

- IV – autenticação multifator;
- V – criptografia em trânsito e em repouso;
- VI – gestão segura de credenciais;
- VII – registro e monitoramento de eventos;
- VIII – gestão de vulnerabilidades e correções;
- IX – testes periódicos de segurança;
- X – backup, continuidade e recuperação de desastres;
- XI – proteção contra códigos maliciosos;
- XII – descarte seguro;
- XIII – prevenção contra perda de dados;
- XIV – revisão periódica de acessos;
- XV – capacitação e compromisso de confidencialidade;
- XVI – preservação de evidências;
- XVII – controles específicos para dispositivos móveis, mídias removíveis e trabalho remoto.

Parágrafo único. As medidas deverão observar a PoSIC, a PGSI da Seduc, as normas técnicas aplicáveis e os requisitos definidos pela Astin.

Art. 35. Os agentes públicos, unidades, operadores e terceiros deverão comunicar à Seduc qualquer incidente ou suspeita de incidente envolvendo dados pessoais.

§1º. O operador deverá comunicar o incidente à Seduc, sem demora injustificada e, no máximo, em 24 (vinte e quatro) horas contadas da ciência, apresentando:

- I – data e hora da detecção e da ciência;
- II – descrição da natureza do incidente;
- III – categorias e volume estimado de dados afetados;
- IV – categorias e número estimado de titulares;
- V – sistemas, ambientes e localidades afetados;
- VI – medidas de segurança existentes;
- VII – possíveis impactos;
- VIII – medidas de contenção e mitigação adotadas;
- IX – ponto de contato responsável;
- X – demais informações disponíveis.

§2º. A ausência de todas as informações não deverá retardar a comunicação inicial, que será complementada à medida que a apuração avançar.

§3º. A Astin apoiará a contenção, investigação técnica, preservação de evidências e recuperação.

§4º. O Encarregado apoiará a avaliação do risco aos titulares e a preparação das comunicações.

§5º. A Asjur será acionada quando houver repercussão jurídica, contratual, judicial ou de responsabilização.

§6º. Compete ao Controlador decidir sobre a comunicação à ANPD e aos titulares.

§7º. Quando o incidente puder acarretar risco ou dano relevante, a comunicação à ANPD e aos titulares deverá ocorrer no prazo e nas condições definidos pela Resolução CD/ANPD n.º 15/2024, ressalvado prazo específico previsto em lei.

§8º. O incidente deverá ser registrado, ainda que se conclua pela desnecessidade de comunicação externa.

Art. 36. As operações relevantes de tratamento deverão ser registradas em trilhas de auditoria contendo, no mínimo:

- I – identificador do usuário, sistema ou aplicação;
- II – data e hora;
- III – operação realizada;
- IV – dado, recurso ou conjunto acessado;
- V – origem do acesso;
- VI – indicação de sucesso ou falha;
- VII – alterações de permissões;
- VIII – exportações, extrações ou compartilhamentos relevantes.

§1º. Os registros deverão ser protegidos contra alteração e acesso não autorizado.

§2º. Os registros serão conservados pelo prazo mínimo de 12 (doze) meses, salvo:

- I – prazo superior previsto em lei, contrato, tabela de temporalidade ou norma de segurança;
 - II – necessidade de preservação para auditoria, investigação ou processo;
 - III – impossibilidade técnica devidamente justificada e acompanhada de controle compensatório.
- §3º. O conteúdo dos registros deverá respeitar o princípio da necessidade e não deverá armazenar dados pessoais além do indispensável à finalidade de auditoria.

Art. 37. Encerrado o tratamento realizado por operador ou terceiro, deverá ocorrer, conforme instrução da Seduc:

- I – devolução dos dados;
- II – eliminação segura;
- III – anonimização;
- IV – transferência para ambiente indicado pela Seduc;
- V – conservação excepcional, quando exigida por lei.

§1º. O operador deverá apresentar comprovação da destinação realizada quando exigido.

§2º. A conservação excepcional deverá limitar o acesso, impedir novos usos e observar o prazo legal correspondente.

§3º. O término do contrato não extingue as obrigações de confidencialidade e proteção aplicáveis aos dados anteriormente acessados.

Art. 38. A Seduc poderá realizar auditorias, inspeções ou avaliações de conformidade em operadores, suboperadores, fornecedores e parceiros.

§1º. As auditorias observarão a finalidade, a proporcionalidade, a confidencialidade, a economicidade e a proteção de segredos comercial e industrial.

§2º. Os instrumentos jurídicos deverão assegurar à Seduc acesso às informações e evidências necessárias à verificação da conformidade.

§3º. Poderão ser exigidos relatórios sobre:

- I – acessos e trilhas de auditoria;
- II – vulnerabilidades e correções;
- III – testes de continuidade e recuperação;
- IV – incidentes e medidas adotadas;
- V – suboperadores;
- VI – transferências internacionais;
- VII – capacitações;
- VIII – eliminação, anonimização ou devolução de dados;
- IX – certificações e avaliações independentes.

Art. 39. Contratos, convênios, acordos de cooperação, termos de fomento, termos de colaboração, instrumentos de pesquisa, termos aditivos e instrumentos congêneres que envolvam tratamento de dados pessoais deverão conter cláusulas ou anexo específico de proteção de dados.

§1º. Os instrumentos deverão ser submetidos:

- I – à manifestação técnica do Encarregado, quanto à proteção de dados pessoais;
- II – à manifestação da Astin, quando envolver tecnologia, sistemas, integrações, APIs, armazenamento, acesso remoto ou segurança;
- III – obrigatoriamente à análise jurídica da Asjur.

§2º. As cláusulas deverão observar os modelos e orientações aprovados pela Asjur e disciplinar, conforme aplicável:

- I – objeto, natureza, duração e finalidade do tratamento;
- II – categorias de dados e titulares;
- III – papéis e responsabilidades dos agentes;
- IV – instruções documentadas do Controlador;
- V – confidencialidade;
- VI – medidas de segurança;
- VII – controle e registro de acessos;
- VIII – atendimento dos direitos dos titulares;
- IX – contratação de suboperadores;
- X – compartilhamentos posteriores;
- XI – transferência internacional;