PORTARIA N.º XX-R, DE XX DE JULHO DE 2026.

Institui a Política Interna de Segurança da Informação da Secretaria de Estado da Educação do Espírito Santo.

A **SECRETÁRIA DE ESTADO DA EDUCAÇÃO**, no uso das atribuições que lhe foram conferidas pela Lei nº 3.043/1975, e considerando:

- a **Constituição da República Federativa do Brasil**, de 5 de outubro de 1988, em especial o disposto nos incisos X, XII e LXXIX do art. 5º e no art. 37;

- a **Lei Federal n.º 8.069**, de 13 de julho de 1990, que dispõe sobre o **Estatuto da Criança e do Adolescente** e dá outras providências;

- a **Lei Federal n.º 9.394**, de 20 de dezembro de 1996, que estabelece as diretrizes e bases da educação nacional (**Lei de Diretrizes e Bases da Educação Nacional - LDB**);

- o **Decreto Estadual n.º 2.884-R**, de 21 de outubro de 2011, que institui a **Política Estadual de Segurança da Informação** no âmbito do Poder Executivo do Estado - **PESI**;

- a **Portaria SEGER n.º 068-R**, de 04 de novembro de 2011, que **regulamenta a Política Estadual de Segurança da Informação** no âmbito do Poder Executivo do Estado do Espírito Santo, instituída pelo Decreto Estadual n.º 2.884-R/2011.

- a **Lei Federal n.º 12.527**, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências (**Lei de Acesso à Informação - LAI**);

- a **Lei Estadual n.º 9.871**, de 09 de julho de 2012, que regula o acesso a informações previsto no inciso II do § 4º do artigo 32 da Constituição do Estado do Espírito Santo (**Lei Estadual de Acesso à Informação**);

MINUTA

- o **Decreto Estadual n.º 3.152-R**, de 26 de novembro de 2012, que regulamenta a Lei Estadual de Acesso à Informação;

- a **Lei Federal n.º 12.965**, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (**Marco Civil da Internet**);

- a **Lei Federal n.º 13.709**, de 14 de agosto de 2018, a **Lei Geral de Proteção de Dados Pessoais** (**LGPD**);

- o **Decreto Estadual n.º 4.410-R**, de 18 de abril de 2019, que dispõe sobre o **uso do meio eletrônico e não presencial para a interação do cidadão com o Estado** e a realização de processo administrativo no âmbito dos órgãos e das entidades do Poder Executivo Estadual;

- o **Decreto Estadual n.º 4.411-R**, de 18 de abril de 2019, que institui o **Sistema de Gestão de Documentos Arquivísticos Eletrônicos (e-Docs)**;

- a **Lei Federal n.º 14.129**, de 29 de março de 2021, que dispõe sobre princípios, regras e instrumentos para o **Governo Digital** e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017;

- o **Decreto Estadual n.º 4.922**, de 09 de julho de 2021, que instituiu a **Política Estadual de Proteção de Dados Pessoais e da Privacidade** do Poder Executivo Estadual em consonância com a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

- a **Lei Federal n.º 14.533**, de 11 de janeiro de 2023, que institui a **Política Nacional de Educação Digital** e altera as Leis Federais nº 9.394/1996 (Lei de Diretrizes e Bases da Educação Nacional - LDB), 9.448/1997, 10.260/2001, e 10.753/2003;

- o **Decreto Estadual n.º 5.778**, de 24 de julho de 2024, que regulamenta o **Governo Digital Estadual**, no âmbito da administração pública estadual direta, autarquias, fundações, empresas públicas e às empresas de sociedade de economia mista do Estado do Espírito Santo;

MINUTA

- a **Lei Federal n.º 15.211**, de 17 de setembro de 2025, que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (**Estatuto Digital da Criança e do Adolescente - ECA Digital**);

- a **Portaria SEDU n.º 010-R**, de 14 de janeiro de 2026, que institui o **Comitê Estratégico de Governança de Dados - CEGD** e o **Comitê Interno de Governança de Dados - CIGD** da Secretaria de Estado da Educação do Espírito Santo, e dá outras providências; e

- o **Decreto Federal n.º 12.880**, de 18 de março de 2026, que regulamenta a Lei Federal nº 15.211/2025, que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais, e institui a **Política Nacional de Promoção e Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital**;

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a **Política Interna de Segurança da Informação (PISI)** da Secretaria de Estado da Educação do Espírito Santo, em consonância com o disposto no Decreto Estadual nº 2.884-R, de 21 de outubro de 2011, que institui a **Política Estadual de Segurança da Informação (PESI)** no âmbito do Poder Executivo do Estado do Espírito Santo.

§ 1º Esta Política Interna de Segurança da Informação alinha-se às estratégias de Governança de Dados, Proteção de Dados Pessoais e Tecnologia da Informação e Comunicação do Governo do Estado do Espírito Santo e da Secretaria de Estado da Educação (SEDU), articulando-se com as demais normas, políticas e procedimentos institucionais correlatos.

§ 2º As disposições desta Política aplicam-se às informações produzidas, custodiadas, tratadas ou armazenadas em meio físico ou eletrônico e estabelecem princípios, diretrizes e regras voltadas à proteção da confidencialidade, integridade, disponibilidade e autenticidade das informações no âmbito da Secretaria de Estado da Educação (SEDU).

MINUTA

§ 3º As disposições desta Política vinculam todas as unidades administrativas e escolares que compõem a estrutura organizacional da SEDU, incluindo-se o Conselho Estadual de Educação do Espírito Santo (CEE-ES), e aplicam-se a todos os usuários de informações ou ativos de informação sob responsabilidade da SEDU, em especial aqueles que possuam vínculo com a Secretaria e que, em razão desse vínculo, tenham acesso ou atuem sobre tais informações ou ativos.

§ 4º A Faculdade de Música do Espírito Santo (FAMES), enquanto unidade do Sistema de Ensino Superior Estadual vinculada à SEDU, poderá estabelecer sua Política de Segurança da Informação por ato próprio, respeitando os ritos de suas instâncias deliberativas superiores e observando as diretrizes da Política Estadual de Segurança da Informação, bem como as normas legais e regulamentares vigentes e aplicáveis.

§ 5º Esta Política considera as prioridades, as especificidades e a realidade operacional das unidades administrativas e escolares da Secretaria, tomando-se por base os princípios e diretrizes da Política Estadual de Segurança da Informação, e orienta a adoção de processos de gerenciamento de riscos e de medidas destinadas à prevenção, detecção e mitigação de incidentes de segurança da informação.

