IOMAT
Superintendência da Imprensa Oficial do Estado de Mato Grosso
Protocolo: ***1688634***
Data: ***30/04/2025***
Título: ***DECRETO 1428-25***
Página(s): ***4 a 6***

DECRETO Nº 1.428, DE 30 DE ABRIL DE 2025.

Institui a Política de Segurança da Informação do Poder Executivo do Estado de Mato Grosso, e dá outras providências.

O GOVERNADOR DO ESTADO DE MATO GROSSO, no uso da atribuição que lhe confere o art. 66, inciso III, da Constituição Estadual, tendo em vista o que consta no Processo SEPLAG-PRO-2025/03937, e

CONSIDERANDO o disposto no art. 24, VI da Lei Complementar Estadual nº 612, de 28 de janeiro de 2019, que estabelece competência à Secretaria de Estado de Planejamento e Gestão de Mato Grosso para gerir os sistemas centrais de informações e tecnologia da informação do Poder Executivo;

CONSIDERANDO a Lei Federal nº 12.527, de 18 de novembro de 2011, conhecida como Lei de Acesso à Informação (LAI);

CONSIDERANDO a Lei Federal nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO o Decreto Federal nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação (PNSI), no âmbito da administração pública federal;

CONSIDERANDO o disposto nas normas ABNT NBR/ISO/IEC 27001:2022, 27002:2022, 27701:2022, 27005:2023, que estabelecem requisitos, diretrizes e controles de segurança da informação, cibersegurança e proteção da privacidade;

CONSIDERANDO o Decreto Estadual nº 806, de 22 de janeiro de 2021, que regulamenta a aplicação da Lei Federal nº 12.527, de 18 de novembro de 2011 (acesso às informações), no âmbito do Poder Executivo;

CONSIDERANDO o Decreto Estadual nº 951, de 20 de maio de 2021, que institui o Sistema de Governança Digital no Poder Executivo Estadual;

CONSIDERANDO o Decreto Estadual nº 1.208 de 21 de dezembro de 2021, que dispõe sobre o Sistema Estadual de Tecnologia da Informação - SETI no âmbito do Poder Executivo do Estado de Mato Grosso; e

CONSIDERANDO o Decreto Estadual nº 338, de 20 de junho de 2023, que institui a Agenda Estratégica Digital do Governo de Mato Grosso para o período de 2023 a 2027, no âmbito dos órgãos e entidades do Poder Executivo estadual,

DECRETA:

Seção I
Das Disposições Gerais

Art. 1º Fica instituída a Política de Segurança da Informação do Poder Executivo do Estado de Mato Grosso (PSI-MT), com o objetivo de assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações no âmbito da administração estadual.

Parágrafo único A PSI-MT será complementada por normas, procedimentos, processos e controles específicos para a gestão da segurança da informação, em conformidade com os planos institucionais e estruturas organizacionais do Poder Executivo Estadual.

Art. 2º Considera-se para fins deste Decreto:

I - **ambiente em nuvem:** infraestrutura de computação que fornece, por meio da internet, acesso a recursos de Tecnologia da Informação - TI, como armazenamento, processamento e software;

II - **configuração e manuseio seguros de dispositivos do usuário:** são práticas e procedimentos destinados a garantir que dispositivos, como computadores, sejam configurados e utilizados forma segura, protegendo contra vulnerabilidades e ameaças de segurança;

III - **controle de acesso:** conjunto de métodos e tecnologias utilizados para regular e gerenciar permissões de acesso a recursos específicos em um sistema ou ambiente, podendo abranger processos como autenticação, autorização e auditoria;

IV - **gestão de ativos físicos e lógicos:** processo integrado de monitoramento, manutenção e otimização de recursos de uma organização, abrangendo ativos tangíveis e intangíveis;

V - **gestão da continuidade de negócio:** processo de planejamento, implementação e monitoramento de medidas que garantam a capacidade de uma organização de manter suas operações mesmo diante de eventos disruptivos, como desastres naturais, falhas de sistemas, pandemias ou outros incidentes graves;

VI - **gestão de incidentes:** processo de resposta e gerenciamento eficiente de incidentes de segurança, como violações de dados, ataques cibernéticos ou outras ameaças à segurança da informação;

VII - **proteção, *backup* e recuperação de dados e informações:** englobam medidas e práticas voltadas para garantir a confidencialidade, integridade e disponibilidade dos dados e informações de uma organização;

VIII - **segurança de redes:** abrange medidas e práticas destinadas a proteger as redes de uma organização contra acessos não autorizados, ataques cibernéticos, intrusões e outros tipos de ameaças;

IX - **treinamento e conscientização:** são processos complementares destinados a capacitar indivíduos com conhecimentos e habilidades específicas, ao mesmo tempo em que promovem a conscientização sobre a importância de práticas e comportamentos seguros e eficientes;

X - **uso da Inteligência Artificial (IA):** refere-se à aplicação de algoritmos e sistemas computacionais capazes de realizar tarefas que normalmente requerem inteligência humana.

