Goiânia, 26 de novembro de 2021.

TERMO DE REFERÊNCIA
CONTRATAÇÃO DE SERVIÇOS
TR N.º 030/2021

De: Tecnologia da Informação – CEAP-SOL.
Para: Departamento de Contratos – CEAP-SOL

1. DO OBJETO

Contratação de empresa especializada para adequar a unidade à Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18) correlata a padrões mercadológicos de padrões e boas práticas, tais como ISO 27001 (Segurança da Informação) e ISO 27701 (Proteção de Dados), bem como apoiar o processo com avaliação de vulnerabilidades de segurança que possam ocasionar em vazamento de dados, emitindo relatórios técnicos especializados com as recomendações de melhoria e evolução que se façam necessárias.

2. JUSTIFICATIVAS PARA CONTRATAÇÃO DO SERVIÇO

O CEAP-SOL - Centro Estadual de Atenção Prolongada e Casa de Apoio Condomínio Solidariedade tem como princípios o Sigilo as informações de seus clientes e a manutenção, disponibilidade, qualidade e garantia dos serviços, estando sempre a vanguarda dos processos reconhecidos de mercado no mundo, com uma qualidade amplamente reconhecida para prestação de serviços em seu segmento de saúde e atendimento ao público. Considerando a necessidade de aprimoramento dos processos, em especial de segurança da informação e proteção de dados.

Podemos dizer que de 2018 a 2020 foram os anos em que vários países colocaram em xeque como anda a segurança da informação de pessoas físicas e jurídicas, em um ano marcado por grandes escândalos de vazamentos de dados de empresas que são familiares a nós, como o Facebook, Google e outras

por exemplo. Diante disto, entendemos o quanto a proteção de dados é um assunto sério, em maio de 2018 a União Europeia transformou a proteção de dados em lei a GDPR (General Data Protection Regulation), e, três meses depois, foi a vez do Brasil, por meio da Lei nº 13.709/2018.

A nossa Lei Geral de Proteção de Dados (LGPD) nacional regulamenta o uso e tratamento dos dados pessoais, tanto pela iniciativa privada quanto do poder público, na tentativa de protegê-los contra vazamentos e uso indevido. Não nos esquecendo de padrões relevantes e implementados e existentes no mercado que complementam o tema, que são sobre segurança da Informação (ISO 27001) e normas de proteção de dados (como a ISO 27701).

Nesse caso, caberá a todas as empresas que lidam com dados pessoais (setor público ou privado, estejam elas em meio digital ou não) algumas responsabilidades a se preocuparem. Ou seja, se hospital realiza um simples cadastro de CPF, por exemplo, temos de nos ajustar à nova lei de dados, considerando inclusive os dados pessoais de nossos funcionários também e mapeamento de todos os serviços que existem em nosso ambiente sob nossa gestão completa ou compartilhada.

3. DESCRIÇAO MINUCIOSA DO SERVIÇO

Contratação de empresa especializada para implementação de Controles e documentação de processos da Lei Geral de Proteção de Dados (LGPD), com alinhamento ao padrão internacional (ISO 27701 – Proteção de Dados) e práticas internacionais correlatas (Ex.: ISO 27001 – Segurança da Informação), alinhados aos aspectos e serviços continuados para o ambiente Institucional em questão, com repasse posterior de conhecimento interno para operacionalização de atividades, habilitando a replicação da iniciativa, processos e controles, conforme detalhado no projeto. De forma complementar, temos pretensão de alinhamento aos requisitos previstos aos aspectos de Segurança da Informação (ISO 27001) e a norma ISO 27701 (Proteção de Dados) uma norma mundial correlata ao tema e divulgada a pouco tempo no mercado.

O projeto será dividido em 2 (duas) etapas macro que são:

a) Etapa 1 - Implantação de processos, atividades técnicas especializadas, apoio na implementação de controles, processos educacionais, análises e repasse de conhecimento relativo ao processo de LGPD; e
b) Etapa 2 - Processo continuado de apoio como DPO (Data Protection Officer), monitoramento de ações, apoio a respostas a questionamentos legais, acompanhamento de legislações, iniciativas e responsabilidades em relação ao tema.

