RESOLUÇÃO CGE/MS N. 150, DE 21 DE AGOSTO DE 2026.

Aprova a Política de Segurança da Informação da Controladoria-Geral do Estado de Mato Grosso do Sul (PSI/CGE-MS).

Publicado no DOE n. 12.257, de 24 de agosto de 2026, págs. 12 - 19.

O CONTROLADOR-GERAL DO ESTADO DE MATO GROSSO DO SUL, no uso das atribuições que lhe confere o inciso II do art. 13-A da Lei Complementar Estadual n. 230/2016;

Considerando a necessidade de assegurar a proteção das informações institucionais contra o uso indevido, a perda, a alteração, a destruição, a divulgação ou o acesso não autorizado, em consonância com os princípios constitucionais da Administração Pública;

Considerando a importância da segurança da informação como pilar da governança, da integridade e da transparência pública, de modo a garantir o exercício pleno das funções de controle interno, no exercício das atribuições inerentes às atividades de auditoria interna governamental, inspeção, fiscalização, avaliação de gestão, prevenção à corrupção, ouvidoria, transparência pública e controle social, correição e governança pública e compliance;

Considerando o disposto na Política de Segurança da Informação do Governo do Estado de Mato Grosso do Sul, aprovada pela Deliberação CETI n. 02, de 24 de fevereiro de 2022;

Considerando a observância ao disposto na Lei Federal n. 12.527/2011 (Lei de Acesso à Informação), na Lei Estadual n. 4.416/2013 (Lei de Acesso à Informação no âmbito do Estado de Mato Grosso do Sul), na Lei Federal n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e em outras normas correlatas;

Considerando as boas práticas de governança e gestão da segurança da informação preconizadas nas normas ABNT NBR ISO/IEC 27001, 27002 e 27701;

Considerando o compromisso da Controladoria-Geral do Estado com a preservação da confiabilidade, da integridade, da autenticidade, da rastreabilidade e da disponibilidade das informações sob sua guarda;

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Instituir a Política de Segurança da Informação (PSI/CGE-MS) a fim de estabelecer os princípios, diretrizes, controles e responsabilidades para a proteção das informações produzidas, recebidas, armazenadas, processadas ou transmitidas no âmbito da Controladoria-Geral do Estado de Mato Grosso do Sul (CGE-MS).

§ 1º A PSI/CGE-MS se aplica a todos os agentes públicos, colaboradores, estagiários, consultores, fornecedores e visitantes que acessem, operem ou manipulem informações ou recursos tecnológicos da CGE-MS, independentemente do vínculo funcional, regime de trabalho ou localização.

§ 2º As disposições desta Política observarão as competências da Secretaria-Executiva de Transformação Digital (Setdig) quanto à infraestrutura corporativa de tecnologia da informação e aos serviços compartilhados do Poder Executivo Estadual.

CAPÍTULO II
PRINCÍPIOS E OBJETIVOS

Art. 2º A PSI/CGE-MS é orientada pelos seguintes princípios:

I - confidencialidade: acesso às informações restrito às pessoas autorizadas;

II - integridade: informações exatas, completas e protegidas contra alterações indevidas;

III - disponibilidade: informações e sistemas acessíveis quando necessário;

IV - autenticidade: garantia da identidade da fonte das informações;

V - rastreabilidade: capacidade de identificar quem acessou ou modificou informações, quando e como;

VI - responsabilidade: cada usuário responde pelas ações realizadas com as credenciais que lhe forem atribuídas;

VII - conformidade: aderência às leis, normas e regulamentos aplicáveis;

VIII - privacidade: respeito aos direitos dos titulares de dados pessoais.

Art. 3º São objetivos desta Política:

I - proteger os ativos de informação e tecnológicos contra acessos, modificações, destruições ou divulgações indevidas;

II - estruturar modelo de governança de segurança da informação alinhado às estratégias institucionais e à Política de Segurança da Informação do Governo do Estado de Mato Grosso do Sul;

III - promover cultura contínua de segurança da informação e privacidade;

IV - estabelecer controles, papéis e responsabilidades;

V - garantir a conformidade com a legislação vigente, inclusive a Lei Geral de Proteção de Dados Pessoais (LGPD);

VI - assegurar a continuidade dos serviços e processos críticos da CGE-MS.

