RESOLUÇÃO N. 216, DE 4 DE FEVEREIRO DE 2020

Institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Militar do Estado de Minas Gerais.

O PLENO DO TRIBUNAL DE JUSTIÇA MILITAR DO ESTADO DE MINAS GERAIS, no uso das atribuições que lhe confere o art. 11, VIII, "c", do Regimento Interno deste Tribunal,

CONSIDERANDO a Resolução n. 211, de 15 de dezembro de 2015, do Conselho Nacional de Justiça, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o período de 2015-2020;

CONSIDERANDO a necessidade de estabelecer, no âmbito do Tribunal de Justiça Militar do Estado de Minas Gerais, diretrizes e padrões para garantir um ambiente tecnológico controlado, eficiente e seguro, que favoreça as atividades jurisdicionais e administrativas com integridade, confidencialidade e disponibilidade, preservando a credibilidade na prestação jurisdicional;

CONSIDERANDO as deliberações do Comitê de Governança e Gestão de Tecnologia da Informação e Comunicação (CGTIC/TJMMG);

CONSIDERANDO a deliberação do Pleno deste Tribunal na sessão administrativa realizada em 11 de dezembro de 2019,

RESOLVE:

CAPÍTULO I
DO OBJETIVO

Art. 1° Fica instituída a Política de Segurança da Informação (PSI) da Justiça Militar do Estado de Minas Gerais (JMEMG), na forma do disposto nesta Resolução.

Art. 2° A Política de Segurança da Informação tem por objetivo estabelecer diretrizes e instituir responsabilidades com a finalidade de garantir mecanismos de controle e proteção dos processos de negócios, serviços, materiais e recursos, preservando a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações da Justiça Militar do Estado de Minas Gerais.

Parágrafo único. Os mecanismos de prevenção e proteção devem levar em consideração a informação em qualquer meio ou suporte, seja este papel, nato-digital ou digitalizado e os serviços de telemática, que incluem as redes

digitais, sistemas de videoconferência e de transmissão e gravação de sessões de audiência.

CAPÍTULO II
DAS DEFINIÇÕES

Art. 3° Para os efeitos desta Resolução aplicam-se as seguintes definições:

I - ativo de informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio;

II - comitê gestor de segurança da informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito da JMEMG;

III - confidencialidade: garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;

IV - disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos recursos correspondentes sempre que necessário;

V - gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão na identificação, na avaliação, no tratamento, no monitoramento e na análise crítica dos riscos que incidam sobre o bem a ser protegido com o objetivo de eliminá-los ou minimizar seus efeitos;

VI - incidente de segurança da informação: situação ocasionada por um ou vários eventos indesejados ou inesperados que tenha uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

VII - informação: conjunto de dados utilizados para transferência de mensagem entre indivíduos, usuários e máquinas, em processos comunicativos, desenvolvidos em qualquer meio, seja ele impresso, escrito ou falado, em ambiente físico ou virtual;

VIII - integridade: salvaguarda de exatidão e completeza da informação e dos métodos de processamento;

IX - plano de contingência de informações: conjunto de ações de prevenção e procedimentos de recuperação a serem seguidos para proteger os processos críticos de trabalho contra efeitos de falhas de equipamentos, acidentes, ações intencionais ou desastres naturais significativos, assegurando a disponibilidade das informações;

X - recurso de tecnologia de informação: qualquer recurso humano, equipamento, dispositivo, serviço, infraestrutura, instalação física ou sistema de processamento que abriguem as informações;

XI - usuários: os magistrados, os servidores e os estagiários, bem como os empregados de empresas prestadoras de serviços terceirizados, os consultores e outras pessoas que se encontrem a serviço da JMEMG, utilizando, em caráter temporário, os recursos tecnológicos disponibilizados, desde que previamente autorizados;

XII - autenticidade: veracidade da informação produzida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

XIII - ciclo de vida da informação/documento: período que compreende a produção, o recebimento, a classificação, o acesso, o uso, a alteração, o arquivamento o transporte e o descarte da informação;

XIV - documento: unidade de registro de informação, em qualquer suporte ou formato;

XV - governança de TIC: conjunto de diretrizes, estruturas organizacionais, processos e mecanismos de controle que visam assegurar que as decisões e ações relativas à gestão e ao uso da TIC se mantenham em conformidade com as necessidades institucionais e contribuam para o cumprimento da missão e o alcance das metas organizacionais;

XVI - Política de Segurança da Informação (PSI): conjunto de regras e diretrizes cujo objetivo é monitorar o tratamento da informação, definindo normas/técnicas e práticas de segurança.