A nova lei de proteção de dados, denominada Lei Geral de Proteção de Dados (LGPD), sancionada em agosto de 2018 e entrou em vigor em setembro de 2020 após sanção presidencial. Seu principal objetivo é garantir transparência no uso dos dados das pessoas físicas em quaisquer meios. Esta lei chega para alterar a Lei n° 12.965, de 23 de abril de 2014, popularmente chamada de Marco Civil da Internet que regulava estas transações até então.

A LGPD tem como base a GDPR, regulamentação europeia já aprovada e vigente e que usa os direitos fundamentais de liberdade e de privacidade como norte para estabelecer regras a respeito da coleta e armazenamento, de dados pessoais e seu compartilhamento. A intenção é proporcionar privacidade às pessoas físicas contando com a penalidade de multas para motivar o seu cumprimento por parte das empresas.

Diante desta regulamentação, entendemos que a Instituição terá grandes responsabilidades em relação à proteção dos dados pessoais de seus funcionários, fornecedores e clientes/pacientes. Apesar da data de início de vigência da LGPD parecer distante, as medidas necessárias devem ser tomadas desde já. Por isso, é preciso se mover com rapidez para que a LGPD não impacte negativamente os negócios e garantindo que a empresa esteja em compliance aos aspectos previstos, alinhados aos padrões mundiais e de segurança da informação.

O objetivo da referida contratação é selecionar empresa qualificada com especialização e conhecimento em consultoria, auditoria, avaliações de segurança, testes de vulnerabilidades técnicas e Implantação de Proteção de Dados, para atuar com a implantação, análise e garantia de aderência de controles na implantação de controles para atendimento ao processo de Proteção de dados dos recursos e soluções corporativas existentes, com uso se necessário de técnicas e soluções especializadas, assim como o repasse de conhecimento, com objetivo de atender necessidades técnicas operacionais requeridas pela legislação, alinhadas as práticas institucionais de segurança da informação e do segmento de saúde, assim como com a integração com os recursos internos que possam ser pré-existentes e disponíveis.

A intenção principal é obter um parceiro especializado para apoiar e preparar a estrutura corporativa para a LGPD, do Assessment de Vulnerabilidades de dados por aplicação/recurso, Construção do Roadmap de Ações priorizadas com integração e apoio na sustentação da segurança da informação, análises técnicas de segurança da informação, provimento de educação continuada, indicando ações, recomendações e/ou necessidades para que a Instituição tenha estruturados processos. Tudo isto terá o objetivo de prover:

a) Estruturação, capacitação, apoio à institucionalização e formalização de uma estrutura de DPO (Data Protection Officer) institucional, que como recomendação será operada pelo prestador, prevendo a entrega de estrutura de educação continuada que fique sob domínio e gestão da empresa;
b) Estruturação de processos de monitoramento e tratamento de dados institucionais, avaliações de segurança, vulnerabilidades e testes de invasão;
c) Mapeamento, estruturação e monitoramento dos riscos de tratamento dos dados na empresa, em sistema próprios e/ou em terceiros;
d) Identificar necessidades de gestão e mascaramento de dados, proteção de informações e/ou ajustes para exigência mínima de informações;

e) Estabelecimento de regras e padrões de proteção de dados atrelados à segurança e controles de acessos e soluções críticas em relação a proteção de dados, seu armazenamento de informações, proteção e retenção de dados;

f) Gestão de identidade, autorizações, regras e matrizes de criticidade de clientes e consumidores em relação a proteção de dados no que tangue ao controle, processamento e proteção e os papeis em cada um dos casos;

g) Revisão de todos os contratos de tecnologia e serviços para avaliar critérios, riscos e necessidades em relação a aspectos de proteção de dados e propor ações, aditivos ou ajustes documentais e técnicos;

h) Realização de análises/questionários AIPD (Análise de Impacto de Proteção de Dados) e todos os insumos, sistemas, recursos, ambientes e correlação em matrizes e documentações correlatas necessárias para análise, tomada de decisão, ajuste e correta proteção;

i) Avaliação de arquiteturas tecnológicas e práticas de proteção de dados incorporadas em todo novo ambiente e aplicação por padrão (privacy by default) e por Design/concepção (privacy by design), como o acesso controlado e a encriptação nativa de dados pessoais assim que forem coletados, ou anonimização e/ou pseudonimização bem como a guarda segura deles, sua retenção, proteção e descarte (ciclo de vida do dado), recomendando sempre que necessário e apoiando na justificativa técnica de soluções a adquirir;