CAPÍTULO III
GOVERNANÇA E RESPONSABILIDADES

Art. 4º A governança da segurança da informação na CGE-MS obedece à seguinte estrutura de níveis:

I - estratégico, sob responsabilidade da Alta Administração, à qual compete aprovar, revisar e supervisionar a PSI/CGE-MS;

II - tático, sob responsabilidade da Assessoria de Tecnologia da Informação (Asti) e da Superintendência de Administração (Suad), às quais compete planejar, coordenar e implementar as políticas, normas e ações relacionadas à segurança da informação, contando com a participação do Encarregado de Dados nas matérias relacionadas à privacidade e à proteção de dados pessoais;

III - operacional, sob responsabilidade dos gestores e servidores, aos quais compete aplicar cotidianamente os controles de segurança e comunicar incidentes ou não conformidades.

Parágrafo único. A atuação da Asti observará as diretrizes da Política de Segurança da Informação do Governo do Estado de Mato Grosso do Sul, aprovada pela Deliberação CETI n. 02, de 24 de fevereiro de 2022.

Art. 5º São responsabilidades, no âmbito da PSI/CGE-MS, sem prejuízo de outras atribuições legais, regimentais ou normativas:

I - do Controlador-Geral, na condição de alta administração:

a) aprovar e revisar a PSI/CGE-MS;

b) promover a cultura de segurança da informação no órgão;

c) prover os recursos necessários à implementação e à manutenção das medidas de segurança da informação;

d) delegar competências, quando cabível, para a execução das ações previstas nesta Política.

II - da Asti:

a) implementar, operar e monitorar os controles de segurança da informação, podendo, quando pertinente, contar com o apoio do Encarregado de Dados, nos aspectos relacionados à privacidade e à proteção de dados pessoais;

b) gerir riscos e incidentes de segurança da informação;

c) manter inventário de ativos de software;

d) elaborar, com o auxílio do Centro de Estudos e Orientações Técnicas (Ceot), normas complementares destinadas à padronização das operações relacionadas à PSI/CGE-MS;

e) capacitar os usuários quanto às boas práticas e diretrizes de segurança da informação.

III - da Suad:

a) manter inventário de ativos de hardware;

b) desenvolver e gerir as medidas de controle de acesso físico;

c) gerenciar os controles de acesso a ativos de informação sob sua responsabilidade, podendo, quando pertinente, contar com o apoio do Encarregado de Dados, nos aspectos relacionados à privacidade e à proteção de dados pessoais.

IV - dos gestores de unidade:

a) solicitar a concessão e a revisão de acessos, conforme a necessidade do serviço;

b) orientar suas equipes quanto ao cumprimento desta Política e das normas complementares;

c) comunicar incidentes de segurança da informação;

d) participar das revisões de risco, quando demandado.

V - dos servidores e colaboradores:

a) cumprir esta Política e as normas complementares aplicáveis;

b) assinar o Termo de Ciência e Adesão;

c) proteger suas credenciais de acesso;

d) comunicar imediatamente incidentes de segurança da informação de que tenham conhecimento.

VI - dos fornecedores e terceiros:

a) assinar Termo de Confidencialidade, Responsabilidade e Sigilo, quando aplicável;

b) cumprir as diretrizes de segurança da informação aplicáveis ao escopo contratado.

Parágrafo único. Todos os agentes referidos neste artigo deverão atuar de forma colaborativa para a prevenção, a identificação, o tratamento e a comunicação de incidentes de segurança da informação.

CAPÍTULO IV
CLASSIFICAÇÃO E GESTÃO DE ATIVOS DE INFORMAÇÃO

Art. 6º Todos os ativos de informação e de tecnologia da CGE-MS devem ser inventariados, classificados quanto à criticidade e à confidencialidade, e protegidos de forma proporcional ao seu valor e ao risco associado.

§ 1º São considerados ativos de informação os dados, documentos, bases de dados, sistemas, equipamentos, redes, processos e qualquer suporte que contenha informações institucionais.

§ 2º Cada ativo deverá ter um responsável por sua correta utilização, classificação, guarda e controle de acesso.

§ 3º A Suad é responsável pelo inventário de ativos de hardware;

§ 4º A Asti é responsável pelo inventário de ativos de software, sistemas internos e demais ativos lógicos.

Art. 7º As informações são classificadas nas seguintes categorias:

I - pública: informações de divulgação irrestrita ao público externo;

II - interna: informações de acesso restrito ao âmbito institucional, cuja divulgação externa não autorizada pode causar danos à imagem da CGE-MS;

III - restrita: informações de acesso limitado a grupos específicos, cuja divulgação pode causar danos graves à CGE-MS, aos cidadãos ou a terceiros.

§ 1º Cabe ao proprietário do ativo classificar corretamente a informação no momento de sua criação ou recebimento.

