Publicação: 11/2/2020
DJe: 10/2/2020

PORTARIA Nº 4718/PR/2020

Institui a Política de Segurança da Informação no âmbito da Tecnologia da Informação e Comunicação do Tribunal de Justiça do Estado de Minas Gerais e dispõe sobre o Modelo de Gestão de Segurança da Informação.

O **PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DE MINAS GERAIS**, no uso das atribuições que lhe confere o inciso II do art. 26 do Regimento Interno do Tribunal de Justiça, aprovado pela Resolução do Tribunal Pleno nº 3, de 26 de julho de 2012,

CONSIDERANDO que o Tribunal de Justiça do Estado de Minas Gerais - TJMG, no exercício de suas competências institucionais, produz, adquire e concentra informações, que devem permanecer íntegras, disponíveis e, quando for o caso, com o sigilo resguardado;

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado, eficiente e seguro, de forma a oferecer todas as informações necessárias à prestação jurisdicional com integridade, confidencialidade e disponibilidade;

CONSIDERANDO que a Resolução do Conselho Nacional de Justiça - CNJ nº 211, de 15 de dezembro de 2015, em seu art. 9º, determina que cada órgão deverá elaborar e aplicar política, gestão e processos de Segurança da Informação, por meio de um Comitê Gestor de Segurança da Informação, e em harmonia com as diretrizes nacionais para a Gestão de Segurança da Informação preconizadas pelo CNJ;

CONSIDERANDO as boas práticas preconizadas pelas normas ABNT NBR ISO/IEC, série 27000, e outras normas nacionais e internacionais relativas à Segurança da Informação;

CONSIDERANDO a necessidade de estabelecer responsabilidades internas quanto à Segurança da Informação;

CONSIDERANDO a Portaria Conjunta da Presidência nº 634, de 15 de maio de 2017, que "Dispõe sobre o Plano Estratégico de Tecnologia da Informação e Comunicação - PETIC, no âmbito do Tribunal de Justiça do Estado de Minas Gerais - TJMG";

CONSIDERANDO que a Portaria Conjunta da Presidência nº 658, de 20 de julho de 2017, instituiu o Comitê Gestor de Segurança da Informação - CGSI e o Núcleo Técnico de Segurança da Informação - NTSI, com as atribuições de propor e aprovar a Política de Segurança do TJMG;

CONSIDERANDO a Portaria Conjunta da Presidência nº 723, de 27 de fevereiro de 2018, que "institui o Comitê de Tecnologia da Informação e Comunicação - CTIC e dispõe sobre a sua composição e sobre o encaminhamento de demandas relativas à Tecnologia da Informação e Comunicação - TIC";

CONSIDERANDO a Portaria do CNJ nº 47, de 29 de novembro de 2017, que Institui a Política de Segurança da Informação do Conselho Nacional de Justiça;

CONSIDERANDO a Lei federal nº 13.709 - Lei Geral de Proteção de Dados Pessoais - LGPD, de 14 de agosto de 2018, que "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural";

CONSIDERANDO o que constou no Processo do Sistema Eletrônico de Informações - SEI nº 0023323-70.2018.8.13.0000.

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Seção I
Do princípio básico da Política de Segurança da Informação, no âmbito de Tecnologia da Informação e Comunicação do Tribunal de Justiça do Estado de Minas Gerais

Art. 1º Fica instituída a Política de Segurança da Informação no âmbito de Tecnologia da Informação e Comunicação do Tribunal de Justiça do Estado de Minas Gerais - PSI-TIC/TJMG, nos termos desta Portaria.

Parágrafo único. A PSI-TIC/TJMG, aprovada pelo Comitê Gestor de Segurança da Informação - CGSI, possui como princípio norteador a garantia da integridade, da autenticidade, da confidencialidade, da disponibilidade e da irretratabilidade dos ativos de informação e de processamento, que tenham sido produzidos ou custodiados pelo TJMG, alinhada às estratégias do Conselho Nacional de Justiça - CNJ e ao Plano Estratégico de Tecnologia da Informação e Comunicação - PETIC, do TJMG.

