Nome	Privacidade e Proteção de Dados Pessoais
Departamento Responsável	Compliance
Data Início	Abril/2024
Data de Revisão	Abril/2025
Diretoria Responsável	Finanças e Riscos
Versão	2.0

SUMÁRIO

1. OBJETIVO

O ***Banco Inbursa S.A.*** se esforça por atender aos requisitos das leis e regulamentos aplicáveis relacionados à privacidade e proteção de Dados Pessoais nos países onde opera.

Esta Política descreve os princípios básicos e estratégias do Programa de Privacidade e Proteção de Dados Pessoais- LGPD do ***Banco Inbursa***, incluindo definições, estrutura organizacional, organização e responsabilidades visando a segurança e proteção dos dados de clientes, fornecedores, parceiros de negócios, funcionários e outras pessoas, dentro das melhores práticas de mercado para gerenciamento de riscos à exposição e/ou vazamento de dados sensíveis e/ou pessoais, durante o processamento e/ou armazenamento de dados pessoais

Definir a política de privacidade e proteção de dados pessoais no ***Banco Inbursa***, dentro de padrões estabelecidos, observando-se a Gestão de Riscos Operacionais, a Política de Segurança da Informação (PSI), Resoluções, Instruções Normativas e legislação vigentes.

Para tanto deve:

- Manter ações de identificação, prevenção e mitigação dos riscos de ameaças à exposição e/ou vazamento de dados pessoais;
- Estruturar, organizar, definir processos, atribuições e responsabilidades individuais e das equipes envolvidas no Programa de Privacidade e Proteção de Dados Pessoais no ***Banco Inbursa***.

2. ABRANGÊNCIA

Esta política se aplica a todo o escopo do Sistema de Privacidade e Proteção de Dados Pessoais do ***Banco Inbursa***. Deve, portanto, ser cumprida e aplicada em todas as áreas da organização.

3. APLICAÇÃO

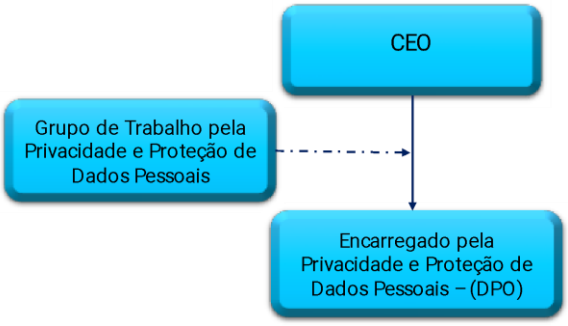
Esta política se aplica a todos as áreas, departamentos e colaboradores do ***Banco Inbursa***, que recebem, tratem e/ou manipulem e armazenem dados sensíveis e/ou pessoais.

Esta Política também se aplica as entidades ou subsidiárias pertencentes ou operadas pelo ***Banco Inbursa***, e não diverge de leis ou regulamentos municipais, estaduais ou federais que possam ser aplicáveis.

4. ORGANIZAÇÃO

4.1. Estrutura do Programa de Privacidade e Proteção de Dados Pessoais

O ***Banco Inbursa*** entende que a estrutura organizacional adequada para o gerenciamento do Programa de Privacidade, Proteção de Dados e resposta a situações de incidente na(s) linha(s) de negócios representada pela estrutura ao lado:



5. RESPONSABILIDADE

O ***Banco Inbursa*** entende que a organização adequada para a gestão e gerenciamento e operação do programa de continuidade de negócios, é a constituída conforme segue:

5.1. Diretor de Finanças e Riscos

É responsabilidade do Diretor de Finanças e Riscos do ***Banco Inbursa***, no âmbito de suas atribuições:

- Estabelecer os processos formais a serem utilizado na gestão da privacidade e proteção de dados pessoais;
- Definir e coordenar a implementação e os padrões a serem seguidos na privacidade e proteção de dados pessoais, os sistemas de suporte, as formas e a periodicidade dos seus reportes.
- Instituir o Grupo de Trabalho pela Privacidade e Proteção de Dados Pessoais, composto por representantes das áreas representativas da empresa a fim de conduzir, coordenar, definir, controlar e dirimir todas as questões sobre proteção de dados pessoais no ***Banco Inbursa***;
- Elaboração/ Revisão do Relatório de Privacidade e Proteção de Dados Pessoais (RIPDP) com foco em segurança da informação e proteção de dados pessoais no ***Banco Inbursa***, periodicamente, e reportá-los à alta direção da empresa.
- Estabelecer processos formais para conscientização dos gestores e colaboradores do ***Banco Inbursa*** sobre a importância da proteção de dados pessoais e a responsabilidade inerente aos administradores, funcionários e prestadores de serviços alocados.

5.2. Grupo de Trabalho pela Privacidade e Proteção de Dados Pessoais

É responsabilidade do Grupo de Trabalho pela Privacidade e Proteção de Dados Pessoais do ***Banco Inbursa***, no âmbito de suas atribuições:

- Reunir informações sobre a situação, e seus desdobramentos, de forma rápida e precisa, para a correta condução do incidente com dados pessoais.
- Estabelecer ações e acompanhar seus desdobramentos para a resolução do incidente, visando o correto gerenciamento, a continuidade dos negócios e o retorno às atividades normais do ***Banco Inbursa***.
- Assegurar que a(s) autoridade(s) competente(s) foi (foram) informada(s) (Agência Nacional de Proteção de ados), onde quando aplicável;
- Comunicar o incidente e seus desdobramentos, com as medidas necessárias, aos acionistas, empregados, clientes, fornecedores e mídia, onde aplicável.
- Mobilizar o apoio externo necessário.
- Validar proposições, políticas e procedimentos oriundos de colaboradores, grupos, comissões provisórias ou permanentes.

5.3. Encarregado pela Privacidade e Proteção de Dados Pessoais

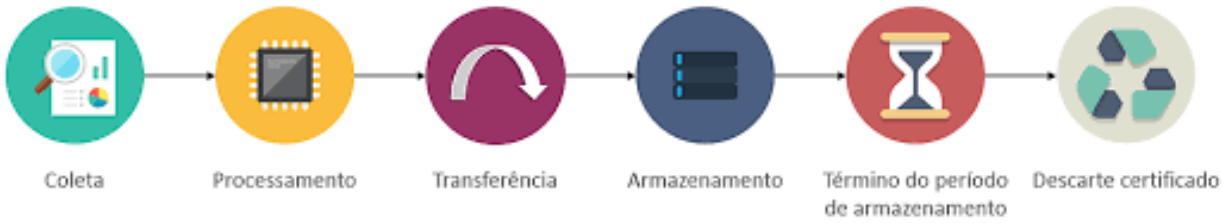
Dentre suas responsabilidades, todas previstas na Lei Geral de Proteção de Dados- LGPD, as atividades do encarregado consistem em:

- Aceitar solicitações, 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 privacidade e proteção de dados pessoais; e
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

6. DIRETRIZES GERAIS

6.1. Organização e Ciclo da Proteção de Dados Pessoais

A LGPD estabelece regras detalhadas para a coleta, uso, tratamento e armazenamento de dados pessoais e afeta as relações entre clientes e fornecedores de produtos e serviços, empregado e empregador, relações comerciais transnacionais e nacionais, além de outras relações nas quais dados pessoais sejam coletados, tanto no ambiente digital quanto fora dele.



6.2. Princípios básicos sobre o processamento de dados pessoais

Os princípios de proteção de dados descrevem as responsabilidades básicas do ***Banco Inbursa*** ao tratar com dados pessoais:

6.2.1. Legalidade, justiça e transparência

Os dados pessoais devem ser processados de forma legal, justa e transparente em relação ao titular dos dados.

6.2.2. Limitação de finalidade

Os dados pessoais devem ser coletados para fins especificados, explícitos e legítimos e não devem ser processados de maneira incompatível com esses fins.