j) Seguir, apoiar e aplicar o conceito de Privacy by Design para as aplicações institucionais com análises e recomendações pertinentes, com uso de pilares como:

    a. Proativo não reativo; preventiva não corretiva: O objetivo é antecipar os problemas e entregar soluções que impeçam que eles aconteçam. O Privacy by Design não apresentará soluções para violações de privacidade após esses eventos terem ocorrido. Deve haver a prevenção desses incidentes com constante monitoramento desses riscos e entrega de novas funcionalidades

que excluam os riscos identificados. A agilidade com que ocorrem as evoluções tecnológicas não pode impactar negativamente nessa ideia.

b. Privacidade incorporada ao design: em linha gerais, trata-se da ideia de que o usuário terá o controle para alterar as configurações padrão e optar por fornecer ou não seus dados, e ainda assim conseguirá utilizar o produto ou serviço.
c. Funcionalidade completa: seguindo as premissas da privacidade incorporada ao design, o produto ou serviço deve ser plenamente utilizável caso o usuário não altere as configurações de privacidade. Não deve haver alguma funcionalidade adicional ou vantagem ao usuário caso altere a configuração de privacidade. A proteção da privacidade precisa ser protegida.
d. Segurança de ponta a ponta: é a proteção total do ciclo de vida do dado. A proteção da privacidade não se limita à configuração do produto ou serviço. Quando o usuário autorizar a coleta de algum dado, o tratamento desse dado deve ser de forma segura, desde a coleta até sua eliminação.
e. Visibilidade e transparência: as empresas devem permitir que seja verificado que elas cumprem o que prometem sobre os dados dos usuários, seja diretamente ou por auditorias independentes. É necessário que a companhia possa comprovar que passou do discurso para a prática e que protege os dados dos usuários. Isso pode ser realizado de diversas formas e deve estar disponível às pessoas.
f. Respeito pela privacidade do usuário: a privacidade do usuário deve ser a principal preocupação. Portanto, garantir a segurança dos dados do usuário envolve diretrizes de segurança da informação capazes de assegurar a confidencialidade, integridade e disponibilidade dos dados e informações durante todo seu ciclo de vida.

g. Seguir, apoiar e aplicar o conceito de privacidade como configuração padrão (Privacy by Default): provendo uma garantia dentro do desenho da privacidade como uma decorrência do Privacy by Design. Em outras palavras, trata-se da ideia de que o produto ou serviço lançado e recebido pelo usuário com todas as salvaguardas que foram concebidas durante o seu desenvolvimento. Ou seja, todas as medidas para proteger a privacidade que foram idealizadas desde o início do desenvolvimento do projeto, atendendo o princípio do Privacy by Design. A configuração de privacidade mais restritiva possível é estabelecida desde o momento zero. Apenas os dados essenciais para prestar o serviço ou entregar o produto devem ser coletados. Ainda assim, o usuário deverá ser informado de quais informações estão sendo coletadas e para qual propósito. Caberá ao usuário, caso deseje, desativar uma ou todas essas salvaguardas. A Instiuição não deve fornecer, utilizar ou manter produtos ou serviços com essas proteções desativadas, dependendo de uma ação do usuário para serem ativadas.

Importante ressaltar que o projeto será de implantação operacional nos 6 (seis) primeiros meses, tendo uma iniciativa continuada de 12 (doze) meses no total, renovável por iguais períodos para prestação dos serviços, monitoração contínua, revisão, adequação de processos, procedimentos e sistemas em relação ao escopo e objetivos previstos.

4. PRAZO DE EXECUÇÃO DO SERVIÇO

Prazo do serviço de execução do projeto será de implantação operacional nos 6 (seis) primeiros meses, renovável automaticamente por mais 6 (seis) meses, para prestação dos serviços, monitoração contínua, revisão, adequação de processos, procedimentos e sistemas em relação ao escopo e objetivos previstos totalizando 1 (um) ano, Condicionado a vigência do Termo de Transferencia de Gestão 003/2013, firmado entre o SES-GO e o ISG/CEAPSOL.

