

Políticas e Normas

Proteção de Dados Pessoais



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANCA E C. TECNOLOGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

Política de Privacidade e Proteção de Dados Pessoais

Sumário

Privacidade e Proteção de Dados Pessoais	2
1. Objetivo	2
2. Princípios da Proteção de Dados Pessoais	2
2.1. Tratamento de Dados Pessoais	3
2.2. Tratamento de Dados Pessoais Sensíveis	3
2.3. Tratamento de Dados Pessoais de Criança ou Adolescente	3
3. Diretrizes de Retenção e Descarte de Dados Pessoais	3
4. Gestão das Relações entre Controlador e Operador	4
5. Transferência Internacional de Dados Pessoais	4
6. Direitos dos Titulares de Dados Pessoais	4
7. Gestão de Incidentes de Segurança da Informação	5
8. Auditorias de Proteção de Dados	5
9. Encarregado de Dados Pessoais (DPO)	5
10. Avaliação de Impacto (RIPD) e Teste de Balanceamento	6
11. Uso de Inteligência Artificial (IA)	6
12. Consequências do Descumprimento	7

Políticas e Normas

Proteção de Dados Pessoais



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANÇA E C. TECNOLÓGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

Privacidade e Proteção de Dados Pessoais

1. Objetivo

Esta Política tem como meta principal guiar a todos sobre como lidar com a privacidade e a proteção de dados pessoais aqui na SGM, devendo ser interpretada de forma integrada à Política de Segurança da Informação, à Política de Resposta a Incidentes de Segurança, à Política de Terceirização, à Política de Auditoria Interna, à Política de Anticorrupção e à Política de Desenvolvimento de Novos Produtos e Serviços.

Você deve observar este documento como referência central para o tratamento de dados pessoais, assegurando que toda coleta, uso, armazenamento, compartilhamento e eliminação de dados ocorra de forma lícita, proporcional, segura, rastreável e alinhada à governança corporativa.

2. Princípios da Proteção de Dados Pessoais

O tratamento de dados pessoais deve seguir alguns princípios fundamentais que orientam as nossas ações como instituição e que também servem de guia para o seu trabalho diário. Você deve tratar dados pessoais de maneira transparente, legítima e não discriminatória, garantindo que os titulares tenham ciência das finalidades do tratamento e de seus direitos, em consonância com os controles de segurança, acesso e rastreabilidade definidos na Política de Segurança da Informação.

Lembre-se: o uso de dados pessoais deve ser limitado ao estritamente necessário para atender finalidades específicas e legítimas, vedado qualquer tratamento excessivo, desproporcional ou desvinculado do propósito original. A retenção e a eliminação de dados devem respeitar critérios institucionais formais, de modo a impedir manutenção indevida de informações e reduzir riscos operacionais, jurídicos e reputacionais.

A exatidão, a integridade, a confidencialidade e a disponibilidade dos dados pessoais devem ser preservadas por meio de medidas técnicas e administrativas adequadas. A responsabilização e a prestação de contas exigem que você mantenha registros compatíveis com auditoria e supervisão institucional.

Políticas e Normas

Proteção de Dados Pessoais



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANÇA E C. TECNOLÓGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

2.1. Tratamento de Dados Pessoais

O tratamento de dados pessoais somente deve ocorrer quando necessário para a execução de contratos, cumprimento de obrigações legais ou regulatórias, exercício regular de direitos ou atendimento de interesses legítimos institucionais, devendo sempre ser avaliado à luz da gestão de riscos e dos controles internos. O tratamento deve ser interrompido ou ajustado sempre que a finalidade original deixar de existir ou se tornar incompatível.

2.2. Tratamento de Dados Pessoais Sensíveis

Dados pessoais sensíveis são aqueles que exigem um cuidado redobrado, como informações sobre saúde, origem racial ou étnica, opiniões políticas, religião, dados genéticos ou biométricos. O tratamento de dados pessoais sensíveis exige cautela reforçada e somente pode ocorrer nas hipóteses estritamente necessárias e autorizadas.

