MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TOCANTINS
REITORIA

POLÍTICA DE GESTÃO DE ATIVOS

Estabelece a Política de Gestão de Ativos no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO).

CAPÍTULO I
DO ESCOPO

Art. 1º A Política de Gestão de Ativos tem o objetivo de garantir que os ativos de Tecnologia da Informação (TI) sejam identificados adequadamente e que os controles de proteção recomendados sejam implementados visando a garantia da disponibilidade e a integridade dos ativos de TI no IFTO para a plena e adequada prestação de serviços durante todo o seu ciclo de vida.

§ 1º Os ativos de TI são divididos em ativos de *hardware*, *software* e dados:

I - *hardware:* equipamentos de escritório, tais como: computadores, notebooks, monitores, nobreaks, impressoras; infraestrutura: switches, roteadores, access points; multimídia: TV, projetores etc;

II - *software:* sistemas de informação, aplicativos desenvolvidos pelo IFTO ou outras instituições, softwares livres ou licenciados, dentre outros; e

III - dados: pessoais, institucionais, de propriedade do usuário ou IFTO ou sob a guarda do instituto.

§ 2º Esta política é complementada por: norma interna complementar, planos, processo, procedimentos, medidas de controle, competências, responsabilidades e direcionamentos a serem adotados para a gestão de ativos associados à TI, considerando os processos, requisitos legais, planos institucionais e estrutura organizacional do IFTO.

Art. 2º Esta política se aplica a todos os usuários que utilizam de forma direta ou indireta os ativos de TI pertencentes ao IFTO, incluindo ativos fora da instituição armazenados em um *software* ou serviço de computação em nuvem.

CAPÍTULO II
DOS TERMOS E DEFINIÇÕES

Art. 3° Para fins de compreensão dos termos utilizados nesta política serão utilizados os seguintes conceitos e definições:

I - ameaça: conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;

II - alta administração: representa o mais alto nível estratégico e decisório de um órgão ou

entidade, seja ela parte da administração pública federal;

III - atividade: ação ou conjunto de ações executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

IV - ativo: tudo que tenha valor para a organização, material ou não;

V - ativos de informação: 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;

VI - *backup/cópia de segurança:* conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

VII - banco de dados: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

VIII - comitê de segurança da informação (CSI): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

IX - computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem;

X - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

XI - controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estrutura organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

XII - controles de segurança: certificado que autoriza uma pessoa natural para o tratamento de informação classificada;

XIII - criptografia: arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

XIV - CTIR GOV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República;

XV - descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

XVI - diretriz: descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas;

XVII - documento: unidade de registro de informações, qualquer que seja o suporte ou o formato;

XVIII - e-mail: sigla de correio eletrônico (*electronic mail*);

XIX - eliminação: exclusão de dado ou conjunto de dados, armazenados em banco de dados,

independentemente do procedimento empregado;

XX - equipe de tratamento e resposta a incidentes cibernéticos (ETIR): grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade;

XXI - evento: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

XXII - evento de segurança: qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança;

XXIII - *firewall*: ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de *hardware* ou *software*, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo *firewall*, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

XXIV - incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XXV - incidente cibernético: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema;

XXVI - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXVII - informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXVIII - internet: rede global, composta pela interligação de inúmeras redes;

XXIX - medidas de segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

XXX - política: intenções e diretrizes globais formalmente expressas pela direção;

XXXI - política de segurança da informação: documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

XXXII - prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

XXXIII - rede de computadores: conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

XXXIV - recursos de processamento da informação: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem;

XXXV - risco: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

XXXVI - risco de segurança da informação: risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XXXVII - segurança da informação: preservação da confidencialidade, integridade, disponibilidade, adicionalmente outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

XXXVIII - serviços: meio de fornecimento de valor a clientes, com vistas a entregar os resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;

XXXIX - SI: sigla de segurança da informação;

XL - sistema de informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada;

XLI - tecnologia da informação: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações; e

XLII - usuário: pessoa física ou jurídica, seja servidor público, estudante ou prestador de serviços, voluntário habilitado pela administração para acessar os ativos de informação do IFTO.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 4º Esta política considera os seguintes princípios:

I - respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a administração pública federal;

II - garantia de integridade, autenticidade e disponibilidade da informação sob a custódia do IFTO, com respeito ao princípio da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos na legislação;

III - alinhamento estratégico da Política de Segurança da Informação com os demais planos institucionais;

IV - responsabilidade pelo cumprimento das normas pertinentes à segurança da informação vigentes; e

V - conscientização, educação e comunicação como alicerces fundamentais para o fomento da cultura em segurança da informação.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 5º As diretrizes gerais constituem os pilares da gestão de ativos no IFTO, norteando a elaboração de normas, processos, planos, procedimentos e ações de controles que garantem que os princípios básicos de segurança da informação sejam atingidos.

§ 1º Esta política deve estar alinhada com a Política de Segurança da Informação, aos princípios, diretrizes e legislações pertinentes que regem a administração pública federal, bem como aos normativos internos, objetivos estratégicos, planos institucionais e processos

internos do IFTO.

§ 2º Os ativos conectados à rede devem ser inventariados, com o objetivo de identificar precisamente quais necessitam ser monitorados e/ou protegidos mapeando todos os ativos não autorizados para uma possível remoção ou remediação futura.

§ 3º Os softwares instalados nos ativos institucionais devem ser inventariados de forma que apenas o software autorizado seja instalado e possa ser executado, e que todo o software não autorizado e não gerenciado seja encontrado e impedido de instalação ou execução.

§ 4º Regras e procedimentos para aquisição, uso, manutenção, transferência e descarte de ativos devem ser identificadas, documentadas e implementadas para que sejam permitidos o uso de informações e de ativos associados aos recursos de processamento da informação.

§ 5º A concessão de acesso à ativos de TI para usuários sem vínculo com o IFTO fica a critério do responsável pelo setor de Tecnologia da Informação do campus.

§ 6º A instalação e execução de softwares em ativos de TI se restringe a softwares autorizados pela setor de TI do Campus.

§ 7º É vedada a utilização e/ou instalação de software que possa de qualquer forma ferir as disposições desta política, bem como direitos autorais, de propriedade intelectual ou quaisquer legislações vigentes.

§ 8º Os ativos devem ser devolvidos após a rescisão do contrato de trabalho ou contrato.

CAPÍTULO V
DA GESTÃO DE ATIVOS

Art. 6º A gestão de ativos envolve a supervisão e o controle de todos os recursos relacionados à tecnologia da informação em uma organização. Neste contexto, é crucial implementar diretrizes específicas envolvendo a aquisição, identificação, operação, manutenção e descarte de ativos.

§ 1º Um inventário atualizado contendo todos os ativos de TI, incluindo *hardware, software,* dados e dispositivos conectados à rede deve ser estabelecido, documentado e atualizado continuamente.

§ 2º O processo de mapeamento de ativos de informação deve considerar, preliminarmente os objetivos estratégicos da organização, seus processos internos, os requisitos legais, planos institucionais e sua estrutura organizacional;

§ 3º O processo de gestão de ativos associados deve subsidiar a implantação de controles e ações com vistas a assegurar a adequada proteção dos ativos e das informações que armazenam, processam ou transmitem.

§ 4º A gestão dos os *softwares* (sistemas operacionais e aplicações) instalados na rede deve ser realizada para que apenas o *software* autorizado seja instalado e possa ser executado, e que o *software* não autorizado e não gerenciado seja encontrado e impedido de ser instalado ou executado.

Seção I
Aquisição

Art. 7º A aquisição de ativos deve ser pautada por normativa pertinente no âmbito da administração pública federal. Esta fase do processo de gestão de ativos refere-se a definição de especificações, planejamento de contratação,seleção do fornecer e gestão de contratos de TI.

Parágrafo único. Um plano de padronização, manutenção, expansão e atualização de ativos de

Tecnologia da Informação deve ser estabelecido, documentado e atualizado continuamente de forma a acompanhar as demandas das áreas de ensino, pesquisa e extensão bem como a evolução tecnológica.

Seção II
Identificação

Art. 8º As rotinas de inventário e mapeamento de ativos devem ser orientadas para a identificação dos ativos de informação da organização, a fim de manter o escopo da organização mapeado, documentado e atualizado.