5. REAJUSTE

O reajuste de preços será anualmente, acordado e firmado mediante termo aditivo, tomando por base a variação do ÍNDICE GERAL DE PREÇOS DO MERCADO – IGPM da Fundação Getúlio Vargas ou, na falta, de acordo com o índice que legalmente vier a lhe substituir, com até 30 dias de antecedência ao termo final do contrato.

6. REGIME DE EMPREITADA

Empreitada por preço global.

7. QUALIFICAÇÕES TÉCNICAS E REQUISITOS EXIGIDOS

A empresa deve ser especializada em segurança da informação possuir consultorias especializadas para implantação de normas e padrões, proteção de dados e compliance, assessment de vulnerabilidades, construção do roadmap de ações priorizadas e sustentação da segurança da informação, sendo que para tal, os seguintes padrões e modelos, se farão necessários para cumprimento:

7.1. Modelo de Serviço

Com a implementação de um sistema de Service Level Agreement (SLA) serão objetivos a serem alcançados na prestação do serviço:

- A Instituição não ter responsabilidade operacional direta sobre o projeto, sendo parte demandada e apoiadora;
- Permitir à Instituição concentrar seus esforços em decisões estratégicas e operacionais do dia a dia;
- Melhorar a eficiência dos serviços, produtos e recursos em relação ao tema;
- Melhorar a decisão da gestão fazendo através da qualidade das informações recebidas, tratadas e controladas; e
- Melhorar a qualidade percebida pelo usuário final e cumprimento com seus direitos.

A implementação deste tipo de serviço é baseada nos seguintes conceitos-chave que serão sempre que possível almejados pela Instituição:

- Indicadores: Vitais na implementação de serviços para atividade de gestão, com mecanismos desenvolvidos para obter tais métricas e ajustados periodicamente no âmbito de fornecer o status do serviço e permitir a tomada de medidas nas áreas de melhoria detectadas, que poderão ter reportes mensais.
- Gestão: Equipe de gestão altamente treinada e experiente na implementação deste tipo de serviço, com práticas de Gestão de Projetos (PMP), práticas de proteção de dados (com a norma de extensão ISO 27701 sobre proteção de dados), operação de Data Protection Officer (com qualificação DPO em nível Praticioner obrigatoriamente para coordenar o projeto e ser indicado como DPO institucional) e outras que possam ser julgadas necessárias ou previamente requeridas nesta contratação. Esta equipe terá como objetivo, alcançar as metas estabelecidas baseadas com o SLA, além da competência e qualificação técnica do time em projetos de consultoria e implantação de padrões e avaliação de sistemas e vulnerabilidades e revisão de contratos técnicos;
- Melhora contínua: Acompanhar, monitorar e ampliar continuamente a implementação de serviços sob contrato de nível de modo Serviço (que poderá ser adaptado em comum acordo a qualquer momento) com uma política de melhoria contínua que permitirá melhorar a prestação de serviço ao longo da execução do contrato, contendo recomendações mensais, anuais, tempestivas e/ou emergentes que possam surgir;
- Metodologia: implementar serviços utilizando metodologia específica para a operação e o apoio tanto para a gestão subjacente às diferentes linhas de serviço para a gestão integrada;
- Ferramentas: Projetadas e desenvolvidas para suportar este tipo de serviço de gestão para ambos os requisitos de gestão, educação e outras, tais como ferramentas de medição de produtividade de

serviços constante, que poderão ser alinhadas e implementadas em comum acordo entre as partes além dos objetivos prévios estabelecidos. A empresa prestadora deverá obrigatoriamente utilizar ferramentas próprias ou as já disponíveis e vigentes no ambiente da Instituição, pensando desde mapeamento de dados, fluxos de operação, análises, estatísticas, educação corporativa presencial ou virtual, controles gerenciais e dashboards estatísticos (de dados, informações e fragilidades sobre o processo);

- Ambientes: Os ambientes e recursos, serviços e contratos a serem considerados são dos ambientes do estado de Goiás, podendo ser ampliadas e aditivadas para outras localidades se alinhado em comum acordo entre as partes.

