TERMO DE REFERÊNCIA

1. OBJETO

Constitui objeto deste Termo de Referência, contratação de empresa de prestação do serviços de implantação de programa de governança em proteção e privacidade de dados, e integração ao SGI – Sistema de Gestão Integrado da empresa, que seja aderente às referências legais e normativas, focando principalmente nas Leis federais 13.709/2018 e 13.853/19, Lei Geral de Proteção de Dados, nos Decretos Estaduais 844/2020 e 1.184/2021, IN SEA Nº 20/2021, na NBR ISO 9001:2015 e que atenda às condições de organização e regime de funcionamento do Porto de São Francisco do Sul, de acordo com o item 3, que detalha as características do objeto.

2. JUSTIFICATIVA

A CONTRATANTE possui aproximadamente 240 colaboradores e mais de 70 contratos vigentes, envolvendo mais de **600** colaboradores (diretos ou indiretos). Possui aproximadamente **250** dispositivos endpoints, entre notebooks e desktops. Possui volumes de armazenamento de dados em storage local e na nuvem. A CONTRATANTE é uma empresa provedora de infraestrutura de navegação, movimentação e armazenagem de mercadorias destinadas ou provenientes do transporte aquaviário. Seus principais Stakeholders são: Colaboradores; Diretoria executiva; CONSAD; COFINS; Acionista Único; Órgãos intervenientes: ANTAQ, ANVISA, Receita Federal, Marinha, Polícia Federal, dentre outros; Exportadores, importadores e embarcadores; Arrendatários e Operadores Portuários; Agências Marítimas; e Armadores e diversos Prestadores de Serviços ao Porto.

A Lei 13.709/2018, Lei Geral de Proteção de Dados – LGPD, entrou em vigor em agosto de 2020. Aliada aos decretos estaduais 844/2020 e 1.184/2021 a LGPD traz exigências quanto ao tratamento de dados pessoais, sendo necessário mudanças importantes em processos de negócios da empresa, com a finalidade de trazer segurança e garantia da privacidade dos dados pessoais tratados pela CONTRATANTE, a atualização e aplicação efetiva da política de segurança da informação, em conformidade com a legislação estadual, e a integração das metodologias para tratamento de dados pessoais ao seu Sistema de Gestão Integrado (SGI).

Para realizar o levantamento das ações necessárias para adequação, para validar os processos existentes e integrar as metodologias de tratamento de dados pessoais ao SGI, faz-se necessário a contratação de uma empresa com experiência nesse tipo de implantação.

3. DETALHAMENTO DO OBJETO

O objeto deste Termo Referência será composto em 6 (seis) etapas demonstradas abaixo:

Item	Descrição
01	Planejamento e Treinamento na LGPD
02	Diagnóstico da Situação Atual frente aos requisitos da LGPD – Governança, Proteção de Dados e Segurança da Informação.
03	Determinação do Plano de Ações incluindo ações para os Riscos identificados
04	Criação do Programa de Conformidade e da Política de Segurança da Informação
05	Integração com o Sistema de Gestão integrado - SGI
06	Treinamento para o setor de auditoria interna e compliance apoio na determinação nas ações de divulgação
07	Disponibilização em formato digital, do treinamentos a serem aplicados na integração de novos colaboradores e de fornecedores/prestadores de serviço, cuja atividade envolve o acesso a dados sensíveis sob administração da contratante. Material de divulgação a ser aplicado regularmente quanto à política de governança estabelecida.

4. DESENVOLVIMENTO

O desenvolvimento ocorrerá de acordo com as etapas abaixo:

4.1. Planejamento e Treinamento na LGPD

4.1.1. Para implantação da Lei Geral de Proteção de Dados aos processos organizacionais da CONTRATANTE, a CONTRATADA deverá, inicialmente, definir o escopo de trabalho e sua abrangência por meio de reuniões com colaboradores da CONTRATANTE, especialmente designados para este fim.

