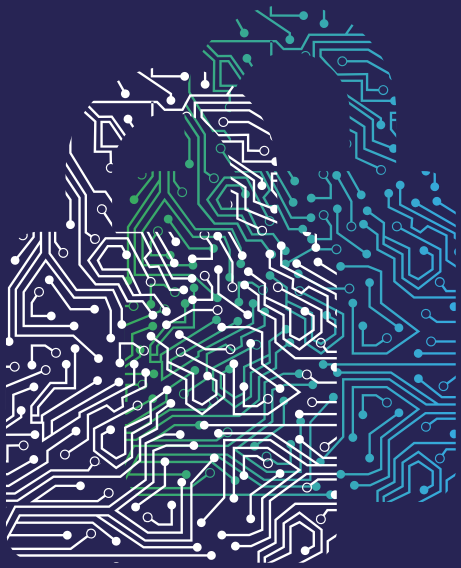
Por dentro da LGPD

E a sua aplicação na ALESP



Alesp 190 anos

Por dentro da LGPD

E a sua aplicação na ALESP

Sumário

Por que preciso conhecer a LGPD?

A LGPD faz parte do seu trabalho diário

Como servidor da Alesp, você lida com dados pessoais constantemente, mesmo que não perceba:

- Ao atender cidadãos no balcão ou por telefone;
- Ao receber documentos com informações de pessoas;
- Ao manter registros de visitantes;
- Ao acessar sistemas institucionais;
- Ao compartilhar informações entre departamentos;
- Ao manipular dados de outros servidores.

Todos esses dados precisam ser protegidos conforme a LGPD.

Responsabilidades legais e institucionais

De acordo com o **Ato da Mesa nº 10 de 2023**, todos os servidores da Alesp devem:

- Conhecer e aplicar as diretrizes da LGPD;
- Comunicar ao Encarregado de Dados possíveis violações a LGPD;
- Adotar medidas para proteger os dados sob sua responsabilidade.

Consequências do descumprimento

O descumprimento da LGPD pode gerar:

Para você, servidor:

- Responsabilização administrativa;
- Processos disciplinares;
- Responsabilidade pessoal pelos danos materiais e morais causados.

Para a Alesp:

- Advertências e multas aplicadas pela ANPD;
- Suspensão de atividades de tratamento de dados;
- Bloqueio dos dados pessoais;
- Perda de confiança pública.

Para os cidadãos:

- Exposição indevida de informações pessoais;
- Discriminação baseada em dados sensíveis;
- Prejuízos morais e materiais;
- Vulnerabilidade a fraudes e crimes.

A proteção de dados não é apenas uma obrigação legal, mas um compromisso ético com a cidadania e a transparência pública.

O que é a LGPD e quando ela se aplica?

Contexto histórico e definição

A **Lei Geral de Proteção de Dados (Lei nº 13.709/2018)** é um marco legal que regulamenta o tratamento de dados pessoais no Brasil, inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia.

Foi aprovada em agosto de 2018 a LGPD (Lei Geral de Proteção de Dados).

Entrou em vigor em setembro de 2020.

Teve sanções aplicáveis a partir de agosto de 2021.

Em 2022 a Autoridade Nacional de Proteção de Dados (ANPD) se transforma em autarquia de natureza especial.

Objetivos da LGPD

A LGPD tem como principais objetivos:

- Proteger os direitos fundamentais de liberdade e privacidade;
- Garantir o livre desenvolvimento da personalidade da pessoa natural;
- Estabelecer regras claras sobre o tratamento de dados pessoais;
- Fomentar o desenvolvimento econômico e tecnológico;
- Fortalecer a confiança e segurança nas relações entre cidadãos e organizações.

Aplicabilidade da lei

A LGPD SE APLICA A:

- Operações de tratamento realizadas no território nacional;
- Dados pessoais coletados no Brasil;
- Tratamento que tenha por objetivo a oferta de produtos/serviços no Brasil;
- Dados de pessoas localizadas no território nacional.

Independentemente de:

- Meio utilizado (físico ou digital);
- País da sede da organização;
- Natureza dos dados (públicos ou privados).

A LGPD NÃO SE APLICA A DADOS:

- Tratados por pessoa natural para fins exclusivamente particulares;
- Para fins exclusivamente jornalísticos e artísticos;
- Para fins exclusivos de segurança pública, defesa nacional ou segurança do Estado;
- Provenientes de fora do território nacional e que não sejam objeto de comunicação ou compartilhamento com agentes brasileiros.

Quem são os agentes de tratamento de dados?

Titular de Dados

Quem é: A pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Na prática: Cidadãos que interagem com a Alesp, visitantes, servidores, fornecedores, parlamentares.

Exemplo: Maria Silva, que enviou um e-mail solicitando informações sobre um projeto de lei.

Controlador

Quem é: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Na prática: A Alesp como instituição é o controlador dos dados que coleta e processa.

Exemplo: Quando a Alesp decide implementar um sistema de cadastro de visitantes e define quais dados serão coletados.

Operador

Quem é: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Na prática: Empresas terceirizadas que processam dados sob instrução da Alesp.

Exemplo: Empresa contratada para gerenciar o sistema biométrico de acesso ao prédio da Alesp.

Entidade e Autoridades

ANPD (Autoridade Nacional de Proteção de Dados):

- Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD;
- Pode aplicar sanções em caso de descumprimento da lei.

Entidades Reguladoras Setoriais:

- Podem emitir regulamentações específicas para seus setores, em cooperação com a ANPD e obedecendo a LGPD.

Exemplo: BACEN, SUSEP, ANATEL.

Outros órgãos públicos:

- Recebedores de dados por obrigação legal;

Exemplo: INSS, Receita Federal, Tribunais.

Encarregado de Dados (DPO)

Quem é: Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares e a ANPD.

Na prática: Na Alesp, o Encarregado está na Coordenadoria de Governança e Conformidade.

Responsabilidades:

- Aceitar reclamações e comunicações dos titulares;
- Orientar os funcionários sobre práticas de proteção de dados;
- Executar as demais atribuições determinadas pelo controlador;
- Comunicar-se com a ANPD.

