

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA

OBJETO: Contratação de empresa especializada para prestação de serviços relacionados à SEGURANÇA DA INFORMAÇÃO e à PROTEÇÃO DE DADOS PESSOAIS, pelo prazo de 6 (seis) meses.

JUSTIFICATIVA:

Os ataques cibernéticos vêm preocupando gestores públicos e privados. O número de ataques cresce a cada dia, com aumento exponencial durante e após a pandemia, impactando serviços em todas as áreas, inclusive na administração pública.

A segurança da informação é tema indispensável em qualquer organização, que deve proteger seus ativos, e dentre eles, figuram os dados da organização (essenciais para a manutenção de sua existência) e também os dados pessoais dos quais é responsável, sejam dados de seus colaboradores, clientes, usuários, cidadãos.

A Lei Geral de Proteção de Dados Pessoais (LGPD) apresenta exigências que devem ser cumpridas por órgãos públicos e privados.

O SEPREV, buscando melhorar a segurança da informação, reduzir os riscos, aumentar a maturidade do processo de gestão da segurança da informação e garantir a conformidade com a LGPD, busca com esta contratação obter um diagnóstico atual da segurança da informação e com base nisso elaborar um plano de ação para implantação de novos processos de segurança da informação ou de melhoria nos processos já existentes.

Outro resultado esperado por esta contratação é a capacitação e a conscientização dos colaboradores do SEPREV, permitindo a manutenção de ações para garantia da conformidade com as exigências da LGPD.

DETALHAMENTO DO OBJETO:

1. VISÃO MACRO DAS ETAPAS DO PROJETO

- a) Reunião para apresentação do projeto de execução e da equipe;
- b) Elaboração de diagnóstico;
- c) Elaboração de plano de ação;
- d) Realização de treinamento sobre a LGPD; e
- e) Apresentação dos resultados (relatório final de serviços prestados)

2. ESPECIFICAÇÃO DAS ATIVIDADES A SEREM REALIZADAS EM CADA ETAPA DO PROJETO:

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

2.1. Fase 1: Reunião para apresentação da equipe e do projeto

A contratada deverá realizar a apresentação da equipe e do cronograma do projeto, em reunião remota ou presencial, mediante alinhamento de data e horário com o gestor do contrato. O cronograma deverá contemplar, no mínimo, as etapas previstas neste Termo de Referência, respeitando o prazo máximo de 06 (seis) meses de execução.

Produtos: reunião realizada e cronograma de trabalho entregue

2.2. Fase 2: Elaboração de diagnóstico

Nesta fase, a equipe técnica da contratada deverá elaborar o diagnóstico da situação atual do SEPREV com relação a cada um dos procedimentos e boas práticas previstas nas normas ISO/IEC 27.001/27.002 (e adendos/relacionadas), ISO/IEC 27.701 (e adendos/relacionadas), bem como em cada um dos controles previstos no CIS – *Critical Security Controls* versão 8 – pelo menos até o Grupo de Implementação de Controles CIS 2 (IG2).

A contratada avaliará ainda a topologia de rede e principais ativos tecnológicos, analisando as vulnerabilidades do ambiente, utilizando técnicas como o Portscanning (Mapeamento de rede) e Varredura de vulnerabilidade.

O SEPREV fornecerá os documentos e informações necessárias para que a Contratada realize as atividades, inclusive mediante entrevistas realizadas pelos técnicos da Contratada.

É nesta fase que a Contratada avalia, por exemplo:

- A aplicação de ações específicas de Segurança da Informação, essencial para a implantação posterior da camada de “privacidade”, em busca da conformidade com a LGPD;
- A capacidade do SEPREV de identificar, proteger e defender os dados e informações críticas contra as formas mais comuns de ataques cibernéticos, de forma a alcançar uma redução mensurável no risco e aumento da maturidade do processo de gestão da segurança da informação.

A contratada se obriga a avaliar o ambiente de TI, procedimentos, processos, documentos, políticas e outros aspectos relevantes para elaboração do diagnóstico e da análise de vulnerabilidades, a partir do entendimento da topologia de rede e principais ativos tecnológicos, entrevistas e coleta de informações.

Os técnicos da contratada deverão efetuar análise crítica que permita compreender o grau de aderência em relação às normas e práticas de segurança referenciadas (ISO, CIS, etc), bem como à LGPD.

Deverá ser emitido relatório detalhado com a situação atual do SEPREV, registrando os controles existentes, ausentes ou insuficientes e não aplicáveis

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

ao ambiente do SEPREV, as vulnerabilidades e as recomendações de boas práticas para mitigação e eliminação de riscos e vulnerabilidades, e as ações necessárias para conformidade legal. Este relatório servirá de insumo para a elaboração do plano de ação.