§ 2º Na ausência de classificação explícita, a informação será tratada como interna até definição pelo proprietário.

§ 3º Informações classificadas como restritas devem ser transmitidas apenas por canais seguros e armazenadas com controles de acesso diferenciados.

CAPÍTULO V
CONTROLE DE ACESSOS

Art. 8º O acesso a ativos de informação da CGE-MS obedecerá aos princípios do menor privilégio, da necessidade de saber e da autenticação robusta.

Art. 9º O ciclo de vida do acesso compreende as seguintes etapas obrigatórias:

I - solicitação, que consiste na formalização, pelo gestor da unidade, de pedido de acesso por meio de formulário da Setdig;

II - concessão, que consiste na validação da necessidade de criação do perfil de acesso, observada a regra do privilégio mínimo, sob responsabilidade dos gestores de unidade e da Asti;

III - revisão periódica, que consiste na verificação semestral dos acessos ativos e da adequação dos perfis, sob responsabilidade conjunta da Asti, do Encarregado de Dados e dos gestores de unidades;

IV - revogação, que consiste no encerramento imediato do acesso em caso de desligamento, afastamento ou mudança de função, sob responsabilidade conjunta da Asti, do Encarregado de Dados e da Suad;

V - auditoria contínua, que consiste no registro e na manutenção de trilha de auditoria das concessões, alterações e revogações de acessos, sob responsabilidade do Centro de Informações Estratégicas (CIE), com o auxílio da Asti.

Art. 10. São obrigações do usuário quanto a credenciais e senhas:

I - manter as credenciais sob sigilo absoluto, sendo vedado o compartilhamento em qualquer hipótese;

II - usar senhas de acordo com as especificações de autenticação de cada sistema, combinando, sempre que possível, letras maiúsculas e minúsculas, números e caracteres especiais;

III - trocar a senha conforme a solicitação do sistema ou imediatamente em caso de suspeita de comprometimento;

IV - não reutilizar senhas;

V - habilitar autenticação multifator (MFA) sempre que o sistema oferecer o recurso;

VI - bloquear imediatamente a estação de trabalho ao se ausentar.

CAPÍTULO VI
USO ACEITÁVEL DOS RECURSOS TECNOLÓGICOS

Art. 11. Os recursos tecnológicos da CGE-MS constituem patrimônio público e se destinam exclusivamente ao desempenho das atividades institucionais.

Art. 12. É expressamente vedado:

I - utilizar os recursos para fins particulares, ilícitos ou contrários ao interesse público;

II - armazenar, compartilhar ou transmitir conteúdo ofensivo, discriminatório, pornográfico ou difamatório;

III - instalar programas, extensões, aplicativos ou dispositivos não autorizados pela Setdig ou pela Asti;

IV - transferir ou armazenar informações institucionais por meios, dispositivos ou canais não oficiais, como aplicativos de mensagens pessoais, e-mails privados, serviços de nuvem não homologados, dentre outros;

V - alterar configurações de rede, segurança ou autenticação sem autorização expressa da Asti;

VI - contornar ou desabilitar controles de segurança, incluindo antivírus, firewall e filtros de conteúdo;

VII - conectar dispositivos pessoais não autorizados à rede institucional;

VIII - acessar sistemas ou dados além do escopo das atribuições funcionais.

Art. 13. A CGE-MS poderá realizar auditorias, inspeções e monitoramento técnico do uso dos recursos, observados os princípios da necessidade, da proporcionalidade e da transparência.

Parágrafo único. O monitoramento poderá abranger a utilização de correio eletrônico institucional, acesso à internet, sistemas corporativos e demais recursos tecnológicos disponibilizados pela CGE-MS, exclusivamente para fins de segurança da informação, auditoria, conformidade e proteção dos ativos institucionais, não havendo expectativa de privacidade quanto aos registros decorrentes do uso desses recursos, sem prejuízo do controle e da restrição de acesso às informações neles tratadas, observada a legislação aplicável.

CAPÍTULO VII
TELETRABALHO E MOBILIDADE

Art. 14. Os servidores e colaboradores em regime de teletrabalho, trabalho híbrido ou remoto observarão integralmente esta Política e as normas complementares específicas.

Art. 15. São requisitos obrigatórios para o teletrabalho:

I - acesso aos sistemas institucionais exclusivamente por meio de VPN corporativa autorizada pela Asti;

II - equipamento com antivírus atualizado, firewall ativo e bloqueio automático de tela configurado;

III - vedação ao armazenamento de informações institucionais em dispositivos pessoais;

IV - garantia de que terceiros não acessem os equipamentos ou documentos institucionais;

V - sigilo das credenciais e das informações sob custódia, inclusive em ambiente doméstico.