§ 1º O inventário de ativos deve conter minimamente as informações críticas que os ativos armazenam, processam ou transmitem; os responsáveis (proprietários e custodiantes) de cada ativo de informação; as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação; os contêineres de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.

§ 2º Os ativos institucionais devem ser classificados de acordo com sua criticidade para o IFTO.

§ 3º Ferramenta de gerenciamento de endereço IP deve ser utilizada para atualizar o inventário de ativos institucionais.

Seção III
Implementação

Art. 9º A implementação de ativos de TI refere-se ao processo de instalação, configuração e distribuição de ativos de TI no ambiente organizacional de forma a garantir que os ativos sejam integrados de maneira eficiente e segura, atendendo aos requisitos tecnológicos e necessidades das áreas de ensino, pesquisa e extensão do IFTO.

§ 1º Um procedimento padronizado de configuração segura deve ser estabelecido, documentado e atualizado continuamente para todos os ativos de TI.

§ 2º As rotinas de implementação e configuração de ativos institucionais devem ser estabelecidas, padronizadas, documentadas e atualizadas continuamente.

§ 3º Controles de acesso devem ser implementados e mantidos continuamente para limitar o acesso aos ativos institucionais apenas a usuários autorizados.

§ 4º Controles técnicos devem ser implementados em ativos institucionais para garantir que apenas *softwares* autorizados sejam executados e apenas bibliotecas e *scripts* autorizados, e assinados digitalmente tenham permissão para serem executados.

§ 5º Serviços, *softwares* e aplicativos desnecessários devem ser desinstalados ou desativados nos ativos institucionais.

§ 6º Sempre que possível os ativos associados a TI devem ser testados para avaliar a eficácia e a resiliência dos controles de segurança da informação.

§ 7º Medidas de segurança para ativos institucionais que operem fora das dependências do IFTO devem ser tomadas, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora da instituição.

§ 8º Sistemas de monitoramento contínuo para detectar atividades incomuns ou padrões de tráfego suspeitos nos ativos de TI devem ser implementados.

§ 9º Ferramentas de descoberta ativa e/ou passiva devem ser implementados para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos.

Seção IV
Operação e manutenção

Art. 10º A operação e manutenção de ativos são partes críticas da gestão de ativos de TI, pois impactam diretamente a eficiência operacional, a confiabilidade e a segurança dos recursos organizacionais. Referem-se ao conjunto de atividades envolvidas na gestão contínua, controle, execução, monitoramento, manutenção e preservação de ativos de TI em uma organização.

§ 1º Uma norma sobre o uso seguro de recursos de TI deve ser estabelecida, documentada e analisada continuamente.

§ 2º Um procedimento operacional padrão para operação e manutenção de ativos deve ser estabelecido, documentado e analisado continuamente.

§ 3º Sempre que possível deve-se realizar o acompanhamento do desempenho dos ativos para identificar problemas potenciais, otimizar o uso e garantir a eficiência operacional.

§ 4º Manutenções em ativos de TI devem ser planejadas para evitar falhas e prolongar a vida útil dos ativos, incluindo inspeções, substituições de peças, entre outros.

Seção V
Descarte

Art. 11º O descarte envolve o processo de remoção segura e eficiente de equipamentos e componentes de tecnologia que atingiram o final de sua vida útil. Essa fase é crítica para garantir a segurança da informação, a conformidade regulatória e a gestão ambientalmente responsável dos ativos.

§ 1º Um procedimento para descarte seguro de ativos de informação deve ser mantido atualizado continuamente para ser executado quando os ativos de TI forem considerados inservível ou irrecuperável.

§ 2º Ativos de TI que estão no final de sua vida útil ou que não sãos mais necessários devem ser identificados e devem se examinados antes do descarte, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido removidos com segurança.

§ 3º Antes de realizar o descarte do ativo uma avaliação da possibilidade de reutilização, reciclagem ou descarte do ativo deve ser realizada considerando fatores como valor residual, segurança e conformidade.

§ 4º O setor de TI pressumirá que o backup de dados armazenados nos ativos de TI foi feito pelo responsável antes de repasse e descarte.

