

ANEXO I – Especificações Técnicas Da Solução

Este Anexo é parte integrante do Termo de Referência, como se transcrito fosse, compreendendo as especificações técnicas (características do objeto) da solução a ser selecionada.

CARACTERÍSTICAS GERAIS OBRIGATÓRIAS DO ERP WEB

Conforme Estudo Técnico Preliminar (ETP), a Administração possui uma série de necessidades com relação aos princípios da prestação do serviço público e de sua gestão, como princípio da eficiência, da continuidade, disponibilidade, segurança, regularidade, universalidade, qualidade, e a produtividade e bemestar das pessoas e de responsabilidade com o meio ambiente.

Nesse sentido, são características gerais obrigatórias do sistema de ERP a ser fornecido a Administração:

1. Os módulos que compõe o sistema devem aplicar a LEGISLAÇÃO vigente (Leis, decretos, etc.), federais e estaduais, adequando-as sempre que for necessário;
2. A solução deve ser projetada e desenvolvida para rodar em ambiente web, isto é que contenha as seguintes características básicas:
 - a. A aplicação deverá ser estruturada no conceito de “n” camadas, sendo ao menos elas: Front- End (operável através do navegador local), Servidor de Aplicação (podendo ser distribuído em “n” serviços distintos) e Servidor de Banco de Dados, por motivos de segurança da informação e usabilidade;
 - b. O Tráfego de dados entre o cliente e o servidor, deverá ser o mínimo necessário para execução das atividades do usuário, de maneira para que consuma menos link de internet, procurando transferir na maior parte dos casos apenas conteúdo no formato JSON, para interpretação e apresentação da camada Front-End;
 - c. Fica vedado o uso de aplicações tradicionais, desktop cliente-servidor (2 camadas) emuladas para serem executadas através de navegador ou por outros meios como área de trabalho remota, cujo protocolo RDP é inseguro, por motivos de segurança da informação e performance da aplicação;
 - d. Desenvolvido em linguagem para funcionamento pela internet (por exemplo: Java, PHP, C# ou outra que permita operação via Internet), de forma a garantir a segurança da informação e performance adequada no ambiente web e padrão de arquitetura em nuvem;
 - e. Ser operável através dos principais navegadores (padrão de mercado), nas seguintes versões: Internet Explorer (versão 11 ou superior), Firefox (versão 70 ou superior), Chrome (versão 70 ou superior), Microsoft Edge (versão 80 ou superior) e Safari (versão 10 ou superior);
3. O sistema deverá operar sob o paradigma de “Multiusuários” (mais de um usuário acessando ao mesmo tempo a aplicação e um usuário acessando múltiplas sessões ao mesmo tempo, permitindo mobilidade, acessibilidade, evitando retrabalho ou perda de informações e promovendo redução de custos operacionais), com integração total entre os módulos, garantindo que os usuários alimentem as informações em cadastro ÚNICO para todas as áreas (evitando-se inconsistências e erros sistemáticos), e que sejam integráveis automaticamente os existentes e os que vierem a ser implantados de outras áreas e ser *multientidades* (Órgão da Administração), buscando exercícios anteriores constantes do banco de dados, sem que seja

necessário sair de um sistema para entrar em outro;

4. Deverá possuir recursos próprios internos que permitam a operação através de *multi-janelas*, abrindo quantas telas forem necessárias simultaneamente para consulta e desempenho dos serviços, permitindo alternar entre exercícios e entidades, sem que seja necessário fechar a aplicação e abrir outra, ou sair de um módulo para entrar em outro;

5. Permitir na estrutura *multi-janelas* que o usuário alterne entre as janelas abertas na mesma sessão, na mesma aba do navegador e também faça ocultação (minimização) ou fechamento de janelas de forma geral;

6. Por questão de usabilidade, performance, segurança da informação e integridade, para operação do sistema não deverá ser exigido baixar em estações-cliente ou instalar recursos como runtimes e plugins exceto em casos onde houver necessidade de sistema intermediário para acesso a outros dispositivos (como leitor biométrico, impressoras, leitor de e-CPF/e-CNPJ) ou integração com aplicativos da estação cliente (como Microsoft Office, exibição de documentos PDF). Nesses casos, porém, não é permitida a integração através de aplicações que utilizem o recurso NPAPI dos navegadores (cujo suporte nativo foi abolido pelos navegadores padrão do mercado) como Applets Java, por questão de segurança da informação e integridade dos sistemas;

