POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

INTRODUÇÃO

A Segurança da Informação é um conjunto de ações de proteção aos ativos de informação contra todas as formas de agressões em seu ambiente físico, lógico e humano.

Este documento estabelece diretrizes, princípios, responsabilidades e objetivos para a Política de Segurança da Informação e Comunicação (PSIC) da Secretaria de Estado de Saúde de Mato Grosso – SES-MT, a qual deverá ser adotada e cumprida por todos os servidores, estagiários, prestadores de serviços e demais trabalhadores do SUS que utilizem suas informações.

Além disso, esta PSIC tem como escopo fundamentar todas as ações de proteção às informações das unidades administrativas da SES-MT, em atendimento às recomendações da Controladoria Geral do Estado de Mato Grosso (Recomendação Técnica nº 0427/CGE-MT) e de outros órgãos de controle.

A Segurança da Informação é matéria atinente a todas as atividades das unidades administrativas, sejam atividades meio ou fim, devendo essa responsabilidade ser compartilhada por todas suas áreas.

A informação não está apenas nos sistemas informatizados, mas também em papéis, documentos e pessoas. Portanto, para o sucesso desta PSIC é necessário contar com o comprometimento de todos os gestores, servidores, estagiários, prestadores de serviços e usuários das informações.

Diversas ações e outros normativos de Segurança da Informação serão implementados com o fim de padronizar e regrar os processos institucionais da SES-MT.

1. OBJETIVO

Art. 1º O objetivo desta política é instituir diretrizes e princípios de Segurança da Informação e Comunicação no âmbito das unidades administrativas da Secretaria de Estado de Saúde de Mato Grosso (SES-MT), com o propósito de limitar a exposição ao risco a níveis aceitáveis e buscar continuamente a disponibilidade, a integridade, a confidencialidade, a autenticidade e o não repúdio das informações que suportam os objetivos estratégicos das unidades administrativas.

2. DO ESCOPO DA POLÍTICA

Art. 2º A PSIC/SES-MT aplica-se a todas as unidades da estrutura administrativa e deverá ser fielmente observada por todos os servidores públicos, colaboradores, estagiários, consultores externos, prestadores

de serviço e qualquer outra pessoa que tenha acesso a dados e informações do Estado e/ou do órgão, sob pena de responsabilidade, na forma da lei.

3. DOS PRINCÍPIOS

Art. 3º O conjunto de documentos que compõe esta PSIC deverá se guiar pelos seguintes princípios:

I. **Simplicidade:** A complexidade aumenta a chance de erros, portanto todos os controles de segurança deverão ser simples e objetivos;

II. **Privilégio Mínimo:** Usuários devem ter acesso apenas aos recursos de Tecnologia da Informação necessários para realizar as tarefas que lhe foram designadas;

III. **Segregação de função:** Funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos, bem como permitir maior eficácia dos controles de segurança;

IV. **Auditabilidade:** Todos os eventos significantes de usuários e processos devem ser rastreáveis até o evento inicial por meio de registro consistente e detalhado;

V. **Mínima dependência de segredos:** Os controles deverão ser efetivos ainda que se conheça a existências deles e como eles funcionam;

VI. **Resiliência:** Os controles de segurança devem ser projetados para que possam resistir ou se recuperarem dos efeitos de um desastre;

VII. **Defesa em profundidade:** Os controles de segurança devem ser concebidos em múltiplas camadas de modo a prover redundância para que, no caso de falha, outro controle possa ser aplicado.

4. DIRETRIZES GERAIS

4.1. DA ESTRUTURA NORMATIVA

Art. 4º A Estrutura Normativa da Segurança da Informação da SES-MT é composta por quatro níveis hierárquicos distintos, relacionados a seguir:

I. Plano Diretor de Tecnologia da Informação – PDTI da SES-MT: constituído por documento complementar que norteia a Tecnologia da Informação e Comunicação no órgão em termos de sua importância estratégica para a Saúde, o Estado e o cidadão.

