MEMORIAL DESCRITIVO

OBJETO: Contratação de Empresa especializada em Tecnologia da Informação para orientar na Readequação dos Sistemas de Informática utilizados e Tratamento dos Dados Coletados pela Autarquia à Lei Geral de Proteção de Dados, através da Definição das Diretrizes Essenciais da LGPD a serem aplicadas na SAEC.

1. OBJETIVO

O objetivo da Dispensa de Licitação é a contratação de uma empresa especializada para apoiar a SAEC na implementação de projeto para atender a Lei Geral de Proteção de Dados.

2. ESCOPO MACRO

2.1. **Estruturar o Projeto de Implementação da LGPD**
2.2. **Análise de Gaps**
2.3. **Inventário de Dados**
2.4. **Plano de Ação**
2.5. **Implementação de Políticas e Processos Operacionais**
2.6. **Treinamento e Conscientização**

3. ESPECIFICAÇÕES E FASES DO PROJETO

3.1. **Estruturar o Projeto de Implementação da LGPD**

3.1.1. A estruturação do Projeto de Implementação da LGPD será a primeira etapa do projeto.
3.1.2. Esta etapa representará 10% do valor total do contrato.
3.1.3. Estabelecimento da Estrutura de Governança de Privacidade e Proteção de Dados.

3.1.4. Orientar a alta administração, para que esta compreenda as implicações da Lei, positivas e negativas, para que possam alocar os recursos necessários para obter e manter a conformidade com a Lei Geral de Proteção de Dados. Para isto deverá:

3.1.4.1. Expor os riscos envolvidos no processo de construção da segurança da informação, privacidade e proteção de dados e os benefícios da conformidade com a LGPD;

3.1.4.2. Instituir o Comitê Gestor da Privacidade e Proteção de Dados responsável pela avaliação dos mecanismos de tratamento e proteção dos dados existentes e pela proposição de ações voltadas a seu aperfeiçoamento, visando o cumprimento das disposições da Lei n. 13.709;

3.1.4.3. Definir funções e atribuir responsabilidades pela privacidade dos dados em toda a organização (rede de privacidade);

3.1.4.4. Elaborar a Política de Ação Regulatória de Privacidade, ou seja, a norma que irá reger os objetivos, obrigações, funções, poderes e prerrogativas do Comitê Gestor.

3.2. **Análise de Gaps**

3.2.1. A Análise de Gaps será a segunda etapa do projeto.

3.2.2. Esta etapa representará 10% do valor total do contrato.

3.2.3. Realizar um "gap analysis" detalhado para ajudar a SAEC a avaliar seu fluxo de trabalho, seus processos e procedimentos atuais para identificar as inconformidades que a Autarquia apresenta em relação à LGPD. Essa análise de Gaps deverá conter pelo menos:

3.2.3.1. Auditoria do status de conformidade com os requisitos da LGPD;

3.2.3.2. Detecção de falhas de conformidade para correção.

3.2.3.3. Definir o Plano de Avaliação de Riscos;

3.2.3.4. Identificar os Riscos;

3.2.3.5. Analisar e Avaliar os Riscos;

3.2.3.6. Definir os Métodos de Correção e Controle dos Riscos identificados.

3.3. **Inventário de Dados**

3.3.1. O Inventário de Dados será a terceira etapa do projeto.

3.3.2. Esta etapa representará 20% do valor total do contrato.

3.3.3. Determinar quais áreas da Empresa se enquadram no escopo da LGPD;

3.3.4. Avaliar se a proteção de dados por design e por padrão foi incorporada em processos e sistemas;

3.3.5. Determinar e avaliar as categorias de dados que a empresa possui;

3.3.6. Determinar de onde vêm e as bases legais que justifiquem o processamento;

3.3.7. Classificar os dados de acordo com a sensibilidade e o tipo de dados pessoais, conforme definido pelos contextos estatutários, regulamentares e contratuais apropriados;

3.3.8. Realizar e manter um inventário dos tipos de dados pessoais e de elementos de dados pessoais específicos, bem como dos sistemas, aplicativos e processos que coletam, criam, usam, disseminam, mantêm e/ou divulgam esses dados;

3.3.9. Criar um Mapa do Fluxo de Dados;

3.3.10. Utilizar o mapa de dados para identificar os riscos nas atividades de processamento de dados e determinar se é necessária uma DPIA (Data Protection Impact Assessment);

3.3.11. Criar registros de atividades de tratamento de dados pessoais, extraídos da auditoria do fluxo de dados e da análise de lacunas.

