

Com a palavra, a Direção,

Reafirmamos nosso compromisso com a proteção dos dados pessoais, como parte essencial do nosso Programa de COMPLIANCE e do respeito aos direitos fundamentais. Reconhecemos a privacidade como um valor central da sociedade atual e, por isso, adotamos uma postura ativa, ética e transparente no tratamento das informações que nos são confiadas.

Mais do que atender às exigências legais, esta política reflete nosso compromisso com a dignidade, a liberdade e a autonomia informacional dos indivíduos. Esperamos que todos os nossos colaboradores, parceiros e prestadores de serviço atuem com responsabilidade e zelo, assegurando a segurança, confidencialidade e integridade dos dados pessoais sob nossa gestão.

1. Introdução

A proteção de dados pessoais é essencial para garantir a privacidade e a segurança das informações em um cenário cada vez mais digitalizado, no qual o tratamento de dados se torna parte integrante das atividades cotidianas. Em conformidade com a Lei Geral de Proteção de Dados (LGPD), proteger essas informações vai além do cumprimento legal: trata-se de um compromisso ético que fortalece a confiança entre indivíduos, organizações e o poder público.

A adoção de medidas eficazes de proteção de dados contribui para a prevenção de usos indevidos, como fraudes, roubo de identidade e outras formas de violação da privacidade. Dessa forma, assegura-se a integridade, a confidencialidade e a transparência no tratamento de dados pessoais, conforme os princípios estabelecidos pela LGPD.

Adicionalmente, a proteção de dados reforça o direito fundamental à privacidade e promove uma cultura de responsabilidade, respeito e governança no uso das informações pessoais. Em última instância, a observância da LGPD apoia a autodeterminação informativa dos titulares de dados, garantindo-lhes maior controle sobre suas informações em um mundo cada vez mais interconectado.

2. Objetivo

A principal finalidade da Política de Proteção de Dados Pessoais é assegurar a privacidade, a segurança e a integridade das informações dos titulares, regulando de forma clara e transparente como os dados pessoais são coletados, tratados, armazenados e compartilhados. Essa política está alinhada com os princípios e diretrizes da Lei Geral de Proteção de Dados (LGPD), garantindo o respeito aos direitos fundamentais de liberdade, privacidade e à livre formação da personalidade de cada indivíduo.

A Política visa promover a transparência no tratamento de dados pessoais, estabelecendo diretrizes que orientam o uso ético e responsável das informações, além de fomentar a cultura de proteção de dados dentro da organização. Ao adotar essas práticas, busca-se fortalecer a confiança entre os titulares de dados e a organização, incentivando a conformidade com as normas legais e a aplicação de boas práticas em segurança da informação.

Adicionalmente, são previstos mecanismos de responsabilização, monitoramento e sanções em caso de incidentes ou descumprimento das obrigações legais, reforçando o compromisso institucional com a proteção dos dados pessoais.

3. A quem se destina

Todos os que fazem parte da Walter Lopes e que, direta ou indiretamente, possam realizar o tratamento de dados pessoais em nome da Walter Lopes, devem observar as diretrizes estabelecidas nesta Política de Proteção de Dados, incluindo, mas não se limitando a:

Organizações Privadas: Empresas de diferentes portes vinculadas à Walter Lopes, que colem, tratem ou armazenem dados pessoais no desempenho de suas atividades.

Entidades Públicas: Órgãos ou instituições públicas que atuem em parceria ou sob responsabilidade da Walter Lopes, manipulando dados pessoais no exercício de funções como prestação de serviços públicos, segurança ou administração.

Organizações Sem Fins Lucrativos: ONGs, associações, fundações ou outras entidades sem fins lucrativos associadas à Walter Lopes que realizem o tratamento de dados pessoais para cumprir suas finalidades institucionais.

Titulares dos Dados: Indivíduos a quem os dados pessoais se referem. A política da Walter Lopes tem como objetivo proteger os direitos e liberdades fundamentais desses titulares, especialmente no que diz respeito à privacidade, à autodeterminação informativa e ao controle sobre seus dados.

Fornecedores de Serviços e Terceiros: Parceiros comerciais, prestadores de serviços, consultores, e quaisquer terceiros que, por força contratual ou operacional, tenham acesso a dados pessoais no contexto de suas atividades com a Walter Lopes. Esses agentes devem observar os princípios da segurança e confidencialidade no tratamento dos dados.

