TERMO DE REFERÊNCIA

OBJETO: Ferramenta de Gestão de Privacidade

I.Do Objeto

Constitui o objeto do presente a aquisição de Ferramenta de Gestão de Privacidade na modalidade software como serviço.

II.Justificativa da Contratação

A LGPD (Lei Geral de Proteção de Dados Pessoais), prevê que o controlador de dados, garanta que as normas e os princípios estabelecidos pela lei estejam sendo respeitados.

A ferramenta de Gestão de Privacidade servira como um recurso tecnológico de apoio ao gestor de privacidade e contribuirá para que o os direitos dos titulares de dados sejam atendidos de forma rápida e organizada.

III. Dos Serviços

a) Ferramenta de Gestão de Privacidade (SaaS)

Módulos:

- **Configurações gerais e de Segurança**

1. O sistema de gestão da privacidade deve ser acessível através dos navegadores de internet mais populares, sem limitações ou exigência de plugins ou complementos para sua plena execução.
2. O sistema deve funcionar em protocolo HTTPS para todas as requisições.
3. Deve ser possível registrar usuários adicionais com controle de perfil de acesso para cada um, e deve ser possível o registro de até 5 funcionários.
4. Deve ser possível configurar permissões de acesso e perfis com determinadas permissões conforme preferência do administrador.
5. O sistema deve permitir integração com mecanismos de autenticação interna como LDAP, AD e SSO (Single sign-on).
6. O sistema deve permitir autenticação através do protocolo SAML e também OpenID.
7. Deve ser possível configurar o provedor de envio de emails através de protocolo SMTP para notificação de alertas e mensagens do sistema.
8. O software deve funcionar, sem limitações, no idioma Português do Brasil, com exceção de palavras e termos comuns da língua inglesa como “mouse”.
9. A plataforma deve possuir manual para operação em idioma Português do Brasil.

- ✓ Toda e qualquer documentação, manuais, inclusive de API's e integrações, devem estar disponíveis no idioma Português do Brasil.

10. Deve permitir acesso através de dispositivos móveis como tablets e celulares através do navegador de internet.
11. Deve possuir trilha de auditoria com todas as ações e eventos que um determinado usuário do sistema realizou.
12. Deve ser possível configurar determinado usuário(s) como sendo o DPO(Encarregado) da organização.
13. O sistema deve permitir relacionar áreas de negócio, cargo e funções para um usuário do sistema.
14. Deve permitir configurar o tempo de timeout (tempo da sessão) dos usuários conectados na plataforma.
15. O sistema deve ter em um local centralizado todas as tarefas do projeto de adequação. As tarefas podem ser cadastradas em diferentes módulos do sistema.
16. Deve ter possibilidade de configurar a quantidade máxima de tentativas de login na plataforma.
17. A senha dos usuários deve expirar após um determinado número de dias, configurável pela plataforma.
18. O sistema deve permitir a importação de usuários administradores da ferramenta através de planilha excel.
19. O sistema deve permitir a importação de usuários administradores da ferramenta através de API REST.
20. O sistema deve permitir que se configure a quantidade máxima de dias que um determinado usuário pode ficar sem autenticar na ferramenta antes de ser automaticamente bloqueado.
21. Todos os módulos e recursos devem fazer parte da mesma plataforma e fabricante.
22. API - Todos os serviços (API) que a plataforma disponibiliza devem utilizar meios seguros de autenticação padrão oAuth2.0.
    - ✓ As credenciais de autenticação devem poder ser gerenciadas pelo administrador do sistema através da interface web.
    - ✓ O administrador deve poder gerar múltiplas chaves e gerenciar suas permissões.

❖ **Monitoramento de Sites**

1. O sistema deve realizar o monitoramento de websites da organização para identificar falhas, riscos de privacidade e outros critérios e verificações aqui especificadas.

2. Permitir o cadastro de websites para monitoramento sem limitação de quantidade de domínios
3. Para cada website cadastrado exigir a verificação de propriedade do domínio do website através de DNS ou conferência de arquivo hospedado no website;
4. Permitir informar uma periodicidade de recorrência do monitoramento automático.
5. Quando informada a periodicidade deve exibir a data agendada da próxima execução automática do monitoramento.
6. Exibir relatório técnico para que a área de tecnologia possa tomar providências quanto ao resultado do monitoramento.
7. Exibir relatório não-técnico para que a área de negócios possa tomar providências quanto ao resultado do monitoramento.
8. O monitoramento deve avaliar no mínimo os seguintes critérios, apresentando resultados em sistema web.
    - ✓ Existência de políticas de privacidade, políticas de cookies e termos de uso no site;
    - ✓ Existência de tratamento de dados sensíveis;
    - ✓ Validar se respeita o princípio da necessidade da coleta para o tratamento de dados pessoais;
    - ✓ Validar se a finalidade da coleta está bem definida para cada tratamento de dado pessoal;
    - ✓ Verificar o uso excessivo de recursos do navegador como “local storage”, “banco de dados”, “cookies”, “scripts” e “plugins”
    - ✓ Indicar se o website monitorado respeita o conceito de “privacidade por padrão”;
    - ✓ Validar a existência de compartilhamento de dados pessoais com terceiros;
    - ✓ Verificar se todas as páginas estão sendo tratadas em um canal seguro de criptografia ponta-a-ponta;
    - ✓ Exibir a lista de formulários, campos e classificação de risco para cada campo que represente um dado pessoal;
    - ✓ Exibir a lista de todos os identificadores eletrônicos (cookies) encontrados e seus metadados mais comuns.
9. Deve permitir indicar um endereço de email para envio de notificações quando um monitoramento completar a sua execução.
    - ✓ O email com a notificação deve possuir um relatório resumido da varredura realizada.
10. Deve permitir sincronizar o monitoramento com a gestão de cookies para sempre exibir os cookies mais atualizados na plataforma de gerenciamento de cookies.

11. Deve ser possível visualizar e navegar pelos monitoramentos anteriores (histórico de monitoramento) para poder comparar os resultados.
12. O sistema deve permitir o cadastramento de domínios extras vinculados ao website como no caso de subdomínios.

