dashboards.
4. Permitir definição de perfis: usuário, administrador de sistema, analista N1, analista N2, com níveis de autorização distintos.
5. Permitir permissões em nível de funcionalidades para equipes e usuários (exemplo: um grupo pode abrir um chamado, mas não fechá-lo).
6. Deve possibilitar recurso logs e trilha de auditoria, identificando usuários, operações e timestamps.
7. Exportação de dados para, no mínimo, os formatos CSV, XSLX ou ODS e PDF.
8. Permitir impressão de dados (relatórios, consultas etc)
9. Envio de emails para notificações sobre requisições (abertura, atualizações, encerramento e feedback).
10. Permitir consultas pelos usuários aos registros do sistema (catálogos de serviços, histórico de incidentes, bases de conhecimento, etc.) e ordenação/filtro dos registros.
11. Relatórios e métricas pré-definidas e também customizáveis de acordo com as necessidades do Tribunal.
12. Disponibilizar Portal de autoatendimento com base em questões/problemas conhecidos e integrado aos artigos da solução de gestão de conhecimento.
13. Criação de fluxos de trabalho/aprovações com base no tipo de mudança.
14. Possuir certificação PinkVERIFY ITIL 4 para, no mínimo, as práticas abaixo:
    1. Gerenciamento de Requisições de Serviços (SRM)
    2. Gerenciamento de Catálogo de Serviços (SCM)
    3. Gerenciamento de Incidentes (IM)
    4. Gerenciamento de Conhecimento (KM)
    5. Gerenciamento de Configuração (SCM)
    6. Gerenciamento de Ativos de TI (IAM)
    7. Habilitação de Mudanças (CE)
15. Possibilitar a utilização e/ou criação dos seguintes relatórios:
    1. Carga de trabalho dos agentes (workload): número de requisições para cada agente.
    2. Satisfação dos usuários.
    3. Utilidade da base de conhecimento: número de vezes que os usuários viram um artigo da base de conhecimento e marcaram como útil (curtir).
    4. Requisições resolvidas.
    5. Requisições criadas x resolvidas.
    6. Tempo para resolução, tanto por tipo quanto prioridade de requisições.
    7. ANS atendido x perdido.
    8. Incidentes por prioridade.
    9. Taxa de sucesso de ANS.
    10. Tipos de requisições de serviço solicitadas.
    11. Problemas por prioridade.
    12. Mudanças por tipo (padrão, normal e emergencial).
    13. Tempo para aprovar mudanças.
16. Possibilitar criar outros relatórios, com base em métricas existentes na ferramenta.
17. Permitir a criação e manutenção/atualização do catálogo de serviços.
18. Permitir relacionar os serviços do catálogo com os respectivos acordos de nível de serviço - ANS ( SLA's Service Level Agreement).
19. Permitir a priorização da solicitação de serviço, atribuição a um agente responsável e o escalonamento do atendimento.
20. Possibilitar recurso para envio de mensagens, alertas e atualizações (no mínimo, por e-mail).
21. Central de Serviço:
    1. Possuir um portal web de autoatendimento para os usuários pesquisarem por soluções para seus problemas e gerenciar suas solicitações (abertura, acompanhamento, atualização, fechamento e reabertura).
    2. Possibilitar criar telas e formulários customizados.
    3. Possuir painéis de indicadores de desempenho.
    4. Permitir a identificação dos usuários solicitantes e classificação da prioridade de atendimento.
    5. Permitir o controle do tempo para resolução do ticket com notificações e alertas.
    6. Gerar automaticamente número de identificação único para qualquer item aberto no sistema.
    7. Deverá fornecer autoatendimento para abertura de requisições.
    8. Permitir que o usuário devolva a requisição em caso de insatisfação com o atendimento.
    9. Permitir a rastreabilidade das requisições por filtros.
22. Gerenciamento de Requisições de Serviços:
    1. Permitir a criação de requisições por meio do catálogo de serviços ou pela Central de Serviços.