Dados pessoais: o que são e como identificá-los

Definição de dados pessoais

Segundo o Art. 5º, inciso I da LGPD, **dado pessoal** é:

> *"Informação relacionada a pessoa natural identificada ou identificável."*

São dados que, sozinhos ou combinados com outros, permitem identificar uma pessoa específica.

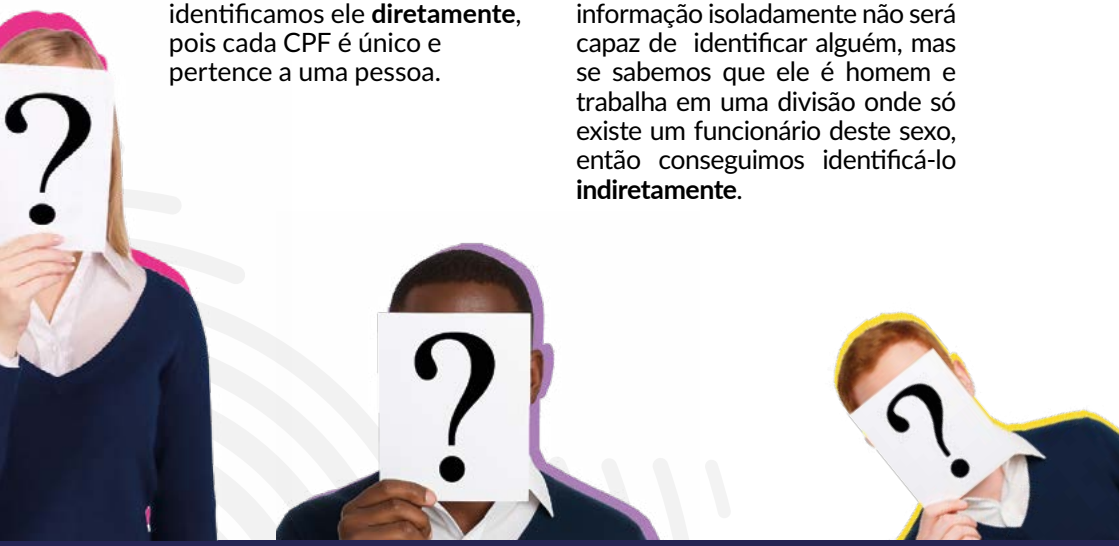
Métodos de identificação

Identificação direta: Dados que identificam uma pessoa de forma imediata e inequívoca.

Exemplo: Se sabemos o CPF de um servidor da Alesp, identificamos ele **diretamente**, pois cada CPF é único e pertence a uma pessoa.

Identificação indireta: Dados que identificam uma pessoa de forma imediata e inequívoca.

Exemplo: Se sabemos que o gênero de um servidor é masculino, esta informação isoladamente não será capaz de identificar alguém, mas se sabemos que ele é homem e trabalha em uma divisão onde só existe um funcionário deste sexo, então conseguimos identificá-lo **indiretamente**.



Exemplos comuns no ambiente da Alesp

Tipo de Documento	Dados Pessoais Presentes
Ofícios	Nome, cargo, contatos
Processos administrativos	CPF, endereço, histórico funcional
Listas de presença	Nome, assinatura, horário
Cadastros de visitantes	RG, foto, horário de entrada/saída
E-mails institucionais	Nome, contatos, conteúdo das comunicações
Contracheques	Nome, matrícula, dados bancários, salário

Dados pessoais x Dados anonimizados

Dados anonimizados: São dados que perderam a possibilidade de associação com uma pessoa específica, utilizando meios técnicos razoáveis e disponíveis.

Exemplo de anonimização:

Dado pessoal

"João Silva, 45 anos, servidor desde 2005, lotado na Diretoria de TI".

Dado anonimizado

"Servidor da área técnica, faixa etária 40-50 anos, tempo de serviço entre 15-20 anos".

Importante: A LGPD não se aplica a dados anonimizados, exceto quando o processo de anonimização for reversível ou quando for usado para gerar comportamentos discriminatórios.

Dados sensíveis: cuidados especiais

O que são dados sensíveis?

Conforme o Art. 5º, inciso II da LGPD, **dado pessoal sensível** é:

> *"Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural."*

Por que merecem proteção especial?

Os dados sensíveis:

- Podem levar à discriminação se usados indevidamente;
- Referem-se a aspectos íntimos da personalidade e da vida privada;
- Seu vazamento pode causar danos mais graves aos titulares;
- Têm potencial para afetar direitos fundamentais.

Exemplos de dados sensíveis no contexto da Alesp

Saúde:
Atestados médicos, prontuários, histórico de doenças, exames.

Biometria:
Impressão digital para acesso, reconhecimento facial.

Orientação sexual:
Declarações para inclusão de dependentes, licenças.

Religião:
Solicitações de horários especiais para práticas religiosas.

Origem racial/étnica:
Autodeclarações para políticas de diversidade.

Filiação sindical:
Registros de filiação, descontos em folha para sindicatos.

Opinião política:
Filiação partidária, posicionamentos políticos.

X

Dados Pessoais "Comuns"	Dados Pessoais Sensíveis
Nome completo	Registro de saúde mental
Endereço residencial	Classificação Estatística Internacional de Doenças e Problemas Relacionados com a Saúde (CID)
Número de telefone	Tipo sanguíneo
Data de nascimento	Orientação sexual
Endereço de e-mail	Convicções religiosas
Número de matrícula	Filiação partidária
Formação acadêmica	Dados de impressão digital
Histórico profissional	Reconhecimento facial
Dados bancários	Dados genéticos
Placa de veículo	Origem racial/étnica

ATENÇÃO:

1. Dados de saúde ocupacional são considerados sensíveis pela LGPD;
2. Dados de remuneração, embora delicados, não são classificados como sensíveis pela lei;
3. Dados de crianças e adolescentes, mesmo não sensíveis, recebem proteção especial.

Os 10 princípios fundamentais da LGPD

A LGPD estabelece 10 princípios que devem orientar todas as atividades de tratamento de dados pessoais. Estes princípios estão definidos no Art. 6º da lei.

1. Finalidade

O que é: Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular.

Na prática:

- Defina claramente por que você está coletando os dados;
- Informe ao titular para que os dados serão usados;
- Não use os dados para finalidades diferentes das informadas.