Seção II
Das definições relativas à PSI-TIC/TJMG

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

I - ameaça: qualquer circunstância ou evento com o potencial de causar dano ou violação sobre a confidencialidade, a integridade, a autenticidade e a disponibilidade da informação, do sistema ou da organização;

II - ativo crítico: aquele que gera, armazena, processa, transmite e descarta informações de valor e criticidade altos para o negócio;

III - ativo de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação e os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - autenticidade: propriedade de que uma entidade (dado, informação, documento, sistema, usuário, etc.) é quem ou o que afirma ser;

V - avaliação de riscos: processo de comparar o risco estimado com critérios predefinidos para determinar a importância do risco;

VI - Comitê Gestor de Segurança da Informação - CGSI: comitê composto por representantes de áreas relevantes do TJMG, responsável pela formulação, implementação, acompanhamento e revisão das ações de segurança pertinentes;

VII - confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos que não possuam autorização;

VIII - continuidade de serviços essenciais de TIC: capacidade estratégica e tática do TJMG de se planejar e responder a incidentes e interrupções devido às vulnerabilidades de TIC, minimizando seus impactos e recuperando perdas de ativos de informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

IX - diretriz: descrição que orienta o que deve ser feito para alcançar os objetivos estabelecidos no PSI-TIC/TJMG e no Modelo de Gestão de Segurança da Informação - MGSI;

X - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por indivíduos, entidades ou processos autorizados;

XI - evento de segurança da informação: ocorrência ou mudança identificada do estado de um sistema, serviço ou rede, indicando uma possível violação da PSI, ou falha de controles ou, ainda, uma situação previamente desconhecida que possa ser relevante para a Segurança da Informação;

XII - gestão da segurança da informação: conjunto de políticas, normas e procedimentos para a gestão sistemática de dados sensíveis em uma organização, visando minimizar os riscos e garantir a continuidade de serviços essenciais de TIC, limitando o impacto de uma possível violação de segurança;

XIII - gestão de riscos: atividades coordenadas para dirigir e controlar uma organização, no que se refere aos riscos. Normalmente inclui a avaliação, o tratamento, a aceitação e a comunicação do risco;

XIV - incidente de segurança: evento ou conjunto de eventos de segurança da informação, indesejados ou inesperados, confirmados ou sob suspeita, que tenham

grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

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

XVI - integridade: propriedade de completude e precisão de uma informação que não foi indevidamente modificada ou destruída, de maneira não autorizada ou acidental, por indivíduos, entidades ou processos;

XVII - norma: instrumentos de apoio para regular atos, padrões e regras, a fim de garantir a aplicabilidade de recursos para o alcance dos atributos da segurança da informação (autenticidade, confidencialidade, integridade, disponibilidade);

XVIII - Política de Segurança da Informação - PSI: documento aprovado pelo CGSI, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicação;

XIX - procedimento: instrumentos de apoio necessários de como proceder para garantir a aplicabilidade de recursos para o alcance dos atributos da segurança da informação (autenticidade, confidencialidade, integridade, disponibilidade);

XX - recurso de tecnologia de informação: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, ou as instalações físicas que os abriguem;

XXI - riscos de segurança da informação: potencial exploração de vulnerabilidades de ativos de informação por uma ou mais ameaças, comprometendo a autenticidade, confidencialidade, disponibilidade e integridade das informações;

XXII - segurança da informação: preservação da disponibilidade, integridade e confidencialidade da informação, podendo envolver outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade;

XXIII - serviços essenciais de TIC: são os serviços de TIC imprescindíveis à atividade fim do TJMG, ou seja, a prestação jurisdicional e aos operadores de direito;

XXIV - serviços de TIC: é o serviço fornecido por provedores de serviços de TIC, composto por uma combinação de soluções de tecnologia da informação, pessoas e processos;

XXV - tratamento do risco: processo de seleção e implantação de medidas de controle para modificar um risco;

XXVI - usuário: pessoa que utiliza sistemas e demais recursos de TIC do TJMG;

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

Seção III
Dos objetivos da PSI-TIC/TJMG

Art. 3º A PSI-TIC/TJMG tem como objetivo geral estabelecer diretrizes e normas de apoio necessárias para assegurar o sigilo, a integridade, a autenticidade e a disponibilidade de dados, informações e conhecimentos no âmbito do TJMG, de modo a resguardar a legitimidade de sua atuação e contribuir para o cumprimento de suas atribuições legais.