7.2. Sobre o Serviço

Este serviço compreende o fornecimento de consultores especializados, quer remotamente e no local para suportar e apoiar os controles e implementações requeridas e o repasse de conhecimento formal, emissão, apresentação e discussão de relatórios, documentos e padrões (que serão providos pelo prestador), garantindo a totalidade de controles implementados em relação a obrigatoriedade legal, nacional e interconexão com a legislação internacional, além do seu monitoramento contínuo (com emissão de relatórios de acompanhamento, monitoração e controle). Como vantagens almejadas da ação, podemos relacionar como almejado:

- Definição de padrões, modelos, norteadores;
- Provimento e/ou customização de recursos tecnológicos, operacionais e de gestão sobre o tema;
- Provimento de recursos de educação continuada (Ex.: Plataforma EAD) com materiais de treinamento para formação de times internos e campanhas internas a todos os colaboradores, sem limite de turmas, alunos ou prazos;
- Suporte metodológico e repasse de conhecimento;

- Relatórios e alertas de pontos relevantes que devem ser avaliados, periodicamente, tempestivamente ou sempre que necessário ou requerido (internamente ou se requeridos para organismos de controle e proteção);
- Matrizes de documentações com informações, sistemas, dados, fornecedores e outras informações julgadas necessárias que devam ser mapeadas, tratadas e norteadas para acompanhamento, ação e solução proposta;
- Revisão de contratos e projetos relevantes com impacto a proteção de dados institucionais, com emissão de relatórios de pontos de atenção, com solução e ajustes propostos;
- Auditoria de projetos, processos e sistemas correlatos sempre que demandado ou julgado necessário;
- Consultoria para provimento de padronização documental, de políticas e práticas atreladas a proteção de dados;
- Casos de uso correlatos para garantir o alinhamento e conformidade com controles de proteção de dados da ISO 27701 (Proteção de Dados) em relação as exigências de proteção de dados ou legais que possam surgir; e
- Apoio com responsabilidades de DPO (Departamento de Proteção de Dados) independente e empoderado, para interface com as Agências Regulamentadoras como a Agência Nacional de Proteção de Dados (ANPD), conforme requerido legalmente.

O tempo de implementação preliminar será de 6 (seis) meses, provendo serviço continuado posteriormente, totalizando até 12 (doze) meses de serviço, para entendimento do ambiente, implementação de recursos, provimento de padrões e modelos, configurações e proposições de adequações, sendo iniciada a operação na assinatura do contrato, onde é pertinente que a equipe técnica principal e/ou preposto atue em campo para facilitar reuniões, ações presenciais, intervenções conjuntas, repasse de conhecimento e outras ações que possam se fazer necessárias.

7.3. Principais entregáveis previstos:

Entregáveis	Foco
Relatório de estudo da LGPD e demais leis que regulamentam o negócio com recomendações priorizadas.	Operacional para todas as áreas e departamentos
Estruturação e capacitação para definição de departamento e funções de DPO (*Data Protection Officer*), juntamente com a capacitação de time chave interno.	Operacional para todas as áreas e departamentos aplicáveis.
Mapear a entrada e o tratamento dos dados pessoais das principais aplicações, sistemas e serviços institucionais.	Operacional para todas as áreas e departamentos
Mapear os riscos do tratamento de dados necessários e atuar no seu tratamento contínuo.	Para os itens aplicáveis.
Relatório de revisão de contratos correlatos e suas proposições, com recomendações priorizadas e proposições de ações e iniciativas.	Para os itens aplicáveis.
Elaborar o Relatório de Impacto e Análises de AIPD (Análise de Impacto de Proteção de Dados) por recurso/sistema/departamento, provendo revisões e ampliações semestrais das análises. Prover relatórios com priorização de recomendações e proposições.	Operacional para todas as áreas e departamentos

Entregáveis	Foco
Criar e propor política de proteção de dados customizada por recurso, serviço, sistema impactado e propor as adaptações dos documentos/sistemas internos e externos, de contratações, de contratos vigentes, e soluções existentes (internas com acordos operacionais).	Operacional para todas as áreas e departamentos
Estruturar organização para gerenciar os pedidos dos titulares e dos órgãos de proteção de dados que possam vir a surgir, com estabelecimento de canal de proteção de dados, gerindo as demandas, ações e questões nos prazos regulamentares.	Operacional para todas as áreas e departamentos
Treinamento das equipes que tratam dados pessoais e workshops institucionais para garantir todo e qualquer aspecto ou recomendação legal ou regulamentar em relação ao aspecto de capacitação e repasse de conhecimento.	Operacional para todas as áreas e departamentos
Alinhamento de práticas e padrões operacionais par se manter compliance com a proteção de dados mediante governança e gestão interna, com emissão de relatórios, pareceres, cartilhas, modelos e padrões recomendados em ações e reportes mensais.	Operacional para todas as áreas e departamentos
Exigir o compliance de proteção de dados de seus fornecedores (novos e antigos), mediante revisões contratuais e aditivos se necessário, sendo apoiador chave com proposição de	Operacional para área de compras, jurídico e contratos.

