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

INSTRUÇÃO NORMATIVA IFTM Nº 145 DE 17 DE JULHO DE 2025

Dispõe sobre a Política de Gestão de Ativos do Instituto Federal do Triângulo Mineiro.

A Substituta do Reitor do Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro, no uso de suas atribuições legais, conferidas pela Portaria IFTM-Reitoria nº 47 de 05/01/2024, publicada no DOU de 08/01/2024, e Lei nº 11.892 de 29/12/2008, publicada no DOU de 30/12/2008,

RESOLVE:

Art. 1° Aprovar a Política de Gestão de Ativos do Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro, como norma complementar da Política de Segurança da Informação (POSIN), conforme anexo I.

Art. 2° Esta Instrução Normativa entra em vigor na data de sua publicação.

Uberaba, 17 de julho de 2025.

gov.br
Documento assinado digitalmente
DANIELLE FREIRE PAOLONI
Data: 17/07/2025 16:03:28-0300
Verifique em https://validar.iti.gov.br

Danielle Freire Paoloni
Substituta do Reitor do Instituto Federal do Triângulo Mineiro

ANEXO I

Norma Complementar da POSIN:

Política de Gestão de Ativos

Uberaba, 2025

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor
13/05/2024	1.0	Versão inicial com base no modelo oficial	Coordenação de Governança de Tecnologia da Informação e Comunicação
10/03/2025	1.1	Revisão e adequações	Coordenação de Governança de Tecnologia da Informação e Comunicação
28/04/2025	1.2	Revisão e formatação	Gestor de Segurança da Informação e Comunicação
16/06/2025	1.3	Revisão	Gestor de Segurança da Informação e Comunicação
09/07/2025	1.4	Revisão	Gestor de Segurança da Informação e Comunicação

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS

Esse documento refere-se a Política de Gestão de Ativos do Instituto Federal do Triângulo Mineiro (IFTM), em conformidade com as diretrizes estabelecidas pelo art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados que estão sob sua custódia. Adicionalmente, a Política de Gestão de Ativos visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento foi adaptado pela equipe de Governança em Tecnologia da Informação e Gestor de Tecnologia da Informação e Comunicação do IFTM com base em referências do Guia do Framework do Programa de Privacidade e Segurança da Informação (PPSI), compiladas a partir de diversas fontes, incluindo publicações do *Center for Internet Security* (CIS), da *International Organization for Standardization* (ISO) e do *National Institute of Standards and Technology* (NIST).

Nesse cenário, é importante ressaltar que:

a) O IFTM não representa oficialmente o CIS, a ISO ou o NIST, nem se manifesta em nome de autoridades de privacidade e segurança da informação;

b) Este documento não é coautoria das publicações internacionais mencionadas e não assume responsabilidade por interpretações inadequadas do seu conteúdo;

c) Recomenda-se que o leitor consulte diretamente as fontes oficiais para garantir o atendimento integral dos requisitos das publicações mencionadas.

Agradecemos ao CIS, à ISO, ao NIST e à equipe técnica responsável pela implantação do PPSI pela valiosa contribuição para a elaboração deste documento.

INTRODUÇÃO

Atualmente, o Instituto Federal do Triângulo Mineiro (IFTM) utiliza tecnologia de forma estratégica para aprimorar e ampliar a oferta de serviços públicos aos cidadãos, por meio de sistemas informatizados e infraestrutura dedicada.

Nesse cenário, o IFTM, seja por meio de sua própria infraestrutura ou de contratos com terceiros, realiza diversas operações relacionadas à coleta, processamento, armazenamento e transmissão de informações confidenciais e públicas. Essas informações são essenciais para o fornecimento de serviços fundamentais, como o processamento de dados acadêmicos, concessão de benefícios para alunos de baixa renda com o objetivo de auxiliar a sua permanência na instituição, emissão de documentos como histórico escolar e diploma, serviços administrativos, entre outros.

A proteção dessas informações é de responsabilidade do IFTM, conforme estabelecido no art. 46 da Lei Geral de Proteção de Dados (LGPD):

"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

É importante ressaltar que a adoção deste modelo não substitui a necessidade de considerar as diretrizes gerais para implementação da Política de Segurança da Informação conforme estabelecido na Resolução IFTM/CONSUP nº 447 de 02 de dezembro de 2024, que regem os processos relacionados à gestão de segurança da informação do IFTM.

