Política de Proteção de Dados Pessoais - LGPD

1. NATUREZA DAS ALTERAÇÕES

Item	Natureza das alterações	Versão	Data	Elaborado por	Aprovação Final
01	Elaboração	1.0	18/07/2025	CISO Douglas Araújo	VP Fabiano Theis
02	Ajustes de Formatação	1.1	23/07/2025	Analsita Jules Alves	CISO Douglas Araújo
03	Revisão	1.2	23/07/2025	CISO Douglas Araújo	DPO Pedro Calejon

2. INTRODUÇÃO E OBJETIVO

A Servix Informática, empresa brasileira especializada em soluções tecnológicas para os setores público e privado, reconhece a importância fundamental da proteção de dados pessoais como direito fundamental dos cidadãos e pilar essencial para a construção de uma sociedade digital segura e confiável. Em um cenário onde a transformação digital acelera a coleta, o processamento e o compartilhamento de informações pessoais, nossa organização assume o compromisso irrevogável de proteger a privacidade e os dados de todos os indivíduos que confiam em nossos serviços.

Esta Política de Proteção de Dados Pessoais estabelece as diretrizes, princípios, procedimentos e responsabilidades que orientam todas as atividades de tratamento de dados pessoais realizadas pela Servix Informática, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, de 14 de agosto de 2018 [1], e demais normas aplicáveis à proteção de dados e privacidade no Brasil.

A Servix Informática atua como uma ponte tecnológica entre o setor público e privado, desenvolvendo e implementando soluções inovadoras que modernizam processos, otimizam recursos e melhoram a prestação de serviços à sociedade. Nossa expertise abrange desde sistemas de gestão pública até plataformas de e-commerce, sempre com foco na excelência técnica e na segurança da informação. Neste contexto, o tratamento de

dados pessoais é uma atividade inerente e essencial ao nosso modelo de negócio, exigindo um framework robusto de proteção que garanta a conformidade legal e a confiança dos nossos stakeholders.

O objetivo principal desta política é estabelecer um conjunto abrangente de normas e procedimentos que assegurem o tratamento adequado, seguro e transparente de dados pessoais em todas as operações da Servix Informática. Especificamente, esta política visa garantir o cumprimento integral dos princípios estabelecidos pela LGPD, incluindo finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização [2]. Além disso, busca-se estabelecer mecanismos eficazes para o exercício dos direitos dos titulares de dados, implementar medidas técnicas e organizacionais apropriadas para a proteção de dados, e criar uma cultura organizacional voltada à privacidade e proteção de dados.

Esta política aplica-se a todos os colaboradores, prestadores de serviços, parceiros e terceiros que, em nome da Servix Informática ou em colaboração com ela, realizem qualquer forma de tratamento de dados pessoais. A abrangência inclui todas as modalidades de trabalho adotadas pela empresa, sejam presenciais, remotas ou híbridas, reconhecendo os desafios específicos de cada ambiente e estabelecendo controles adequados para cada situação. A política também se estende a todas as relações contratuais e comerciais da empresa, incluindo contratos com clientes do setor público e privado, fornecedores, prestadores de serviços e demais parceiros de negócio.

O compromisso da Servix Informática com a proteção de dados pessoais transcende o mero cumprimento legal, representando um valor fundamental que permeia toda a organização. Reconhecemos que a confiança dos nossos clientes, colaboradores e da sociedade em geral é construída através de práticas transparentes, éticas e responsáveis no tratamento de dados pessoais. Por isso, esta política não apenas estabelece obrigações e responsabilidades, mas também promove uma cultura de privacidade que valoriza e protege os direitos fundamentais de cada indivíduo cujos dados são confiados aos nossos cuidados.

3. FUNDAMENTAÇÃO LEGAL

A presente Política de Proteção de Dados Pessoais da Servix Informática fundamenta-se em um sólido arcabouço jurídico nacional e internacional, que reconhece a proteção de dados pessoais como direito fundamental e estabelece obrigações específicas para organizações que realizam tratamento de dados pessoais. Esta fundamentação legal não apenas orienta a elaboração e implementação desta política, mas também assegura que todas as práticas da empresa estejam alinhadas com os mais altos padrões de proteção de dados e privacidade.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, constitui o principal marco regulatório para a proteção de dados pessoais no Brasil [1]. Esta lei, inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, estabelece um regime jurídico abrangente para o tratamento de dados pessoais por pessoas naturais ou jurídicas de direito público ou privado. A LGPD tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, criando um ambiente de maior segurança jurídica para titulares de dados e agentes de tratamento.

A Constituição Federal de 1988 fornece o fundamento constitucional para a proteção de dados pessoais, especialmente através do artigo 5º, inciso X, que estabelece como invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas [3]. Além disso, o inciso XII do mesmo artigo protege o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas. A Emenda Constitucional nº 115, de 2022, incluiu expressamente a proteção de dados pessoais entre os direitos fundamentais, consolidando sua importância no ordenamento jurídico brasileiro [4].

O Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, incluindo disposições específicas sobre a proteção da privacidade e dos dados pessoais [5]. Esta lei complementa a LGPD ao regular aspectos específicos do ambiente digital, como a neutralidade da rede, a guarda de registros de conexão e de acesso a aplicações de internet, e a responsabilidade civil de provedores de internet.

A Lei nº 13.853, de 8 de julho de 2019, que alterou a LGPD, criou a Autoridade Nacional de Proteção de Dados (ANPD) como órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional [6]. A ANPD possui competências regulamentares, fiscalizatórias e sancionatórias, sendo responsável por elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, e promover na população o conhecimento das normas e políticas públicas sobre proteção de dados pessoais.

No âmbito internacional, a Servix Informática reconhece e observa os princípios estabelecidos em tratados e convenções internacionais sobre direitos humanos e proteção de dados, incluindo a Declaração Universal dos Direitos Humanos, o Pacto Internacional sobre Direitos Civis e Políticos, e as Diretrizes da OCDE sobre Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais [7]. Estes instrumentos internacionais fornecem um framework global para a proteção da privacidade e orientam as melhores práticas adotadas pela empresa.

Para empresas que prestam serviços ao setor público, como é o caso da Servix Informática, aplicam-se também normas específicas da administração pública, incluindo a Lei de Acesso à Informação (Lei nº 12.527/2011), que estabelece procedimentos para garantir o acesso a informações públicas, e a Lei de Licitações e Contratos Administrativos (Lei nº 14.133/2021), que pode incluir cláusulas específicas sobre proteção de dados em contratos públicos [8].

A fundamentação legal desta política também considera normas técnicas e padrões internacionais de segurança da informação, como a família de normas ISO/IEC 27000, especialmente a ISO/IEC 27001 (Sistemas de Gestão da Segurança da Informação) e a ISO/IEC 27701 (Extensão da ISO/IEC 27001 e ISO/IEC 27002 para gestão da privacidade da informação) [9]. Estas normas fornecem diretrizes técnicas para a implementação de controles de segurança e privacidade que complementam os requisitos legais estabelecidos pela LGPD.

4. DEFINIÇÕES E CONCEITOS

Para a adequada compreensão e aplicação desta Política de Proteção de Dados Pessoais, é fundamental estabelecer definições claras e precisas dos termos técnicos e jurídicos utilizados. As definições apresentadas nesta seção baseiam-se primariamente na Lei Geral de Proteção de Dados Pessoais (LGPD) e em orientações da Autoridade Nacional de Proteção de Dados (ANPD), sendo complementadas por padrões internacionais e melhores práticas do setor.

Dados Pessoais são informações relacionadas a pessoa natural identificada ou identificável [1]. Uma pessoa natural é considerada identificável quando pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como nome, número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural. Na prática da Servix Informática, dados pessoais incluem, mas não se limitam a: nomes completos, números de documentos (CPF, RG, CNH), endereços residenciais e comerciais, números de telefone, endereços de e-mail, dados bancários, informações profissionais, dados de localização, endereços IP, cookies e outros identificadores digitais.

Dados Pessoais Sensíveis constituem uma categoria especial de dados pessoais que merecem proteção reforçada devido ao seu potencial de causar discriminação ou danos aos titulares [1]. Segundo a LGPD, são considerados sensíveis os dados pessoais sobre 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. O tratamento de dados sensíveis exige bases legais específicas e medidas de segurança reforçadas, sendo geralmente necessário o consentimento específico do titular ou outra base legal expressamente prevista em lei.

Dados Anonimizados são dados relativos a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento [1]. O processo de anonimização deve ser irreversível, ou seja, não deve ser

possível, por meios razoáveis, reverter o processo e identificar o titular dos dados. Dados efetivamente anonimizados não se enquadram no conceito de dados pessoais e, portanto, não estão sujeitos às disposições da LGPD. A Servix Informática utiliza técnicas de anonimização para análises estatísticas, desenvolvimento de produtos e pesquisas, sempre observando as melhores práticas técnicas para garantir a irreversibilidade do processo.