§ 6º Esta Política será disponibilizada em locais de fácil acesso, inclusive no sítio eletrônico da Secretaria de Estado da Educação, em seção específica destinada aos documentos institucionais relativos à segurança da informação.

Art. 2º Para os fins desta Política Interna de Segurança da Informação, aplicam-se as definições constantes na legislação e nas normas estaduais e federais pertinentes, sem prejuízo das definições complementares estabelecidas neste artigo, conforme a seguir:

I - Agente Público: pessoa física que possui vínculo funcional direto com o Governo do Estado do Espírito Santo, no exercício de cargo, emprego ou função pública no âmbito da Secretaria de Estado da Educação, estando sujeito ao seu regime disciplinar estatutário ou às normas específicas de estágio,

MINUTA

compreendendo os servidores públicos estatutários, efetivos, comissionados, designados temporários (DTs) e estagiários;

II - Alta administração: integrantes do **Nível de Direção da SEDU** e o **Conselho Estadual de Educação**, nos termos da legislação vigente;

III - Ativo de informação: conjunto de informações, sistemas, bases de dados, documentos, processos, serviços, equipamentos, meios de armazenamento, infraestrutura tecnológica ou qualquer outro recurso que suporte a criação, o processamento, o armazenamento, a transmissão ou o uso da informação no âmbito da SEDU e que possua valor para a Administração Pública;

IV - Autenticidade: propriedade que assegura que a informação foi produzida, alterada ou transmitida por quem declara ser seu autor, bem como que sua origem e autoria possam ser verificadas;

V - Colaborador Externo: pessoa física ou jurídica que, sem possuir vínculo funcional direto com o Governo do Estado do Espírito Santo, atue em nome da Secretaria de Estado da Educação ou em parceria com esta, em razão de contrato, convênio, termo de cooperação, instrumento congênere ou outra forma de vínculo jurídico, envolvendo atividades que demandem acesso a informações ou a ativos de informação;

VI - Comitê Estratégico de Governança de Dados (CEGD): instância superior destinada a orientar, deliberar e promover as ações estratégicas relacionadas à gestão e à governança de dados no âmbito da SEDU;

VII - Comitê Interno de Governança de Dados (CIGD): instância colegiada técnica responsável pela orientação, supervisão e execução das ações necessárias à gestão e à governança de dados no âmbito da SEDU;

VIII - Confidencialidade: propriedade que assegura que a informação seja acessada apenas por pessoas, sistemas ou processos devidamente autorizados;

IX - Disponibilidade: propriedade que assegura que a informação e os ativos de informação estejam acessíveis e utilizáveis sob demanda, por pessoas, sistemas ou processos autorizados;

MINUTA

X - Integridade: propriedade que assegura a exatidão, a completude e a fidedignidade da informação, bem como a proteção contra alterações não autorizadas ou indevidas;

XI - Incidente de Segurança da Informação: evento adverso, confirmado ou sob suspeita, que comprometa ou possa comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade das informações ou dos ativos de informação sob responsabilidade da SEDU, independentemente de envolver ou não dados pessoais;

XII - Gestão de Riscos de Segurança da Informação: processo contínuo e sistemático de identificação, análise, avaliação e tratamento de riscos relacionados à segurança da informação, com vistas à redução da probabilidade e do impacto de incidentes;

XIII - Segurança da Informação: conjunto de princípios, diretrizes, práticas, controles e medidas administrativas, técnicas e físicas destinadas a proteger a informação e os ativos de informação contra acessos não autorizados e de situações acidentais ou ilícitas de uso indevido, divulgação, modificação, destruição ou interrupção;

XIV - Terceiro: pessoa física ou jurídica que não possua vínculo funcional, contratual, convenial ou congênere com a SEDU, mas que, por qualquer meio, interaja com a Secretaria ou com seus sistemas, serviços, instalações ou informações;

XV - Unidade Administrativa: Unidade pertencente à estrutura organizacional da SEDU, responsável pela execução de atividades administrativas e/ou de suporte à Educação Pública Estadual;

XVI - Unidade Escolar: Unidade pertencente à estrutura organizacional da SEDU, responsável pela execução de atividades administrativas e pedagógicas que concretizam a oferta da Educação Básica para a população capixaba;

XVII - Usuário da Informação: agente público, colaborador externo ou terceiro que, de forma autorizada, tenha acesso, utilize, manipule ou de qualquer modo

MINUTA

interaja com informações ou ativos de informação sob responsabilidade da Secretaria de Estado da Educação.

Art. 3º São objetivos da Política Interna de Segurança da Informação da Secretaria de Estado da Educação do Espírito Santo:

I - proteger as informações e os ativos de informação sob responsabilidade da SEDU, em qualquer meio ou suporte, contra incidentes de segurança da informação;

II - assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações, de modo a preservar a confiabilidade dos processos administrativos, pedagógicos e de gestão educacional;

III - estabelecer diretrizes institucionais para a prevenção, a detecção, a contenção, a resposta e a mitigação dos efeitos decorrentes de incidentes de segurança da informação, inclusive aqueles que envolvam dados pessoais;

IV - apoiar a continuidade e a resiliência dos serviços públicos educacionais, minimizando impactos decorrentes de falhas ou incidentes de segurança da informação;

V - promover a cultura de segurança da informação no âmbito da SEDU, por meio da conscientização, da capacitação e da responsabilização de agentes públicos, colaboradores externos e demais usuários da informação;

VI - alinhar a segurança da informação às estratégias de governança de dados, proteção de dados pessoais, transparência, governo digital e tecnologia da informação e comunicação da Secretaria, assegurando a observância das normas e atos normativos vigentes e aplicáveis;

VII - orientar a adoção de processos sistemáticos de gestão de riscos de segurança da informação, compatíveis com a natureza das informações, com a criticidade dos ativos e com a realidade operacional das unidades administrativas e escolares;

VIII - assegurar a proteção e o melhor interesse de crianças e adolescentes no ambiente digital, inclusive por meio de ações de educação digital, conscientização e prevenção de riscos online;

MINUTA

IX - orientar o uso ético e seguro de sistemas e novas tecnologias no âmbito da SEDU, garantindo a conformidade com a legislação e os atos normativos vigentes e aplicáveis; e

X - assegurar que o tratamento da informação no âmbito da SEDU observe os princípios da legalidade, da eficiência, da publicidade, da transparência e da proteção de dados pessoais, em consonância com a legislação vigente e aplicável.

