POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA MTI

2026

REVISÃO Nº: 003	**DATA:** 27/03/2026	**MOTIVO:** Revisão	
PALAVRAS CHAVE: Segurança da Informação, Ativo, Integridade, Disponibilidade			
ELABORADO POR UNICRS		**APROVADO POR DIREX**	
NOME **Ana B. C. C. Albuquerque**	**RUBRICA**	**NOME** **DIREX**	**RUBRICA**

SUMÁRIO

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º A Política de Segurança da Informação da Empresa Mato-grossense de Tecnologia da Informação – MTI estabelece o referencial institucional para a proteção das informações e dos ativos de informação e para a orientação das práticas de segurança da informação no âmbito da organização, em consonância com sua missão institucional e com as diretrizes da Administração Pública Estadual.

Art. 2º A Política de Segurança da Informação da MTI estabelece diretrizes para a adoção de mecanismos estruturados de governança e proteção da informação, considerando a crescente dependência de recursos tecnológicos e o uso estratégico da informação na prestação de serviços públicos, com a finalidade de:

I – assegurar a continuidade dos serviços institucionais;

II – garantir a confiabilidade das operações organizacionais;

III – promover a adequada gestão dos riscos associados ao tratamento da informação.

Art. 3º Esta Política formaliza o compromisso institucional da MTI com a adoção de práticas de segurança da informação alinhadas à legislação vigente, aos normativos estaduais aplicáveis e às boas práticas nacionais e internacionais, visando:

I – ao fortalecimento da governança institucional;

II – à promoção da cultura organizacional de segurança da informação;

III – ao aumento da confiança nos serviços digitais prestados pela empresa.

CAPÍTULO II
DA FINALIDADE E DOS OBJETIVOS

SEÇÃO I
DA FINALIDADE

Art. 4º Esta Política tem por finalidade estabelecer diretrizes institucionais para a gestão da segurança da informação no âmbito da MTI, assegurando a proteção dos ativos de informação e o suporte seguro às atividades institucionais.

SEÇÃO II
DO OBJETIVO ESTRATÉGICO

Art. 5º A Segurança da Informação constitui função estratégica essencial para a sustentação das atividades institucionais da MTI, devendo estar integrada aos seguintes elementos organizacionais:

I – ao planejamento estratégico;

II – à gestão de riscos corporativos;

III – à governança institucional;

IV – aos processos de tomada de decisão organizacional.

Art. 6º A presente política tem como objetivo estratégico fortalecer a resiliência organizacional da MTI por meio:

I – da proteção adequada dos ativos de informação;

II – da prevenção e mitigação de riscos e vulnerabilidades de segurança;

III – da promoção da confiança nos serviços digitais prestados;
IV – do suporte seguro à transformação digital da Administração Pública Estadual.
Art. 7º A gestão da segurança da informação deverá contribuir para o alcance dos objetivos estratégicos institucionais, assegurando que riscos relacionados à informação e à tecnologia sejam identificados, avaliados, tratados e monitorados de forma contínua, proporcional e alinhada às prioridades organizacionais.

SEÇÃO III
DOS OBJETIVOS ESPECÍFICOS

Art. 8º Constituem objetivos específicos desta Política:
I – preservar a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações sob responsabilidade da MTI;
II – promover a implementação, manutenção e melhoria contínua dos processos e controles de segurança da informação;
III – fortalecer a cultura institucional de segurança da informação;
IV – ampliar a observância das políticas, normas e procedimentos de segurança aplicáveis;
V – assegurar conformidade com legislações, normativos e diretrizes estaduais aplicáveis;
VI – garantir que medidas de segurança observem critérios de proporcionalidade, razoabilidade e alinhamento aos riscos institucionais;
VII – apoiar a gestão de riscos institucionais e a tomada de decisão baseada em risco;
VIII - oferecer diretrizes para que os requisitos de segurança e privacidade sejam integrados desde a concepção de projetos, sistemas e serviços digitais (security and privacy by design).