Você deve aplicar controles de segurança, acesso e monitoramento ainda mais rigorosos para essa categoria de dados. É vital saber que qualquer incidente envolvendo dados sensíveis demanda uma resposta com alta prioridade e uma avaliação de impacto muito mais aprofundada.

2.3. Tratamento de Dados Pessoais de Criança ou Adolescente

O tratamento de dados pessoais de crianças ou adolescentes é uma questão extremamente delicada e só é permitido em situações verdadeiramente excepcionais. Nesses casos, é obrigatório obter o consentimento explícito do responsável legal da criança ou adolescente, e todas as ações devem ser guiadas pelo "melhor interesse do titular". Antes de qualquer tratamento, devemos analisar cuidadosamente a necessidade, os riscos envolvidos e as medidas de proteção (salvaguardas) que serão implementadas para garantir a segurança dos dados e o bem-estar dos menores.

3. Diretrizes de Retenção e Descarte de Dados Pessoais

A SGM segue critérios bem definidos para decidir por quanto tempo os dados pessoais devem ser guardados e como devem ser descartados. Esses critérios são baseados no objetivo pelo qual o dado

Políticas e Normas

Proteção de Dados Pessoais



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANCA E C. TECNOLOGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

foi coletado, nas exigências da lei e de regulamentações, e nas necessidades de auditoria e gestão de riscos.

Você deve garantir que os dados pessoais não sejam mantidos por mais tempo do que o necessário. Além disso, o descarte deve ser feito de forma segura, permitindo que se possa rastrear a exclusão, e sempre de acordo com a importância (classificação) da informação. As instruções detalhadas sobre como reter, descartar, eliminar (seja de forma física ou digital) e registrar essas atividades serão fornecidas em um documento complementar específico.

4. Gestão das Relações entre Controlador e Operador

O compartilhamento de dados pessoais com terceiros (operadores) somente pode ocorrer mediante autorização formal, análise prévia de riscos e formalização contratual adequada, conforme a Política de Terceirização. Você deve assegurar que terceiros atuem sob instruções documentadas e estejam sujeitos a controles, auditorias e responsabilização.

5. Transferência Internacional de Dados Pessoais

A transferência de dados pessoais para outros países é uma operação que exige muita atenção, pois diferentes países têm diferentes leis e níveis de proteção. Qualquer transferência internacional de dados pessoais deve ser precedida de uma cuidadosa avaliação sobre o nível de proteção oferecido pelo país e pela organização que receberá os dados. Além disso, é indispensável obter uma autorização específica da instituição antes de realizar a transferência. Todas essas operações devem ser rigorosamente documentadas e rastreáveis para garantir a conformidade e a segurança.

6. Direitos dos Titulares de Dados Pessoais

A SGM garante que as pessoas detentoras dos dados (titulares) possam exercer seus direitos em relação às suas informações. Isso inclui o direito de acessar seus dados, corrigi-los, pedir sua exclusão em certas circunstâncias, ou saber com quem seus dados foram compartilhados, entre outros. Suas solicitações devem ser tratadas de forma segura, serem documentadas e estar em total conformidade com nossos controles de governança e auditoria. É seu dever, como integrante da instituição, colaborar para que esses direitos sejam plenamente respeitados e atendidos.

Políticas e Normas

Proteção de Dados Pessoais



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANÇA E C. TECNOLÓGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

7. Gestão de Incidentes de Segurança da Informação

Um incidente de segurança da informação ocorre quando há um acesso não autorizado, perda, alteração ou divulgação indevida de dados pessoais (ex: um e-mail enviado para a pessoa errada, um dispositivo perdido com dados, um ataque cibernético).

Eventos ou incidentes envolvendo dados pessoais devem ser identificados e comunicados imediatamente e conforme as diretrizes da Política de Resposta a Incidentes de Segurança. A equipe responsável fará uma avaliação humana sobre o impacto do incidente, a necessidade de comunicação aos envolvidos e as medidas corretivas que devem ser tomadas.