CAPÍTULO II
DOS PRINCÍPIOS E DIRETRIZES

Art. 4º A Política Interna de Segurança da Informação da Secretaria de Estado da Educação do Espírito Santo será regida pelos seguintes princípios:

I - Confidencialidade, assegurando que as informações sob responsabilidade da SEDU sejam acessadas exclusivamente por usuários devidamente autorizados, observadas as restrições legais e institucionais aplicáveis;

II - Integridade, garantindo a exatidão, a rastreabilidade, a completude, a consistência e a fidedignidade das informações, bem como a proteção contra alterações não autorizadas ou indevidas;

III - Disponibilidade, assegurando que as informações e os ativos de informação estejam acessíveis e utilizáveis, de forma tempestiva e em formato interoperável, pelos usuários autorizados por meio de credenciais de acesso, conforme as necessidades institucionais e o interesse público;

IV - Autenticidade, assegurando a identificação e a verificação da autoria, da origem e da integridade das informações e das transações realizadas;

V - Legalidade, observando a legislação vigente, especialmente as normas relativas à segurança da informação, à proteção de dados pessoais, à transparência, ao acesso à informação e à governança digital;

VI - Responsabilização, atribuindo responsabilidades claras aos agentes públicos, colaboradores externos e demais usuários da informação, de acordo com suas atribuições e níveis de acesso;

MINUTA

VII - Prevenção, priorizando a adoção de medidas e controles destinados a evitar a ocorrência de incidentes de segurança da informação;

VIII - Gestão de Riscos, orientando a identificação, a análise, a avaliação, o tratamento e o monitoramento contínuo dos riscos relacionados à segurança da informação, de forma proporcional à criticidade das informações e dos ativos envolvidos;

IX - Segurança física e lógica, garantindo o controle de acesso adequado aos ambientes físicos e aos sistemas institucionais da SEDU, a adoção de medidas de prevenção de falhas humanas e operacionais, bem como o controle adequado de entrada, saída e descarte de ativos da informação e dados pessoais;

X - Continuidade dos Serviços Públicos, assegurando que a segurança da informação contribua para a manutenção e a resiliência dos serviços educacionais prestados pela SEDU, inclusive em situações de incidentes ou eventos adversos;

XI - Transparência e Publicidade, assegurando que a proteção da informação não seja utilizada como fundamento para restringir indevidamente o acesso à informação, nos termos da legislação vigente;

XII - Garantia do melhor interesse das crianças e adolescentes, garantindo que a segurança da informação no contexto das atividades da SEDU priorize a proteção, a privacidade e o desenvolvimento seguro de crianças e adolescentes;

XIII - Segurança por padrão e desde a concepção, integrando medidas técnicas e administrativas e salvaguardas de privacidade e segurança da informação em todo o ciclo de vida de sistemas, projetos e processos institucionais; e

XIV - Adequação à Realidade Institucional, considerando as especificidades, capacidades operacionais e contextos das unidades administrativas e escolares da SEDU e do CEE-ES.

Art. 5º A implementação da Política Interna de Segurança da Informação da Secretaria de Estado da Educação do Espírito Santo observará, dentre outras, as seguintes diretrizes:

MINUTA

I - adoção de medidas administrativas, técnicas e físicas adequadas à proteção das informações e dos ativos de informação, considerando sua natureza, criticidade, sensibilidade e o contexto em que são utilizados;

II - estabelecimento e manutenção de mecanismos de controle de acesso às informações e aos sistemas institucionais, com base nos princípios da necessidade, da proporcionalidade e do menor privilégio, observadas as atribuições e responsabilidades dos usuários da informação;

III - adoção de mecanismos de rastreabilidade, compatíveis com a realidade das unidades administrativas e escolares, que permitam a identificação de qualquer criação, alteração ou exclusão de informações nos sistemas institucionais da SEDU, preservando-se, sempre que possível, o histórico dos dados ou ativos da informação modificados;

IV - classificação das informações quanto ao grau de sigilo, restrição ou publicidade, em conformidade com a legislação vigente, especialmente as normas relativas ao acesso à informação, à proteção de dados pessoais e à segurança da informação;

V - promoção do uso adequado, responsável e seguro dos recursos de tecnologia da informação e comunicação, incluindo sistemas, redes, equipamentos, serviços e meios de armazenamento disponibilizados ou utilizados no âmbito da SEDU;

VI - definição e adoção de procedimentos para a prevenção, a detecção, o registro, a comunicação, a resposta e a recuperação de incidentes de segurança da informação, inclusive aqueles que envolvam dados pessoais, em articulação com as instâncias competentes e em observância às normas aplicáveis;

VII - integração das ações de segurança da informação com as políticas e estratégias de governança de dados, proteção de dados pessoais, tecnologia da informação e comunicação, transparência e governo digital da Secretaria;

VIII - realização periódica de ações de conscientização, orientação e capacitação dos agentes públicos, colaboradores externos e demais usuários da informação, com vistas ao fortalecimento da cultura de segurança da informação e à proteção

MINUTA

de dados no âmbito da SEDU, com foco na correta utilização dos ativos de informação e na mitigação de riscos de incidentes de segurança da informação;

IX - adoção de processos contínuos de gestão de riscos de segurança da informação, compatíveis com a realidade das unidades administrativas e escolares, de modo a orientar a priorização de controles e medidas de proteção;

X - observância dos prazos de retenção das informações, fundamentados nas finalidades institucionais, nas obrigações legais ou regulatórias e nos normativos da Política de Gestão Documental do Poder Executivo Estadual e da SEDU;

XI - garantia de que a segurança da informação seja considerada desde a concepção de novos sistemas, processos, projetos, serviços ou soluções tecnológicas, bem como nas alterações significativas daqueles já existentes;

XII - estabelecimento de responsabilidades claras quanto ao uso, à guarda, à transmissão, ao compartilhamento, ao armazenamento e ao descarte das informações, inclusive em ambientes físicos e digitais;

XIII - monitoramento, avaliação e revisão periódica das práticas, controles e medidas de segurança da informação adotadas, com vistas ao seu aperfeiçoamento contínuo;

XIV - definição de padrões mínimos de segurança para o uso de canais digitais institucionais de atendimento e comunicação com a comunidade escolar, assegurando, quando aplicável, a identificação do solicitante, o registro da solicitação, a rastreabilidade do atendimento, a limitação de acesso e a prevenção do compartilhamento indevido de informações;

XV - previsão obrigatória de cláusulas de segurança da informação, sigilo, confidencialidade e proteção de dados pessoais nos editais de contratação, contratos, convênios, acordos de cooperação e instrumentos congêneres celebrados pela SEDU, com a estipulação de responsabilidades e sanções em caso de descumprimento;

XVI - observância do princípio da transparência, assegurando que as medidas de segurança da informação não sejam utilizadas para restringir indevidamente o acesso à informação pública, nos termos da legislação aplicável.