Exemplo na Alesp: Os dados coletados para cadastro de visitantes devem ser usados apenas para controle de acesso, não é permitido a utilização desses dados para outra finalidade.

2. Adequação

O que é: Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Na prática:

- O tratamento deve ser coerente com o que foi informado;
- Considere o contexto e as expectativas razoáveis do titular.

Exemplo na Alesp: Se você coletou dados para emissão de crachá temporário, não é adequado usar esses dados para criar um perfil de comportamento do visitante.

3. Necessidade

O que é: Limitação do tratamento ao mínimo necessário para a realização de suas finalidades.

Na prática:

- Colete apenas os dados essenciais para a finalidade;
- Não pense em “irei coletar esses outros dados por via das dúvidas”;
- Questione: “Preciso realmente deste dado?”.

Exemplo na Alesp: Para acesso a um evento público na Alesp, é necessário nome e documento de identidade, mas não endereço completo ou profissão.

4. Livre acesso

O que é: Garantia de consulta facilitada e gratuita pelos titulares sobre o tratamento de seus dados.

Na prática:

- Possibilite que as pessoas consultem seus dados facilmente;
- Não cobre por esse acesso;
- Forneça informações completas sobre o tratamento.

Exemplo na Alesp: Implementar canal específico para que cidadãos possam solicitar acesso aos seus dados pessoais mantidos pela instituição.

5. Qualidade dos dados

O que é: Garantia de exatidão, clareza, relevância e atualização dos dados.

Na prática:

- Mantenha os dados precisos e atualizados;
- Corrija prontamente informações inexatas;
- Estabeleça processos de verificação periódica.

Exemplo na Alesp: Revisão periódica dos cadastros de servidores para garantir que informações como endereço e contatos estejam atualizadas.

6. Transparência

O que é: Garantia de informações claras, precisas e facilmente acessíveis sobre o tratamento de dados.

Na prática:

- Comunique de forma simples e direta;
- Evite linguagem técnica ou jurídica excessiva;
- Disponibilize informações visíveis e acessíveis.

Exemplo na Alesp: Política de privacidade no site institucional e avisos claros nos formulários de coleta de dados.

7. Segurança

O que é: Utilização de medidas técnicas e administrativas para proteger os dados de acessos não autorizados e situações acidentais ou ilícitas

Na prática:

- Implemente controles de acesso aos sistemas;
- Utilize criptografia quando necessário;
- Faça backup regular dos dados;
- Estabeleça políticas de segurança da informação.

Exemplo: Necessidade de implementação de login com múltiplos fatores para acesso a sistemas com dados sensíveis.

8. Prevenção

O que é: Adoção de medidas para prevenir danos em virtude do tratamento de dados.

Na prática:

- Antecipe possíveis problemas;
- Realize avaliações de risco;
- Implemente controles preventivos.

Exemplo na Alesp: Realizar análise de impacto antes de implementar novo sistema de coleta de dados biométricos.

9. Não discriminação

O que é: Impossibilidade de tratamento de dados para fins discriminatórios, ilícitos ou abusivos.

Na prática:

- Não use dados para prejudicar pessoas;
- Evite decisões automatizadas que possam gerar exclusão;
- Verifique se algoritmos não causam discriminação indireta.

Exemplo na Alesp: Não utilizar dados de origem étnica, religião ou opinião política para diferenciação no atendimento aos cidadãos.

10. Responsabilização e prestação de contas

O que é: Demonstração da adoção de medidas eficazes para cumprir as normas de proteção de dados.

Na prática:

- Documente processos relacionados a dados pessoais;
- Mantenha registros das operações de tratamento;
- Demonstre conformidade quando solicitado.

Exemplo: Manter registros das operações de tratamento, documentar políticas de segurança e realizar auditorias periódicas.

Bases legais: quando é permitido usar dados pessoais?

A LGPD determina que o tratamento de dados pessoais só pode ocorrer quando fundamentado em uma das bases legais previstas no Art. 7º:

1. Consentimento

O que é: Manifestação livre, informada e inequívoca do titular concordando com o tratamento de seus dados para uma finalidade determinada.

Na prática:

- Deve ser específico para uma finalidade;
- Precisa ser obtido previamente ao tratamento;
- Deve ser livre de vícios, condicionamentos ou coações;
- Pode ser revogado a qualquer momento.

Exemplo na Alesp: Formulário para inscrição em newsletter da Alesp, com caixa de seleção específica para autorizar o uso do e-mail.

2. Obrigação legal ou regulatória

O que é: Tratamento necessário para cumprir uma obrigação legal ou regulatória a que o controlador está sujeito.

Na prática:

- A lei ou regulamento deve exigir especificamente o tratamento;
- Não depende do consentimento do titular;
- Limitado ao necessário para cumprir a obrigação.

Exemplo na Alesp: Para cumprimento do Ato de Mesa nº 06 de 2020, a Alesp publica em seu portal a lista com nome do servidor e a sua respectiva remuneração.

3. *Execução de políticas públicas*

O que é: Tratamento necessário para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos ou convênios.

Características:

- Aplicável à administração pública;
- Deve ser para finalidades específicas e legítimas;
- Requer transparência sobre a política pública em questão.

Exemplo na Alesp: Coleta de dados para a implementação de programas de participação popular na formulação de projetos de lei.

4. *Realização de estudos e pesquisas*

O que é: Tratamento para estudos por órgão de pesquisa, garantindo, sempre que possível, a anonimização dos dados.

Características:

- Realizado por órgãos de pesquisa reconhecidos;
- Preferencialmente com dados anonimizados;
- Para finalidade acadêmica ou estatística.

Exemplo na Alesp: Disponibilização de dados anonimizados sobre participação popular em audiências públicas para pesquisadores universitários.

5. *Execução de contrato*

O que é: Tratamento necessário para a execução de contrato ou procedimentos preliminares relacionados a contrato do qual seja parte o titular.

Características:

- O titular deve ser parte no contrato;
- Limitado aos dados necessários para cumprir as obrigações contratuais;
- Inclui a fase pré-contratual a pedido do titular.

Exemplo na Alesp: Coleta de dados bancários de fornecedores para efetuar pagamentos previstos em contrato.

6. *Exercício regular de direitos*

O que é: Tratamento necessário para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Características:

- Inclui processos judiciais, administrativos e arbitrais;
- Aplicável a procedimentos prévios, durante e após processo;
- Limitado aos dados relevantes para o caso.