XVII - segurança da informação: conjunto de medidas visando garantir a disponibilidade, a integridade, a autenticidade e a confidencialidade da informação, minimizando riscos, promovendo a eficácia da comunicação e preservando a imagem da JMEMG;

XVIII - Tecnologia da Informação e Comunicação (TIC): ativo estratégico que suporta processos institucionais, por meio da conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, utilizar e disseminar informações;

XIX - tratamento da informação/documento: conjunto de ações que compreende a produção, o recebimento, a classificação, a utilização, a distribuição, a reprodução, o uso, o arquivamento e a eliminação da informação.

CAPÍTULO III
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 4º A Política de Segurança da Informação da JMEMG observa os seguintes requisitos legais e normativos:

I - Constituição Federal de 1988: artigo 5º, inciso XXXIII; artigo 37, inciso II, § 3º; e artigo 216, § 2º;

II - Lei n. 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e dá outras providências;

III - Lei n. 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial;

IV - Lei n. 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação;

V - Norma ABNT NBR ISO/IEC 27003:2011, que dispõe sobre técnicas de segurança e diretrizes para implantação de um sistema de gestão da segurança da informação;

VI - Decreto n. 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo e dispõe sobre o Núcleo de Segurança e Credenciamento;

VII - Norma ABNT NBR ISO/IEC 27001:2013, que dispõe sobre os requisitos para sistemas de gestão da segurança da informação;

VIII - Norma ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da informação;

IX - Norma ABNT NBR ISO/IEC 27014:2013, que dispõe sobre a Governança de Segurança da Informação;

X - Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil;

XI - Norma ABNT NBR ISO/IEC 27004:2017, que dispõe sobre Sistemas de gestão da segurança da informação: monitoramento, medição, análise e avaliação;

XII - Resolução CNJ n. 211/2015, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

XIII - Resoluções CNJ ns. 91/2009, 121/210, 182/2013 e 185/2013;

XIV - Resolução TJMMG n. 175, de 5 de setembro de 2016, que dispõe sobre sistema de governança, no âmbito da Justiça Militar de Minas Gerais.

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 5° As ações relacionadas à Segurança da Informação, no âmbito da JMEMG, são norteadas pelos princípios delineados a seguir:

I - precedência: a segurança das pessoas tem precedência sobre qualquer ativo da JMEMG;

II - legalidade: todas as ações de segurança da informação devem seguir as legislações vigentes sobre o tema;

III - moralidade: é expressamente proibido o acesso, o uso, a guarda e o encaminhamento de material antiético, discriminatório, malicioso, obsceno ou ilegal;

IV - responsabilidade: os agentes públicos devem conhecer e respeitar as normas desta Política de Segurança da Informação, zelando pelo seu cumprimento;

V - irretratabilidade: não poderá haver negação da autoria de uma transação realizada com a utilização de certificado digital ou mediante *login* e senha;

VI - privacidade: informações que firam o respeito, a intimidade, a integridade e a honra dos cidadãos não podem ser divulgadas;

VII - publicidade: deve ser observado o zelo pela transparência das informações públicas;

VIII - acessibilidade: o acesso à informação deve ser garantido às pessoas portadoras de necessidades especiais;

IX - preservação da imagem: as ações de segurança devem garantir a proteção da reputação e da imagem institucional;

X - sustentabilidade: deve-se zelar pela economia, combatendo o desperdício;

XI - transparência: as informações não sigilosas e de amplo conhecimento devem ser disponibilizadas aos públicos interno e externo.

CAPÍTULO V
DAS DIRETRIZES GERAIS

Art. 6° A Política de Segurança da Informação (PSI) é desenvolvida para prevenir vulnerabilidades na Gestão Documental e de TIC, devendo ser de fácil compreensão e aplicação, tratando suas questões de forma objetiva, em normas pontuais, específicas e concisas.

Art. 7° Toda informação sob a responsabilidade da JMEMG deve ser classificada considerando seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento.

§ 1° A classificação da informação/documento deverá assegurar uma parametrização no nível adequado de proteção, que deve ser observado durante todo o seu ciclo de vida.

§ 2° O Tribunal viabilizará meios de proteção ao ativo de informação proporcionais ao seu grau de confidencialidade e de criticidade.

§ 3° No descarte de informação/documento institucional, devem ser observadas as políticas, as normas, os procedimentos internos, a classificação da informação possui, bem como a temporalidade prevista na legislação.

