ANEXO I

TERMO DE REFERÊNCIA

1. DO OBJETO

1.1 – O objeto do presente Termo de Referência é a contratação de empresa especializada em prestação de serviços em diagnóstico e consultoria, para avaliação dos processos executados e a realização do processo de inventário e mapeamento de dados, afim de adequação às exigências da Lei Geral de Proteção de Dados – LGPD nº 13.709/2018, no tocante aos requisitos tecnológicos e jurídicos, bem como aos processos de negócios que fazem tratamento de dados pessoais, tanto dos clientes quanto dos empregados do Sesc Espírito Santo, pelo período de operação de 06 (seis) meses.

2. DA JUSTIFICATIVA

2.1 - A implementação dos requisitos da LGPD impacta diretamente em diversos processos internos da empresa, especialmente aqueles em que dados pessoais transitam como insumos. Dessa forma, a contratação da empresa de consultoria visa promover adequação nos processos de mapeamento e inventário de dados, que precisam de adequação, bem como a análise dos demais processos concluídos, para cumprimento de obrigações impostas pela Lei nº 13.709/2018.

3. DOS SERVIÇOS A SEREM REALIZADOS

3.1 – Os requisitos técnicos estabelecidos neste Anexo I devem ser totalmente atingidos.

3.2 - As ações aqui descritas visam participar do Programa de Implantação à Lei Geral de Proteção de Dados, e devem ser realizadas em todas Unidades do Sesc Espírito Santo.

3.3 - O trabalho deverá ser executado em 02 fases. Assim como atender os seguintes requisitos:

1. O objetivo principal da primeira fase é de avaliação. A licitante vencedora deverá entender em detalhes o funcionamento atual do modelo de negócio do Sesc Espírito Santo, para identificação e avaliação das ações já concretizadas no escopo vigente.

2. Na segunda fase, deverá ser entregue o inventário completo de dados e o mapeamento do seu ciclo de vida, destacando os recursos tecnológicos utilizados, os operadores externos envolvidos e todos as políticas, normas e procedimentos associados ao tratamento dos dados pessoais.

3. Deverá ser identificado o cenário atual do Sesc/ES em relação aos processos, tecnologias, governança, políticas e normas e realizar a avaliação em relação às exigências da Lei nº 13.709/2018.

4. Considerar para a realização do serviço as atividades:

I. Analisar e avaliar as ações de implantação concretizadas pelo DPO e grupo de trabalho vigente;

II. Mapear e documentar as políticas, normas e procedimentos que suportam os controles dos fluxos de dados pessoais.

III. Realizar a busca de dados pessoais estruturados e não estruturados nos setores da empresa.

IV. Descrever os macroprocessos dos principais serviços fornecidos pela empresa a fim de identificar os processos críticos e as interações entre os setores.

V. Mapear e elaborar o inventário dos principais processos de negócio que envolvem dados pessoais e dados sensíveis, nos termos da lei.

VI. Identificar a finalidade de processamento de dados pessoais em cada processo de negócio.

VII. Identificar cada base legal para o tratamento de dados, de acordo com as finalidades dos processos mapeados.

VIII. Identificar os dados pessoais e dados sensíveis tratados em cada processo de negócio.

IX. Documentar os fluxos dos dados pessoais.

X. Mapear a infraestrutura tecnológica de apoio aos processos e o ciclo de vida da informação.

XI. Apresentar documento elaborado com o inventário, mapeamento e fluxo de dados dos processos mapeados com as suas respectivas finalidades, bases legais para tratamento e operadores externos.

XII. Apresentar diagrama relacionando os processos mapeados, sistemas que dão apoio e itens da infraestrutura de Tecnologia da Informação utilizados.

XIII. Apresentar desenho do processo para atendimento dos direitos dos titulares dos dados pessoais.

XIV. Realizar a análise dos sistemas computacionais, gerando um relatório de GAPS e suas soluções propostas.

XV. Realizar análise de vulnerabilidades no ambiente de tecnologia da informação para detecção das falhas a serem corrigidas descrevendo as suas respectivas correções.