Dentre as atividades a serem desenvolvidas, deverá a CONTRATADA efetuar reuniões para detalhamento do plano de projeto, contemplando a metodologia de gestão do projeto, macro programa, plano de comunicação, relatórios de status e interfaces.

4.1.2. Nas reuniões de início do projeto deverão ser tratados os temas:

I. A LGPD e seus aspectos direcionados à Administração Pública;

II. A importância da conformidade para a CONTRATANTE;
III. O processo de adequação;
IV. O processo de construção do programa de conformidade;
V. O processo de adequação da documentação ao SGI – Sistema de Gestão Integrado;
VI. A definição dos agentes envolvidos e seus respectivos papéis de acordo com a Lei Geral de Proteção de Dados.

4.1.3. As reuniões deverão ser realizadas de forma presencial na sede da CONTRATANTE.

4.1.4. Deverá realizar treinamento presencial para a diretoria, grupo de trabalho de apoio a implantação da LGPD visando a apresentação dos requisitos básicos da LGPD e uniformização de linguagem e conceitos;

4.1.5. Deverá realizar treinamento **presencial para os multiplicadores**, visando a apresentação dos requisitos básicos da LGPD e uniformização de linguagem e conceitos e de estabelecer o seu papel na difusão e manutenção dos processos e políticas inerentes à proteção de dados.

4.1.6. Realizar treinamento **presencial para os colaboradores,** visando a apresentação dos requisitos básicos da LGPD e uniformização de linguagem e conceitos.

4.1.7. Deverá disponibilizar treinamento dos requisitos básicos da LGPD, em **formato digital** para orientação de colaboradores que não puderam participar dos treinamentos presenciais ou ainda para capacitação de **novos colaboradores** que vierem a compor o quadro da contratante.

4.1.8. Deverá disponibilizar treinamento em **formato digital** a ser aplicado na **integração de fornecedores e prestadores de serviço**, cuja atividade envolve o acesso a dados sensíveis sob administração da contratante, sobre as políticas de **segurança da informação, restrições e responsabilidades.**

4.1.9. Para cada tipo de treinamento executado (gestores, multiplicadores, colaboradores e terceiros) a contratada deverá elaborar um **rol de perguntas e respostas** do tipo múltipla escolha, a serem aplicadas de forma randomizada em plataforma definida pela contratante, **para avaliação do conhecimento** dos participantes após o curso.

4.1.5. Entrega da etapa:
I. Relatório com detalhamento do plano de projeto de adequação dos processos organizacionais da CONTRATANTE à LGPD, conforme metodologia do PMBOK.
II. Lista de Presença e certificados dos treinamentos realizados;

III. Treinamentos gravados em formato digital acompanhado da cessão de direitos que permita a aplicação a novos colaboradores e terceiros sem ônus adicional;
IV. Questionários de avaliação a ser aplicado a cada tipo de treinamento disponibilizado.

4.2. Diagnóstico da Situação Atual frente aos requisitos da LGPD – Governança, Proteção de Dados e Segurança da Informação.

4.2.1. Identificar o cenário atual da CONTRATANTE em relação a processos, tecnologias, governança, políticas e normas e realizar a avaliação em relação às exigências da Lei nº 13.709/2018 (ex: gerenciamento de incidentes de privacidade; segurança da informação; gerenciamento do ciclo de vida dos dados; responsabilidade de processamento de dados; entre outros) e do Decreto Estadual nº 1.184/2021 .

4.2.2. Avaliar os tipos de contratos existentes quanto ao impacto da lei de privacidade, identificando a necessidade de atualização ou inclusão de cláusulas contratuais.

4.2.3. Identificar quais dados pessoais são processados em cada setor, documentar o fluxo dos dados, a infraestrutura de suporte (tratamento, armazenamento, importação/exportação de dados, sistemas de informação internos e externos, empresas, etc.), ciclo de vida das informações e controles relacionados ao consentimento do titular.

