



**JP ENGENHARIA**  
**MEDICINA E SEGURANÇA DO TRABALHO**

*Segurança da Informação e  
Tratamento de Dados Pessoais*

## SUMÁRIO

1. Introdução - Página 3
2. Programa de Privacidade - Página 4
  - 2.1 Diretrizes e Responsabilidades - Página 4
    - 2.1.1 Diretrizes Gerais para o Tratamento de Dados Pessoais - Página 4
    - 2.1.2 Responsabilidades - Página 5
      - Encarregado de Proteção de Dados (DPO)
      - Equipe de Tecnologia da Informação (TI)
      - Equipe Jurídica
      - Gestores de Áreas
  - 2.2 Estrutura de Comunicação Interna - Página 6
    - 2.2.1 Canais de Comunicação - Página 6
    - 2.2.2 Relatórios e Auditorias - Página 6
    - 2.2.3 Procedimento para Reportar Incidentes - Página 6
  - 2.3 Monitoramento e Revisão Contínua - Página 6
3. Política de Segurança da Informação (PSI) - Página 7
  - 3.1 Diretrizes para Colaboradores - Página 7
  - 3.2 Diretrizes para Terceiros - Página 10
4. Plano de Comunicação sobre Incidentes de Segurança da Informação e Violação de Dados Pessoais - Página 11
  - 4.1 Procedimento de Comunicação - Página 11
  - 4.2 Plano de Ação e Mitigação - Página 13
  - 4.3 Documentação e Registros - Página 14
  - 4.4 Revisão do Plano - Página 14
5. Privacy by Design – LCA Dos Santos Consultoria - Página 15
  - 5.1 Princípios de Privacidade - Página 15
  - 5.2 Avaliação de Impacto à Proteção de Dados (DPIA) - Página 16
6. Plano de Conformidade com a Base Legal para Tratamento de Dados Pessoais - Página 19
  - 6.1 Bases Legais para o Tratamento de Dados Pessoais - Página 20
  - 6.2 Processo de Garantia de Conformidade - Página 21
  - 6.3 Responsabilidades - Página 21

## Introdução

A LCA dos Santos Consultoria tem como prioridade a conformidade com a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que regula o tratamento de dados pessoais no Brasil. Essa legislação representa um marco na proteção da privacidade e segurança das informações, estabelecendo diretrizes claras para a coleta, armazenamento, uso e compartilhamento de dados pessoais.

Em um cenário de transformação digital acelerada, a LGPD surge como uma resposta às crescentes preocupações com o uso indiscriminado de dados, buscando equilibrar a inovação tecnológica com o respeito aos direitos fundamentais dos indivíduos. Essa lei estabelece princípios fundamentais, como a transparência, a necessidade e a adequação, que norteiam as boas práticas no tratamento de dados pessoais, sejam eles comuns ou sensíveis.

A LCA dos Santos Consultoria, reconhecendo a relevância e o impacto da LGPD, implementa rigorosas políticas de governança e segurança da informação para garantir a conformidade em todas as suas atividades. O compromisso da empresa vai além do atendimento às exigências legais; buscamos promover a confiança e a tranquilidade de nossos clientes, colaboradores e parceiros ao assegurar que os dados pessoais estejam protegidos contra qualquer tipo de incidente ou uso inadequado.

Em nossas operações, especialmente nas áreas de Medicina Ocupacional e Segurança do Trabalho, lidamos com informações sensíveis que requerem atenção especial, como dados médicos e registros de saúde. Cientes da responsabilidade que isso implica, adotamos medidas preventivas, políticas robustas e soluções para garantir a segurança desses dados.

A conformidade com a LGPD também reflete nosso compromisso com a ética e a transparência. Cada etapa do tratamento de dados na LCA dos Santos Consultoria é realizada de forma criteriosa, respeitando os direitos dos titulares, incluindo o acesso às informações, a retificação e a exclusão de dados, conforme previsto pela legislação.

Além disso, entendemos que a implementação da LGPD é uma oportunidade estratégica para aprimorar nossos processos internos, fortalecer nossa governança corporativa e posicionar a LCA dos Santos Consultoria como referência em boas práticas de proteção de dados. Essa abordagem proativa permite não apenas atender às exigências legais, mas também antecipar-se às demandas do mercado e às expectativas dos clientes, promovendo um diferencial competitivo.

Ao longo deste documento, apresentamos as diretrizes, políticas e processos que compõem o Programa de Proteção de Dados da LCA dos Santos Consultoria. Nosso objetivo é oferecer um guia claro e abrangente para garantir que todos os colaboradores e parceiros compreendam sua importância e contribuam para o sucesso desse programa, assegurando um ambiente de conformidade, segurança e confiança para todos.