    2. Permitir a modificação, atualização e fechamento de requisições.
    3. Fornecer funcionalidade de aprovações.
    4. Possibilitar ao usuário o acompanhamento de sua requisição.
    5. Enviar notificações aos interessados durante o andamento da requisição.
    6. Permitir a criação de modelos de requisições.
    7. Permitir gerenciar o ciclo de vida das requisições.
    8. Permitir associar informações do módulo de CMDB (da mesma solução) às requisições requisições.
    9. Permitir atribuição de indicadores de impacto, prioridade e urgência às requisições.
23. Gerenciamento de Nível de Serviço:
    1. Permitir a criação, manutenção e monitoramento de acordos de níveis de serviços distintos de acordo com as necessidades de atendimento (ANS diferentes para cada equipe/contrato de suporte, por exemplo).
    2. Permitir escalar e notificar quando o ANS de uma requisição estiver próximo do vencimento.
    3. Permitir calcular o cumprimento de ANS e o rendimento dos fornecedores.
    4. Permitir a definição e envio de alertas dos registros (de incidentes, problemas, mudanças, entre outros) estiverem próximos dos limites de ANS estabelecidos.
    5. Manter histórico dos ANS.
    6. Criar indicadores de desempenho de ANS.
    7. Permitir o monitoramento dos ANS por períodos específicos e por mês calendário.
24. Gerenciamento de Incidentes:
    1. Permitir a criação, modificação e fechamento de registros de incidentes.
    2. Permitir relacionar um incidente aos ICs (itens de configuração) cadastrados no sistema.
    3. Possuir, no mínimo, os campos de informações do incidente: Nome, Impacto, Prioridade e Urgência.
    4. Permitir a criação de modelos de resposta a incidentes, com usuários específicos (atendentes, stakeholders, entre outros) a serem notificados.
    5. Permitir a associação de ANS de acordo com os tipos de incidentes.
    6. Permitir notificação por mais de um canal de comunicação (email, SMS, push notification, etc.) aos usuários e equipe de suporte quando o incidente/problema for atualizado ou resolvido.
    7. Possuir recurso de pesquisa de satisfação.
    8. Permitir a interrupção e reinício de ANS.
    9. Possuir relatórios de desempenho do atendimento de incidentes/problemas.
    10. Permitir o gerenciamento de categorias dos incidentes.
    11. Permitir a consulta de incidentes/problemas com base em campos específicos (ex: categorias, usuários, atendentes, etc.).
    12. Permitir anexos aos incidentes (imagens, documentos, etc.).
    13. Permitir a criação de modelos de incidentes pré-definidos.
    14. Permitir a criação de tarefas em um incidente, com o respectivo responsável.
25. Gerenciamento de Problemas:
    1. Permitir a criação de um problema a partir de um incidente.
    2. Permitir o envio de e-mail para o usuário e equipes de suporte quando o problema for aberto.
    3. Permitir associar prazos e ANS com as categorias de problemas.
    4. Permitir escalar o problema após limites determinados terem sido ultrapassados.
    5. Permitir relacionar ou abrir uma Requisição de Mudança a partir de um problema.
    6. Permitir que novas informações incluídas no registro sejam enviadas por e-mail ao usuário e/ou agente de suporte.
    7. Possuir modelos pré-definidos e customizáveis de processo de gerenciamento de problema de acordo com as melhores práticas da metodologia ITIL.
    8. Possuir modelos pré-definidos e customizáveis para abertura de problemas.
    9. Permitir a criação de campos customizáveis para o preenchimento do formulário de abertura do problema.
    10. Permitir a associação de um problema a outros problemas existentes, incidentes, requisições de serviços e itens de configuração.
    11. Permitir a criação de tarefas em um problema.
26. Gerenciamento de Configuração e de Ativos de TIC (SCM e IAM).