3.4. **Plano de Ação**

3.4.1. A Elaboração do Plano de Ação será a quarta etapa do projeto;

3.4.2. Esta etapa representará 20% do valor total do contrato;

3.4.3. Estabelecer padrões para criação de uma estrutura na SAEC para a definição das prioridades referentes às inconformidades apresentadas pela Autarquia;

3.4.4. Definir os processos e as atividades necessárias para identificar, definir, combinar, unificar e coordenar as várias tarefas e atividades do projeto;

3.4.5. Determinar os processos necessários para assegurar que o projeto atinja o objetivo definido, dentro do prazo acordado em contrato;

3.4.6. Determinar os processos exigidos para identificar os colaboradores/funcionários, setores, departamentos, empresas prestadoras de serviço e organizações externas que podem impactar ou serem impactados pelo projeto;

3.4.7. Analisar as expectativas das partes interessadas e seu impacto no projeto;

3.4.8. Desenvolver estratégias de gerenciamento apropriadas e eficazes para guiar a Tomada de decisão e Execução do projeto;

3.4.9. Definir e preparar todos os componentes do plano de ação visando consolidar o Plano de Gerenciamento Integrado do projeto;

3.5. **Implementação de Políticas e Processos Operacionais**

3.5.1. A Implementação das políticas e Processos Operacionais será a quinta etapa do projeto;

3.5.2. Esta etapa representará 30% do valor total do contrato;

3.5.3. Deverá ser realizado o alinhamento das políticas, processos e procedimentos existentes com os requisitos da LGPD, além disto também deverão ser desenvolvidos novos processos e procedimentos para garantir o cumprimento de suas obrigações legais. Essa implementação deverá conter pelo menos:

3.5.4. Verificar se as políticas de proteção de dados e avisos de privacidade existentes estão em conformidade com a LGPD;

3.5.5. Onde o consentimento for utilizado como base legal para justificar o processamento dos dados pessoais, verificar se ele atende aos requisitos da LGPD;

3.5.6. Revisar os contratos das empresas prestadoras de e fornecedores e indicar as alterações necessárias para o cumprimento da LGPD;

3.5.7. Planejar como fornecer respostas apropriadas às solicitações realizadas pelos titulares dos dados;

3.5.8. Analisar o modo de transferência externa (para fora dos da Autarquia) está em conformidade com a LGPD;

3.5.9. Criar políticas, normas, processos, procedimentos e controles voltados para:

3.5.9.1. A implementação dos princípios do Privacy by Design no ambiente de negócios;

3.5.9.2. O registro das operações de tratamento de dados pessoais que a SAEC realiza, especialmente quando baseado no legítimo interesse;

3.5.9.3. A transparência das atividades de tratamento de dados;

3.5.9.4. O compartilhamento de dados com terceiros;

3.5.9.5. A transferência de dados pessoais para país estrangeiro;

3.5.9.6. A gestão dos direitos e solicitações dos titulares dos dados;

3.5.9.7. A avaliação da gravidade das violações de dados pessoais;

3.5.9.8. A notificação das violações de dados pessoais à ANPD e aos titulares de dados;

3.5.9.9. Uso de Sistemas de Monitoramento (Câmeras);

3.5.9.10. Uso de dispositivos biométricos;

3.5.9.11. Gestão de Arquivo Vivo;

3.5.9.12. Gestão de Arquivo Morto;

3.5.10. Elaboração do relatório de impacto à privacidade e proteção de dados pessoais

3.5.11. Desenvolver e implementar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

3.5.11.1. Avaliar a necessidade de utilização de criptografia e / ou pseudonimização, quando apropriado;

3.5.11.2. Verificar se existem políticas e procedimentos para detectar, relatar e investigar violações de dados pessoais;

3.5.11.3. Elaborar e implementar políticas, normas, manuais e guias voltados a segurança da informação e cibernética; e

3.5.11.4. Implantar medidas, salvaguardas e mecanismos de mitigação dos riscos e tratamento de dados tais como:

3.5.11.4.1.Gerenciamento de riscos;

3.5.11.4.2.Política de segurança cibernética e da informação;

3.5.11.4.3.Inventário e controle de ativos;

3.5.11.4.4.Gerenciamento Contínuo de Vulnerabilidades;

3.5.11.4.5.Uso controlado de privilégios;

3.5.11.4.6.Gestão de configurações seguras de hardware e software;

3.5.11.4.7.Trilhas de Auditoria;

3.5.11.4.8.Gestão de configurações seguras para dispositivos de rede;

3.5.11.4.9.Defesa de Fronteira (Boundary Defense);

3.5.11.4.10.Proteção de dados;

3.5.11.4.11.Acesso controlado com base na necessidade;

3.5.11.4.12.Controle de acesso sem fio;