Autoridades Reguladoras: Órgãos governamentais ou entidades independentes com competência para fiscalizar o cumprimento da legislação de proteção de dados, incluindo a Autoridade Nacional de Proteção de Dados (ANPD), com os quais a Walter Lopes se compromete a cooperar.

3. Princípios da Proteção de Dados

Além dos princípios estabelecidos pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), é fundamental destacar os princípios aos quais a Walter Lopes, bem como todas as partes interessadas anteriormente identificadas, está submetida:

Legalidade, Justiça e Transparência: O tratamento de dados pessoais deve ser realizado de forma legal, justa e transparente em relação ao titular. A Walter Lopes compromete-se a garantir que todas as operações de tratamento possuam base legal adequada e sejam comunicadas de forma clara e acessível.

Limitação da Finalidade: Os dados pessoais devem ser coletados para finalidades determinadas, explícitas e legítimas. A Walter Lopes assegura que os dados não serão tratados de forma incompatível com os propósitos originais informados aos titulares, respeitando os limites legais.

Minimização dos Dados: A Walter Lopes compromete-se a coletar apenas os dados pessoais estritamente necessários para atingir as finalidades pretendidas, evitando o tratamento excessivo ou irrelevante.

Exatidão: Os dados pessoais tratados devem ser precisos e atualizados sempre que necessário. A Walter Lopes adota medidas para corrigir ou eliminar, sem demora, quaisquer informações inexatas, assegurando a qualidade dos dados.

Limitação de Conservação: Os dados serão armazenados somente pelo tempo necessário ao cumprimento das finalidades que justificaram sua coleta e tratamento. Após esse período, a Walter Lopes providenciará sua eliminação ou anonimização, conforme a legislação aplicável.

Integridade e Confidencialidade (Segurança): A Walter Lopes implementa medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra acessos não autorizados, uso indevido, perda, destruição ou qualquer forma de tratamento ilícito ou acidental.

Responsabilidade e Prestação de Contas: A Walter Lopes é responsável por assegurar o cumprimento dos princípios de proteção de dados e por demonstrar a sua conformidade. Isso inclui a adoção de políticas internas, treinamentos contínuos, auditorias regulares e mecanismos eficazes de governança em proteção de dados.

4. Identificação e Classificação de Dados Pessoais

A Lei Geral de Proteção de Dados (LGPD) do Brasil, estabelece um marco legal para a proteção de dados pessoais e impacta todas as organizações que processam dados de indivíduos no Brasil.

A LGPD classifica os dados pessoais em duas categorias principais: dados pessoais e dados pessoais sensíveis. A identificação e classificação desses dados são cruciais para a adequação e o cumprimento da lei.

Dados Pessoais

São informações relacionadas a pessoa natural identificada ou identificável. Isso inclui uma ampla gama de informações que, direta ou indiretamente, podem identificar uma pessoa. Exemplos de dados pessoais incluem, não se limitando a:

Nome completo;

Número de identidade (RG, CPF);

Endereço de e-mail;

Endereço residencial;

Número de telefone;

Informações de localização;

Identificadores digitais (como endereços IP, cookies);

Dados de comportamento e preferências pessoais.

Dados Pessoais Sensíveis

São um subconjunto de dados pessoais que estão relacionados a características específicas que podem ser utilizadas de forma discriminatória. A LGPD dá especial atenção a esses dados devido ao potencial risco de causar danos aos titulares dos dados. Incluem:

Origem racial ou étnica;

Convicção religiosa;

Opinião política;

Filiação a sindicato ou a organização de caráter religioso, filosófico ou político;

Dados referentes à saúde ou à vida sexual;

Dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

A correta identificação e classificação dos dados pessoais e sensíveis são fundamentais para determinar o nível de proteção e as medidas de segurança necessárias. A LGPD exige que as organizações adotem procedimentos e práticas que garantam a proteção desses dados, com atenção especial aos dados sensíveis, que exigem consentimento específico e destacado para seu tratamento, exceto em casos previstos por lei.

5. Tratamento de Dados Pessoais

A coleta e o tratamento de dados devem atender aos princípios, acima postos e apresentados na LGPD, e só pode ser realizada sob condições que garantam a proteção dos direitos fundamentais de liberdade e de privacidade.