Produtos:

- Reuniões e entrevistas realizadas
- Emissão de relatório de *Gap Analysis* e de Análise de Risco.
- Relatório com o resultado da Análise de Vulnerabilidades

2.3. Fase 3: Elaboração de plano de ação

Nesta fase, as recomendações identificadas, analisadas e avaliadas pela contratada, registradas no relatório de diagnóstico, serão objeto de discussão pelas equipes da Contratada e do SEPREV, para que em conjunto, sejam priorizadas e inseridas em um plano de ação.

Produtos:

- Reuniões realizadas
- Plano de ação priorizado

2.4. Fase 4: Realização de treinamento sobre a LGPD

A contratada deverá realizar treinamento sobre a LGPD aos colaboradores e dirigentes do SEPREV, na sede da Autarquia, devendo ser abordado no mínimo o conteúdo da Lei Federal nº 13.709/2018, com utilização de exemplos relacionados ao dia a dia para facilitar o entendimento e compreensão sobre o tema, bem como demonstrando a relação com a ISO 27.701, com carga horária mínima de 6 (seis) horas.

A empresa contratada deverá indicar qual é o momento mais adequado para realização do treinamento, entre o início e o fim previsto da prestação dos serviços.

Produtos:

- Treinamento realizado

2.5. Fase 5: Apresentação dos resultados

A contratada deverá apresentar os resultados dos trabalhos através de um relatório final dos serviços prestados, de forma remota ou presencial.

Produto:

- Apresentação final dos resultados

3. REQUISITOS PARA CONTRATAÇÃO E PARA A PRESTAÇÃO DOS SERVIÇOS

A empresa contratada deverá possuir experiência anterior, comprovada através de atestado de desempenho anterior emitido por pessoa jurídica, que demonstre experiência prática na execução de serviço de características semelhantes às descritas neste Termo de Referência.

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

A contratada deverá ainda apresentar a qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos.

Os serviços poderão ser realizados de forma remota, exceto o treinamento previsto na Fase 4, que deverá ser realizado na sede do SEPREV.

4. PRAZO, REMUNERAÇÃO E PAGAMENTOS

O contrato terá duração de até 6 (seis) meses.

Os pagamentos respeitarão o seguinte cronograma financeiro:

Fase	Percentual de pagamento
1 - Reunião para apresentação da equipe e do projeto	0%
2 – Elaboração do diagnóstico	40%
3 – Elaboração do plano de ação	30%
4 – Realização de treinamento sobre a LGPD	20%
5 – Apresentação dos resultados	10%
TOTAL	100%

Os pagamentos serão realizados pelo SEPREV mediante apresentação de documento fiscal ao gestor do contrato, no prazo de 10 (dez) dias. O gestor do contrato é o responsável pelo ateste dos serviços prestados e liberação do pagamento. Eventuais ajustes e não conformidades deverão ser dirimidas pela Contratada junto ao gestor.

5. DAS RESPONSABILIDADES

5.1. RESPONSABILIDADES DO SEPREV:

- Fornecer os dados necessários para a execução dos serviços.
- Designar equipe composta por profissionais que detenham conhecimento do negócio e da tecnologia, com o propósito de acompanhar as atividades e subsidiar as ações da contratada;
- Facilitar o acesso a equipamentos, instalações, documentos e informações solicitadas para a execução do projeto;
- Promover a sinergia entre os funcionários envolvidos direta e indiretamente no projeto, agendando as reuniões e entrevistas necessárias;
- Efetuar os pagamentos devidos

5.2. RESPONSABILIDADES DA CONTRATADA:

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

- Manter total sigilo dos dados informados pelo SEPREV para execução dos serviços
- Garantir que a equipe da contratada que será alocada no projeto assine TERMO DE CONFIDENCIALIDADE E SEGURANÇA com relação aos dados que terão acesso durante a execução dos trabalhos, com dados mínimos relacionados a:
 - Não utilizar QUAISQUER informações (Técnicas Administrativas ou Gerenciais), confidenciais ou não, a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;
 - não efetuar nenhuma gravação ou cópia da documentação a que tiver acesso;
 - não apropriar-se de QUALQUER material técnico, gerencial ou administrativo que venha a ser disponível;
- Responsabilizar-se pela conduta e comportamento da equipe alocada no projeto, especialmente com relação à confidencialidade descrita no parágrafo anterior
- Garantir que a equipe da contratada, ao acessar os recursos do SEPREV, o façam a partir de dispositivos seguros e homologados pela Contratada
- Cuidar para que as informações confidenciais fiquem restritas ao conhecimento tão somente das pessoas que estejam diretamente envolvidos nas discussões, análises, reuniões e negócios
- Cumprir todas as etapas do trabalho, utilizando-se de técnicas e padrões aderentes aos serviços contratados
- Apresentar os relatórios e documentos exigidos

Thiago Fonseca Gonçalves
Diretor do Departamento de TI