7. Utilizar na camada cliente apenas recursos padrões já amplamente difundidos, como HTML + CSS + JavaScript, não necessitando de instalação de nenhum plugin ou runtime adicional na estação cliente para operação do sistema, exceto nos casos de restrição de acesso a máquina local pelo navegador, e próprios da arquitetura de aplicações Web;

8. Permitir ao administrador local que, através de interface dentro do próprio Sistema, consulte sessões ativas no servidor de aplicação, disponibilizando informações como:

- a. Data de Início da Sessão;
- b. Data da Última requisição;
- c. Código e nome do usuário (quando sessão logada);
- d. Tempo total da sessão;
- e. Endereço IP da estação de trabalho.

9. Permitir ainda que:

- a. A sessão seja finalizada pelo administrador;
- b. O administrador consiga enviar mensagens internas no Sistema para um ou mais usuário(s) logado(s);

10. Possibilitar ao administrador local que este gerencie os acessos (permitir/restringir) aos logs de auditoria do Sistema;

11. O Sistema deverá fornecer múltiplos meios de auditoria (logs), sendo no mínimo:

- a. Logs de Ações realizadas no Sistema (operações como consultar, imprimir, por exemplo);
- b. Logs de Operações realizadas que afetem dados do banco de dados (incluir, excluir, alterar, etc.);
- c. Logs de Autenticação de usuários (toda ação de login/logout, incluindo dados adicionais);

12. Permitir que TODAS as telas de consulta do sistema, incluindo as consultas

personalizadas criadas através do gerador de consultas para a entidade, disponibilizem os seguintes recursos aos usuários:

- a. Informar e adicionar filtros personalizáveis pelas chaves de acesso disponíveis ao cadastro, de maneira isolada ou combinada;
- b. Disponibilizar diversos operadores de consulta: Menor ou igual, Maior ou igual, Igual, Contém, Não Contém, Contido em, Não contido em, Inicia com, Termina com e Entre. Observar logicamente a aplicação de cada operador conforme tipo do dado relacionado a ser pesquisado;
- c. Especialmente os operadores de conjunto “Contido em” e “Não Contido em”, devem disponibilizar opção para informar os dados por intervalo e intercalado, ex: 1,2,10-15, ou seja, o valor 1 e o valor 2, incluindo ainda os valores de 10 a 15;
- d. Realizar o reposicionamento, bem como o ajuste do tamanho e disposição das colunas disponíveis na consulta. Também deverá permitir ocultar ou exibir colunas;
- e. Realizar a ordenação da consulta de forma ascendente (do menor para o maior) ou descendente (do maior para o menor), utilizando uma ou várias colunas ao mesmo tempo;
- f. Recurso para seleção múltipla de registros, para que operações consideradas comuns para todas as linhas selecionadas possam ser executadas em lote, como por exemplo: excluir, imprimir e selecionar (quando for o caso);
- g. Permitir que o usuário selecione o número de registros por página e faça a navegação entre as páginas;
- h. Impressão da visualização atual da consulta, com opção de informar: título, formato de saída e totalizadores de colunas. Além disso deve permitir ainda a definição do formato de saída podendo ser no mínimo: PDF, DOC, DOCX, XLS, XLSX, HTML, XML, CSV. Deve-se permitir emitir todos os registros da consulta ou apenas aqueles selecionados;
- i. Permitir que o usuário retorne à consulta em seu estado original (default);
- j. Permitir que o usuário salve múltiplas preferências da consulta (campos em exibição incluindo posição e ordenação, informações de filtros em tela, etc.), permitindo definir um nome para cada uma delas e dispor da capacidade de compartilhar a preferência com todos os demais usuários, que possuam privilégio para a mesma consulta.