Entregáveis	Foco
cláusulas requeridas para novos contratos firmados.	
Apoio na definição de metodologia e padrões de concepção de novos produtos com o princípio de *privacy by design* e *privacy by default*; Sendo aplicável a análise e adequação para serviços já existentes e implementados (providos internamente ou por terceiros), fazendo as devidas recomendações ao que for necessário de forma tempestiva.	Operacional para área de tecnologia e prestadores do segmento.
Eleger/nomear, capacitar continuamente e desenvolver um DPO com conhecimentos regulatórios sobre proteção de dados no segmento institucionalmente. Que será responsável também para atuar com campanhas internas, comunicados, apoio continuo na estruturação de padrões e discussões.	Operacional para toda a empresa.
Implementação de controles de educação continuada, como com utilização de plataforma EAD própria, sem limite de turmas, alunos ou prazos.	Operacional para toda a empresa.
Realização de testes de invasão para avaliar os níveis de segurança dos dados institucionais e seus sistemas, minimamente dos tipos BlackBox e GrayBox.	Operacional para toda a empresa.
Outros aspectos necessários e/ou pertinentes avaliados e aprovados conjuntamente entre as partes devido ao negócio ou atuação	Operacional para toda a empresa.

Entregáveis	Foco
corporativa que possam não ter sido considerados inicialmente.	
Apoio contínuo como Departamento de Proteção de Dados (DPO) independente e de relacionamento com a ANPD (Agência Nacional de Proteção de Dados).	Operacional para todas as áreas e departamentos aplicáveis.

Importante ressaltar que aspectos definidos em normas, leis ou regulamentos correlatos ao tema podem alterados no decorrer do tempo, ser complementados, desmembrados ou inclusos nos entregáveis previstos, bem como propostos pelo próprio fornecedor ou equipe interna. Sendo estes itens apresentados considerados como entregáveis mínimos previstos.

7.4. Requisitos Internos

O projeto referenciado deve contemplar os sistemas, recursos e fornecedores utilizados corporativamente, lembrando que outros sistemas, aplicações e plataformas que possam ser referenciados, bem como normas, padrões e documentos já existentes também devem ser considerados e entendidos como passíveis de inclusão no escopo a qualquer tempo.

7.5. Requisitos Legais

Todos os requisitos legais e regulamentares aplicáveis ao ramo de negócio e atuação da Instituição, bem como as legislações e práticas vigentes ou que possam ser consideradas no decorrer do trabalho devem ser considerados, previstos e garantidos, a qualquer tempo, prevendo inclusive contemplar atualizações ou mudanças que possam ocorrer no decorrer do tempo.

7.6. Requisitos de Experiência profissional e técnica

a) Atestado de capacidade técnica declarando possuir experiência na aplicação e implementação de controles de consultorias técnicas especializadas, análises, auditorias, gestão de tecnologia e segurança da Informação para garantia de dados (confidencialidade, integridade e disponibilidade dos dados);

b) Atestados de capacidade técnica de execução de análises de impacto de aplicações, recursos ou processos (BIA – Business Impact Analisys e/ou RIA – Risk Impact Analisys) e/ou a execução de análises de questionários AIPD (Análise de Impactos de Proteção de Dados);

c) Atestado de capacidade técnica de avaliação de soluções e sistemas e suas vulnerabilidades de dados e segurança;

d) Atestado de capacidade e comprovação técnica profissional, declarando ter competência profissional (certificados) e também corporativa nos seguintes temas (como perfis mínimos, unificados e/ou desmembrados em quantos profissionais forem necessários):

e) Qualificação em Auditorias de Tecnologia e Segurança, com gestão de segurança da Informação (confidencialidade, integridade e disponibilidade de dados e operações) (Auditor ISO 27001);

f) Gestão de Projetos (PMP ou Prince2) e de Projetos Ágeis (Scrum);

g) Qualificação profissional de time com competência de Hacker Ético (para realizar avaliações da estrutura de sistemas e ambientes sem danos e dentro da legislação aplicável);

h) Gestão de qualidade e documentação técnica (ISO 9001);

i) Análises técnicas especializadas e/ou auditorias de Gestão de Contratos e sua maturidade (ex.: Cobit, ITIL);

j) Gestão de Riscos; e

k) Qualificação corporativa e atestação profissional em Proteção de Dados (LGPD), minimamente em nível Praticioner.