CAPÍTULO III
DO ESCOPO E DA ABRANGÊNCIA

Art. 9º Esta política aplica-se a todos os agentes públicos da MTI, independentemente do cargo, função ou vínculo, bem como a estagiários, colaboradores, prestadores de serviços, fornecedores, parceiros institucionais e demais terceiros que tenham acesso a informações ou recursos tecnológicos sob responsabilidade da empresa.
Art. 10. A política abrange todas as informações institucionais, em meio físico ou digital, independentemente da forma de criação, armazenamento, processamento, transmissão ou descarte.
Art. 11. Incluem-se no escopo desta política:
I – ativos de informação, sistemas corporativos e serviços digitais;
II – infraestruturas tecnológicas, redes e dispositivos computacionais;
III – ambientes físicos, lógicos e em nuvem;
IV – processos organizacionais que utilizem informações;
V – contratos, convênios e instrumentos que envolvam tratamento de informações.
Art. 12. As diretrizes desta política aplicam-se aos ambientes internos e externos à infraestrutura institucional, incluindo trabalho remoto, acesso remoto e uso de dispositivos móveis.
Parágrafo único. Em regimes de teletrabalho, o usuário é responsável por garantir a segurança física e lógica de seu ambiente remoto, sendo obrigatório o uso de canais criptografados (como VPN institucional) para acesso a sistemas internos, bem como a adoção de boas práticas em redes de internet domésticas e dispositivos pessoais (BYOD), conforme normativos específicos da MTI.

Art. 13. O cumprimento desta política constitui requisito obrigatório para concessão e manutenção de acesso às informações e recursos tecnológicos institucionais.
Parágrafo único. O descumprimento das disposições desta política poderá ensejar medidas administrativas, contratuais ou legais cabíveis.

CAPÍTULO IV
DO REFERENCIAL NORMATIVO E LEGAL

Art. 14. Esta política fundamenta-se na legislação vigente, nos normativos aplicáveis à Administração Pública Estadual e em boas práticas de governança e segurança da informação.
Art. 15. Constituem referenciais legais e normativos:
I – Constituição da República Federativa do Brasil de 1988;
II – Lei nº 12.527/2011 – Lei de Acesso à Informação;
III – Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais;
IV – Lei nº 14.129/2021 – Lei do Governo Digital;
V – legislação federal e estadual correlata;
VI – Política Estadual de Segurança da Informação do Poder Executivo do Estado de Mato Grosso (Decreto nº 1.428/2025);
VII – demais atos normativos estaduais aplicáveis.
Art. 16. Esta Política integra o conjunto de instrumentos de governança da MTI e deverá ser observada em conjunto com:
I – o Código de Conduta e Integridade da MTI;
II – políticas corporativas e normas internas;
III – instrumentos de gestão de riscos e controles internos;
IV – contratos e instrumentos institucionais relacionados à segurança da informação;
V – diretrizes institucionais relacionadas à proteção da propriedade intelectual, direitos autorais e uso legal de informações e recursos tecnológicos.
Art. 17. Para fins de orientação e melhoria contínua, poderão ser adotados referenciais técnicos e boas práticas reconhecidos nacional e internacionalmente em segurança da informação e gestão de riscos.

CAPÍTULO V
DOS PRINCÍPIOS

Art. 18. A gestão da Segurança da Informação no âmbito da MTI observará aos seguintes princípios:
I – **Confidencialidade:** assegurar que as informações sejam acessadas somente por pessoas, entidades ou processos devidamente autorizados, prevenindo acessos ou divulgações indevidas;
II – **Integridade:** garantir a exatidão, completude e confiabilidade das informações e dos processos associados, protegendo-as contra alterações não autorizadas;
III – **Disponibilidade:** assegurar que informações e serviços estejam acessíveis e utilizáveis pelas entidades autorizadas sempre que necessários às atividades institucionais;

IV – **Autenticidade:** garantir a veracidade da origem das informações, comunicações e transações realizadas nos ambientes institucionais;
V – **Rastreabilidade:** assegurar que ações realizadas sobre informações e sistemas possam ser registradas, monitoradas e auditadas, permitindo a identificação de responsabilidades;
VI – **Legalidade e conformidade:** assegurar que o tratamento das informações observe a legislação vigente, normativos aplicáveis e diretrizes institucionais;
VII – **Gestão baseada em riscos:** orientar a adoção de medidas de segurança a partir da identificação, análise e tratamento dos riscos institucionais;
VIII – **Proporcionalidade:** garantir que os controles de segurança sejam compatíveis com o valor dos ativos protegidos e com os riscos envolvidos;
IX – **Responsabilização:** promover a clara definição de responsabilidades quanto ao uso, proteção e tratamento das informações;
X – **Melhoria contínua:** estimular o aperfeiçoamento permanente dos processos, controles e práticas de segurança da informação.

