MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais
Reitoria

PORTARIA Nº 1966/IFMG, DE 16 DE DEZEMBRO DE 2024

O **REITOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS**, no uso das atribuições que lhe são conferidas pelo Estatuto da Instituição, republicado com alterações no Diário Oficial da União do dia 08/05/2018, Seção 1, Páginas 09 e 10, e pelo Decreto de 11 de setembro de 2023, publicado no DOU de 12 de setembro de 2023, Seção 2, Edição nº 174, página 01

Considerando a Lei nº 13.709, 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. (LGPD).

Considerando a Lei nº 12.965, de 23 de abril de 2014, Marco Civil da Internet que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Considerando o Decreto n° 11.856, de 26 de dezembro de 2023 que institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.

Considerando o Decreto nº 10.748, de 16 de julho de 2021 que institui a Rede Federal de Gestão de Incidentes Cibernéticos.

Considerando a Portaria SGD/MGI nº 852, de 28 de março de 2023 que Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI.

e o que consta no Processo nº **23208.003392/2024-13**,

RESOLVE

Atualizar a Política de Segurança da Informação (POSIN) do IFMG.

CAPÍTULO I

DA FINALIDADE

Art. 1º A Política de Segurança da Informação (POSIN), do Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais (IFMG), é uma declaração formal da Instituição acerca de seu compromisso com a proteção dos ativos de informação de sua propriedade e/ou sob sua guarda.

Art. 2º Esta POSIN estabelece diretrizes e responsabilidades adequadas para o manuseio, tratamento, controle e proteção dos ativos de informação pertinentes ao IFMG, em conformidade com a legislação vigente, com os valores éticos e com as melhores práticas. Visa garantir a confidencialidade, integridade e disponibilidade das informações, assegurando o seu uso adequado e a mitigação de riscos à segurança da informação.

Art. 3º Esta POSIN também irá nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação, por conseguinte, serão parte integrante desta política.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 4º Os conceitos e definições abordadas na Política de Segurança da Informação do IFMG, são tratados e atualizados no Glossário de Segurança da Informação, instituído pelo Gabinete de Segurança Institucional da Presidência da República. Disponível em: https://www.gov.br/gsi/pt-br/ssic/glossario-de-seguranca-da-informacao-1.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 5º As ações de segurança da informação do IFMG são guiadas pelos preceitos constitucionais e administrativos que norteiam a Administração Pública Federal, bem como pelos seguintes princípios:

I. Confidencialidade: garante que a informação seja acessada somente

pelas pessoas ou processos que tenham autorização para tal;

II. Integridade: garante a não violação das informações, com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital;

III. Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;

IV. Autenticidade: princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;

V. Criticidade: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;

VI. Celeridade: às ações de segurança da informação devem oferecer respostas rápidas a incidentes e falhas de segurança;

VII. Responsabilidade: as responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas. Todos os servidores do IFMG são responsáveis pelo tratamento da informação e pelo cumprimento das Normas de Segurança da Informação advindas desta Política;

VIII. Ciência: todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço devem ter ciência das políticas, normas, procedimentos e instruções que permitam a execução de suas atribuições sem comprometer a segurança;

IX. Ética: todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, prestadores de serviço e usuários do sistema de Informação do IFMG devem ser respeitados;

X. Legalidade: além de observar os interesses do IFMG, as ações de Segurança da Informação levarão em consideração leis, normas, políticas organizacionais, administrativas, técnicas e operacionais, padrões, procedimentos aplicáveis e contratos com terceiros, dando atenção à propriedade da informação e aos direitos de uso;

XI. Proporcionalidade: o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações no âmbito do IFMG serão adequados ao entendimento administrativo e ao nível de risco do ativo a proteger;

XII. Conscientização: educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação; e

XIII. Transparência: observância da publicidade como preceito geral e do sigilo como exceção.

Art. 6º. Estes princípios constituem os pilares centrais da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito do IFMG;

CAPÍTULO IV

DO ESCOPO

Art. 7º. Esta POSIN abrange todas as unidades do IFMG e refere-se aos aspectos estratégicos, estruturais e organizacionais, preparando a base para elaboração dos demais documentos normativos que farão parte de sua área de ação;

Art. 8º. Esta Política se aplica a todos os ativos de informação do IFMG, incluindo dados, sistemas, aplicativos, dispositivos e redes. A Política se aplica a todos os colaboradores, servidores, contratados, parceiros e terceiros que acessam ou processam as informações do IFMG.

Art. 9. Esta política se aplica em todas as instalações físicas administradas ou utilizadas pelo IFMG.