Exemplo na Alesp: Coleta e armazenamento de documentos com dados pessoais para defender a instituição em ação trabalhista.

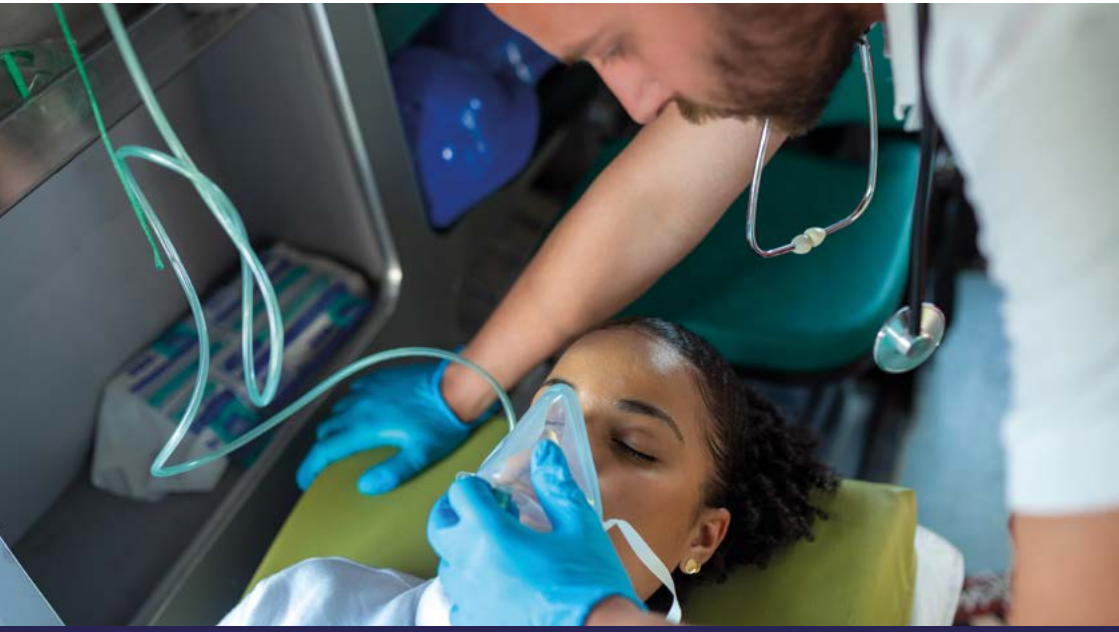
7. Proteção da vida

O que é: Tratamento necessário para a proteção da vida ou da incolumidade física do titular ou de terceiro.

Características:

- Situações de emergência ou risco à saúde/vida, nas quais o Titular está incapacitado de manifestar o seu consentimento;
- Limitado ao necessário para a proteção.

Exemplo na Alesp: Acesso a informações médicas de visitante que passa mal durante visita ao prédio para informar à equipe de emergência.



8. Tutela da saúde

O que é: Tratamento necessário para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Características:

- Exclusivo para procedimentos de saúde;
- Realizado por profissionais ou instituições de saúde;
- Sujeito ao sigilo profissional.

Exemplo na Alesp: Coleta de dados de saúde por profissionais da Divisão Médica para realização de exames periódicos dos servidores.

9. Legítimo interesse

O que é: Tratamento necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto quando prevalecerem direitos e liberdades fundamentais do titular.

Características:

- Requer teste de balanceamento de interesses;
- Deve ser para finalidades legítimas e específicas;
- Exige transparência sobre o interesse legítimo.

Exemplo na Alesp: Monitoramento por câmeras de segurança para proteção do patrimônio público e segurança das pessoas.

10. Proteção ao crédito

O que é: Tratamento necessário para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Características:

- Específico para relações de crédito;
- Deve seguir legislação específica (como Código de Defesa do Consumidor);
- Inclui prevenção à fraude e segurança do titular.

Exemplo na Alesp: Verificação de dados para evitar fraudes em contratos de crédito consignado para servidores.

Tratamento de dados sensíveis e dados de menores

Dados sensíveis: regras específicas

Devido à sua natureza especial, os dados sensíveis possuem regras mais restritivas para tratamento, conforme Art. 11 da LGPD:

Hipóteses para tratamento de dados sensíveis:

Com consentimento específico e destacado:

- O consentimento deve ser para finalidades específicas
- Precisa ser destacado das demais autorizações
- Deve informar claramente as consequências do tratamento

Sem consentimento, apenas nas seguintes situações:

- Para cumprimento de obrigação legal ou regulatória
- Para execução de políticas públicas
- Para estudos por órgão de pesquisa (preferencialmente anonimizados)
- Para exercício regular de direitos em processos
- Para proteção da vida ou incolumidade física
- Para garantia da segurança do titular em sistemas eletrônicos
- Para tutela da saúde, por profissionais da área
- Para garantia da prevenção à fraude nos processos de identificação e autenticação

Exemplo na Alesp:

Dados biométricos só podem ser coletados para controle de acesso se houver consentimento específico ou previsão legal que obrigue essa coleta.

Dados de menores de idade: proteção especial

A LGPD dedica atenção especial à proteção de dados de crianças e adolescentes (menores de 18 anos):

Requisitos para tratamento de dados de menores (Art. 14):

1

Consentimento específico por pelo menos um dos pais ou responsável legal.

- O consentimento deve ser verificável;
- Deve ser para finalidade específica e no melhor interesse do menor.

2

Informações claras e acessíveis:

- Sobre o tipo de dados coletados;
- Sobre como serão utilizados;
- Sobre os direitos do titular e responsável.

3

Exceção para contato único:

- É permitida coleta de dados de contato (como telefone) uma única vez e sem armazenamento, exclusivamente para contatar os pais ou responsável legal;
- Os dados não podem ser repassados a terceiros sem consentimento.

4

Princípio do melhor interesse:

- O tratamento deve considerar prioritariamente o melhor interesse da criança/adolescente;
- Não devem ser solicitados dados excessivos.

Exemplo na Alesp:

Para visitas escolares, o responsável pelo grupo deve apresentar autorização dos pais para registro fotográfico dos menores.