Parágrafo único. A Asti poderá suspender imediatamente o acesso remoto quando houver indícios de vulnerabilidade, comprometimento de credenciais ou risco à integridade da rede institucional.

CAPÍTULO VIII
CÓPIAS DE SEGURANÇA E CONTINUIDADE

Art. 16. A CGE-MS manterá cópias de segurança dos ativos sob sua guarda direta e que não são custodiados pela Setdig.

Art. 17. A realização de cópias de segurança pela Asti observará o princípio da segregação de funções e as seguintes diretrizes:

I - será realizada mediante solicitação do gestor da unidade responsável pelo ativo de informação, acompanhada de avaliação técnica da Asti quanto à necessidade de proteção complementar às cópias de segurança disponibilizadas pela Setdig;

II - as cópias de segurança serão armazenadas pela Asti, com o apoio da Suad, em mídia externa, observadas as medidas adequadas de proteção contra acesso não autorizado;

III - as mídias utilizadas permanecerão desconectadas dos equipamentos e da rede institucional quando não estiverem em uso;

IV - a necessidade de manutenção, atualização ou descarte das cópias será avaliada conjuntamente pela Asti e pelo gestor da unidade responsável pelo ativo de informação, de acordo com a finalidade que motivou sua criação.

Art. 18. As cópias de segurança previstas neste capítulo possuem caráter complementar, eventual e preventivo, não substituindo os mecanismos institucionais de backup mantidos pela Setdig.

Parágrafo único. As cópias de segurança serão utilizadas exclusivamente para fins de recuperação de informações ou continuidade das atividades da CGE-MS.

CAPÍTULO IX
GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 19. Todo usuário que detectar ou suspeitar de incidente de segurança deve comunicá-lo imediatamente à Asti por meio de canal oficial, não podendo aguardar, omitir ou tentar resolver a situação por conta própria.

Art. 20. O processo de gestão de incidentes compreende as seguintes fases:

I - identificação e registro: detecção de possível incidente, com o registro imediato das informações disponíveis sobre o ocorrido;

II - classificação: avaliação do impacto e nível de criticidade (baixo, médio, alto ou crítico);

III - contenção: ações emergenciais para limitar o dano;

IV - erradicação e recuperação: eliminação da causa e restauração do ambiente;

V - comunicação: notificação às partes afetadas e, quando exigível, à ANPD e aos titulares de dados pessoais;

VI - lições aprendidas: análise pós-incidente e atualização de controles.

Art. 21. Quando o incidente envolver dados pessoais, a Asti comunicará imediatamente o Encarregado de Dados e adotará as medidas técnicas e operacionais necessárias à contenção, análise e tratamento do incidente.

Parágrafo único. Compete ao Encarregado de Dados, no âmbito de suas atribuições, avaliar os aspectos relacionados à proteção de dados pessoais e à LGPD, inclusive quanto à necessidade de comunicação à ANPD e aos titulares, quando cabível, observados os requisitos e prazos estabelecidos na legislação aplicável.

CAPÍTULO X
GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Art. 22. A CGE-MS adotará processo contínuo e integrado de gestão de riscos de segurança da informação e privacidade, conforme a Resolução Conjunta CGE/SEGOV n. 2, de 14 de novembro de 2025, que regulamenta a Política de Gestão de Riscos no âmbito da Política de Compliance Público do Poder Executivo Estadual.

Art. 23. Os riscos relacionados à segurança da informação serão identificados e tratados pela Asti, no âmbito de suas competências, com a orientação e o apoio do Encarregado de Dados, quando envolverem aspectos relacionados à privacidade e à proteção de dados pessoais.

CAPÍTULO XI
CAPACITAÇÃO E CONSCIENTIZAÇÃO

Art. 24. A CGE-MS manterá programa contínuo de capacitação e conscientização em segurança da informação, coordenado pela Asti, com o apoio das áreas envolvidas.

Art. 25. O programa de capacitação observará as seguintes diretrizes:

I - treinamento introdutório obrigatório para todo novo servidor, colaborador ou prestador de serviço antes do início das atividades;

II - capacitações periódicas para todos os usuários dos recursos tecnológicos;

III - treinamentos temáticos voltados a perfis específicos, como administradores de sistemas, gestores de unidade e Encarregado de Dados;

IV - campanhas de conscientização sobre ameaças recorrentes, como phishing, engenharia social, ransomware, dentre outros;

V - participação obrigatória nos treinamentos, com registro e controle de presença, devendo as ausências ser justificadas.