13. Possibilitar que o sistema disponibilize recurso para consistência de dados, de múltiplas áreas/módulos, constantes da base de dados, com o objetivo de coibir eventuais falhas geradas por dados inconsistentes, sejam esses gerados pela própria aplicação ao longo do tempo ou então migrados de aplicações legadas, permitindo também:

- a. A cada execução logs devem ser armazenados, para verificar se determinada consistência apresentou alguma falha na última execução;
- b. Emitir relatório com os apontamentos de inconsistências encontradas nas verificações, indicando a gravidade de cada uma;
- c. Executar as consistências em primeiro ou segundo plano (tarefa em background, no servidor). Caso em segundo plano, o usuário deverá ser alertado quando a mesma encerrar;

14. Realizar entrada de dados apenas via sistema, não sendo permitido o acesso direto ao Banco de Dados;

15. Oferecer total segurança contra a violação dos dados ou acessos indevidos às informações. Essa segurança total deve ser aplicada em camadas que vão desde validações no

lado cliente (front-end), passado pelo canal de comunicação (HTTPS), aplicando restrições de acesso aos endereços e portas dos serviços;

16. Acesso ilimitado de usuários simultâneos, sem necessidade de aquisição de novas licenças de qualquerdos softwares locados;

17. O sistema deverá conter Cadastro Único, sob o conceito de compartilhamento de dados e não integração por intermédio de outros artifícios, que podem danificar a integridade dos cadastros ao longo do tempo. Este deverá ser formado no mínimo com o seguinte conjunto de dados:

- a) Cadastro de Pessoas;
- b) Textos Jurídicos - Leis, Portarias, Decretos entre outros;
- c) Centros de custo/Organograma;
- d) Entidades;
- e) Bancos;
- f) Agências;
- g) Tributos;
- h) Moedas;
- i) Cidades;
- j) Bairros;
- k) Logradouros;
- l) Produtos;
- m) Assinantes de Relatórios Legais;
- n) CBO - Cadastro Brasileiro de Ocupações.

18. O Cadastro Único deve permitir o compartilhamento de dados com todos os demais módulos do sistema;

19. Garantir integridade referencial entre as tabelas do Banco de Dados, não permitindo a exclusão de informações que tenham vínculo com outros registros ativos via sistema e pelo banco de dados;

20. Ser construído com o conceito de controle de transações (ou tudo é gravado ou nada é gravado e nada é corrompido/comprometido), garantindo a integridade das informações do banco de dados em casos de queda energia, falhas de hardware ou software. O usuário sempre deverá ser informado, sobre a finalização com sucesso ou não das transações operacionais (inclusão, alteração e/ou exclusão de registros), antes deliberar o controle da aplicação para a realização de outras atividades;

21. Possuir recursos de segurança no SGBD para impedir que usuários não autorizados obtenham êxito em acessar a base de dados para efetuar consulta, alteração, impressão ou cópia. Não será permitido o acesso do sistema ao SGBD através de usuário DBA (Superusuário) do Banco de Dados, devendo existir usuário específico para acesso da aplicação e usuários adicionais para consulta;

22. Não será permitido a contratante ou terceiros acessos ao SGDB e Banco de Dados durante a vigência do contrato ou sua integração com outras aplicações, ainda que por cópias, ou bkp, sem anuência expressada Contratada desenvolvedora, sob pena de violação da Lei de Direitos Autorais e Lei de Proteção aos Direitos de Software, ao qual a Contratante será objetivamente responsabilizada civil e penalmente em caso de violação;