§ 5º Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes do descarte, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido removidos com segurança.

§ 6º Procedimentos rigorosos para garantir a remoção segura de todos os dados sensíveis armazenados nos ativos devem ser realizados.

§ 7º Métodos de exclusão de dados confiáveis, como formatação segura ou destruição física de mídias de armazenamento devem ser utilizados.

CAPÍTULO VI
DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Seção I

Da Alta Administração

Art. 12º Compete à alta administração:

I - prover a orientação e o apoio necessário às ações de segurança da informação, de acordo com os objetivos estratégicos, planos institucionais, leis e regulamentos pertinentes; e

II - destinar recursos (humanos, tecnológicos e financeiros) para a execução da gestão de ativos associados à TI no âmbito do IFTO.

Seção II
Do Gestor de Tecnologia da Informação

Art. 13° Compete ao Gestor de Tecnologia da Informação:

I - planejar, implementar e melhorar continuamente os controles de ativos institucionais em soluções de tecnologia da informação e comunicações, nos termos da legislação vigente na administração pública federal.

Seção III
Do Gestor de Segurança da Informação

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

I - coordenar a elaboração da política de gestão de ativos e da norma interna de complementar, observadas a legislação pertinente exaradas pelo gabinete de segurança institucional da presidência da república.

II - assessorar a alta administração na implantação da política de gestão de ativos associados à TI;

III - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à gestão de ativos;

IV - propor recursos necessários às ações de gestão de ativos;

V - verificar os resultados dos trabalhos de auditoria sobre a gestão de ativos; e

VI - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos relacionados à gestão de ativos.

Seção IV
Do Comitê de Segurança da Informação

Art. 15° Compete ao Comitê de Segurança da Informação:

I - deliberar sobre política e norma interna complementar sobre gestão de ativos;

II - assessorar a implementação das ações de gestão de ativos; e

III - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre gestão de ativos.

Seção V
Da Equipe de Tratamento e Resposta a Incidentes Cibernéticos

Art. 16° Compete à Equipe de Tratamento e Resposta a Incidentes Cibernéticos:

I - deliberar sobre procedimentos internos para gestão de ativos;

II - receber, analisar e responder às notificações e atividades relacionadas à ativos institucionais;

III - desenvolver as atividades de prevenção, tratamento e resposta a incidentes relacionados à ativos de TI; e

IV - propor diretrizes e responsabilidades para a política e norma interna complementar de gestão de ativos.

Seção VI
Da Diretoria de Tecnologia da Informação e demais Setores de TI das unidades do IFTO

Art. 17° Compete à Diretoria de Tecnologia da Informação e demais setores de TI das unidades do IFTO:

I - definir características técnicas e funcionalidades de ativos de TI;

II - conferir os ativos de TI a serem recebidos, oriundos de processos de aquisição ou doação e assinar os termos de recebimento provisório e definitivo;

III - instalar e configurar os ativos de TI para o uso seguro dos ativos de TI;

IV - identificar e classificar os ativos de TI por nível de criticidade;

V - identificar potenciais ameaças e vulnerabilidades aos ativos de TI;

VI - consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação;

VII - avaliar os riscos relacionados aos ativos de TI;

VIII - proceder à análise e redistribuição de ativos de TI, considerando demanda setoriais e perfis de utilização de *hardware e software*;

IX - apoiar a alta administração no processo de disponibilização de bens e ativos de TI;

X - realizar manutenções de *hardware e software* e dar suporte técnico operacional quando necessário em ativos de TI;

XI - homologar os *softwares* a serem utilizados em âmbito institucional;

XII - prover condições para que os *softwares* instalados em ativos de TI possam ser atualizados em suas respectivas versões mais recentes;

XIII - proteger os ativos de TI contra violações de segurança da informação;

XIV - prover a infraestrutura de inventário eletrônico automatizado dos equipamentos;

XV - definir as características da obsolescência de ativos de TI;

XVI - definir as características de perfis de usuários correlacionando-os com os recursos mínimos de performance dos ativos de TI;

XVII - definir taxa de renovação anual de ativos de TI considerando as demandas institucionais alinhadas como o Comitê Gestor de TI; e

XVIII - realizar a análise e, quando aplicável, emitir o laudo de constatação de bem inservível para ativos de TI;

XIX - zelar pela segurança da informação contidas nos ativos de TI do IFTO por meio de:

a) inutilização de informações contidas nos HDs antes do processo de descarte e/ou baixa patrimonial, quando solicitado pela unidade administrativa responsável pelo bem; e

b) inutilização de informações contidas nos HDs para os casos em que uma empresa externa

for acionada para a realização de um conserto em um ativo de TI, garantia de fornecedor, por exemplo.