O tratamento de dados é qualquer operação ou conjunto de operações realizadas com dados pessoais ou conjuntos de dados pessoais. Isso inclui desde a coleta inicial dos dados até sua eliminação final, abrangendo uma ampla gama de atividades que podem ser realizadas manualmente ou por meios automatizados. Constitui tratamento de dados: a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

6. Base legal que fundamenta o tratamento de dados

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) define que o tratamento de dados pessoais somente pode ocorrer nas hipóteses legalmente previstas, garantindo a proteção dos direitos dos titulares. A coleta e o uso de dados pessoais devem observar uma base legal legítima, entre as quais destacam-se:

Consentimento do Titular: O tratamento pode ocorrer mediante consentimento livre, informado e inequívoco do titular, com a devida transparência quanto à finalidade específica dos dados coletados.

Cumprimento de Obrigação Legal ou Regulatória: Quando o tratamento for necessário para que o controlador atenda exigências legais ou regulatórias, nos termos da legislação vigente.

Execução de Políticas Públicas: Em situações previstas em lei, o tratamento pode ser realizado pela administração pública para fins de execução de políticas públicas.

Estudos por Órgão de Pesquisa: O tratamento é permitido para fins de pesquisa, desde que garantida, sempre que possível, a anonimização dos dados pessoais.

Execução de Contrato ou Procedimentos Preliminares: Quando os dados forem necessários para a celebração ou execução de contrato do qual o titular seja parte, ou para diligências pré-contratuais a pedido do titular.

Exercício Regular de Direitos: O tratamento é autorizado para assegurar o exercício de direitos em processos judiciais, administrativos ou arbitrais.

Proteção da Vida ou da Incolumidade Física: Quando for imprescindível para resguardar a vida ou a integridade física do titular ou de terceiros.

Tutela da Saúde: Exclusivamente para procedimentos realizados por profissionais ou entidades da área da saúde, ou ainda por autoridade sanitária, conforme a necessidade.

Interesse Legítimo do Controlador ou de Terceiro: É permitido o tratamento quando necessário para atender interesses legítimos, desde que não se sobreponham aos direitos e liberdades fundamentais do titular.

Proteção do Crédito: Inclui o tratamento de dados pessoais necessário para atividades legítimas voltadas à proteção do crédito, conforme a legislação aplicável.

7. Direitos dos Titulares dos Dados

A legislação brasileira vigente, especialmente a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), estabelece um conjunto de direitos assegurados aos titulares de dados pessoais, com o objetivo de garantir a proteção de suas informações e proporcionar maior controle sobre o uso de seus dados. Esses direitos são essenciais para promover a transparência nas relações e fortalecer a confiança entre os titulares e a Walter Lopes, bem como outras entidades que realizam o tratamento de dados pessoais.

Os principais direitos garantidos pela LGPD incluem:

Confirmação da Existência de Tratamento: O titular tem o direito de confirmar se seus dados pessoais estão sendo tratados pela Walter Lopes.

Acesso aos Dados: O titular pode solicitar acesso aos seus dados pessoais, incluindo informações sobre o tratamento realizado e a obtenção de cópias desses dados.

Correção de Dados Incompletos, Inexatos ou Desatualizados: Caso identifique inconsistências, o titular pode solicitar a correção ou complementação dos seus dados pessoais.

Anonimização, Bloqueio ou Eliminação de Dados Desnecessários, Excessivos ou Tratados em Desconformidade com a LGPD: Sempre que o tratamento não estiver de acordo com a legislação, o titular poderá requerer tais medidas.

Portabilidade dos Dados: Mediante requisição expressa, o titular poderá solicitar a portabilidade de seus dados a outro fornecedor de serviços ou produtos, respeitando a regulamentação da Autoridade Nacional e os segredos comercial e industrial.

Eliminação dos Dados Tratados com Base no Consentimento: O titular tem o direito de solicitar a eliminação dos dados tratados com base no consentimento, salvo quando houver outra base legal que justifique a manutenção do tratamento.

Informação sobre Compartilhamento de Dados: O titular pode solicitar informações acerca das entidades públicas ou privadas com as quais a Walter Lopes compartilhou seus dados pessoais.

Informação sobre a Possibilidade de Não Fornecer Consentimento e Consequências da Negativa: O titular deve ser informado sobre a opção de não fornecer consentimento e as consequências dessa escolha para o uso dos serviços.