3.5.11.4.13.Monitoramento e controle de contas;

3.5.11.4.14.Segurança de software aplicativo;

3.5.11.4.15.Resposta e gerenciamento de incidentes de segurança;

3.5.11.4.16.Plano de recuperação de desastres e continuidade do negócio;

3.5.11.4.17.Programa de Gestão de Mudanças;

3.5.11.4.18.Segurança de serviços de computação em nuvem;

3.5.11.4.19.Proteções criptográficas;

3.5.11.4.20.Tecnologia embarcada;

3.5.11.4.21.Segurança de endpoint;

3.5.11.4.22.Segurança de Pessoal;

3.5.11.4.23.Identificação e autenticação;

3.5.11.4.24.Monitoramento;

3.5.11.4.25.Engenharia e arquitetura seguras;

3.5.11.4.26.Gerenciamento de terceiros;

3.5.11.4.27.Vulnerabilidade e gerenciamento de patches;

3.5.11.4.28.Segurança de dispositivos e dados biométricos;

3.5.11.4.29.Segurança de dispositivos e dados de videomonitoramento;

3.5.11.4.30.Segurança de dispositivos multifuncionais (impressoras);

3.5.11.4.31.Métricas de segurança.

3.6. **Treinamento e Conscientização**

3.6.1.O Treinamento e Conscientização das Políticas e Processos Operacionais implementados na etapa 5 (item3.5), será a sexta etapa do projeto;

3.6.2.Esta etapa representará 10% do valor total do contrato;

3.6.3.Conscientizar e Educar os funcionários de todos os departamentos da Autarquia, todos os envolvidos no processamento de dados deverão ser treinados adequadamente para seguir os processos e procedimentos apropriados e aprovados para a garantia da privacidade e da proteção dos dados pessoais tratados.Com relação a este aspecto deverá:

3.6.3.1. Para todas as funções da organização (priorizando aquelas de missão crítica para a SAEC e sua segurança), identificar os conhecimentos, habilidades gerais e habilidades específicas necessários para apoiar a

proteção dos dados coletados, armazenados e compartilhados pela autarquia;

3.6.3.2. Fornecer treinamento geral que cobrirá áreas como, por exemplo, princípios de proteção de dados, direitos de titulares de dados e segurança de dados pessoais;

3.6.3.3. Fornecer treinamento geral aos funcionários que deverá incluir também:

3.6.3.3.1. Explicação detalhada da Lei;

3.6.3.3.2. Descrição dos princípios básicos da LGPD e como eles se aplicam às atividades da organização;

3.6.3.3.3. Informações sobre os principais pontos da política de proteção de dados da organização e onde podem ser encontrados; e

3.6.3.3.4. Informações sobre onde obter respostas às suas dúvidas sobre a lei e sobre privacidade e proteção de dados.

3.6.3.4. Fornecer treinamento adicional para os funcionários que têm acesso ou responsabilidade pelos dados pessoais coletados, armazenados e compartilhados, tais como:

3.6.3.4.1. Os membros da equipe de TI;

3.6.3.4.2. Funcionários responsáveis pela elaboração, emissão e atualização de avisos de privacidade;

3.6.3.4.3. Funcionários com responsabilidade por lidar com violações de segurança reais ou suspeitas;

3.6.3.4.4. Funcionários da equipe de RH;

3.6.3.4.5. Funcionários da equipe de Marketing, Relacionamento com o Cliente e SAC; e

3.6.3.4.6. Funcionários que são responsáveis pela obtenção ou elaboração de contratos comerciais.

3.6.4. Os treinamentos deverão ser realizados na forma presencial na Sede da Autarquia ou local a ser definido pela CONTRATANTE durante o horário de funcionamento, 07h30 às 11h30 e das 13h00 às 17h00, de segunda à sexta-feira.

3.6.5. A CONTRATADA deverá disponibilizar o Material Didático Impresso e Digital para todos os Treinados, sem custo adicional.

3.6.6. Todos os custos referentes ao Treinamento serão de responsabilidade da CONTRATADA.

3.6.7.Tipos de Treinamentos, quantidades e cargas horárias:

3.6.7.1. Treinamento tipo: Controlador

3.6.7.1.1.Quantidade de turmas:01;

3.6.7.1.2.Carga Horária: 08 horas;

3.6.7.1.3.Quantidade de Pessoas: até 20 pessoas;

3.6.7.1.4.Público Alvo: Gestores.

3.6.7.2. Treinamento tipo: Encarregado

3.6.7.2.1.Quantidade de turmas:01;

3.6.7.2.2.Carga horária: 08 horas;

3.6.7.2.3.Quantidade de Pessoas: até 10 pessoas;

3.6.7.2.4.Publico Alvo: Jurídico e Tecnologia.