Fluxo para tratamento de dados de menores:

1. Identificar se os dados são de pessoas menores de 18 anos;
2. Obter consentimento específico de ao menos um dos pais ou responsável legal;
3. Registrar o consentimento obtido;
4. Verificar se o tratamento é no melhor interesse do menor;
5. Adotar medidas de segurança adequadas;
6. Informar de forma transparente e acessível sobre o tratamento.

ATENÇÃO:

1. Não trate dados de menores sem consentimento dos responsáveis (exceto para contato único);
2. Não armazene ou repasse dados de menores obtidos sem consentimento;
3. Em caso de dúvida, consulte o Encarregado de Dados da Alesp.

Ciclo de vida dos dados: do início ao término do tratamento

Fases do tratamento de dados pessoais

1. Coleta

- Obtenção dos dados diretamente do titular ou de terceiros;
- Deve ser baseada em uma das bases legais da LGPD;
- Deve informar a finalidade e forma de tratamento.

2. Armazenamento

- Guarda dos dados em sistemas físicos ou digitais;
- Requer medidas de segurança adequadas;
- Deve observar o prazo necessário para a finalidade.

3. Processamento

- Operações realizadas com os dados;
- Inclui classificação, modificação, uso;
- Deve respeitar a finalidade informada.

4. Compartilhamento

- Transferência dos dados para terceiros;
- Requer base legal específica;
- Exige contratos ou termos com os recipientes.

5. Eliminação

- Exclusão dos dados após cumprimento da finalidade;
- Pode ser solicitada pelo titular em certos casos;
- Deve ser feita de forma segura e completa.

Término do tratamento de dados

Segundo o Art. 15 da LGPD, o tratamento de dados pessoais deve ser encerrado nas seguintes hipóteses:

1. Verificação de que a finalidade foi alcançada

Quando o objetivo para o qual os dados foram coletados foi atingido.

Exemplo: Dados de visitante após término da visita.

2. Fim do período de tratamento

Quando o período predeterminado para o tratamento chega ao fim.

Exemplo: Dados de um evento após sua conclusão e período de avaliação.

3. Comunicação do titular

Quando o titular revoga o consentimento (se esta for a base legal).

Exemplo: Cidadão solicita remoção da lista de e-mails.

4. Determinação da autoridade nacional

Quando a ANPD determinar o fim do tratamento.

Exemplo: Ordem específica para cessar determinada atividade.

Obrigação de eliminação dos dados

Após o término do tratamento, os dados pessoais devem ser eliminados, exceto nos seguintes casos:

1. Cumprimento de obrigação legal ou regulatória

Quando a lei exige a manutenção dos dados.

Exemplo: Dados de visitante após término da visita.

2. Estudo por órgão de pesquisa

Para uso exclusivo em pesquisas, preferencialmente anonimizados.

Exemplo: Dados históricos para estudos estatísticos.

3. Transferência a terceiros

Desde que respeitados os requisitos de tratamento da LGPD.

Exemplo: Transferência legítima para prestador de serviços.

4. Uso exclusivo do controlador

Dados anonimizados para uso interno.

Exemplo: Ordem específica para cessar determinada atividade.

Retenção de dados

A definição dos prazos de retenção na ALESP deve considerar principalmente a Tabela de Temporalidade (em caso de dúvidas, contate a Divisão de Gestão Documental):

Exemplo de documento	Base legal para retenção	Prazo típico
Ficha de Inscrição para curso interno	Anexo I do Ato de Mesa nº 08/25 Alesp	2 anos
Formulário de Levantamento de Necessidades de Treinamento	Anexo I do Ato de Mesa nº 08/25 Alesp	2 anos
Formulário de Solicitação de Sistema	Anexo I do Ato de Mesa nº 08/25 Alesp	2 anos
Solicitação de Reembolso de Auxílio Saúde	Anexo I do Ato de Mesa nº 08/25 Alesp	5 anos a partir da decisão final do benefício
Prontuário Funcional	Anexo I do Ato de Mesa nº 08/25 Alesp	100 anos
Solicitação de Reembolso de auxílio pré-escolar	Anexo I do Ato de Mesa nº 08/25 Alesp	5 anos a partir da decisão final do benefício

BOAS PRÁTICAS:

1. Documente a base legal para retenção de cada tipo de dado;
2. Implemente processos de eliminação automática após o prazo;
3. Revise periodicamente a necessidade de manutenção dos dados;
4. Verifique se não há meios menos invasivos para atingir a mesma finalidade.

Direitos dos titulares: o que os cidadãos podem solicitar

A LGPD estabelece diversos direitos aos titulares de dados, que devem ser atendidos pelos controladores. Estes direitos estão previstos principalmente no Art. 18.

1. Confirmação da existência de tratamento

O que é: Direito de saber se o controlador possui e trata seus dados pessoais.

Como atender:

- Responder de forma clara e completa;
- Informar se realiza ou não tratamento de dados do solicitante;
- Prazo: imediato (for mato simplificado) ou 15 dias (declaração completa).

Exemplo na Alesp: O cidadão pergunta se seus dados estão registrados nos sistemas da Alesp após participação em audiência pública.

2. *Acesso aos dados*

O que é: Direito de obter cópia dos dados pessoais que estão sendo tratados.

Como atender:

- Fornecer cópia integral dos dados em formato acessível;
- Incluir informações sobre fonte dos dados, quando não coletados diretamente;
- Prazo: 15 dias da solicitação.

Exemplo na Alesp: Servidor solicita cópia de todos os seus dados armazenados no departamento de recursos humanos.

3. *Correção de dados incompletos, inexatos ou desatualizados*

O que é: Direito de solicitar a atualização ou correção de dados incorretos.

Como atender:

- Corrigir prontamente as informações;
- Notificar agentes com quem os dados foram compartilhados;
- Informar ao titular sobre a correção.

Exemplo na Alesp: Cidadão solicita correção de seu nome que foi cadastrado com erro de grafia em sistema de atendimento.

4. Anonimização, bloqueio ou eliminação

O que é: Direito de solicitar que dados excessivos, desnecessários ou tratados em desconformidade com a LGPD sejam anonimizados, bloqueados ou eliminados.