A empresa participante deverá possuir profissionais formalmente qualificados em cada uma das práticas requeridas, e que sejam declarados participantes do projeto e/ou do quadro societário que estará envolvido com o projeto como preposto e/ou responsável, independentemente da quantidade de profissionais envolvidos para compor a qualificação requerida. A composição do time e qualificações do time mínimo será recomendada a ser apresentada como previamente disponível já para assinatura do contrato.

7.7. Requisitos de Homologação do Serviço/Contrato

As propostas técnicas deverão vir com um cronograma físico x financeiro proposto para os 6 (seis) meses de implantação e também para os 12 (doze) meses de operação continuada, onde os pagamentos serão realizados mensalmente após a assinatura do contrato, com parcelas de igual valor, juntamente com todas as evidências de execução e cumprimento dos requisitos esperados, disponíveis mediante um cronograma físico financeiro previsto e declaração de composição do time de trabalho atuante e com as qualificações requeridas. Taxas e Custos de soluções, equipamentos, implantação e operação deverão ser considerados nos valores propostos e serão homologados também conjuntamente com o serviço entregue.

7.8. Requisitos Básicos de Segurança, Ética e Confidencialidade

- Ressaltamos a importância do comprometimento com o uso das informações corporativas disponibilizadas, onde o prestador deve comprometer-se em não divulgar a terceiros não autorizados, quaisquer dados ou informações correlatas ao projeto ou a empresa e manter sigilo e confidencialidade de quaisquer dados, aspectos de integridade, fatos ou informações relevantes durantes e após o projeto;
- Os dados de funcionários, clientes, fornecedores, sistemas, recursos, ambientes e da empresa como um todo não deverão ser divulgados ou utilizados indevidamente.

- Dados e informações críticas que não sejam inerentes as execuções do trabalho não deverão ser solicitadas;
- A Instituição poderá questionar a qualquer momento o uso e finalidade de informações solicitadas;
- A atuação com cordialidade deverá ser mantida na execução do trabalho como prática, e caso seja identificada a ocorrência de ação ou informação interna indevida, a Instituição será imediatamente comunicada e quaisquer penalidades de ética e segurança poderão ser aplicadas;
- A manutenção da ética, sigilo e confidencialidade será mantida durante todo o decorrer do contrato e após no mínimo de 5 (cinco) anos a 20 (vinte) anos de acordo com o dado ou informação de relevância, ou conforme legislação vigente e aplicável.

8. OBRIGAÇÕES DA EMPRESA CONTRATADA

8.1. O projeto devera iniciar em um prazo máximo de 30 dias após a assinatura do contrato;

8.2. Manter durante toda a execução do contrato, em compatibilidade com as obrigações por ela assumidas;

8.3. A CONTRATADA deverá garantir o fornecimento de docume ntação de entrega de projeto, com descrição de todos os entregáveis previstos;

8.4. Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes da execução dos serviços, objeto deste Termo de Referência;

8.5. Responsabilizar-se por todos os ônus referentes aos serviços objeto deste Termo de Referência;

8.6. Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços ou em conexão com eles, ainda que acontecido nas dependências da CONTRATANTE;

8.7. Responsabilizar-se por qualquer prejuízo causado a CONTRATANTE, a seus prepostos ou a terceiros, provocados por ação ou omissão da

CONTRATADA em decorrência de falhas ou imperfeições na execução dos serviços;

8.8. Comunicar ao Gestor do Contrato, designado formalmente pela CONTRATADA, qualquer fato extraordinário ou anormal que ocorra durante a vigência do contrato;

8.9. Exigir dos seus empregados, quando em serviço nas dependências do CEAPSOL, o uso obrigatório de crachás de identificação;