6.2.3. Minimização de dados

Os dados pessoais devem ser adequados, relevantes e limitados ao necessário em relação aos propósitos para os quais são processados. O ***Banco Inbursa*** deve aplicar anonimização ou pseudo anonimização aos dados pessoais, se possível, para reduzir os riscos para os titulares de dados em questão, quando possível.

6.2.4. Precisão

Os dados pessoais devem ser precisos e, quando necessário, atualizados; devem ser tomadas medidas razoáveis para garantir que os dados pessoais imprecisos, tendo em conta as finalidades para as quais são processados, sejam descartados ou retificados em tempo hábil.

6.2.5. Limitação do período de armazenamento

Os dados pessoais não devem ser mantidos por mais tempo do que o necessário para os fins para os quais os dados pessoais são processados.

6.2.6. Integridade e confidencialidade

Levando em conta o estado da tecnologia e outras medidas de segurança disponíveis, a probabilidade e gravidade dos riscos e outras medidas de segurança disponíveis, o ***Banco Inbursa*** deve aplicar medidas técnicas ou organizacionais apropriadas para processar os dados pessoais de uma maneira que garanta a proteção contra destruição acidental ou ilegal, perda, alternância, acesso não autorizado ou divulgação.

6.2.7. Responsabilidade

O ***Banco Inbursa*** demonstra conformidade com os princípios adotados e descritos acima, cumprindo integralmente as melhores práticas de proteção de dados e as diretrizes de execução determinadas pelos controladores das informações

6.3. Elementos da Gestão da Privacidade e Proteção de Dados Pessoais

O ***Banco Inbursa*** busca assegurar a privacidade e proteção de dados pessoais adotando a abordagem a seguir:

6.3.1. Análise de Impacto a Privacidade e Proteção de Dados (DPIA)

Fornece os princípios e considerações para lidar com riscos específicos de privacidade e proteção de dados pessoais, quando realizados para sistemas e processos.

6.3.2. Procedimentos, Orientações, Instrução Técnica/ Administrativas de Privacidade e Proteção de Dados Pessoais

Devem ser elaborados dentro de uma metodologia única, a partir dos princípios básicos sobre a privacidade e proteção de dados pessoais e por determinação legal/ regulatória.

O documento "Diretriz para Gestão da Privacidade e Proteção de Dados Pessoais" deve estar disponível para utilização e gerenciamento de atividades rotineiras, eventos e incidentes envolvendo dados pessoais, possibilitando o atendimento aos eventos (solicitações) e/ou respostas dentro de prazos e condições aceitáveis.

7. DESCRIÇÃO DO PROCESSO

7.1. Coleta de Dados

O ***Banco Inbursa*** se esforçar para coletar a menor quantidade possível de dados pessoais. Se os dados pessoais forem coletados de terceiros, a Empresa deverá garantir que os dados pessoais sejam coletados legalmente e as cláusulas contratuais devem garantir a questão da coleta e/ou obtenção das informações pessoais.

7.2. Uso, Retenção e Descarte

Os propósitos, métodos, limitação de armazenamento e período de retenção de dados pessoais devem ser consistentes com as informações contidas no Aviso de Privacidade. O ***Banco Inbursa*** deve manter a precisão, integridade, confidencialidade e relevância dos dados pessoais com base na finalidade do processamento.

Mecanismos de segurança adequados projetados para proteger os dados pessoais devem ser usados para impedir que dados pessoais sejam subtraídos, mal utilizados ou abusados e para impedir violações de dados pessoais.

7.3. Divulgação a Terceiros

Sempre que o ***Banco Inbursa*** usar um fornecedor terceirizado ou parceiro de negócios para processar dados pessoais em seu nome, deve garantir que este processador forneça medidas de segurança para proteger dados pessoais adequados aos riscos associados (como uso indevido de dados pessoais), uma divulgação autorizada de dados pessoais, violações de dados etc.). Para essa finalidade, o Questionário de conformidade com o LGPD do processador deve ser usado.