CAPÍTULO V

DAS DIRETRIZES GERAIS

Art. 10. As ações de segurança da informação devem:

I. considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a missão do IFMG;

II. suportar a tomada de decisões dos gestores, bem como coordenar a utilização de recursos de forma eficiente, possibilitando alcançar os objetivos estratégicos do Plano de Desenvolvimento Institucional (PDI) do IFMG;

III. ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades do IFMG;

IV. ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade dos ativos de informação;

V. considerar, também, as normas da Associação Brasileira de Normas Técnicas (ABNT) relacionadas à Segurança da Informação; e

VI. visar à prevenção da ocorrência de incidentes.

CAPÍTULO VI

DAS DIRETRIZES ESPECÍFICAS

Art. 11. Para cada uma das diretrizes constantes das seções deste capítulo deve ser observada a pertinência de elaboração de políticas, normas, procedimentos e instruções que disciplinam ou facilitem o seu entendimento.

Parágrafo único. Poderão ser constituídos grupos de trabalho para elaboração de políticas, normas, procedimentos e instruções a fim de auxiliar o Comitê de Segurança da Informação na construção das documentações necessárias, assim como atender situações específicas de cada unidade.

Seção I

Do Uso de Recursos Computacionais e Comunicações

Art. 12. Todos os recursos computacionais e de comunicação disponibilizados pelo IFMG aos agentes públicos ou à comunidade acadêmica, devem ser utilizados com responsabilidade, respeitando-se os princípios da ética, da razoabilidade e da legalidade.

Seção II

Segurança Física e do Ambiente

Art. 13. Processo referente à proteção de todos os ativos físicos do IFMG, englobando instalações físicas, internas e externas, em todas as localidades em que a instituição se fizer presente.

Art. 14. As instalações de rede e equipamentos de TI, deverão possuir mecanismos adequados de controle de acesso físico, que possibilitem a identificação das pessoas e/ou usuários que as utilizem.

Art. 15. A alta administração do IFMG, irá dimensionar e aplicar os investimentos necessários em medidas de segurança, segundo o valor do ativo de informação que está sendo protegido e de acordo com a identificação de riscos de potenciais prejuízos ao negócio, à atividade fim e aos objetivos institucionais.

Seção III

Gestão de Incidentes em Segurança da Informação

Art. 16. Os incidentes de segurança deverão ser identificados, monitorados, comunicados e devidamente tratados de forma a impedir a interrupção das atividades e não afetar o alcance dos objetivos estratégicos do IFMG.

Art. 17. Os agentes públicos e as partes externas que usam os sistemas e serviços de informação do IFMG deverão ser instruídos a notificar e registrar quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços.

Art. 18. Os eventos de segurança da informação deverão ser avaliados e decididos se a sua classificação será de incidente de segurança da informação pela Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos do IFMG.

Seção IV

Gestão de Ativos

Art. 19. Os ativos devem ser devidamente inventariados e protegidos, utilizando-os estritamente dentro do seu propósito.

Art. 20. Todas as informações e ativos associados a recursos de processamento da informação serão controladas pela unidade que dispõe do serviço ou recurso;

Art. 21. A eliminação de informações deve seguir a norma de procedimentos internos e classificação, e a temporalidade prevista na legislação.

Seção V

Da Auditoria e Conformidade

Art. 22. O uso dos recursos computacionais e de comunicação, acessos, tráfego de dados, operações e intervenções que envolvam tais recursos, sejam de

forma automática ou por monitoramento dos usuários são passíveis de monitoramento e auditoria sempre que se fizer necessário.

Art. 23. Os procedimentos de auditoria e de monitoramento de uso dos recursos serão realizados periodicamente pela Diretoria de Tecnologia da Informação (DTI) e/ou áreas responsáveis pela Tecnologia da Informação nos campi com o objetivo de observar o cumprimento desta política pelos usuários e com vistas à gestão de desempenho e segurança.

Art. 24. Havendo evidência de qualquer atividade que possa comprometer o desempenho e/ou a segurança dos recursos de tecnologia da informação ou que infrinja a Política de Segurança da Informação, será permitido à DTI ou a área responsável pela Tecnologia da Informação no campus, auditar e monitorar atividades de usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso da fonte causadora do problema, remover dados, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário, à direção geral do campus, à Reitoria do IFMG e/ou à Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos do IFMG a depender da gravidade.