II. Política de Segurança da Informação e Comunicação da SES-MT (PSIC - SES-MT): constituída neste documento, define a estrutura, diretrizes gerais, princípios e as obrigações referentes à segurança

da informação e comunicação da SES-MT, servindo de base para elaboração dos demais documentos da estrutura normativa e possui caráter estratégico;

III. Normas de Segurança da Informação e Comunicação (NoSIC): de caráter tático, as normas estabelecem regras para a utilização de ativos e recursos de Tecnologia da Informação e Comunicação com o intuito de atingir os objetivos da Política elaborada pela SES-MT;

IV. Procedimentos de Segurança da Informação e Comunicação (POPSIC): descrevem, detalhadamente, as medidas operacionais necessárias para atingir os resultados estabelecidos nas Normas e na Política, abordando aspectos técnicos e práticos, adaptados à realidade do ambiente.

Parágrafo Único: A PSIC da SES-MT tem caráter corporativo e sua elaboração é de competência do Comitê Gestor da Política de Segurança da Informação – CGPSI em conjunto com a Superintendência de Tecnologia da Informação – STI. As NoSICs são de competência da STI, quando institucionais e das unidades administrativas quando contemplarem necessidades específicas das mesmas.

4.2. DO CICLO DE VIDA DA INFORMAÇÃO

Art. 5º As medidas de proteção devem ser adotadas durante todo o ciclo de vida da informação, compreendendo as fases de criação, manipulação, armazenamento, transporte e descarte.

4.3. NORMAS E PROCEDIMENTOS COMPLEMENTARES

Art. 6º As normas e procedimentos que complementam esta Política deverão abordar, mas não limitados a estes, os seguintes aspectos: segurança física; gestão de mudanças; privacidade; criptografia; acesso à rede; gestão de senhas e contas de usuário; dispositivos móveis; gestão de incidentes; plano de continuidade de negócios; proteção à propriedade intelectual; treinamento e sensibilização para segurança;

4.4. DA DIVULGAÇÃO

Art. 7º Esta política bem como suas normas deverão ser disponibilizadas e agrupadas em sítio institucional em local de fácil acesso, proporcionando ampla difusão e atualização simplificada. Em todos os documentos deverá constar a data de sua publicação e/ou revisão.

Art. 8º Os Procedimentos de Segurança da Informação, por conterem informações sensíveis, deverão ser classificados na forma da lei e divulgados para aqueles cujas atribuições requerem conhecimento das mesmas.

4.5. DA SEGURANÇA FÍSICA E DO AMBIENTE

Art. 9º As instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física.

Art. 10 Os equipamentos deverão ser protegidos contra ameaças físicas e ambientais, incluindo aqueles utilizados fora da instalação.

4.6. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO E COMUNICAÇÃO

Art. 11 Deverão ser desenvolvidas ações que garantam que a segurança seja parte integrante dos sistemas de informação e comunicação existentes, e também os que forem desenvolvidos e adquiridos.

Art. 12 Todos os requisitos de segurança deverão ser identificados na fase de definição de requisitos de um projeto e justificados, acordados e documentados como parte do caso geral de negócios do sistema de informação.

4.7. EDUCAÇÃO CONTINUADA

Art. 13 Para uma efetiva proteção das informações, a SES-MT deverá elaborar um plano contínuo de capacitação de recursos humanos em segurança da informação, de modo a promover maior consciência da responsabilidade individual dos usuários e maior independência do Estado na contratação de serviços de segurança.

4.8. PENALIDADES

Art. 14 O descumprimento às diretrizes desta política assim como às suas normas e procedimentos vinculados acarretará em sanções administrativas, sem prejuízo às ações cíveis e criminais cabíveis.

