ou autorizações cabíveis, manifestação técnica da unidade envolvida e avaliação do Encarregado pelo Tratamento de Dados Pessoais.
Art. 34. A Seduc poderá exigir que o pesquisador ou instituição apresente relatório final, produto técnico, síntese dos resultados ou comprovação de descarte/anonimização dos dados após a conclusão da pesquisa, conforme definido na anuência ou instrumento aplicável.

CAPÍTULO VII
ACORDOS DE COOPERAÇÃO, CONTRATOS, CONVÊNIOS E PARCERIAS

Art. 35. Os acordos de cooperação técnica, convênios, contratos, termos de parceria, termos de fomento, termos de colaboração, termos aditivos e instrumentos congêneres que envolvam acesso, cessão, tratamento, compartilhamento, interoperabilidade ou uso de dados sob responsabilidade da Seduc deverão ser submetidos à análise quanto à proteção de dados pessoais, segurança da informação e governança de dados, quando aplicável.
Art. 36. O processo deverá conter, sempre que aplicável:
I – minuta do instrumento principal;
II – plano de trabalho ou documento equivalente;
III – descrição do objeto e da finalidade pública;
IV – identificação dos dados envolvidos;
V – indicação dos titulares;
VI – identificação dos agentes de tratamento e seus papéis;
VII – fluxo de dados;
VIII – medidas de segurança;
IX – cláusulas de proteção de dados, sigilo, confidencialidade, auditoria, incidentes, retenção e descarte;
X – identificação de sistemas, plataformas, APIs ou ambientes utilizados;
XI – previsão de compartilhamento com terceiros, suboperadores ou parceiros;
XII – avaliação sobre necessidade de ROPA, RIPD ou dispensa motivada;
XIII – manifestação da unidade gestora dos dados;
XIV – manifestação do Encarregado;
XV – manifestação da Astin, quando houver integração tecnológica, sistema, API, ambiente digital, acesso remoto, extração automatizada ou risco técnico;
XVI – manifestação da Asjur.
Art. 37. Nenhum instrumento de parceria, contrato ou cooperação que envolva dados pessoais sob responsabilidade da Seduc deverá ser formalizado sem cláusulas mínimas de proteção de dados pessoais, segurança da informação, confidencialidade, finalidade, auditoria, incidentes, retenção, eliminação, responsabilização e vedação de uso indevido.

CAPÍTULO VIII
LEI DE ACESSO À INFORMAÇÃO E DIREITOS DOS TITULARES

Art. 38. Os pedidos de acesso à informação formulados com fundamento na LAI deverão ser apresentados pelo Portal Ceará Transparente, observados os prazos, recursos, hipóteses de restrição de acesso, informações pessoais, sigilo e demais regras do Decreto Estadual n.º 36.552/2025.
§1º. Quando o pedido LAI envolver dados pessoais, informações pessoais, documentos escolares individualizados, dados funcionais, dados de estudantes, informações protegidas por sigilo, dados de crianças e adolescentes ou risco de identificação indevida, a unidade responsável deverá observar a LGPD e poderá solicitar orientação do Encarregado e da Asjur.
§2º. A LAI não deverá ser utilizada como via substitutiva para compartilhamento massivo, contínuo, interoperável ou estruturado de bases de dados pessoais, hipótese em que deverá ser observado o fluxo específico de compartilhamento, interoperabilidade, acordo, contrato ou instrumento próprio.
Art. 39. O exercício de direitos dos titulares de dados pessoais será atendido pelos canais oficiais definidos pela Seduc e pelo Estado do Ceará, observadas a LGPD, a Lei Estadual n.º 18.699/2024 e a Política Geral de Privacidade e Proteção de Dados da Seduc.
§1º. O atendimento aos titulares poderá envolver confirmação de tratamento, acesso, correção, atualização, informação sobre compartilhamento, anonimização, bloqueio, eliminação, portabilidade, revisão de decisões automatizadas, revogação de consentimento, oposição ou demais direitos previstos na legislação.
§2º. O atendimento poderá ser limitado, fundamentadamente, quando houver proteção de segredo comercial, industrial, segurança pública, proteção de terceiros, sigilo legal, política pública, obrigação legal ou regulatória, direitos de crianças e adolescentes ou outra hipótese legítima.

CAPÍTULO IX
SEGURANÇA DA INFORMAÇÃO, RETENÇÃO, DESCARTE E AMBIENTE SEGURO

Art. 40. O tratamento e compartilhamento de dados no âmbito da Seduc deverão observar medidas técnicas e administrativas proporcionais ao risco, incluindo, quando aplicável:
I – controle de acesso baseado em perfil;
II – autenticação segura;
III – segregação de ambientes;
IV – criptografia em trânsito e em repouso;
V – logs de acesso, consulta, extração e compartilhamento;
VI – gestão de vulnerabilidades;
VII – cópias de segurança;
VIII – restrição de download, impressão, cópia ou exportação;
IX – anonimização, pseudonimização ou agregação;
X – revisão periódica de acessos;
XI – trilhas de auditoria;
XII – treinamento e ciência dos usuários;
XIII – descarte seguro;
XIV – monitoramento de incidentes.
Art. 41. O compartilhamento deverá observar prazo de retenção compatível com a finalidade autorizada, a legislação arquivística, a Tabela de Temporalidade Documental, obrigações legais ou regulatórias e as orientações da Seduc.
§1º. Encerrada a finalidade autorizada, os dados deverão ser eliminados, anonimizados, devolvidos ou mantidos apenas quando houver obrigação legal, regulatória, contratual ou justificativa institucional documentada.
§2º. O recebedor poderá ser obrigado a apresentar comprovação de eliminação, anonimização, devolução, encerramento de acesso ou descarte seguro.
Art. 42. Quando o risco recomendar, a Seduc poderá substituir o envio de base de dados por acesso controlado em ambiente seguro ou data room virtual.
Parágrafo único. O ambiente seguro poderá prever, entre outras medidas:
I – acesso individualizado e autenticado;
II – restrição de download, impressão, exportação, cópia e captura;
III – marca d'água dinâmica;
IV – logs de sessão;
V – limitação temporal;
VI – restrição de variáveis;
VII – supervisão de uso;
VIII – aprovação prévia de resultados antes de divulgação, quando necessária para evitar reidentificação.

CAPÍTULO X
INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Art. 43. Qualquer suspeita ou confirmação de incidente de segurança envolvendo dados pessoais deverá ser comunicada imediatamente ao Encarregado pelo Tratamento de Dados Pessoais, ao Gestor de Dados e à Astin, em até 24 (vinte e quatro) horas do conhecimento do fato.
§1º. A comunicação deverá conter, sempre que disponível:
I – descrição do incidente;
II – data e hora de identificação;
III – sistemas, bases, documentos ou ambientes afetados;
IV – natureza dos dados envolvidos;
V – categorias e quantidade estimada de titulares afetados;
VI – medidas de contenção adotadas;
VII – riscos preliminares;
VIII – responsáveis pelo tratamento;
IX – evidências disponíveis.