❖ **Gestão de Cookies**

1. Permitir o cadastro de grupos de cookies de modo que os mesmos possam ser exibidos em categorias.
2. Permitir ordenar os grupos de cookies de forma fácil utilizando recursos como "drag and drop".
3. Permitir definir um ou mais grupos de cookies como sendo "Obrigatórios" de modo que os cookies pertencentes a este grupo não irão solicitar consentimento do usuário.
4. Permitir agrupar cada cookie importado pelo "Monitoramento de sites" em um dos grupos registrados.
5. Permitir registrar novos cookies manualmente e também agrupá-los em um dos grupos registrados.
6. Permitir gerenciar os metadados de cada cookies com no mínimo os seguintes atributos:
    - ✓ Nome do cookie
    - ✓ Host do cookie
    - ✓ Tipo de cookie (Persistente ou de Sessão)
    - ✓ Responsável pelo cookie (se o próprio website ou um terceiro)
    - ✓ Finalidade do cookie
    - ✓ Nome do fornecedor
7. Para cada website deve ser permitido a criação de um número ilimitado de variações de janelas de consentimento dos cookies classificados anteriormente.
8. Permitir que o administrador configure as propriedades visuais de cada janela, sem precisar conhecer linguagem de programação, de forma fácil e prática, com no mínimo as seguintes possibilidades:
    - ✓ Alteração do título e descrição da janela;
    - ✓ Alteração das cores (fundo, borda, fonte, botões);
    - ✓ Inserção de links externos ;
    - ✓ Controle de botões e seus textos;
    - ✓ Exibição de botão para fechar o banner, aceitar os cookies ou rejeitar os cookies;
    - ✓ Controle de conteúdo adicional na janela com informações úteis para o usuário final (texto livre).
    - ✓ Inserção dinâmica de código CSS (folhas de estilo) para personalização mais técnica.

9. O administrador poderá optar em realizar o registro de logs de consentimentos de modo que cada consentimento registrado pelo usuário irá registrar um evento para análise e acompanhamento da administração.
10. Os logs de consentimento não devem gravar o IP e dados do navegador do usuário que consentiu, contudo, o administrador da ferramenta deve poder habilitar essa coleta de dados se ele achar necessário.
11. Deve permitir exibir para o administrador os logs de eventos de consentimento com no mínimo as seguintes informações:
    - ✓ Identificador anonimizado da origem da coleta;
    - ✓ Ação realizada pelo usuário (Aceitação de cookies, Rejeição de cookies, Aceitação de Grupos de cookies, Rejeição de Grupos de cookies, Aceitação de todos os cookies, Rejeição de todos os cookies)
    - ✓ Data e hora da ocorrência
    - ✓ IP e dados do navegador do usuário (se habilitado esse tipo de coleta pelo administrador)
12. Deve permitir que o administrador faça filtros no controle de logs de eventos de consentimento.
13. Deve exibir uma lista de todos os links de script (javascript) importados pelo módulo de "monitoramento de sites" e permitir que o administrador faça o vínculo de cada script com os seus cookies possíveis.
14. Deve permitir a geração de um código da janela para inserção no código-fonte do website de modo a exibir a janela de consentimento de cookies para o público final.
15. Deve permitir realizar o bloqueio de cookies de dois modos: Automático e Manual.
    - ✓ Bloqueio automático: Apenas a inserção do código no website é suficiente para que todos os cookies dos grupos "não obrigatórios" sejam bloqueados, ou seja, sem a necessidade de programação adicional.
    - ✓ Bloqueio manual: A inserção do código no website combinado com eventuais mudanças na estrutura do código-fonte do website é necessária para que todos os cookies dos grupos "não obrigatórios" sejam bloqueados.
16. Deve permitir exibir a janela de controle de consentimento nos websites vinculados.
17. Deve permitir que o usuário final faça a escolha entre aceitar ou rejeitar cookies com no mínimo as seguintes opções:
    - ✓ Aceitar todos os cookies;
    - ✓ Rejeitar todos os cookies;

- ✓ Aceitar grupos de cookies específicos;
- ✓ Rejeitar grupos de cookies específicos;
- ✓ Aceitar um cookie específico
- ✓ Rejeitar um cookie específico

18. O sistema deve permitir que se faça uma gestão de conteúdos adicionais na janela de cookies para exibição de políticas e termos de uso, por exemplo.
    - ✓ As políticas podem ser escritas pelo administrador da plataforma na própria ferramenta de cookies
    - ✓ O sistema deve poder importar políticas já escritas anteriormente.
19. O sistema deve exibir dashboards de aceites de cookies e transferência de dados entre países.
20. O sistema irá permitir duas formas de coleta do consentimento de cookies a ser exibida ao usuário:
    - ✓ Coleta baseada em cookies: O usuário poderá escolher individualmente qual o cookies dentro de um determinado grupo ele deseja habilitar.
    - ✓ Coleta baseada em grupos: O usuário poderá escolher um grupo de finalidades de coleta de cookies para fornecer o consentimento, no qual aceitando esta opção habilita-se todos os cookies agrupados neste.
21. A plataforma deve possuir integração nativa com o Google Tag Manager para facilitar a gestão das tags de controle.
22. A plataforma deve possuir integração nativa com sites desenvolvidos em Wordpress.
23. A plataforma deve possuir integração nativa com páginas desenvolvidas em SPA (Single Page Application) e AMP (Accelerated Mobile Pages).
24. Quando o administrador do sistema alterar qualquer finalidade de um cookie ou o sistema adicionar novos cookies, os usuários que aceitaram ou recusaram os cookies anteriormente devem ser questionados novamente ao voltar ao website.
25. Deve ser possível relacionar finalidades de tratamento de dados pessoais com categorias de cookies.