5. COMPETÊNCIAS E RESPONSABILIDADES

5.1. DA ALTA ADMINISTRAÇÃO

Art. 15 Compete à alta administração da SES-MT:

I. Apoiar e exigir o cumprimento da Política, Normas e Procedimentos de Segurança da Informação e Comunicação;

II. Zelar para que contratos, convênios e outros instrumentos similares estejam alinhados à presente política e suas normas adjacentes;

III. Priorizar a capacitação contínua de seus recursos humanos de modo a promover maior independência do Estado na gestão e execução das atividades de segurança da informação e comunicação;

IV. Coordenar a execução da PSIC, mobilizando gestores para o cumprimento da Política;

V. Promover a cultura de segurança da informação e comunicação;

VI. Exercer outras atividades decisórias afetas à Gestão de Segurança da Informação e Comunicações no âmbito do órgão;

VII. Subsidiar o Comitê Gestor da Política de Segurança da Informação (CGPSI) no âmbito institucional.

Parágrafo único. O CGPSI será composto conforme Regimento Interno do foro.

5.2. DO COMITÊ GESTOR DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 16 As competências do CGPSI serão determinadas em Regimento Interno próprio do foro, publicado via portaria do Gabinete do Secretário de Estado de Saúde, além das quais caberá

I. Orientar e homologar a Política de Segurança da Informação e Comunicação (PSIC) e as Normas de Segurança da Informação e Comunicação (NoSIC) da SES-MT.

II. Orientar e homologar o Programa de Gestão de Riscos, atualizando-o quando necessário;

III. Orientar e homologar o Plano de Continuidade de Negócios, que deverá ser testado periodicamente;

IV. Orientar e acompanhar as ações do gestor da Segurança da Informação e Comunicação da SES-MT.

5.3. DO GESTOR DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 17 Compete ao Gestor da Segurança da Informação e Comunicação:

I. Presidir o Comitê Gestor da Política de Segurança da Informação (CGPSI);

II. Monitorar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III. Cobrar dos respectivos gestores a classificação das informações na área sob sua gestão;

IV. Propor recursos necessários às ações de segurança da informação e comunicação;

V. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis *impactos* na segurança da informação e comunicações;

VI. Propor Normas e procedimentos relativos à segurança da informação e comunicações;

VII. Definir métricas que permitam aferir a eficiência e eficácia dos controles de segurança.

Parágrafo Único: A gestão de segurança da informação deverá somente ser realizada por servidores e empregados públicos.

5.4. DO GESTOR DE ÁREA

Art. 18 Compete ao Gestor de Área:

I. Zelar e fazer cumprir a PSIC;

II. Identificar desvios de conduta na utilização das informações obtidas durante o exercício das funções de seus subordinados e adotar as medidas preventivas e corretivas apropriadas;

III. Aplicar medidas que visem a garantir que o pessoal sob sua supervisão proteja informações da área de gestão sob sua responsabilidade;

IV. Proteger, em nível físico e lógico, os ativos de informação e de processamento da área de gestão sob sua responsabilidade;

V. Impedir o acesso de pessoal desligado de área ou função aos ativos de informação sob sua responsabilidade, utilizando-se dos mecanismos previstos no plano de desligamento implementado;

VI. Comunicar formalmente o desligamento (exoneração, demissão, transferência, cessão, licença) de usuários à Superintendência de Gestão de Pessoas, os quais deverão notificar a área de Tecnologia da Informação para medidas cabíveis;

VII. Colaborar para o levantamento de dados para o Gerenciamento de Riscos da área sob sua gestão e informar novos riscos ainda não mapeados na área em que atua.

5.5. DO USUÁRIO

Art. 19 São obrigações do usuário:

I. Observar rigorosamente esta Política de Segurança de Informação e Comunicação, bem como as Normas e Procedimentos a ela vinculados;

II. Assegurar o sigilo e evitar o vazamento de dados e informações que estejam sob sua responsabilidade e/ou acesso e não estejam classificados como "públicos";

III. Assegurar o uso racional dos recursos de Tecnologia da Informação e Comunicação colocados à sua disposição, priorizando o interesse público e institucional;

IV. Comunicar a Área competente quaisquer riscos ou incidentes de segurança que venha a tomar conhecimento;

V. Assegurar-se que as senhas e credenciais para acesso aos ativos de processamento e de informações estejam de acordo com os procedimentos estabelecidos e que as mesmas sejam protegidas e confidenciais, não devendo ser compartilhadas, ou seja, toda senha é de uso PESSOAL e INTRANSFERÍVEL;

VI. Manter, obrigatoriamente, os dados críticos da sua unidade e setor em compartilhamentos de rede disponibilizados pela área de TIC;

VII. Não utilizar serviços de e-mail gratuitos para atividades institucionais, visto que tais serviços não possuem garantia de autenticidade, disponibilidade e confidencialidade das informações;

VIII. Ativar e utilizar adequadamente sua conta de e-mail corporativo apenas para fins institucionais e de forma a não cometer qualquer ato que possa prejudicar o trabalho, a imagem de terceiros ou do próprio Estado, em consonância com as determinações legais;

IX. Acessar a Internet apenas para navegação em sítios cujo conteúdo esteja adequado aos dispositivos legais, às suas determinações e às suas atribuições institucionais.

5.6. DA SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO DAS UNIDADES ADMINISTRATIVAS

Art. 20 São obrigações da Superintendência de Tecnologia da Informação:

I. Elaborar e atualizar a Política de Segurança da Informação (PSIC) e as Normas de Segurança da Informação e Comunicação (NoSIC), sob orientação do CGPSI, bem como os Procedimentos de Segurança da Informação e Comunicação (POPSIC) do órgão e de suas unidades, em conformidade com a PSIC, NoSIC(s) da SES-MT, legislação e regulamentos pertinentes;

II. Desenvolver, orientar e homologar um Programa de Gestão de Riscos, atualizando-o quando necessário;

III. Desenvolver Plano de Continuidade Tecnológica do Negócio para o órgão

IV. Realizar, com a periodicidade necessária, cópias de segurança dos dados armazenados nos compartilhamentos de rede, precavendo-se quanto a catástrofes;

V. Assegurar o pleno e efetivo funcionamento dos recursos de Tecnologia da Informação e Comunicação disponibilizados;

VI. Assegurar a integridade e a disponibilidade dos ativos que se encontram no seu ambiente computacional;

VII. Dar assistência ao CGPSI na elaboração de Políticas, Normas e Procedimentos de Segurança da Informação no tocante às informações, comunicações e processos relativos presentes no ambiente computacional;

VIII. Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação que se encontram no ambiente computacional;

IX. Requisitar informações às demais áreas da SES-MT, realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação e Comunicação no tocante aos ativos informatizados;

X. Elaborar o Plano de Resposta a Incidentes em complemento ao Plano de Continuidade Tecnológica do Negócio;

XI. Manter registro das atividades de usuários (logs), de maneira a abranger o máximo de ações possíveis dentro dos sistemas e pelo maior tempo possível;

XII. Solicitar criação e manutenção de ambiente de correio eletrônico institucional ao custodiante responsável por prover o serviço de correio eletrônico corporativo e deverá seguir as determinações do custodiante em conformidade com legislação e regulamentos específicos.

XIII. Priorizar o uso institucional do acesso à internet, podendo bloquear e/ou limitar acesso a determinados sítios de Internet e estabelecendo categorias passíveis de acesso em horários restritos.

XIV. Zelar para que custodiantes responsáveis por prover serviços de Tecnologia para o órgão não promovam ações que entrem em conflito com esta PSIC, normas e procedimentos, bem como legislação e regulamentos pertinentes.

5.7. DO PROPRIETÁRIO DA INFORMAÇÃO

Art. 21 São obrigações do Proprietário da Informação:

I. Identificar e definir as informações críticas e os requisitos de confidencialidade, integridade, disponibilidade, autenticidade e não repúdio;

II. Classificar e rever periodicamente a classificação dos ativos sob sua propriedade que requerem algum grau de sigilo, observando a legislação em vigor;

III. Participar do processo de avaliação e aceitação de risco;

IV. Participar nas decisões relacionadas a qualquer violação de segurança dos ativos sob sua propriedade;

V. Autorizar a liberação de acesso à informação sob sua responsabilidade;

VI. Participar da definição dos critérios para estabelecer perfis de acesso a informações sob sua responsabilidade;

VII. Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;

VIII. Participar, sempre que convocado, das reuniões do Comitê de Gestão de Segurança da Informação, prestando os esclarecimentos solicitados.