MINUTA

CAPÍTULO III

DA CLASSIFICAÇÃO E DO CONTROLE DE ACESSO À INFORMAÇÃO

Art. 6º As disposições deste Capítulo aplicam-se a todas as informações e ativos de informação produzidos, recebidos, custodiados ou tratados pela Secretaria de Estado da Educação, independentemente do meio, suporte, formato, tecnologia empregada ou fase do seu ciclo de vida.

Art. 7º Toda informação sob responsabilidade da Secretaria deverá ser protegida de forma compatível com o seu valor, criticidade, sensibilidade e com os riscos associados ao seu uso, acesso, divulgação, alteração ou perda, nos termos das normas aplicáveis.

Seção I

Da Classificação da Informação

Art. 8º A classificação da informação consiste no processo de atribuição de um nível de acesso e de proteção às informações, com a finalidade de definir as medidas de segurança necessárias à sua adequada salvaguarda.

Art. 9º A informação deverá ser classificada pelo agente público no momento de sua criação, produção, recebimento ou obtenção, devendo a classificação ser mantida e, quando necessário, revista ao longo de todo o seu ciclo de vida.

Art. 10. A classificação da informação observará, no mínimo, os seguintes níveis e categorias, conforme a legislação estadual vigente:

I - Informação Pública, cujo acesso é franqueado a qualquer interessado sem restrições de acesso, nos termos da legislação vigente e aplicável;

II - Informação Organizacional, cujo acesso é restrito aos agentes públicos lotados nos órgãos ou unidades por onde a informação tramitar, em razão de suas atribuições institucionais;

III - Informação Sigilosa, cujo acesso é restrito aos usuários da informação diretamente envolvidos em sua produção, tramitação ou utilização, ou àqueles que detenham autorização formal de acesso;

MINUTA

IV - Informação Classificada, submetida a graus específicos de sigilo, nos termos da legislação aplicável, compreendendo:

a) informação reservada;

b) informação secreta; e

c) informação ultrassecreta.

Art. 11. A atribuição dos graus de sigilo, os prazos de restrição de acesso, as hipóteses de reclassificação e desclassificação e as autoridades competentes para tais atos observarão o disposto na legislação estadual e federal vigente, em especial a Lei de Acesso à Informação e seus regulamentos.

Parágrafo único. Sempre que as informações submetidas à classificação ou restrição de acesso envolverem o tratamento de dados pessoais, deverão ser observadas, no que couber, as disposições da Lei Federal n.º 13.709/2018 (LGPD) e do Decreto Estadual n.º 4.922/2021 (PEPDP).

Seção II

Do Controle de Acesso à Informação

Art. 12. O acesso às informações sob responsabilidade da Secretaria será concedido de forma proporcional às atribuições, responsabilidades e necessidades institucionais do usuário da informação, observados os princípios do privilégio mínimo e da necessidade de conhecimento.

§ 1º A identificação do agente público ou do colaborador externo para fins de acesso aos ativos da informação deverá ser única, pessoal e intransferível.

§ 2º Em caso de exoneração, transferência, desligamento ou qualquer alteração de vínculo do agente público ou do colaborador externo, compete à respectiva unidade administrativa ou escolar providenciar a revogação imediata de suas credenciais de acesso, ou no prazo máximo fixado em regulamentação própria.

§ 3º Compete às unidades administrativas e escolares da SEDU e ao CEE-ES, no limite de suas especificidades e em consonância com a regulamentação vigente, realizar revisões periódicas quanto à regularidade das autorizações de acesso concedidas a agentes públicos e colaboradores externos.

MINUTA

Art. 13. O controle de acesso à informação deverá considerar, de forma integrada:

I - a classificação da informação;

II - a existência de sigilo legal ou judicial;

III - a proteção de dados pessoais e de informações pessoais;

IV - a preservação do interesse público, da segurança institucional e da continuidade dos serviços educacionais.

Art. 14. As informações protegidas por sigilo legal específico, independentemente de classificação formal, terão seu acesso restrito nos termos da legislação que lhes seja aplicável, incluindo, entre outras hipóteses:

I - informações pessoais e dados pessoais protegidos por legislação específica;
II - documentos preparatórios para tomada de decisão administrativa , enquanto não concluído o processo decisório, nos termos da legislação aplicável;
III - processos e procedimentos sujeitos a sigilo administrativo, funcional, profissional, fiscal, bancário, comercial, industrial, contábil ou judicial;
IV - informações cuja divulgação possa comprometer a segurança institucional, a investigação administrativa, a fiscalização, a apuração de infrações ou a preservação de direitos fundamentais.

Art. 15. Os sistemas corporativos utilizados pela Secretaria deverão implementar mecanismos de controle de acesso compatíveis com a classificação da informação e com os fundamentos legais de restrição aplicáveis, assegurando a rastreabilidade, a integridade e a confidencialidade das informações.

Parágrafo único. O acesso às informações referidas no caput deverá considerar a necessidade de conhecimento dos agentes públicos e colaboradores externos que as acessem, a partir de suas atribuições e competências funcionais, observada a devida classificação de sigilo.

MINUTA

CAPÍTULO IV

DA ESTRUTURA DE GOVERNANÇA E DAS RESPONSABILIDADES

Seção I

Da Estrutura de Governança

Art. 16. A Secretaria de Estado da Educação (SEDU), enquanto órgão integrante da Administração Pública Estadual, é responsável por instituir, manter e supervisionar a conformidade das práticas de segurança da informação realizadas no âmbito de suas competências com a legislação vigente, com a Política Estadual de Segurança da Informação (PESI) e com esta Política Interna.

§ 1º A responsabilidade institucional referida no caput compreende a definição de estruturas de governança, a designação de instâncias responsáveis, a adoção de controles técnicos e organizacionais e o suporte necessário à implementação desta Política.

§ 2º A responsabilidade institucional não exclui a responsabilização administrativa, civil e penal dos usuários da informação que, no exercício de suas atribuições ou atividades, descumprirem a legislação ou os normativos internos aplicáveis.

Art. 17. As unidades administrativas e escolares da SEDU e o Conselho Estadual de Educação do Espírito Santo (CEE-ES) são responsáveis por executar e operacionalizar, no âmbito de suas atribuições, as disposições desta Política Interna e das normas de segurança da informação aplicáveis às informações e aos ativos de informação sob sua responsabilidade.

Parágrafo único. As unidades referidas no caput deverão observar a classificação da informação, os controles de acesso estabelecidos, as diretrizes de uso seguro dos recursos tecnológicos, os procedimentos de comunicação de incidentes de segurança da informação e, no que couber, as demais disposições desta Política Interna.