4.2.4. Identificar o propósito de processamento de dados pessoais em cada processo de negócio. Identificar as hipóteses legais para cada tratamento. Identificar os processos nos quais o consentimento do titular dos dados pessoais utilizados deve ser solicitado e formalizado, e de que forma isso deve ocorrer.

4.2.5. Realizar avaliação para identificação de eventuais lacunas entre o cenário atual e as exigências da LGPD e respectivas alterações (ex: identificação de eventuais dados pessoais que não atendam aos critérios de finalidade de processamento; necessidades de alteração de processos/sistemas de informação para garantir atendimento à lei; eventuais necessidades de alteração na gestão do consentimento entre outros).

4.2.6. Identificar e mapear os controles de proteção de dados pessoais existentes frente aos requisitos descritos na LGPD.

4.2.7. Mapear os serviços e processos que tratam dados pessoais e todos os ativos da informação que os suportam: equipamentos, sistemas, recursos humanos e os respectivos dados pessoais tratados.

4.2.8. Identificar e mapear os controles de segurança (técnicos, administrativos e operacionais) implementados que ajam como salvaguardas para os tratamentos de dados pessoais efetuados.

4.2.9. Mapear os controles de segurança existentes frente aos requisitos descritos nas normas aplicáveis.

4.2.10. O mapeamento dos fluxos de tratamento de dados deve ser realizado para cada setor que trata dados pessoais, agrupado por macroprocessos do SGI e detalhar para cada atividade do fluxo, os seguintes itens:

I. Finalidade do tratamento;
II. A atividade realizada (tratamento);
III. Hipótese de tratamento;
IV. Dados pessoais tratados;
V. Tipo de dado: pessoal, pessoal sensível, menores;
VI. Titular dos dados;
VII. Fonte dos dados: direta ou indireta;
VIII. Setor de origem e meio de compartilhamento;
IX. Forma de obtenção e coleta dos dados;
X. Onde os dados são arquivados;
XI. Compartilhamentos externos realizados. Especificar meios, sistemas e setores.
XII. Compartilhamentos internos realizados. Especificar meios e setores.
XIII. Prazo de retenção dos dados pessoais tratados;
XIV. Como é feito o descarte dos dados;
XV. Controles de segurança e proteção de dados implementados.

4.2.11. Levantamento de dados pessoais não estruturados em pastas de arquivos digitais, correio eletrônico etc., utilizando ferramenta de varredura de dados que atenda a esta necessidade, e as operações de tratamento de dados pessoais com eles realizadas. A ferramenta utilizada deve ser devidamente **licenciada pela CONTRATADA sem ônus adicional.**

4.2.12. Identificação de vulnerabilidades internas de segurança da informação, através de **testes de vulnerabilidades**, que possam ser facilitadores de violações de dados. A ferramenta utilizada deve ser devidamente **licenciada pela CONTRATADA sem ônus adicional.**

Entregas da etapa:

I. Relatório da situação atual da CONTRATANTE em relação à LGPD, incluindo a Avaliação Inicial de Riscos por Setor e Geral.
II. Mapa de Dados Pessoais completo, contendo todas as informações constantes no subitem 4.2.10
III. Mapa de Compartilhamento dos Dados.
IV. Relação de gaps identificados.
V. Relatório contendo os locais, documentos e tipos de dados não estruturados;
VI. Relatório contendo as vulnerabilidades encontradas nos testes de vulnerabilidades.

4.3. Determinação do Plano de Ações incluindo ações para os Riscos identificados

4.3.1. Com base no mapeamento do tratamento de dados disposto no item 4.2.10, a CONTRATADA deverá efetuar a análise das necessidades de adequação à LGPD pela CONTRATANTE, especificando:

I. Situação encontrada no levantamento;

II. Recomendação para adequação;

III. Propostas de ações de conformidade.

4.3.2. A análise deverá mencionar o dispositivo legal da LGPD relacionado a cada uma das situações encontradas, bem como avaliar a criticidade e apontar aquelas consideradas como preferenciais para início da adequação.

Entregas da etapa:

I. Medidas necessárias para a mitigação dos riscos identificados capazes de gerar impacto potencial sobre o titular dos dados pessoais, sensíveis ou não, bem como a análise de riscos para o caso de um não atingimento de níveis aceitáveis de compliance em relação à LGPD.

II. Plano de ação identificando as rotinas em que há necessidade de adequação à lei, definindo as ações que precisam ser implementadas para adequação dos processos por setor e o papel de cada responsável de acordo com a LGPD.

4.4. Criação do Programa de Conformidade e da Política de Segurança da Informação

4.4.1. Com base em todas as evidências e recomendações apontadas, a CONTRATADA deverá desenvolver um Programa de Conformidade da CONTRATANTE à LGPD, contemplando um conjunto de ações.

4.4.2. A CONTRATADA, em conjunto com a equipe da CONTRATANTE, deverá indicar os papéis, funções e responsabilidades que a CONTRATANTE deve estabelecer segundo os requisitos da LGPD (controlador, operador, encarregado, entre outros).

4.4.3. Elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), previsto na LGPD, e, após, disponibilizar modelo de preenchimento, bem como dar suporte à equipe da CONTRATANTE no desenvolvimento de novos RIPD's.

4.4.4. Estruturar a política de proteção de dados pessoais, a política de privacidade dos indivíduos, bem como revisar os planos existentes e auxiliar na elaboração da Política de Segurança da Informação em conformidade com a IN SEA 20/2021.

4.4.5. Indicar a necessidade de contratação de softwares específicos e de implementação das alterações nos sistemas de informação existentes na CONTRATANTE, se necessário.

4.4.6. Criar processo para garantir o direito do titular de acesso, de retificação, de exclusão e, caso aplicável, de portabilidade dos dados pessoais, indicando a melhor forma possível de integrá-lo aos processos já existentes, quando necessário ao atendimento de disposição legal.

4.4.7. Criar o processo e canal de interação do titular de dados pessoais com a CONTRATANTE, nos processos em que houver necessidade.

4.4.8. Criar o processo de gerenciamento de incidentes envolvendo dados pessoais e notificações necessárias.

4.4.9. Criar o plano de gestão de crise em caso de incidente/violação de dados.

4.4.10. Revisar e propor alterações necessárias nos termos de acordos de confidencialidade e sigilo com fornecedores, prestadores de serviços, funcionários e elaborar modelos de termos que se fizerem necessários.

4.4.11. A contratada deverá, com base na IN SEA 20/2021, auxiliar o encarregado de dados e grupo de trabalho na revisão e/ou elaboração dos planos que compõem a política de segurança da informação. A contratada, deverá estabelecer em conjunto com o encarregado de dados e a direção, quais indicadores de acompanhamento de implantação dos referidos planos, serão mensurados e integrados ao SGI.

Entregas da etapa:

I. Modelos de contratos e cláusulas-padrão;

II. Relatórios de Impacto à Proteção de Dados pessoais, bem como o modelo a ser adotado pela CONTRATANTE (DPIA);

III. Relatório de Avaliação de Legítimo Interesse (LIA);

IV. Proposta de metodologia de conformidade contínua para governança, gestão da privacidade e segurança da informação na CONTRATANTE;

V. Política corporativa de proteção de dados pessoais e de privacidade dos indivíduos;

VI. Documentação técnica gerada em todas as etapas das atividades desenvolvidas;

VII. Descritivo dos processos de retificação, de exclusão e, caso aplicável, de portabilidade dos dados pessoais, contendo canal de interação do titular dos dados;

VIII. Plano de gestão de crise em caso de incidente/violação de dados.

IX. Planos que compõem a política de segurança da informação, elaborados em conformidade com a IN SEA 20/2021.

4.5. Integração com o SGI

4.5.1. Integrar toda a documentação gerada nos processos acima aos processos do SGI, estabelecer a interrelação entre as políticas existentes e as que forem criadas no processo de adequação à LGPD e propor a forma de integração dos controles, riscos e auditorias referentes à LGPD à metodologia de governança, risco e compliance existentes.

4.5.2. Todo o material deverá ser fornecido de acordo com o padrão da documentação do SGI da CONTRATANTE.

4.6. Treinamento para o setor de auditoria interna e compliance apoio na determinação nas ações de divulgação

4.6.1. Adequar a metodologia de Auditoria Interna de conformidade, realizada pela supervisão de auditoria interna para verificação da eficácia das medidas implantadas.

4.6.2. Treinar os servidores que atuam na área de auditoria interna e compliance na metodologia proposta.

4.6.3. Realizar auditoria interna em conjunto com a supervisão de auditoria interna da CONTRATANTE, em relação aos controles de proteção de dados;

Entregas da etapa:

I. Relatório de Integração da documentação e processos propostos ao SGI;

II. Atualização do Procedimentos de Auditoria Interna;

III. Lista de presença e certificados dos treinamentos dos Auditores Internos;

IV. Relatório de Auditoria Interna;

V. Lista de presença e certificados dos treinamentos para as diretorias, gerências e multiplicadores.

4.7. Disponibilização em formato digital dos treinamentos

4.7.1. Preparar o material e realizar os treinamentos presenciais, a diretoria, gerentes e multiplicadores, referentes aos processos implantados, ou ajustados, de acordo com a LGPD, incluindo modificações introduzidas no Sistema de Gestão Integrado e dos planos que compõem a Política de Segurança da Informação. Os treinamentos deverão também ser fornecidos em formato digital, para aplicação futura sem ônus adicional.

4.7.2. Propor modalidades de disseminação da política de governança adotada para todos os empregados da empresa.

Entregas da etapa:

I. Treinamentos em formato digital;

II. Estratégia e peças de divulgação a serem utilizadas para divulgação regular da política de governança;

4.8. Condições de Prestação de Serviço

4.8.1 A empresa contratada contará com, pelo menos, três colaboradores da CONTRATANTE para auxiliar a contratada para acompanhar a evolução do projeto e ser o interlocutor junto à

consultoria, facilitando acessos demandados, a marcação de reuniões e validar atividades e relatórios gerados.

4.8.2 Definir em conjunto com o Porto de São Francisco do Sul a metodologia formal de trabalho, a gestão e o cronograma que serão adotados durante o desenvolvimento dos trabalhos.

4.8.3 Definir o plano de comunicação e divulgação do projeto, incluindo o engajamento inicial de todas as partes.

4.8.4 Realizar a gestão do projeto segundo o PMBOK (Project Management Body of Knowledge).

4.8.5 Apurar, apresentar e acompanhar os indicadores de gestão dos serviços sob a responsabilidade da CONTRATADA.

4.8.6 Todas as atividades que envolvam usuários e profissionais da CONTRATANTEdeverão ser realizadas em língua portuguesa, incluindo todos os níveis de atendimento, material fornecido, sites e conteúdos disponibilizados, mensagens, entre outros.

4.8.7 Profissionais da CONTRATANTE poderão compor a equipe de trabalho com o objetivo de acompanhar as atividades desenvolvidas e absorver a transferência dos conhecimentos gerados pela CONTRATADA.

4.8.8 As reuniões de trabalho deverão ocorrer em São Francisco do Sul, sem ônus para a CONTRATANTE

4.8.9 A CONTRATADA deverá designar um representante para o gerenciamento do CONTRATO durante sua vigência.

4.8.10 A CONTRATADA deverá prover aos seus profissionais designados os recursos necessários à execução das atividades (microcomputadores e softwares compatíveis com a rede do Porto de São Francisco do Sul, entre outros).

4.8.11 A CONTRATANTE proporcionará à contratada: acesso aos locais, equipamentos, documentos e informações solicitadas.

4.8.12 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 Porto de São Francisco do Sul, de acordo com o cronograma estabelecido.

5. VISITA TÉCNICA

5.1 A proponente deverá realizar visita técnica à CONTRATANTE, para obtenção de atestado, visando conhecer a empresa e contextualizar os trabalhos previstos neste edital para participação no presente processo licitatório. A visita deverá ser realizada pelos licitantes após agendamento

prévio pelo telefone: (47) 3481-4800 ou e-mail: gtlgpd@portodesaofranciscodosul.com.br no horário das 09h às 12h e das 14h às 16h. As visitas técnicas poderão ser agendadas até o terceiro dia útil anterior à data da licitação.

5.2 Caso a proponente não queira participar da visita técnica, deverá apresentar, em substituição ao atestado, declaração formal, assinada pelo responsável técnico, sob penalidade da lei, de que tem pleno conhecimento das condições, necessidades, plano de trabalho, condições de prestação dos serviços, instalações, do local e demais informações de natureza técnica, suficientes e necessárias à sua participação na presente licitação, e que não utilizará deste para quaisquer questionamentos futuros que ensejem avenças técnicas ou financeiras com a CONTRATANTE.

6. REQUISITOS TÉCNICOS

6.1.1. Comprovação de experiência do Proponente:

A proponente deverá providenciar os atestados de capacidade relacionados abaixo, emitidos por instituição pública ou privada.

a) Comprovar experiência em adequação de empresa(s), pública(s) ou privada(s) à LGPD. A descrição deverá conter informações que permitam o entendimento dos trabalhos realizados, bem como aferir o grau de sua compatibilidade, semelhança ou afinidade com o objeto licitado.

b) Comprovar a prestação de serviço de consultoria relacionada à Gestão ou implantação de Sistemas de Gestão da Qualidade baseado na Norma NBR ISO 9001:2015.

6.1.2. Comprovação de experiência e vínculo do(s) profissional(is):

a) Atestado(s) fornecido(s) por pessoa(s) jurídica(s) e emitido(s) em nome da empresa e/ou do(s) responsável(is) técnico(s) pela realização dos serviços objeto deste Edital, comprovando a experiência bem sucedida em consultoria em temas relacionados a Sistema de Gestão Integrado e LGPD – Lei Geral de Proteção de Dados.

c) Atestado(s) fornecido(s) por pessoa(s) jurídica(s) e emitido(s) em nome do(s) profissional(is) que será(ão) responsável(is) pelo gerenciamento do projeto deste Edital, comprovando a experiência bem-sucedida desse(s) profissional(is) em gestão de projetos, utilizando a metodologia PMBoK.

d) Para a equipe responsável pelo serviço objeto deste edital será exigida a Certificação da Exin (ou equivalente) para a Lei Geral de Proteção de Dados, de pelo menos um dos participantes da equipe.

d) Diploma de formação superior na área jurídica, para o profissional responsável por realizar o mapeamento da base legal para o tratamento dos dados;

6.1.3. A CONTRATANTE reserva-se no direito de realizar diligências para comprovação dos documentos apresentados.

7. Prazo de Execução

7.1. O contratado deverá apresentar um cronograma de execução de trabalho que não deve ultrapassar 6 (seis) meses de execução.

7.2. O início dos serviços será contabilizado a partir da Ordem de Início de Serviços (OIS), oficializada pelo administrador do contrato.

8. CRONOGRAMA FÍSICO FINANCEIRO:

O recebimento pelos serviços prestados será realizado em parcelas, mediante apresentação e validação dos entregáveis, conforme quadro abaixo:

FASES	
Planejamento e Treinamento na LGPD	10%
Diagnóstico da Situação Atual frente aos requisitos da LGPD – Governança, Proteção de Dados e Segurança da Informação.	30%
Determinação do Plano de Ações incluindo ações para os Riscos identificados	20%
Criação do Programa de Conformidade e da Política de Segurança da Informação e Integração com o Sistema de Gestão Integrado - SGI	20%
Treinamento da área de auditoria interna e compliance e apoio na determinação das ações de divulgação.	10%
Fornecimento dos treinamentos em formato digital e do material de divulgação relativo à política de governança.	10%

São Francisco do Sul-SC, 4 de agosto de 2022.