SERVIÇO PÚBLICO FEDERAL
MEC - INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TRIÂNGULO MINEIRO

RESOLUÇÃO IFTM/CONSUP Nº 447 DE 02 DE DEZEMBRO DE 2024

Dispõe sobre a Política de Segurança da Informação – POSIN - no âmbito do IFTM.

O CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TRIÂNGULO MINEIRO, no uso das atribuições que lhe confere a Lei nº 11.892/2008 e as Portarias nº 572 de 07/03/2024, publicada no DOU de 11/03/2024, Portaria nº 923 de 10/05/2024, publicada no DOU de 14/05/2024 e Portaria nº 2.219 de 22/10/2024, publicada no DOU 25/10/2024, tendo em vista a 16ª reunião ordinária do Conselho Superior do IFTM e o processo nº 23199.016061/2024-08,

RESOLVE:

Art. 1º Fica aprovada a Política de Segurança da Informação – POSIN do Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro (IFTM), conforme anexo.

Art. 2º Fica revogada a Resolução nº 27/2013, de 27 de agosto de 2013.

Art. 3º Esta resolução entra em vigor na data de sua publicação.

Uberaba, 202 de dezembro de 2024.

gov.br
Documento assinado digitalmente
MARCELO PONCIANO DA SILVA
Data: 02/12/2024 12:51:12-0300
Verifique em https://validar.iti.gov.br

Marcelo Ponciano da Silva

Presidente do Conselho Superior do IFTM

INSTITUTO FEDERAL
Triângulo Mineiro

POSIN

Política de Segurança da Informação

Uberaba, 2024

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TRIÂNGULO MINEIRO

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor
15/10/2024	1.0	Política de Segurança da Informação do IFTM	Gestor de Segurança da Informação

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TRIÂNGULO MINEIRO

SUMÁRIO

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TRIÂNGULO MINEIRO

CAPÍTULO I
DO PROPÓSITO

Art. 1º A Política de Segurança da Informação (POSIN) do Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro (IFTM) é uma declaração formal da Instituição acerca do seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda.

Art. 2º O seu objetivo é estabelecer os princípios, diretrizes, responsabilidades e práticas para o manuseio, tratamento, controle e proteção das informações pertinentes ao IFTM. A Política visa garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas e/ou custodiadas pelo IFTM, assegurando o seu uso adequado e a mitigação de riscos à segurança da informação, bem como o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras normas vigentes.

CAPÍTULO II
DO ESCOPO

Art. 3º Esta Política se aplica a todos os ativos de informação do IFTM, incluindo dados, sistemas, aplicativos, dispositivos e redes.

Art. 4º Esta política se aplica em todas as instalações físicas administradas ou utilizadas pelo IFTM incluindo polos de Educação a Distância.

Art. 5º Esta Política, suas normas e procedimentos deverão ser observados por todos os servidores, alunos, colaboradores, consultores externos, estagiários, bolsistas, prestadores de serviço e a quem, de alguma forma, tenham acesso a dados e informações no âmbito do IFTM, por meio da assinatura de Termo de Responsabilidade, para acessar os ativos de informação sob responsabilidade do IFTM.

CAPÍTULO III
DAS DISPOSIÇÕES GERAIS

Art. 6º. São objetivos da Política de Segurança da Informação:

I. estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;
II. estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

III. estabelecer competências e responsabilidades quanto à segurança da informação;
IV. nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;
V. promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional do IFTM.

CAPÍTULO IV
DOS CONCEITOS E DEFINIÇÕES

Art. 7º Para efeitos desta política e suas regulamentações, aplicam-se os termos do Glossário de Segurança da Informação, instituído pelo Gabinete de Segurança Institucional da Presidência da República, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021 e do Art. 5º da LEI nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados (LGPD).

CAPÍTULO V
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 8º A implementação, o controle e a gestão desta política são de responsabilidade da seguinte infraestrutura de gerenciamento:

I. Conselho Superior (CONSUP);
II. Alta administração do IFTM, representada pelo Colégio de Dirigentes (CODIR);
III. Diretoria de Tecnologia da Informação e Comunicação;
IV. Coordenação de Tecnologia da Informação e Comunicação dos campi;
V. Gestor de Segurança da Informação;
VI. Comitê Gestor de Segurança da Informação;
VII. Encarregado do tratamento de dados pessoais;
VIII. Responsável pela Unidade de Controle Interno;
IX. Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos; e
X. Usuários da Informação.

Art. 9º Compete ao CONSUP aprovar a Política de Segurança da Informação do IFTM, bem como suas alterações e atualizações;

Art. 10 Compete à alta administração do IFTM fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação do IFTM, bem como o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados.

Art. 11. Compete à Diretoria de Tecnologia da Informação e Comunicação:

I. zelar pela segurança da informação no âmbito do IFTM quando estas informações estiverem sob custódia dos recursos de tecnologia da informação;

II. 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. 12 Compete à Coordenação de Tecnologia da Informação e Comunicação dos *campi* zelar pela segurança da informação no âmbito do *campus* quando estas informações estiverem sob custódia dos recursos de tecnologia da informação;

Art. 13 Compete ao Gestor de Segurança da Informação:

I. coordenar a elaboração e revisão da POSIN, suas normas complementares, observadas a legislação vigente e as melhores práticas sobre o tema;
II. assessorar a alta administração na implementação da POSIN;
III. estimular ações de capacitação de recursos humanos em temas relacionados à segurança da informação;
IV. promover a cultura de Segurança da Informação, através da ampla divulgação desta Política, suas normas e procedimentos;
V. incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;
VI. propor recursos necessários às ações de segurança da informação;
VII. acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;
VIII. verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;
IX. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;
X. manter contato com as entidades do Governo Federal relacionadas à Segurança da Informação;

Art. 14. Compete ao Comitê Gestor de Segurança da Informação:

I. assessorar a 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 e revisão periódica 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; e
V. deliberar sobre normas internas de segurança da informação;
VI. avaliar as ações propostas apresentadas pelo gestor de segurança da informação.

Parágrafo Único: A composição e diretrizes gerais do Comitê Gestor de Segurança da Informação estão definidos no Regimento Geral do IFTM.

Art. 15. Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na 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. 16. Compete ao Responsável pela Unidade de Controle Interno, dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

Art. 17 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 IFTM;
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.

Parágrafo único. A composição, estrutura, recursos e funcionamento da Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos serão definidos em normativo específico.

Art. 18 Compete aos Usuários de informação:

I. tratar os ativos da informação como patrimônio do IFTM;
II. conhecer a POSIN e seguir suas normas e procedimentos, adotando comportamento seguro a fim de promover a proteção das informações do IFTM;
III. propor alterações em normas e procedimentos a fim de aumentar o nível de segurança da informação. As propostas devem ser encaminhadas ao Comitê Gestor de Segurança da Informação.
IV. utilizar os ativos da informação, os sistemas e produtos computacionais de propriedade ou direito de uso do IFTM exclusivamente para interesse do serviço;
V. preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las.

CAPÍTULO VI
DOS PRINCÍPIOS

Art. 19 As ações de segurança da informação do IFTM são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, bem como pelos seguintes princípios:

I. Alinhamento estratégico: garantir que esta Política de Segurança da Informação esteja alinhada com o planejamento estratégico do IFTM, assim como demais normas específicas de segurança da informação da Administração Pública Federal;
II. Autenticidade: assegurar a responsabilidade do autor da criação ou divulgação de uma dada informação;
III. Ciência: todos os servidores, alunos, colaboradores, consultores externos, estagiários, bolsistas, prestadores de serviço, e quem, de alguma forma, tenham acesso a dados e informações no âmbito do IFTM, devem ter ciência das normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança;
IV. Confidencialidade: somente pessoas devidamente autorizadas pelo gestor da segurança da informação, ou pelas equipes de TI mediante autorização, devem ter acesso à informação não pública;
V. Conformidade: garantir a conformidade das normas e das ações de segurança da informação com a legislação e regulamentos aplicáveis;
VI. Continuidade do negócio: permitir a continuidade dos processos e serviços essenciais para o funcionamento do IFTM;
VII. Criticidade: definir a importância da informação para a continuidade da atividade-fim do IFTM;
VIII. Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;
IX. Economicidade: da proteção dos ativos de informação;
X. Educação e Comunicação: tratar a educação e a comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.
XI. Ética: todos os direitos e interesses legítimos de servidores, alunos, colaboradores, consultores externos, estagiários, bolsistas, prestadores de serviço e usuários do sistema de informação do IFTM devem ser respeitados;
XII. Integridade: qualquer tratamento de informações, no âmbito do IFTM, deve ser realizado apenas após autorização, assegurando a consistência, precisão e confiabilidade dos dados;
XIII. Publicidade: observância da publicidade como preceito geral e do sigilo como exceção;
XIV. Legalidade: além de observar os interesses do IFTM, 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 direitos de uso;
XV. Proporcionalidade: o nível, a complexidade e os custos das ações de segurança da informação no IFTM serão adequados ao entendimento administrativo e ao valor do ativo a proteger;

XVI. Respeitabilidade: respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

XVII. 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 IFTM são responsáveis pelo tratamento da informação e pelo cumprimento das normas de segurança da informação advindas desta política.

CAPÍTULO VII
DAS DIRETRIZES GERAIS

Art. 20 Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito do IFTM e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 21 As normas, procedimentos, manuais e metodologias de segurança da informação do IFTM devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 22 As ações de segurança da informação devem:

I. considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade do IFTM;
II. ser tratadas de forma integrada, respeitando as especificidades e a autonomia dos campi do IFTM
III. ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;
IV. visar à prevenção da ocorrência de incidentes.

Art. 23 É dever de todos zelar pela Segurança da Informação e Comunicações.

Art. 24 O IFTM, como usuário dos serviços providos pela Rede Nacional de Pesquisa (RNP) é, por princípio, signatário de suas Políticas e Normas de Segurança.

Art. 25 Usuários internos e externos devem observar que:

I. o acesso à informação será regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IFTM é considerada seu patrimônio e deve ser protegida;
II. os recursos disponibilizados pelo IFTM, de sua propriedade, são fornecidos com o propósito único de garantir o desempenho das suas atividades;
III. as normas para as operações de armazenamento, divulgação, reprodução, transporte, recuperação e destruição da informação serão definidas de acordo com a classificação desta, sem prejuízo de outros cuidados que vierem a ser especificados pelo gestor.

Art. 26 O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos ao IFTM.

Art. 27 Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada no IFTM compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

Parágrafo único. As informações citadas no caput, que tramitem pelo ambiente computacional do IFTM, são passíveis de monitoramento e auditoria pelo IFTM, respeitados os limites legais.

Art. 28 Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Parágrafo único. É condição para acesso aos recursos de tecnologia da informação do IFTM a assinatura, preferencialmente eletrônica, de Termo de Responsabilidade indicando a ciência aos termos desta Política, as responsabilidades e os compromissos em decorrência deste acesso, bem como as penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação do IFTM.

Art. 29 A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação do IFTM devem ser divulgadas amplamente a todos os Usuários de Informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

CAPÍTULO VIII
DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 30. A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:

I. tratamento da informação;
II. segurança física e do ambiente;
III. gestão de incidentes em segurança da informação;
IV. gestão de ativos;
V. gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;
VI. controles de acesso;
VII. gestão de riscos;
VIII. gestão de continuidade;
IX. auditoria e conformidade;

Parágrafo Único: O Comitê de Segurança da Informação poderá definir outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.

Seção I
Tratamento da Informação

Art. 31 Toda informação de propriedade e/ou sob guarda do IFTM deve ser tratada de forma adequada para viabilizar e assegurar a sua disponibilidade, integridade, confidencialidade e autenticidade da informação. Ademais, deve ser observada a conformidade com as diretrizes dispostas na LGPD e demais normativos e orientações emitidas pela ANPD;

Art. 32 É expressamente proibido o acesso, a guarda ou o encaminhamento de material discriminatório, malicioso, não ético, obsceno ou ilegal por intermédio de quaisquer meios e recursos de tecnologia da informação disponibilizados pelo IFTM.

Art. 33 Toda informação tratada por usuários, no exercício de suas atividades laborais, é considerada bem e propriedade do IFTM e deve ser protegida segundo as diretrizes descritas nesta Política, em suas normas e procedimentos.

Art. 34 No contexto de atividades remotas, todos os usuários, internos ou externos, do IFTM devem observar as mesmas diretrizes de tratamento de informações estabelecidas nos artigos anteriores desta Política.

I. É fundamental que os princípios de disponibilidade, integridade, confidencialidade e autenticidade da informação sejam rigorosamente mantidos ao manipular dados fora das instalações físicas da instituição.
II. Os usuários são responsáveis por adotar medidas de segurança adequadas, como a utilização de redes seguras, dispositivos protegidos, a conformidade com a política de segurança da informação do IFTM e as orientações apresentadas pelo Comitê Gestor de Segurança da Informação do IFTM e Diretoria de Tecnologia da Informação e Comunicação.
III. A proteção contra acesso não autorizado, a prevenção de vazamento de dados sensíveis e o cumprimento da legislação aplicável continuam sendo essenciais no ambiente remoto.
IV. O acesso a plataformas digitais como o VirtualIF, SIAFI, SIAPE, SIADS e outras que subsidiam as atividades administrativas do IFTM, devem respeitar as orientações do Comitê Gestor de Segurança da Informação.

Seção II
Segurança Física e do Ambiente

Art. 35 Devem ser definidos controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos do IFTM e que garantam a proteção dos recursos de forma que apenas as pessoas autorizadas tenham acesso, restringindo a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança.

Seção III
Gestão de Incidentes em Segurança da Informação

Art. 36 A gestão de incidentes em segurança da informação no âmbito do IFTM será tratada pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) do IFTM.
Art. 37 Todos os usuários dos sistemas e serviços de informação do IFTM devem notificar e registrar quaisquer fragilidades de segurança da informação observada ou suspeita nos sistemas e/ou serviços do IFTM para dtic@iftm.edu.br.
Art. 38 Todos os usuários do IFTM deverão comunicar incidentes em relação a dados pessoais para lgpd@iftm.edu.br.

Seção IV
Gestão de Ativos

Art. 39 A gestão de ativos será tratada em normativo próprio e deverá abordar aspectos relacionados à proteção dos ativos, sua classificação de acordo com a criticidade do ativo para a organização; a manutenção de inventário atualizado de ativos da organização, contendo o tipo de ativo, sua localização, seu proprietário ou custodiante e seu status de segurança; uso aceitável de ativos, vedado o uso para fins particulares de seu responsável; o mapeamento de vulnerabilidades, ameaças e suas respectivas interdependências; o monitoramento de ativos, de acordo com os princípios legais de segurança da informação e privacidade; a investigação de sua operação e uso quando houver indícios de quebra de segurança e/ou privacidade;

Seção V
Gestão do Uso dos Recursos Operacionais e de Comunicações

Art. 40 O uso de recursos operacionais e de comunicação deve seguir procedimentos estabelecidos pelas áreas competentes em conformidade com a POSIN e observando, no mínimo, o seguinte:

I. o correio eletrônico institucional é uma forma de comunicação oficial e deve ser utilizado segundo as disposições da Instrução Normativa que trata do tema;
II. as contas de parcerias institucionais com outras organizações, como espaço de armazenamento e aplicativos disponibilizados pelas empresas Microsoft e Google, devem ser utilizadas exclusivamente no desempenho das atividades funcionais;
III. o acesso à Internet, provido pelo IFTM, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto;
IV. o uso de dispositivos móveis deve ser controlado com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário;
V. a implementação ou contratação de computação em nuvem deve ser precedida de procedimentos de conformidade com a legislação vigente.

Seção VI

Controle de Acesso

Art. 41 A gestão do controle de acesso aos ativos do IFTM será tratada em normativo próprio.

Seção VII
Gestão de Riscos

Art. 42 A Gestão de Riscos de Tecnologia da Informação será tratada em normativo próprio tendo como promissa de que os riscos devem ser monitorados e analisados periodicamente, a fim de verificar mudanças nos critérios de avaliação e aceitação dos riscos, no ambiente, nos ativos da informação e em fatores de risco, como ameaça, vulnerabilidade, probabilidade e impacto.

Seção VIII
Gestão de Continuidade

Art. 43 A gestão de continuidade será tratada em normativo próprio visando reduzir a possibilidade de interrupção causada por desastres ou falhas graves nos recursos que suportam as operações críticas do Instituto.

Seção IX
Auditoria e Conformidade

Art. 44 Deverá ser levantado regularmente os aspectos legais de segurança aos quais as atividades do IFTM estão submetidas, de forma a evitar ações penais decorrentes da não observância de tais aspectos por desconhecimento ou omissão.
Art. 45 O IFTM deverá realizar periodicamente auditorias internas de sua segurança da informação para assegurar que ela esteja em conformidade com esta Política e com outros requisitos de segurança da informação aplicáveis.
Art. 46 Todas as ações, realizadas pelo IFTM, que envolvem a segurança da informação devem estar em conformidade com as leis e regulamentos aplicáveis à esta temática.
Art. 47 As atividades, produtos e serviços desenvolvidos no IFTM devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes.

Seção X
Sensibilização, Conscientização e Capacitação

Art. 48 A Política e as Normas de Segurança da Informação devem ser divulgadas a todos os servidores do IFTM, e dispostas de maneira que o seu conteúdo possa ser consultado a qualquer momento.

Art. 49. Os *campi* e reitoria do IFTM devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.

Art. 50 As áreas atingidas por esta POSIN são imediatamente responsáveis pela elaboração e proposição de normas, procedimentos e atividades necessárias ao cumprimento em conformidade com o Comitê.

I. As áreas deverão submeter suas propostas de normas ao "Comitê Gestor de Segurança da Informação" para análise, discussão e aprovação no âmbito do Comitê.
II. Após aprovação, estas normas e procedimentos serão divulgados aos interessados pela área responsável por sua proposição e manutenção.

CAPÍTULO IX
DAS VEDAÇÕES

Art. 51. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pelo IFTM para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.
Art. 52 São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pelo IFTM.
Art. 53 É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.
Art. 54 É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

CAPÍTULO X
DAS PENALIDADES

Art. 55 O descumprimento ou violação de um ou mais itens desta política poderá resultar na aplicação de sanções administrativas, penais ou civis, bem como a suspensão dos direitos de acesso.

Art. 56 A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TRIÂNGULO MINEIRO

CAPÍTULO XI
DA POLÍTICA DE ATUALIZAÇÃO

Art. 57 A POSIN e todos os instrumentos normativos gerados a partir dela devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 4 (quatro) anos.
Art. 58 A presente Política passa a vigorar a partir da data de sua publicação.

CAPÍTULO XII
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 59 A POSIN foi elaborada de acordo com as seguintes referências e sua aplicação deve considerar as alterações posteriores:

I. Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal;
II. Lei nº 7.232, de 29 de outubro de 1984 – Dispõe sobre a Política Nacional de Informática, e dá outras providências;
III. Lei nº 8.027, de 12 de abril de 1990 – Dispõe sobre as normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências;
IV. Lei nº 8.112, de 11 de dezembro de 1990 - Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;
V. Lei nº 8.159 de 8 de janeiro de 1991 – Dispões sobre a política nacional de arquivos públicos e privados e dá outras providências;
VI. Lei nº 8.429 de 2 de junho de 1992 - Dispõe sobre as sanções aplicáveis em virtude da prática de atos de improbidade administrativa, de que trata o § 4º do art. 37 da Constituição Federal; e dá outras providências;
VII. Decreto 1.171, de 24 de junho de 1994 –Aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;
VIII. Constituição Federal de 1988 reformada em 2008;
IX. Lei nº 9.983, de 14 de julho de 2000 - Altera o Decreto Lei nº 2848, de 7 de setembro de 1940 – Código Penal e dá outras providências;
X. Decreto nº 6.029, de 1º de fevereiro de 2007 – Institui Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências;
XI. Decreto Nº 7.579, de 11 de outubro de 2011 - Dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal;
XII. Lei 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;

XIII. Decreto nº 7.724, de 16 de maio de 2012 - Regulamenta a Lei nº12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2ºdo art. 216 da Constituição;

XIV. Decreto nº 7.845, de 14 de novembro de 2012 - 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;

XV. Decreto nº 8.539, de 8 de outubro de 2015 – Dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;

XVI. Lei nº 13.105, de 16 de março de 2015 – Código de Processo Civil;

XVII. Decreto nº 9.637, de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

XVIII. Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

XIX. Decreto nº 10.148, de 2 de dezembro de 2019 - Institui a Comissão de Coordenação do Sistema de Gestão de Documentos e Arquivos da administração pública federal, dispõe sobre a Comissão Permanente de Avaliação de Documentos e dá outras providências;

XX. Portaria GSI/PR nº 93, DE 18 de outubro de 2021 – Aprova o Glossário de Segurança da Informação;

XXI. Decreto nº 10.222, de 5 de fevereiro de 2020 - Aprova a Estratégia Nacional de Segurança Cibernética;

XXII. Decreto nº 12.069, de 21 de junho de 2024 - Dispõe sobre a Estratégia Nacional de Governo Digital e a Rede Nacional de Governo Digital – Rede Gov.br e institui a Estratégia Nacional de Governo Digital para o período de 2024 a 2027;

XXIII. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 - Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

XXIV. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021 - Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

XXV. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009 - Criação de equipes de tratamento e resposta a incidentes em redes computacionais - ETIR;

XXVI. Acórdão 1603/2008 do Plenário do Tribunal de Contas da União – TCU

XXVII. ABNT NBR ISO/IEC 27000:2018 – Sistemas de Gerenciamento de Segurança da Informação

XXVIII. ABNT NBR ISO/IEC 27001:2022 - Segurança da Informação, segurança cibernética e proteção à privacidade – Sistemas de gestão de segurança da informação - Requisitos;

XXIX. ABNT NBR ISO/IEC 27002:2022 – Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação;

XXX. ISO/IEC 27005:2019 – Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação;

XXXI. ISO/IEC 27035:2023 – Tecnologia da Informação – Gestão de incidentes de segurança da informação Parte 1: Princípios e processo;

XXXII. ISO/IEC GUIDE 51:2014 – fornece, aos elaboradores de normas, recomendações para a inclusão dos aspectos de segurança nas normas.

CAPÍTULO XIII
DISPOSIÇÕES FINAIS

Art. 60. As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação e feitas através dos seguintes canais: GSS ou endereço eletrônico dtic@iftm.edu.br

Art. 61 Os casos omissos e as dúvidas sobre a Política de Segurança da Informação e seus documentos serão analisados e deliberados pelo Comitê Gestor de Segurança da Informação do IFTM.