## 2. Programa de Privacidade

### 2.1 Diretrizes e Responsabilidades

#### 2.1.1 Diretrizes Gerais para o Tratamento de Dados Pessoais

A LCA DOS SANTOS CONSULTORIA se compromete a tratar os dados pessoais de forma segura, transparente e conforme os princípios estabelecidos pela LGPD. As principais diretrizes para o tratamento de dados pessoais incluem:

- **Princípio da Necessidade:** Os dados pessoais serão coletados e tratados somente na medida do necessário para o cumprimento das finalidades estabelecidas.
- **Princípio da Transparência:** A empresa fornecerá informações claras e acessíveis aos titulares sobre o tratamento de seus dados pessoais.
- **Princípio da Segurança:** Serão adotadas medidas de segurança adequadas para proteger os dados pessoais contra acessos não autorizados, vazamentos, danos ou destruição.
- **Princípio da Minimização de Dados:** A coleta de dados será limitada à quantidade necessária para o cumprimento das finalidades e objetivos estabelecidos pela empresa.
- **Princípio da Qualidade:** Os dados pessoais serão mantidos corretos, atualizados e completos durante todo o período de tratamento.

#### 2.1.2 Responsabilidades

As responsabilidades para garantir a implementação e monitoramento do Programa de Privacidade na LCA DOS SANTOS CONSULTORIA são atribuídas às seguintes áreas e cargos:

##### - Encarregado de Proteção de Dados (DPO)

**Responsabilidade:** O Encarregado de Proteção de Dados (DPO) será o principal responsável por garantir a conformidade da empresa com a LGPD e coordenar todas as atividades relacionadas à proteção de dados pessoais.

- Supervisionar a implementação do Programa de Privacidade.
- Garantir que o ROPA (Registro das Operações de Tratamento de Dados Pessoais) seja mantido atualizado.
- Coordenar a realização de Avaliações de Impacto à Proteção de Dados (DPIA).
- Ser o ponto de contato para os titulares dos dados e autoridades de proteção de dados.
- Gerenciar incidentes de segurança e não conformidades.

### **- Equipe de Tecnologia da Informação (TI)**

**Responsabilidade:** A Equipe de TI será responsável por implementar e manter as medidas de segurança para proteger os dados pessoais da empresa.

- Garantir a segurança física e lógica dos sistemas que armazenam ou processam dados pessoais.
- Implementar e monitorar controles de acesso.
- Colaborar com a equipe jurídica para garantir que os contratos com fornecedores de tecnologia estejam em conformidade com a LGPD.

### **- Equipe Jurídica**

**Responsabilidade:** A Equipe Jurídica será responsável por garantir que todos os processos da empresa estejam em conformidade com a LGPD.

- Orientar sobre as obrigações legais e regulamentares relacionadas à privacidade e proteção de dados.
- Revisar e aprovar contratos com fornecedores e parceiros que envolvam o tratamento de dados pessoais.
- Apoiar na elaboração e revisão das políticas internas de privacidade e segurança.

### **- Gestores de Áreas**

**Responsabilidade:** Os gestores de áreas serão responsáveis por garantir que as práticas de privacidade sejam seguidas dentro de suas respectivas áreas e equipes.

- Assegurar que todos os colaboradores sigam as diretrizes de privacidade em suas atividades diárias.
- Monitorar o cumprimento das políticas de privacidade nos processos internos da sua área.

## **2.2. Estrutura de Comunicação Interna**

### **2.2.1 Canais de Comunicação**

A LCA DOS SANTOS CONSULTORIA estabelecerá canais de comunicação para garantir que todas as partes interessadas possam acessar informações relacionadas à privacidade e proteção de dados pessoais.

- **E-mail institucional para privacidade:** [engenharia@engenhariajp.com.br](mailto:engenharia@engenhariajp.com.br).

### **2.2.2 Relatórios e Auditorias**

A empresa realizará relatórios periódicos sobre o andamento do Programa de Privacidade, bem como auditorias internas e externas para verificar o cumprimento das políticas e processos estabelecidos.

- **Periodicidade de Auditorias:** Auditorias internas serão realizadas anualmente.
- **Relatórios de Conformidade:** O Encarregado de Proteção de Dados (DPO) será responsável por elaborar relatórios anuais sobre a conformidade com a LGPD, que serão apresentados à alta gestão.

### 2.2.3 Procedimento para Reportar Incidentes

Qualquer incidente relacionado à segurança de dados ou à não conformidade com a LGPD deverá ser reportado imediatamente por qualquer colaborador ou área à equipe de privacidade. A empresa seguirá um procedimento claro para tratar e resolver tais incidentes.

