

§2º. O Encarregado, com apoio da Astin, do Gestor de Dados e das unidades competentes, coordenará a avaliação inicial do incidente, que deverá ocorrer, sempre que possível, em até 72 (setenta e duas) horas do conhecimento do fato.

§3º. Quando o incidente envolver compartilhamento por interoperabilidade, a plataforma de interoperabilidade, órgão recebedor, órgão solicitante ou terceiro autorizado, deverão ser adotadas as comunicações e medidas de contenção necessárias junto aos envolvidos.

§4º. A comunicação à ANPD e aos titulares observará a LGPD, os regulamentos da ANPD e as orientações do Encarregado, sem prejuízo de comunicação a outros órgãos competentes quando necessário.

§5º. O recebedor de dados, operador, terceiro, parceiro ou pesquisador deverá comunicar imediatamente à Seduc qualquer incidente, suspeita, acesso indevido, uso incompatível, perda, destruição, alteração, divulgação não autorizada ou violação de segurança que envolva dados compartilhados pela Seduc.

CAPÍTULO XI

ROPA, RIPD, AUDITORIA, MONITORAMENTO E CONFORMIDADE

Art. 44. Cada serviço, sistema, processo, projeto, compartilhamento ou atividade que envolva tratamento de dados pessoais deverá possuir Registro das Operações de Tratamento de Dados Pessoais (ROPA) ou registro equivalente, nos termos da LGPD e da Política Geral de Privacidade e Proteção de Dados da Seduc.

§1º. O ROPA deverá conter, no mínimo:

I – identificação do controlador e, quando aplicável, do operador;

II – descrição da atividade de tratamento;

III – finalidade;

IV – bases legais;

V – categorias de titulares;

VI – categorias de dados pessoais;

VII – dados pessoais sensíveis, quando houver;

VIII – origem dos dados;

IX – destinatários e hipóteses de compartilhamento;

X – uso de interoperabilidade, APIs, plataforma, planilhas ou outros meios;

XI – retenção, eliminação ou anonimização;

XII – medidas de segurança;

XIII – canais de atendimento aos titulares;

XIV – existência de decisões automatizadas relevantes;

XV – transferência internacional, quando houver;

XVI – versão e data de atualização.

§2º. Todo compartilhamento aprovado que envolva dados pessoais deverá gerar novo ROPA ou atualização de ROPA existente.

Art. 45. O RIPD será elaborado ou revisado quando o tratamento puder gerar alto risco às liberdades civis e aos direitos fundamentais, especialmente quando envolver:

I – dados pessoais sensíveis;

II – crianças ou adolescentes;

III – pessoas em situação de vulnerabilidade;

IV – tratamento em larga escala;

V – monitoramento sistemático;

VI – decisões automatizadas relevantes;

VII – compartilhamento massivo ou contínuo;

VIII – integração de bases;

IX – uso de biometria, imagem, voz, inteligência artificial, geolocalização ou tecnologias emergentes;

X – risco de discriminação, estigmatização, exposição ou dano significativo.

Parágrafo único. A dispensa de RIPD deverá ser motivada e documentada no processo, sem prejuízo de revisão posterior.

Art. 46. O Encarregado pelo Tratamento de Dados Pessoais coordenará, no que couber, auditorias de conformidade em proteção de dados pessoais, com apoio do Gestor de Dados, da Astin, das unidades responsáveis, do Comitê e do Colegiado, quando cabível.

Art. 47. Deverão ser monitorados, no mínimo, os seguintes indicadores:

I – prazo médio de atendimento das solicitações;

II – percentual de processos com ROPA atualizado;

III – percentual de processos com RIPD ou dispensa motivada;

IV – tempo médio de concessão, revisão e revogação de acessos;

V – número de compartilhamentos por categoria;

VI – número de compartilhamentos por meio da plataforma de interoperabilidade;

VII – número de compartilhamentos fora da plataforma;

VIII – percentual de logs auditados;

IX – número de incidentes e tempo de comunicação;

X – número de treinamentos e ações de conscientização;

XI – número de não conformidades e planos de correção.

Art. 48. As não conformidades identificadas em auditoria, monitoramento, incidente ou análise técnica ensejarão plano de correção com responsáveis e prazos, podendo implicar:

I – suspensão de acesso;

II – revogação de autorização;

III – bloqueio de compartilhamento;

IV – exigência de reforço de controles;

V – comunicação à autoridade competente;

VI – revisão de instrumento jurídico;

VII – abertura de apuração administrativa;

VIII – outras medidas proporcionais ao risco e à gravidade.

CAPÍTULO XII

INDEFERIMENTO, SUSPENSÃO, REVOGAÇÃO E RESPONSABILIZAÇÃO

Art. 49. A solicitação de acesso, cessão, tratamento, compartilhamento ou interoperabilidade poderá ser indeferida, suspensa ou revogada, total ou parcialmente, quando houver:

I – finalidade genérica, incompatível ou não demonstrada;

II – ausência de base legal;

III – excesso de dados solicitados;

IV – possibilidade de atendimento por dados anonimizados, agregados ou minimizados;

V – risco elevado sem mitigação suficiente;

VI – ausência de medidas de segurança adequadas;

VII – descumprimento de diligência;

VIII – ausência de instrumento jurídico exigível;

IX – ausência de termo de responsabilidade, quando aplicável;

X – inconsistência documental;

XI – dúvida sobre competência institucional do solicitante;

XII – descumprimento anterior de obrigações de proteção de dados;

XIII – risco de exposição de crianças, adolescentes ou grupos vulneráveis;

XIV – risco de violação de sigilo legal, segredo de justiça, informação pessoal ou informação classificada;

XV – desconformidade com a LGPD, com a Lei Estadual n.º 18.699/2024, com o Decreto Estadual n.º 37.059/2026, com a Resolução n.º 01/2026 ou com esta Portaria.

Art. 50. O descumprimento das disposições desta Portaria por agentes públicos da Seduc, servidores, colaboradores, estagiários, terceirizados, consultores, prestadores de serviço ou quaisquer pessoas que, por vínculo formal ou autorização específica, acessem ou tratem dados sob responsabilidade ou custódia da Secretaria, poderá ensejar, sem prejuízo da responsabilização civil, penal, contratual e por improbidade administrativa, quando cabível, a responsabilização administrativa nos termos da legislação aplicável, das normas internas de conduta, da Política Geral de Segurança da Informação, da Política Geral de