Art. 8º A publicidade das informações é preceito geral, e o sigilo é exceção.

Parágrafo único. O acesso às informações não públicas sob responsabilidade da Justiça Militar do Estado de Minas Gerais deve ser restrito aos usuários que tenham necessidade de conhecê-las.

Art. 9º O tratamento da informação e da documentação perpassa diretamente pela segurança física e patrimonial e deverá ter por objetivo a prevenção de danos e interferências nas instalações do TJMMG que possam causar prejuízos irreparáveis à informação.

Parágrafo único. Cabe ao Centro de Segurança Institucional (CESI) planejar, estabelecer, monitorar e revisar os procedimentos de acesso à edificação e suas condições quanto à prevenção de incêndio e pânico.

CAPÍTULO VI
DA GESTÃO DOS RISCOS

Art. 10. O serviço de Gestão e Tratamento de Riscos visa identificar os riscos reais, relevantes e prováveis, oriundos da inexecução parcial ou total desta política, e minimizar possíveis impactos associados aos ativos da informação, possibilitando a seleção e a priorização dos ativos a serem protegidos, bem

como a definição e implementação de controles para a identificação e o tratamento de possíveis falhas de segurança.

Parágrafo único. A gestão de riscos deverá ser implementada pelo Comitê de Governança e Gestão de Tecnologia da Informação e Comunicação (CGTIC) da Justiça Militar do Estado de Minas Gerais.

CAPÍTULO VII
DAS PENALIDADES

Art. 11. O descumprimento da Política de Segurança da Informação desta JMEMG acarretará, isolada ou cumulativamente, nos termos da legislação vigente, sanções administrativas, civis e penais.

CAPÍTULO VIII
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 12. Os agentes públicos da JMEMG devem reportar à Administração quaisquer incidentes que afetem a segurança do ativo de informação ou o descumprimento desta política.

Art. 13. As informações, os sistemas e os métodos gerados ou criados por empresas contratadas e/ou pelos usuários, no exercício de suas funções, são de propriedade da JMEMG.

Art. 14. Compete aos gestores da informação, seja de produção ou de custódia, adotar critérios de classificação e procedimentos de acesso, propondo regras específicas para uso da informação.

Art. 15. Compete à Gerência de Informática:

I - propor regulamentação da política de *backup* e restauração de arquivos e armazenamento;

II - propor regulamentação da política de certificação digital;

III - propor regulamentação da política de acesso aos recursos de TIC;

IV - propor regulamentação da política de videoaudiências;

V - propor regulamentação da política de acesso à internet, intranet e correio eletrônico;

VI - estabelecer procedimentos para descarte e baixa do acervo magnético e digital.

Art. 16. Compete à Auditoria Interna realizar, regularmente, auditorias ordinárias relacionadas à segurança da informação e encaminhar os relatórios produzidos ao CGTIC/TJMMG.

Art. 17. Compete à área de Recursos Humanos comunicar imediatamente à Gerência de Informática as movimentações, os afastamentos, os desligamentos de servidores, estagiários e terceirizados da JMEMG.

Art. 18. Compete à Comissão Permanente de Avaliação Documental (CPAD) da JMEMG:

I - propor regulamentação para proteção, reprodução, digitalização, manuseio, remoção, exposição, empréstimos, trânsito, guarda, conservação e restauração do acervo documental, museológico e bibliográfico.

II - propor regulamentação para classificação dos documentos e informações, quanto a seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento.

III - propor regulamentação de descarte e baixa de documentos.

CAPÍTULO IX
DISPOSIÇÕES FINAIS

Art. 19. A Política de Segurança da Informação deve ser revisada e atualizada a cada 2 (dois) anos, bem como divulgada para todos os agentes públicos da JMEMG.

Parágrafo único. A revisão a que se refere o *caput* deste artigo também poderá ocorrer a qualquer tempo, caso haja eventos ou fatos relevantes que a justifiquem.

Art. 20. Os contratos e os convênios firmados pela JMEMG devem conter cláusula exigindo a observância desta Resolução.

Art. 21. As disposições desta Resolução aplicam-se a todos que utilizam os recursos de tecnologia da informação no âmbito da JMEMG.

Art. 22. Os casos omissos serão resolvidos pelo Presidente do Tribunal.

Art. 23. Esta Resolução entra em vigor na data de sua publicação.

Assinado de forma digital por JAMES FERREIRA SANTOS:39176770672 (17/04/2018 ~ 16/04/2021)

Juiz **JAMES FERREIRA SANTOS**
Presidente