7.4. Transferência transfronteiriça de dados pessoais

Antes de transferir dados pessoais para fora do território nacional, devem ser usadas salvaguardas adequadas, em conformidade com a legislação no local de recebimento dos dados, autorização da Autoridade de Proteção de Dados, se necessário.

A entidade que recebe os dados pessoais deve cumprir os princípios de processamento de dados pessoais estabelecidos no Procedimento de transferência de dados entre fronteiras.

7.5. Direitos de acesso dos titulares dos dados

O ***Banco Inbursa*** ao atuar como controlador de dados será responsável por fornecer aos titulares dos dados um mecanismo de acesso razoável para permitir que acessem seus dados pessoais e deve permitir que eles atualizem, retifiquem, apaguem ou transmitam seus dados pessoais, se apropriado ou requerido pela lei.

7.6. Portabilidade de Dados

O Encarregado pela Privacidade e Proteção de Dados Pessoais (DPO) é o responsável por receber e garantir que tais solicitações efetuadas pelo titular do dado, sejam processadas dentro de um período razoável e que não sejam excessivas e não afetem os direitos de dados pessoais de outras pessoas.

7.7. Direito ao esquecimento

Mediante solicitação, os titulares dos dados têm o direito de obter do ***Banco Inbursa*** a exclusão de seus dados pessoais. Quando o ***Banco Inbursa*** atuar como Controladora, o Encarregado pela Privacidade e Proteção de Dados Pessoais (DPO) deve tomar as medidas necessárias (incluindo medidas técnicas) para informar os terceiros que usam ou processam esses dados para atender à solicitação.

7.8. Resposta a incidentes de violação de dados pessoais

Quando o ***Banco Inbursa*** identificar de forma inequívoca uma violação real ou potencial de dados pessoais, o Encarregado pela Privacidade e Proteção de Dados Pessoais (DPO) deve realizar investigação interna e tomar as medidas corretivas apropriadas em tempo hábil, de acordo com a Diretriz "Gestão Incidente" envolvendo Dados Pessoais. Havendo risco para os direitos e liberdades, o ***Banco Inbursa*** deve notificar as autoridades relevantes de proteção de dados sem demora injustificada e dentro do prazo de até 4 dias úteis.

7.9. Notificação aos titulares dos dados

O ***Banco Inbursa*** deve prover diferentes tipos de avisos de acordo com as várias atividades de processamento de dados que a mesma realiza.

Nos casos em que os dados pessoais estão sendo compartilhados com terceiros, o Encarregado pela Privacidade e Proteção de Dados Pessoais- DPO deve garantir que os titulares dos dados sejam notificados por meio de um Aviso de Privacidade.

7.10. Obtenção de consentimentos

Sempre que o processamento de dados pessoais se basear no consentimento do titular dos dados ou em outros motivos legais, deve ser apresentado ao responsável titular do dado, opções para seu consentimento e garantir que possa ser retirado a qualquer momento.

8. CONSIDERAÇÕES FINAIS

Qualquer situação não contemplada neste procedimento, deve ser validada com o Encarregado pela Privacidade e Proteção de Dados, posteriormente com o Grupo de Trabalho pela Privacidade e Proteção de Dados e em seguida junto ao Diretor de Finanças e Riscos

9. VIOLAÇÕES

Qualquer suspeita de violação desta Política deve ser reportada imediatamente à Equipe de Segurança da Informação. Todos os casos de suspeita de violações desta Política devem ser investigados e tomadas as medidas apropriadas.

A tentativa de burlar esta política, diretrizes e controles estabelecidos pelo ***Banco Inbursa***, quando constatada, deve ser tratada como uma violação.

O não cumprimento desta Política implica em falta grave e poderá resultar em ação disciplinar e estará sujeito as responsabilidades civil e/ou criminal se sua conduta violar leis ou regulamentos.

10. REVISÃO

O Encarregado pela Privacidade e Proteção de Dados Pessoais é responsável por manter atualizados os documentos do Programa de Gestão da Privacidade e Proteção de Dados Pessoais.