A gestão de ativos institucionais é um processo fundamental para o IFTM, envolvendo a aquisição, identificação, rastreamento, manutenção e descarte adequado dos ativos de sua propriedade. A política de gestão de ativos estabelece os processos e procedimentos para governar o ciclo de vida desses ativos, garantindo que um inventário seja mantido para apoiar a missão da instituição. Este inventário deve ser atual e refletir os ativos atuais de propriedade e operados pela instituição.

CAPÍTULO I
DO PROPÓSITO

Art. 1° Levando em consideração a natureza e finalidade do IFTM, esta política tem como objetivo:

I - Garantir a identificação adequada e a implementação de controles de proteção para os ativos de informação;

II - Buscar assegurar a segurança e continuidade das operações da instituição, por meio do mapeamento, monitoramento e gestão eficaz dos ativos tecnológicos;

III - Garantir que os ativos de informação sejam identificados adequadamente e que os controles de proteção recomendados para estes ativos de informação estejam em vigor.

Art. 2° Para manter a segurança e continuidade do negócio do IFTM, em sua missão, é fundamental mapear e monitorar os ativos tecnológicos para maior controle da organização, auxiliando na aplicação de atualizações, implementação de controles de segurança e gestão de riscos, bem como na recuperação de incidentes.

Art. 3° Os ativos de informação do IFTM devem ser classificados a fim de permitir a definição de níveis de segurança para eles.

Art. 4° Cada ativo de informação deverá ter um “dono”, no qual realizará a classificação do ativo de informação e deverá ser registrado em uma base de dados gerenciada de forma centralizada.

Art. 5° Os benefícios esperados com a aplicação desta política são:

I - redução de custos: otimiza o uso de recursos, evita gastos desnecessários, controla licenciamento de software e permite uma melhor alocação financeira, resultando em economia de custos;

II - aumento da eficiência operacional: melhora a produtividade ao permitir a visão dos ativos de informação disponíveis e em efetivo funcionamento;

III - melhoria na tomada de decisão: fornece dados precisos e atualizados sobre o inventário de ativos, permitindo decisões mais informadas sobre investimentos, atualizações e substituições;

IV - conformidade e mitigação de riscos: assegura conformidade com regulamentações e políticas, além de minimizar riscos de segurança, financeiros e legais associados aos ativos de informação;

V - aumento da segurança da informação: garante a implementação de práticas de segurança adequadas, protegendo os ativos de informação contra ameaças e vulnerabilidades;

VI - maximização do valor dos ativos: acompanha o ciclo de vida dos ativos para garantir que sejam utilizados da melhor forma possível e prolonga sua vida útil quando apropriado;

VII - melhoria na gestão de fornecedores: facilita negociações mais eficazes, garantindo que os fornecedores de TI cumpram acordos e contratos, melhorando os relacionamentos comerciais;

VIII - suporte à estratégia de negócios: alinha os ativos de informação com os objetivos e metas organizacionais, facilitando a inovação e a adaptação às mudanças do mercado;

IX - aprimoramento da gestão de mudanças: facilita a implementação de mudanças de maneira mais controlada e eficiente, minimizando impactos negativos nos serviços;

X - melhoria na satisfação do cliente interno e externo: garante que os serviços oferecidos pela TI sejam confiáveis, consistentes e atendam às necessidades dos usuários finais e clientes da organização.

CAPÍTULO II
ESCOPO

Art. 6° Esta Política de Gestão de Ativos se aplica a todos os ativos de informação que se encontram sob domínio do IFTM (*campi,* pólos e reitoria), incluindo aqueles armazenados fora da instituição, como em serviços de nuvem.

Parágrafo único. Considera-se como ativos de informação os meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização[1].

Art. 7° Para fins desta política, as coordenações e serviços de apoio de tecnologia da informação dos *campi* e reitoria serão denominados unidade de tecnologia da informação.

CAPÍTULO III
DOS PRINCÍPIOS GERAIS

Art. 8° A Política de Gestão de Ativos de informação deve estar alinhada à Política de Segurança da Informação (POSIN) do IFTM.

[1] Definição de ativos de informação dado pelo Glossário de Segurança da Informação Portaria GSI/PR nº 93, de 18 de outubro de 2021.

Parágrafo único: Os conceitos e definições desta política, bem como seu período de atualização deverão ser observados diretamente na POSIN.

Art. 9° A Política de Gestão de Ativos de informação deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 10. A gestão de ativos de informação será responsabilidade das unidades de tecnologia da informação do IFTM sob supervisão do Gestor de Segurança da Informação e Comunicação.

Art. 11. O processo de mapeamento de ativos de informação deve estruturar e manter um registro de ativos de informação, destinados a subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

Art. 12. As rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação da instituição, a fim de manter o escopo da organização mapeado e documentado de forma estruturada.

Art. 13. As rotinas de inventário de ativos de informação não substituem as ações de inventário realizadas pelas áreas de patrimônio das unidades do IFTM.

Art. 14. O processo de mapeamento de ativos de informação deve considerar, preliminarmente os objetivos estratégicos da instituição, seus processos internos, os requisitos legais e sua estrutura organizacional.

Art. 15. O inventário resultante do processo de mapeamento de ativos de informação deverá ser categorizado e classificado, conforme disposto nesta política.

Art. 16. Os seguintes ativos de informação devem ser considerados no processo de mapeamento e inventário de ativos de informação:

I - Ativos físicos: computadores desktop, notebooks, dispositivos móveis (tablets, smartphones, etc.), servidores físicos, equipamentos de armazenamento removível (HDs Externos, Pen drives, cartões de memória, etc.), equipamentos de rede (switches, roteadores e pontos de acesso Wi-Fi), equipamentos de impressão e digitalização (impressoras, scanners, multifuncionais), mídias ópticas (unidades de backup físico), dispositivos de autenticação física (tokens, *smartcards*).

II - Ativos de Softwares: sistemas operacionais, aplicativos de produtividade (suítes de escritório, navegadores, editores de imagem), sistemas corporativos (financeiros, pedagógicos, etc.), sistemas de comunicação e colaboração (e-mail, plataformas de videoconferência, chats corporativos), softwares de segurança da informação (antivírus, *firewall*, soluções de *backup*, criptografia, gestão de logs, etc.), licenças de softwares (por assinatura, perpétuas e OEM - *Original Equipment Manufacturer*), sistemas de gestão de banco de dados, sistemas de terceiros hospedados no IFTM, aplicações desenvolvidas internamente, serviços de software em nuvem.

CAPÍTULO IV
DAS DIRETRIZES

Art. 17. Todos os ativos de informação que estejam dentro do território de alguma unidade da instituição, mesmo que transitoriamente, deverá ser identificado considerando as diretrizes desta política.

Art. 18. A organização deverá utilizar da segmentação de rede para organizar seus ativos de informação.

Art. 19. A organização deve implementar o controle de acessos e privilégios mínimos para a administração dos ativos de informação.

Art. 20. A organização deve implementar a centralização de autenticação, autorização e auditoria (AAA) para a administração de seus ativos de informação, principalmente os ativos que fazem parte da infraestrutura de rede da organização.

Art. 21. Os ativos devem ser categorizados de acordo com sua finalidade de uso:

I - Administrativa;

II - Pedagógica;

III - Infraestrutura.

Art. 22. Os ativos devem ser classificados de acordo com o nível de criticidade que geram para a instituição em relação a Segurança da Informação (vide Capítulo VI desta Política):

I - Crítico;

II - Alto;

III - Moderado;

IV - Baixo.

Art. 23. A categorização e classificação do inventário deve ser aprovada pela alta gestão da unidade.

Art. 24. A atualização do mapeamento e inventário dos ativos de informação deverá ocorrer semestralmente ou sempre que houver alguma alteração significativa em relação a aquisição/substituição de ativos.

Art. 25. As unidades de tecnologia da Informação deverão elaborar e manter diagramas e demais documentações da arquitetura de rede da respectiva unidade.

Parágrafo Único: A revisão destas documentações deverá ser realizada de forma periódica, no mínimo, a cada ano, ou quando ocorrerem mudanças significativas, que possam impactar tais artefatos.

Art. 26. A unidade de tecnologia da informação deverá garantir que a infraestrutura de rede da instituição esteja atualizada.

Parágrafo Único: Deverá ser realizada uma revisão das versões de software de forma periódica, ou quando for identificada uma vulnerabilidade que eleve o risco da organização

Art. 27. A unidade de tecnologia da informação poderá empregar o uso de mecanismos automatizados ou não automatizados para identificar ativos incluindo físicos e/ou software.

Art. 28 A unidade de tecnologia da informação poderá bloquear/banir ativos que coloquem em risco a Segurança da Informação institucional.

Art. 29. A Diretoria de Tecnologia da Informação e Comunicação e/ou Gestor de Segurança da Informação da instituição poderá solicitar a qualquer momento acesso ao inventário de ativos ou mapeamento da arquitetura de rede das unidades do IFTM para fins de acompanhamento e verificação de conformidade com as práticas de Segurança da Informação da instituição.

Seção I
Do mapeamento e inventário de ativos físicos

Art. 30. Cada ativo de informação deve ter uma etiqueta afixada ao dispositivo com um identificador (patrimônio).

Art. 31. O inventário dos ativos físicos deve conter, no mínimo, os seguintes dados:

I - Identificador/patrimônio do ativo;

II - Tipo do ativo;

III - Data da compra;

VI - Preço de compra;

V - Descrição do item;

VI -Fabricante;

VII -Número do modelo;

VIII -Número de série;

IX - Nome do responsável do ativo;

X - Localização física do ativo;

XI - Endereço físico (controle de acesso à mídia (MAC)), quando aplicável;

XII - Endereço de Protocolo de Internet (IP), quando aplicável;

XIII - Data de validade da garantia/vida útil;

XIV - Nível de acesso (servidor, cargo, setor);

XV - Qualquer informação de licenciamento relevante.

Art. 32. A unidade de tecnologia da informação poderá empregar o uso de ferramentas de descoberta ativa e/ou passiva para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos.

Art. 33. A unidade de tecnologia da informação poderá empregar o uso de ferramentas para o mapeamento visual dos ativos físicos.

Art. 34. A unidade de tecnologia da informação poderá utilizar controles técnicos em todos os ativos de hardware autorizados a utilizar a rede.

Art. 35. A unidade de tecnologia da informação deve assegurar, sempre que possível, que os ativos de informação inventariados possuam contrato de suporte em vigor.

Art. 36. A unidade de tecnologia da informação poderá utilizar ferramenta de gerenciamento de endereços IP - ex.: *Dynamic Host Configuration Protocol* (DHCP) - para atualizar o inventário de ativos da instituição.

Seção II
Do mapeamento e inventário de software

Art. 37. No caso de softwares deve ser registrado no inventário, no mínimo, os seguintes dados:

I. Solicitante do software (servidor, setor);

I - Nível de acesso (servidor, cargo, setor);

II - Título do software;

III - Desenvolvedor ou editor de software;

IV - Data de aquisição;

V - Data de instalação;

VI - Data de atualização, se aplicável;

VII - Duração do uso;

IX - Finalidade comercial;

IX - Lojas de aplicativos;

X - Versões;

XI - Mecanismo de implantação;

XII - Data de fim do suporte, se conhecida;

XIII - Qualquer informação de licenciamento relevante;

XIV - Data de descomissionamento.

Art. 38. A unidade de tecnologia da informação poderá utilizar ferramentas de inventário de software, quando possível, em toda a organização para automatizar a descoberta e documentação do software instalado.

Art. 39. A unidade de tecnologia da informação poderá utilizar controles técnicos em todos os ativos para garantir que apenas software autorizado seja executado, sendo estes reavaliados periodicamente a critério da unidade.

Art. 40. A unidade de tecnologia da informação poderá utilizar controles técnicos para garantir que apenas bibliotecas e scripts autorizados, e assinados digitalmente tenham permissão para serem executados.

Art. 41. As atualizações e novas versões de softwares devem ser avaliadas e aprovadas pela unidade de tecnologia da informação e alta gestão da unidade antes da instalação.

CAPÍTULO V
DAS RESPONSABILIDADES DO RESPONSÁVEL PELO ATIVO
(RECOMENDA-SE A LEITURA AO ART. 9º DA IN GSI/PR Nº 3/2021)

Art. 42. Cabe ao agente responsável pela gestão dos ativos de TIC:

I - Identificar potenciais ameaças aos ativos de informação;

II - Identificar vulnerabilidades dos ativos de informação;

III - Consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;

IV - Avaliar os riscos dos ativos de informação ou do grupo de ativos de informação;

V - Garantir que indivíduos que requerem acesso aos sistemas de informação devem seguir o procedimento adequado para receber tal acesso, como descritos na política de controle de acesso e catalogadas no sistema de gestão de ativos de TIC;

VI - Monitorar a associação da gestão de ativos de TIC com os processos em torno do gerenciamento de mudança e de configuração de ativo de serviço, e outros correlatos;

VII - Promover meios que garantam que todos os ativos de informação devem ser devolvidos após a rescisão de vínculo com o instituto.

CAPÍTULO VI
CRITICIDADE DO ATIVO DE INFORMAÇÃO

Art. 43. A criticidade dos ativos de informação críticos da organização é determinada pelo:

I - Natureza da utilização/finalidade;
II - Requisitos legais;
III - Nível básico de disponibilidade;
IV - Pelo valor financeiro;
V - Pelo seu potencial de agregar valor ao negócio;
VI - Por sua vida útil.

Art. 44. O nível básico de disponibilidade é definido como a capacidade mínima exigida de disponibilidade de um ativo de informação para assegurar que as funções institucionais suportadas por ele não sejam interrompidas ou impactadas de forma significativa.

Parágrafo único. O nível básico de disponibilidade representa o tempo máximo tolerável de indisponibilidade do ativo, considerando sua natureza e sua importância para a continuidade dos serviços prestados pela instituição.

CAPÍTULO VII
CLASSIFICAÇÃO DE NÍVEL DE ACESSO DAS INFORMAÇÕES

Art. 45. Todos os ativos de informação devem ser classificados de acordo com seu nível de acesso, a fim de assegurar o direito fundamental de acesso à informação, bem como dispor sobre a devida restrição de acesso sobre informações sigilosas, conforme previsto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) e demais normas aplicáveis.

Art. 46. As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação do IFTM, independentemente de seu formato e suporte, devem ser classificadas segundo seu nível de acesso, de acordo com a legislação pertinente, sobretudo com as disposições da LAI, do Decreto nº 7.724, de 16 de maio de 2012, e orientações ou normas complementares editadas por órgãos competentes.

Art. 47. A classificação de nível de acesso das informações deve observar às diretrizes constantes na LAI, Decreto nº 7.724, de 16 de maio de 2012 e outros normativos complementares que abordam o assunto.

Art. 48. As informações devem ser classificadas conforme os seguintes níveis de acesso:

I - Pública, com acesso irrestrito e visível a todos os usuários, inclusive pelo público externo;

II - Restrita, quando se tratar de informação sigilosa não classificada em grau de sigilo, protegidas por demais hipóteses legais de restrição de acesso; e

III - Sigilosa classificada em grau de sigilo, nos termos do art. 23 da Lei nº 12.527/2011, subdividida nos graus ultrassecreto, secreto ou reservado.

Art. 49. Os ativos de informação serão rotulados e manuseados com base nos procedimentos apropriados de classificação de nível de acesso de informações usados pela instituição.

CAPÍTULO VIII
MANIPULAÇÃO DE MÍDIA

Art. 50. A mídia removível também deve ser gerenciada pelo mesmo procedimento de classificação de ativos de informação usado pela organização.

Art. 51. A mídia removível deve ser protegida contra acesso não autorizado e uso indevido durante o uso e em trânsito, e deve ser descartada com segurança, usando os procedimentos apropriados.

Art. 52. A mídia contendo informações confidenciais e internas do IFTM devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

CAPÍTULO IX
USO ACEITÁVEL

Art. 53. Padrões ou diretrizes para o uso aceitável de ativos devem ser documentados para indicar o que os usuários dos ativos de informação podem ou não fazer.

Parágrafo Único. As diretrizes de uso aceitável são apresentadas na POSIN ou Normas Complementares.

CAPÍTULO X
NÃO CONFORMIDADE

Art. 54. O descumprimento ou violação de um ou mais itens desta política poderá resultar na aplicação de sanções previstas na POSIN/IFTM.

Art. 55. É fundamental que todos os servidores do IFTM, estudantes, parceiros externos e terceirizados, estejam cientes de suas responsabilidades e dos potenciais riscos associados ao não cumprimento destas diretrizes.

Art. 56. A gestão do IFTM se reserva no direito de escalar os casos de não conformidade repetida para as instâncias administrativas superiores, visando assegurar a adoção de medidas corretivas adequadas e a manutenção da integridade, confidencialidade e disponibilidade dos dados institucionais.

CAPÍTULO XI
DISPOSIÇÕES FINAIS

Art. 57. As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação e feitas através dos seguintes canais: módulo de Gestão de Serviços e Solicitações do Virtual IF (GSS) ou endereço eletrônico dtic@iftm.edu.br.

Art. 58. Os casos omissos e as dúvidas sobre a Política de Gestão de Ativos e seus documentos serão analisados e deliberado pelo Comitê Gestor de Segurança da Informação do IFTM.