CAPÍTULO VI
DAS DIRETRIZES GERAIS

Art. 19. A gestão da Segurança da Informação no âmbito da MTI deverá observar as seguintes diretrizes gerais:
I – assegurar a proteção dos ativos de informação contra acessos não autorizados, perdas, alterações indevidas, vazamentos e quaisquer formas de comprometimento;
II – garantir que o acesso às informações e aos recursos tecnológicos ocorra de forma controlada, mediante critérios de necessidade de conhecimento e privilégio mínimo;
III – promover a classificação da informação de acordo com seu grau de sensibilidade e criticidade, observando requisitos legais, institucionais e operacionais;
IV – assegurar a adoção de controles técnicos e administrativos compatíveis com os riscos identificados no processo de gestão de riscos de segurança da informação;
V – preservar a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações institucionais;
VI – promover a conscientização, capacitação e responsabilização dos usuários quanto às boas práticas de segurança da informação;
VII – garantir que terceiros, fornecedores e parceiros observem os requisitos de segurança da informação estabelecidos pela MTI, mediante cláusulas contratuais e mecanismos de controle;
VIII – assegurar a conformidade com a legislação vigente, normas regulamentares e diretrizes estabelecidas pela Administração Pública Estadual;
IX – promover a melhoria contínua dos processos de segurança da informação, com base em monitoramento, avaliações periódicas e lições aprendidas;
X – adotar a prática de “Mesa Limpa e Tela Limpa”, assegurando que documentos físicos contendo informações sensíveis não permaneçam expostos em mesas, impressoras ou outros ambientes de fácil acesso, bem como que as estações de trabalho sejam devidamente bloqueadas sempre que o usuário se ausentar, de modo a prevenir acessos visuais ou físicos não autorizados;
XI – assegurar a existência e manutenção de política corporativa de cópias de segurança, contemplando diretrizes para armazenamento seguro, segregado e resiliente, bem como procedimentos de validação periódica da capacidade de restauração;

XII – definir e implementar diretrizes para registro, monitoramento, análise e correlação de eventos relevantes de segurança, assegurando meios adequados de retenção e tratamento dessas informações;
XIII – estabelecer diretrizes para o uso de criptografia na proteção de informações sensíveis, abrangendo dados em trânsito, em repouso e mecanismos seguros de gestão de chaves;
XIV – assegurar a existência de processo contínuo de identificação, avaliação e tratamento de vulnerabilidades, incluindo aplicação tempestiva de correções e mecanismos de priorização baseados em risco;
XV – estabelecer diretrizes para uso seguro de serviços em nuvem, incluindo definição de responsabilidades, requisitos mínimos de controle de acesso e mecanismos de monitoramento do ambiente;
XVI – promover programa contínuo de conscientização, capacitação e treinamento em segurança da informação, alinhado ao perfil e às responsabilidades dos usuários, com avaliação periódica de efetividade;
XVII – definir diretrizes para configuração segura, uso adequado e proteção de dispositivos utilizados no acesso a recursos institucionais, sejam corporativos ou pessoais, incluindo requisitos mínimos de segurança e restrições aplicáveis;
XVIII – estabelecer diretrizes para o uso seguro, ético e responsável de soluções baseadas em Inteligência Artificial, contemplando avaliação de riscos, proteção de dados e definição de permissões e restrições aplicáveis.
Parágrafo único. As diretrizes estabelecidas neste artigo deverão orientar a elaboração de normas complementares, procedimentos operacionais, padrões técnicos e demais instrumentos internos de segurança da informação da MTI.

CAPÍTULO VII
DAS RESPONSABILIDADES E COMPETÊNCIAS

Art. 20. A Segurança da Informação constitui responsabilidade compartilhada entre a Alta Administração, gestores, agentes públicos, colaboradores, prestadores de serviços e demais usuários que utilizem ou tenham acesso aos ativos de informação da MTI, observadas as competências estabelecidas nesta Política.

SEÇÃO I
DA ALTA ADMINISTRAÇÃO

Art. 21. Compete à Alta Administração da MTI:
I – aprovar, apoiar e assegurar a efetiva implementação da Política de Segurança da Informação e de seus instrumentos complementares;
II – garantir o alinhamento da segurança da informação ao planejamento estratégico institucional;
III – promover a integração da segurança da informação à governança, à gestão de riscos e aos controles internos institucionais;
IV – assegurar a disponibilização de recursos humanos, tecnológicos e orçamentários necessários à gestão da segurança da informação;
V – fomentar a cultura organizacional de segurança da informação no âmbito institucional.
VI - aprovar os planos de continuidade e deliberar sobre sua ativação.