Seção VII
Dos usuários

Art. 18° Compete aos usuários:

I - atender aos princípios e diretrizes contidos nesta política, incluindo norma interna complementar sobre gestão de ativos;

II - guiar-se pelos princípios de confidencialidade, autenticidade, integridade, não repúdio, conformidade, controle de acesso e disponibilidade no decorrer de suas atividades.

III - utilizar os ativos institucionais prioritariamente para a realização das atividades desempenhadas nos limites da ética, razoabilidade e legalidade;

IV - realizar *backup* de dados pessoais armazenados em ativos de TI periodicamente ou quando houver necessidade de formatação do sistema operacional;

V - não entregar os computadores, componentes internos, como HDs, e equipamentos em geral a pessoas sem autorização;

VI - não realizar por conta própria nenhum tipo de manutenção, formatação ou conserto em ativos de TI; e

VII - devolver todos os ativos de TI que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.

Seção VIII
Dos responsáveis pelos setores do IFTO

Art. 19° Compete aos responsáveis pelos setores do IFTO:

I - zelar pela guarda, integridade física e condições de uso dos ativos institucionais sob sua responsabilidade e de propriedade patrimonial do IFTO;

II - manter armazenamento seguro e fazer o *backup* periódico, ou quando houver necessidade de solicitação de suporte, de dados corporativos sob sua guarda; e

III - limitar a utilização de ativos institucionais sob sua responsabilidade a pessoas autorizadas.

Seção IX
Dos responsáveis pelo setor de Patrimônio

Art. 20° Compete ao responsável pelo setor de Patrimônio:

I - efetuar o recolhimento de bens inservíveis e gerenciar seu destino de forma a melhor atender os interesses do IFTO com base nas normas vigentes; e

II - realizar os procedimentos institucionais adequados para o descarte seguro de ativos institucionais.

CAPÍTULO VII
DAS PENALIDADES

Art. 21° Ações que violem esta política, norma interna complementar, procedimentos, ou que quebrem os controles de segurança da informação relacionados à ativos institucionais serão passíveis de investigação, podendo implicar em penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

Parágrafo único. Casos omissos não tratados neste documento serão submetidos, analisados, tratados e decididos pelo Comitê de Segurança da Informação.

CAPÍTULO VIII
DA REVISÃO E ATUALIZAÇÃO

Art. 22° Esta política bem como os documentos gerados a partir dela deverão ser revisados, aprovados e atualizados em função de alterações na legislação pertinente, diretrizes políticas do governo federal, normativas internas do IFTO ou, quando considerado necessário pelo Comitê de Segurança da Informação.

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS

Art. 23° As regras, procedimentos, medidas e controles de proteção de dados e segurança da informação relacionados à ativos institucionais serão detalhadas em norma interna complementar, que apresentarão suas particularidades e procedimentos relativos à segurança da informação alinhados às diretrizes emanadas pelo Comitê de Segurança da Informação e aos respectivos planos institucionais do IFTO.

Art. 24° Esta política e suas atualizações, bem como norma interna complementar para ativos institucionais, deverão ser divulgadas amplamente a todos os usuários, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

Art. 25° A alta administração deverá disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução das diretrizes contidas nesta política.

Art. 26º Esta política entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 19/12/2023, às 10:46, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Kleyton Matos Moreira**, **Diretor**, em 22/12/2023, às 16:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2222407** e o código CRC **66DCF4BA**.

Avenida Joaquim Teotônio Segurado
Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul
CEP 77020-450 Palmas - TO
(63) 3229-2200
www.ifto.edu.br - reitoria@ifto.edu.br

Referência: Processo nº 23235.021679/2023-17

SEI nº 2222407