CAPÍTULO XII
TERCEIROS, FORNECEDORES E PARCEIROS

Art. 26. Terceiros, fornecedores e parceiros que tenham acesso a informações ou sistemas da CGE-MS deverão:

I - assinar Termo de Confidencialidade, Responsabilidade e Sigilo antes do início das atividades;

II - submeter-se às diretrizes desta política, no que couber;

III - submeter-se ao monitoramento do cumprimento das obrigações de segurança, quando aplicável.

§ 1º Qualquer incidente causado ou identificado por terceiro deve ser comunicado imediatamente à Asti.

§ 2º Os contratos celebrados com terceiros, fornecedores e parceiros que tenham acesso a informações ou sistemas da CGE-MS deverão conter cláusula específica que estabeleça a obrigatoriedade de observância desta Política e das normas complementares de segurança da informação aplicáveis ao objeto contratado.

CAPÍTULO XIII
DESCARTE SEGURO DE INFORMAÇÕES E ATIVOS

Art. 27. O descarte de informações e ativos de tecnologia deverá ser realizado de forma segura, impedindo a recuperação de dados por pessoas não autorizadas.

Art. 28. Para fins de descarte, observar-se-á:

I - documentos físicos com informações internas ou restritas, bem como CDs/DVDs, devem ser destruídos por fragmentação mecânica;

II - mídias digitais (HDs, SSD e pen drives) devem ser submetidas a processo de sanitização certificado antes do descarte ou reaproveitamento;

III - equipamentos ou dispositivos retirados de operação, ou movimentados internamente, devem ter os dados apagados sob supervisão da Asti;

IV - o descarte de dados pessoais obedecerá às bases legais de eliminação previstas na LGPD, com registro da operação.

CAPÍTULO XIV
VIOLAÇÕES E SANÇÕES

Art. 29. O descumprimento desta Política ou de normas complementares sujeitará o infrator a sanções administrativas na forma estabelecida na Lei Estadual n. 1.102/1990 ou equivalente, sem prejuízo da responsabilização que se faça necessária no âmbito cível ou penal.

Art. 30. Constituem condutas vedadas, dentre outras que contrariem a PSI/CGE-MS:

I - compartilhar credenciais de acesso;

II - divulgar, sem autorização, informações restritas ou dados pessoais;

III - omitir comunicação de incidente de segurança;

IV - instalar softwares maliciosos ou não autorizados;

V - burlar controles de segurança ou sistemas de monitoramento;

VI - acessar informações além do escopo das atribuições funcionais.

CAPÍTULO XV
VIGÊNCIA E REVISÃO

Art. 31. Esta Política entra em vigor na data de sua publicação no Diário Oficial do Estado de Mato Grosso do Sul, revogando disposições internas em contrário.

Art. 32. A PSI/CGE-MS deverá ser revisada a cada 12 (doze) meses ou sempre que ocorrer:

I - mudança significativa na legislação aplicável;

II - alteração relevante na infraestrutura tecnológica ou nos processos da CGE-MS;

III - incidente de segurança de grande impacto que revele lacunas na Política;

IV - recomendação de auditoria interna ou externa.

§ 1º O processo de revisão será conduzido pela Asti, com a participação das unidades organizacionais, e submetido à aprovação do Controlador-Geral do Estado.

§ 2º Toda versão revisada será comunicada formalmente a todos os usuários, com prazo de 30 (trinta) dias para adaptação.

CAPÍTULO XVI
DISPOSIÇÕES FINAIS

Art. 33. Compõem a presente Política o Glossário de Termos e Definições, o Termo de Ciência e Adesão e o Termo de Confidencialidade, Responsabilidade e Sigilo, conforme os Anexos I, II e III desta Resolução.

Art. 34. Compete à Asti:

I - revisar periodicamente os Anexos desta Resolução, propondo as modificações necessárias para mantê-los atualizados;

II - manter o histórico de versões das normas complementares e dos Anexos, para controle de sua divulgação.

CAMPO GRANDE-MS, 21 DE AGOSTO DE 2026.

CARLOS EDUARDO GIRÃO DE ARRUDA
Controlador-Geral do Estado

Clique no link para acessar os Anexos:

ANEXO I
GLOSSÁRIO DE TERMOS E DEFINIÇÕES

ANEXO II
TERMO DE CIÊNCIA E ADESÃO

ANEXO III
TERMO DE CONFIDENCIALIDADE, RESPONSABILIDADE E SIGILO