23. Fornecer em todo o sistema relatórios e consultas com opção de visualização em

- que uma determinada ação for realizada;
- b. Exigir que o usuário possa prosseguir apenas ao realizar nova autenticação, no ato da ação;
 - c. Solicitar para que um supervisor realize liberação em tela, para poder prosseguir;
 - d. Limitar e Liberar acesso temporário para determinadas ações do sistema, podendo configurar dia(s) do mês e horários do dia;
 - e. Permitir definir determinados usuários onde as regras não se aplicam (exceção);
 - f. Permitir definir regras para desativar ou ativar campos das telas cadastrais do sistema, definindo valor inicial (default) para um determinado campo, verificar se um campo (ou mais) foram alterados, a fim de determinar de forma condicional esses comportamentos podendo emitir mensagens de aviso, inibir a execução de uma ação como incluir, alterar ou excluir, enviar uma mensagem de e-mail para outro usuário, de acordo com regras da entidade sem depender de customização do sistema.
29. Manter histórico de acessos por usuário, rotina e ação, registrando a data, hora e o nome do usuário, IP local do usuário no momento da operação;
30. Manter LOG de auditoria de todas as inclusões, alterações e exclusões efetuadas nas tabelas do sistema, registrando:
- a. o tipo da operação realizada;
 - b. a partir de qual rotina do sistema ela fora executada;
 - c. a partir de qual estação de trabalho ela fora executada (ip da máquina local);
 - d. identificação do usuário;
 - e. tabela alterada;
 - f. operação realizada (inclusão, alteração ou exclusão);
 - g. os dados incluídos, alterados ou excluídos.
31. Na visualização dos registros de auditoria, deve-se exibir os novos dados para inclusões, novos dados e dados anteriores para alterações e dados anteriores para exclusões;
32. Permitir cruzamento de informações entre os módulos da solução;
33. Estruturar o sistema para que seja evitado a redundância de tabelas, exceto quanto a replicação de informações em outros ambientes (como integrações com outras aplicações externas);
34. Integrar com o Diretório Nacional de Endereços (DNE) dos Correios. A base de endereçamento deve ser atualizada mensalmente e um serviço de consulta de endereços deve ser disponibilizado integrado a aplicação, desta forma quando configurado para integrar com o DNE, toda vez que um endereço é informado no sistema o mesmo deve ser validado conforme o DNE e inconformidades alertadas ao usuário podendo ajustar o endereço;
35. As tabelas de cidade, estado e país, incluindo seus relacionamentos devem ser disponibilizadas pela ferramenta de gestão e atualizadas periodicamente de maneira automática sem que haja necessidade de manutenção desses dados pelos usuários, salvo quando o endereço for estrangeiro;
36. Consultar cidades disponibilizando pesquisa através no mínimo das seguintes chaves de acesso: Nome da Cidade, Nome do Estado, Sigla do Estado, CEP, Código DNE, Código Receita Federal e Código IBGE. Essas chaves de acesso são importantes pois permitirão o cruzamento de dados com outras bases de governo em esferas diferentes, cuja codificação de

idades é diversa, normalmente utilizando uma dessas;

37. Disponibilizar estrutura que permita configurar campos adicionais para determinadas rotinas, com as seguintes características mínimas:

- a. Permitir que através de configurações simples, sem necessidade de customização, personalize a adição de novos campos;
- b. Permitir criar agrupamentos de campos, para serem exibidos em conjunto em área específica nas janelas de entrada de dados já existentes no sistema, como área complementar;
- c. Permitir que seja definida uma ordem de exibição dos campos adicionais;
- d. Permitir definir o tipo do campo, podendo ser no mínimo: Texto, Numérico, Data, Valor, Lista, Hora, Booleano e Campo Texto Formatado.
- e. A opção lista deverá permitir a definição de listas estáticas e/ou dinâmicas sendo carregadas, por exemplo via SQL;
- f. A opção Texto, deverá permitir selecionar um formato de entrada, podendo ser no mínimo CPF, CNPJ, CEP, Telefone e E-Mail;
- g. Permitir definir um valor padrão para o campo bem como a obrigatoriedade do mesmo;
- h. Permitir definir regras, como exemplo: exibir uma mensagem caso determinado valor seja informado no campo, ou então desabilitar um campo caso determinado valor seja informado em outro;
- i. Permitir definir para o campo adicional, se o mesmo aceitará a entrada de arquivo digital relacionado, como uma imagem, arquivo PDF ou outro, podendo selecionar quais as extensões permitidas para entrada.

38. O sistema deverá dispor de recurso de Repositório de Certificados digitais, que garanta segurança contendo as seguintes funcionalidades mínimas:

- a. Permitir vincular certificados digitais do tipo A1, de propriedade do usuário, neste caso permitindo uso exclusivo dele para assinaturas digitais, ou seja, apenas quando ele estiver logado no sistema;
- b. Permitir vincular certificados digitais do tipo A1 para a entidade, neste caso permitindo uso compartilhado do certificado, mediante concessão de privilégio de uso;
- c. Permitir que o usuário crie um certificado digital auto assinado, para uso em assinaturas digitais do tipo Avançada, conforme Lei 14.063/2020. Este tipo de certificado deverá ser utilizado apenas pelo usuário;
- d. Realizar controle de vencimento de certificados no repositório, notificando o usuário toda vez que ele acessar a aplicação quanto a necessidade de renovação;
- e. Registrar em log exclusivo (auditoria) toda vez que o certificado é utilizado, indicando data/hora de uso, informações sobre o procedimento realizado e qual usuário estava logado no sistema no instante do uso.