Revogação do Consentimento: O titular poderá revogar o consentimento a qualquer momento, por meio de procedimento simples e gratuito. A Walter Lopes deverá eliminar os dados, salvo nos casos em que a legislação permita ou exija sua conservação.

A Walter Lopes compromete-se a disponibilizar os meios adequados e eficazes para que os titulares possam exercer plenamente esses direitos, conforme previsto na LGPD.

8. Compartilhamento de Dados com Terceiros

O compartilhamento de dados deve respeitar os princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Isso significa que qualquer compartilhamento de dados deve ter uma finalidade legítima, específica e informada ao titular, além de ser compatível com as finalidades originais para as quais os dados foram coletados.

Condições para o Compartilhamento de Dados

A LGPD estabelece que o compartilhamento de dados pessoais deve ocorrer em situações específicas e sob condições claras:

Com Consentimento do Titular: O compartilhamento pode ocorrer com o consentimento explícito do titular dos dados, que deve ser informado sobre com quem os dados serão compartilhados e para quais finalidades.

Sem Consentimento do Titular: Em certas condições, o compartilhamento pode ocorrer sem o consentimento do titular, como para o cumprimento de uma obrigação legal, para a execução de políticas públicas, para a realização de estudos por órgão de pesquisa, para a proteção da vida ou da incolumidade física do titular ou de terceiros, para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias, ou para a proteção do crédito.

Transparência e Direitos dos Titulares

A transparência é um pilar fundamental, exigindo que os titulares dos dados sejam informados sobre o compartilhamento de seus dados, incluindo as entidades com as quais os dados são compartilhados e os propósitos específicos do compartilhamento. Além disso, os titulares têm o direito de acessar informações sobre o compartilhamento de seus dados e podem exercer outros direitos previstos na LGPD, como a correção de dados incompletos, inexatos ou desatualizados.

Medidas de Segurança

As organizações envolvidas no compartilhamento de dados devem adotar medidas de segurança, técnicas e administrativas adequadas para proteger os dados pessoais de

acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Responsabilidade e Prestação de Contas

Organizações que tratam dados pessoais devem não apenas cumprir com as obrigações estabelecidas pela LGPD, mas também demonstrar a qualquer momento que estão fazendo isso, adotando práticas e políticas que assegurem a conformidade com a lei, incluindo no contexto de compartilhamento de dados.

Site

Nosso site utiliza cookies e tecnologias semelhantes para melhorar a experiência do usuário, personalizar conteúdo e anúncios, fornecer funcionalidades de redes sociais e analisar o tráfego em nosso site.

Cookies são pequenos arquivos de texto armazenados no dispositivo do usuário ao acessar determinadas páginas da internet. Eles são amplamente utilizados para garantir o funcionamento eficiente dos sites, bem como para fornecer informações aos proprietários das páginas.

Ao continuar a navegação em nosso site, o usuário concorda expressamente com o uso de cookies, conforme descrito nesta Política. O usuário poderá, a qualquer momento, configurar seu navegador para bloquear os cookies ou alertá-lo quando estiverem sendo enviados. No entanto, a desativação dos cookies poderá afetar a funcionalidade e a experiência de navegação no site.

Todos os dados coletados por meio de cookies serão tratados conforme as disposições da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), respeitando os princípios da finalidade, necessidade, transparência e segurança.

Quaisquer dados coletados no site poderão ser armazenados e tratados por prazo não superior a 05 (cinco) anos.

9. Segurança dos Dados

A segurança de dados é um aspecto crítico da gestão de informações na era digital, envolvendo a implementação de medidas técnicas, físicas e administrativas para proteger dados pessoais e corporativos contra acessos não autorizados, perdas, alterações indevidas, divulgação, destruição ou qualquer outra forma de tratamento inseguro.

Essas medidas incluem, mas não se limitam a criptografia, controle de acesso, avaliações de vulnerabilidade, treinamentos de conscientização em segurança para funcionários, backups regulares e planos de resposta a incidentes. A segurança de dados não apenas salvaguarda as informações importantes das organizações e indivíduos contra ameaças cibernéticas, mas também assegura a conformidade com regulamentações de proteção de dados, como a GDPR na União Europeia e a LGPD no Brasil, fortalecendo a confiança dos stakeholders e mantendo a integridade e a reputação das entidades envolvidas. Observar a POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

10. Violação de Dados

A LGPD enfatiza a importância da adoção de medidas preventivas, mas também reconhece que violações podem ocorrer e, quando isso acontece, é crucial ter um plano de resposta bem definido. Os procedimentos a serem seguidos incluem:

Detecção e Avaliação do Incidente: Imediatamente após a identificação de uma violação de dados, a Walter Lopes deve avaliar a extensão e a gravidade do incidente, determinando quais dados foram afetados e qual o potencial impacto para os titulares dos dados.