❖ **Gestão de Políticas**

1. Permitir a gestão de políticas para cada website cadastrado e que se possa definir políticas comuns para todos os websites.
2. Deve permitir o versionamento de políticas e suas alterações.
3. Deve permitir criar políticas privadas (internas) ou políticas públicas (com link aberto acessível ao público).
4. Deve permitir a edição das políticas em formato aberto (HTML) para aplicações na internet.

5. Deve permitir escolher modelos já prontos de políticas para personalização com no mínimo os seguintes modelos:
    - ✓ Código de conduta
    - ✓ Política de BYOD
    - ✓ Política de backup
    - ✓ Política de contingência
    - ✓ Política de cookies
    - ✓ Política de desligamento de funcionários
    - ✓ Política de privacidade
    - ✓ Política de privacidade do funcionário
    - ✓ Política de redes sociais
    - ✓ Política de retenção de dados
    - ✓ Política de utilização aceitável
    - ✓ Política do escudo de privacidade
    - ✓ Termos de uso
6. No caso da "Política de cookies" deve permitir exibir de forma atualizada um quadro resumo de todos os cookies mapeados no módulo de "Gestão de cookies" para o usuário final
7. Deve permitir imprimir a política em PDF.
8. Deve permitir gerar um link público da política para exibição em websites, envio por email, aplicativos entre outros.
9. Deve permitir o controle de revisões onde um usuário pode enviar para outro usuário registrado no sistema para revisão da política, que ficará pendente aprovação.
10. O sistema deve gerar uma chave de integridade da política e exibir essa chave no conteúdo da política.
11. O sistema deve permitir o gerenciamento de múltiplos leiautes de políticas com no mínimo as seguintes configurações:
    - ✓ Cores de fundo
    - ✓ Cores de fontes
    - ✓ Opção para customização do CSS de forma mais técnica
    - ✓ Opção para inserção de scripts e metatags
12. Deve permitir agregar uma área para coleta do consentimento do usuário em uma determinada política utilizando o módulo de gestão do consentimento.
13. Deve ser possível enviar uma política para aprovação de outro usuário cadastrado.
14. O sistema deve permitir que o usuário visitante navegue por todas as versões da política publicada.
15. O sistema deve permitir que o usuário visitante faça uma comparação visual das mudanças que foram feitas entre versões diferentes de uma política.

16. Deve ser possível conferir os consentimentos/atestamentos em uma política através de relatórios no sistema.

❖ **Gestão do Consentimento**

1. A plataforma deve possuir uma gestão de dados dos titulares identificados com no mínimo os seguintes atributos:
    - ✓ Nome
    - ✓ Email
    - ✓ Documento de identificação (CPF, CNPJ)
    - ✓ Telefone
    - ✓ Origem ou sistema (sistema que originou o cadastro)
2. O sistema deve fazer o registro de ID's anônimos (pseudo) que são titulares não identificados diretamente.
3. A plataforma deve oferecer gestão visual de todos esses titulares (identificados ou não) e fácil acesso aos seus consentimentos registrados
4. A plataforma deve permitir a busca por um Documento, email e por um ID de usuário de forma fácil
5. Deve permitir o cadastro de finalidades de consentimento e agrupá-las por categorias
6. Deve possuir controle de tempo máximo de retenção do consentimento de modo que a ferramenta faça a revogação do consentimento automaticamente após expiração da data
7. Para cada finalidade de consentimento deve permitir a inclusão de um ou mais atributos (dados pessoais) que serão coletados por essa finalidade
8. Deve permitir criar links para redirecionar o usuário que concedeu ou revogou um determinado consentimento
9. Deve possuir uma área de testes para que o administrador possa garantir o funcionamento da coleta de consentimentos antes de utilizá-la em seus sistemas
10. A plataforma deve permitir que se faça um filtro por titulares que concederam e/ou revogaram consentimentos de determinadas finalidades de processamento.
11. A plataforma deve possuir uma API REST para integração entre sistemas com documentação em Português do Brasil
12. A plataforma deve possuir um SDK em Javascript e para integração e pedido de consentimentos em portais web.
    - ✓ Deve ter SDK nativo para no mínimo os frameworks React.JS e Angular, devidamente publicados no repositório NPM para consulta
13. Deve permitir gerenciar a coleta de consentimentos em aplicativos para dispositivos móveis através de um SDK.

14. Exige-se que o SDK para aplicativos seja entregue para no mínimo as plataformas IOS (Apple) e Android (Google) em linguagem nativa, compatível com Android (Java/Kotlin) e IOS (Swift/Objective-C)
15. Deve ser possível cadastrar aplicativos para terem um controle de consentimentos.
16. Deve ser possível gerar chaves de segurança para utilização no aplicativo de modo a garantir outros aplicativos de maneira indevida utilizem o componente.
17. Deve permitir o controle das permissões a serem gerenciadas no aplicativo através de um sistema web onde cada permissão permite a escrita da sua finalidade para o usuário final.
18. Cada aplicativo pode ter no máximo uma política de aplicativos ativa.
19. Deve permitir que o usuário final habilite ou desabilite as permissões no aplicativo através da interface do controle de privacidade.
20. Deve ser fácil para o programador do aplicativo inserir um botão ou link para abrir a interface do controle de privacidade provido pela biblioteca a ser entregue, com documentação clara e sem necessidade de acoplamento de código em mão dupla.
21. Deve possuir dashboard de consentimentos com dados e estatísticas
22. Deve permitir que o operador do sistema faça a revogação ou aceite de consentimentos em nome de um titular para casos onde o titular não tenha como fazer a ação livre de consentimento.
    - ✓ No caso de registros feitos por operadores do sistema, a plataforma deve guardar todos os logs para auditoria dessa ação realizada.
23. Deve permitir vincular uma finalidade de consentimento com os registros das operações de tratamento (ROPA).
24. O sistema deve ter um relatório sintético de finalidades onde seja possível ver quantos consentimentos positivos ou negativos foram coletados para cada finalidade.
25. Se o administrador do sistema alterar uma finalidade, os usuários que aceitaram ou recusaram essa finalidade devem ser questionados novamente para atualizar o seu consentimento.
26. O sistema deve possuir um local para gerar um QRCODE para coleta de consentimentos que pode ser usada em atendimentos presenciais ou para enviar por canais digitais.
27. Como podem ter várias dezenas de funcionários coletando consentimentos em diferentes pontos de atendimento, o sistema deve ter uma extensão de navegador para acelerar a coleta de consentimentos com poucos cliques, sem que o funcionário precise estar conectado no sistema web.