39. Permitir o uso de Assinatura Digital na modalidade Qualificada (conforme Lei 14.063/2020) em procedimentos como login no sistema e atividades relacionadas a usuários externos;

40. Permitir o uso de Assinatura Digital, nas modalidades Básica, Avançada e Qualificada (conforme Lei 14.063/2020) nos seguintes procedimentos:

- a. Assinatura de Documentos Digitais Diversos;

- b. Após a emissão de relatórios, permitindo assinar o documento emitido;
- c. Pareceres.

41. Permitir assinatura digital de documentos diretamente pela aplicação, sem necessidade de utilizar outros sistemas ou recursos, exceto aqueles necessários para acesso ao dispositivo de leitura do certificado digital na máquina local do próprio usuário;

42. Permitir o uso de Solicitações de Assinatura, onde um usuário realiza a solicitação de assinatura de um ou mais documentos, para que outro(s) usuário(s) o façam, contendo os seguintes recursos:

- a. Permitir definir se a execução das assinaturas será de forma sequencial (um após o outro) ou não (todos ao mesmo tempo);
- b. Permitir que durante a assinatura de uma solicitação o usuário possa rejeitar um documento enviado para sua assinatura.

43. O procedimento de assinatura digital deverá ser simples e prático para o usuário, contendo os seguintes recursos/facilitadores:

- a. Permitir que sejam configurados carimbos/estampas de assinatura, por usuário ou para a entidade toda, com possibilidade de configurar o conteúdo a ser colocado como “estampa” sobre o documento PDF assinado;
- b. Exibir alerta para o usuário quando o mesmo já fez assinatura digital de um documento, podendo ele optar por cancelar a nova assinatura;
- c. Permitir realizar assinatura digital com certificados do repositório e/ou instalados localmente na máquina do usuário sejam nos modelos A1 ou A3;
- d. Os certificados devem ser listados para o usuário antes da assinatura para que ele possa escolher. Deverá listar apenas certificados do próprio usuário;
- e. O usuário deverá ver claramente quando um certificado está vencido;
- f. A ação de assinatura digital deverá ser transparente para o usuário, sendo operada diretamente do próprio sistema, através de interface padronizada (comum a todo o sistema), dentro da própria aplicação web, sem que haja necessidade de trocar de aplicação para executar o procedimento;
- g. A ação de assinatura digital, deverá exibir o documento que o usuário está realizando assinatura no ato da mesma (quando individual) ou permitir a visualização dos documentos relacionados (quando assinatura em lote). Desta forma o usuário/assinante saberá exatamente do que se trata e o que ele está assinando;
- h. Todo documento PDF assinado digitalmente, deverá conter estampa automática com informações sobre a consulta de autenticidade do mesmo incluindo endereço de consulta em QR CODE para poder fazê-lo através de leitura pelo Smartphone.

44. Controlar a emissão de relatórios, dispondo dos seguintes recursos:

- a. Emitir vários relatórios ao mesmo tempo, pelo mesmo usuário;
- b. Permitir que relatórios sejam colocados em execução através de fila de impressão e caso o usuário finalize a aplicação, mesmo assim o relatório continue em execução;
- c. Controlar para que um relatório em emissão para o usuário não possa ser colocado em execução novamente até que o primeiro finalize, quando os parâmetros de emissão forem iguais;
- d. Possuir opção para emitir e assinar digitalmente qualquer relatório impresso;
- e. Manter uma cópia do relatório emitido, armazenada no banco de dados, identificando cada emissão por um código único que deverá ser impresso junto com

o relatório em todas as páginas, com informações de: filtros utilizados, usuário que emitiu, data e hora de emissão e id do relatório emitido;

- f. Consultar relatórios emitidos, filtrando pelo ID da emissão do relatório ou por outros dados como modelo/layout, usuário que fez a emissão, data/hora da emissão, visualizando os detalhes da emissão como os parâmetros informados, bem como a opção de imprimir.

45. Possuir gerador de relatórios, com as seguintes características mínimas:

- a. Possuir um cadastro de “Formatos de Relatórios” sendo reutilizáveis por diversos relatórios e configuráveis: Tamanho de página, Margens do Documento, Cabeçalhos e Rodapé, contendo: Brasão, número da página, filtros utilizados, nome da entidade e Configurar marca d’água através do upload de imagem;
- b. Editar relatórios atuais ou adição de novos relatórios de forma avançada, contendo recursos como formatação de campos, adição de imagens ao corpo do relatório, configuração de agrupamentos, uso de códigos de barras/QR codes, etc. A edição avançada de relatórios poderá ser realizada por ferramenta externa a aplicação, desde que não haja custo adicional a contratante;
- c. Permitir que novos layouts sejam criados/alterados para os relatórios disponíveis no sistema, podendo esses layouts novos serem criados com base em cópia de layouts já existentes, sejam eles padrões ou não;
- d. Definir privilégios para os relatórios e consultas gerados a partir do gerador de relatórios e consultas;
- e. Permitir gerenciar os relatórios por versões, permitindo que uma nova versão do relatório seja criada e esta não afete o uso da aplicação pelos usuários enquanto não estiver totalmente finalizada. Permitir restaurar uma versão anterior se necessário.