Titular dos Dados é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento [1]. Na operação da Servix Informática, os titulares incluem clientes pessoas físicas, colaboradores, prestadores de serviços pessoas físicas, usuários de sistemas e aplicações desenvolvidas pela empresa, beneficiários de serviços públicos atendidos através de soluções da empresa, e qualquer outra pessoa natural cujos dados sejam tratados pela organização. O titular é o sujeito de direitos estabelecidos pela LGPD e possui prerrogativas específicas em relação aos seus dados pessoais.

Controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais [1]. O controlador determina as finalidades e os meios do tratamento de dados pessoais, sendo responsável por garantir a conformidade com a LGPD e por implementar medidas técnicas e organizacionais adequadas para proteger os dados pessoais. A Servix Informática atua como controladora em relação aos dados de seus colaboradores, clientes diretos e usuários de seus sistemas proprietários. Em contratos com clientes, especialmente do setor público, a empresa pode atuar como controladora, operadora ou controladora conjunta, dependendo das especificidades de cada relação contratual.

Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador [1]. O operador deve seguir estritamente as instruções do controlador e implementar medidas técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais. A Servix Informática atua como operadora quando presta serviços de processamento de dados para clientes que mantêm o controle sobre as finalidades e meios do tratamento, situação comum em contratos de desenvolvimento e manutenção de sistemas para órgãos públicos.

Encarregado pelo Tratamento de Dados Pessoais (DPO - Data Protection Officer) é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) [1]. O encarregado deve ter conhecimento técnico e jurídico adequado para o desempenho de suas funções, que incluem aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, receber comunicações da autoridade nacional e adotar providências, orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Tratamento é toda operação realizada com dados pessoais, como as que se referem 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 [1]. Esta definição abrangente engloba qualquer atividade que envolva dados pessoais, desde a coleta inicial até a eliminação final, passando por todas as etapas intermediárias de processamento, análise e compartilhamento.

Consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada [1]. O consentimento deve ser específico para cada finalidade de tratamento, não sendo válidas autorizações genéricas. Deve ser dado de forma livre, sem vícios de vontade, e de maneira informada, com o titular tendo conhecimento claro sobre o que está consentindo. O consentimento pode ser revogado a qualquer momento pelo titular, devendo o controlador facilitar este processo.

Anonimização é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo [1]. O processo de anonimização deve considerar fatores como custo e tempo necessários para reverter o processo de anonimização, utilizando os meios técnicos disponíveis, e a utilização exclusiva de meios próprios ou disponibilização de meios a terceiros.

Pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro [1]. Diferentemente da anonimização, a pseudonimização é um processo reversível, mantendo-se a possibilidade de reidentificação através de informações adicionais controladas.

Uso Compartilhado de Dados é a comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados [1]. Para a Servix Informática, que atende tanto o setor público quanto privado, o uso compartilhado de dados é uma atividade relevante que exige controles específicos e bases legais adequadas.

Transferência Internacional de Dados é a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro [1]. A LGPD estabelece requisitos específicos para transferências internacionais, incluindo a necessidade de que o país de destino proporcione grau de proteção de dados pessoais adequado ao previsto na lei brasileira, ou que sejam oferecidas garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados.

Autoridade Nacional de Proteção de Dados (ANPD) é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional [6]. A ANPD possui competências regulamentares, orientativas, fiscalizatórias e sancionatórias, sendo a principal autoridade de supervisão da proteção de dados pessoais no Brasil.

Estas definições constituem a base conceitual para a compreensão e aplicação desta política, devendo ser observadas por todos os colaboradores, prestadores de serviços e

parceiros da Servix Informática em suas atividades relacionadas ao tratamento de dados pessoais.

5. PRINCÍPIOS DA PROTEÇÃO DE DADOS

A Servix Informática fundamenta todas as suas atividades de tratamento de dados pessoais nos princípios estabelecidos pela Lei Geral de Proteção de Dados Pessoais, que constituem diretrizes fundamentais para garantir o respeito aos direitos dos titulares e a conformidade legal de todas as operações. Estes princípios não são meramente conceitos abstratos, mas orientações práticas que permeiam cada decisão, processo e procedimento relacionado ao tratamento de dados pessoais na organização.

O **Princípio da Finalidade** estabelece que o tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades [2]. Na Servix Informática, este princípio se materializa através da definição clara e documentada de todas as finalidades de tratamento antes do início de qualquer atividade de processamento de dados. Cada projeto, sistema ou processo que envolva dados pessoais deve ter suas finalidades explicitamente definidas, comunicadas aos titulares de forma transparente e limitadas ao escopo necessário para atingir os objetivos legítimos da empresa. A empresa mantém um registro detalhado de todas as finalidades de tratamento, assegurando que não haja desvio de propósito ou utilização de dados para fins incompatíveis com aqueles originalmente declarados.

O **Princípio da Adequação** exige que o tratamento seja compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento [2]. Este princípio orienta a Servix Informática a avaliar constantemente se os métodos, tecnologias e procedimentos utilizados no tratamento de dados são apropriados e proporcionais às finalidades declaradas. Por exemplo, se a finalidade é o envio de comunicações comerciais, o tratamento deve se limitar aos dados necessários para essa comunicação, utilizando meios adequados e seguros. A empresa implementa revisões periódicas para verificar se os tratamentos permanecem adequados às finalidades, especialmente quando há mudanças tecnológicas, organizacionais ou regulamentares que possam afetar essa adequação.

O **Princípio da Necessidade** determina a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento [2]. A Servix Informática aplica este princípio através da implementação de práticas de minimização de dados, coletando e processando apenas as informações estritamente necessárias para atingir as finalidades declaradas. Isso inclui a avaliação regular dos dados coletados, a eliminação de campos desnecessários em formulários, a implementação de controles de acesso baseados no princípio do menor privilégio, e a revisão periódica dos dados armazenados para identificar e eliminar informações que não sejam mais necessárias.

O **Princípio do Livre Acesso** garante aos titulares consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais [2]. A Servix Informática implementa este princípio através de canais de comunicação acessíveis e eficientes, permitindo que os titulares exerçam seus direitos de forma simples e sem custos. A empresa mantém sistemas e procedimentos que permitem o atendimento rápido e preciso às solicitações de acesso, fornecendo informações claras sobre como os dados são tratados, por quanto tempo são mantidos, e quais são os direitos dos titulares. Além disso, a empresa disponibiliza informações proativas sobre suas práticas de tratamento de dados através de avisos de privacidade claros e acessíveis.

O **Princípio da Qualidade dos Dados** assegura aos titulares a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento [2]. A Servix Informática implementa controles rigorosos de qualidade de dados, incluindo validações automáticas durante a coleta, procedimentos de verificação e atualização periódica, e mecanismos para correção de dados incorretos ou desatualizados. A empresa também facilita aos titulares a correção de seus dados pessoais, mantendo processos eficientes para atualização e retificação de informações. Sistemas de monitoramento contínuo identificam inconsistências e problemas de qualidade, garantindo que os dados utilizados sejam sempre precisos e atualizados.

O **Princípio da Transparência** garante aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de

tratamento, observados os segredos comercial e industrial [2]. A Servix Informática promove a transparência através de avisos de privacidade detalhados, comunicações claras sobre práticas de tratamento de dados, e canais de comunicação diretos com o Encarregado de Proteção de Dados. A empresa publica informações sobre suas práticas de proteção de dados em seu website, fornece relatórios de transparência quando aplicável, e mantém documentação acessível sobre suas políticas e procedimentos de proteção de dados. A transparência também se estende às relações contratuais, com cláusulas claras sobre tratamento de dados em todos os contratos relevantes.

O **Princípio da Segurança** exige a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão [2]. A Servix Informática implementa um programa abrangente de segurança da informação que inclui controles técnicos como criptografia, controles de acesso, monitoramento de segurança, backup e recuperação de dados, e controles administrativos como políticas de segurança, treinamento de colaboradores, gestão de incidentes e auditoria regular. A empresa adota padrões internacionais de segurança da informação, como a família ISO 27000, e mantém certificações relevantes para demonstrar seu compromisso com a segurança dos dados.

O **Princípio da Prevenção** determina a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais [2]. A Servix Informática implementa uma abordagem proativa de gestão de riscos, incluindo avaliações regulares de impacto à proteção de dados, implementação de controles preventivos, monitoramento contínuo de ameaças e vulnerabilidades, e planos de contingência para resposta a incidentes. A empresa mantém programas de conscientização e treinamento para prevenir violações de dados causadas por erro humano, e implementa tecnologias de proteção de dados para detectar e prevenir vazamentos acidentais ou maliciosos.

O **Princípio da Não Discriminação** proíbe a realização do tratamento para fins discriminatórios ilícitos ou abusivos [2]. A Servix Informática compromete-se a não utilizar dados pessoais para práticas discriminatórias, implementando controles específicos em sistemas de tomada de decisão automatizada, promovendo a diversidade e inclusão em suas práticas de negócio, e mantendo políticas claras contra discriminação. A empresa

também monitora seus algoritmos e sistemas automatizados para identificar e corrigir possíveis vieses discriminatórios, especialmente em sistemas que possam afetar oportunidades de emprego, acesso a serviços ou outros direitos fundamentais.