28. O sistema deve ter uma área para que a empresa faça o pedido ou renovação de consentimentos de titulares por email.
    - ✓ Deve permitir a criação de campanhas para envio por email sem limitação do número de pessoas ou emails enviados.
    - ✓ Deve existir um local para configurar os templates/modelos de emails que serão enviados.
    - ✓ O administrador deve conseguir segmentar os titulares para criar diferentes segmentações e critérios para envio de email pedindo consentimentos.
    - ✓ O administrador deve conseguir relacionar diferentes finalidades de tratamento de dados para justificar a coleta do consentimento.

❖ **Pedidos dos titulares**

1. Deve ser possível gerenciar os pedidos dos titulares de dados pessoais na mesma plataforma.
2. Deve ser possível gerenciar as fases de atendimento do pedido e seus respectivos prazos de atendimento
3. Deve ser possível gerenciar o template de e-mails trocados entre o controlador e o titular do dado pessoal.
4. Os templates de email devem suportar o padrão HTML e a plataforma deve oferecer guias e variáveis para que o administrador possa personalizar o email.
5. Deve ser possível gerar um link do formulário de atendimento para inclusão em websites com o formulário de atendimento dos titulares de dados pessoais.
6. Deve permitir gerar links para o formulário de atendimento já pré-configurado em um determinado idioma
7. Deve ser possível oferecer ao titular dos dados pessoais no mínimo os seguintes direitos:
    - ✓ Confirmação da existência de tratamento
    - ✓ Correção de dados
    - ✓ Portabilidade de dados
    - ✓ Acessar meus dados
    - ✓ Remover todos os meus dados
8. Deve ser possível configurar os direitos acima personalizando nome, criando novos direitos ou removendo direitos existentes.
9. Deve ser possível alterar o idioma da ferramenta do usuário final para oferecer em outros idiomas além do Português do Brasil que deve ser o padrão.
10. Deve ser possível gerenciar os pedidos dos titulares de vários sites em uma só plataforma, podendo filtrar os pedidos de cada site.
11. Deve ser possível anonimizar os dados do titular uma vez o atendimento seja concluído conforme critério do controlador.

12. Deve ser possível verificar a integridade de um pedido (hash) através de webservice.
13. Deve ser possível imprimir todo o histórico do atendimento de um determinado pedido.
14. Deve ser possível responder o pedido do titular.
15. Deve oferecer interfaces de integração para outros sistemas através de padrões e protocolos conhecidos de mercado.
16. Deve ser possível inserir anotações privadas no atendimento do pedido.
17. Deve exibir um mecanismo de controle de segurança (captcha) no formulário público de atendimento.
18. Deve permitir configurar um endereço de email para receber as notificações de novos pedidos.
19. Deve permitir integração através de conectores de webservices com ferramentas internas para automatizar o atendimento dos titulares.
20. O titular que fez um pedido deverá receber um email para confirmar a sua identidade com um link seguro de confirmação.
21. A plataforma deve permitir personalizar de forma fácil a tela de confirmação que aparece após o titular abrir o link de confirmação com no mínimo as seguintes propriedades:
    - ✓ Ícone indicando o sucesso da confirmação
    - ✓ Cor de fundo da página
    - ✓ Cor de fundo da área de conteúdo
    - ✓ Mensagem de sucesso e sua respectiva cor de fonte
    - ✓ Mensagem customizada e sua respectiva cor de fonte
22. A plataforma deve permitir que o titular envie um arquivo em anexo na sua solicitação
23. A plataforma deve permitir que o responsável responda a solicitação do titular anexando um arquivo
24. A plataforma deve permitir realizar filtros por atributos comuns de atendimentos com no mínimo as seguintes propriedades:
    - ✓ Protocolo de atendimento
    - ✓ Datas de criação e de expiração
    - ✓ Nome do titular solicitante
    - ✓ Website destino
    - ✓ Tipo de direito solicitado
    - ✓ Fase de atendimento
25. Deve exibir em uma tela de atendimento todo o histórico de interações com o titular, desde todas as respostas até anotações e trilhas de auditoria
26. Deve registrar em trilhas de auditoria todas as mudanças e eventos de um atendimento

27. A plataforma deve possuir uma API REST para integração da plataforma de atendimento com outros sistemas da empresa
28. O sistema deve permitir que a empresa crie portais para atendimento dos titulares, sem limite de quantidade, com no mínimo as seguintes configurações possíveis:
    - ✓ Alteração de logotipo, cores e layout
    - ✓ Permitir mudanças no CSS para cada portal
    - ✓ Personalização avançada do HTML do portal
    - ✓ Permitir o cadastramento e alteração de dados de titulares
    - ✓ Permitir exclusão de titulares no portal
    - ✓ Exibir todos os pedidos do titular logado
    - ✓ Permitir que o titular responda os pedidos
    - ✓ Permitir que o titular veja o prazo de atendimento nos seus pedidos
    - ✓ Garantir que o titular consiga ver todos os seus consentimentos aceitos e revogados
    - ✓ Garantir que o titular consiga modificar o seu consentimento de forma livre
    - ✓ Garantir que o titular consiga encerrar um pedido criado anteriormente
    - ✓ Permitir que o titular consulte o status de um pedido através do protocolo e email, sem precisar autenticar
29. O sistema deve ter um local onde o operador do sistema possa criar pedidos em nome de titulares para ser usado em casos onde o titular esteja impossibilitado de exercer seu direito em um canal digital
30. Deve ser possível definir agentes (funcionários) responsáveis por um determinado pedido de titular
31. O formulário de pedidos dos titulares deve poder ser customizado com novos campos a qualquer momento.
    - ✓ Para cada novo campo deve ser possível definir uma expressão regular de validação
    - ✓ Para cada novo campo deve ser possível definir uma dependência com outro campo
32. Deve ser possível vincular tarefas relacionadas a um pedido de um titular de modo que outras pessoas do time possam trabalhar no atendimento.
33. O sistema deve apresentar um relatório sintético de atendimentos realizados mês a mês com no mínimo os seguintes filtros: Pedido recebidos, Respostas feitas, Pedidos sem resposta, Respostas do titular, Expiração de prazo.