Como atender:

- Analisar a conformidade e necessidade dos dados;
- Proceder com a medida solicitada quando cabível;
- Justificar caso não seja possível atender (por exemplo, por obrigação legal).

Exemplo na Alesp: Visitante solicita eliminação de seus dados biométricos após visita única à instituição.

5. Portabilidade dos dados

O que é: Direito de receber seus dados em formato estruturado para transferir a outro fornecedor de serviço ou produto.

Como atender:

- Fornecer os dados em formato interoperável e estruturado;
- Facilitar a transferência para outro controlador;
- Assegurar a segurança das informações no processo.

Exemplo na Alesp: Funcionário solicita seus dados funcionais para apresentar em outro órgão público.

6. Informação sobre compartilhamento

O que é: Direito de saber com quais entidades públicas e privadas o controlador compartilhou seus dados.

Como atender:

- Listar todas as entidades que receberam os dados;
- Informar a base legal e finalidade do compartilhamento;
- Manter registro atualizado de compartilhamentos.

Exemplo na Alesp: O cidadão pergunta quais órgãos tiveram acesso aos dados fornecidos em cadastro de programa institucional.

7. Informação sobre consentimento

O que é: Direito de ser informado sobre a possibilidade de não fornecer consentimento e sobre as consequências disso.

Como atender:

- Informar claramente se o fornecimento do dado é obrigatório ou opcional;
- Explicar as consequências do não consentimento;
- Não condicionar serviços essenciais ao consentimento.

Exemplo na Alesp: Informar claramente que o não fornecimento de e-mail para newsletter não impede o acesso a outros serviços da Alesp

8. Revogação do consentimento

O que é: Direito de revogar o consentimento a qualquer momento, mediante manifestação expressa.

Como atender:

- Disponibilizar mecanismo simples e gratuito para revogação;
- Cessar o tratamento após a revogação (salvo outras bases legais);
- Informar claramente como revogar o consentimento.

Exemplo na Alesp: Link de descadastramento em todas as comunicações por e-mail enviadas pela instituição.

Prazos para atendimento

- **Formato simplificado:** Resposta imediata
- **Declaração completa:** 15 dias da solicitação do titular
- **Correção, eliminação, anonimização:** Sem prazo específico (recomenda-se 15 dias)
- **Demais solicitações:** Prazo razoável (recomenda-se até 15 dias)

Canais para exercício dos direitos

A Alesp deve disponibilizar canais para que os titulares possam exercer seus direitos:

- **Portal da Alesp:** Formulário específico para solicitações relacionadas à LGPD
- **E-mail dedicado:** cgc@al.sp.gov.br
- **Presencialmente:** Na Coordenadoria de Governança e Conformidade, Sala M26, Andar Monumental
- **Correspondência:** Endereçada ao Encarregado de Dados da Alesp

ATENÇÃO!

Todas as solicitações dos titulares devem ser:

- Registradas em sistema próprio
- Encaminhadas ao setor responsável
- Respondidas dentro do prazo
- Reportadas ao Encarregado de Dados

Transferência internacional de dados

O que é transferência internacional?

Transferência internacional de dados é o envio de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Isso pode ocorrer quando:

- Dados são armazenados em servidores localizados em outros países;
- Informações são compartilhadas com empresas ou órgãos internacionais;
- Sistemas ou aplicativos utilizados processam dados fora do Brasil.

Requisitos para transferência internacional

Segundo o Art. 33 da LGPD, a transferência internacional de dados só é permitida nas seguintes hipóteses:

1. **Para países com nível adequado de proteção**
   - Países que possuem legislação compatível com a LGPD;
   - Determinados pela ANPD.
2. **Mediante garantias específicas**
   - Cláusulas contratuais específicas para a transferência;
   - Cláusulas-padrão contratuais;
   - Normas corporativas globais (binding corporate rules);
   - Selos, certificados e códigos de conduta aprovados.
3. **Com base em derrogações específicas**
   - Consentimento específico e destacado do titular;
   - Execução de contrato no interesse do titular;
   - Proteção da vida ou incolumidade física do titular;

- Autorização da ANPD;
- Compromisso internacional de cooperação;
- Execução de política pública;
- Cumprimento de obrigação legal;
- Exercício regular de direitos em processo judicial.

Riscos da transferência internacional

A transferência internacional pode apresentar riscos:

- **Jurisdições com baixa proteção:** Países sem leis adequadas de proteção de dados;
- **Dificuldade de fiscalização:** Menor controle sobre como os dados são tratados;
- **Conflito de leis:** Diferentes jurisdições podem ter regras conflitantes;
- **Acesso governamental:** Alguns países permitem acesso amplo a dados por autoridades;
- **Dificuldade de exercício de direitos:** Titulares podem encontrar barreiras para exercer seus direitos.

Importante: A Alesp não recomenda o uso de serviços de comunicação, armazenamento ou processamento não institucionais que possam enviar dados para fora do Brasil sem as garantias adequadas.

Recomendações para transferência internacional na Alesp

Diretrizes para servidores da Alesp:

1. **Evite usar serviços de armazenamento em nuvem não aprovados.**
   - Não utilize serviços pessoais como Google Drive, Dropbox ou OneDrive para dados institucionais;
   - Use apenas soluções aprovadas pelo departamento de TI.
2. **Verifique a localização do processamento de dados.**
   - Antes de contratar serviços ou sistemas, verifique onde os dados serão armazenados;
   - Prefira soluções que mantenham os dados no Brasil.
3. **Consulte o Encarregado de Dados.**
   - Antes de enviar dados para fora do Brasil, consulte o Encarregado;
   - Obtenha orientação sobre requisitos legais e procedimentos.
4. **Realize avaliação de impacto.**
   - Para transferências significativas, realize avaliação de impacto;
   - Considere riscos e medidas mitigatórias.
5. **Documente adequadamente.**
   - Mantenha registro de todas as transferências internacionais;
   - Documente as garantias e salvaguardas aplicadas.

Boas práticas no ambiente de trabalho

Proteção de dados no dia a dia

Como servidor da Alesp, você pode adotar medidas práticas para proteger os dados pessoais:

1. Segurança física

- **Mesa limpa**
  - Não deixe documentos com dados pessoais expostos sobre a mesa;
  - Guarde documentos em gavetas ou armários com chave ao se ausentar;
  - Descarte documentos utilizando fragmentadoras de papel.