Seção II
Dos Princípios da Política de Segurança da Informação

Art. 3º São princípios norteadores da Política de Segurança da Informação:

I - disponibilidade: garantia de que as informações estão acessíveis às pessoas devidamente autorizadas sempre que necessário ou demandado;

II - prevenção e tratamento de incidentes: conjunto de ações e estratégias destinadas a identificar, mitigar e responder a ameaças ou vulnerabilidades;

III - cultura: adoção da segurança da informação como um elemento essencial para sua organização;

IV - confidencialidade: assegura que somente pessoas autorizadas tenham acesso às informações;

V - integridade: garantia que alterações, supressões e adições sejam realizadas apenas por pessoas devidamente autorizadas;

VI - autenticidade: certificação de que uma informação, produto ou documento pertence ao autor a quem se atribui;

VII - não repúdio: garantia de que um autor participante numa operação não possa negar sua participação ou autoria.

Seção III
Dos Objetivos da Política de Segurança da Informação

Art. 4º São objetivos específicos da Política de Segurança da Informação:

I - implantar a gestão da segurança da informação nas unidades administrativas do Poder Executivo Estadual;

II - capacitar servidores para uso adequado dos recursos informacionais, identificação de ataques e ameaças cibernéticas;

III - assegurar a interoperabilidade e o intercâmbio de informações na Administração Pública do Poder Executivo Estadual;

IV - garantir a continuidade dos serviços mediante gestão ativa de ameaças, vulnerabilidades, incidentes e riscos;

V - padronizar as atividades de gestão de segurança da informação nas unidades da Administração Pública do Poder Executivo Estadual;

VI - definir e manter a estrutura de controles de segurança da informação;

VII - promover a proteção de informações confidenciais.

Seção IV
Das Diretrizes para a Implementação de Procedimentos de Segurança da Informação

Art. 5º Os órgãos e entidades do Poder Executivo Estadual devem implementar procedimentos de acordo com as diretrizes da Política de Segurança da Informação estabelecidas pela Secretaria de Estado de Planejamento e Gestão, órgão central de governança de dados e informações, relativos aos seguintes temas:

I - controle de acesso;
II - proteção, *backup* e recuperação de dados e informações;
III - gestão de ativos físicos e lógicos;
IV - treinamento e conscientização;
V - configuração e manuseio seguros de dispositivos do usuário;
VI - segurança de redes;
VII - gestão de incidentes;
VIII - gestão da continuidade de negócio;
IX - ambiente em nuvem;
X - uso da Inteligência Artificial (IA).

Seção V
Do Comitê Central de Governança da Política de Segurança da Informação

Art. 6º Fica instituído o Comitê Central de Governança da Política de Segurança da Informação, composto por membros da Secretaria de Estado de Planejamento e Gestão, responsáveis pelas áreas centrais de dados e informações, de tecnologia da informação e de transformação digital, com as seguintes atribuições:

I - monitorar a implementação da PSI-MT nos órgãos e entidades do Poder Executivo Estadual;

II - avaliar relatórios periódicos de desempenho e incidentes relacionados à segurança da informação;

III - propor revisões e aprimoramento nas normativas que regulamentam à PSI-MT;

IV - promover a integração da PSI-MT com as políticas de governo digital e proteção de dados pessoais.

Parágrafo único A coordenação do comitê instituído no *caput* deste artigo será exercida pela área central de dados e informações da Secretaria de Estado de Planejamento e Gestão.

Seção VI
Das Competências

Art. 7º Compete aos órgãos e as entidades do Poder Executivo Estadual, em seu âmbito de atuação:

I - apoiar e exigir a implementação da Política de Segurança da Informação;

II - designar um Gestor Setorial de Segurança da Informação, com capacidade e competências adequadas;

III - instituir o Comitê Setorial de Segurança da Informação, composto, obrigatoriamente, pelo Gestor Setorial de Segurança da Informação;

IV - fomentar ações de capacitação e profissionalização relacionadas à segurança da informação.

Art. 8º Compete ao Gestor Setorial de Segurança da Informação dos órgãos e entidades, a que se refere o inciso II do art. 7º deste Decreto:

I - coordenar o Comitê Setorial de Segurança da Informação;

II - planejar, implementar e gerenciar as ações da Política de Segurança da Informação;

III - consolidar e analisar os resultados das auditorias relacionadas à gestão de segurança da informação;

IV - propor, atualizar e gerenciar normas internas relativas à segurança da informação;

V - monitorar o desempenho e avaliar a implementação e os resultados da Política de Segurança da Informação e das normas internas relacionadas ao tema;

VI - apoiar a alta administração na tomada de decisão referente à Política de Segurança da Informação;

VII - exigir a execução e o cumprimento dos procedimentos relativos aos temas previstos no art. 5º deste Decreto, observando as diretrizes da SEPLAG;

VIII - cooperar e subsidiar o Comitê Central de Governança da Segurança da Informação com informações técnicas, gerenciais e indicadores de conformidade.

§ **1º** O Gestor Setorial de Segurança da Informação deverá observar as normativas que instruem procedimentos buscando resguardar a continuidade de processos organizacionais em casos de incidentes de segurança da informação, decorrentes de desastres ou falhas em recursos de tecnologia da informação e comunicação.