Art. 4º São objetivos específicos da PSI-TIC/TJMG:

I - dotar o TJMG de instrumentos normativos e organizacionais necessários à efetiva implementação da PSI-TIC/TJMG;

II - orientar a adoção de mecanismos, medidas e procedimentos de proteção a dados, informações e conhecimentos relativos à privacidade das pessoas, ao interesse institucional e aos direitos de propriedade intelectual;

III - nortear a adoção de mecanismos, medidas e procedimentos internos para que o acesso a dados e informações sensíveis e sigilosos seja permitido apenas a pessoas e órgãos autorizados, respeitando-se a legislação vigente;

IV - subsidiar ações voltadas à salvaguarda da exatidão e da integridade de dados, informações e conhecimentos, bem como dos métodos de trabalho;

V - orientar as ações permanentes de conscientização, capacitação e educação sobre a importância da proteção de dados, informações e conhecimentos, com o propósito de internalizar o compromisso com a segurança da informação;

VI - combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição.

CAPÍTULO II
DO MODELO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 5º A PSI-TIC/TJMG integra o Modelo de Gestão de Segurança da Informação - MGSI, do TJMG, composto, no mínimo, pelos seguintes processos:

I - Classificação e Tratamento da Informação;

II - Gestão de Riscos de Segurança da Informação;

III - Gestão de Acesso e Uso de Recursos de TIC;

IV - Gestão e Controle de Ativos de Informação;

V - Gestão de Incidentes de Segurança da Informação;

VI - Gestão da Continuidade de Serviços Essenciais de TIC;

VII - Divulgação e Conscientização.

§ 1º Parágrafo único. Os processos do MGSI :

I - são interdependentes e devem ser estruturados e monitorados de forma a permitir sua melhoria contínua;

II - serão regulamentados em normas específicas, em conformidade com as normas e diretrizes de Gestão de Segurança da Informação estabelecidas pelo CNJ e pelo TJMG;

III - deverão ser revisados periodicamente.

Art. 6º A implantação dos processos do MGSI observará:

I - a classificação e o tratamento da informação com o objetivo de assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para o TJMG;

II - a definição e a utilização de Termos de Sigilo e Responsabilidade para acesso às informações classificadas;

III - a avaliação contínua dos riscos de segurança da informação por meio de análise sistemática e periódica;

IV - a gestão de riscos em segurança da informação com o objetivo de minimizar os riscos associados à informação, apresentando as medidas de segurança necessárias;

V - a gestão de acesso (lógico e físico) a sistemas de informação, de forma que o acesso seja controlado e esteja de acordo com as normas e os procedimentos definidos;

VI - o inventário e a gestão dos ativos de TIC, que devem ser inventariados, classificados, atualizados periodicamente e mantidos em condições de uso, principalmente os ativos críticos;

VII - a implantação de uma equipe de resposta a incidentes de segurança da informação para avaliar fragilidades e eventos associados, principalmente, aos ativos críticos de TIC, de forma que esses eventos possam ser comunicados para tomada de ação corretiva em tempo hábil, visando impedir, interromper ou minimizar o impacto de uma ação maliciosa ou acidental;

VIII - a continuidade do negócio, visando reduzir para um nível aceitável a interrupção causada por desastres ou falhas, principalmente, nos ativos que suportam os processos críticos de informação do TJMG;

IX - o estabelecimento de um programa de capacitação e conscientização de todos os envolvidos, inclusive usuários, em relação à adoção de comportamento seguro na utilização das informações;

X - validação das evidências de cumprimento da PSI-TIC/TJMG e do MGSI;

XI - a definição de uma política de geração e restauração de cópias de segurança.

Art. 7º O uso adequado dos recursos de TIC visa garantir a continuidade da prestação jurisdicional do TJMG.

