TERMO DE REFERÊNCIA

Contratação de Pessoa Jurídica

Nº 1308/2021

1. Objeto

Contratação de pessoa jurídica para serviços de Consultoria de Implementação da LGPD e de Segurança da Informação.

2. Contextualização

A Conexsus – Instituto Conexões Sustentáveis - é uma organização da sociedade civil de interesse público (OSCIP) que tem como missão ativar o ecossistema de negócios comunitários de impacto socioambiental (NCIS), ampliando sua contribuição para a geração de renda no campo e conservação de florestas e biomas naturais. Estes negócios são cooperativas e associações produtivas que atuam nas cadeias da alimentação saudável e sustentável, agroflorestal, da sociobiodiversidade e do extrativismo, da pesca artesanal sustentável e do manejo florestal comunitário. Entendemos que estas organizações geram benefícios ambientais, contribuindo para a conservação de florestas e biomas, a resiliência dos territórios e a mitigação e adaptação às mudanças do clima. Em termos sociais e econômicos, as organizações geram renda em áreas rurais e de floresta, muitas vezes como única alternativa ao uso predatório dos recursos naturais. Além disso, a organização comunitária fortalece as comunidades e permite a manutenção de modos de vida diferenciados, tais como de populações extrativistas e quilombolas, povos indígenas e agricultores familiares.

A Conexsus desenvolve suas iniciativas com foco em três pilares:

2.2.1. Melhoria dos modelos de negócios comunitários;

2.2.2. Acesso aos mercados através de novas parceiras mais igualitárias;

2.2.3. Desenvolvimento de diversos instrumentos financeiros adequados à realidade destas organizações em suas distintas fases de amadurecimento.

3. Descrição dos Serviços

A Empresa será responsável pela implementação de projetos de adequação às normas de Proteção de Dados Pessoais e Segurança da Informação na Conexsus, à luz da LGPD e demais normas internacionais aplicáveis às operações de tratamentos de dados realizadas pela organização.

As atividades a serem realizadas na prestação dos serviços são:

- Mapeamento de dados, mapeamento de fluxo de dados;
- Avaliação de conformidade, diagnóstico, elaboração e/ou revisão de procedimentos e relatórios;
- Acompanhamento das ações de adequação dos clientes;
- Elaboração e/ou revisão de políticas e procedimentos;
- Identificação de gaps e definição de recomendações, estruturadas em planos de ação;

- Implementação de ferramentas de segurança segundo melhores práticas;
- Definição de controles de segurança da informação e políticas, processos e procedimentos;
- Análises de ROPA´s e DPIA´s;
- Condução de workshops de privacidade de dados;
- Gerir os planos de ação para mitigação dos riscos do Programa de Privacidade;
- Analisar os riscos de segurança da informação e proteção de dados pessoais;
- Analisar e responder os pedidos dos titulares, controladores e partes interessadas;
- Manter as políticas, normas e cláusulas de Proteção de Dados e contratos;
- Avaliação de Impacto a Privacidade e Privacy by Desing;
- Implementação de Projeto e Iniciativas em Segurança de Informação, Auditoria, Governança;
- Ciclo de vida dos dados pessoais e soluções de proteção, GRC;

4. Produtos

Produto 1

Relatório Preliminar: Relatório contendo informações e análises do contexto da organização, essenciais para a execução do Data Mapping, dos sistemas de tecnologida da informação adotados e as recomendações iniciais;

Produto 2

Data Mapping: Inventário de dados com, pelo menos, o RoPA (Record of Processing Activities); fluxo do tratamento de dados; registros do ciclo da vida dos dados; categorização dos dados; especificação da base legal para o tratamento; pessoas relacionadas; formatos das bases de dados; motivação para o tratamento; delimitação temporal; formato de armazenamento; métodos de transferência; técnicas de anonimização; formato dos dados; protocolos de tratamento e segurança da informação.;

Produto 3

Relatório de Impacto à Proteção de Dados (RIPD ou DPIA): Deverá conter, no mínimo, a descrição dos tipos de dados coletados; a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas ;salvaguardas e mecanismos de mitigação de risco adotados; as não-conformidades encontradas; avaliação dos riscos encontrados e plano de ação.;