❖ **Diagnósticos de áreas e Fornecedores**

1. A plataforma deve permitir o gerenciamento de modelos de diagnósticos de maturidade a serem realizados com interessados.
2. Cada modelo de diagnóstico deve permitir o cadastramento de uma ou várias categorias de questionários que fazem parte da entrevista de diagnóstico.
3. As questões devem ser dinâmicas. O administrador da plataforma deve pode criar questões com diversos tipos e formatos, sendo exigido no mínimo os seguintes formatos:
    - ✓ Campo texto para coleta de respostas em texto puro
    - ✓ Campo de caixa de marcação para coleta de respostas booleanas
    - ✓ Campo numérico
    - ✓ Campo de seleção de opções
    - ✓ Arquivo para upload
4. O sistema deve permitir o controle de tamanho máximo, tamanho mínimo e obrigatoriedade de cada campo.
5. Deve ser possível criar uma instância do modelo e gerar um formulário de entrevista.
6. O sistema deve permitir o envio do formulário de entrevista para usuários internos e usuários externos através de email
7. O sistema deve permitir o envio de formulário de entrevista para fornecedores, inclusive enviando para todos os fornecedores da base.
8. O sistema deve armazenar todas as respostas coletadas para posterior análise
9. A plataforma deve permitir o arquivamento de respostas já concedidas.
10. A plataforma deve possibilitar a geração de formulários dinâmicos sem limitação de perguntas para que áreas da empresa possam responder questões a respeito do tratamento de dados pessoais.
11. A plataforma deve possibilitar a geração de formulários prontos para atividades comuns no fluxo de tratamento de dados pessoais e procedimentos de segurança, sendo no mínimo formulários prontos para:
    - ✓ Relatório de impacto para processamento de dados pessoais (DPIA)
    - ✓ Relatório de impacto para uso do legítimo interesse (LIA)
    - ✓ ISO27001
12. O sistema deve permitir a configuração de normas e controles de conformidade.
13. Deve exibir dashboards e relatórios de maturidade para cada dimensão e para cada critério de conformidade
14. Deve permitir vincular um diagnóstico com um fornecedor para poder avaliar a maturidade do mesmo.
15. O sistema deve permitir configurar níveis de maturidade conforme metodologias conhecidas de mercado como CMMI

16. A plataforma deve permitir a criação de medidas de conformidade sugeridas para que a empresa possa saber quais são as medidas recomendadas para cada diagnóstico realizado
17. Deve ser possível importar uma planilha com as questões já pré-existentes
18. O sistema deve oferecer um controle de planos de ação com atividades utilizando metodologia Kambam
19. A plataforma deve poder relacionar atividades do plano de ação com responsáveis, prazo de conclusão e percentual de andamento
20. Deve ser possível vincular riscos de negócio com um determinado fornecedor
21. Deve ser possível exibir relatórios e dashboard com matriz de risco para fornecedores
22. O sistema deve permitir que o operador do sistema registre comentários internos sobre as respostas feitas pelo fornecedor

❖ **Data Mapping**

1. Deve permitir a gestão dos pontos de coleta de dados pessoais.
2. A gestão dos pontos de coleta de dados pessoais deve poder ser relacionado a algum website existente para que seja feito a análise de conformidade de sites.
3. Deve permitir o cadastramento de vários tipos de pontos de coleta como: banco de dados, API, formulários web, whatsapp, entre outros meios analógicos ou digitais.
4. Deve possuir sistema para registro de operações de tratamento de dados (ROPA), sem limitações.
5. Deve ser possível agrupar as operações de tratamento (ROPA) para facilitar a organização
6. Deve permitir a gestão de fornecedores para que seja feita uma análise de risco de processamento de dados pessoais.
7. Deve permitir vincular um fornecedor com qualquer país para que seja controlado a transferência internacional de dados.
8. O cadastro do fornecedor deve permitir informar os contatos com o encarregado pelo tratamento de dados pessoais.
9. O sistema deve ter uma base de fornecedores comuns de mercado já populada para importação de modo que facilite o trabalho.
10. O sistema deve permitir a importação de fornecedores através de planilha excel.
11. O sistema deve permitir que relatórios e dados de due diligence sejam anexados ao registro do fornecedor
12. O cadastro do fornecedor deve permitir informar o link do DPA, link da política de privacidade e link do DSAR (canal dos titulares) do fornecedor.

