

PORTARIA Nº 033/2025/MT-SAUDE

Institui a Política de Segurança da Informação, no âmbito do Instituto de Assistência à Saúde dos Servidores do Estado - Mato Grosso Saúde, e elenca suas atribuições, conforme preceitua o Decreto n.º 1.428, de 30 de abril de 2025.

A Presidente do Instituto de Assistência à Saúde dos Servidores do Estado - Mato Grosso Saúde, no uso de suas atribuições legais; e

CONSIDERANDO o artigo 7º, inciso II, do Decreto nº 1.428, de 30 de abril de 2025;

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

CAPÍTULO I - DAS DEFINIÇÕES

Art. 1º (Objetivo) Fica instituída a Política Setorial de Segurança da Informação (PSSI) do Instituto de Assistência à Saúde dos Servidores do Estado, em conformidade com a Política de Segurança da Informação do Poder Executivo do Estado de Mato Grosso (PSI-MT), instituída pelo Decreto nº 1.428/2025. Esta política visa estabelecer os princípios, as diretrizes e as responsabilidades para proteger os ativos de informação, assegurando sua disponibilidade, integridade, confidencialidade e autenticidade.

Art. 2º (Escopo) Esta Política aplica-se a todos os servidores, empregados públicos, estagiários, prestadores de serviço e quaisquer outros indivíduos que acessem, manuseiem ou utilizem os ativos de informação, dados, sistemas e recursos de tecnologia da informação sob a responsabilidade do Instituto de Assistência à Saúde dos Servidores do Estado, em qualquer localidade, incluindo regime de trabalho remoto.

Art. 3º (Definições) Para os fins desta Política, aplicam-se os termos do Glossário de Segurança da Informação do Gabinete de Segurança Institucional (GSI/PR), da Lei Geral de Proteção de Dados (LGPD) e do Art. 2º do Decreto nº 1.428/2025, destacando-se:

I. Ativo de Informação: Dados, informações, hardware, software, sistemas, serviços, pessoas e instalações que têm valor para o órgão.

II. Confidencialidade: Garantia de que a informação é acessível somente por pessoas autorizadas.

III. Disponibilidade: Garantia de que os usuários autorizados tenham acesso à informação sempre que necessário.

IV. Gestor Setorial de Segurança da Informação: Servidor designado pela Alta Administração para coordenar as ações de segurança da informação no âmbito do órgão.

V. Incidente de Segurança da Informação: Qualquer evento adverso, confirmado ou suspeito, relacionado à segurança dos sistemas ou dos dados.

VI. Integridade: Garantia da exatidão e completude da informação e dos seus métodos de processamento.

CAPÍTULO II - DA GOVERNANÇA E DAS RESPONSABILIDADES

Art. 4º A estrutura de Governança Setorial de Segurança da Informação, subordinada às diretrizes da Secretaria de Estado de Planejamento e Gestão (SEPLAG) e da PSI-MT, é composta por:

I. Alta Administração do Órgão;

II. Gestor Setorial de Segurança da Informação;

III. Comitê Setorial de Segurança da Informação;

IV. Encarregado pelo Tratamento de Dados Pessoais;

V. Usuários da informação.

Art. 5º (Competências da Alta Administração do Órgão) Compete à presidente e aos demais gestores de alto nível do Instituto de Assistência à Saúde dos Servidores do Estado:

I. Apoiar e exigir a implementação e o cumprimento desta Política.

II. Designar formalmente o Gestor Setorial e os membros do Comitê Setorial de Segurança da Informação.

III. Prover os recursos necessários para as ações de segurança da informação e proteção de dados pessoais.

Art. 6º (Competências do Gestor Setorial de Segurança da Informação) Compete ao Gestor Setorial, conforme Art. 8º do Decreto nº 1.428/2025:

I. Coordenar o Comitê Setorial de Segurança da Informação.

II. Planejar e gerenciar a implementação das ações desta Política.

III. Propor e gerenciar as normas internas de segurança da informação.

IV. Monitorar os resultados e reportar à Alta Administração e ao Comitê Central de Governança (SEPLAG).

V. Apoiar a Alta Administração na tomada de decisão referente à segurança da informação.

Art. 7º (Competências do Comitê Setorial de Segurança da Informação) Compete ao Comitê Setorial, conforme Art. 9º do Decreto nº 1.428/2025:

I. Assessorar o Gestor Setorial na implementação desta Política.

II. Propor alterações nesta Política e em suas normas complementares.

III. Deliberar sobre as normas internas de segurança da informação.

IV. Sugerir medidas e procedimentos para garantir a segurança dos ativos de informação.

Art. 8º (Competência do encarregado de proteção de dados) Compete ao encarregado de proteção de dados, conforme Art. 12º da Decreto Nº 1.427/2025:

I - Atuar como canal de comunicação entre o Controlador, os titulares de dados, a Secretaria Adjunta de Planejamento e Governo Digital/SEPLAG e a Autoridade Nacional de Proteção de Dados (ANPD);

II - Monitorar a adoção de providências internas no órgão ou entidade para garantir a conformidade com a LGPD;

III - Monitorar as operações de tratamento de dados para assegurar a conformidade com a LGPD;

IV - Propor medidas para a mitigação de riscos relacionados ao tratamento de dados pessoais;

V - Gerenciar solicitações e reclamações apresentadas por titulares de dados;

VI - Elaborar o Relatório de Impacto à Proteção de Dados (RIPD), com a colaboração dos operadores;

VII - Orientar os operadores do MT Saúde quanto às melhores práticas a serem tomadas à proteção de dados pessoais;

VIII - Reportar imediatamente todas as comunicações com a Autoridade Nacional de Proteção de Dados (ANPD) à Secretaria Adjunta de Planejamento e Governo Digital/SEPLAG e ao Comitê Técnico de Proteção de Dados Pessoais (CTPD).

Art. 9º (Competências dos Usuários da Informação) Compete a todos os usuários, conforme Art. 10 do Decreto nº 1.428/2025:

I. Conhecer e cumprir as diretrizes desta Política e das normas dela decorrentes.

II. Comunicar imediatamente ao gestor da segurança da informação e o comitê de segurança da informação qualquer incidente ou vulnerabilidade de segurança da informação.

III. Zelar pela segurança dos ativos de informação que utiliza, incluindo seu computador, conta de usuário e senha.

IV. Participar dos treinamentos e ações de conscientização promovidos pelo órgão.

CAPÍTULO III - DAS DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Art. 10 O Instituto de Assistência à Saúde dos Servidores do Estado deve implementar processos e controles de segurança, em conformidade com as normas a serem expedidas pela SEPLAG - Secretaria de Planejamento e Gestão, para os temas prioritários definidos no Art. 5º da PSI-MT:

I. Controle de Acesso Lógico:

a. O acesso a sistemas e informações deve ser baseado no princípio do "menor privilégio".

b. O uso de senhas fortes e de Autenticação de Múltiplos Fatores (MFA) é obrigatório para os sistemas críticos e para o acesso remoto.

II. Controle de acesso físico:

a. Devem ser estabelecidos perímetros de segurança física (ex.: paredes, catracas, portas com controle) para proteger as instalações e os ativos de informação do MT Saúde.

b. As áreas físicas devem ser classificadas por níveis de segurança (públicas, restritas e de segurança), e controles de acesso apropriados devem ser implementados para cada nível.

c. O acesso de servidores, prestadores de serviço e visitantes a áreas restritas e de segurança deve ser devidamente autorizado, identificado e registrado.

d. Os procedimentos detalhados para o controle de acesso físico serão definidos em Instrução Normativa específica.

III. Proteção, Backup e Recuperação de Dados:

a. As informações devem ser classificadas quanto à sua sensibilidade (ex.: Pública, Interna, Confidencial).

b. Devem ser executadas rotinas de backup (cópia de segurança) periódicas dos dados críticos.

c. O descarte de mídias (papel, HDs, pen drives) com informações sensíveis deve ser feito de forma a impossibilitar a recuperação dos dados.