O **Princípio da Responsabilização e Prestação de Contas** exige a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas [2]. A Servix Informática implementa este princípio através da manutenção de documentação abrangente sobre suas práticas de proteção de dados, realização de auditorias regulares, implementação de métricas e indicadores de conformidade, e preparação de relatórios periódicos sobre o cumprimento da LGPD. A empresa também mantém registros detalhados de todas as atividades de tratamento, implementa programas de treinamento e conscientização, e estabelece responsabilidades claras para todos os colaboradores envolvidos no tratamento de dados pessoais.

6. BASES LEGAIS PARA TRATAMENTO

O tratamento de dados pessoais pela Servix Informática fundamenta-se exclusivamente nas bases legais estabelecidas pela Lei Geral de Proteção de Dados Pessoais, que constituem os fundamentos jurídicos que legitimam e autorizam o processamento de informações pessoais. A identificação e aplicação correta da base legal apropriada é fundamental para garantir a legalidade do tratamento e proteger os direitos dos titulares de dados. A empresa mantém documentação detalhada sobre a base legal aplicável a cada atividade de tratamento, assegurando transparência e conformidade legal em todas as suas operações.

O **Consentimento** representa uma das bases legais mais importantes e amplamente utilizadas, caracterizando-se como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada [1]. Na Servix Informática, o consentimento é obtido de forma específica para cada finalidade de tratamento, utilizando linguagem clara e acessível que permita ao titular compreender exatamente para que seus dados serão utilizados. A empresa implementa mecanismos técnicos e organizacionais para facilitar a obtenção, registro e gestão do

consentimento, incluindo sistemas que permitem aos titulares visualizar, modificar ou revogar seus consentimentos a qualquer momento. O consentimento é documentado de forma que seja possível comprovar quando, como e para que finalidade foi obtido, e a empresa mantém registros que demonstram a validade e especificidade de cada consentimento coletado.

Para dados pessoais sensíveis, a Servix Informática reconhece que o consentimento deve ser específico e destacado, para finalidades específicas, exigindo maior rigor na obtenção e documentação. A empresa implementa controles adicionais para o tratamento de dados sensíveis, incluindo medidas de segurança reforçadas, limitação de acesso a pessoal autorizado, e procedimentos específicos para obtenção de consentimento específico quando esta for a base legal aplicável.

O **Cumprimento de Obrigação Legal ou Regulatória** constitui base legal fundamental para muitas atividades da Servix Informática, especialmente considerando sua atuação junto ao setor público [1]. Esta base legal aplica-se quando o tratamento é necessário para cumprir obrigações estabelecidas em leis, regulamentos, normas ou determinações de autoridades competentes. Exemplos incluem o cumprimento de obrigações trabalhistas e previdenciárias em relação aos dados de colaboradores, atendimento a requisições de autoridades fiscais, cumprimento de normas de auditoria e compliance, e observância de regulamentações específicas do setor de tecnologia da informação. A empresa mantém um mapeamento atualizado de todas as obrigações legais que exigem tratamento de dados pessoais, assegurando que o processamento seja limitado ao estritamente necessário para o cumprimento da obrigação específica.

A **Execução de Políticas Públicas** representa uma base legal especialmente relevante para a Servix Informática, considerando sua significativa atuação no desenvolvimento e implementação de soluções tecnológicas para o setor público [1]. Esta base legal permite o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. A empresa atua frequentemente como operadora de dados para órgãos públicos, processando informações de cidadãos para viabilizar a prestação de serviços públicos digitais, implementação de sistemas de gestão pública, e modernização de

processos administrativos. Nestes casos, o tratamento deve observar rigorosamente as finalidades específicas da política pública, os limites estabelecidos em contratos e convênios, e as diretrizes de transparência e accountability exigidas para o setor público.

A **Realização de Estudos por Órgão de Pesquisa** constitui base legal aplicável quando a Servix Informática desenvolve projetos de pesquisa e desenvolvimento, especialmente em parceria com instituições acadêmicas ou órgãos de pesquisa [1]. Esta base legal exige que, sempre que possível, os dados sejam anonimizados, e que o tratamento seja limitado ao estritamente necessário para a realização da pesquisa. A empresa implementa protocolos específicos para projetos de pesquisa, incluindo avaliação ética, medidas de proteção reforçadas, e procedimentos para anonimização ou pseudonimização de dados quando tecnicamente viável.

A **Execução de Contrato** representa uma base legal fundamental para as atividades comerciais da Servix Informática, aplicando-se quando o tratamento é necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular [1]. Esta base legal abrange o tratamento de dados de clientes para prestação de serviços contratados, processamento de dados de fornecedores para execução de contratos de aquisição, e tratamento de dados de colaboradores para cumprimento de contratos de trabalho. A empresa assegura que o tratamento baseado nesta base legal seja limitado ao necessário para o cumprimento das obrigações contratuais específicas, mantendo documentação que demonstre a relação direta entre o tratamento e a execução contratual.

O **Exercício Regular de Direitos** em processo judicial, administrativo ou arbitral constitui base legal aplicável quando a Servix Informática precisa tratar dados pessoais para defender seus direitos ou cumprir obrigações em procedimentos legais [1]. Esta base legal abrange a defesa em processos judiciais, participação em procedimentos administrativos, cumprimento de determinações judiciais, e exercício do direito de defesa. A empresa implementa controles específicos para assegurar que o tratamento seja limitado ao estritamente necessário para o exercício do direito específico, mantendo a confidencialidade e segurança dos dados durante todo o processo.

A **Proteção da Vida ou da Incolumidade Física** do titular ou de terceiro representa uma base legal de caráter emergencial, aplicável em situações excepcionais onde o tratamento de dados é necessário para proteger interesses vitais [1]. Embora seja uma base legal de aplicação limitada na operação regular da Servix Informática, a empresa mantém procedimentos para situações de emergência que possam exigir o tratamento de dados com base nesta fundamentação legal.

A **Tutela da Saúde** constitui base legal específica para tratamento de dados relacionados à saúde, aplicável exclusivamente em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária [1]. Esta base legal pode ser relevante para a Servix Informática quando desenvolve soluções para o setor de saúde pública ou privada, exigindo controles específicos e medidas de segurança reforçadas para dados de saúde.

O **Interesse Legítimo** do controlador ou de terceiro constitui uma base legal flexível, mas que exige cuidadosa avaliação para assegurar que não prevaleçam direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais [1]. A Servix Informática utiliza esta base legal após realizar teste de balanceamento que considera a necessidade do tratamento, o impacto sobre os titulares, e a existência de medidas de proteção adequadas. Exemplos de interesse legítimo incluem segurança da informação, prevenção de fraudes, marketing direto para clientes existentes, e melhoria de produtos e serviços. A empresa documenta cuidadosamente a avaliação de interesse legítimo, demonstrando que o tratamento é necessário, proporcional e que foram implementadas medidas adequadas para proteger os direitos dos titulares.

A **Proteção do Crédito** representa base legal específica para atividades relacionadas à análise de crédito e prevenção de inadimplência [1]. Embora não seja uma atividade principal da Servix Informática, esta base legal pode ser aplicável em situações específicas relacionadas à gestão de relacionamentos comerciais e avaliação de riscos contratuais.

A seleção e aplicação da base legal apropriada é uma decisão fundamental que deve ser tomada antes do início de qualquer atividade de tratamento de dados pessoais. A Servix Informática mantém procedimentos específicos para avaliação e documentação da base legal aplicável, assegurando que todos os tratamentos sejam fundamentados

adequadamente e que os direitos dos titulares sejam respeitados em conformidade com cada base legal específica.

7. DIREITOS DOS TITULARES

A Servix Informática reconhece e garante o exercício pleno de todos os direitos estabelecidos pela Lei Geral de Proteção de Dados Pessoais aos titulares de dados pessoais, implementando mecanismos eficazes, acessíveis e gratuitos para que esses direitos possam ser exercidos de forma simples e efetiva. O respeito aos direitos dos titulares constitui um pilar fundamental da cultura de proteção de dados da empresa, refletindo seu compromisso com a transparência, a responsabilidade e o respeito à dignidade humana.

O **Direito de Confirmação da Existência de Tratamento** garante ao titular o direito de obter confirmação sobre se a Servix Informática realiza tratamento de seus dados pessoais [1]. Este direito fundamental permite que os indivíduos tenham conhecimento sobre se suas informações pessoais estão sendo processadas pela empresa, constituindo o primeiro passo para o exercício de outros direitos. A Servix Informática implementa procedimentos específicos para atender a essas solicitações de forma imediata e gratuita, fornecendo confirmação clara e objetiva sobre a existência ou não de tratamento. Quando há tratamento de dados, a empresa fornece informações básicas sobre as finalidades e a natureza dos dados tratados, direcionando o titular para canais específicos onde pode obter informações mais detalhadas.

O **Direito de Acesso aos Dados** permite ao titular obter acesso aos seus dados pessoais que estão sendo tratados pela Servix Informática, incluindo informações sobre as finalidades do tratamento, as categorias de dados tratados, a origem dos dados, a existência de decisões automatizadas, e os critérios utilizados [1]. A empresa implementa sistemas e procedimentos que permitem fornecer essas informações de forma clara, completa e acessível, utilizando linguagem simples e evitando termos técnicos desnecessários. O acesso é fornecido em formato eletrônico, seguro e de fácil compreensão, permitindo que o titular visualize e compreenda como seus dados estão sendo utilizados. A Servix Informática mantém sistemas que permitem a extração eficiente

dos dados pessoais de um titular específico, assegurando que as informações fornecidas sejam precisas e atualizadas.

O **Direito de Correção de Dados Incompletos, Inexatos ou Desatualizados** garante ao titular a possibilidade de solicitar a retificação de dados pessoais que estejam incorretos, incompletos ou desatualizados [1]. A Servix Informática implementa procedimentos eficientes para receber, avaliar e processar solicitações de correção, incluindo mecanismos de verificação da identidade do solicitante e validação das correções solicitadas. A empresa mantém sistemas que permitem a atualização rápida e precisa dos dados em todas as bases e sistemas onde estejam armazenados, assegurando a consistência das informações. Quando a correção afeta dados que foram compartilhados com terceiros, a empresa notifica esses terceiros sobre as alterações realizadas, garantindo que as correções sejam propagadas adequadamente.

O **Direito de Anonimização, Bloqueio ou Eliminação** permite ao titular solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD [1]. A Servix Informática avalia cuidadosamente cada solicitação, considerando as bases legais aplicáveis, os períodos de retenção estabelecidos, e as obrigações legais de conservação de dados. Quando procedente, a empresa implementa as medidas solicitadas de forma técnica e segura, assegurando que a anonimização seja irreversível, que o bloqueio impeça efetivamente o acesso aos dados, ou que a eliminação seja completa e definitiva. A empresa mantém registros das ações realizadas para demonstrar o cumprimento das solicitações dos titulares.

O **Direito de Portabilidade dos Dados** garante ao titular o direito de obter seus dados pessoais em formato estruturado, de uso comum e legível por máquina, e de transmitir esses dados a outro controlador [1]. A Servix Informática implementa mecanismos técnicos que permitem a exportação de dados pessoais em formatos padronizados e interoperáveis, facilitando a transferência para outros prestadores de serviços quando solicitado pelo titular. Este direito aplica-se especificamente aos dados fornecidos pelo titular ou coletados com base no consentimento ou para execução de contrato, observando-se os segredos comercial e industrial. A empresa desenvolve interfaces e procedimentos que tornam o exercício deste direito simples e eficiente, respeitando os prazos estabelecidos pela LGPD.

O **Direito de Eliminação dos Dados Pessoais** permite ao titular solicitar a exclusão definitiva de seus dados pessoais quando o tratamento não for mais necessário para as finalidades para as quais foram coletados, quando o consentimento for revogado, ou quando o tratamento estiver sendo realizado em desconformidade com a LGPD [1]. A Servix Informática implementa procedimentos técnicos e organizacionais para a eliminação segura e definitiva de dados pessoais, assegurando que a exclusão seja completa e irreversível. A empresa considera cuidadosamente as obrigações legais de retenção de dados antes de proceder à eliminação, mantendo apenas os dados estritamente necessários para o cumprimento de obrigações legais específicas.

O **Direito de Informação sobre Compartilhamento** garante ao titular o conhecimento sobre as entidades públicas e privadas com as quais a Servix Informática realizou uso compartilhado de dados [1]. A empresa mantém registros detalhados de todos os compartilhamentos de dados realizados, incluindo a identificação dos destinatários, as finalidades do compartilhamento, as bases legais aplicáveis, e as medidas de proteção implementadas. Essas informações são disponibilizadas aos titulares de forma clara e acessível, permitindo que compreendam o fluxo de seus dados pessoais e exerçam seus direitos junto a outros controladores quando aplicável.

O **Direito de Informação sobre Consequências da Negativa** assegura ao titular o conhecimento sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa [1]. A Servix Informática fornece informações claras e específicas sobre quais serviços ou funcionalidades podem ser afetados caso o titular opte por não fornecer determinados dados pessoais ou não conceder consentimento para finalidades específicas. Essas informações são apresentadas de forma transparente e compreensível, permitindo que o titular tome decisões informadas sobre o fornecimento de seus dados pessoais.

O **Direito de Revogação do Consentimento** permite ao titular retirar seu consentimento a qualquer momento, de forma gratuita e facilitada [1]. A Servix Informática implementa mecanismos técnicos e organizacionais que tornam a revogação do consentimento tão simples quanto sua concessão, utilizando interfaces intuitivas e processos eficientes. A

empresa assegura que a revogação seja processada imediatamente, cessando o tratamento baseado no consentimento revogado, exceto quando houver outra base legal aplicável. Os titulares são informados sobre as consequências da revogação do consentimento, incluindo possíveis impactos na prestação de serviços.

Procedimentos para Exercício dos Direitos: A Servix Informática estabelece canais específicos e acessíveis para o exercício dos direitos dos titulares, incluindo formulários online, endereço de e-mail dedicado, e contato direto com o Encarregado de Proteção de Dados. A empresa implementa procedimentos padronizados para recebimento, análise e resposta às solicitações dos titulares, assegurando que todas as solicitações sejam tratadas de forma consistente, eficiente e em conformidade com os prazos estabelecidos pela LGPD.

As solicitações são atendidas gratuitamente, e a empresa pode solicitar informações adicionais apenas quando necessário para confirmar a identidade do titular ou esclarecer a natureza da solicitação. A Servix Informática mantém registros de todas as solicitações recebidas e das ações tomadas, demonstrando seu compromisso com a transparência e a responsabilização. Quando uma solicitação não puder ser atendida integralmente, a empresa fornece explicações claras sobre os motivos, orientando o titular sobre alternativas disponíveis ou recursos cabíveis.

8. GOVERNANÇA E RESPONSABILIDADES

A Servix Informática estabelece uma estrutura de governança robusta e abrangente para a proteção de dados pessoais, definindo claramente as responsabilidades, autoridades e mecanismos de supervisão necessários para assegurar o cumprimento integral da Lei Geral de Proteção de Dados Pessoais e a proteção efetiva dos direitos dos titulares. Esta estrutura de governança permeia todos os níveis organizacionais, desde a alta direção até os colaboradores operacionais, criando uma cultura de responsabilidade compartilhada e comprometimento com a proteção de dados.

Estrutura Organizacional: A governança de proteção de dados da Servix Informática é estruturada em múltiplas camadas, cada uma com responsabilidades específicas e

complementares. No nível estratégico, a Diretoria Executiva assume a responsabilidade final pela proteção de dados pessoais, definindo políticas gerais, aprovando investimentos em segurança e privacidade, e assegurando que a proteção de dados seja considerada em todas as decisões estratégicas da empresa. A diretoria também é responsável por nomear o Encarregado de Proteção de Dados e garantir que este tenha a autonomia e os recursos necessários para desempenhar suas funções efetivamente.

No nível tático, o Comitê de Proteção de Dados, composto por representantes de diferentes áreas da empresa, incluindo jurídico, tecnologia da informação, recursos humanos, comercial e operações, coordena a implementação das políticas de proteção de dados e monitora o cumprimento das obrigações legais. Este comitê reúne-se regularmente para avaliar riscos, revisar incidentes, aprovar novos procedimentos, e assegurar que as práticas de proteção de dados sejam consistentes em toda a organização.

No nível operacional, cada área de negócio possui responsabilidades específicas relacionadas à proteção de dados em suas atividades, com gestores designados como pontos focais para questões de privacidade e proteção de dados. Estes gestores são responsáveis por implementar as políticas e procedimentos em suas respectivas áreas, treinar suas equipes, e reportar questões e incidentes ao Comitê de Proteção de Dados.

Responsabilidades do Controlador: Como controladora de dados pessoais, a Servix Informática assume responsabilidades abrangentes que incluem a determinação das finalidades e meios do tratamento de dados pessoais, a implementação de medidas técnicas e organizacionais adequadas para proteger os dados, e a demonstração de conformidade com a LGPD [1]. A empresa é responsável por realizar avaliações de impacto à proteção de dados quando o tratamento puder resultar em alto risco aos direitos e liberdades dos titulares, implementar medidas de segurança apropriadas ao risco, e manter registros detalhados de todas as atividades de tratamento.

A Servix Informática também é responsável por garantir que todos os operadores que processam dados pessoais em seu nome implementem medidas adequadas de proteção, fornecendo instruções claras e específicas sobre o tratamento, monitorando o cumprimento dessas instruções, e assegurando que os contratos com operadores incluam cláusulas

adequadas de proteção de dados. A empresa mantém um programa de due diligence para avaliar e selecionar operadores, considerando suas capacidades técnicas, medidas de segurança, e histórico de conformidade com normas de proteção de dados.

Responsabilidades do Operador: Quando atua como operadora de dados pessoais, especialmente em contratos com clientes do setor público, a Servix Informática assume responsabilidades específicas que incluem o tratamento de dados pessoais apenas conforme instruções documentadas do controlador, a implementação de medidas técnicas e organizacionais adequadas para proteger os dados, e a assistência ao controlador no cumprimento de suas obrigações [1]. A empresa assegura que todos os colaboradores autorizados a processar dados pessoais estejam sujeitos a obrigações de confidencialidade, implementa medidas para garantir a segurança do tratamento, e notifica o controlador sobre qualquer violação de dados pessoais sem demora injustificada.