SEÇÃO II
DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO E RISCOS

Art. 22. O Comitê de Segurança da Informação e Riscos (CSIR) é o órgão colegiado consultivo, deliberativo e propositivo responsável por apoiar a governança de segurança da informação e gestão de riscos no âmbito da MTI. Compete ao Comitê:

I – deliberar sobre temas relacionados à segurança da informação, visando assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações institucionais;

II – propor a instituição, elaboração e revisões da Política de Segurança da Informação e demais normas complementares;

III – dirimir dúvidas e deliberar sobre questões não contempladas na Política de Segurança da Informação ou em suas normas complementares;

IV – validar e acompanhar o Plano Anual de Segurança da Informação e os resultados de auditorias, avaliações de conformidade e demais mecanismos de controles;

V – definir iniciativas voltadas à melhoria contínua da segurança da informação, apoiando o planejamento e a articulação das ações junto às unidades setoriais.

VI - coordenar a manutenção e atualização dos planos de continuidade.

SEÇÃO III
DA UNIDADE RESPONSÁVEL PELA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 23. Compete à unidade responsável pela gestão de Segurança da Informação, sob a perspectiva de governança institucional:

I – coordenar a implementação, manutenção e melhoria contínua da governança de segurança da informação no âmbito da MTI;

II – propor a elaboração de políticas, normas complementares, diretrizes e procedimentos institucionais relacionados à segurança da informação;

III – acompanhar a conformidade institucional com esta Política e demais normativos correlatos;

IV – promover ações de conscientização, capacitação e disseminação de boas práticas de segurança da informação;

V – apoiar a integração da segurança da informação à gestão de riscos corporativos, à governança institucional e aos controles internos;

VI – acompanhar indicadores, riscos e níveis de maturidade relacionados à segurança da informação;

VII – acompanhar a evolução de requisitos legais, regulatórios e boas práticas aplicáveis à segurança da informação.

VIII - executar as ações e responsabilidades definidas nos respectivos planos e processos de continuidade.

SEÇÃO IV
DAS UNIDADES TÉCNICAS DE SEGURANÇA CIBERNÉTICA

Art. 24. Compete à unidade técnica responsável pela segurança cibernética, defesa digital ou função equivalente, conforme estrutura organizacional da MTI:

I – implementar e operar controles técnicos de segurança da informação nos ambientes tecnológicos

institucionais;
II – monitorar eventos de segurança e vulnerabilidades nos ativos tecnológicos;
III – coordenar operacionalmente a prevenção, detecção, resposta e recuperação relacionados a incidentes de segurança da informação;
IV – adotar medidas técnicas necessárias à proteção das infraestruturas, sistemas e redes institucionais;
V – comunicar incidentes relevantes às instâncias de governança e às unidades afetadas;
VI – apoiar tecnicamente as ações institucionais de gestão de riscos de segurança da informação.
Parágrafo único. A coordenação operacional do tratamento de incidentes de segurança da informação constitui atribuição da unidade técnica competente, não abrangendo a execução técnica pela unidade responsável pela governança de segurança da informação.

SEÇÃO V
DOS GESTORES DAS UNIDADES ADMINISTRATIVAS

Art. 25. Compete aos gestores das unidades organizacionais:
I – assegurar a aplicação desta Política no âmbito de suas unidades;
II – garantir a adequada classificação e proteção das informações sob sua responsabilidade;
III – autorizar e revisar acessos às informações conforme necessidade institucional e princípio do menor privilégio;
IV – comunicar incidentes ou riscos de segurança da informação às unidades competentes;
V – promover a conscientização das equipes quanto às boas práticas de segurança da informação;
VI – assegurar que processos sob sua gestão observem requisitos de segurança da informação aplicáveis.

SEÇÃO VI
DOS USUÁRIOS

Art. 26. Compete aos usuários que utilizem ou tenham acesso a ativos de informação da MTI:
I – utilizar informações e recursos tecnológicos prioritariamente para fins institucionais autorizados, observadas as normas internas aplicáveis;
II – cumprir esta Política e os normativos complementares de segurança da informação;
III – proteger as credenciais de acesso sob sua responsabilidade, sendo vedado seu compartilhamento ou utilização por terceiros;
IV – comunicar imediatamente, pelos canais institucionais definidos, incidentes, suspeitas de incidentes ou vulnerabilidades identificadas;
V – zelar pela proteção das informações acessadas ou sob sua custódia;
VI – ter ciência de que o uso de informações e recursos tecnológicos institucionais poderá ser monitorado, registrado e auditado pela MTI, nos termos da legislação vigente e dos normativos institucionais aplicáveis.