46. O sistema deve possuir recurso de desenho, configuração e execução de workflow, com as seguintes características mínimas:

- a. Deverá fazer parte do sistema de gestão, no mesmo SGBD, sem necessidade de acesso ou integração com outro sistema;
- b. Permitir a realização de documentação, manual e/ou através do relacionamento de documentos digitais e textos jurídicos constantes no cadastro único;
- c. Permitir execução automática de funções e carregamento de formulário/telas integrantes da solução através de um gerenciador único.
- d. A ferramenta de Workflow, deverá permitir desenho de processos utilizando-se da metodologia BPMN (*Business Process Model and Notation*), incluindo Raias (horizontal e vertical), Eventos, Atividades, etc.
- e. Permitir o controle de ativação/desativação/homologação e versionamento de processos, possibilitando a evolução natural dos processos;
- f. Registrar a cada alteração histórico de alterações realizadas no Work-Flow, permitindo também visualizar em histórico cada manutenção realizada, contendo recursos para de comparar e restaurar entre uma alteração e outra.

47. Objetivando atender a regras impostas pela LGPD (Lei Geral de Proteção de Dados), os seguintes recursos mínimos são necessários na aplicação:

- a. O sistema deverá conter mecanismo que permita a configuração e o gerenciamento de “Termos e Condições de Uso”, tanto para usuários internos (funcionários) como para usuários externos (cidadãos). A entidade poderá configurar os termos conforme necessidade, individualmente por perfil de usuário e por serviço disponível no

portal;

- b. Possuir inventário dos Tratamentos de Dados Pessoais realizados em processos/operações do sistema de gestão, incluindo a(s) hipótese(s) previstas em lei em que eles estão relacionados, cadastrados no próprio sistema;
- c. Permitir que a entidade mapeie e cadastre outros Tratamentos de Dados Pessoais que a mesma realiza seja por meio digital, através de outros sistemas de gestão (de outras áreas) ou por meio físico;
- d. Deverá dispor de área exclusiva para que o cidadão possa visualizar todos os tratamentos de dados pessoais realizados pela entidade, incluindo aqueles que não são realizados no software de gestão (Transparência Ativa) e permitir que ele solicite relatório dos usos realizados (Transparência Passiva);
- e. Permitir emitir relatório automático dos relacionamentos do cidadão com a entidade, com base nos dados do sistema de gestão, informando quais são os vínculos que ele possui;
- f. O tratamento de dado pessoal poderá exigir o consentimento do usuário, nos casos em que não forem de interesse público. Nessa situação sempre que o tratamento for realizado deve-se verificar se há consentimento realizado e ativo do titular;
- g. Permitir definir quem é o Controlador local e indicar seus dados de acesso/contato em área exclusiva no portal da transparência;
- h. Permitir definir quem são o(s) Encarregado(s) de tratamento de dados pessoais indicados pelo controlador e disponibilizar seus dados de acesso/contato em área exclusiva no portal da transparência;
- i. No primeiro acesso do usuário a aplicação, seja usuário funcionário (interno) ou cidadão (portal), deve-se solicitar que o mesmo visualize as políticas de uso do sistema incluindo política de tratamento de cookies e realize o aceite deles, devendo este ficar registrado para posterior consulta e auditoria;
- j. Deverá dispor de WebService para que outras aplicações autorizadas possam verificar se há consentimento realizado pelo titular em determinado Tratamento de Dados mapeado.

48. Permitir realizar a impressão de documentos diretamente pelo dispositivo móvel (smartphone e/ou tablet), na plataforma Android (equipamentos naturalmente mais acessíveis), por meio de impressoras Térmicas Bluetooth. Deverá o fornecedor informar quais são os requisitos mínimos necessários, incluindo os equipamentos homologados.