    1. Fornecer uma identificação única para cada Item de Configuração (IC).
    2. Permitir o registro, atualização, manutenção e exclusão dos ICs e seus respectivos atributos.
    3. Permitir a cópia de um IC e seus atributos para a geração de um novo IC, com identificação única.
    4. Possuir modelos pré-definidos e permitir a customização para ativos e fluxos de ciclo de vida de ativos, com base nas melhores práticas ITIL.
    5. Permitir a associação do tipo "pai-filho" entre os ICs.
    6. Permitir o cadastro de estações de trabalho com parâmetros customizáveis (ex: IP, ativo ou inativo, tamanho do storage, memória RAM, patrimônio, etc.).
    7. Permitir a consulta dos ICs e exportação de dados para relatórios.
    8. Permitir a visualização de requisições, incidentes, problemas e mudanças relacionadas aos ativos.
    9. Possibilitar o uso de componente de descoberta de ativos (Assets Discovery) para a descoberta automática de hardwares (servidores, switches, etc.) e softwares conectados à rede do Tribunal.
    10. O componente de descoberta deve ser capaz de manter uma base de dados das informações dos ICs, ativos e respectivas interdependências.
    11. Permitir a criação da linha de base (baseline) no CMDB.
    12. Possibilitar a geração de relatórios de discovery dos itens de configuração (ICs).
27. Gerenciamento de Mudanças (CE):
    1. Permitir que requisições de mudança sejam consultadas a partir de filtros como, no mínimo, data, status da mudança, IC, categoria e usuário criador.
    2. Fornecer modelos pré-definidos e customizáveis de fluxos de trabalho para mudanças com base nas melhores práticas da metodologia ITIL.
    3. Permitir a criação de modelos customizáveis de mudança (ex: campos de informações necessários, perguntas, riscos, impactos, etc.).
    4. Fornecer calendário de mudanças com acesso aos usuários e equipes de suporte.
    5. Permitir criar janelas de indisponibilidade para manutenção no calendário de mudanças.
    6. Fornecer painel de visualização de requisições de mudança (ex: em andamento, relacionadas a um IC específico, etc.).
    7. Permitir a configuração de envio de notificações relacionadas às mudanças via e-mail, SMS e push notification.
    8. Permitir que o solicitante questione e/ou reabra a solicitação de mudança não aprovada.
    9. Permitir a associação de um ou mais ICs afetados pela mudança na respectiva requisição.
    10. Permitir a associação de um ou mais serviços afetados pela mudança na respectiva requisição.
    11. Permitir a categorização da mudança por, no mínimo, urgência, prioridade e impacto.
    12. Permitir associar ANS às requisições de mudança.
    13. Registrar os andamentos realizados na solicitação de mudança, contendo data, hora e usuário.
    14. Permitir o controle/gerenciamento das aprovações das mudanças, com base em regras de negócio.
    15. Identificar conflitos entre requisições de mudança que impactem o mesmo IC ou serviço.
28. Gerenciamento do Conhecimento (KM):
    1. Fornecer base de conhecimento, permitindo aos usuários consultá-la de forma interativa e intuitiva.
    2. Permitir a criação, manutenção e remoção de informações e artigos, com base nas credenciais de acesso previamente definidas pelo administrador.
    3. Permitir associar artigos de conhecimento a incidentes, problemas ou requisições de serviços.
    4. Fornecer portal de autoatendimento ao usuário, com recomendações de artigos para solicitações mais comuns, possibilitando a auto resolução do chamado.
    5. Permitir ao usuário pesquisar por possíveis soluções para problemas.
    6. Permitir ao técnico encontrar soluções em scripts de atendimento com base no chamado aberto.
    7. Possibilitar o uso de indicadores de desempenho da utilização da base de conhecimento.