SEÇÃO VII
DOS TERCEIROS

Art. 27. Os terceiros, fornecedores, parceiros e prestadores de serviços que tenham acesso a ativos de informação da MTI deverão:
I – cumprir esta Política e os requisitos contratuais de segurança da informação;

II – adotar medidas de proteção compatíveis com os riscos associados aos serviços prestados;
III – assegurar que seus colaboradores observem as regras de segurança da informação aplicáveis;
IV – comunicar prontamente incidentes que possam impactar ativos de informação da MTI.

SEÇÃO VIII
DO COMPROMISSO E DA RESPONSABILIZAÇÃO

Art. 28. A concessão e manutenção de acesso às informações e aos recursos tecnológicos institucionais estarão condicionadas à ciência e ao compromisso formal de cumprimento desta Política e de seus instrumentos complementares.
Art. 29. O descumprimento das disposições desta Política poderá ensejar a aplicação de medidas administrativas, contratuais, civis ou legais cabíveis, observada a legislação vigente e os normativos institucionais aplicáveis.

CAPÍTULO VIII
DA GESTÃO DE CONTINUIDADE DE NEGÓCIOS

Art. 30. A Gestão de Continuidade de Negócios da MTI tem por finalidade assegurar a resiliência organizacional e a manutenção dos serviços essenciais diante de interrupções significativas, preservando a integridade dos ativos, a continuidade das operações e a confiança institucional.
Art. 31. A Gestão de Continuidade de Negócios deve observar as seguintes diretrizes:
I – identificar processos, sistemas e recursos críticos da MTI, bem como os impactos decorrentes de sua indisponibilidade;
II – manter processos formais de avaliação de impactos e riscos relacionados à continuidade;
III – estabelecer, manter e atualizar os planos necessários à continuidade e à recuperação dos serviços essenciais;
IV – submeter os planos à aprovação da Alta Administração e à coordenação do Comitê de Segurança da Informação e Riscos;
V – executar, pelas áreas responsáveis, as ações previstas nos planos, assegurando a retomada dos serviços dentro dos prazos definidos;
VI – realizar testes periódicos dos planos, registrar os resultados obtidos e promover melhorias contínuas.

CAPÍTULO IX
DA GESTÃO DE ATIVOS DE INFORMAÇÃO E DA CLASSIFICAÇÃO DA INFORMAÇÃO

SEÇÃO I
DA GESTÃO DE ATIVOS DE INFORMAÇÃO

Art. 32. A MTI deverá manter processo institucional de gestão de ativos de informação, com o objetivo de identificar, registrar, proteger e monitorar os ativos necessários à execução de suas

atividades institucionais.

Art. 33. Para fins desta Política, consideram-se ativos de informação todos os elementos que possuam valor para a organização e que suportem o tratamento da informação, incluindo:

I – informações em meio físico ou digital;

II – sistemas corporativos e aplicações;

III – bases de dados e repositórios informacionais;

IV – infraestruturas tecnológicas, redes e equipamentos;

V – serviços digitais e ambientes computacionais;

VI – documentos institucionais;

VII – serviços contratados que processem ou armazenem informações institucionais.

Art. 34. As informações produzidas, recebidas, armazenadas ou tratadas pela MTI no exercício de suas competências institucionais constituem ativos de informação da organização.

§1º As informações pertencentes a órgãos, entidades, clientes, usuários ou terceiros e mantidas sob guarda, processamento ou tratamento pela MTI são consideradas informações sob sua custódia.

§2º As informações de propriedade da MTI ou sob sua custódia deverão ser utilizadas exclusivamente para finalidades institucionais, contratuais ou legais autorizadas.

§3º A proteção das informações deverá ser assegurada durante todo o seu ciclo de vida, observada a classificação atribuída e os requisitos legais aplicáveis.

Art. 35. Os ativos de informação deverão possuir responsável institucional designado, denominado Curador do Ativo da Informação, ao qual competirá coordenar a gestão do ativo e apoiar a adoção das medidas necessárias à sua adequada proteção, em articulação com as unidades responsáveis pela segurança da informação, gestão da informação e proteção de dados pessoais.

Art. 36. A MTI deverá manter inventário dos ativos de informação críticos, atualizando periodicamente ou sempre que houver alterações relevantes nos ativos de informação.

SEÇÃO II
DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 37. Todas as informações produzidas, recebidas, custodiadas ou tratadas pela MTI deverão ser classificadas conforme seu grau de sensibilidade, criticidade e requisitos de proteção, com a finalidade de:

I – definir níveis adequados de proteção da informação;

II – orientar controles de acesso e compartilhamento;

III – reduzir riscos de divulgação indevida ou perda de informações;

IV – apoiar a gestão de riscos e a tomada de decisão institucional.

Art. 38. Os critérios detalhados de classificação, rotulagem, tratamento e proteção das informações serão estabelecidos em normas complementares, conforme necessidade institucional.

CAPÍTULO X
DO CONTROLE DE ACESSO E DA GESTÃO DE IDENTIDADES

Art. 39. O acesso às informações e aos recursos tecnológicos da MTI deverá ser controlado e concedido de forma segura, observando os princípios da necessidade de conhecimento, do menor privilégio e da segregação de funções.

Art. 40. O controle de acesso tem por finalidade:

I – proteger as informações contra acessos não autorizados;
II – assegurar que usuários possuam apenas os acessos necessários ao desempenho de suas atividades;
III – reduzir riscos de uso indevido, alteração ou divulgação não autorizada de informações;
IV – possibilitar a rastreabilidade das ações realizadas nos sistemas e recursos tecnológicos institucionais;
V – contribuir para a mitigação de riscos de fraude, uso indevido ou alterações não autorizadas em ativos de informação.
Art. 41. Para assegurar a adequada proteção das informações e dos recursos tecnológicos institucionais, a MTI deverá estabelecer processos institucionais de gestão de identidades e de controle de acesso aos ativos de informação.
Parágrafo único. Os processos de que trata o caput deverão abranger, no mínimo, a gestão e a segregação de contas privilegiadas, a utilização de cofres de credenciais, o registro e a auditoria de sessões privilegiadas, bem como a adoção de autenticação multifator (MFA) para acessos críticos.

CAPÍTULO XI
DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 42. A MTI deverá manter processo institucional para gestão de incidentes de segurança da informação, destinado à prevenção, detecção, registro, análise, resposta e recuperação de eventos que possam comprometer a segurança das informações ou a continuidade dos serviços institucionais.
Art. 43. A gestão de incidentes deverá observar, no mínimo:
I – comunicação imediata do incidente ou de sua suspeita pelos agentes públicos, colaboradores, prestadores de serviço ou terceiros por meio dos canais institucionais definidos;
II – registro formal e classificação do incidente quanto à criticidade, impacto e urgência, conforme critérios definidos em normativos complementares;
III – adoção de medidas para contenção do incidente, mitigação de impactos institucionais, operacionais, legais ou reputacionais e preservação das evidências necessárias à análise técnica;
IV – comunicação às unidades responsáveis, às áreas afetadas e, quando cabível, à Alta Administração;
V – realização de análise posterior do incidente, com identificação de causas e definição de medidas corretivas ou preventivas.
VI – preservação de evidências digitais conforme boas práticas de cadeia de custódia.
Art. 44. As informações decorrentes da gestão de incidentes deverão subsidiar a gestão de riscos de segurança da informação, a revisão de controles institucionais, a atualização de normas e procedimentos e ações de capacitação e conscientização institucional.
Parágrafo único. Quando o incidente envolver dados pessoais, deverão ser observadas também as disposições da legislação de proteção de dados pessoais e dos normativos institucionais específicos aplicáveis.

CAPÍTULO XII
DA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 45. A gestão de riscos de Segurança da Informação constitui processo contínuo, estruturado e sistemático destinado à identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos relacionados aos ativos de informação da Empresa Mato-grossense de Tecnologia da Informação – MTI.

Art. 46. O processo de gestão de riscos de Segurança da Informação deverá observar:

I – o alinhamento aos objetivos estratégicos institucionais;

II – as diretrizes de governança, gestão de riscos e controles internos da MTI;

III – a legislação vigente e os normativos estaduais aplicáveis;

IV – as melhores práticas nacionais e internacionais de Segurança da Informação.

Art. 47. O processo de gestão de riscos deverá contemplar identificação, análise, avaliação, tratamento e monitoramento dos riscos relacionados aos ativos de informação.

Art. 48. O tratamento dos riscos poderá envolver, conforme avaliação institucional:

I – mitigação do risco mediante adoção de controles de segurança;

II – compartilhamento do risco;

III – aceitação formal do risco pela autoridade competente;

IV – eliminação da atividade que origine o risco, quando aplicável, evitando-o.