8.10. Todos os equipamentos a serem fornecidos deverão ser novos e passíveis de comprovação, não recondicionados ou remanufaturados e sem qualquer uso anterior;

8.11. Os equipamentos disponibilizados pela CONTRATADA para a prestação dos serviços devem ser identificados pela própria empresa e comunicado formalmente a equipe de Patrimônio da CONTRATADA. Obrigatoriamente com o uso de identificação patrimonial evidente, de modo a diferenciá-los dos demais equipamentos;

8.12. Suporte técnico 24 horas e tempo de atendimento e reparo contratual;

8.13. O serviço de suporte (SAC) deverá ser prestado diretamente pela CONTRATADA não podendo ser terceirizado;

9. OBRIGAÇÕES DA CONTRATANTE

9.1. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA com relação ao objeto deste Contrato;

9.2. Realizar o acompanhamento de todo e qualquer tipo de serviço prestado pela CONTRADADA dentro das dependências da unidade;

9.3. Fiscalizar e orientar quanto às medidas necessárias de biossegurança para garantir a eficiência e eficácia no serviço prestado buscando a excelência na execução das atividades em todo o processo.

10. DA PROPOSTA

A proposta deverá ser apresentada de maneira a:

10.1. Não conter rasuras ou emendas;

10.2. Estar assinada;

10.3. Conter com clareza e sem omissões as especificações do serviço ofertado, mencionando a descrição, quantidade, valores unitários e totais, de forma a obedecer à discriminação do objeto;

10.4. Os valores deverão ser apresentados em Reais;

10.4.1. Ocorrendo divergência entre os valores unitários e totais prevalecerão os unitários;

10.5. O prazo para entrega da proposta será de acordo como esta disposto no extrato do chamamento publicado no site do ISG/CEAPSOL (http://www.isgsaude.org/novo/condominio-solidariedade/transparencia-cs.php

10.6. A proposta devera ser emitida com validade de 30 dias;

10.7. A proposta deverá constar, forma de pagamento, prazo de pagamento, inicio da prestação dos serviços;

10.8. A apresentação da proposta pelo proponente implica a declaração de conhecimento e aceitação de todas as condições do presente termo de referência.

10.9.

11. JULGAMENTO

11.1. O julgamento das propostas será realizado com base no Regulamento de Compras e Serviços;

12. A REALIZAÇÃO DO SERVIÇO

12.1. Os serviços ora cotados serão prestados no Centro Estadual de Atenção Prolongada e Casa de Apoio Condomínio Solidariedade – CEAP-SOL;

12.2. Cumprir os prazos de execução dos serviços;

12.3. Promover condições à fiscalização de todos os serviços contratados, bem como, dos seus procedimentos e técnicas empregados.

13. CONDIÇÕES DE PAGAMENTO

13.1. O prazo para o pagamento será de 60 (sessenta) dias a partir da apresentação da nota fiscal.

13.2. A nota fiscal deverá ser emitida em nome/razão social: Instituto Sócrates Guanaes - ISG -TTG 003/2013 CNPJ/MF nº 03.969.808/0008-46, com endereço

na Av. Veneza, Qd. 62, Lt. 1-10 - Jardim Europa, CEP: 74.325-100 Goiânia-GO, devendo esta a nota apresentada sem rasuras, no período de validade de sua emissão e obrigatoriamente deverá constar acostada a(s) nota(s) fiscal(is):

Certidão de Regularidade junto ao FGTS;

Certidão Negativa de Débitos Trabalhistas - CNDT;

Certidão Negativa de Débitos junto a Secretaria da Fazenda Municipal;

Certidão Negativa de Débitos junto a Secretaria da Fazenda Estadual;

Certidão Negativa de Débitos junto a Secretaria da Fazenda Federal;

Qualquer pagamento devido pela CONTRATANTE somente será efetuado mediante apresentação, pelo CONTRATADO, de cópias legíveis e sem rasuras dos documentos previstos acima.

14. DISPOSIÇÕES FINAIS

14.1. Não serão aceitas propostas que apresentem preço global ou unitário simbólicos, irrisórios ou de valor zerado, incompatíveis com os preços praticados pelo mercado.

Eduardo Campos Soares
SUPERVISOR DE TI
CEAP-SOL

Jessé Chinelles Barreto Tomaz
Gerente Administrativo
ISG - CEAP-SOL