Art. 18. A governança da Política Interna de Segurança da Informação da SEDU é exercida por meio de instâncias internas e externas, articuladas de forma

MINUTA

coordenada, observadas as competências legais e institucionais de cada órgão ou entidade.

§ 1º Integram a estrutura interna de governança da segurança da informação, no âmbito da SEDU:

I - o Comitê Estratégico de Governança de Dados (CEGD);

II - o Comitê Interno de Governança de Dados (CIGD); e

III - a Gerência de Tecnologia da Informação (GTI).

§ 2º Integram a estrutura externa de governança da segurança da informação, no âmbito de suas respectivas competências, em conformidade com o disposto no Decreto Estadual n.º 2.884-R/2011 (PESI), suas atualizações e regulamentações:

I - o Comitê Estadual de Segurança da Informação (CESI);

II - o Comitê Estadual de Tratamento e Resposta a Incidentes de Segurança da Informação do Poder Executivo do Estado (CETRIN); e

III - o Instituto de Tecnologia da Informação e Comunicação do Estado do Espírito Santo (PRODEST).

§ 3º A atuação das instâncias referidas neste artigo observará os princípios da cooperação institucional, da segregação de funções, da proporcionalidade e da não sobreposição indevida de competências.

Seção II
Das Responsabilidades das Instâncias de Governança

Art. 19. Compete ao CEGD, enquanto instância máxima da estrutura interna de governança da segurança da informação:

I - promover, apoiar e supervisionar a implementação desta Política Interna;

II - assegurar a disponibilização de recursos humanos, técnicos e organizacionais necessários à segurança da informação;

III - fomentar a cultura institucional de segurança da informação;

MINUTA

IV - respaldar as instâncias responsáveis pela governança e pela operacionalização da segurança da informação;

V - deliberar sobre temas estratégicos relacionados à segurança da informação, por iniciativa própria ou quando provocado pelas instâncias competentes.

Art. 20. Compete ao CIGD, no âmbito da Política Interna de Segurança da Informação, sem prejuízo de suas atribuições previstas em ato próprio:

I - apoiar a implementação, o monitoramento e o aprimoramento das ações de segurança da informação;

II - promover a integração entre segurança da informação, proteção de dados pessoais, governança de dados, transparência e gestão de riscos institucionais;

III - deliberar, em nível tático, sobre diretrizes e orientações relacionadas à segurança da informação, quando demandado;

IV - acompanhar a implementação de medidas corretivas decorrentes de avaliações de riscos ou incidentes de segurança da informação;

V - fomentar ações de capacitação e conscientização em segurança da informação no âmbito institucional.

Art. 21. Compete à GTI da SEDU:

I - implementar e manter controles técnicos de segurança da informação compatíveis com a classificação das informações;

II - propor medidas técnicas e salvaguardas administrativas que possam vir a ser adotadas para promover o uso seguro de ativos da informação;

III - apoiar a gestão de acessos aos sistemas e aos ativos de informação;

IV - prevenir, detectar, registrar e apoiar a resposta a incidentes de segurança da informação relacionados aos recursos tecnológicos;

V - colaborar com as unidades administrativas e escolares na adoção de soluções tecnológicas seguras;

VI - observar as diretrizes, normas e orientações técnicas expedidas pelo PRODEST e demais atos normativos vigentes e aplicáveis.

MINUTA

Seção III

Das Responsabilidades dos Usuários da Informação

Art. 22. Compete às unidades administrativas e escolares da SEDU e ao CEE-ES:

I - observar e cumprir as disposições desta Política e de suas normas complementares;

II - zelar pela adequada proteção das informações e dos ativos de informação sob sua responsabilidade;

III - realizar, no âmbito de suas competências e atribuições legais, a correta classificação das informações produzidas, recebidas ou custodiadas no âmbito de suas atividades;

IV - comunicar tempestivamente à instância competente a ocorrência ou a suspeita de incidentes de segurança da informação, observando os canais, procedimentos e prazos definidos em normas complementares e em conformidade com a legislação vigente e aplicável;

V - colaborar com ações de gestão de riscos, auditorias, avaliações e demais iniciativas relacionadas à segurança da informação.

Art. 23. Compete a todos os usuários da informação:

I - utilizar informações e ativos de informação exclusivamente para fins institucionais legítimos e compatíveis com suas atribuições;

II - respeitar a classificação da informação e os controles de acesso estabelecidos;

III - proteger credenciais, dispositivos, documentos e meios de acesso sob sua responsabilidade contra acessos não autorizados ou usos indevidos;

IV - comunicar imediatamente a ocorrência ou a suspeita de incidentes de segurança da informação;

V - participar das campanhas de capacitação e conscientização sobre práticas de segurança da informação;

VI - observar as disposições desta Política e das normas complementares.

MINUTA

Seção IV

Da Articulação Institucional e da Responsabilização

Art. 24. A implementação e o cumprimento desta Política Interna deverão observar, de forma integrada, as diretrizes estaduais de segurança da informação, transformação digital, gestão de riscos e continuidade de serviços.

Art. 25. O descumprimento das disposições desta Política poderá ensejar a adoção das medidas administrativas, civis e penais cabíveis, nos termos da legislação vigente, sem prejuízo de outras sanções previstas em normas específicas.

Art. 26. A apuração de responsabilidades decorrentes de incidentes de segurança da informação observará os princípios do contraditório, da ampla defesa, da proporcionalidade e da razoabilidade, nos termos da legislação aplicável.

CAPÍTULO V

DA SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DA TRANSFORMAÇÃO DIGITAL E DO USO DE INTELIGÊNCIA ARTIFICIAL

Art. 27. A Política Interna de Segurança da Informação da Secretaria de Estado da Educação do Espírito Santo será implementada de forma integrada às iniciativas de transformação digital, governo digital e inovação tecnológica adotadas no âmbito institucional, observadas as diretrizes estaduais vigentes.

§ 1º A segurança da informação constitui elemento essencial e indissociável da transformação digital, devendo ser considerada desde a concepção, o desenvolvimento, a contratação, a implantação, a operação e a descontinuação de sistemas, serviços, processos e soluções tecnológicas utilizados pela SEDU.

§ 2º As iniciativas de transformação digital deverão observar, de forma proporcional aos riscos envolvidos, medidas técnicas e organizacionais destinadas a assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações e dos ativos de informação.