Art. 49. Os riscos de Segurança da Informação deverão ser revisados periodicamente ou sempre que ocorrerem:

I – mudanças tecnológicas relevantes;

II – implantação ou alteração significativa de sistemas e serviços digitais;

III – incidentes de Segurança da Informação;

IV – alterações normativas ou estruturais na organização.

Art. 50. Os resultados da gestão de riscos deverão subsidiar o planejamento institucional, a priorização de investimentos em Segurança da Informação e o processo decisório das instâncias de governança da MTI.

CAPÍTULO XIII
DA SEGURANÇA NO DESENVOLVIMENTO

Art. 51. A MTI deve assegurar que a segurança da informação seja integrada ao ciclo de vida de desenvolvimento de sistemas, desde a concepção até a descontinuação, adotando práticas de desenvolvimento seguro alinhadas à abordagem DevSecOps.

Art. 52. Os sistemas desenvolvidos ou mantidos pela MTI devem observar os princípios de proteção de dados pessoais e as disposições da Lei Geral de Proteção de Dados (LGPD), incorporando medidas de privacidade desde a concepção e por padrão.

Art. 53. A MTI deve estabelecer normas e padrões técnicos de desenvolvimento seguro, incluindo requisitos mínimos de segurança, testes, controles e validações aplicáveis às etapas de construção, manutenção e evolução de sistemas.

Art. 54. As equipes envolvidas no desenvolvimento, sustentação e operação de sistemas são responsáveis por observar as normas complementares de desenvolvimento seguro e adotar práticas que reduzam vulnerabilidades, garantam a qualidade do código e promovam a proteção dos dados

tratados.

CAPÍTULO XIV
DAS DISPOSIÇÕES FINAIS

Art. 55. O descumprimento das disposições estabelecidas nesta política poderá ensejar a aplicação de medidas administrativas, contratuais e legais cabíveis, observado o devido processo legal e a legislação vigente.

Art. 56. Os procedimentos operacionais, padrões técnicos e orientações detalhadas para aplicação desta Política encontram-se definidos no Manual de Segurança da Informação da MTI e em demais normas complementares que poderão vir a ser instituídos para regulamentar e detalhar a aplicação desta Política.

§1º As normas complementares deverão manter alinhamento com os princípios e diretrizes estabelecidos nesta Política.

§2º Os instrumentos normativos derivados desta Política possuirão caráter vinculante no âmbito da MTI.

Art. 57. A presente política deverá ser revisada periodicamente, no mínimo a cada 2 (dois) anos, ou sempre que ocorrer:

I – alteração relevante na legislação aplicável;

II – mudanças significativas na estrutura organizacional ou tecnológica da MTI;

III – ocorrência de incidentes relevantes de Segurança da Informação;

IV – recomendações oriundas de auditorias internas ou externas;

V – atualização da Política Estadual de Segurança da Informação.

Art. 58. Compete à unidade responsável pela gestão de Segurança da Informação coordenar o processo de revisão, atualização e disseminação desta política, em articulação com as unidades institucionais competentes.

Art. 59. Os casos omissos e as dúvidas decorrentes da aplicação desta Política serão dirimidos pelas instâncias de governança competentes da MTI.

Art. 60. Integra esta política, para fins de interpretação e aplicação, o Anexo I — Glossário de Termos e Definições, contendo os conceitos utilizados no âmbito da Segurança da Informação da MTI.

Parágrafo único. O glossário possui caráter interpretativo e complementar, não substituindo as disposições normativas desta política.

Art. 61. Esta política entra em vigor na data de sua aprovação pela autoridade competente, revogadas as disposições em contrário.

ANEXO I
TERMOS E DEFINIÇÕES

As definições constantes deste anexo possuem caráter interpretativo e complementar, destinando-se a apoiar a compreensão, interpretação e aplicação da Política de Segurança da Informação da Empresa Mato-grossense de Tecnologia da Informação – MTI.