Produto 4

Relatório de implementação e ajustes nos processos e políticas internas: Deverá conter, pelo menos, o registro das ações executadas com base no plano de ação do RIPD, descrição do programa de govenança de dados, a gestão de consentimentos, mitigação dos riscos com base nas fases anteriores, sistemas e ferramentas de segurança da informação adotadas ou ajustadas para a adequada proteção dos dados pessoais.;

Produto 5

Capacitação: Conscientização dos interessados do programa de governança em privacidade e segurança da informação da Conexsus, instrução sobre as boas práticas e mecanimos de controle e gestão para cada setor, com materiais didáticos para posterior consulta;

Produto 6

Relatório Final: Deverá conter, pelo menos, informações sobre testes de confiança e validação, revisão do Plano de Ação do RIPD com avaliação e mitigação de riscos/problemas; recomendações para manutenção e melhoria do programa de governança e sistemas de segurança da informação da Conexsus;

5. Cronograma:

O trabalho terá duração de 06 meses, iniciando em outubro de 2021 e encerrando em março de 2022.

A forma de pagamento será realizada conforme tabela a seguir:

Entrega	%
Produto 1	15%
Produto 2	20%
Produto 3	15%
Produto 4	20%
Produto 5	15%
Produto 6	15%

6. Entrega dos Produtos:

Os produtos deverão ser entregues em formato digital, por e-mail, para o seguinte endereço eletrônico: marcos.souza@conexsus.org

7. Condições de contratação:

- Contrato de prestação de serviço através de pessoa jurídica;
- As atividades e execução do escopo do presente TDR estão previstas o período de Outubro de 2021 a Março de 2022;
- Classificação Nacional de Atividades Econômicas - CNAE compatível com o escopo do serviço;
- Estar regular com as obrigações trabalhistas, fiscais, previdenciárias e outras compatíveis com seu ramo de negócio;
- Ter conta corrente jurídica para a realização dos pagamentos (até a data da contratação);

8. Qualificações obrigatórias:

- Pessoa Jurídica com qualificação técnica comprovada, por meio de apresentação de portfolio de trabalho e/ou currículo profissional, atestados de capacidade técnica, contratos anteriormente executados.
- Disponibilizar equipe qualificada para executar o escopo da proposta.
- Experiencia em condução e implementação de projetos de segurança da informação.
- Consultores com certificações internacionais em Privacidade da Informação, Proteção de Dados

Pessoais e Governança em Privacidade de Dados, além das certificações DPO, ITIL, COBIT e ISO27000.

- Equipe multidisciplinar com conhecimentos em Direito Digital, Segurança da Informação, Forense Computacional, Ethical Hacking, regulamentações de privacidade e tecnologia da informação, privacy by design and default e infraestrutura tecnológica.
- Experiência em projetos de governança de segurança incluindo frameworks tais como ISO 27000 e NIST, entre outros.
- Experiência em projetos de adequação à LGPD/Privacidade de Dados/Segurança da Informação - nas fases de avaliação, implementação e/ou operação do escritório de privacidade, implementação de ferramentas privacidade.
- Visão abrangente de Tecnologia da Informação (Implantação e Integração de Sistemas).
- Domínio - Proteção de Dados, Gestão de Riscos, Segurança da Informação.
- Frameworks de TI, Privacidade, Segurança ISO 27..001 / 27.701, NIST.
- Certificação Profissional em domínios de Segurança, Privacidade e Proteção de Dados - ISO 27000, IAPP/CIPM, EXIN DPO, ISACA.
- Equipe com conhecimento avançado em inglês (nível proficiência técnica profissional).

9. Apresentação da proposta:

A proposta deverá ser enviada da seguinte forma:

- Utilizar papel timbrado da empresa ou instituição;
- Informar os dados cadastrais (Razão Social, CNPJ, IE, endereço, telefone);
- Informar cronograma para a realização de todas as atividades descritas;
- Informar a composição da equipe executora;
- Informar a composição do preço global da proposta (incluindo impostos), conforme tabela do item 5.

10. Orientações e prazos para envio da proposta:

As propostas serão enviadas até 22/10/2021 para o endereço: gestaoconexsus@conexsus.org

11. Critérios e Seleção:

As propostas serão avaliadas com base na qualificação técnica da proponente em relação ao serviços descritos e proposta financeira.