- **Controle de acesso físico**
  - Não permita que pessoas não autorizadas acessem áreas restritas;
  - Utilize crachá de identificação visível;
  - Acompanhe visitantes em áreas com documentos sensíveis.

- **Proteção de telas**
  - Posicione monitores para evitar visualização por terceiros;
  - Use protetor de tela com senha para bloqueio automático;

- Bloqueie manualmente o computador ao se ausentar (Win+L).

2. Segurança digital

Senhas fortes

- Use senhas complexas (letras, números e caracteres especiais);
- Não compartilhe suas credenciais de acesso;
- Utilize gerenciadores de senha aprovados pela instituição.

E-mail e comunicações

- Verifique sempre o destinatário antes de enviar e-mails com dados pessoais;
- Evite encaminhar e-mails em cadeia com dados pessoais;
- Utilize criptografia ou proteção por senha para arquivos sensíveis.

Uso de sistemas e dispositivos

- Utilize apenas softwares autorizados pela instituição;
- Não instale programas sem autorização da TI;
- Mantenha sistemas e antivírus atualizados.

3. Comportamento seguro

Minimização de dados

- Solicite apenas os dados necessários para cada atividade;
- Não crie bancos de dados paralelos não autorizados;
- Questione a necessidade de cada dado coletado.

Descarte seguro

- Utilize fragmentadoras para documentos físicos;
- Solicite à TI apoio para descarte seguro de mídias digitais;
- Não descarte documentos com dados pessoais em lixo comum.

Comunicação cuidadosa

- Evite discutir informações pessoais em locais públicos;
- Não compartilhe dados de terceiros em redes sociais;
- Tenha cuidado com ligações telefônicas em viva-voz.

Dicas de segurança digital

Ação	Risco	Prática segura
Uso de senhas	Invasão de contas	Use senhas fortes, diferentes para cada serviço e troque-as periodicamente
Anexos de e-mail	Malware e phishing	Não abra anexos suspeitos ou de remetentes desconhecidos
Uso de dispositivos pessoais	Mistura de dados pessoais e profissionais	Separe dispositivos ou use perfis diferentes
Acesso a sistemas	Vazamento de credenciais	Encerre a sessão ao terminar de usar sistemas
Armazenamento de arquivos	Perda ou vazamento de dados	Use apenas sistemas institucionais aprovados
Compartilhamento de informações	Exposição indevida	Verifique duas vezes antes de compartilhar

Lista de verificação diária

- ✓ Bloqueei meu computador ao me ausentar?
- ✓ Guardei documentos físicos em local seguro?
- ✓ Verifiquei os destinatários antes de enviar e-mails?
- ✓ Utilizei apenas sistemas autorizados pela instituição?
- ✓ Descartei documentos com dados pessoais de forma segura?
- ✓ Compartilhei dados apenas com pessoas autorizadas?
- ✓ Coletei apenas os dados necessários para minha atividade?

O que fazer em caso de incidente

O que é um incidente de segurança?

Incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança que leve à destruição, perda, alteração, vazamento ou acesso não autorizado a dados pessoais.

Tipos comuns de incidentes

- **Acesso não autorizado:** Invasão de sistemas, acesso indevido a documentos;
- **Vazamento de dados:** Divulgação não autorizada de informações pessoais;
- **Perda ou roubo:** Desaparecimento de documentos, dispositivos ou mídias;
- **Alteração indevida:** Modificação não autorizada de dados pessoais;
- **Indisponibilidade:** Impossibilidade de acesso a dados necessários;
- **Phishing e engenharia social:** Obtenção de dados por meio de fraude.

Procedimento em caso de incidente

Se você identificar ou suspeitar de um incidente envolvendo dados pessoais, siga este procedimento:

1. Contenção imediata

- **Limite o dano**
  - Se possível, tome medidas imediatas para conter o incidente;
  - Exemplo: desconectar computador da rede, bloquear acesso ao sistema.

- **Preserve evidências**
  - Não apague registros ou provas do incidente;
  - Anote informações relevantes (horário, sistemas afetados, etc.).

2. Comunicação interna

- **Informe imediatamente**
  - Seu superior imediato;
  - Equipe de TI (em caso de incidente digital);
  - Encarregado de Dados da Alesp.

- **Forneça detalhes**
  - O que aconteceu;
  - Quais dados foram afetados;

- Quando ocorreu;
- Como foi detectado;
- Quais medidas já foram tomadas.

3. Comunicação interna

Documento o incidente

- Preencha o formulário de registro de incidentes;
- Inclua todos os detalhes conhecidos;
- Mantenha o registro atualizado conforme novas informações surgirem.

4. Acompanhamento

Colabore com a investigação

- Preencha o formulário de registro de incidentes (disponível pelo QR code ao lado);
- Inclua todos os detalhes conhecidos;
- Mantenha o registro atualizado conforme novas informações surgirem.

Implemente medidas corretivas

- Aplique as recomendações para evitar novos incidentes;
- Participe de treinamentos de atualização se necessário.

Responsabilidades do Encarregado de Dados

Após ser comunicado sobre um incidente, o Encarregado de Dados deve:

1. **Avaliar a gravidade**
   - Classificar o incidente conforme sua severidade;
   - Determinar potenciais impactos para titulares e instituição.
2. **Coordenar a resposta**
   - Articular ações com equipes relevantes (TI, Jurídico, Comunicação);
   - Garantir a documentação adequada.
3. **Comunicar à ANPD e titulares afetados**
   - Reportar incidentes relevantes à ANPD em prazo razoável;
   - Notificar titulares quando houver risco ou dano relevante.
4. **Rever procedimentos**
   - Analisar causas do incidente;
   - Propor melhorias nos processos.