- **Canal de comunicação para incidentes:** [engenharia@engenhariajp.com.br](mailto:engenharia@engenhariajp.com.br), [comercial@engenhariajp.com.br](mailto:comercial@engenhariajp.com.br).
- **Prazo de resposta:** A empresa se compromete a analisar e responder a incidentes em até 72 horas.

### 2.3 Monitoramento e Revisão Contínua

A empresa se compromete a revisar periodicamente este Programa de Privacidade para garantir que ele esteja atualizado e alinhado com as mudanças na legislação e nas práticas de mercado.

- **Revisão do Programa de Privacidade:** A revisão do programa será realizada anualmente ou sempre que ocorrerem alterações significativas na legislação ou nas operações de tratamento de dados da empresa.

**JP ENGENHARIA**  
MEDICINA E SEGURANÇA DO TRABALHO

## 3. Política de Segurança da Informação (PSI)

### 3.1 Colaboradores.

#### Objetivo

Estabelecer diretrizes claras para assegurar que os colaboradores da empresa compreendam e implementem medidas adequadas de proteção de dados pessoais e informações sensíveis, em conformidade com a LGPD e outras normas aplicáveis.

#### Abrangência

Esta política aplica-se a todos os colaboradores da empresa, incluindo funcionários efetivos, temporários, estagiários e contratados que tenham acesso a sistemas, informações ou dados pessoais no exercício de suas atividades.

## **Diretrizes Gerais**

### **Tratamento de Dados Pessoais**

- Os colaboradores devem garantir que o tratamento de dados pessoais siga as bases legais e as finalidades específicas definidas pela empresa.
- Qualquer uso de dados pessoais fora do escopo permitido é estritamente proibido.
- É obrigatório reportar qualquer incidente envolvendo dados pessoais ao Encarregado de Proteção de Dados (DPO).

### **Confidencialidade e Proteção de Informações**

- Todos os dados e informações acessados são confidenciais e devem ser protegidos contra acessos não autorizados.
- Documentos físicos e digitais devem ser armazenados de forma segura, com restrição de acesso e controle adequado.
- É vedado o uso de dispositivos pessoais não autorizados para acessar informações corporativas.

### **Uso de Sistemas e Tecnologias**

- As credenciais de acesso (login e senha) são individuais e intransferíveis, sendo proibido o compartilhamento com terceiros.
- Os colaboradores devem usar redes seguras e evitar conexões públicas ou não confiáveis para acessar sistemas corporativos.
- Todos os dispositivos fornecidos pela empresa devem conter ferramentas de segurança, como o registro dos equipamentos autorizados para uso na empresa.

### **Treinamento e Conscientização**

- Todos os colaboradores participarão de treinamentos regulares sobre a Política de Segurança da Informação e proteção de dados pessoais.
- A empresa disponibiliza materiais educativos e promove campanhas de conscientização periódicas para reforçar a cultura de segurança da informação.

### **Comunicação de Incidentes**

- É responsabilidade dos colaboradores comunicar imediatamente qualquer incidente de segurança, como perda de dispositivos, acessos indevidos ou suspeitas de vazamento de dados, ao setor de TI ou ao DPO.

### **Monitoramento e Auditoria**

- A empresa realiza auditorias internas periódicas para verificar o cumprimento desta política.
- Não conformidades detectadas podem resultar em ações corretivas e sanções disciplinares.

### **Declaração de Concordância**

Todos os colaboradores devem assinar um termo de adesão, comprometendo-se a seguir rigorosamente esta política e a zelar pela proteção das informações da empresa, representada abaixo.

## **CONTRATO DE PROTEÇÃO DE DADOS E CONFIDENCIALIDADE**

Contratante: **LCA DOS SANTOS CONSULTORIA** com sede em Rua Gilson Claudinei Bernardes, nº178, Parque Residencial Rondon – Lençóis Paulista – SP inscrita no CNPJ sob o nº **47.530.461/0001-30**;

Contratada: **NOME DO FUNCIONARIO** com sede ( **endereço do funcionário** ) inscrito no CPF sob o nº **000.000.000-00**, tem entre si justo e acertado, o presente **CONTRATO DE PROTEÇÃO DE DADOS E CONFIDENCIALIDADE**, que será regido pelas cláusulas e condições elencadas abaixo:

1. O presente contrato tem por objeto assegurar a proteção, confidencialidade e integridade dos dados pessoais e/ou informações sensíveis fornecidos pela Contratante à Contratada, conforme a Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018.

2. Para os fins deste contrato, aplicam-se as seguintes definições:

a) **Dados Pessoais:** Qualquer informação relacionada à pessoa natural identificada ou identificável.

b) **Tratamento de Dados:** Toda operação realizada com dados pessoais, como coleta, armazenamento, compartilhamento e exclusão.

c) **Dado Sensível:** Informações sobre origem racial, convicções religiosas, saúde, dados biométricos, entre outros.

3.1 A Contratada compromete-se a:

a) Utilizar os dados pessoais exclusivamente para as finalidades especificadas pela Contratante;

b) Adotar medidas técnicas e organizacionais para proteger os dados contra acessos não autorizados, perda, destruição ou alteração;

c) Comunicar à Contratante qualquer incidente de segurança que comprometa os dados.

3.2. A Contratante compromete-se a fornecer somente os dados estritamente necessários para a execução dos serviços contratados.

4. Ambas as partes se comprometem a manter sigilo sobre todas as informações confidenciais obtidas em razão deste contrato, não podendo divulgá-las a terceiros sem prévia autorização por escrito.

5.1. O descumprimento das obrigações previstas neste contrato sujeitará a parte infratora às seguintes penalidades:

- a) Advertência formal: Na primeira ocorrência de descumprimento.
- b) Multa contratual: Em caso de reincidência ou violação grave, será aplicada multa equivalente a valor ou percentual sobre o contrato, corrigida monetariamente.
- c) Rescisão contratual: No caso de descumprimento reiterado ou comprometimento severo dos dados.
- d) Indenização por perdas e danos: Caso haja prejuízos comprovados decorrentes da violação de dados ou informações confidenciais.

6. Este contrato entra em vigor na data de sua assinatura e permanecerá vigente pelo prazo indeterminado, podendo ser renovado mediante acordo entre as partes.

As partes elegem o foro da comarca de LENÇÓIS PAULISTA - SP para dirimir quaisquer controvérsias oriundas deste contrato, renunciando a qualquer outro, por mais privilegiado que seja.

E por estarem assim justos e contratados, assinam o presente contrato em duas vias de igual teor e forma, na presença das testemunhas abaixo.

\_\_\_\_\_  
LCA DOS SANTOS CONSULTORIA 01/08/2024

\_\_\_\_\_  
NOME DO FUNCIONARIO 01/08/2024

Testemunhas:

1. \_\_\_\_\_ CPF: \_\_\_\_\_

2. \_\_\_\_\_ CPF: \_\_\_\_\_

---

## 3.2 Terceiros

### Objetivo

Definir diretrizes para assegurar que terceiros que prestam serviços à empresa compreendam e cumpram os requisitos de proteção de dados pessoais e segurança da informação, minimizando riscos associados ao compartilhamento de informações.

### Abrangência

Aplica-se a todos os terceiros, incluindo fornecedores, consultores, parceiros e prestadores de serviços que tratem dados pessoais ou tenham acesso a informações sensíveis da empresa.

### Diretrizes Gerais

#### Tratamento de Dados Pessoais por Terceiros

- Os terceiros devem assegurar que o tratamento de dados pessoais siga as diretrizes e bases legais definidas pela empresa.
- O compartilhamento de dados pessoais só será permitido mediante contrato formal e com medidas de segurança adequadas.
- Terceiros devem nomear um responsável pelo cumprimento das diretrizes de segurança e proteção de dados acordadas.

#### Requisitos Contratuais

- Todos os contratos com terceiros devem conter cláusulas específicas sobre a proteção de dados pessoais, confidencialidade e segurança da informação.
- Os contratos devem prever penalidades em caso de descumprimento das diretrizes ou incidentes de segurança.

#### Segurança e Confidencialidade

- Os terceiros devem implementar controles adequados de segurança, como criptografia, autenticação e backup seguro, para proteger os dados pessoais compartilhados pela empresa.
- É proibido o uso de dados pessoais para finalidades não autorizadas ou além do escopo contratado.

## **Comunicação de Incidentes**

- Os terceiros devem reportar imediatamente à empresa qualquer incidente de segurança envolvendo dados pessoais ou informações sensíveis.
- A empresa poderá exigir relatórios detalhados e medidas corretivas para mitigar os impactos de incidentes reportados.

## **Monitoramento e Auditoria**

- A empresa reserva-se o direito de realizar auditorias nos terceiros para verificar a conformidade com as diretrizes de segurança e proteção de dados.
- O não cumprimento das diretrizes poderá levar à rescisão contratual ou aplicação de penalidades previstas no contrato.

## **Treinamento e Suporte**

- Sempre que necessário, a empresa fornecerá orientações ou manuais com diretrizes específicas para os terceiros relacionados ao tratamento de dados pessoais e segurança da informação.

## **Declaração de Concordância**

Todos os terceiros devem assinar um termo de compromisso, confirmando a adesão às diretrizes estabelecidas nesta política e a responsabilidade pelo cumprimento das cláusulas contratuais.

---

## **4. Plano de Comunicação sobre Incidentes de Segurança da Informação e Violação de Dados Pessoais**

### **Objetivo**

Estabelecer um procedimento claro e eficiente para a comunicação interna e externa sobre incidentes de segurança da informação e violação de dados pessoais, com o objetivo de mitigar os impactos e garantir a conformidade com a legislação aplicável, como a Lei Geral de Proteção de Dados (LGPD).

### **Abrangência**

Este plano se aplica a todos os incidentes de segurança da informação que envolvam dados pessoais, seja dentro da empresa ou por parte de terceiros que tratem dados pessoais em nome da empresa.

### **Definições**

- **Incidente de Segurança da Informação:** Qualquer evento, intencional ou acidental, que comprometa a confidencialidade, integridade ou disponibilidade das informações.
- **Violação de Dados Pessoais:** Qualquer ato que comprometa, de maneira inadequada ou não autorizada, a segurança dos dados pessoais coletados e armazenados pela empresa.

## 4.1 Procedimento de Comunicação

### Identificação do Incidente

- Qualquer funcionário que identificar um incidente de segurança ou uma violação de dados pessoais deve imediatamente reportar o ocorrido ao time de TI ou ao Encarregado de Proteção de Dados (DPO), utilizando os canais de comunicação previamente definidos.
- Os incidentes podem ser identificados através de alertas automáticos do sistema, notificações de sistemas de monitoramento, ou comunicação direta de colaboradores, terceiros ou clientes.

### Análise Inicial e Avaliação

- O time de TI e o DPO devem realizar uma análise preliminar do incidente para entender a gravidade, o escopo e o impacto da violação de dados pessoais.
- Determinar, com base na avaliação, se a violação de dados deve ser comunicada à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados afetados.

### Comunicação Interna

- **Imediata Notificação:** Assim que um incidente for identificado e avaliado, a comunicação interna deve ser realizada imediatamente para alertar as áreas afetadas e evitar maiores impactos.
- **Público Interno:** Notificação para todos os colaboradores, com informações sobre o ocorrido, medidas adotadas e como proceder caso os dados pessoais sejam afetados.
- **Liderança e Gestores:** Comunicação direta com os gestores e líderes das equipes envolvidas, para que possam tomar as ações necessárias e responder adequadamente a perguntas dos colaboradores.

### Comunicação Externa

Comunicação à Autoridade Nacional de Proteção de Dados (ANPD)

- Caso a violação de dados pessoais apresente risco ou danos aos direitos e liberdades dos titulares, a empresa deve notificar a ANPD dentro do prazo de 72 horas, conforme determina a LGPD.
- A notificação deve conter informações sobre a natureza do incidente, categorias de dados pessoais envolvidos, número estimado de pessoas afetadas, medidas tomadas para mitigar os danos e medidas planejadas para evitar novos incidentes.

#### Comunicação aos Titulares dos Dados Pessoais

- Quando o incidente representar um risco significativo aos direitos dos titulares, a empresa deve enviar uma comunicação clara e objetiva aos indivíduos afetados.
- A comunicação deve incluir:
  - Descrição do incidente.
  - Dados pessoais afetados.
  - Medidas que a empresa está tomando para mitigar os impactos.
  - Instruções sobre como os titulares podem proteger seus dados pessoais.
  - Contato da equipe responsável pela proteção de dados da empresa (DPO ou outro).

#### Comunicação a Terceiros e Parceiros

- Caso os incidentes envolvam terceiros ou parceiros, é necessário que eles sejam notificados de imediato, principalmente se seus sistemas ou dados pessoais tenham sido comprometidos.
- A comunicação deve seguir as diretrizes do contrato, sempre informando sobre as ações corretivas que estão sendo tomadas para evitar danos adicionais.

MEDICINA E SEGURANÇA DO TRABALHO

## 4.2 Plano de Ação e Mitigação

### Ações Imediatas

- Remoção da vulnerabilidade que causou o incidente.
- Isolamento de sistemas comprometidos para evitar a propagação de danos.
- Iniciação de investigação técnica para rastrear a origem e o alcance da violação.

### Medidas de Longo Prazo

- Atualização e fortalecimento das políticas de segurança da informação.
- Implementação de novos controles para evitar a recorrência do incidente.
- Realização de treinamentos contínuos para colaboradores sobre proteção de dados e segurança da informação.

## Treinamento e Conscientização

Todos os colaboradores devem ser treinados sobre como identificar possíveis incidentes de segurança e sobre o processo de comunicação, garantindo uma resposta rápida e eficaz.

## Monitoramento e Auditoria

- Após a implementação das medidas corretivas, a empresa deve realizar um acompanhamento para avaliar a eficácia das ações tomadas e ajustar o plano conforme necessário.
- Auditorias periódicas devem ser realizadas para verificar a aderência aos processos de segurança e identificar possíveis melhorias.

### 4.3 Documentação e Registros

- Todos os incidentes de segurança devem ser documentados, com relatórios detalhados sobre o ocorrido, as ações tomadas e os resultados obtidos.
- Os registros devem ser mantidos para possíveis auditorias internas ou externas e como parte do processo de aprendizado e melhoria contínua.

---

### 4.4 Revisão do Plano

- O plano de comunicação sobre incidentes será revisado periodicamente para garantir sua eficácia e conformidade com as normas e regulamentações, além de se ajustar a novos tipos de incidentes que possam surgir.

MEDICINA E SEGURANÇA DO TRABALHO

---

## 5. Privacy by Design - LCA Dos Santos Consultoria

**Objetivo:** Garantir que a proteção de dados pessoais seja incorporada desde a concepção de todos os processos e serviços oferecidos pela LCA Dos Santos Consultoria, com foco na segurança e privacidade dos dados dos colaboradores, clientes e demais partes interessadas.

### 5.1 Princípio da Minimização de Dados

A LCA dos Santos Consultoria compromete-se a coletar apenas os dados necessários para a execução de suas atividades. A coleta de dados será limitada ao mínimo necessário para a prestação de serviços em Medicina Ocupacional e Segurança do Trabalho, sempre de acordo com as necessidades contratuais e regulamentações legais aplicáveis.

- **Exemplo de Implementação:** Quando coletar informações dos colaboradores para exames médicos ocupacionais, a empresa solicitará apenas os dados essenciais para a realização dos exames e a emissão dos laudos.

### **Privacidade desde a Concepção**

Todos os sistemas, processos e atividades que envolvem o tratamento de dados pessoais serão desenvolvidos com a privacidade como um elemento central, respeitando os direitos dos indivíduos e as regulamentações da Lei Geral de Proteção de Dados (LGPD).

- **Exemplo de Implementação:** Durante o desenvolvimento de novos serviços ou soluções tecnológicas, a empresa garantirá que todas as funcionalidades respeitem as diretrizes de privacidade, como a anonimização de dados sensíveis quando possível.

### **Segurança dos Dados Pessoais**

A LCA dos Santos Consultoria adotará medidas técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais, prevenindo acessos não autorizados, vazamentos ou qualquer outro tipo de incidente de segurança.

- **Exemplo de Implementação:** Implementação de criptografia em sistemas que armazenam dados sensíveis, realização de auditorias regulares e treinamentos periódicos para os colaboradores sobre a importância da segurança da informação.

### **Transparência e Direitos dos Titulares**

A empresa se compromete a fornecer informações claras e transparentes sobre o tratamento dos dados pessoais, incluindo o propósito da coleta, o período de retenção dos dados e os direitos dos titulares.

- **Exemplo de Implementação:** Inclusão de cláusulas de consentimento claras nos contratos com clientes e colaboradores, permitindo o acesso fácil e a compreensão sobre como seus dados serão utilizados.

### **Limitação do Prazo de Retenção**

A LCA dos Santos Consultoria manterá os dados pessoais apenas pelo tempo necessário para cumprir as finalidades para as quais foram coletados, em conformidade com as exigências legais e contratuais.

- **Exemplo de Implementação:** Estabelecimento de um período de retenção específico para os registros de exames médicos ocupacionais, conforme a legislação vigente, com a eliminação dos dados após esse prazo.

### **Responsabilidade e Governança de Dados**

A empresa criará uma estrutura de governança de dados, com a nomeação de um encarregado de proteção de dados (DPO), que será responsável por assegurar que as práticas de tratamento de dados pessoais estejam em conformidade com as regulamentações e diretrizes internas.

- **Exemplo de Implementação:** Nomeação de um DPO responsável por revisar políticas de privacidade, realizar auditorias internas e responder a eventuais solicitações de titulares dos dados.

## 5.2 Avaliação de Impacto à Proteção de Dados (DPIA)

A LCA dos Santos Consultoria realizará Avaliações de Impacto à Proteção de Dados (DPIA) para identificar e mitigar riscos associados ao tratamento de dados pessoais em novos projetos ou processos.

- **Exemplo de Implementação:** Antes de iniciar novos tratamentos de dados ou tecnologias que envolvam dados sensíveis, a empresa realizará uma avaliação de impacto para avaliar riscos e tomar medidas corretivas.

### MODELO DO DPIA

#### 1. Informações Gerais

- **Nome da empresa:** LCA dos Santos Consultoria
- **Data de elaboração:** [Data]
- **Responsável pelo tratamento de dados:** [Nome do responsável]
- **Encarregado de Proteção de Dados (DPO):** [Nome do DPO ou responsável]
- **Departamento/Setor:** [Nome do departamento que realiza o tratamento]

#### Descrição do Tratamento de Dados

- **Objetivo do tratamento:**  
Descrever o propósito para o qual os dados pessoais serão processados.  
Exemplo: "Coleta e análise de dados médicos ocupacionais de colaboradores para cumprimento das exigências de saúde e segurança no ambiente de trabalho."
- **Tipos de dados pessoais tratados:**  
Especificar os dados coletados, como:
  - Dados pessoais identificáveis (nome, CPF, RG)
  - Dados de saúde (resultados de exames médicos, histórico de saúde)
  - Dados de contato (telefone, e-mail)
- **Categorias de titulares:**  
Defina as categorias de indivíduos cujos dados são tratados, como:

- Colaboradores
- Prestadores de serviço
- Clientes (em casos específicos)
- **Método de coleta:**  
Indicar como os dados são coletados. Exemplo: "Através de formulários de saúde, registros em sistemas eletrônicos, exames médicos periódicos."
- **Armazenamento e processamento:**  
Descrever como os dados serão armazenados e processados. Exemplo: "Os dados serão armazenados em sistemas internos, acessíveis apenas por profissionais autorizados, e mantidos em servidores seguros."

### **Necessidade e Proporcionalidade**

- **Necessidade do tratamento:**  
Justificar o tratamento de dados pessoais. Exemplo: "A coleta de dados médicos é necessária para garantir a saúde dos colaboradores e o cumprimento das normas regulamentadoras de segurança do trabalho."
- **Proporcionalidade:**  
Verificar se a coleta de dados é proporcional e não excessiva. Exemplo: "Serão coletados apenas os dados médicos essenciais para avaliar as condições de trabalho e saúde ocupacional."

### **Riscos Identificados**

- **Identificação de riscos:**  
Listar os riscos que podem surgir no tratamento dos dados pessoais. Exemplo:
  - Acesso não autorizado aos dados sensíveis
  - Vazamento de dados durante a transmissão
  - Perda de dados devido a falhas nos sistemas
- **Probabilidade e impacto dos riscos:**  
Avaliar a probabilidade e o impacto de cada risco. Exemplo:
  - "Risco de acesso não autorizado: Probabilidade média, impacto alto."
  - "Risco de vazamento de dados: Probabilidade baixa, impacto médio."

### **Medidas Mitigadoras**

- **Medidas técnicas:**  
Descrever as soluções técnicas adotadas para mitigar os riscos. Exemplo:

- Implementação de criptografia para armazenar e transmitir dados médicos.
- Uso de sistemas com controle de acesso restrito, garantindo que apenas pessoas autorizadas possam acessar os dados.
- **Medidas organizacionais:**  
Definir ações dentro da estrutura organizacional para proteger os dados.  
Exemplo:
  - Treinamento periódico dos colaboradores sobre a proteção de dados pessoais.
  - Revisão contínua das políticas de segurança da informação e procedimentos de acesso.

### **Consulta à Autoridade de Proteção de Dados (se aplicável)**

- **Necessidade de consulta:**  
Caso os riscos não possam ser adequadamente mitigados, é necessário consultar a autoridade de proteção de dados (como a ANPD no Brasil).

Exemplo: "Após análise dos riscos, não há necessidade de consulta à Autoridade Nacional de Proteção de Dados, pois todas as medidas de mitigação foram implementadas."

### **Decisão sobre o Tratamento**

- **Aprovação do tratamento:**  
Decidir se o tratamento pode seguir conforme planejado ou se há necessidade de ajustes nas medidas de segurança.  
Exemplo: "O tratamento pode prosseguir, com as medidas de mitigação descritas neste relatório."
- **Ações corretivas:**  
Caso haja necessidade de ajustes, liste as ações corretivas. Exemplo: "Implementar autenticação multifatorial para acesso aos dados sensíveis."

### **Plano de Monitoramento e Revisão**

- **Plano de revisão:**  
Defina quando a DPIA será revisada. Exemplo: "A DPIA será revisada semestralmente, ou sempre que houver alterações nos processos de tratamento de dados ou na legislação."
- **Monitoramento contínuo:**  
Descrever como o tratamento de dados será monitorado de forma contínua.