Art. 1º Para fins desta Política de Segurança da Informação, adotam-se as seguintes definições:

I – **Agente público:** toda pessoa física que exerça, ainda que temporariamente ou sem remuneração, cargo, função, emprego ou atividade pública no âmbito da MTI, incluindo empregados públicos, dirigentes, estagiários e colaboradores;
II – **Ativo:** qualquer elemento que possua valor para a organização e que necessite de proteção, incluindo informações, sistemas, serviços, pessoas, processos, infraestrutura tecnológica e recursos físicos;
III – **Ativo de informação:** conjunto de dados, informações, sistemas, aplicações, serviços, equipamentos ou meios que armazenem, processem ou transmitam informações institucionais;
IV – **Autenticidade:** propriedade que assegura que uma informação, comunicação ou transação é genuína e proveniente da fonte declarada;
V – **Classificação da informação:** processo de categorização das informações conforme seu grau de sensibilidade e necessidade de proteção, visando definir controles adequados de acesso, uso e compartilhamento;
VI – **Confidencialidade:** propriedade que garante que a informação esteja acessível somente a pessoas, entidades ou processos devidamente autorizados;
VII – **Disponibilidade:** propriedade que assegura que informações e serviços estejam acessíveis e utilizáveis quando necessários às atividades institucionais;
VIII – **Gestão de riscos de segurança da informação:** processo contínuo e estruturado de identificação, análise, avaliação, tratamento e monitoramento dos riscos relacionados à segurança da informação;
IX – **Incidente de segurança da informação:** evento confirmado ou sob suspeita que comprometa ou possa comprometer a confidencialidade, integridade, disponibilidade, autenticidade ou rastreabilidade das informações ou dos ativos de informação;
X – **Informação:** conjunto de dados organizados ou processados que possuem significado e valor para a organização, independentemente do meio em que estejam armazenados ou transmitidos;
XI – **Integridade:** propriedade que assegura a exatidão, completude e consistência das informações e dos métodos de processamento;
XII – **Rastreabilidade:** capacidade de identificar, registrar e acompanhar ações realizadas sobre informações, sistemas ou ativos, permitindo auditoria e responsabilização;
XIII – **Risco:** possibilidade de ocorrência de evento que possa causar impacto negativo aos objetivos institucionais, resultante da combinação entre probabilidade de ocorrência e impacto associado;
XIV – **Segurança da informação:** conjunto de práticas, processos, controles e medidas destinadas a proteger as informações contra acessos não autorizados, uso indevido, divulgação, alteração ou destruição;
XV – **Sistema de informação:** conjunto organizado de recursos tecnológicos, aplicações, dados e

procedimentos utilizados para coletar, processar, armazenar ou transmitir informações;
XVI – **Tratamento da informação:** qualquer operação realizada com informações, incluindo coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, armazenamento, arquivamento, compartilhamento ou eliminação;
XVII – **Usuário:** pessoa física autorizada a acessar informações ou utilizar ativos de informação da MTI, independentemente do vínculo institucional;
XVIII – **Vulnerabilidade:** fragilidade ou deficiência em ativos, processos ou controles que possa ser explorada por uma ameaça, resultando em incidente de segurança da informação.

Art. 2º As definições constantes deste anexo poderão ser atualizadas por ato administrativo complementar da MTI, desde que tais atualizações não alterem o conteúdo normativo desta Política de Segurança da Informação.

Art. 3º Os termos não definidos expressamente neste anexo deverão ser interpretados conforme:
I – a legislação vigente aplicável à Administração Pública e à segurança da informação;
II – os normativos estaduais e institucionais relacionados à governança, tecnologia da informação, proteção de dados e gestão de riscos;
III – as normas técnicas e boas práticas nacional e internacionalmente reconhecidas em segurança da informação e gestão de riscos;
IV – os referenciais técnicos adotados oficialmente pela MTI em seus instrumentos normativos complementares.

Art. 4º Em caso de divergência conceitual entre este anexo e normativos legais ou regulamentares supervenientes, prevalecerá o disposto na legislação vigente.

CESAR FERNANDO BERRIEL VIDOTTO:01578991870
Assinado de forma digital por CESAR FERNANDO BERRIEL VIDOTTO:01578991870
Dados: 2026.04.29 08:17:06 -04'00'

PAULO MARCIO PINHEIRO MACEDO:78618568104
Assinado de forma digital por PAULO MARCIO PINHEIRO MACEDO:78618568104
Dados: 2026.04.29 09:36:49 -04'00'

SOCRATES FARIAS DE BARROS:71156844134
Assinado de forma digital por SOCRATES FARIAS DE BARROS:71156844134
Dados: 2026.05.13 13:51:51 -04'00'

CLEBERSON ANTONIO SAVIO GOMES:80180663100
Assinado de forma digital por CLEBERSON ANTONIO SAVIO GOMES:80180663100
Dados: 2026.05.14 16:16:57 -04'00'

Documento aprovado pela Diretoria Executiva em 27 de março de 2026, conforme registrado na Ata de Reunião nº 00028/2026/GADP/MTI.