5.8. DO CUSTODIANTE DOS ATIVOS DA INFORMAÇÃO

Art. 22 São obrigações do custodiante dos Ativos da Informação:

I. Prestar assistência ao Proprietário da Informação na definição dos procedimentos operacionais e de controle, referentes a manuseio, armazenamento e disposição final dos ativos;

II. Controlar e proteger os ativos sob sua custódia;

III. Realizar, verificar e manter cópias de segurança (*backups*) dos ativos de informação sob sua custódia, a menos que outra solução seja acordada formalmente entre o proprietário da informação e o custodiante;

IV. Comunicar à STI e ao proprietário da informação qualquer incidente de segurança que afete os ativos sob sua custódia;

V. Implementar os controles de segurança e contratar, se necessário, bens e serviços de Segurança da Informação e Comunicação exigíveis por lei ou regulamentações específicas.

5.9. DO GRUPO DE RESPOSTA A INCIDENTES DE SEGURANÇA EM COMPUTADORES (GRISC)

Art. 23 O CSIRT será responsável por:

I. Suspender, a qualquer tempo, o acesso de usuário ou processo a informações ou recursos de Tecnologia da Informação e Comunicação, quando evidenciados riscos à segurança da informação, notificando, de imediato, o Gestor de Segurança da Informação e Comunicação;

II. Dar tratamento e encaminhamento aos incidentes de redes, tomando as medidas necessárias para conter as ameaças, minimizar os impactos e evitar futuras ocorrências, restabelecendo juntamente com o setor responsável, a integridade, confidencialidade e disponibilidade dos ativos;

III. Registrar, classificar e filtrar as notificações de Incidentes de Segurança;

IV. Executar o Plano de Resposta a Incidentes;

V. Recolher e preservar as evidências para subsidiar a forense computacional;

VI. Investigar as causas dos incidentes no ambiente computacional.

Parágrafo Único: Na ausência ou indisponibilidade da GRISC, as responsabilidades correspondentes passarão à Superintendência de Tecnologia da Informação.

6. ATUALIZAÇÃO

Art. 24 Esta Política, bem como Normas e Procedimentos que dela se originam deverão ser atualizadas com periodicidade mínima anual ou quando mudanças significativas, que afetem a base de avaliação de risco original, ocorrerem.

7. CONCLUSÃO

Este documento, responsável pela instituição da PSIC da SES-MT, norteará a elaboração de outros documentos relacionados à Segurança da Informação, os quais deverão observar as diretrizes e terminologias aqui apresentadas no intuito de assegurar um padrão documental.

Os dispositivos aqui estabelecidos apresentam as principais atividades a serem desenvolvidas. A sua priorização será definida pelos Gestores e Comitês aqui nominados.

Com esta PSIC, a SES-MT reafirma seu compromisso com a segurança de seus ativos e a prestação de serviços de excelência à sociedade e reitera aos usuários de suas informações a responsabilidade no cumprimento da Política ora apresentada.

ANEXO I - DOS CONCEITOS E DEFINIÇÕES

Para efeitos desta Política, adotam-se os seguintes conceitos e definições:

Aceitação de Risco: decisão de aceitar um risco. A aceitação pode ser necessária em razão do custo-benefício para se proteger um ativo ou devido ao risco residual remanescente após o tratamento de riscos.

Ameaça: são agentes ou condições causadoras de incidentes contra ativos. Exploram as vulnerabilidades, ocasionando perda de confidencialidade, integridade ou disponibilidade.

Alta Administração: dirigentes máximos da unidade, como Secretários de Estado e Subsecretários.

Análise / Avaliação de Risco: processo de identificação de ameaças e vulnerabilidades associadas a um ativo de modo a estimar a probabilidade e o impacto na ocorrência de um incidente.

Ativo: é tudo aquilo que tenha valor para a organização e consequentemente exige proteção.

Autenticidade: garantia de que o dado ou informação são verdadeiros.

Backup / Cópia de Segurança: é o processo de cópia de dados de um dispositivo de armazenamento para outro com o objetivo de proporcionar a proteção contra a perda dos originais.

Classificação da Informação: é o processo de identificar e definir níveis e critérios de proteção adequados para as informações de forma a garantir sua confidencialidade, integridade e disponibilidade, de acordo com a importância para a organização.

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Controle de Acesso: são restrições de acesso a um ativo da organização.

Controle de Segurança: são práticas de gestão de risco (políticas, normas, procedimentos ou mecanismos) que podem proteger os ativos contra ameaças, reduzir ou eliminar vulnerabilidades, limitar o impacto de um incidente ou ajudar na sua detecção.

Custódia: responsabilidade de se guardar um ativo para terceiros. A custódia não permite automaticamente o direito de acesso ao ativo, nem a capacidade de conceder direito de acesso a outros.

Custodiante: indivíduo a quem é dada a custódia de um ativo.

Direito de Acesso: privilégio associado a um usuário para ter acesso a um ativo.

Diretriz: o que deve ser feito e como, para atender aos objetivos declarados na política.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Forense Computacional: Conjunto de técnicas para coleta e exame de evidências digitais, reconstrução e dados e ataques, identificação e rastreamento de invasores.

Grupo de Resposta a Incidentes de Segurança em Computadores: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.

Gestor de área: responsável por qualquer unidade de uma organização, tais como: gerentes, coordenadores, superintendentes, diretores e todos os demais dirigentes que mantêm subordinados sob sua responsabilidade.

Gestão de Riscos: Atividade contínua de identificação, análise, tratamento, aceitação e comunicação de riscos.

Gestor de Segurança da Informação e Comunicação: é responsável pelas ações de segurança da informação e comunicações no âmbito da SES-MT.

Impacto: Tamanho do prejuízo, medido através de propriedades mensuráveis ou abstratas, que a concretização de uma determinada ameaça causará.

Incidente de Segurança: Qualquer evento que resulte no descumprimento da Política de Segurança da Informação e Comunicação que possa representar ameaça aos ativos, tais como: quebra da segurança, fragilidade, mau funcionamento, vírus, acesso indevido ou desnecessário a pastas/diretórios de rede, acesso indevido à internet ou programas instalados sem conhecimento da área de Tecnologia da Informação.

Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Log: é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional. Os registros devem conter hora e data das atividades, identificação do usuário, comandos e argumentos executados, identificação da estação local ou da estação remota que iniciou a conexão, entre outros.

Monitoramento: atividade de verificação manual ou automática de eventuais ameaças, incidentes de segurança ou quaisquer descumprimentos às diretrizes presentes na Política, Normas ou Procedimentos de Segurança da Informação e Comunicação.

Não repúdio: garantia de segurança de informação que impede uma entidade de negar ter participado de uma dada operação.

Plano de Continuidade de Negócio (PCN): documento que estabelece mecanismos para restabelecer a atividade de uma organização, em caso de interrupção.

Plano de Resposta a Incidentes: documento que estabelece metodologias que visam minimizar o impacto de um incidente e permitir o restabelecimento dos serviços o mais rápido possível.

Proprietário: Indivíduo que, em virtude de suas funções ou atribuições legais, tenha poder de decisão para identificar e classificar as informações geradas por sua área de gestão.

Proteção: vide Controle de Segurança.

Recursos de Tecnologia da Informação e Comunicação: conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio de *hardware e software*, a criação, acesso, armazenamento, transmissão e processamento de dados e informações.

Risco: é a probabilidade de uma determinada ameaça se concretizar, combinada com os impactos que ela trará.

Segurança da Informação: é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Servidor Público: pessoa física que exerce cargo, emprego ou função pública.

Tratamento do risco: processo de seleção e implementação de controles de segurança.