Em particular, incidentes que possam acarretar risco ou dano relevante aos titulares de dados serão comunicados à Autoridade Nacional de Proteção de Dados (ANPD) e aos próprios titulares, nos prazos e termos exigidos pela legislação. Se você identificar ou suspeitar de um incidente, comunique-o sem demora ao canal apropriado para que possamos agir rapidamente.

8. Auditorias de Proteção de Dados

A conformidade com esta Política será regularmente verificada por meio de auditorias internas ou realizadas por empresas independentes, seguindo o que estabelece nossa Política de Auditoria Interna. É sua total responsabilidade cooperar plenamente com todas as inspeções e revisões. As auditorias são essenciais para assegurarmos que estamos cumprindo as regras, protegendo os dados de forma eficaz e aprimorando continuamente nossas práticas.

9. Encarregado de Dados Pessoais (DPO)

A SGM designou um Encarregado de Dados Pessoais (DPO), que atua como nosso ponto de contato para a Autoridade Nacional de Proteção de Dados (ANPD) e para os titulares de dados. O DPO é responsável por supervisionar a conformidade com esta Política e com a legislação aplicável, além de atuar como canal de comunicação para quaisquer dúvidas ou preocupações relacionadas à proteção de dados. Você pode contatar o DPO pelo seguinte endereço de e-mail: dpo@embrasi.com.br ou telefone: 11 97333-5179.

Políticas e Normas

Proteção de Dados Pessoais



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANÇA E C. TECNOLÓGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

10. Avaliação de Impacto (RIPD) e Teste de Balanceamento

Para projetos ou operações de tratamento de dados que envolvam alto risco às liberdades civis e aos direitos fundamentais dos titulares, a SGM realizará um Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Da mesma forma, sempre que o tratamento de dados for baseado no nosso "Interesse Legítimo", realizaremos um Teste de Balanceamento.

Esse teste serve para garantir que os interesses da instituição estejam em equilíbrio com os direitos e expectativas dos titulares, assegurando que não haja impacto desproporcional à sua privacidade.

Estes documentos têm como objetivo analisar os riscos envolvidos, as medidas de segurança e mitigação e a conformidade com a legislação, garantindo que a proteção de dados seja considerada desde a concepção (*privacy by design*). Sua cooperação será solicitada nesses processos.

11. Uso de Inteligência Artificial (IA)

O uso de ferramentas de Inteligência Artificial (IA) pode trazer agilidade ao nosso dia a dia, mas exige cuidados fundamentais para proteger a privacidade e a segurança dos dados. Ao utilizar qualquer ferramenta de IA, você deve seguir estas diretrizes obrigatórias:

- É terminantemente proibido inserir dados pessoais (de clientes, colegas ou parceiros) ou informações confidenciais da SGM em ferramentas de IA públicas ou não autorizadas. Lembre-se: as informações inseridas nessas ferramentas podem se tornar públicas ou ser usadas para treinar outros sistemas.
- Todo conteúdo gerado por IA deve passar por uma revisão humana cuidadosa antes de ser utilizado. A IA pode apresentar informações incorretas, imprecisas ou enviesadas (alucinações), e a responsabilidade final pelo trabalho realizado é sempre do colaborador.
- O uso da IA deve ser ético e transparente, garantindo que os resultados não gerem qualquer tipo de discriminação ou tratamento injusto.
- Utilize apenas as ferramentas de IA que foram formalmente aprovadas pela nossa equipe de TI e Segurança da Informação. Se tiver dúvidas sobre a segurança de uma ferramenta, consulte o DPO ou o gestor responsável antes de usá-la.

Políticas e Normas

Proteção de Dados Pessoais



ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	DATA DE PUBLICAÇÃO: 16 DE JULHO DE 2026	REVISÃO: ANUAL
AUTOR: EMBRASI GOVERNANCA E C. TECNOLOGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		CNPJ: 00.306.499/0001-60

12. Consequências do Descumprimento

O não cumprimento das diretrizes estabelecidas nesta Política ou na legislação de proteção de dados poderá acarretar sanções disciplinares, sem prejuízo das responsabilidades civis e criminais que possam ser imputadas ao infrator, à SGM e aos seus colaboradores.