Art. 28. A contratação, o desenvolvimento ou a adoção de projetos, produtos ou serviços de tecnologias digitais de informação, pelas unidades administrativas e

MINUTA

escolares da SEDU e pelo CEE-ES, que envolvam o tratamento de informações institucionais ou de dados pessoais, a integração com outros sistemas, acessos externos ou impactos na continuidade dos serviços educacionais, deverá ser precedida de avaliação de riscos de segurança da informação formalizada em conformidade com os normativos institucionais, considerando:

I - a natureza e a sensibilidade das informações envolvidas;

II - a existência de dados pessoais, especialmente de crianças e adolescentes;

III - o grau de exposição a acessos externos, integrações ou compartilhamentos;

IV - os impactos potenciais à continuidade dos serviços educacionais e à segurança institucional.

§ 1º A avaliação de riscos referida no caput deverá ser compatível com a complexidade da solução tecnológica e com a realidade operacional das unidades administrativas e escolares da SEDU e do CEE-ES.

§ 2º A avaliação de riscos referida no caput deverá contar com o apoio do Encarregado Interno e poderá subsidiar a elaboração de documentos regulatórios aplicáveis, nas hipóteses em que a solução tecnológica envolver dados pessoais.

Art. 29. O uso de sistemas, ferramentas ou soluções baseadas em Inteligência Artificial (IA) no âmbito da SEDU deverá observar, além da legislação vigente, os princípios da segurança da informação, da proteção de dados pessoais, da equidade e não-discriminação, da transparência e do interesse público.

§ 1º Para os fins desta Política, considera-se Inteligência Artificial o conjunto de sistemas computacionais capazes de realizar análises, gerar conteúdos, formular recomendações ou apoiar processos decisórios a partir de dados ou modelos automatizados.

§ 2º O uso de IA no âmbito institucional terá caráter **auxiliar e complementar**, não substituindo o juízo crítico, a responsabilidade funcional ou a tomada de decisão humana, permanecendo o agente público ou o colaborador externo responsável pelas implicações decorrentes do uso das soluções desenvolvidas com auxílio desse recurso tecnológico.

MINUTA

Art. 30. O uso institucional de sistemas de Inteligência Artificial deverá observar, no mínimo, os seguintes princípios e diretrizes:

I - supervisão humana obrigatória, assegurando que os resultados produzidos por sistemas de IA sejam analisados, validados e assumidos por usuário responsável, garantindo-se a capacidade de intervenção humana, quando necessário;

II - verificabilidade e precisão, exigindo a conferência das informações, referências e conclusões sugeridas por sistemas de IA antes de sua utilização institucional;

III - segurança da informação e confidencialidade institucional, vedando o uso de IA de forma que exponha informações protegidas ou estratégicas, bem como o uso de ativos da informação ou dados sob guarda das unidades administrativas e escolares da SEDU e do CEE-ES para treinamento de modelos;

IV - transparência e rastreabilidade, garantindo que o uso de IA seja identificável e auditável, quando aplicável;

V - proteção de dados pessoais, em especial de crianças e adolescentes, observando-se a legislação específica e os princípios da minimização e da finalidade;

VI - prevenção de vieses discriminatórios, especialmente em contextos educacionais, avaliativos ou decisórios, mediante uso monitorado para assegurar que os resultados obtidos não tenham viés potencialmente discriminatório;

VII - finalidade pública, assegurando que o uso de IA esteja alinhado às competências institucionais da SEDU.

Art. 31. É vedado o uso de sistemas de Inteligência Artificial, no âmbito das unidades administrativas e escolares da SEDU e do CEE-ES, para:

I - tratamento direto ou indireto de informações classificadas, sigilosas ou protegidas por sigilo legal, salvo quando expressamente autorizado em norma específica;

MINUTA

II - tratamento direto ou indireto de dados pessoais, sensíveis ou excessivos, desnecessários à finalidade pretendida, nos termos da Lei Federal n.º 13.709/2018 (LGPD);

III - treinamento, alimentação, ajuste ou aprimoramento de modelos de IA externos com dados ou informações institucionais, salvo mediante autorização formal da Administração;

IV - substituição automática da análise técnica, pedagógica, administrativa ou decisória humana.

Art. 32. Os usuários da informação permanecem integralmente responsáveis pelos conteúdos, análises, decisões e documentos produzidos com o auxílio de sistemas de IA, inclusive quanto à exatidão das informações, à conformidade legal e à observância desta Política.

Parágrafo único. Eventuais falhas, inconsistências, incidentes ou riscos decorrentes do uso de IA deverão ser comunicados às instâncias competentes, nos termos das normas de segurança da informação e de gestão de incidentes vigentes.

Art. 33. As diretrizes específicas, os procedimentos operacionais, as soluções autorizadas, os fluxos de uso, os controles técnicos e as capacitações relacionadas ao uso institucional de Inteligência Artificial serão disciplinados em normas complementares, observado o disposto nesta Política.

CAPÍTULO VI
DA PROTEÇÃO DE CRIANÇAS E ADOLESCENTES NO AMBIENTE DIGITAL

Art. 34. A Secretaria de Estado da Educação do Espírito Santo adotará medidas técnicas, administrativas e pedagógicas destinadas a assegurar a proteção integral de crianças e adolescentes no ambiente digital, nos termos da Lei Federal nº 8.069, de 13 de julho de 1990 (ECA), da Lei Federal nº 13.709/2018 (LGPD) e da Lei nº 15.211, de 17 de setembro de 2025 (ECA Digital), aplicáveis aos produtos e serviços de tecnologia da informação utilizados ou disponibilizados sob sua responsabilidade.

MINUTA

§ 1º As medidas de que trata o caput observarão os princípios da prioridade absoluta e do melhor interesse da criança e do adolescente, considerando os riscos específicos decorrentes do uso de tecnologias digitais no contexto educacional.

§ 2º As medidas de que trata o caput aplicam-se a todo produto ou serviço de tecnologia da informação direcionado a crianças e a adolescentes no âmbito das atividades desenvolvidas pela SEDU ou de acesso provável por eles, nos termos do ECA Digital.

Art. 35. Os produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles devem garantir a proteção prioritária desses usuários, ter como parâmetro o seu melhor interesse e contar com medidas adequadas e proporcionais para assegurar um nível elevado de privacidade, de proteção de dados e de segurança, nos termos definidos na legislação vigente e aplicável.

§1º A criança e o adolescente têm o direito de ser educados, orientados e acompanhados por seus pais ou responsáveis legais quanto ao uso da internet e à sua experiência digital, e a estes incumbe o exercício do cuidado ativo e contínuo, por meio da utilização de ferramentas de supervisão parental adequadas à idade e ao estágio de desenvolvimento da criança e do adolescente.

§2º A atuação da família prevista neste artigo não afasta o dever concorrente das unidades administrativas e escolares da SEDU na promoção da educação digital e no fomento ao uso seguro, ético e responsável das tecnologias da informação no ambiente escolar.