Como operadora, a Servix Informática também auxilia o controlador na resposta às solicitações dos titulares de dados, fornece informações necessárias para demonstrar conformidade com a LGPD, e retorna ou elimina os dados pessoais após o término da prestação de serviços, conforme instruções do controlador. A empresa mantém registros detalhados de todas as atividades de tratamento realizadas em nome de controladores, permitindo a demonstração de conformidade e a prestação de contas adequada.

Papel do Encarregado (DPO): O Encarregado de Proteção de Dados da Servix Informática desempenha um papel central na governança de proteção de dados, atuando como ponto focal para questões de privacidade e proteção de dados tanto internamente quanto nas relações com titulares de dados e autoridades de supervisão [1]. O Encarregado possui autonomia para desempenhar suas funções, reportando-se diretamente à alta direção e tendo acesso a todos os recursos necessários para cumprir suas responsabilidades.

As responsabilidades do Encarregado incluem aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências adequadas, receber comunicações da Autoridade Nacional de Proteção de Dados e adotar as providências necessárias, orientar funcionários e contratados sobre práticas de proteção de dados, e executar demais

atribuições determinadas pelo controlador ou estabelecidas em normas complementares. O Encarregado também coordena a resposta a incidentes de segurança, supervisiona a realização de avaliações de impacto à proteção de dados, e mantém relacionamento com autoridades de supervisão e outras partes interessadas.

Comitê de Proteção de Dados: O Comitê de Proteção de Dados da Servix Informática é um órgão multidisciplinar responsável por coordenar e supervisionar a implementação das políticas de proteção de dados em toda a organização. O comitê é composto por representantes seniores de diferentes áreas, incluindo o Encarregado de Proteção de Dados, representantes das áreas jurídica, de tecnologia da informação, de recursos humanos, comercial e de operações. O comitê reúne-se mensalmente ou conforme necessário para avaliar questões relacionadas à proteção de dados, revisar e aprovar políticas e procedimentos, analisar incidentes e não conformidades, e coordenar ações de melhoria.

As responsabilidades do Comitê incluem a aprovação de políticas e procedimentos relacionados à proteção de dados, a avaliação e aprovação de novos projetos que envolvam tratamento de dados pessoais, a supervisão da implementação de medidas de segurança e privacidade, a coordenação da resposta a incidentes de segurança, e a supervisão do programa de treinamento e conscientização em proteção de dados. O Comitê também é responsável por monitorar indicadores de conformidade, avaliar a eficácia das medidas implementadas, e reportar à alta direção sobre o status da conformidade com a LGPD.

Responsabilidades dos Colaboradores: Todos os colaboradores da Servix Informática, independentemente de sua função ou nível hierárquico, possuem responsabilidades específicas relacionadas à proteção de dados pessoais. Estas responsabilidades incluem o cumprimento de todas as políticas e procedimentos de proteção de dados, a participação em treinamentos obrigatórios, a notificação imediata de incidentes de segurança ou violações de dados, e a manutenção da confidencialidade de dados pessoais a que tenham acesso no exercício de suas funções.

Os colaboradores são responsáveis por tratar dados pessoais apenas conforme autorizado e necessário para o desempenho de suas funções, implementar medidas de segurança adequadas em suas atividades, e cooperar com auditorias e avaliações de conformidade. Colaboradores que ocupam posições de liderança possuem responsabilidades adicionais, incluindo a supervisão do cumprimento das políticas de proteção de dados por suas equipes, a implementação de controles adequados em seus processos, e a promoção de uma cultura de proteção de dados em suas áreas de responsabilidade.

A Servix Informática implementa um programa abrangente de responsabilização que inclui a definição clara de responsabilidades, a implementação de controles de supervisão, a realização de avaliações regulares de desempenho em relação à proteção de dados, e a aplicação de medidas disciplinares quando necessário. A empresa também reconhece e recompensa boas práticas de proteção de dados, promovendo uma cultura positiva de privacidade e segurança da informação.

9. TRATAMENTO DE DADOS NA SERVIX INFORMÁTICA

A Servix Informática realiza diversas modalidades de tratamento de dados pessoais em suas operações, cada uma com características específicas, finalidades distintas e bases legais apropriadas. O mapeamento detalhado e a documentação de todas as atividades de tratamento constituem elementos fundamentais para assegurar a conformidade com a LGPD e a proteção adequada dos direitos dos titulares. A empresa mantém um inventário abrangente de todas as atividades de tratamento, incluindo descrições detalhadas das finalidades, categorias de dados, bases legais, medidas de segurança e períodos de retenção aplicáveis.

Dados de Clientes do Setor Público: O tratamento de dados pessoais de cidadãos através de sistemas desenvolvidos e mantidos para órgãos públicos constitui uma das principais atividades da Servix Informática. Nestes casos, a empresa geralmente atua como operadora de dados, processando informações pessoais conforme instruções específicas dos órgãos públicos controladores. As finalidades do tratamento incluem a prestação de serviços públicos digitais, modernização de processos administrativos, implementação de

políticas públicas, e melhoria da eficiência na gestão pública. A base legal predominante é a execução de políticas públicas, conforme previsto no artigo 7º, inciso III da LGPD [1].

Os dados tratados nesta categoria incluem informações de identificação civil (nome, CPF, RG), dados de contato (endereço, telefone, e-mail), informações socioeconômicas, dados de beneficiários de programas sociais, informações de contribuintes, e dados específicos relacionados aos serviços públicos prestados. A Servix Informática implementa controles rigorosos para assegurar que o tratamento seja limitado às finalidades específicas de cada política pública, mantendo a segregação adequada entre diferentes sistemas e órgãos, e implementando medidas de segurança reforçadas considerando a sensibilidade e o volume dos dados tratados.

A empresa estabelece contratos específicos com cada órgão público que detalham as responsabilidades de cada parte, as medidas de segurança a serem implementadas, os procedimentos para resposta a incidentes, e os mecanismos de supervisão e auditoria. Estes contratos incluem cláusulas específicas sobre proteção de dados, definindo claramente os papéis de controlador e operador, as instruções para tratamento, e os procedimentos para atendimento aos direitos dos titulares.

Dados de Clientes do Setor Privado: Para clientes do setor privado, a Servix Informática pode atuar como controladora ou operadora, dependendo da natureza específica dos serviços prestados. Quando atua como controladora, as finalidades incluem a prestação de serviços de desenvolvimento de software, consultoria em tecnologia da informação, suporte técnico, e gestão de relacionamento comercial. As bases legais aplicáveis incluem execução de contrato, interesse legítimo, e consentimento, conforme a natureza específica de cada tratamento.

Os dados tratados incluem informações de contato de representantes das empresas clientes, dados técnicos necessários para prestação de serviços, informações de faturamento e cobrança, dados de usuários de sistemas desenvolvidos, e informações de suporte técnico. A empresa implementa medidas específicas para assegurar a confidencialidade e segurança destes dados, incluindo controles de acesso baseados na

necessidade de conhecer, criptografia de dados sensíveis, e monitoramento de atividades de acesso.

Dados de Colaboradores: O tratamento de dados pessoais de colaboradores abrange todo o ciclo de vida da relação de trabalho, desde o processo de recrutamento e seleção até o desligamento e período pós-contratual. As finalidades incluem gestão de recursos humanos, cumprimento de obrigações trabalhistas e previdenciárias, administração de benefícios, controle de acesso e segurança, avaliação de desempenho, e desenvolvimento profissional. As bases legais predominantes são execução de contrato de trabalho e cumprimento de obrigação legal.

Os dados tratados incluem informações pessoais básicas (nome, CPF, RG, endereço), dados familiares para fins de benefícios, informações bancárias, dados de saúde ocupacional, registros de ponto e frequência, avaliações de desempenho, dados de treinamento e desenvolvimento, e informações disciplinares quando aplicável. A empresa implementa controles específicos para proteger a privacidade dos colaboradores, incluindo limitação de acesso a pessoal autorizado, segregação de dados sensíveis, e procedimentos específicos para tratamento de dados de saúde.

Para colaboradores em modalidade de trabalho remoto ou híbrido, a Servix Informática implementa controles adicionais que incluem monitoramento de segurança de dispositivos, controles de acesso remoto, e procedimentos específicos para proteção de dados em ambientes domésticos. A empresa fornece treinamento específico sobre proteção de dados em trabalho remoto e implementa tecnologias que asseguram a segurança dos dados independentemente da localização do colaborador.

Dados de Fornecedores e Prestadores de Serviços: O tratamento de dados de fornecedores e prestadores de serviços inclui informações necessárias para gestão de relacionamento comercial, avaliação de fornecedores, execução de contratos, e cumprimento de obrigações fiscais e regulamentares. As bases legais incluem execução de contrato, cumprimento de obrigação legal, e interesse legítimo para atividades como avaliação de fornecedores e gestão de riscos.

Os dados tratados incluem informações de identificação de representantes, dados de contato, informações financeiras e fiscais, dados de qualificação técnica, histórico de relacionamento comercial, e avaliações de desempenho. A empresa implementa procedimentos de due diligence para avaliar a conformidade de fornecedores com normas de proteção de dados, especialmente quando estes atuam como operadores de dados pessoais.

Dados de Terceiros: A Servix Informática pode tratar dados de terceiros em situações específicas, como usuários finais de sistemas desenvolvidos para clientes, beneficiários de serviços públicos, e outras partes interessadas. Nestes casos, a empresa atua predominantemente como operadora, seguindo instruções específicas dos controladores e implementando medidas adequadas de proteção.

Finalidades Específicas do Tratamento: Todas as atividades de tratamento da Servix Informática são realizadas para finalidades específicas, explícitas e legítimas, incluindo prestação de serviços contratados, cumprimento de obrigações legais, gestão de relacionamento comercial, segurança da informação, prevenção de fraudes, melhoria de produtos e serviços, pesquisa e desenvolvimento, marketing e comunicação (quando baseado em consentimento ou interesse legítimo), e atendimento a solicitações de autoridades competentes.

A empresa mantém documentação detalhada de todas as finalidades de tratamento, assegurando que não haja desvio de propósito ou utilização de dados para fins incompatíveis com aqueles originalmente declarados. Qualquer nova finalidade de tratamento é submetida a avaliação prévia para determinar a base legal aplicável e as medidas de proteção necessárias.

10. SEGURANÇA DA INFORMAÇÃO

A Servix Informática implementa um programa abrangente de segurança da informação, conforme o sistema de gestão de segurança da informação, que visa proteger dados pessoais contra acessos não autorizados, alterações indevidas, destruição acidental ou ilícita, e qualquer forma de tratamento inadequado ou ilícito. Este programa baseia-se em

padrões internacionais reconhecidos, incluindo a família de normas ISO/IEC 27000, e é continuamente atualizado para enfrentar ameaças emergentes e incorporar melhores práticas do setor [9].

Medidas Técnicas de Segurança: A empresa implementa um conjunto robusto de controles técnicos que incluem criptografia de dados em trânsito e em repouso, utilizando algoritmos reconhecidos internacionalmente e chaves de tamanho adequado para proteger a confidencialidade e integridade dos dados pessoais. Todos os dados pessoais sensíveis são criptografados utilizando padrões de criptografia forte, e as chaves criptográficas são gerenciadas através de sistemas seguros de gestão de chaves que asseguram sua proteção e rotação regular.

A arquitetura de rede da Servix Informática implementa segmentação adequada, com firewalls configurados para permitir apenas o tráfego necessário e autorizado. Sistemas de detecção e prevenção de intrusão monitoram continuamente a rede em busca de atividades suspeitas ou maliciosas, e sistemas de proteção de dados identificam e bloqueiam tentativas de exfiltração não autorizada de dados pessoais.

A empresa utiliza tecnologias de virtualização e containerização para isolar aplicações e dados, reduzindo o risco de acesso não autorizado e facilitando a implementação de controles de segurança granulares. Sistemas de backup automatizados asseguram a disponibilidade e recuperabilidade dos dados, com testes regulares de restauração para verificar a integridade e eficácia dos backups.

Medidas Administrativas de Segurança: O programa de segurança da informação da Servix Informática inclui políticas e procedimentos abrangentes que definem responsabilidades, estabelecem controles operacionais, e orientam a resposta a incidentes de segurança. A empresa mantém uma política de segurança da informação aprovada pela alta direção e revisada regularmente para assegurar sua adequação e eficácia.

Procedimentos específicos são estabelecidos para gestão de mudanças em sistemas que processam dados pessoais, assegurando que todas as alterações sejam avaliadas quanto ao seu impacto na segurança e privacidade antes da implementação. A empresa

implementa processos rigorosos de gestão de vulnerabilidades, incluindo varreduras regulares, avaliação de riscos, e aplicação oportuna de patches e atualizações de segurança.

Programas de conscientização e treinamento em segurança da informação são realizados regularmente para todos os colaboradores, com conteúdo específico sobre proteção de dados pessoais, reconhecimento de ameaças como phishing e engenharia social, e procedimentos para resposta a incidentes. A empresa também implementa programas de simulação de ataques para testar a preparação dos colaboradores e identificar áreas que necessitam de treinamento adicional.

Controle de Acesso: A Servix Informática implementa um sistema abrangente de controle de acesso baseado no princípio do menor privilégio, assegurando que colaboradores tenham acesso apenas aos dados pessoais estritamente necessários para o desempenho de suas funções. O sistema de gestão de identidade e acesso (IAM) centraliza a administração de contas de usuário, implementa autenticação multifator para acesso a sistemas críticos, e mantém logs detalhados de todas as atividades de acesso.

Revisões regulares de privilégios de acesso são realizadas para identificar e remover acessos desnecessários ou inadequados. Procedimentos específicos são estabelecidos para concessão, modificação e revogação de acessos, incluindo aprovações adequadas e documentação de justificativas. A empresa implementa controles técnicos que impedem o acesso simultâneo com múltiplas identidades e detectam tentativas de acesso não autorizado.

Para colaboradores em trabalho remoto, controles adicionais incluem o uso obrigatório de VPN para acesso a sistemas corporativos, autenticação multifator reforçada, e monitoramento de segurança de dispositivos. A empresa fornece dispositivos corporativos configurados com controles de segurança adequados e implementa políticas que regulamentam o uso de dispositivos pessoais (BYOD) quando permitido.

Criptografia: A implementação de criptografia na Servix Informática segue padrões internacionais reconhecidos e melhores práticas do setor. Dados pessoais em trânsito são

protegidos através de protocolos seguros como TLS 1.3 ou superior, assegurando a confidencialidade e integridade durante a transmissão. Dados em repouso são criptografados utilizando algoritmos simétricos robustos como AES-256, com chaves gerenciadas através de sistemas dedicados de gestão de chaves.

A empresa implementa criptografia de aplicação para dados particularmente sensíveis, assegurando que permaneçam protegidos mesmo em caso de comprometimento da infraestrutura subjacente. Procedimentos específicos são estabelecidos para geração, distribuição, armazenamento e rotação de chaves criptográficas, incluindo o uso de módulos de segurança de hardware (HSM) para proteção de chaves críticas.

Backup e Recuperação: O programa de backup da Servix Informática assegura a disponibilidade e recuperabilidade de dados pessoais através de múltiplas camadas de proteção. Backups automatizados são realizados regularmente, com diferentes frequências baseadas na criticidade dos dados e nos requisitos de negócio. A empresa implementa a estratégia 3-2-1 de backup, mantendo pelo menos três cópias dos dados, em pelo menos dois tipos diferentes de mídia, com pelo menos uma cópia armazenada externamente.

Testes regulares de restauração são realizados para verificar a integridade e recuperabilidade dos backups, incluindo cenários de recuperação completa e parcial. A empresa mantém planos detalhados de continuidade de negócios e recuperação de desastres que incluem procedimentos específicos para proteção e recuperação de dados pessoais.

Monitoramento e Auditoria: A Servix Informática implementa sistemas abrangentes de monitoramento de segurança que incluem coleta e análise de logs de segurança, detecção de anomalias, e alertas automáticos para atividades suspeitas. Um Security Operations Center (SOC) monitora continuamente a infraestrutura de TI em busca de ameaças e incidentes de segurança, com procedimentos estabelecidos para escalação e resposta.

Auditorias regulares de segurança são realizadas por equipes internas e auditores externos independentes para avaliar a eficácia dos controles implementados e identificar

oportunidades de melhoria. A empresa mantém registros detalhados de todas as atividades de auditoria, incluindo descobertas, recomendações e ações corretivas implementadas.

Sistemas de correlação de eventos de segurança (SIEM) agregam e analisam logs de múltiplas fontes para identificar padrões suspeitos e potenciais violações de segurança. A empresa implementa indicadores de comprometimento (IoCs) e regras de detecção personalizadas para identificar ameaças específicas ao seu ambiente e aos dados pessoais sob sua responsabilidade.

11. TRABALHO REMOTO E MODALIDADES HÍBRIDAS

A Servix Informática reconhece que as modalidades de trabalho remoto e híbrido apresentam desafios específicos para a proteção de dados pessoais, exigindo controles adicionais e medidas de segurança adaptadas para ambientes descentralizados. A empresa desenvolveu políticas e procedimentos específicos para assegurar que a proteção de dados pessoais seja mantida independentemente da localização física dos colaboradores, implementando uma abordagem de segurança que considera os riscos únicos associados ao trabalho fora das instalações corporativas.

Políticas Específicas para Home Office: A política de trabalho remoto da Servix Informática estabelece requisitos claros para colaboradores que acessam ou processam dados pessoais fora das instalações da empresa. Estes requisitos incluem a obrigatoriedade de utilizar dispositivos corporativos ou dispositivos pessoais devidamente configurados com controles de segurança aprovados, a implementação de controles ambientais adequados no local de trabalho remoto, e o cumprimento de procedimentos específicos para proteção de dados pessoais.

Colaboradores em trabalho remoto devem assegurar que o ambiente de trabalho doméstico ofereça privacidade adequada para o tratamento de dados pessoais, incluindo medidas para prevenir acesso não autorizado por familiares ou terceiros, proteção contra observação não autorizada de telas e documentos, e implementação de controles físicos adequados para proteção de dispositivos e documentos. A empresa fornece orientações específicas sobre configuração de espaços de trabalho seguros, incluindo recomendações

sobre posicionamento de telas, uso de filtros de privacidade, e procedimentos para armazenamento seguro de documentos físicos.

A política também estabelece horários específicos para acesso a sistemas que processam dados pessoais sensíveis, limitando o acesso a períodos onde há maior supervisão e suporte técnico disponível. Colaboradores devem notificar imediatamente qualquer incidente de segurança ou suspeita de comprometimento de dados, seguindo procedimentos específicos para trabalho remoto que consideram as limitações de comunicação e suporte técnico fora do ambiente corporativo.

Segurança em Ambientes Remotos: A segurança de dados pessoais em ambientes remotos é assegurada através de múltiplas camadas de controles técnicos e organizacionais. Todos os acessos a sistemas corporativos que processam dados pessoais devem ser realizados através de conexões VPN criptografadas, utilizando protocolos seguros e autenticação multifator obrigatória. A empresa implementa soluções de VPN que criam túneis seguros entre dispositivos remotos e a infraestrutura corporativa, assegurando que todos os dados em trânsito sejam protegidos contra interceptação e modificação.

Sistemas de monitoramento de segurança são estendidos para dispositivos remotos, incluindo detecção de malware, monitoramento de atividades suspeitas, e alertas automáticos para tentativas de acesso não autorizado. A empresa utiliza soluções de Endpoint Detection and Response (EDR) que fornecem visibilidade em tempo real sobre atividades em dispositivos remotos e permitem resposta rápida a incidentes de segurança.

Controles de rede são implementados para assegurar que dispositivos remotos mantenham configurações de segurança adequadas, incluindo firewalls pessoais ativados, sistemas operacionais atualizados, e software antimalware em funcionamento. A empresa implementa políticas de conformidade de dispositivos que verificam automaticamente o status de segurança antes de permitir acesso a sistemas corporativos.

BYOD (Bring Your Own Device): Quando permitido, o uso de dispositivos pessoais para acesso a dados pessoais corporativos é rigorosamente controlado através de políticas específicas e controles técnicos. A empresa implementa soluções de Mobile Device

Management (MDM) ou Mobile Application Management (MAM) que permitem a gestão segura de aplicações corporativas em dispositivos pessoais, mantendo a separação entre dados pessoais e corporativos.

Dispositivos pessoais autorizados devem atender a requisitos mínimos de segurança, incluindo sistemas operacionais atualizados, configurações de segurança específicas, e instalação de aplicações de segurança aprovadas pela empresa. A política BYOD estabelece responsabilidades claras para colaboradores em relação à manutenção da segurança de seus dispositivos, incluindo a obrigação de reportar perda ou roubo imediatamente.

Controles técnicos incluem a containerização de aplicações corporativas, criptografia de dados corporativos armazenados em dispositivos pessoais, e capacidade de limpeza remota (remote wipe) de dados corporativos em caso de comprometimento ou término da relação de trabalho. A empresa mantém inventário de todos os dispositivos pessoais autorizados e implementa monitoramento de conformidade contínuo.

Controles de Acesso Remoto: O sistema de controle de acesso remoto da Servix Informática implementa múltiplas camadas de autenticação e autorização para assegurar que apenas usuários autorizados possam acessar dados pessoais. Autenticação multifator é obrigatória para todos os acessos remotos, utilizando combinações de fatores como senhas, tokens de hardware, autenticação biométrica, ou aplicações de autenticação móvel.

Treinamento para Trabalho Remoto: A Servix Informática implementa programas específicos de treinamento para colaboradores em trabalho remoto, abordando os riscos únicos associados ao processamento de dados pessoais fora do ambiente corporativo. O treinamento inclui módulos sobre segurança física em ambientes domésticos, reconhecimento e prevenção de ataques de engenharia social direcionados a trabalhadores remotos, uso seguro de redes Wi-Fi domésticas e públicas, e procedimentos específicos para resposta a incidentes em ambientes remotos.

Simulações regulares de incidentes de segurança são realizadas especificamente para cenários de trabalho remoto, testando a capacidade dos colaboradores de identificar e responder adequadamente a ameaças. A empresa fornece recursos contínuos de conscientização, incluindo alertas sobre ameaças emergentes direcionadas a trabalhadores remotos e atualizações sobre melhores práticas de segurança.

Monitoramento e Compliance: O programa de monitoramento da Servix Informática é estendido para cobrir atividades de trabalho remoto, incluindo verificação de conformidade com políticas de segurança, monitoramento de acesso a dados pessoais, e detecção de atividades anômalas. Relatórios regulares são gerados para avaliar a eficácia dos controles de trabalho remoto e identificar áreas que necessitam de melhoria.

Auditorias específicas são realizadas para avaliar a conformidade de ambientes de trabalho remoto com políticas de proteção de dados, incluindo verificações de configurações de segurança, avaliação de controles ambientais, e teste de procedimentos de resposta a incidentes. A empresa mantém métricas específicas para trabalho remoto, incluindo indicadores de segurança, conformidade com políticas, e eficácia de treinamentos.

12. RELACIONAMENTO COM SETOR PÚBLICO

A Servix Informática mantém relacionamento estratégico com diversos órgãos e entidades do setor público, desenvolvendo e implementando soluções tecnológicas que modernizam a gestão pública e melhoram a prestação de serviços aos cidadãos. Este relacionamento exige atenção especial às especificidades legais e regulamentares aplicáveis ao setor público, incluindo requisitos específicos de transparência, accountability, e proteção de dados pessoais de cidadãos.

Especificidades para Clientes Públicos: O tratamento de dados pessoais em contratos com o setor público é regido por princípios específicos que incluem supremacia do interesse público, legalidade estrita, impessoalidade, moralidade, publicidade, e eficiência. A Servix Informática reconhece que, nestes casos, frequentemente atua como operadora de dados pessoais, processando informações de cidadãos conforme instruções específicas dos órgãos públicos controladores.

A empresa implementa controles específicos para assegurar que o tratamento de dados pessoais em contratos públicos seja realizado exclusivamente para as finalidades estabelecidas nas políticas públicas específicas, respeitando os limites e condições estabelecidos em leis, regulamentos, e instrumentos contratuais. Particular atenção é dada ao princípio da finalidade, assegurando que dados coletados para uma política pública específica não sejam utilizados para finalidades incompatíveis ou não autorizadas.

Compartilhamento de Dados com Órgãos Públicos: O uso compartilhado de dados pessoais com órgãos públicos é realizado em estrita conformidade com o artigo 26 da LGPD, que permite a comunicação ou o uso compartilhado de dados pessoais de pessoa natural entre órgãos e entidades públicos ou entre esses e entes privados, reciprocamente, com autorização específica [1]. A Servix Informática implementa controles rigorosos para assegurar que todo compartilhamento seja baseado em autorização legal específica, limitado às finalidades autorizadas, e documentado adequadamente.

Procedimentos específicos são estabelecidos para avaliar solicitações de compartilhamento de dados, incluindo verificação da base legal, avaliação da necessidade e proporcionalidade, e implementação de medidas de segurança adequadas. A empresa mantém registros detalhados de todos os compartilhamentos realizados, incluindo identificação dos órgãos envolvidos, finalidades específicas, dados compartilhados, e medidas de proteção implementadas.

Bases Legais Específicas: Para contratos com o setor público, a Servix Informática utiliza predominantemente a base legal de execução de políticas públicas, conforme estabelecido no artigo 7º, inciso III da LGPD [1]. Esta base legal exige que o tratamento seja necessário para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da LGPD.

A empresa também pode utilizar outras bases legais quando aplicáveis, incluindo cumprimento de obrigação legal para atendimento a determinações de autoridades competentes, execução de contrato para prestação de serviços específicos, e interesse

legítimo para atividades como segurança da informação e prevenção de fraudes, sempre observando os limites e condições específicas de cada base legal.

Transparência e Accountability: O relacionamento com o setor público exige níveis elevados de transparência e accountability, incluindo a disponibilização de informações sobre práticas de tratamento de dados, implementação de mecanismos de controle social, e prestação de contas regular sobre o cumprimento de obrigações contratuais e legais. A Servix Informática implementa procedimentos específicos para atender a esses requisitos, incluindo elaboração de relatórios de transparência, participação em auditorias governamentais, e disponibilização de informações para controle social.

A empresa mantém canais específicos para comunicação com órgãos de controle, incluindo Tribunais de Contas, Controladoria-Geral da União, Ministério Público, e outros órgãos de fiscalização. Procedimentos específicos são estabelecidos para atendimento a solicitações de informações, fornecimento de documentação, e cooperação em investigações e auditorias.

13. GESTÃO DE INCIDENTES

A Servix Informática mantém um programa abrangente de gestão de incidentes de segurança da informação e proteção de dados pessoais, projetado para detectar, responder, conter e remediar violações de dados de forma rápida e eficaz. Este programa baseia-se em melhores práticas internacionais e atende aos requisitos específicos estabelecidos pela LGPD para notificação e gestão de incidentes de segurança.

Definição de Incidente de Segurança: Para os propósitos desta política, um incidente de segurança é definido como qualquer evento que resulte em acesso não autorizado, alteração, destruição, perda, ou qualquer forma de tratamento inadequado ou ilícito de dados pessoais [1]. Isso inclui, mas não se limita a, ataques cibernéticos que resultem em acesso não autorizado a dados pessoais, perda ou roubo de dispositivos contendo dados pessoais, erro humano que resulte em divulgação não autorizada de dados, falhas de sistema que comprometam a integridade ou disponibilidade de dados pessoais, e tentativas de acesso não autorizado, mesmo que não sejam bem-sucedidas.

A empresa classifica incidentes de acordo com sua severidade, considerando fatores como volume de dados afetados, sensibilidade dos dados envolvidos, número de titulares afetados, potencial de dano aos titulares, e impacto nas operações da empresa. Esta classificação orienta a priorização da resposta e determina os procedimentos específicos a serem seguidos.

Procedimentos de Resposta: O procedimento de resposta a incidentes da Servix Informática é estruturado em fases distintas que incluem detecção e análise inicial, contenção e erradicação, recuperação e normalização, e lições aprendidas. Cada fase possui objetivos específicos, responsabilidades definidas, e critérios claros para progressão para a fase seguinte.

A fase de detecção e análise inicial envolve a identificação do incidente, avaliação preliminar de seu escopo e impacto, e ativação da equipe de resposta a incidentes. A empresa mantém sistemas automatizados de detecção que monitoram continuamente a infraestrutura em busca de indicadores de comprometimento, complementados por procedimentos para reporte manual de incidentes por colaboradores.

A fase de contenção e erradicação foca na limitação do impacto do incidente e eliminação da causa raiz. Isso pode incluir isolamento de sistemas comprometidos, revogação de credenciais de acesso, aplicação de patches de segurança, e implementação de controles temporários para prevenir escalação do incidente.

Comunicação à ANPD: A Servix Informática cumpre rigorosamente os requisitos de notificação estabelecidos no artigo 48 da LGPD, comunicando à Autoridade Nacional de Proteção de Dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares [1]. A notificação é realizada em prazo razoável, não superior a 72 horas contadas do momento em que a empresa toma conhecimento do incidente.

A comunicação à ANPD inclui informações específicas sobre a natureza dos dados pessoais afetados, os titulares envolvidos, as medidas técnicas e de segurança utilizadas para a proteção dos dados, os riscos relacionados ao incidente, os motivos da demora na

comunicação (quando aplicável), e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente.

Comunicação aos Titulares: Quando o incidente de segurança puder acarretar risco ou dano relevante aos titulares de dados, a Servix Informática comunica o ocorrido aos titulares afetados em linguagem clara e acessível, fornecendo informações sobre a natureza do incidente, os dados pessoais afetados, as medidas imediatas tomadas para mitigar os efeitos do incidente, e as recomendações sobre medidas que os titulares podem adotar para se proteger.

A comunicação aos titulares é realizada através dos meios mais eficazes disponíveis, considerando a urgência da situação e a necessidade de alcançar todos os afetados. Quando não for possível a comunicação individual, a empresa utiliza meios de comunicação de massa, como publicação em website, comunicados à imprensa, ou outros meios apropriados.

Plano de Contingência: A Servix Informática mantém planos de contingência específicos para diferentes tipos de incidentes de segurança, incluindo procedimentos para manutenção da continuidade dos negócios durante e após incidentes. Estes planos incluem identificação de sistemas críticos, procedimentos de backup e recuperação, recursos alternativos para manutenção de operações essenciais, e critérios para ativação de instalações de contingência.

Os planos de contingência são testados regularmente através de exercícios simulados que avaliam a eficácia dos procedimentos, a preparação das equipes, e a adequação dos recursos disponíveis. Resultados destes testes são utilizados para aprimorar os planos e melhorar a preparação da organização.

14. TREINAMENTO E CONSCIENTIZAÇÃO

A Servix Informática reconhece que a proteção eficaz de dados pessoais depende fundamentalmente do conhecimento, conscientização e comprometimento de todos os colaboradores. Por isso, a empresa implementa um programa abrangente de treinamento e

conscientização em proteção de dados que abrange todos os níveis organizacionais e é continuamente atualizado para refletir mudanças na legislação, ameaças emergentes, e melhores práticas do setor.

Programa de Treinamento: O programa de treinamento em proteção de dados da Servix Informática é estruturado em múltiplos níveis, considerando as diferentes responsabilidades e necessidades de cada função. O treinamento básico, obrigatório para todos os colaboradores, aborda conceitos fundamentais da LGPD, princípios de proteção de dados, direitos dos titulares, responsabilidades individuais, e procedimentos básicos de segurança da informação.

Treinamentos especializados são desenvolvidos para funções específicas, incluindo desenvolvedores de software, administradores de sistemas, profissionais de recursos humanos, equipes comerciais, e gestores. Estes treinamentos abordam aspectos específicos da proteção de dados relevantes para cada função, incluindo técnicas de privacy by design, implementação de controles de segurança, gestão de consentimento, e procedimentos específicos para tratamento de dados em suas respectivas áreas.

Treinamento Inicial: Todos os novos colaboradores da Servix Informática participam de treinamento obrigatório em proteção de dados como parte do processo de integração. Este treinamento introduz os conceitos fundamentais da LGPD, apresenta as políticas e procedimentos da empresa, e estabelece expectativas claras sobre responsabilidades individuais em relação à proteção de dados pessoais.

O treinamento inicial inclui módulos práticos que simulam situações reais de trabalho, permitindo que os colaboradores pratiquem a aplicação dos conceitos aprendidos. Avaliações são realizadas para verificar a compreensão dos conceitos e identificar necessidades de treinamento adicional.

Treinamento Continuado: A empresa implementa um programa de treinamento continuado que inclui atualizações regulares sobre mudanças na legislação, novas ameaças de segurança, e evolução das melhores práticas. Treinamentos de reciclagem

são realizados anualmente para todos os colaboradores, com frequência maior para funções que envolvem maior exposição a dados pessoais.

Webinars, workshops, e sessões de conscientização são realizados regularmente para abordar tópicos específicos, discutir casos práticos, e promover o compartilhamento de experiências entre colaboradores. A empresa também promove a participação de colaboradores em eventos externos, conferências e cursos de especialização em proteção de dados.

15. DISPOSIÇÕES FINAIS

Esta Política de Proteção de Dados Pessoais da Servix Informática entra em vigor na data de sua aprovação pela Diretoria Executiva e substitui todas as versões anteriores de políticas relacionadas à proteção de dados pessoais. A política será revisada anualmente ou sempre que houver mudanças significativas na legislação, na estrutura organizacional da empresa, ou nas atividades de tratamento de dados pessoais.

Vigência e Atualizações: A presente política tem vigência indeterminada e será atualizada conforme necessário para manter sua adequação e eficácia. Todas as atualizações serão aprovadas pela Diretoria Executiva, comunicadas a todos os colaboradores, e publicadas nos canais oficiais da empresa. Versões anteriores da política serão mantidas em arquivo para fins de auditoria e demonstração de conformidade histórica.

Publicação e Divulgação: Esta política é publicada no website da Servix Informática e disponibilizada a todos os colaboradores através da intranet corporativa. Resumos executivos e materiais de divulgação são desenvolvidos para facilitar a compreensão e aplicação da política por diferentes públicos. A empresa assegura que todos os stakeholders relevantes tenham acesso às informações necessárias sobre suas práticas de proteção de dados.

Contatos e Canais de Comunicação: Para questões relacionadas à proteção de dados pessoais, exercício de direitos dos titulares, ou comunicação de incidentes de segurança, os interessados podem entrar em contato com:

Encarregado de Proteção de Dados (DPO)

DPO: Pedro Calejon

E-mail: dpo@servix.com

Telefone: +55 (11) 3525-3400

Endereço: R. Pequetita, 215 - 7º andar - Vila Olímpia, São Paulo - SP, 04552-060

Ouvidoria de Proteção de Dados

DPO: Pedro Calejon

E-mail: dpo@servix.com

Formulário online

A Servix Informática reafirma seu compromisso com a proteção de dados pessoais e com o cumprimento integral da Lei Geral de Proteção de Dados Pessoais, reconhecendo que a confiança dos titulares de dados é fundamental para o sucesso de suas operações e para o cumprimento de sua missão de contribuir para a modernização e melhoria dos serviços públicos e privados através da tecnologia.

16. REFERÊNCIAS

[1] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[2] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Art. 6º. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[3] BRASIL. Constituição da República Federativa do Brasil de 1988. Art. 5º, incisos X e XII. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

[4] BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm

[5] BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

[6] BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

[7] OECD. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Disponível em: https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm

[8] BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

[9] ISO/IEC 27001:2022. Information security management systems — Requirements. International Organization for Standardization.