Em caso de alterações nos procedimentos, é responsabilidade do gestor do Departamento Responsável providenciar as alterações e encaminhar ao Compliance, para que seja atualizado o controle deste documento.

A revisão da documentação de Privacidade e Proteção de Dados Pessoais deve ocorrer em intervalo máximo de 12 meses, de forma planejada, ou após qualquer alteração significativa nos processos de negócios, de modo a refletir as necessidades do ***Banco Inbursa*** e da Proteção de Dados Pessoais.

11. CONFLITO DE DIREITOS

Esta política destina-se a cumprir as leis e regulamentos no local de estabelecimento e nos países em que o ***Banco Inbursa*** opera. No caso de qualquer conflito entre esta Política e as leis e regulamentos aplicáveis, estas últimas prevalecerão.

12. AUDITORIA E RESPONSABILIDADE

O Gestor de Tecnologia da Informação ou Gestor de Segurança da Informação, em conjunto com o Encarregado pela Privacidade e Proteção de Dados (DPO), são responsáveis por auditar e avaliar os projetos, departamentos e recursos e se os mesmos estão atuando de acordo com esta política.

13. DIVULGAÇÃO

A Política de Privacidade e Proteção de Dados Pessoais deve ser divulgada através de todos os meios, fóruns e âmbitos disponíveis, priorizando os meios de comunicação internos como espaço de disseminação a todos os funcionários e demais colaboradores do ***Banco Inbursa***, bem como às demais partes interessadas.

14. VIGÊNCIA

Esta política entra em vigor a partir da data de sua publicação.

15. PROCEDIMENTOS, POLÍTICAS, REGULAMENTAÇÃO E DOCUMENTOS RELACIONADOS

15.1. Documentos Internos

- Política de segurança da informação.

15.2. Documentos externos

- LGPD - LEI Nº 13.709, de 14 de Agosto de 2018.
- Marco Civil da Internet - LEI Nº 12.965, DE 23 DE ABRIL DE 2014.
- Resolução do Banco Central do Brasil nº 4.893, de 26 de fevereiro de 2021

16. GLOSSÁRIO

As seguintes definições dos termos utilizados neste documento em acordo com a LGPD - Lei Geral de Proteção de Dados:

Dados pessoais: qualquer informação relacionada a uma pessoa física identificada ou identificável ("**Titular dos dados**") que possa ser identificado, direta ou indiretamente, principalmente por referência a um identificador como um nome, um número de identificação, dados de localização, um

identificador on-line ou um ou mais fatores específicos à identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.

Dados pessoais sensíveis: dados pessoais que são, por natureza, particularmente sensíveis em relação aos direitos e liberdades fundamentais merecem proteção específica, pois o contexto de seu processamento pode criar riscos significativos para os direitos e liberdades fundamentais. Esses dados pessoais incluem dados pessoais que revelam origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou associação a sindicatos, dados genéticos, dados biométricos com o objetivo de identificar exclusivamente uma pessoa natural, dados relativos à saúde ou dados relativos ao sexo de uma pessoa singular. vida ou orientação sexual.

Controlador de dados: a pessoa singular ou coletiva, autoridade pública, agência ou qualquer outro órgão, que sozinho ou em conjunto com outros, determina os propósitos e os meios do processamento de dados pessoais.

Processador de dados: Uma pessoa singular ou coletiva, autoridade pública, agência ou qualquer outro organismo que processe dados pessoais em nome de um Controlador de dados.

Processamento: Uma operação ou conjunto de operações que são executadas em dados pessoais ou em conjuntos de dados pessoais, independentemente de serem automatizados, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição dos dados.

Anonimização: identificação irreversível de dados pessoais, de modo que a pessoa não possa ser identificada usando tempo, custo e tecnologia razoáveis pelo controlador ou por qualquer outra pessoa para identificar esse indivíduo. Os princípios de processamento de dados pessoais não se aplicam aos dados anônimos, pois não são mais dados pessoais.