13. Deve possibilitar o cadastramento de sistemas e entidades para que seja feita uma análise dos sistemas digitais, setores da empresa, profissionais ou qualquer outra entidade que venha a processar dados pessoais.
14. Deve permitir vincular uma entidade de tratamento de dados pessoais com um fornecedor previamente cadastrado.
15. Deve permitir vincular um usuário do sistema com uma entidade.
16. Deve permitir vincular uma entidade com qualquer país para que seja controlado a transferência internacional de dados.
17. Deve permitir o cadastro de dados pessoais dentro de uma atividade de tratamento de dados.
18. Deve permitir vincular metadados diversos (tags) às operações de tratamento com “chave=valor”
19. Deve permitir a gestão de riscos relacionados a cada ROPA com no mínimo as seguintes propriedades de controle:
    - ✓ Nível do risco
    - ✓ Categoria de risco (Reputação, Financeiro, Operacional, etc..)
    - ✓ Ameaça
    - ✓ Vulnerabilidade
    - ✓ Controles e Normas
    - ✓ Informações sobre a ameaça e vulnerabilidades
    - ✓ Plano de tratamento do risco
    - ✓ Data da solução
    - ✓ Usuário responsável pela mitigação e tratamento do risco
20. O administrador deve poder personalizar novas ameaças, vulnerabilidades, controles e categorias.
21. O sistema deve permitir que o administrador crie modelos de riscos prontos e reutilize estes modelos quando for atribuir um novo risco.
22. O sistema deve sugerir possíveis riscos no ROPA conforme o preenchimento do mesmo vai acontecendo.
23. Deve permitir cadastrar atributos (dados pessoais) vinculados ao ROPA.
24. Deve permitir importar atributos (dados pessoais) de websites cadastrados no sistema (campos de formulários).
25. Deve permitir informar se um dado pessoal é relacionado a criança ou adolescente.
26. Deve permitir cadastrar transações e fluxos de dados com no mínimo as seguintes propriedades:
    - ✓ Direção da transação (saída de dados ou entrada de dados)
    - ✓ Entidade de tratamento de dados de origem
    - ✓ Entidade de tratamento de dados de destino
    - ✓ Quantidade média de dados afetados pela transação

- ✓ Volume de dados transacionados
- ✓ Seguranças empregadas na transação

27. Deve permitir um trabalho de classificação e mapeamento de tratamento de dados pessoais para cada atributo de cada ROPA registrado.
28. Deve permitir informar para cada atributo no mínimo as seguintes informações relacionadas com o fluxo de tratamento de dados pessoais:
    - ✓ Validação se é um dado identificado ou identificável
    - ✓ Validação se é um dado sensível e um dado obrigatório
    - ✓ Aspectos de criptografia e segurança do dado
    - ✓ Aspectos de auditoria e logs do dado
29. Deve permitir o registro das finalidades de processamento para cada dado pessoal e para cada operação de tratamento.
30. Deve permitir cadastrar categorias de dados pessoais (atributos) para melhor classificá-los
31. O controle de finalidades de processamento deve prever todas as hipóteses de tratamento de dados pessoais da LGPD e GDPR.
    - ✓ No caso da hipótese de tratamento “Legítimo interesse” deve ser viável realizar um teste de balanceamento de interesses seguindo as boas práticas do mercado.
    - ✓ No caso da hipótese de tratamento “Consentimento” deve ser viável realizar um controle adicional para justificar o uso dessa hipótese
32. Deve possuir ferramentas de controle de transferência internacional de dados para orientar o controlador quanto aos riscos dessa ação.
33. Deve possuir ferramentas de controle quanto à remoção de dados pessoais para orientar o controlador quanto aos riscos dessa ação.
34. Deve ser possível visualizar de modo gráfico o ciclo de vida dos dados pessoais dentro da organização.
35. Deve ser exibido relatórios e gráficos de controle do mapeamento de dados tais como:
    - ✓ Relatório de dados pessoais sendo processados
    - ✓ Relatório com matriz de riscos
    - ✓ Relatório de transferência internacional de dados
36. Deve possuir um cadastro de regulamentações para uso no mapeamento de dados quanto aos aspectos regulatórios
37. Deve ser possível criar modelos de classificação de atributos para poder re-utilizar um modelo em um novo atributo
38. Deve possuir API REST para integração da plataforma com outros sistemas

39. O Sistema deve gerar automaticamente o DPIA(RIPD) - relatório de impacto de proteção de dados para uma ou mais atividades de processamento conforme escolha do usuário
40. O sistema deve permitir a impressão do relatório de impacto gerado.
41. Deve ser possível vincular tarefas relacionadas a uma operação de tratamento de modo que outras pessoas do time possam trabalhar na adequação.
42. A plataforma deve ter um relatório de temporalidade de modo a exibir em uma única tela todos os dados pessoais e seu prazo de retenção para o devido controle do prazo de processamento do dado.
43. A plataforma deve ter um relatório sintético de bases legais que mostre a quantidade de operações de tratamento, quantidade de dados pessoais e quantidade de dados pessoais sensíveis para cada base legal da LGPD.
44. A plataforma deve possuir uma representação visual/gráfica de todo o ciclo de vida dos dados pessoais de uma determinada operação de tratamento evidenciando a coleta, tratamento, distribuição e remoção de dados.
45. A plataforma deve permitir a exportação do ROPA em Excel e PDF de um ou vários processos.
46. A plataforma deve permitir a importação do ROPA que tenha sido feito em excel.
    - ✓ O formato do excel pode ser o modelo proposto pela ferramenta.
    - ✓ Caso o modelo não seja o modelo proposto pela ferramenta, a ferramenta deve ter um recurso de conversão automatizada que permite que o administrador correlacione as colunas do excel não-padrão e gere automaticamente o excel padrão.
47. O sistema deve possuir uma base de normas e controles para diferentes frameworks e padrões do mercado sendo necessário no mínimo ter disponível: ISO/IEC 27005, AICPA TSC 2017 (SOC 2), NIST (CSF) Core v1.1, LGPD, ISO/IEC 29100:2011, ISO/IEC 27701:2019 e ISO/IEC 27001:2013.

❖ **Integrações**

1. O sistema deve permitir a criação de conectores web para que sejam chamados quando determinados eventos acontecerem.
2. Deve ser intuitivo para o operador da plataforma a criação de conectores sem que seja necessário qualquer programação de software adicional à existência do próprio serviço de destino.
3. Os eventos que devem gerar rotinas de integração devem ser no mínimo:
    - ✓ Quando um novo titular é registrado na plataforma
    - ✓ Quando um novo pedido de titular é registrado
    - ✓ Quando um pedido de titular possui mudança de estado ou conteúdo

- ✓ Quando um novo consentimento é registrado
- ✓ Quando um consentimento existente é modificado

4. Quando ocorrer algum evento o sistema deve enviar para a URL destino as informações suficientes para que seja possível capturar os dados do evento registrado.
5. O conector com URL destino deve suportar diferentes formas de autenticação como senha, oAuth2.0 e Bearer.