§3º A adoção e a disponibilização de produtos e serviços de tecnologias digitais de informação e comunicação pelas unidades administrativas e escolares da SEDU deverão observar estrita intencionalidade pedagógica, compatibilidade com a faixa etária dos estudantes e conformidade com as diretrizes de classificação indicativa estabelecidas pelo órgão competente.

Art. 36. A utilização de produtos ou serviços de tecnologia da informação por crianças e adolescentes tem como fundamentos:

MINUTA

I - a garantia de sua proteção integral;

II - a prevalência absoluta de seus interesses;

III - a condição peculiar de pessoa em desenvolvimento biopsicossocial;

IV - a segurança contra intimidação, exploração, abuso, ameaça e outras formas de violência;

V - o respeito à autonomia e ao desenvolvimento progressivo do indivíduo;

VI - a proteção contra a exploração comercial;

VII - a observância dos princípios estabelecidos na Lei Federal n.º 13.146/2015 (Estatuto da Pessoa com Deficiência);

VIII - a promoção da Educação Digital, com foco no desenvolvimento da cidadania e do senso crítico para o uso seguro e responsável da tecnologia; e

IX - a transparência e a responsabilidade no tratamento de dados pessoais de crianças e de adolescentes.

Art. 37. Os produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão observar, por padrão e desde a concepção, os deveres de prevenção, de segurança, de proteção, de privacidade e de informação previstos nesta Política e na legislação vigente e aplicável, em conformidade com o princípio do melhor interesse da criança e do adolescente e da sua proteção integral, especial e prioritária.

§ 1º Os fornecedores dos produtos ou serviços de tecnologia da informação contratados pelas unidades administrativas e escolares da SEDU e pelo CEE-ES deverão adotar as medidas técnicas adequadas, inclusive mecanismos de segurança amplamente reconhecidos, que possibilitem à família e aos responsáveis legais prevenir o acesso e o uso inadequado por crianças e adolescentes, quando aplicável.

§ 2º Para os fins desta Política, considera-se como expressão do melhor interesse da criança e do adolescente a proteção de sua privacidade, segurança, saúde mental e física, acesso à informação, liberdade de participação na sociedade, acesso significativo às tecnologias digitais e bem-estar.

MINUTA

§ 3º As recomendações e orientações emitidas pela Autoridade Administrativa Autônoma de Proteção dos Direitos de Crianças e de Adolescentes no Ambiente Digital, quando existentes e aplicáveis à Administração Pública, deverão ser consideradas pela SEDU no aperfeiçoamento contínuo de suas práticas, observadas as competências institucionais e a legislação vigente.

Art. 38. Os sistemas, plataformas digitais, ambientes virtuais de aprendizagem, aplicações e serviços tecnológicos, adquiridos, licenciados, contratados, utilizados ou disponibilizados pelas unidades administrativas e escolares da SEDU e pelo CEE-ES deverão ser avaliados quanto aos riscos específicos à segurança da informação e à proteção integral de crianças e adolescentes.

§ 1º A avaliação de riscos referida no caput deverá considerar, especialmente, se o produto ou serviço de tecnologia da informação é direcionado a crianças e adolescentes ou se apresenta acesso provável por esse público, em razão de sua atratividade, facilidade de uso ou potencial impacto à privacidade, à segurança ou ao desenvolvimento biopsicossocial.

§ 2º A avaliação de riscos referida no caput também deverá considerar, entre outros aspectos, se há possibilidades de:

I - coleta excessiva de dados pessoais;

II - exposição indevida de informações;

III - acesso não autorizado;

IV - perfilamento ilícito ou abusivo do usuário, incompatível com o interesse público e com as finalidades públicas da SEDU;

V - monitoramento incompatível com as finalidades informadas;

VI - inferências automatizadas incompatíveis com o interesse público e com as finalidades públicas da SEDU;

VII - compartilhamento indevido de dados com terceiros, em desconformidade com o previsto na legislação vigente e aplicável.

MINUTA

Art. 39. É vedada a utilização, no âmbito das unidades administrativas e escolares da SEDU e do CEE-ES, de sistemas, plataformas ou ferramentas digitais que:

I - exponham crianças e adolescentes a riscos à sua integridade física, psíquica ou moral;

II - realizem tratamento de dados pessoais de forma incompatível com o interesse público e com as finalidades públicas da SEDU;

III - promovam práticas de vigilância excessiva, monitoramento indevido ou perfilamento abusivo, incompatíveis com o interesse público e com as finalidades públicas da SEDU;

IV - compartilhem dados pessoais de crianças e adolescentes sem base legal adequada.

Parágrafo único. As vedações previstas neste artigo deverão ser observadas à luz do contexto educacional, das finalidades pedagógicas legítimas, da proporcionalidade das medidas adotadas e do melhor interesse da criança e do adolescente, sem prejuízo da adoção de salvaguardas técnicas e administrativas adequadas.

Art. 40. As unidades administrativas e escolares da SEDU e o CEE-ES, quando responsáveis pela aquisição, licenciamento, contratação, desenvolvimento, utilização ou disponibilização de sistemas, plataformas digitais, ambientes virtuais de aprendizagem, aplicações ou outros produtos ou serviços de tecnologia da informação, deverão implementar cuidados reforçados quando envolver interações, dados ou conteúdos relacionados a crianças e adolescentes.

§ 1º Os produtos ou serviços de tecnologia da informação aos quais se refere o *caput* deste artigo devem:

I - adotar, por padrão e desde a concepção, a configuração no modelo mais protetivo em relação à privacidade, à proteção de dados e à segurança dos estudantes, principalmente quando se tratar de crianças e adolescentes, em observância ao disposto no art. 7º da Lei Federal n.º 15.211/2025;

MINUTA

II - operar, por padrão, com o grau mais elevado de proteção da privacidade e dos dados pessoais, observando-se a obrigatoriedade da disponibilização de informações claras, acessíveis e adequadas para que a criança ou o adolescente e seus responsáveis possam exercer escolhas informadas quanto à eventual adoção de configurações menos protetivas;

§ 2º As unidades administrativas e escolares da SEDU e o CEE-ES deverão abster-se de utilizar os produtos ou serviços de tecnologia da informação aos quais se refere o *caput* deste artigo quando estes realizarem o tratamento dos dados pessoais de crianças e de adolescentes de forma que causem, facilitem ou contribuam para a violação de sua privacidade ou de quaisquer outros direitos a eles assegurados em lei, observados os princípios previstos no art. 6º da LGPD, e o melhor interesse da criança e do adolescente.

§ 3º Quanto aos produtos e serviços de tecnologia da informação aos quais se refere o *caput* deste artigo, as unidades administrativas e escolares da SEDU e o CEE-ES deverão:

I - realizar avaliação do conteúdo disponibilizado para crianças e adolescentes de acordo com a faixa etária, para que seja compatível com a respectiva classificação indicativa;

II - adotar sistemas e processos projetados para impedir que crianças e adolescentes encontrem, por meio do produto ou serviço ofertado, conteúdos ilegais e pornográficos, bem como outros conteúdos manifestamente inadequados à sua faixa etária, conforme as normas de classificação indicativa e a legislação aplicável;

III - garantir que, no momento do acesso, todos os usuários sejam informados extensivamente sobre a faixa etária indicada para o produto ou serviço, conforme estabelecido pela política de classificação indicativa.

IV - realizar avaliação de impacto à segurança e à saúde dos estudantes, conforme determina o art. 47 do Decreto Federal n.º 12.880/2026, contendo:

a) identificação e análise de riscos;

b) avaliação da probabilidade de ocorrência e da gravidade do impacto potencial;

MINUTA

c) tratamento e mitigação dos riscos, e

d) acompanhamento contínuo da efetividade das medidas adotadas.

Art. 41. A SEDU promoverá ações de orientação, capacitação e conscientização sobre segurança da informação, proteção de dados pessoais e uso seguro de tecnologias digitais voltadas a servidores, gestores escolares, professores, estudantes e responsáveis legais, respeitadas as atribuições de cada público.

Parágrafo único. As ações referidas no caput deverão considerar a linguagem adequada, a faixa etária, o contexto escolar e a promoção da cidadania digital.

Art. 42. Os incidentes de segurança da informação que envolvam dados pessoais de crianças e adolescentes deverão receber tratamento prioritário, observadas as normas internas de gestão de incidentes e a legislação vigente.

Parágrafo único. Sempre que aplicável, deverão ser adotadas medidas para mitigar danos, comunicar responsáveis legais e assegurar a proteção dos direitos dos titulares, observados os prazos, critérios e procedimentos previstos na legislação de proteção de dados pessoais e nas normas internas da SEDU.

Art. 43. As diretrizes específicas, os procedimentos operacionais e os instrumentos complementares relacionados à proteção de crianças e adolescentes no ambiente digital serão disciplinados em normas próprias, observadas as disposições desta Política.

Art. 44. Na contratação, adoção ou disponibilização de produtos e serviços de tecnologia da informação de acesso provável por crianças e adolescentes, as unidades administrativas e escolares da SEDU deverão considerar critérios de segurança da informação, proteção de dados pessoais e proteção integral, exigindo conformidade com a legislação vigente e com esta Política.

CAPÍTULO VII
DAS NORMAS COMPLEMENTARES E DOS INSTRUMENTOS OPERACIONAIS

Art. 45. A implementação, a operacionalização e o detalhamento técnico das disposições desta Política Interna de Segurança da Informação poderão ser

MINUTA

disciplinados por normas complementares e instrumentos operacionais, a serem expedidos por meio de atos administrativos próprios.

Art. 46. Constituem normas complementares e instrumentos operacionais, entre outros:

I - normas de procedimento;

II - manuais, guias e orientações técnicas;

III - padrões de segurança da informação e de tecnologia da informação;

IV - fluxos operacionais e administrativos;

V - modelos, formulários e documentos padronizados;

VI - planos, programas e protocolos específicos; e

VII - demais instrumentos necessários à efetiva implementação desta Política.

Art. 47. As normas complementares e os instrumentos operacionais de que trata este Capítulo:

I - poderão conter anexos, formulários, modelos, checklists e outros elementos técnicos;

II - poderão ser atualizados, revisados ou substituídos com maior frequência do que esta Política, sempre que necessário ao aprimoramento da segurança da informação; e

III - deverão observar, obrigatoriamente, as disposições desta Política Interna.

Art. 48. A elaboração, a revisão e a aplicação das normas complementares e dos instrumentos operacionais deverão observar, no que couber:

I - a Política Estadual de Segurança da Informação (PESI);

II - as normas, diretrizes e orientações técnicas expedidas pelo PRODEST;

III - as deliberações e recomendações do Comitê Estadual de Segurança da Informação (CESI);

MINUTA

IV - as diretrizes de governança digital, tecnologia da informação e segurança da informação estabelecidas pela Secretaria de Gestão e Recursos Humanos (SEGER); e

V - a legislação vigente aplicável.

Art. 49. As normas complementares e os instrumentos operacionais deverão ser amplamente divulgados às unidades administrativas e escolares da SEDU e ao CEE-ES, observadas as restrições decorrentes da classificação da informação e dos requisitos de segurança da informação.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 50. A observância desta Política não exclui o cumprimento das demais normas legais, regulamentares e institucionais aplicáveis à segurança da informação, à proteção de dados pessoais, à transparência pública, à gestão documental e à governança digital.

Art. 51. Os casos omissos e as dúvidas decorrentes da aplicação desta Política serão dirimidos pela SEDU, com o apoio das instâncias internas de governança, à luz da legislação e das normas vigentes e aplicáveis, recorrendo-se às instâncias estaduais competentes quando necessário.

Art. 52. Esta Política Interna deverá ser periodicamente avaliada e poderá ser revisada, total ou parcialmente, sempre que constatada a necessidade de sua atualização, especialmente em razão de:

I - alterações relevantes na legislação ou em normativos superiores;

II - mudanças significativas no contexto tecnológico, organizacional ou institucional;

III - ocorrência de incidentes relevantes de segurança da informação;

IV - recomendações do Comitê Interno de Governança de Dados (CIGD); ou

V - deliberação do Comitê Estratégico de Governança de Dados (CEGD).

MINUTA

Parágrafo único. Compete ao Comitê Interno de Governança de Dados (CIGD) apoiar tecnicamente a avaliação e a proposição de revisões desta Política, observado o disposto nos normativos institucionais vigentes.

Art. 53. As unidades administrativas e escolares da SEDU e o CEE-ES deverão promover, de forma progressiva, a adequação de suas rotinas, processos de trabalho e práticas institucionais às disposições desta Política e de suas normas complementares, no prazo estabelecido em Plano de Implementação a ser editado pelo CIGD, assegurando-se o apoio técnico e pedagógico necessário à sua efetivação.

Art. 54. Ficam revogadas quaisquer disposições normativas internas anteriores que se manifestem em sentido contrário a esta Política sobre a Segurança da Informação no âmbito da SEDU.

Art. 55. Esta Portaria entra em vigor na data de sua publicação.

Vitória, XX de outubro de 2026.

ANDREA GUZZO PEREIRA

Secretária de Estado da Educação

MINUTA