Pseudo anonimização: O processamento de dados pessoais de forma que os dados pessoais não possam mais ser atribuídos a um titular de dados específico sem o uso de informações adicionais, desde que essas informações adicionais sejam mantidas separadamente e estejam sujeitas a medidas técnicas e organizacionais para garantir que os dados pessoais não são atribuídos a uma pessoa singular identificada ou identificável. A pseudo anonimização reduz, mas não elimina completamente, a capacidade de vincular dados pessoais a um titular de dados. Como os dados pseudo anonimizados ainda são dados pessoais, o processamento de dados pseudo anonimizados deve obedecer aos princípios do processamento de dados pessoais.

Tratamento transfronteiriço de dados pessoais: tratamento de dados pessoais que ocorre no contexto das atividades de estabelecimentos em uma ou localidades fora do território Nacional de um responsável pelo tratamento ou processador;

Autoridade de Supervisão: Uma autoridade pública criada pelo regulatório da LGPD no Brasil definido como ANPD (Autoridade Nacional de Proteção de Dados);

Autoridade supervisora principal: a autoridade supervisora com a principal responsabilidade de lidar com uma atividade de processamento de dados transfronteiriça, por exemplo, quando um titular de dados faz uma reclamação sobre o processamento de seus dados pessoais; é responsável, entre outros, por receber as notificações de violação de dados, ser notificado sobre atividades de

processamento de risco e terá total autoridade no que diz respeito às suas obrigações de garantir o cumprimento das disposições da LGPD

Cada "**autoridade supervisora local**" ainda manterá em seu próprio território e monitorará qualquer processamento de dados local que afete os titulares de dados ou que seja realizado por um controlador ou processador em território nacional ou de fora do mesmo quando o processamento deles atingir titulares de dados residentes em seu território.

Suas tarefas e poderes incluem conduzir investigações e aplicar medidas e multas administrativas, promovendo a conscientização pública sobre os riscos, regras, segurança e direitos em relação ao processamento de dados pessoais, bem como obter acesso a quaisquer instalações do controlador e do processador, incluindo qualquer equipamento e meio de processamento de dados.

17. DISTRIBUIÇÃO DE CÓPIAS

Tipo de Mídia	Armazenamento	Tiragem
Arquivo Digital	\\	1

18. HISTÓRICO DE REVISÕES

Histórico do documento				
Revisão	**Data Public.**	**Descrição das alterações**	**Elaborado por**	**Aprovado por**
2.0	Julho/24	Atualização- Inclusão da Matriz RACI		
1.0	Abril/23	Versão Inicial		

19. MATRIZ RACI

Item	Gerente de GRC	Comitê Proteção Dados	Gerentes	Coord. Superv	DPO
Objetivo, Abrangência e Aplicação	A	C	I	I	R
Organização	A	C	I	I	R
Responsabilidade	A	C	I	I	R
Diretrizes Gerais	A	C	I	I	R
Descrição do Processo	A	C	I	I	R
Considerações Finais	A	C	I	I	R

Violações	A	C	I	I	R
Revisão	I	I	I	I	R
Conflito de Direitos	A	C	I	I	R
Auditoria e Responsabilidade	A	C	R	I	R
Divulgação	A	I	I	I	R
Vigência	I	I	I	I	R
Procedimentos, Políticas, Regulamentação e Documentos Relacionados	I	I	I	I	R
Glossário	I	I	I	I	R
Distribuição e Cópias	C	I	I	I	R
Histórico de Revisões	I	I	I	I	R
Matriz RACI	A	C	I	I	R
Anexos	A	C	I	I	R

Onde: A= Aprovador; R= Responsável; C= Consultado; I= Informado;

20. APROVAÇÃO

Ciente e de acordo: São Paulo, julho de 2024.

Documento assinado digitalmente, via plataforma ClickSign, por:

Área responsável	Responsável
Segurança da Informação	

Diretoria envolvida no processo
Vladimir Baciga
Daniela Bovi

21. ANEXOS

Não é aplicável.