3.6.7.3. Treinamento tipo: Operador

3.6.7.3.1.Quantidade de turmas:04;

3.6.7.3.2.Carga horária: 04 horas;

3.6.7.3.3.Quantidade de Pessoas: até 20 pessoas por turma;

3.6.7.3.4.Público Alvo: Equipe administrativa.

4. EXECUÇÃO DOS SERVIÇOS, ATENDIMENTOS E HORÁRIOS DE TRABALHO

4.1. OS Serviços e Atendimentos deverão ser executados presencialmente, ou seja, serão realizados "*In loco*" nas diversas instalações da SAEC:

4.1.1.UAD1 – Unidade Administrativa SAEC (Sede): Rua Paulo,1108, Pq. Higienópolis;

4.1.2.ETE – Estação de Tratamento de Esgoto: Rodovia vicinal Vicente Sanches, Km 2;

4.1.3.UC1 – Unidade de Captação São Vicente: Rua Morro Agudo, 150, Parque Iracema;

4.1.4.UC2 – Unidade de Captação Birigui: R. Birigui, 11 - Parque Glória.

4.2. O horário para execução dos serviços será de segunda à sexta-feira, das 07h30 às 11h30

horas e das 13h00 às 17h00, horário em que a equipe de FISCALIZAÇÃO está presente na SAEC;

4.3. A CONTRATADA deverá disponibilizar um número de telefone, bem como o nome do responsável em atender as solicitações EMERGENCIAIS da SAEC durante os finais de semana, feriados e após o horário comercial.

4.4. A CONTRATADA deverá disponibilizar formalmente os entregáveis de cada etapa para aprovação pela CONTRATANTE, se a contratante identificar necessidades de revisões e adequações nos documentos entregues, a CONTRATANTE irá formalizar as necessidades e a CONTRATADA terá até 05 dias úteis para as adequações. Somente após aprovação pela CONTRATANTE o item será considerado concluído e liberado para faturamento e pagamento.

4.5. PRAZO DE ATENDIMENTO NORMAL:

4.5.1. A CONTRATADA deverá atender às chamadas de prestação de serviço no prazo máximo de 05 (cinco) dias úteis, salvo quando devidamente justificado ou pré-agendado e aceito pelo Gestor do Contrato.

4.6. DO PRAZO DE ATENDIMENTO EMERGENCIAL

4.6.1. O atendimento emergencial destina-se às situações em que durante o Processo de Adequação à LGPD surgir a necessidade de um atendimento não previsto no cronograma de trabalho.

4.6.2. Quando a SAEC solicitar o atendimento emergencial, a CONTRATADA deverá iniciar o atendimento, impreterivelmente, em até 04 (quatro) horas após a solicitação;

4.6.3. O atendimento emergencial poderá ser solicitado pela SAEC a qualquer momento, inclusive fora do horário comercial, feriados, sábados e domingos;

4.6.4. O atendimento emergencial poderá ser realizado num primeiro momento Online, se a solução deste se mostrar complexa, a SAEC poderá solicitará a presença da prestadora de serviço no local para solução.

5. TRANSPORTE E DESLOCAMENTO

5.1. Todas as despesas com transporte, deslocamento são de responsabilidades da EMPRESA CONTRATADA.

6. CAPACIDADE TÉCNICA

6.1. Prova de aptidão para o desempenho de atividade pertinente e compatível com o objeto desta licitação, por meio da apresentação de Atestado(s) ou Certidão(ões), expedido(s) por pessoa jurídica de direito público ou privado necessariamente em nome do licitante, que indique(m) a prestação de serviço de consultoria para adequação à Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

6.2. A licitante vencedora deverá alocar uma equipe de trabalho com as seguintes qualificações e conhecimentos técnicos:

6.2.1. Gestor de projetos com formação comprovada em Gestão de Projetos;

6.2.2. Especialista em TI com formação superior comprovada na área de Tecnologia da Informação;

6.2.3. Especialista em LGPD (Lei Geral de Proteção de Dados) com formação comprovada em Data Protection Officer (DPO), ou especialização em Direito Digital ou especialização em Compliance/Governança Corporativa.

7. PRAZO DE VALIDADE DO CONTRATO:

7.1. O prazo de validade do contrato será de 12 meses.

8. PAGAMENTO:

8.1. Os pagamentos serão feitos em moeda corrente no país, no prazo de 28 DDL (vinte e oito dias do lançamento com respectiva Nota Fiscal.

8.2. Os pagamentos serão realizados em medições de acordo com a fase executada e concluída, conforme o percentual referente a esta.