§ 1º Os recursos de TIC devem ser utilizados em atividades estritamente relacionadas às funções institucionais.

§ 2º A utilização dos recursos de TIC será passível de monitoramento pelo TJMG, conforme as orientações do CGSI.

Art. 8º O acesso às informações de TIC produzidas ou custodiadas pelo TJMG está sujeito às disposições estabelecidas pela PSI-TIC/TJMG, em normas e procedimentos específicos relativos ao tema, estabelecidos no MGSI.

§ 1º O acesso a sistemas de informação do TJMG deve ser controlado de acordo com o valor, sensibilidade e criticidade da informação nele contida e considerando aspectos de restrição legais.

§ 2º O acesso às informações não públicas, por quaisquer colaboradores, deve ser condicionado ao aceite de termo de sigilo e responsabilidade.

Art. 9º A classificação das informações produzidas ou custodiadas pelo TJMG deve indicar a necessidade, a prioridade e o grau de proteção dessas informações, durante todo o seu ciclo de vida, com níveis e critérios para sua criação, manuseio, transporte, armazenamento e descarte.

Art. 10. O processo de classificação das informações estabelecerá critérios e controles para as operações de armazenamento, transferência, divulgação, reprodução, transporte, recuperação e descarte de informações de TIC, de acordo com o nível de classificação e temporalidade, incumbindo-lhe custodiá-las em ambiente propício à adequada proteção e preservação, proporcionais ao grau de sigilo e de criticidade, capazes de assegurar a sua autenticidade, confidencialidade, disponibilidade, integridade e irretratabilidade.

Parágrafo único. Excluem-se da responsabilidade de que trata o "caput" deste artigo as informações de TIC produzidas por iniciativa isolada de usuários, sem o devido respaldo legal e normativo que regulamente ou autorize o ato, o documento ou o processo de trabalho envolvido.

Art. 11. O Processo de Desenvolvimento de "Software" do TJMG deve considerar as boas práticas de desenvolvimento com foco em segurança da informação, de forma a preservar o ambiente tecnológico, assim como prevenir possíveis vulnerabilidades

e incidentes que afetem a autenticidade, a confidencialidade, a integridade e a disponibilidade das informações e dos recursos de TIC do TJMG.

CAPÍTULO III
DAS DISPOSIÇÕES FINAIS

Art. 12. A PSI-TIC/TJMG se aplica a todos os magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos que fazem uso dos ativos de informação e de processamento no âmbito da TJMG.

Parágrafo único. Os destinatários da PSI-TIC/TJMG relacionados no "caput" deste artigo são responsáveis:

I - pela segurança da informação, de acordo com os preceitos estabelecidos nesta Portaria;

II - por informar imediatamente ao NTSI do TJMG os incidentes em segurança da informação de que tenham ciência ou suspeita, bem como a ocorrência de quebra de termos de sigilo e responsabilidade ou vazamento de informações classificadas e controladas;

III - por colaborar na respectiva área de competência com a identificação e o tratamento de incidentes de segurança da informação.

Art. 13. O descumprimento das disposições da PSI-TIC/TJMG ou das normas e procedimentos específicos sobre segurança da informação sujeitam o infrator às penalidades previstas na legislação e nos regulamentos internos do TJMG, a ser apurado em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e cível.

Art. 14. As normas relacionadas à segurança da informação, no âmbito da TIC, editadas pelo TJMG, deverão observar as disposições estabelecidas nesta Portaria.

Art. 15. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo TJMG devem observar, no que couber, o constante da PSI-TIC/TJMG e do MSGI.

Art. 16. A PSI-TIC/TJMG será revisada e atualizada bianualmente ou quando solicitada pelo CGSI.

Art. 17. Casos omissos e dúvidas sobre a aplicação da PSI-TIC/TJMG deverão ser submetidos ao CGSI do TJMG.

Art. 18. Esta Portaria entra em vigor na data de sua publicação.

Belo Horizonte, 10 de fevereiro de 2020.

Desembargador **NELSON MISSIAS DE MORAIS**
Presidente