§ **2º** O Gestor Setorial de Segurança da Informação, a critério de cada órgão ou entidade, poderá acumular a atribuição de Encarregado de Proteção de Dados, previsto no inciso VIII do art. 5º da Lei Federal nº 13.709 de 14 de agosto de 2018.

§ **3º** O Gestor Setorial de Segurança da Informação deve possuir formação ou experiência mínima comprovada nas áreas de tecnologia da informação, segurança da informação, gestão de riscos ou outra área correlata.

Art. 9º Compete ao Comitê Setorial de Segurança da Informação, a que se refere o inciso III do art. 7º deste Decreto:

I - auxiliar o Gestor Setorial de Segurança da Informação na implementação das ações de segurança da informação;

II - propor à SEPLAG alterações na Política de Segurança da Informação;

III - propor normas internas relativas à segurança da informação;

IV - sugerir medidas e procedimentos para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;

V - propor práticas de gestão de ativos de tecnologia da informação a partir do inventário das áreas de ambiente tecnológico, equipamentos de tecnologia, softwares, banco de dados e dados pessoais.

Art. 10 Compete aos usuários da informação:

I - cumprir as normas de segurança da informação estabelecidas;

II - zelar pela segurança da informação e comunicação;

III - comunicar à área competente os incidentes ou irregularidades de segurança da informação;

IV - propor melhorias à segurança da informação e comunicação;

V - garantir o sigilo e evitar o vazamento de dados e informações, não classificados como públicos, que estejam sob sua responsabilidade e/ou acesso;

VI - assegurar o uso racional dos recursos de tecnologia da informação e comunicação colocados à sua disposição, priorizando o interesse público e institucional.

Parágrafo único Os usuários da informação que propuserem melhorias ou identificarem vulnerabilidades relevantes na segurança da informação poderão receber reconhecimento formal, nos termos de instrução normativa a ser publicada pela Secretaria de Estado de Planejamento e Gestão.

Seção VII
Das Disposições Transitórias e Finais

Art. 11 Fica instituído o acompanhamento contínuo da implementação da Política de Segurança da Informação, por meio de indicadores de desempenho (*key performance indicators*), a serem definidos por instrução normativa específica da SEPLAG, tais como:

I - percentual de servidores capacitados anualmente em segurança da informação;
II - número de incidentes de segurança identificados e tratados anualmente;
III - nível de conformidade das unidades administrativas com as normas da PSI-MT, medido por auditorias internas.

Art. 12 A Secretaria de Estado de Planejamento e Gestão poderá estabelecer parcerias e convênios com órgãos federais, estaduais e municipais, entidades públicas e privadas, e organizações internacionais para:

I - troca de informações e boas práticas em segurança da informação;
II - realização de treinamentos e eventos conjuntos;
III - acesso a tecnologias e recursos especializados.

Art. 13 A desobediência ou violação das disposições desta Política de Segurança da Informação, estabelecidas neste Decreto e suas normas complementares implicará na aplicação de sanções administrativas, nos termos da legislação vigente, sem prejuízo das responsabilidades penal e civil.

Art. 14 A SEPLAG deverá revisar esta Política de Segurança da Informação periodicamente, ao menos a cada 2 (dois) anos, ou em caso de mudanças legislativas ou incidentes significativos que demandem sua revisão.

Art. 15 A implementação da Política de Segurança da Informação será realizada de forma escalonada, conforme o seguinte cronograma:

I - designação de Gestores Setoriais de Segurança da Informação e constituição dos Comitês Setoriais de Segurança da Informação, no prazo de 60 (sessenta) dias, contados da publicação deste Decreto;
II - capacitação inicial de servidores em segurança da informação, no prazo de 120 (cento e vinte) dias, contados da publicação deste Decreto;
III - adequação tecnológica e implementação das ações previstas no art. 5º deste Decreto, nos prazos estabelecidos nas Instruções Normativas da SEPLAG.

Art. 16 A Secretaria de Estado de Planejamento e Gestão, órgão central de dados e de informações, será responsável por dirimir os casos omissos e poderá expedir normas complementares que se fizerem necessárias ao fiel cumprimento deste Decreto.

Parágrafo único A SEPLAG deverá expedir no prazo de até 180 (cento e oitenta) dias após a publicação deste Decreto, as instruções normativas regulamentando:

I - diretrizes da Política de Segurança da Informação dos temas relacionados no art. 5º deste Decreto;
II - os indicadores de desempenho;
III - os critérios para capacitação e designação de gestores de segurança da informação;
IV - os mecanismos de reporte e tratamento de incidentes de segurança.

Art. 17 Fica revogada a Resolução COSINT nº 003/2010, publicada no Diário Oficial do Estado de Mato Grosso em 09 de março de 2010.

Art. 18 Este Decreto entra em vigor na data de sua publicação.

Palácio Paiaguás em Cuiabá, 30 de abril de 2025, 204º da Independência e 137º da República.

MAURO MENDES
Governador do Estado

FÁBIO GARCIA
Secretário-Chefe da Casa Civil

BASILIO BEZERRA GUIMARÃES DOS SANTOS
Secretário de Estado de Planejamento e Gestão