Exemplo: "A revisão da segurança dos sistemas será feita trimestralmente e as políticas de proteção de dados serão atualizadas conforme necessidade."

### Aprovação e Assinatura

- **Responsável pela aprovação:**  
Nome do responsável pela aprovação do relatório de DPIA.
- **Assinatura:**  
[Assinatura do responsável]
- **Data de aprovação:**  
[Data]

---

## 6. Plano de Conformidade com a Base Legal para Tratamento de Dados Pessoais

### Objetivo

Garantir que o tratamento de dados pessoais realizado pela empresa esteja em conformidade com as bases legais previstas pela Lei Geral de Proteção de Dados (LGPD) e demais regulamentações aplicáveis, assegurando a legalidade, transparência e segurança no processamento de dados pessoais.

---

### Bases Legais para o Tratamento de Dados Pessoais

A empresa adota as seguintes bases legais para o tratamento de dados pessoais, conforme estabelecido pela LGPD:

1. **Consentimento:** A empresa garante que o tratamento de dados pessoais será realizado com o consentimento explícito do titular, quando necessário, especialmente em situações onde o consentimento seja a única base legal.
2. **Cumprimento de Obrigações Legais ou Regulatórias:** O tratamento de dados pessoais é realizado para cumprir obrigações legais ou regulatórias, como para fins fiscais, de auditoria ou outros requisitos legais.
3. **Execução de Contrato:** A empresa realiza o tratamento de dados pessoais quando necessário para a execução de contratos com os titulares, como contratos de serviços, fornecimento de produtos, etc.
4. **Interesse Legítimo:** A empresa pode tratar dados pessoais para atender ao seu interesse legítimo, sempre respeitando os direitos e liberdades dos titulares de dados, e garantindo que o interesse legítimo seja ponderado com os direitos do titular.

5. **Proteção da Vida ou da Segurança:** Em situações emergenciais, como em casos de risco à vida ou segurança do titular, a empresa pode tratar dados pessoais para garantir a proteção dessas necessidades.
6. **Execução de Políticas Públicas:** O tratamento de dados pessoais pode ser realizado quando necessário para a execução de políticas públicas, conforme autorizado por leis específicas.
7. **Estudos de Viabilidade:** A empresa pode tratar dados para fins de estudos de viabilidade, pesquisas científicas ou históricas, garantindo a anonimização quando possível.

### Processo de Garantia de Conformidade

1. **Identificação da Base Legal:** Antes de iniciar o tratamento de dados pessoais, a equipe responsável identificará qual base legal é aplicável a cada tipo de tratamento realizado.
2. **Documentação de Consentimento:** Quando o tratamento se basear no consentimento, a empresa garantirá que o consentimento seja claro, explícito e documentado. O titular terá a opção de revogar o consentimento a qualquer momento.
3. **Avaliação Periódica:** O tratamento de dados será revisado periodicamente para garantir que continua em conformidade com a base legal aplicada. Caso haja alterações nas atividades de tratamento, uma nova avaliação será realizada.
4. **Transparência e Comunicação com os Titulares:** A empresa garantirá que os titulares sejam informados de forma transparente sobre qual base legal está sendo utilizada para o tratamento de seus dados. Isso será feito por meio de políticas de privacidade claras e acessíveis.
5. **Treinamento e Capacitação:** A equipe envolvida no tratamento de dados pessoais será treinada regularmente sobre as bases legais do tratamento e os procedimentos para garantir conformidade com a LGPD.
6. **Monitoramento e Auditoria:** O DPO (Encarregado de Proteção de Dados) realizará auditorias internas periódicas para verificar a conformidade com as bases legais e os processos de tratamento de dados.
7. **Ação Corretiva:** Caso sejam identificadas não conformidades, a empresa implementará ações corretivas imediatas, como a revisão das práticas de tratamento de dados e a implementação de medidas adicionais de segurança.

### Responsabilidades

- **DPO (Encarregado de Proteção de Dados):** Responsável por supervisionar e garantir que o tratamento de dados pessoais esteja em conformidade com as bases legais e a LGPD.
- **Equipe de TI e Segurança:** Responsável por implementar as medidas de segurança e controle no tratamento de dados, garantindo que os dados pessoais sejam protegidos durante todo o ciclo de vida.

- **Gestores e Funcionários:** Responsáveis por garantir que suas atividades de tratamento de dados pessoais estejam alinhadas às bases legais estabelecidas e que cumpram as normas internas de proteção de dados.



São Manuel, 11 de dezembro de 2024

---

LCA dos Santos Consultoria  
CNPJ: 47.530.461/0001-30

**JP ENGENHARIA**  
MEDICINA E SEGURANÇA DO TRABALHO