Seção VII

Do Tratamento e Uso de Ativos de Informação

Art. 25. Toda informação de propriedade e/ou sob a guarda do IFMG deve ser tratada adequadamente, com o objetivo de assegurar a sua confidencialidade, integridade e disponibilidade, independente do meio de armazenamento, processamento ou transmissão utilizado.

Art. 26. O tratamento das informações pessoais deve considerar o respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais, conforme o disposto na Lei no 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), na Lei no 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), normativos internos e legislações aplicáveis.

Art. 27. As normas para as operações de armazenamento, backup, divulgação, reprodução, transporte, recuperação e destruição das informações serão definidas de acordo com a classificação destas, através de normas e procedimentos específicos e complementares à esta Política, sem prejuízo de outros cuidados que vierem a ser especificados pelo gestor;

Art. 28. O agente público é responsável pela adoção de comportamentos seguros, baseando-se nas recomendações feitas pelo Comitê de Segurança da Informação.

Art. 29. O acesso, pelos agentes públicos, às informações custodiadas ou de propriedade do IFMG deverá ser restrito ao necessário para desempenho de suas funções, além de obedecer às diretrizes e aos procedimentos dispostos nas normas e na legislação vigente.

Seção IX

Da Gestão de Riscos

Art. 30. É de responsabilidade da Comissão Permanente de Gestão de Risco instituída pela Política de Governança, Gestão de Riscos, Controle Interno e Integridade do IFMG, adotar processo contínuo de gestão de riscos, assim como garantir a sua aplicação na gestão de segurança da informação e comunicações.

Art. 31. A adoção do processo contínuo de gestão de riscos deve incluir ações de identificação, classificação, análise qualitativa e quantitativa, registro e documentação, visando à mitigação e à eliminação de riscos.

Seção XI

Da Sensibilização, Conscientização e Capacitação

Art. 32. É de responsabilidade do IFMG o desenvolvimento de processo contínuo de divulgação, sensibilização, conscientização e capacitação dos agentes públicos sobre os cuidados e deveres relacionados à segurança da informação e comunicações, observando as orientações do Comitê de Segurança da Informação.

CAPÍTULO VII

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 33. A estrutura de Gestão de Segurança da Informação é composta por:

I. Alta Administração;

II. Comitê de Segurança da Informação;

III. Gestor de Segurança da Informação;

IV. Diretor de Tecnologia da Informação;

V. Encarregado pelo Tratamento de Dados Pessoais;

VI. Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos; e

VII. Usuários de Informação.

Art. 34. Compete à alta administração do IFMG:

I. fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação do IFMG, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados; e

II. formalizar e aprovar a Política de Segurança da Informação do IFMG, bem como suas alterações e atualizações.

Art. 35. Compete ao Comitê de Segurança da Informação do IFMG:

I. assessorar na implementação das ações de segurança da informação;

II. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III. participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV. propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

V. deliberar sobre normas internas de segurança da informação;

VI. avaliar as ações propostas pelo gestor de segurança da informação.

Art. 36. Compete ao Gestor de Segurança da Informação e Comunicações do IFMG:

I. coordenar o Comitê de Segurança da Informação;

II. coordenar a elaboração da Política de Segurança da Informação - PSI e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;

III. assessorar a Alta Administração na implementação da Política de Segurança da Informação;

IV. estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V. promover a divulgação da política e das normas internas de segurança da informação a todos os servidores, usuários e prestadores de serviços que trabalham no IFMG;

VI. incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;

VII. propor recursos necessários às ações de segurança da informação;

VIII. acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

IX. verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

XI. manter contato direto com o Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação;

Parágrafo único. O Gestor de Segurança da Informação do IFMG será designado pelo reitor em portaria, de acordo com a legislação vigente.

Art. 37. Compete ao Diretor de Tecnologia da Informação, dentre outras

atribuições dispostas na legislação vigente, em especial ao disposto na Portaria SGD/ME nº 778, de 4 de abril de 2019, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.

Art. 38. Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

Art. 39. Compete à Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos:

I. facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos no IFMG;

II. monitorar as redes computacionais;

III. detectar e analisar ataques e intrusões;

IV. tratar incidentes de segurança da informação;

V. identificar vulnerabilidades e artefatos maliciosos;

VI. recuperar sistemas de informação;

VII. promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação;

VIII. orientar as equipes de TIC do IFMG na verificação da conformidade dos controles estabelecidos de segurança da informação;

IX. implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança;

X. apoiar, incentivar e contribuir para a capacitação no tratamento de incidentes de segurança;

XI. participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

XII. propor políticas ao Comitê de Segurança da Informação para gestão de Incidentes em Segurança da Informação;

XII. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI. manter contato direto com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Parágrafo único. A composição, estrutura, recursos e funcionamento da Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos serão definidos em portaria emitida pelo reitor do IFMG, de acordo com a legislação vigente.