IV. Gestão de Ativos Físicos e Lógicos:

a. O MT Saúde deve manter um inventário atualizado de seus principais ativos de tecnologia (servidores, computadores, softwares, sistemas).

V. Treinamento e Conscientização:

a. Devem ser realizadas campanhas e treinamentos periódicos para todos os usuários sobre segurança da informação e proteção de dados pessoais.

VI. Configuração e Manuseio de Dispositivos:

a. Todos os computadores devem possuir software de antivírus homologado e atualizado.

b. É vedada a instalação de softwares não autorizados pela área de TI.

c. O bloqueio de tela automático deve ser configurado em todos os computadores.

VII. Segurança de Redes:

a. O acesso remoto à rede interna do MT Saúde deve ser realizado exclusivamente por meio da VPN (Rede Privada Virtual) homologada.

VIII. Gestão de Incidentes:

a. O MT Saúde deve possuir um procedimento claro para o reporte e tratamento de incidentes de segurança, definindo os canais de comunicação e os responsáveis.

IX. Gestão da Continuidade do Negócio:

a. Os processos de negócio críticos devem ser identificados e devem existir planos para sua continuidade em caso de desastres ou falhas graves.

X. Ambiente em Nuvem:

a. A contratação e o uso de serviços de computação em nuvem devem ser previamente homologados pelo Comitê Setorial, garantindo a segurança e a conformidade contratual.

XI. Uso da Inteligência Artificial (IA):

a. O uso de ferramentas de Inteligência Artificial que envolvam o tratamento de dados institucionais ou pessoais deve ser feito de forma transparente, segura e em conformidade com as diretrizes da SEPLAG e com a LGPD.

CAPÍTULO IV - DAS VEDAÇÕES E DISPOSIÇÕES FINAIS

Art. 11 É expressamente vedado a todos os usuários:

I. Utilizar os recursos do Instituto para finalidades ilegais, ou para acessar, armazenar e distribuir material impróprio ou ofensivo.

II. Instalar softwares, aplicativos ou conectar dispositivos à rede do MT Saúde sem a devida autorização da área de TI.

III. Compartilhar sua senha ou credenciais de acesso com qualquer outra pessoa.

IV. Explorar intencionalmente vulnerabilidades de segurança.

Art. 12 O descumprimento das diretrizes estabelecidas nesta Política sujeita o infrator às sanções administrativas previstas na legislação vigente (ex.: Lei Complementar nº 207/2004), sem prejuízo das responsabilidades civis e penais cabíveis, assegurado o direito ao contraditório e à ampla defesa.

Art. 13 Esta Política será revisada a cada 2 (dois) anos, ou extraordinariamente sempre que houver mudanças significativas no ambiente tecnológico, na legislação ou nas diretrizes da PSI-MT.

Art. 14 Os casos omissos nesta Política serão dirimidos pelo Comitê Setorial de Segurança da Informação do Instituto de Assistência à Saúde dos Servidores do Estado, em alinhamento com o Gestor Setorial e, se necessário, com consulta à SEPLAG.

Art. 15 Esta Portaria entra em vigor na data de sua publicação.

Instituto de Assistência à Saúde dos Servidores do Estado - Mato Grosso Saúde, em Cuiabá-MT, 6 de janeiro de 2026.

Publique-se.

Registre-se.

Cumpra-se.

Misma Thalita dos Anjos Coutinho

Presidente do Mato Grosso Saúde

Superintendência da Imprensa Oficial do Estado de Mato Grosso
Rua Júlio Domingos de Campos - Centro Político Administrativo | CEP 78050-970 | Cuiabá, MT

Código de autenticação: 558beb76

Consulte a autenticidade do código acima em https://iomat.mt.gov.br/legislacao/diario_oficial/consultar