❖ **Gestão de Incidentes**

1. A plataforma deve permitir a criação manual de incidentes
2. A plataforma deve permitir a criação automática de incidentes através de uma API de integração
3. Deve ser possível configurar os diferentes tipos de incidentes
4. O sistema deve permitir definir responsáveis por um incidente
5. A plataforma deve vincular diagnósticos do módulo de diagnósticos com um incidente de modo a mitigar incidentes de fornecedores e seu nível de maturidade
6. O sistema deve exibir uma linha do tempo com todos os eventos e mudanças de um incidente
7. Deve ser possível cadastrar vários impactos à privacidade do titular causado por um incidente
8. O sistema deve permitir relacionar usuários, ativos e empresas com um determinado incidente
9. Deve ser possível modificar os dados e o status de um determinado incidente
10. Deve ser possível vincular riscos com um determinado incidente
11. Deve ser possível anexar documentos e políticas em um determinado incidente
12. A plataforma deve exibir um relatório de incidentes com no mínimo os critérios abaixo:
    - ✓ Linha do tempo de incidentes no período
    - ✓ Incidentes por tipo de incidente
    - ✓ Incidente pelo seu estágio de andamento
    - ✓ Incidente por fornecedores
    - ✓ Incidente por fonte/origem
    - ✓ Incidente por nível do risco
13. Deve ser possível vincular tarefas relacionadas a um incidente de modo que outras pessoas do time possam trabalhar na mitigação.
14. A empresa pode realizar a comunicação do incidente pela própria plataforma, tanto para titulares, DPO quanto para a ANPD.
    - ✓ No caso da comunicação para os titulares ou DPO, o sistema deve enviar por email conforme modelos e parâmetros da ferramenta.

- ✓ No caso da ANPD o sistema deve gerar de forma automatizada o modelo de relatório proposto pela ANPD para comunicação de incidentes.

❖ **Descoberta de dados**

1. Deve possuir API REST para integração da plataforma com outros sistemas de modo que um sistema terceiro possa fazer buscas por dados pessoais e por tipos de dados pessoais encontrados
2. Deve permitir o monitoramento de no mínimo os seguintes ambientes:
   - ✓ Arquivos (via upload direto)
   - ✓ PostgreSQL 9.2 e superiores
   - ✓ Oracle 9, 10, 11 e superiores
   - ✓ MySQL e MariaDB
   - ✓ IBM DB/2
   - ✓ IBM DB/2 - AS/400
   - ✓ SAP HANA
   - ✓ MongoDB versões 4.4 e inferiores até 3.7
   - ✓ Ambientes de FTP/FTPS
   - ✓ Ambientes através de SSH (SFTP)
   - ✓ Sistema de arquivos (storage/NFS)
   - ✓ ElasticSearch
   - ✓ Apache Solr
   - ✓ Microsoft 365 (Onedrive, exchange e sharepoint)
   - ✓ Google Drive
   - ✓ Computadores de uma rede através do download de agentes
3. Deve permitir o agendamento de execução do fluxo de descoberta de dados
4. Deve permitir, por livre escolha da contratante, que a instalação do módulo seja feita em infraestrutura de propriedade da contratante, sem prejuízo dos recursos oferecidos e sem mudança em preço
5. Deve permitir a customização de busca de dados pessoais a partir do uso de expressões regulares ou inteligência artificial
6. Deve possuir controle de tipos de dados(categoria) e severidade de cada tipo
7. Deve permitir percorrer todos os resultados da busca e saber onde estão os dados pessoais
8. Deve permitir integração com o módulo de atendimento de pedidos para acelerar a automação do pedido
9. O sistema deve possuir conexão nativa com o módulo de data mapping (mapeamento de dados) de modo que uma varredura já faça o trabalho inicial de

mapeamento de dados com as operações de tratamento encontrados e seus dados pessoais

10. O sistema deve permitir remover dados pessoais encontrados pelo sistema e colocar o dado em uma 'blacklist' de dados para não serem novamente indexados
11. O sistema deve permitir limpar os resultados de uma varredura anterior quando for executar uma nova varredura.
12. O sistema deve ter componentes para Windows, Linux e Mac para que possa ser feito uma varredura de arquivos no computador em busca de dados pessoais armazenados.

❖ **Open Banking**

1. A plataforma deve oferecer gestão visual de todos esses titulares (pessoas físicas ou jurídicas) e fácil acesso aos seus consentimentos registrados
2. A plataforma deve permitir a busca por um Documento, email e por um ID de usuário de forma fácil
3. Deve possuir o cadastro de finalidades de consentimento conforme normativa vigente do Banco Central do Brasil
4. Deve possuir controle de tempo máximo de retenção do consentimento conforme regras vigentes definidas pelo Banco Central do Brasil de modo que a ferramenta faça a revogação do consentimento automaticamente após expiração da data
5. Deve possuir a possibilidade de envio de dados cadastrais e transacionais ou somente cadastrais do titular de dados
6. Para cada finalidade de consentimento deve permitir a inclusão de um ou mais atributos (dados pessoais) que serão coletados por essa finalidade
7. Deve possuir uma área de testes para que o administrador possa garantir o funcionamento da coleta de consentimentos antes de utilizá-la em seus sistemas
8. A plataforma deve permitir que se faça um filtro por titulares que concederam e/ou revogaram consentimentos das finalidades de processamento.
9. Deve permitir o controle das permissões a serem gerenciadas no aplicativo através de um sistema web onde cada permissão permite a escrita da sua finalidade para o usuário final.
10. Cada aplicativo pode ter no máximo uma política de aplicativos ativa.
11. Deve permitir que o usuário final habilite ou desabilite as permissões no aplicativo através da interface do controle de privacidade.
12. Deve ser fácil para o programador do aplicativo inserir um botão ou link para abrir a interface do controle de privacidade provido pela biblioteca a ser entregue, com documentação clara e sem necessidade de acoplamento de código em mão dupla.
13. Deve possuir dashboard de consentimentos com dados e estatísticas