Art. 40. Compete aos Usuários de Informação conhecer, cumprir e fazer cumprir esta Política e às demais normas específicas de segurança da informação do IFMG.

Parágrafo único. Todos os Usuários de Informação são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

CAPÍTULO VIII

DA ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO

Art. 41. A estrutura normativa da Segurança da Informação do IFMG é composta por um conjunto de documentos, relacionados a seguir:

I. Política de Segurança da Informação (POSIN): constituída por este

documento, define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação, e será detalhada em um conjunto de Normas específicas;

II. Normas de Segurança da Informação (Normas): estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem observados em diversas instâncias em que a informação seja tratada. A cada Norma será associado um conjunto de Procedimentos destinados a orientar sua implementação. A elaboração das Normas seguirá as orientações contidas no documento "Atividade de Normatização" do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República;

III. Procedimentos de Segurança da Informação (Procedimentos): instrumentalizam o disposto nas Normas, permitindo sua direta aplicação nas atividades do IFMG, podendo cada gestor da informação gerá-los, respeitando as diretrizes desta POSIN. Cada procedimento poderá ainda ser detalhado em instruções. Estes procedimentos e instruções serão de uso interno, não sendo obrigatória sua publicação ao público externo, devendo ser disponibilizado aos agentes internos do IFMG que terão impacto direto ou indireto com as medidas presentes nestes documentos.

IV. Termos de Uso: Documento que traz em seu texto as condições e regras para que um usuário de um sistema ou ativo possa utilizar o que é oferecido após o aceite;

V. Termos de Responsabilidade: documento utilizado para formalizar uma obrigação atribuída a alguém. Quando alguém assume uma determinada responsabilidade, como a guarda de um bem ou acesso privilegiado a algum ativo protegido por esta POSIN. Este ato poderá ser devidamente documentado por meio de um termo assinado pelo responsabilizado;

VI. Política de Privacidade: práticas e processos adotados pelo IFMG para tornar transparente sua relação com o usuário, informando todos os direitos, garantias, formas de uso, dados recolhidos, processamento e descarte das informações pessoais.

Art. 42. Os aspectos de segurança física, lógica e de pessoal serão tratados em documentos independentes, com a finalidade de complementar normas e recomendações de segurança no trato das informações.

Art. 43. Toda e qualquer norma, procedimento e instrução específica que trate da segurança da informação do IFMG deve estar de acordo com esta política.

Art. 44. Se tornam complementares a esta política toda e qualquer norma, procedimento e instrução específica que trate da segurança da informação do IFMG.

CAPÍTULO IX

DAS PENALIDADES

Art. 45. A não observância desta Política ou de seus documentos complementares, bem como a quebra de controles de segurança da informação e comunicação, poderá acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

§1º As normas e procedimentos poderão detalhar sanções aplicáveis a incidentes previamente definidos, inclusive indicando a participação em curso de capacitação.

§2º Demais sanções deverão ser aplicadas pelas instâncias competentes, internas ou externas.

§3º Casos omissos em normas e procedimentos ou nas documentações complementares serão analisados e encaminhados pelo Comitê de Segurança da Informação ou outro comitê imediatamente superior da instituição.

CAPÍTULO X

DA POLÍTICA DE ATUALIZAÇÃO

Art. 46. Esta Política, bem como o conjunto de instrumentos normativos gerados a partir dela, serão revisados sempre que se fizer necessário, não excedendo o período máximo de 3 (três) anos.

CAPÍTULO XI

DAS DISPOSIÇÕES FINAIS

Art. 47. Todas as documentações já existentes atingidas por esta POSIN

deverão obrigatoriamente ser readequadas para atender igualmente todos os requisitos contidos nesta Política.

Art. 48. Esta POSIN pode ser regulamentada através de Normativa Interna do Campus/Reitoria, em conjunto com o Comitê de Segurança da Informação.

Art. 49. Revogam-se as disposições em contrário.

Art. 50. A presente política entra em vigor a partir da data de sua publicação.

Publicação: Transparência Ativa em 16 de dezembro de 2024

Documento assinado eletronicamente sob fundamentação, por:
RAFAEL BASTOS TEIXEIRA | Reitor

Data da Assinatura:
16 de dezembro de 2024 as 18:44 (America/Sao_Paulo)

Tipo de Documento:
Portaria

Autenticidade