Modelo de comunicação de incidente

Diretrizes para servidores da Alesp:

1. Identificação do comunicante

- Nome completo:
- Departamento:
- Contato (ramal/e-mail):

2. Descrição do incidente

- Data e hora da ocorrência:
- Data e hora da descoberta:
- Tipo de incidente:
- Descrição detalhada:

3. Dados afetados

- Categorias de dados:
- Categorias de titulares:
- Quantidade estimada de registros:
- Quantidade estimada de titulares:

4. Medidas já adotadas

- Ações para contenção:
- Pessoas já comunicadas:
- Outras providências:

5. Informações adicionais

- Possíveis causas:
- Possíveis consequências:
- Observações relevantes:

Perguntas frequentes

Conceitos básicos

- **Preciso me preocupar com a LGPD se trabalho em área administrativa sem contato com o público?**

  R: Sim. Praticamente todas as áreas da Alesp lidam com dados pessoais de alguma forma, seja de cidadãos, fornecedores ou outros servidores. Até mesmo um simples e-mail ou planilha pode conter dados pessoais que precisam ser protegidos.

- **A LGPD se aplica a dados de pessoas jurídicas?**

  R: Não. A LGPD protege apenas dados de pessoas naturais (físicas). No entanto, dados pessoais de sócios, representantes, funcionários ou contatos de empresas são protegidos pela lei.

- **Posso ser responsabilizado pessoalmente por violações à LGPD?**

  R: Sim. Embora a Alesp seja o controlador de dados, servidores podem ser responsabilizados administrativamente por ações que violem a LGPD, especialmente em casos de negligência grave ou ação deliberada.

Bases legais e consentimento

Sempre preciso pedir consentimento para tratar dados pessoais?

R: Não. O consentimento é apenas uma das dez bases legais previstas na LGPD. Órgãos públicos como a Alesp frequentemente utilizam outras bases como obrigação legal, execução de políticas públicas ou interesse legítimo.

Como saber qual base legal utilizar em cada situação?

R: Verifique primeiro se existe lei ou regulamento que exija o tratamento (obrigação legal). Em seguida, analise se o tratamento é necessário para política pública ou para o exercício das funções institucionais da Alesp. Em caso de dúvida, consulte o Encarregado de Dados.

Como devo obter e registrar o consentimento, quando necessário?

R: O consentimento deve ser livre, informado e inequívoco. Deve ser obtido por escrito ou por outro meio que demonstre a manifestação de vontade do titular, sempre para finalidades específicas e determinadas. É essencial manter registros dessa autorização.

Direitos dos titulares

Devo atender a qualquer solicitação de acesso ou exclusão de dados?

R: Nem sempre. Algumas solicitações podem ser negadas se houver outra base legal que permita a manutenção dos dados, como obrigação legal ou exercício regular de direitos. Toda negativa deve ser justificada e informada ao titular.

Qual o prazo para responder as solicitações dos titulares?

R: A LGPD estabelece o prazo de 15 dias para fornecer declaração completa sobre dados tratados, mas é recomendável responder todas as solicitações nesse mesmo prazo, para demonstrar comprometimento com a lei.

Como proceder se um cidadão solicitar a exclusão de seus dados de um processo administrativo?

R: Dados constantes em processos administrativos geralmente são mantidos por obrigação legal ou para exercício regular de direitos. Explique ao titular que, embora não seja possível eliminar os dados, eles são tratados conforme os princípios da LGPD e têm acesso restrito.

Segurança e incidentes

- **O que devo fazer se perceber que enviei dados pessoais para o destinatário errado?**

  R: Comunique imediatamente seu superior e o Encarregado de Dados, tente contatar o destinatário errado solicitando a exclusão da mensagem, e registre o incidente formalmente seguindo os procedimentos da Alesp.

- **Posso utilizar meu e-mail pessoal para assuntos de trabalho?**

  R: Não é recomendado. E-mails pessoais não oferecem as mesmas garantias de segurança e controle que sistemas institucionais. Além disso, pode dificultar a recuperação de informações importantes e a continuidade do serviço público.

- **É seguro armazenar dados pessoais em serviços de nuvem como Google Drive ou Dropbox?**

  R: Serviços pessoais de nuvem não são recomendados para dados institucionais, pois podem envolver transferência internacional sem as garantias necessárias. Utilize apenas soluções aprovadas pelo departamento de TI da Alesp.

Dúvidas práticas

Posso compartilhar lista de presença de um evento com outros participantes?

R: Em regra, não. Listas de presença contêm dados pessoais (nome, assinatura, etc.) e seu compartilhamento deve ter uma base legal. Se necessário compartilhar, considere versões anonimizadas ou agregadas (ex: número total de participantes).

É permitido tirar fotos durante eventos na Alesp e publicá-las?

R: Para eventos públicos, é recomendável informar previamente os participantes sobre o registro fotográfico e sua possível divulgação. Caso apareçam pessoas em destaque, especialmente crianças, é recomendável obter consentimento específico.

Como devo descartar documentos físicos que contenham dados pessoais?

R: Utilize fragmentadoras de papel para documentos físicos com dados pessoais. Nunca descarte esses documentos em lixeiras comuns ou de reciclagem sem fragmentação prévia.

Canais de contato

Encarregado de Dados da Alesp
Nome: Cairo Mendes Sobrinho
E-mail: cmsobrinho@al.sp.gov.br
Ramal: 6715

Coordenadoria de Governança e Conformidade
E-mail: cgc@al.sp.gov.br
Ramal: 6715
Localização: Andar Monumental, Sala 26

Autoridade Nacional de Proteção de Dados (ANPD)
Site: www.gov.br/anpd
E-mail: encarregado@anpd.gov.br

Este material foi elaborado pela
Coordenadoria de Governança e Conformidade da Alesp.

Alesp - Assembleia Legislativa do Estado de São Paulo
Data de elaboração: 08/05/2025
Versão: 1.0

Presidência
Deputado André do Prado

1ª Secretaria
Deputado Maurici

2ª Secretaria
Deputado Barros Munhoz

SECRETARIA GERAL DE ADMINISTRAÇÃO
Murilo Mohring Macedo

COORDENADORIA DE GOVERNANÇA E CONFORMIDADE
Cairo Mendes Sobrinho

Equipe Técnica
Guilherme Henrique dos Santos Vicente de Azevedo
Tiago Alberto Humboldt
Cairo Mendes Sobrinho

DEPARTAMENTO DE COMUNICAÇÃO
Matheus Perez Granato

DIVISÃO DE COMUNICAÇÃO INSTITUCIONAL
Patricia Yamamoto Weisz

Fotografia
Larissa Navarro
Rodrigo Costa
Freepik
Pexels

Diagramação
Vinicius de Almeida Marciano


Alesp
ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO