# LGPD NA ASPP

## CÓDIGO DE CONDUTA

Entenda quais os comportamentos éticos e seguros que garantem conformidade com a LGPD e padrões como a ISO 27001.

## O que é este código?

Este documento define padrões de comportamento esperado para todos os envolvidos com a ASPP, garantindo transparência, segurança da informação e cumprimento das normas legais. O objetivo é criar um ambiente respeitoso e seguro para todos.

## PRINCÍPIOS FUNDAMENTAIS

1. **Ética e Transparência:**
   Agir com integridade em todas as operações.
2. **Respeito à Privacidade:**
   Garantir o tratamento seguro e responsável de dados pessoais.
3. **Conformidade Legal:**
   Atuar em conformidade com leis, regulamentos e boas práticas.
4. **Responsabilidade Social:**
   Contribuir para um ambiente respeitoso, seguro e igualitário.
5. **Compromisso com a Cultura Organizacional:**
   Manter atitudes que reforcem os valores da ASPP.
6. **Compromisso de Confidencialidade:**
   Todos os colaboradores, fornecedores e parceiros da ASPP devem assinar um termo de compromisso, comprometendo-se a não repassar informações sigilosas da empresa para terceiros, sob pena de sanções disciplinares e legais.

## Termo de Compromisso de Confidencialidade

Todos os colaboradores devem assinar o Termo de Compromisso de Confidencialidade ao ingressar na ASPP, comprometendo-se a:

**Não compartilhar informações sigilosas da empresa com terceiros,**
incluindo dados pessoais, financeiros, estratégicos e operacionais.

**Manter a confidencialidade de documentos e dados**
acessados durante suas funções**.**

**Reportar imediatamente qualquer vazamento,**
incidente de segurança ou compartilhamento indevido de informações**.**

**Utilizar os sistemas e acessos da ASPP de maneira responsável e segura,**
garantindo que apenas pessoas autorizadas tenham acesso às informações.

*O descumprimento do compromisso de confidencialidade pode resultar em sanções disciplinares, incluindo advertências, suspensão e até desligamento, além de possíveis medidas legais cabíveis.*

# Aplicabilidade

Este Código aplica-se a todos os setores da ASPP, incluindo associados, colaboradores, fornecedores e parceiros, abrangendo os seguintes departamentos:

- **CAT (Central de Atendimento)**
- **Financeiro**
- **Contabilidade**
- **Almoxarifado**
- **Patrimônio e Obras**
- **Motoristas e Manobristas**
- **Serviços Gerais (Dia e Noite)**
- **Protocolo**
- **Portaria**
- **Caixa**
- **Recursos Humanos**
- **Gabinete**
- **Auxílio Funeral**
- **Ouvidoria**
- **Manutenção**
- **Conselho Deliberativo e Fiscal**
- **Marketing**
- **T.I (Tecnologia da Informação)**
- **Telefonistas**
- **Jurídico**
- **DAS (Interno)**
- **Compras**
- **Farmácia**

## Boas e más condutas por setor:

### CENTRAL DE ATENDIMENTO

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Utilizar sistemas corporativos seguros para registro de solicitações. | Compartilhar informações de associados em canais não autorizados (WhatsApp pessoal, e-mails externos). |
| Garantir o sigilo de informações pessoais compartilhadas durante o atendimento. | Permitir que terceiros ou não autorizados ouçam conversas de atendimento. |
| Encerrar as telas dos sistemas ao término de cada atendimento. | |

### FINANCEIRO

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Manter a confidencialidade das transações financeiras. | Deixar documentos financeiros expostos. |
| Armazenar documentos fiscais e financeiros em locais seguros. | Compartilhar dados bancários sem autorização. |

### CONTABILIDADE

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Garantir sigilo de informações contábeis. | Usar dados reais em testes sem anonimização. |
| Utilizar sistemas seguros para armazenamento de dados. | Permitir acesso irrestrito a documentos fiscais. |

## ALMOXARIFADO

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Monitorar entradas e saídas de materiais. | Permitir acesso não autorizado ao estoque. |
| Armazenar dados de fornecedores em locais protegidos. | Armazenar documentos sem controle adequado. |

## PATRIMÔNIO E OBRAS

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Proteger contratos e ativos com controle de acesso. | Compartilhar informações de fornecedores sem autorização. |
| Realizar inventários regulares. | Não auditar acessos a documentos estratégicos. |

## MOTORISTAS E MANOBRISTAS

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Garantir a segurança e confidencialidade no transporte de documentos. | Deixar documentos desprotegidos ou em locais de fácil acesso durante o transporte. |
| Assegurar que documentos sensíveis sejam entregues apenas aos destinatários autorizados. | Entregar documentos a pessoas não autorizadas. |
| Utilizar meios de transporte adequados para evitar extravio ou danos aos documentos. | Não comunicar imediatamente em caso de extravio, roubo ou dano de documentos sigilosos. |

## SERVIÇOS GERIAS (DIA E NOITE)

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Respeitar normas de segurança para documentos físicos. | Deixar documentos confidenciais expostos. |
| Manter sigilo sobre informações vistas durante a limpeza de ambientes. | Compartilhar informações obtidas de forma indireta. |

## PROTOCOLO

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Registrar corretamente a entrada e saída de documentos sigilosos. | Permitir acesso indevido a documentos protegidos. |
| Manter a confidencialidade das informações manipuladas. | Extraviar documentos sem notificação aos responsáveis. |

## PORTARIA

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Controlar o acesso a áreas restritas da organização. | Fornecer informações sobre colaboradores sem autorização. |
| Proteger registros de entrada e saída de visitantes. | Deixar registros de acesso expostos a terceiros. |

## CAIXA

| BOA CONDUTA | MÁ CONDUTA |
| --- | --- |
| Proteger informações financeiras e registros de pagamento. | Compartilhar detalhes de transações com terceiros não autorizados. |
| Manter sigilo sobre transações dos associados. | Armazenar documentos financeiros de forma inadequada. |

## RECURSOS HUMANOS

| BOA CONDUTA | MÁ CONDUTA |
| --- | --- |
| Garantir a confidencialidade dos dados dos colaboradores. | Divulgar informações sobre colaboradores sem consentimento. |
| Restringir acesso a informações sensíveis apenas a pessoas autorizadas. | Permitir acesso irrestrito a documentos com dados pessoais. |

## GABINETE

| BOA CONDUTA | MÁ CONDUTA |
| --- | --- |
| Garantir que documentos estratégicos sejam tratados com sigilo. | Compartilhar informações sigilosas de reuniões sem autorização. |

## AUXÍLIO FUNERAL

| BOA CONDUTA | MÁ CONDUTA |
| --- | --- |
| Garantir a confidencialidade dos dados de associados e familiares. | Expor dados pessoais de associados em documentos não protegidos. |

## OUVIDORIA

| BOA CONDUTA | MÁ CONDUTA |
| --- | --- |
| Manter sigilo e anonimato dos denunciantes. | Expor informações de denúncias sem permissão. |

## MANUTENÇÃO

| BOA CONDUTA | MÁ CONDUTA |
| --- | --- |
| Evitar acessar documentos confidenciais durante atividades de reparo. | Divulgar informações obtidas durante manutenções em áreas restritas. |

## CONSELHO DELIBERATIVO E FISCAL

| BOA CONDUTA | MÁ CONDUTA |
| --- | --- |
| Garantir que informações estratégicas sejam mantidas em sigilo. | Permitir acesso irrestrito às atas do conselho sem autorização. |

## MARKETING

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Obter consentimento para uso de imagens ou dados em campanhas. | Divulgar informações pessoais sem autorização explícita. |

## T.I.

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Implementar medidas para proteção de dados pessoais. | Permitir acessos não autorizados a bancos de dados. |
| Monitorar acessos e proteger contra vazamento de informações. | Compartilhar credenciais de acesso. |

## TELEFONISTAS

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Garantir o sigilo de informações recebidas durante os atendimentos. | Fornecer informações a terceiros sem autorização. |

## JURÍDICO

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Garantir o sigilo de documentos e contratos. | Compartilhar dados sensíveis fora do ambiente profissional. |

## DAS (INTERNO)

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Garantir a confidencialidade de dados administrativos. | Expor informações internas sem autorização. |

## COMPRAS

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Avaliar fornecedores quanto à conformidade com a LGPD. | Armazenar informações comerciais sem proteção. |

## FARMÁCIA

| BOA CONDUTA | MÁ CONDUTA |
|---|---|
| Garantir a confidencialidade de dados de saúde de associados. | Deixar receitas ou documentos médicos expostos. |

## E agora?

Fique tranquilo! Nosso objetivo é garantir que todos conheçam seus direitos, deveres e os cuidados necessários no dia a dia. Em caso de dúvida, nosso DPO está à disposição.

## Denúncias

Para reportar incidentes ou violações de privacidade, segurança ou ética, utilize o canal seguro de denúncias:

**brevenlaw.com/lgpd-aspp**

*As denúncias serão tratadas com confidencialidade e protegidas contra retaliações.*

# Incidentes de Segurança da Informação e Privacidade

## IDENTIFICAÇÃO

**Um incidente de segurança ocorre quando há:**

- Vazamento ou perda de dados pessoais ou sensíveis.
- Acesso não autorizado a informações confidenciais.
- Uso indevido de dados por colaboradores ou terceiros.
- Alteração, exclusão ou manipulação indevida de dados.

## AÇÕES IMEDIATAS

**Se houver um incidente de segurança você deve:**

- Relatar o incidente imediatamente ao Encarregado de Proteção de Dados (DPO) ou ao setor de TI.
- Registrar o ocorrido, incluindo data, horário, setor envolvido e descrição do incidente.
- Conter o impacto, suspendendo o acesso ou interrompendo o processo relacionado ao incidente.
- Iniciar a investigação com as equipes responsáveis.

## COMUNICAÇÃO

**Nos casos com risco aos direitos do titular, a ASPP notificará:**

- A Autoridade Nacional de Proteção de Dados (ANPD).
- O titular afetado (se necessário).

# Controle de Documentos e Rastreabilidade

## Gerenciamento de Documentos

### Documentos Físicos:

- Devem ser armazenados em locais seguros.
- O descarte deve ser feito de forma irreversível.

### Documentos Digitais:

- Devem ser protegidos por criptografia.
- Deve-se manter controle de versões e rastreamento de acessos.

## Rastreabilidade

### Documentos Físicos e Digitais:

- Todo documento (físico ou digital) deve conter um registro de movimentação.
- Implementar sistemas de gestão documental que monitorem o fluxo de dados.

## Penalidades e Infrações

1. **Advertência Normal**
   Para infrações leves.
2. **Suspensão Temporária**
   Para casos recorrentes.
3. **Desligamento**
   Para infrações graves.
4. **Medidas Legais**
   Quando houver violação à LGPD.

## Infrações Graves

- **Vazamento ou venda de dados sigilosos.**
- **Não informar incidente de segurança quando havia a obrigação de fazê-lo.**
- **Permitir ou facilitar acessos não autorizados a informações confidenciais.**
- **Manipular indevidamente informações pessoais ou institucionais.**
- **Descumprir intencionalmente normas de privacidade e proteção de dados.**

## Denúncias

A ASPP disponibiliza um canal seguro para denúncias de descumprimento deste Código, de violações à LGPD ou de qualquer incidente de segurança da informação. As denúncias podem ser realizadas de forma anônima ou identificada.

### Tratamento das Denúncias:

- Garantia de confidencialidade ao denunciante.
- Investigação imparcial e criteriosa do caso reportado.
- Acompanhamento do caso pelo setor responsável até sua resolução.

### Acesse o Canal de Denúncias:

**brevenlaw.com/lgpd-aspp**

## Atualização

Este Código será revisado periodicamente pelo Presidente e Diretoria Executiva, em conjunto com o Encarregado de Proteção de Dados (DPO) e o setor Jurídico, para garantir conformidade com legislações e boas práticas.

**Aprovado por:** João Carlos Milani Santos -Presidente da Diretoria Executiva

*Curitiba, janeiro de 2025.*