**item 2 - Confluence Premium**

**Especificações:**

1. Gerenciar os mais diversos conhecimentos da SETIC relacionados às operações, aos projetos e aos sistemas, permitindo organizá-los em páginas;
2. Permitir a criação e o gerenciamento de grupos de páginas relacionadas, com organização hierárquica, que podem ter relação com um projeto específico, com um produto específico ou com uma equipe específica;
3. Permitir a atribuição de permissões de acesso a grupos de páginas de conhecimento ou a páginas individuais, inclusive permitindo acesso público a algumas páginas da base de conhecimento;
4. Controle de permissões por usuário ou grupos de usuários;
5. Unificar todos os conhecimentos da SETIC em uma base única;
6. Possibilitar a inclusão de vídeos, apresentações e documentos nas páginas de conhecimento, com uma apresentação agradável e integrada à página;
7. Compatibilidade com bancos de dados SQL e APIs REST para acesso em tempo real de informações possibilitando a apresentação de resultados em páginas dinâmicas;
8. Permitir a criação de diagramas para Modelagem de Processos e Relacionamentos (BPMN 2.0, ERD, Fluxogramas, Diagramas Swimlane…), para Desenvolvimento de Software e Redes (UML, UML 2.5, AWS, Azure, Cisco, GCP, IBM…) bem como para organogramas, mapas mentais, plantas baixas e infográficos;
9. Permitir a criação de quadro brancos para Reuniões e Brainstormings;
10. Funcionalidade para gerenciar tabelas e dados, criar gráficos, adicionar planilhas nas páginas de conteúdo;
11. Facilitar a localização de conhecimentos na base através de uma ferramenta de pesquisa textual;
12. Permitir o acesso à ferramenta da base de conhecimento através de dispositivos móveis;
13. Permitir a criação de páginas de conhecimentos a partir de modelos (templates) previamente configurados na ferramenta;
14. Permitir realizar a gestão de configuração do produto mediante acesso de superusuário;
15. Versionar todas as mudanças realizadas nas páginas de conhecimento com possibilidade de consulta e restauração de versões anteriores;
16. Suporte para comentários em páginas, com notificações por e-mail;
17. Suporte a atalhos de teclado para navegação e edição rápida.

**item 3 - PocketQuery - SQL & REST for Confluence (Cloud)**

**Especificações:**

1. Plugin para funcionamento com o CONFLUENCE;
2. Permitir a compatibilidade com bancos de dados SQL e APIs REST para acesso em tempo real de informações possibilitando a apresentação de resultados em páginas dinâmicas.

**item 4 - Table Filter, Charts & Spreadsheets for Confluence**

**Especificações:**

1. Plugin para funcionamento com o CONFLUENCE;
2. Permitir a criação de diagramas para Modelagem de Processos e Relacionamentos (BPMN 2.0, ERD, Fluxogramas, Diagramas Swimlane…), para Desenvolvimento de Software e Redes (UML, UML 2.5, AWS, Azure, Cisco, GCP, IBM…) bem como para organogramas, mapas mentais, plantas baixas e infográficos;
3. Permitir a criação de quadros brancos para Reuniões e Brainstormings.

**item 5 - draw.io Diagrams & Whiteboards (Cloud)**

**Especificações:**

1. Plugin para funcionamento com o CONFLUENCE;
2. Funcionalidade para gerenciar tabelas e dados, criar gráficos, adicionar planilhas nas páginas de conteúdo.

**item 6 - Atlassian Guard (Cloud)**

**Especificações:**

1. Sincronização com Active Directory;
2. Integração com LDAP para autenticação de usuários;
3. Gerenciamento de licenças utilizadas;
4. Suportar Single Sign On (SSO);
5. Prover mecanismos de autenticação multi-fator;
6. Prover manual e meios de acesso à equipe de segurança do TRT7 para acessar e utilizar os registros de auditoria;
7. Registrar e manter registros de auditoria (logs) por pelo menos por 180 dias.

**item 7 - Jira Service Management - ativação, configuração e integrações**

**Especificações:**

1. Ativação e configuração de instância Cloud do Jira Service Management (com pessoas e unidades);
2. Integração com Confluence Cloud e Jira Server atualmente em uso no TRT7;
3. Configuração de catálogos de serviços;
4. Configurar fluxos de gerenciamento de serviços de TIC: gerenciamento de incidentes, gerenciamento de requisições, gerenciamento de problemas, gerenciamento de ativos, habilitação de mudanças, gerenciamento de catálogo, central de serviços, nível de serviços;
5. Descoberta de ativos de forma automatizada e alimentação do CMDB;
6. Configuração do portal de chamados e formulários de aberturas de requisições;
7. Automações e criação de regras para integrações.