Contenção e Mitigação: Deve ser tomadas medidas imediatas para conter a violação e mitigar seus efeitos. Isso pode incluir a suspensão de sistemas específicos, a alteração de senhas ou o isolamento de partes da rede.

Notificação às Autoridades: A LGPD exige que a Autoridade Nacional de Proteção de Dados (ANPD) seja notificada em um prazo razoável, que, conforme a regulamentação, é de até 2 dias úteis, dependendo da gravidade do incidente e do risco ou dano aos titulares dos dados.

Comunicação aos Titulares dos Dados: Além de notificar a ANPD, a Walter Lopes deve comunicar o incidente de forma clara e adequada aos titulares dos dados afetados, especialmente se o incidente representar um risco elevado aos seus direitos e liberdades. A comunicação deve incluir informações sobre a natureza do incidente, os dados afetados, os possíveis impactos, as medidas que estão sendo tomadas para resolver a situação e como os titulares podem se proteger.

Documentação e Avaliação: Todo o processo de resposta ao incidente deve ser documentado, incluindo as decisões tomadas e as ações realizadas. Após a resolução do incidente, é recomendável realizar uma avaliação pós-incidente para identificar as causas, avaliar a eficácia das medidas de resposta e ajustar os planos de segurança e resposta a incidentes conforme necessário.

Melhoria Contínua: a Walter Lopes utilizará as lições aprendidas com o incidente para melhorar continuamente as políticas e práticas de segurança de dados, ajustando os controles de segurança para prevenir futuras violações.

Estabelecer e seguir esses procedimentos não apenas cumpre com as exigências da LGPD, mas também demonstra o compromisso Walter Lopes com a proteção de dados pessoais, contribuindo para a confiança do titular e o Compliance.

11. Transferências Internacionais de Dados

As Transferências Internacionais de Dados sob a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, são permitidas, mas estão sujeitas a condições específicas para assegurar que o nível de proteção de dados pessoais não seja comprometido quando estes são transferidos para fora do Brasil. A LGPD estabelece uma série de mecanismos e garantias que devem ser observados para que tais transferências sejam realizadas de forma legal e segura:

Adequação de Proteção de Dados: A transferência pode ocorrer para países ou organismos internacionais que proporcionem um grau de proteção de dados pessoais adequado ao previsto na LGPD. A Autoridade Nacional de Proteção de Dados (ANPD) é responsável por avaliar e declarar a adequação desses níveis de proteção.

Garantias Contratuais: Na ausência de uma decisão de adequação, a transferência internacional de dados pode ser realizada mediante a oferta de garantias suficientes

de proteção, por meio de cláusulas contratuais específicas para a situação, cláusulas-padrão contratuais, normas corporativas globais ou selos, certificados e códigos de conduta aprovados.

Consentimento Específico: A transferência pode ocorrer com o consentimento específico e destacado do titular dos dados, após ser informado sobre as condições internacionais da transferência, a natureza dos dados a serem transferidos, e os riscos envolvidos.

Cumprimento Legal e Proteção do Titular: A LGPD também permite a transferência de dados para a proteção do crédito, bem como para o cumprimento de obrigação legal ou regulatória pelo controlador, para a execução de políticas públicas ou atribuição legal do serviço público, para a realização de estudos por órgão de pesquisa, para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido deste, ou para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Cooperação Internacional: A transferência de dados pode ser necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e fiscalização, conforme os meios legais previstos em acordos internacionais.

A LGPD estabelece que qualquer transferência internacional de dados deve garantir que os dados pessoais estejam sujeitos a um regime de proteção compatível com a legislação brasileira. Além disso, a ANPD pode estabelecer normas complementares sobre as condições de transferência de dados, incluindo a verificação de requisitos específicos para determinados países ou setores. As organizações devem, portanto, avaliar cuidadosamente as condições sob as quais realizam transferências internacionais de dados, assegurando a conformidade com a LGPD e protegendo os direitos dos titulares dos dados.

12. Agentes de tratamento de dados

Os agentes de proteção de dados são categorizados principalmente em dois grupos: o controlador e o operador. Além disso, a figura do encarregado de proteção de dados (DPO - Data Protection Officer) também desempenha um papel crucial no ecossistema de proteção de dados. Cada um desses agentes tem responsabilidades específicas no tratamento de dados pessoais:

Controlador: É a pessoa natural ou jurídica, de direito público ou privado, que tem competências para tomar as decisões referentes ao tratamento de dados pessoais. O controlador é responsável por determinar as finalidades e os meios pelos quais os dados pessoais são processados. Isso inclui decidir sobre quais dados serão coletados, a finalidade da coleta e como os dados serão utilizados. O controlador tem a responsabilidade principal de garantir a conformidade com a LGPD, incluindo a proteção dos direitos dos titulares dos dados.

Operador: É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador atua sob as ordens do controlador, seguindo suas instruções para processar os dados pessoais para os fins determinados por aquele. Embora o operador não tome as decisões sobre os aspectos principais do tratamento de dados (como finalidade e meios), ele tem a responsabilidade de garantir a segurança dos dados durante o processamento e de seguir as diretrizes estabelecidas pelo controlador.

Encarregado de Proteção de Dados (Data Protection Officer - DPO): O DPO é a pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O DPO tem várias responsabilidades, incluindo o monitoramento da conformidade da organização com a LGPD, a orientação de funcionários e contratados acerca das práticas de proteção de dados, a realização de auditorias periódicas para assegurar a conformidade, e o atendimento às solicitações dos titulares dos dados e da ANPD. Embora a LGPD especifique situações em que a nomeação de um DPO é obrigatória, qualquer organização pode se beneficiar da nomeação de um DPO para gerenciar suas obrigações de proteção de dados.

Esses agentes desempenham papéis fundamentais no ecossistema de proteção de dados, trabalhando juntos para garantir que o tratamento de dados pessoais seja realizado de forma segura, transparente e conforme as disposições legais estabelecidas pela LGPD.

13. Treinamento e Conscientização

O treinamento e a conscientização sobre a política de proteção de dados são componentes essenciais para garantir a conformidade com leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil e outras regulamentações semelhantes ao redor do mundo. Essas atividades visam educar os colaboradores e stakeholders sobre a importância da proteção de dados, os princípios fundamentais da LGPD, os direitos dos titulares dos dados, e as responsabilidades dos agentes de tratamento (controladores e operadores). A seguir, detalhamos os aspectos cruciais desses processos de treinamento e conscientização:

Objetivos do Treinamento e Conscientização

Compreender a Importância da Proteção de Dados: Sensibilizar todos os envolvidos sobre a importância de proteger os dados pessoais, destacando as consequências legais, financeiras e de reputação em caso de não conformidade.

Conhecimento da Legislação: Proporcionar um entendimento claro da LGPD e de outras leis aplicáveis, incluindo os princípios de tratamento de dados, as categorias de dados protegidos, e as obrigações legais.

Práticas Seguras de Tratamento de Dados: Instruir sobre as melhores práticas e procedimentos seguros para o tratamento de dados, incluindo coleta, armazenamento, processamento e eliminação de dados pessoais.

Gestão de Incidentes: Ensinar como identificar, reportar e responder a incidentes de segurança de dados, incluindo violações de dados pessoais.

Estratégias de Implementação

Programas de Treinamento Personalizados: Desenvolver programas de treinamento que sejam relevantes para diferentes níveis da organização, desde a alta gestão até os operacionais, adaptando o conteúdo às suas funções específicas.

Uso de Diversos Métodos de Ensino: Aplicar uma variedade de métodos de ensino, como workshops, seminários, e-learning, vídeos educativos e quizzes para reforçar o aprendizado.

Material de Apoio: Disponibilizar manuais, políticas e procedimentos para que possam ser consultados a qualquer momento para esclarecer dúvidas sobre a proteção de dados.

Atualizações Regulares: Garantir que o treinamento seja atualizado regularmente para refletir quaisquer mudanças na legislação, na política interna de proteção de dados ou no ambiente tecnológico.

Avaliações e Feedback: Realizar avaliações periódicas para medir o entendimento e a aplicação dos conhecimentos adquiridos, além de coletar feedback para melhorar continuamente os programas de treinamento.

Criar uma cultura de proteção de dados na organização é fundamental. Isso não se limita a realizar treinamentos obrigatórios; envolve criar uma mentalidade onde a proteção de dados seja uma prioridade em todos os níveis. A conscientização contínua e o engajamento ativo dos colaboradores são cruciais para esse processo. A proteção de dados deve ser vista como um valor da empresa, e não apenas como uma obrigação legal.

Implementar um programa eficaz de treinamento e conscientização sobre a política de proteção de dados não apenas ajuda a minimizar os riscos de não conformidade e violações de dados, mas também reforça a confiança dos clientes e parceiros na capacidade da organização de proteger informações sensíveis.

14. Auditoria e Monitoramento

A auditoria em relação à LGPD envolve a revisão sistemática das práticas, políticas e procedimentos relacionados ao tratamento de dados pessoais dentro de uma organização. O objetivo é verificar a conformidade com a lei, identificar lacunas e riscos, e recomendar melhorias. Isso pode incluir, mas não se limita a:

- a. Avaliação da adequação das políticas de privacidade e proteção de dados.
- b. Verificação da existência e eficácia das medidas de segurança da informação.
- c. Análise da legalidade, transparência e finalidade na coleta e uso dos dados.
- d. Revisão dos processos de consentimento e das práticas de governança de dados.
- e. Exame dos contratos com operadores e parceiros terceirizados, assegurando que estes também estejam em conformidade.

O monitoramento contínuo é crucial para a detecção precoce de qualquer desvio ou não conformidade com a LGPD. Isso pode ser realizado por meio de sistemas automatizados e procedimentos regulares que incluem:

- a. Acompanhamento constante das operações de tratamento de dados para assegurar que sejam executadas conforme as políticas estabelecidas.
- b. Implementação de sistemas de gestão de incidentes para garantir respostas rápidas e eficazes a qualquer violação de dados.
- c. Realização de análises de risco e avaliações de impacto à proteção de dados (DPIA - Data Protection Impact Assessment) para novos projetos ou mudanças significativas nas operações.
- d. Monitoramento da eficácia das medidas técnicas e organizacionais de segurança de dados.

A auditoria e o monitoramento não são apenas requisitos legais, mas também práticas essenciais para a gestão de riscos, fortalecendo a confiança dos titulares dos dados e promovendo uma cultura de transparência e responsabilidade na proteção de dados pessoais.

15. Atualizações da Política

Revisão Anual: Realizar uma revisão anual como prática padrão, mesmo na ausência de mudanças significativas, para garantir que a política permaneça relevante e atualizada.

Após Mudanças Significativas nas Operações ou na Legislação: Sempre que houver mudanças significativas nas operações de negócios, nas tecnologias de processamento de dados, ou nas leis e regulamentações aplicáveis, é crucial revisar e, se necessário, atualizar a política de proteção de dados para refletir essas mudanças.

Em Resposta a Incidentes de Segurança: Após um incidente de segurança de dados, é importante revisar a política para identificar quaisquer lacunas ou deficiências que possam ter contribuído para o incidente e atualizá-la para prevenir futuras ocorrências.

16. Medidas Disciplinares

Advertência Verbal ou Escrita: Para infrações leves ou como primeira medida.

Suspensão: Temporária das atividades do colaborador, sem remuneração, como forma de penalidade por infrações mais graves.

Treinamento ou Reciclagem Obrigatórios: Para reforçar a importância das políticas de proteção de dados e evitar reincidências.

Demissão por Justa Causa: Para casos de descumprimento grave e intencional das políticas de proteção de dados, que coloquem em risco significativo a segurança das informações ou violem direitos de titulares de dados.

Ações Legais: A organização pode tomar medidas legais contra o colaborador, buscando reparação por danos causados à empresa devido ao descumprimento das políticas de proteção de dados.

17. Disposições gerais

Esta Política entra em vigor na data de sua publicação e deve ser respeitada por todos os que atuam em nome da Walter Lopes Engenharia.

Revisões periódicas poderão ser realizadas para assegurar sua atualização e relevância.

Alta Direção.

Tabela de Controle do Documento

Edição	Data	Redigido por	Revisado por	Data de atualização
1ª	26/06/2025	Aurora Barros	Maria Alice e Natasha	25/06/2026