Usuário: Qualquer pessoa, física ou jurídica ou processo em um sistema computacional que faça uso dos recursos de Tecnologia da Informação e Comunicação relativos à SES-MT;

Vulnerabilidade: são fragilidades associadas aos ativos que os tornam susceptíveis às ameaças.

ANEXO II - DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Foram utilizadas as seguintes referências legais e normativas para elaboração desta política:

I. **Lei Complementar n° 04, de 15 de outubro de 1990** – Dispõe sobre o Estatuto dos Servidores Públicos da Administração Direta, das Autarquias e das Fundações Públicas Estaduais. (* suspensa a eficácia do §2º do Art. 272 - ADIN nº 554/06 e também suspensa a eficácia do Art. 57 - ADIN nº 559/06).

II. **Lei Federal nº 12.965, de 23 de abril de 2014** – Estabelece princípios, garantias, direitos e deveres para uso da Internet no Brasil;

III. **Lei Federal nº 12.737, de 30 de novembro de 2012** - Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências;

IV. **Lei Federal nº 12.735, de 30 de novembro de 2012** - Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências;

V. **Lei Federal nº 12.965, de 23 de abril de 2014-** Estabelece princípios, garantias e deveres para o uso da Internet no Brasil;

VI. **Lei Federal nº 12.527, de 18 de novembro de 2011** - 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;

XV. **ABNT NBR 15999-1:2007 - Gestão de continuidade de negócios** - Estabelece o processo, os princípios e a terminologia da gestão da continuidade de negócios (GCN);

XVI. **ABNT NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.** Especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação documentado dentro do contexto dos riscos de negócio globais da organização;

XVII.**ABNT NBR ISO/IEC 27002:2005 - Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação** - Estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização;

XVIII. **ABNT ISO GUIA 73:2009 - Gestão de riscos – Vocabulário** - Fornece as definições de termos genéricos relativos à gestão de riscos;

XIX. **Resolução COSINT nº 001/2005 –** Dispõe sobre as Políticas e Diretrizes do Sistema Estadual de Informação, aplicável aos órgãos e entidades da Administração Pública Direta e Indireta no âmbito do Poder Executivo do Estado de Mato Grosso;

XX. **Resolução CONSINT nº 003/2010 -** Dispõe sobre as Políticas e Diretrizes de Segurança da Informação no âmbito do Poder Executivo do Estado de Mato Grosso;

XXI. **Resolução COSINT nº 008-2010 -** Dispõe sobre as Normas de Segurança Estadual para Acesso à Informação no âmbito do Poder Executivo de Mato Grosso;

XXII. **Resolução COSINT nº 009-2011** - Dispõe sobre as Normas de Segurança para Uso do Correio Eletrônico Corporativo no Âmbito do Poder Executivo de Mato Grosso;

XXIII. **Resolução COSINT nº 010-2011** - Dispõe sobre as Normas de Segurança para uso da Internet no âmbito do Poder Executivo de Mato Grosso;

XXIV. **Resolução COSINT nº 011-2011** - Dispõe sobre as Normas de Segurança para Gerenciamento de Senhas no âmbito do Poder Executivo de Mato Grosso;

XXV. **Resolução COSINT nº 009/2014 -** Dispõe sobre a aprovação do Modelo de Gestão dos Sistemas Corporativos do Poder Executivo do Estado de Mato Grosso e dá outras providências;

XXVI. **Resolução COTEC nº 004/2018 -** Dispõe sobre a instituição da Política do Sistema Estadual de Tecnologia da Informação, no âmbito do Poder Executivo do Estado de Mato Grosso;

Documento:	Política de Segurança da Informação e Comunicação – PSIC
Dimensão:	Estrutura Normativa de Procedimentos
Tipo de Instrumento Normativo:	Política
Categoria do Assunto:	Controle e Conformidade
Assunto:	Sistema de Conformidade

Elaboração:	João Francisco Borba (presidente da CGPSI da SES-MT)
Aprovação:	Pleno do CGPSI da SES-MT
Versão:	1.0/2020
Homologação:	31 de março de 2021