**item 8 - Confluence Cloud - ativação, configuração, migração de dados e integrações**

**Especificações:**

1. Ativação e configuração de instância Cloud Confluence (com pessoas e unidades)
2. Levantamento de espaços, páginas e informações para migração do Confluence Server;
3. Ativação e adequação dos Plugins: draw.io Diagrams, Table Filter and Charts e PocketQuery
4. Migração e transferência de dados do Confluence Server para o Confluence Cloud;
5. Validação dos dados migrados;
6. Configuração e integração do Jira Service Management (Cloud) com o com Jira Server atualmente em uso no TRT7.

**item 9 - Treinamento em Jira Service Management**

**Especificações:**

1. Treinamento sobre a Jira Service Management (Cloud)para os servidores técnicos do TRT7;
2. Quantidade de alunos: 100;
3. Carga horária mínima de 12 horas;
4. Carga horária diária máxima de 4 horas por aluno;
5. Turma com no máximo 25 alunos;
6. O treinamento pode ser realizado presencialmente ou à distância. Neste último caso, não serão admitidas aulas gravadas, somente ao vivo para possibilitar a elaboração de perguntas e esclarecimento de dúvidas;
7. O ambiente de treinamento deverá ser montado tomando com base o ambiente real do TRT7, resultante dos serviços de  **ativação, configuração e integrações do** Jira Service Management (Cloud)
8. Deverá ser emitido certificado com a carga horária e conteúdo programático.
9. Será exigida a transferência de conhecimento sobre a integração entre Jira Service Management (Cloud), Confuence (Cloud) e Jira Server.

**Requisitos técnicos obrigatório relativos à solução:**

1. Toda solução deve ser fornecida na modalidade SaaS (Software as a Service)/Cloud, com pelo menos os seguintes requisitos:
   1. Armazenamento de arquivos ilimitado.
   2. Suporte do fabricante 24X7;
   3. Disponibilidade do serviço de 99,9%;
   4. Notificações/alertas por email;
   5. Fornecer recursos de automação e templates para criação de incidentes e problemas;
   6. Capacidade de integração para monitoramento passivo de sistemas de terceiros (ex: zabbix);
   7. Fornecer APIs para integrações com ferramentas de mercado;
   8. Possuir aplicativo disponível nas plataformas IOS e Android, possibilitando a utilização da ferramenta através de dispositivos móveis;
   9. A interface gráfica da ferramenta deverá ser 100% Web;
   10. Suporte a língua portuguesa (pt\_BR).

**Requisitos de segurança obrigatórios relativos à solução:**

1. Implementar criptografia em trânsito (TRT7 x Cloud);
2. Implementar criptografia sobre os dados armazenados na Cloud;
3. Utilizar um padrão de encriptação seguro, usando padrão internacional reconhecidamente aceito;
4. O ambiente em nuvem a ser disponibilizado ao TRT7 deverá ser protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas e implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados;
5. Conformidade com os padrões de segurança de nuvem, por meio de auditoria anual **Service and Organization Controls 2 (SOC 2)**;
6. Possuir documentação e comunicar seus recursos, papéis e responsabilidades de segurança da informação para o uso de seus serviços em nuvem;
7. Todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como **backups** de segurança, são de propriedade exclusiva do TRT7;
8. É vedado o uso de informações do TRT7 para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;
9. Ao término do contrato será exigida a devolução integral dos dados, informações e sistemas sob custódia ao TRT;
10. Deverá ser eliminado (após devolução de que trata o item anterior), ao término do contrato, qualquer dado, informação ou sistema do TRT7 sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados;
11. Notificar, imediatamente, ao TRT7 a ocorrência de incidente cibernético contra os serviços ou dados sob sua custódia;