14. Deve permitir que o operador do sistema faça a revogação ou aceite de consentimentos em nome de um titular para casos onde o titular não tenha como fazer a ação livre de consentimento.
    - ✓ No caso de registros feitos por operadores do sistema, a plataforma deve guardar todos os logs para auditoria dessa ação realizada.
15. Deve permitir vincular uma finalidade de consentimento com os registros das operações de tratamento (ROPA).
16. O sistema deve ter um relatório sintético de finalidades onde seja possível ver quantos consentimentos positivos ou negativos foram coletados para cada finalidade.
17. Se o administrador do sistema alterar uma finalidade, os usuários que aceitaram ou recusaram essa finalidade devem ser questionados novamente para atualizar o seu consentimento.
18. O sistema deve possuir um local para gerar um QRCODE para coleta de consentimentos que pode ser usada em atendimentos presenciais ou para enviar por canais digitais.
19. Como podem ter várias dezenas de funcionários coletando consentimentos em diferentes pontos de atendimento, o sistema deve ter uma extensão de navegador para acelerar a coleta de consentimentos com poucos cliques, sem que o funcionário precise estar conectado no sistema web.
20. O sistema deve ter uma área para que a empresa faça o pedido ou renovação de consentimentos de titulares por email.
    - ✓ Deve permitir a criação de campanhas para envio por email sem limitação do número de pessoas ou emails enviados.
    - ✓ Deve existir um local para configurar os templates/modelos de emails que serão enviados.
    - ✓ O administrador deve conseguir segmentar os titulares para criar diferentes segmentações e critérios para envio de email pedindo consentimentos.
    - ✓ O administrador deve conseguir relacionar diferentes finalidades de tratamento de dados para justificar a coleta do consentimento.

b) Implantação

1. A implantação deverá ser efetuada por equipe especializada, com início imediato, após a assinatura do contrato.

2. A contratada deverá apresentar em reunião de Abertura de projeto (Kick off) roteiro de implantação e de configuração da plataforma.

3. A implantação deve ser concluída em até 15 dias uteis após a assinatura do contrato.

c) **Treinamento**

1. Treinamentos de capacitação para uso da ferramenta, com certificação de usuários.

2. O treinamento deverá ser ministrado para até 4 funcionários da SP-PREVCOM.

d) **Suporte**

1. Serviço de suporte com analista em LGPD dedicado para solução de problemas de qualquer natureza relativos à utilização da plataforma.

2. O suporte deve contar com Canal de Help Desk Online para abertura de chamados diretos a equipe.

IV. Dos prazos de vigência contratual

O contrato terá vigência por **12 meses**, podendo ser prorrogado até o limite legal.

V. Do início da prestação dos serviços

Os serviços contratados, terão início no dia subsequente à assinatura do contrato.

VI. Obrigações da contratada

1. Obedecer às especificações constantes neste Termo;

2. Indicar um responsável pelo contrato de serviço, com a responsabilidade de ser um ponto de contato entre as partes;

3. Responsabilizar-se pela entrega do material/execução dos serviços, ressaltando que todas as despesas de transporte e outras necessárias ao cumprimento de suas obrigações serão de responsabilidade da contratada;

4. Realizar a entrega/executar os serviços dentro do prazo estipulado;

5. O retardamento na entrega do objeto/execução dos serviços, não justificado considerar-se-á como infração contratual;

6. Manter com a Contratante relação sempre formal, por escrito, ressalvados os entendimentos verbais motivados pela urgência, que deverão ser de imediato, confirmados por escrito;

7. A CONTRATADA deverá manter total sigilo das informações disponibilizadas pela Fundação, não utilizando em proveito próprio ou alheio;

VII. Obrigações da Contratante

1. Exercer a fiscalização da execução do serviço,

2. Tomar todas as providências necessárias ao fiel cumprimento das cláusulas contratuais;

3. Efetuar o pagamento devido, na forma estabelecida neste Termo;

4. Facilitar por todos os meios ao cumprimento da execução pela contratante, dando-lhe acesso e promovendo o bom entendimento entre seus funcionários e empregados da contratada, cumprindo com as obrigações preestabelecidas;

5. Comunicar por escrito à contratada o não recebimento do objeto/não prestação do serviço, apontando as razões de sua não adequação aos termos contratuais;

6. À Contratante, é reservado o direito de, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização sobre o cumprimento das especificações e condições deste objeto;

VIII. Atestação e Condições de Pagamento

A aferição/atestação dos serviços acontecerá mediante a finalização ou a execução de cada produto/SERVIÇO, acompanhado de relatório objetivo das atividades desenvolvidas no período.

IX. Dos Pagamentos

Os pagamentos dos serviços serão efetuados em 30 dias da data da apresentação /protocolo da nota fiscal/fatura, quando toda a documentação exigida estiver em conformidade.

X. Dos valores das propostas

Os valores propostos deverão contemplar todas as despesas relacionadas à prestação de serviços, tais como (mas não se limitando a) despesas de viagem, despachante, cópias, impressões de grande volume, autenticações, correios, publicações, certidões e taxas de atos notariais, bem como despesas relativas à mão-de-obra e respectivos encargos sociais, previdenciários e trabalhistas e todos os tributos incidentes na prestação dos serviços.

XI. Planilha de proposta:

ITEM	Serviço/Produto	Valor Mensal	Valor Total (12 meses)
III. a)	Ferramenta de Gestão de Privacidade - SaaS – válido por 1 ano.	**R$_____,___**	**R$_____,___**
ITEM	**Serviço/Produto**	**Valor único**	**Valor total**
III. b)	Implantação	R$_____,___	R$_____,__
ITEM	**Serviço/Produto**	**Valor único**	**Valor total**
III. c)	Treinamento	R$_____,___	R$_____,___
ITEM	**Serviço/Produto**	**Valor Mensal**	**Valor Total (12 meses)**
III. d)	Suporte	R$_____,___	R$_____,___

XII. Do prazo de validade da proposta

O prazo de validade da proposta será de 60 (sessenta) dias, contados de sua apresentação.