XVI. Definir o funcionamento do sistema de gestão de incidentes de segurança da informação atendendo a todos os requisitos da Lei Geral de Proteção de Dados.

XVII. Elaborar o plano de gestão de riscos composto por todas as correções e ajustes necessários para o perfeito funcionamento do Sistema de Gestão de Privacidade e Proteção de Dados.

XVIII. Relatório de impacto a proteção de dados do processo ou sistema selecionado pelo CONTRATANTE.

XIX. Plano de gestão de riscos para implantação do sistema de gestão da privacidade e proteção de dados.

XX. Dashboard contendo todos os projetos e planos de ações necessários para implementação dos controles técnicos e administrativos visando a adequação à Lei Geral de Proteção de Dados com data de início, data de término, responsável e custos, quando existirem.

XXI. Elaborar plano de processos para atender aos titulares dos dados sobre solicitações, reclamações e retificações relacionado ao uso e manipulação de dados pessoais;

XXII. Elaborar plano de resposta de violação de privacidade de dados, cujas funções são: estabelecer o procedimento de notificação de violação para os titulares afetados, reportar no tempo exigido, os incidentes de privacidade de dados para os órgãos reguladores, manter os logs que registram detalhes dos incidentes, apresentar relatório de métricas para gestores estratégicos, obter cobertura de seguro para os custos associados à violação.

XXIII. Estabelecimento de um cronograma de retenção de dados que defina o período em que eles são armazenados - POLÍTICA DE RETENÇÃO DE DADOS.

XXIV. Criação de um modelo de Relatório de Impacto sobre Proteção de Dados Pessoais (RIPD).

XXV. Inclusão de tarefas relacionadas às medidas de compliance.

XXVI. Criação de mecanismos para efetivação das práticas de compliance, resguardando a organização e seus gestores de responsabilidade cível, administrativa e criminal.

XXVII. Conscientização sobre privacy By design (privacidade desde a concepção) e privacy by default (privacidade por padrão).

XXVIII. Desenvolvimento de uma estratégia de prevenção de perda de dados pessoais.

XXIX. Realização de testes de segurança da informação (pentest).

XXX. Aconselhamento em relação à implementação de sistema de computadores para proteção de dados e privacidade: backup, criptografia, data loss prevention (DPL), web application firewall (WAF), next generation firewall (NGFW), instrucion prevention system (IPS)

4. DAS OBRIGAÇÕES DA LICITANTE VENCEDORA

4.1 - Definir em conjunto com o Sesc/ES a metodologia formal de trabalho, a gestão e o cronograma que serão adotados durante o desenvolvimento dos trabalhos, de forma a atender o prazo estipulados no cronograma de execução.

4.2 - Estar ciente que os colaboradores do Sesc/ES irão compor a equipe de trabalho com o objetivo de acompanhar as atividades desenvolvidas e absorver a transferência dos conhecimentos gerados pela LICITANTE VENCEDORA.

4.3 - Estar ciente que podem ocorrer reuniões que dependam da interação física com os ambientes e colaboradores, sem ônus para o Sesc/ES.

4.4 - Por motivo justificado pelo CONTRATADO, ou devido a pandemia da COVID-19, não for possível reunião presencial, há possibilidade de reuniões remotas.

4.5 - Estar ciente que as etapas de trabalho serão consideradas concluídas após a entrega de todos os documentos solicitados e gerados durante o desenvolvimento da atividade, com a devida formalização do aceite do Sesc/ES, de acordo com o cronograma estabelecido.

5. DOS PRAZOS PARA A EXECUÇÃO DOS SERVIÇOS

Período de operação de 06 (seis) meses.

6. DA QUALIFICAÇÃO TÉCNICA

A empresa licitante deverá comprovar que possui equipe técnica qualificada para executar os serviços.

Vitória/ES, 05 de abril de 2022.