PORTARIA Nº 723/2021/SEMA/MT

Institui a Política de Segurança da Informação - PSI, no âmbito da Secretaria de Estado de Meio Ambiente-SEMA/MT.

A SECRETÁRIA DE ESTADO DE MEIO AMBIENTE, no uso das atribuições legais que lhe confere o art. 71, inciso IV, da Constituição Estadual e o art. 3º, da Lei Complementar nº 612, de 28 de janeiro de 2019, que dispõe sobre a organização administrativa do Poder Executivo Estadual;

CONSIDERANDO a Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso às informações.

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação - PSI no âmbito da Secretaria de Estado de Meio Ambiente - SEMA/MT, em complemento a Política estabelecida pelo Conselho Superior do Sistema Estadual de Informação e Tecnologia da Informação- COSINT, instituídas pela Resolução nº 003/2010.

Parágrafo único. Integram também a PSI as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

CAPÍTULO I

Dos Conceitos e Definições

Art. 2º Para os efeitos desta Portaria, entende-se por:

I - ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

II - ativos de informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

IV - capacitação em SI: Desenvolvimento de aptidões, habilidades e conhecimentos mínimos em SI para o desempenho de suas funções.

V - classificação da informação: Identificação, pelo gerador da informação, do seu nível de classificação para uso dos controles de proteção necessários.

VI - Comitê de Segurança da Informação - CSI: colegiado de caráter deliberativo e multidisciplinar responsável pela normatização e supervisão da segurança da informação no âmbito da SEMA. Em caso de não existência, o CSI deverá ser estabelecido no prazo de 90 dias a partir da data de publicação da PSI;

VII - confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada e credenciada;

VIII - conscientização em SI: saber o que é segurança da informação e aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema;

IX - controle de acesso: conjunto de normas, procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

X - eventos relevantes em SI: ações que possam trazer riscos à confidencialidade, integridade, disponibilidade e autenticidade das informações.

XI - custodiante do ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que lhe pertencem ou não, mas que estão sob sua custódia;

XII - disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade;

XIII - gestão de ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada

dos controles desses ativos;

XIV - gestão de continuidade dos negócios: processo de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem.

XV - gerenciamento de operações: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporta, satisfazendo os acordos de níveis de serviço;

XVI - gestor dos ativos de informação: responsável por gerenciar determinado ativo de SI;

XVII - incidente de SI: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XVIII - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XIX - infraestrutura de TI: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento, rede sem fio e rede telefônica;

XX - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXI - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XXII - recursos criptográficos: sistemas, programas, processos e equipamento isolado ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXIII - risco de SI: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XXIV - segurança física e do ambiente: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

XXV - sensibilização em SI: disponibilizar conhecimento em SI para capacitar os envolvidos em tomar decisões ou reagir em SI;

XXVI - sistema estruturante: conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;

XXVII - terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos à SEMA;

XXVIII - tratamento de incidentes: é a atividade de receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança;

XXIX - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XXX - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO II

Seção I

Do Objetivo da Política de Segurança da Informação -PSI

Art. 3º A PSI deve obedecer aos princípios constitucionais, administrativos e do arcabouço legal vigente que regem a Administração Pública Federal, Estadual e Municipal.

Art.4º A PSI objetiva garantir a confidencialidade, integridade, disponibilidade e autenticidade (CIDA) das informações produzidas ou custodiadas pela SEMA.

Parágrafo único. As diretrizes de Segurança da Informação - SI devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e estrutura da SEMA.

Art. 5º A SEMA deve observar as diretrizes, normas, procedimentos, mecanismos, competências e responsabilidades estabelecidas nesta PSI.

Seção II

Da Abrangência

Art. 6º As diretrizes, normas complementares e manuais de procedimentos da PSI da SEMA aplicam-se a servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, execute atividades vinculadas a esta Secretaria.

§1º A PSI também se aplica, no que couber, ao relacionamento da SEMA com outros órgãos e entidades públicos ou privados.

§2º Todos são responsáveis e devem estar comprometidos com a segurança da informação, seja digital ou física, sob pena de responsabilidade civil, penal e administrativa.

§3º É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas ou custodiadas pela SEMA.

Art. 7º As unidades da Secretaria de Estado de Meio Ambiente devem adotar ou utilizar esta PSI e suas normas complementares como modelos de referência para elaboração dos seus documentos.

Art. 8º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pela SEMA devem atender a esta PSI.

Parágrafo único. Os contratos firmados pela SEMA devem conter cláusulas que determinem a observância da PSI e suas normas respectivas.

CAPÍTULO III

DIRETRIZES GERAIS

Art. 9º O cumprimento desta política de segurança e de suas normas complementares deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente constituído pelo Comitê de Segurança da Informação - CSI, buscando a certificação do cumprimento dos requisitos de segurança da informação.

Art. 10. A SEMA, além das diretrizes estabelecidas nesta PSI, deve também se orientar pelas melhores práticas e procedimentos de SI recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 11. Os recursos tecnológicos, instalações de infraestrutura e os sistemas de informação da SEMA devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 12. Todo e qualquer incidente de SI ocorrido no âmbito da SEMA, devem ser formalmente comunicados ao Secretário Adjunto Executivo e ao CSI.

CAPÍTULO IV

Das Competências

Seção I

Do Comitê de Segurança de Informação -CSI

Art. 13. O CSI deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias da Secretaria e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

Art. 14. Os membros do CSI serão designados por Portaria específica a ser elaborada em até 30 dias.

Art.15. Compete ao Comitê de Segurança da Informação - CSI:

I - instituir programas permanentes e regulares de conscientização, sensibilização e capacitação em SI;

II - convocar as reuniões de deliberação da PSI;

III- buscar parcerias com outros órgãos e entidades;

IV - elaborar norma de descarte de informações;

V- propor à Direção da SEMA normas para regulamentação da computação em nuvem;

VI - criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor;

VII- estabelecer, com auxílio da CTI, normas adequadas relacionadas à SI de tecnologia da informação para a disponibilização dos serviços, sistemas e infraestrutura de TI que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais da SEMA;

VIII - planejar, com auxílio da CTI, medidas de proteção e balancear os custos na aplicação de controles, de acordo com os

danos potenciais de falhas de segurança de tecnologia da informação;

IX- implementar os procedimentos relativos ao uso de recursos criptográficos, no âmbito das informações produzidas e custodiadas na SEMA, em conformidade com as orientações contidas em norma específica;

X - estabelecer o escopo da análise de risco e conformidade das práticas de SI da SEMA;

XI - acompanhar e avaliar os danos decorrentes de quebras de segurança;

XII - propor recursos necessários às ações de SI;

XIII - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SI;

XIV - propor, sempre que necessário, alterações e revisões na PSI e nas normas vigentes;

XV - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SI;

XVI - aprovar o plano de investimentos em SI da SEMA;

XVII - elaborar o seu Regimento Interno.

Art. 16. O CSI deverá elaborar em até 180 dias, a contar da publicação desta Portaria, um modelo para classificação da informação.

Parágrafo único. Após a definição do modelo, as Secretarias Adjuntas terão 90 dias para enviar o relatório, contendo as informações classificadas, que deverá ser aprovado pelo CSI.

Seção II

Do Titular da Unidade Administrativa

Art. 17. Compete ao titular da unidade administrativa:

I - conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SI;

II - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SI;

III - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SI por parte dos usuários sob sua supervisão;

IV- informar à Coordenadoria de Gestão de Pessoas a movimentação de pessoal de sua unidade;

V - realizar o tratamento e a classificação da informação conforme plano de classificação da informação da SEMA;

VI - manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores.

Seção III

Dos Terceiros e Fornecedores

Art. 18. Compete aos terceiros e fornecedores, conforme previsto em contrato:

I - observar, no exercício de suas atividades, a íntegra desta PSI;

II - tomar conhecimento desta PSI;

III - fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato;

IV - fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

Seção IV

Dos Usuários

Art. 19. Compete aos usuários:

I - conhecer e cumprir todas as políticas, normas e procedimentos relacionados à SI; e

II - comunicar formalmente os incidentes que afetam a segurança dos ativos de informação ao CSI.

III- difundir e exigir o cumprimento da PSI, das normas de segurança e da legislação vigente acerca do tema.

CAPÍTULO V

DIRETRIZES ESPECÍFICAS

Art. 20. Para cada uma das diretrizes constantes das seções deste capítulo devem ser elaboradas normas específicas, manuais e procedimentos conforme especialização de cada área da SEMA.

Seção I

Da Gestão de Ativos da Informação

Art. 21. Os ativos de informação devem:

I - ser inventariados e protegidos;

COSINT - II - ter identificados os seus proprietários e custodiantes;

III - ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV - ter a sua entrada e saída nas dependências da SEMA autorizadas e registradas por autoridade competente;

V - ser passíveis de monitoramento e ter seu uso fiscalizado quando houver indícios de quebra de segurança, através de meios que permitam a rastreabilidade do uso desses ativos;

VI - ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 22. O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação.

Parágrafo único: A não designação pressupõe que o gestor é o próprio custodiante.

Art. 23. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite do termo de sigilo e responsabilidade.

Seção II

Da Conscientização e Capacitação

Art. 24. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários da SEMA e que apoiem esta PSI de acordo com suas competências funcionais.

Seção III

Dos Controles de Acessos

Art. 25. Todos os sistemas de informação da SEMA, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente.

Parágrafo único: Compete ao gestor:

I- Definir os privilégios de acesso às informações;

II - Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação;

III - Registrar eventos relevantes para a segurança e o rastreamento de acesso às informações.

Art. 26. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação.

Art. 27. A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

Parágrafo único: Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento, afastamento, licenças.

Art. 28. Os sistemas estruturantes devem possuir normas específicas, no âmbito de sua atuação, que requerem o controle de acesso quanto:

I - ao acesso às suas bases de dados;

II - à extração, carga e transformação de dados; e,

III - aos serviços acessíveis via linguagem de programação.

Art. 29. Os sistemas estruturantes devem possuir mecanismos automáticos para:

I - revogar as concessões e desativar as contas de acesso do servidor nos casos de exoneração, demissão, aposentadoria e falecimento do servidor;

II - criação automática de "log" de acessos, com informações suficientes para inequívoca identificação de qual usuário fez o acesso, quais transações realizou;

III - bloquear as contas de acesso do servidor nos casos de férias, licença, afastamento - mesmo que temporário, cessão e disponibilidade; e

IV - tratar os casos de remoção e redistribuição do servidor, segundo as definições constantes na norma de controle de acesso ao sistema.

Art. 30. É de responsabilidade do Coordenador de Gestão de Pessoas disponibilizar os registros de todas as movimentações de pessoal.

Seção IV

Da Criptografia

Art. 31. O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Responsabilidade e Confidencialidade pelo seu uso.

Seção V

Da Aquisição, do Desenvolvimento e da Manutenção de Sistemas

Art. 32. O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica.

Art. 33. A estrutura da CTI deve estabelecer critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção, em até 180 dias.

Seção VI

Da Conformidade

Art. 34. Deve ser realizada, com periodicidade mínima anual, a verificação da conformidade das práticas de SI da SEMA e de suas unidades administrativas com esta PSI e suas normas e procedimentos complementares, bem como com a legislação específica de SI.

Parágrafo único. O CSI estabelecerá o escopo da análise de risco e conformidade para o período determinado.

Art. 35. A verificação da conformidade da SI de tecnologia da informação será realizada de forma planejada, mediante calendário de ações proposto pela CTI e aprovado pelo CSI.

Art. 36. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a SEMA.

Art. 37. O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos.

Art. 38. Nenhuma unidade administrativa poderá permanecer sem verificação de conformidade de suas práticas de SI por período superior a 2 (dois) anos.

Art. 39. A execução da verificação de conformidade será realizada pelo CSI, podendo ser realizada por terceiros.

Art. 40. É vedado ao prestador de serviços executar a verificação de conformidade dos próprios serviços prestados.

Art. 41. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Gestor de SI ao Gestor da unidade administrativa verificada, para ciência e providências a serem adotadas com relação às vulnerabilidades eventualmente apresentadas.

Seção VII

Do Plano de Investimentos em SI da SEMA

Art. 42. Os investimentos em SI constituirão ação orçamentária específica e permanente na Lei Orçamentária Anual, distinta das outras ações orçamentárias;

Art. 43. Os investimentos em SI serão realizados anualmente, de forma planejada e consolidados em um plano de investimentos.

Parágrafo único. O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

Art. 44. O plano de investimentos, assim como a correspondente proposta orçamentária, será aprovado pelo CSI, mediante recomendação elaborada pela CTI no escopo de tecnologia da informação.

Seção VIII

Da Propriedade Intelectual

Art. 45 As informações produzidas por servidores, colaboradores e prestadores de serviços, no exercício de suas funções, são patrimônio intelectual da SEMA, sujeitas à política de classificação da informação e não cabe a seus criadores qualquer forma de direito autoral.

Art. 46. É vedada a utilização de informações produzidas por terceiros para uso exclusivo da SEMA em quaisquer outros projetos ou atividades de uso diverso do estabelecido pela Secretaria, salvo com autorização específica e formal do Secretário de Estado do Meio Ambiente ou dos Secretários Adjuntos.

Seção IX

Dos Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 47. Nos casos de obtenção de informações de terceiros, o gestor da área em que a informação será utilizada deverá, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre as informações, antes de seu uso.

Art. 48. Os acordos com terceiros devem envolver todas as partes envolvidas.

Parágrafo único. Os acordos que concedam o acesso a terceiros podem incluir, quando necessário e justificado, permissão para designação de outras partes autorizadas e condições para os seus acessos desde que expressamente autorizadas pela SEMA.

Art. 49. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta PSI e suas normas complementares aos seus empregados e prepostos envolvidos em atividades na SEMA.

Art. 50. Todo contrato, convênio, acordos ou instrumentos congêneres deverão prever um plano de contingência para caso de uma das partes desejar o seu encerramento antes dos prazos acordados.

CAPÍTULO IV

Das Penalidades

Art. 51. Ações que violem a PSI ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SI serão devidamente apuradas em processo administrativo e aos responsáveis serão aplicadas as sanções cabíveis.

REGISTRADA, PUBLICADA, CUMPRA-SE.

Cuiabá, 26 de julho de 2021.

Mauren Lazzaretti

Secretária de Estado de Meio Ambiente

SEMA-MT