PORTARIA Nº 1311/REIT - CGAB/IFRO, DE 05 DE JULHO DE 2024

Dispõe sobre a Aprovação da Política de Gestão de Ativos de Tecnologia da Informação e Comunicação do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO).

O REITOR SUBSTITUTO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RONDÔNIA (IFRO), nomeado pela Portaria nº 1.347/REIT - CGAB/IFRO, de 4 de julho de 2023 (SEI nº 1986316), publicada no DOU nº 126, de 5 de julho de 2023, Seção 2, pág. 25, no uso de suas atribuições legais e regimentais conferidas pela Lei nº 11.892, de 29 de dezembro de 2008, publicada no DOU de 30 de dezembro de 2009 e estabelecidas pelo art. 67 do Regimento Geral do IFRO, aprovado pela Resolução nº 65/Consup/IFRO, de 29 dezembro de 2015, e posteriores; tendo em vista o art. 6º do Regimento do Comitê Gestor de Tecnologia da Informação (COGTI) aprovado pela Resolução nº 027/CONSUP/IFRO, de 3 de outubro de 2011, bem como os autos do Processo SEI nº 23243.008477/2023-81, resolve:

Art. 1º Fica aprovada a Política de Gestão de Ativos de Tecnologia da Informação e Comunicação do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), anexo a esta Portaria.

Art. 2º Esta Portaria entra em vigor na data de sua assinatura.

MAURO HENRIQUE MIRANDA DE ALCÂNTARA

Documento assinado eletronicamente por **Mauro Henrique Miranda de Alcântara**, **Reitor(a) Substituto(a)**, em 10/07/2024, às 17:27, 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 https://sei.ifro.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2333161** e o código CRC **004FC0A3**.

POLÍTICA DE GESTÃO DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RONDÔNIA (IFRO)

Histórico de versões

Data	Versão	Descrição	Autores
3/7/2024	1.0	Primeira versão da Política de Gestão de Ativos de Tecnologia da Informação Comunicação do IFRO	**Reitor** - Moisés José Rosa Souza **DGTI** - Bruce Fabian Reis Albuquerque **Encarregado do tratamento de dados pessoais** - Gilberto Paulino da Silva **PRODIN** - Mauro Henrique Miranda de Alcântara **PROAD** - Elisandro de Moura Martins **PROEX** - Marcela Regina Stein dos Santos **PROEN** - Jean Peixoto Campos **PROPESP** - Xênia de Castro Barbosa **DGP** - Cleonice Cabral Costa **DEaD** - Saulo Souza de Macedo ***Campus* Ariquemes** - Adriano Marcos Dantas da Silva ***Campus* Cacoal** - Adilson Miranda de Almeida ***Campus* Colorado do Oeste** - Marcos Aurelio Anequine de Macedo ***Campus* Guajará-Mirim** - Elaine Oliveira Costa de Carvalho ***Campus* Jaru** - Renato Delmonico ***Campus* Ji-Paraná** - Leticia Carvalho Pivetta ***Campus* Porto Velho Calama** - Leonardo Pereira Leocadio ***Campus* Porto Velho Zona Norte** - Jeferson Cardoso da Silva ***Campus* São Miguel do Guaporé** - Mauro Sergio Demicio ***Campus* Vilhena** - Rodrigo Alecio Stiz

DO PROPÓSITO

1. A presente Política, especialmente dirigida aos órgãos e às entidades da Administração Pública Federal (APF), tem como objetivo a Elaboração da Política de Gestão de Ativos e *Softwares*, para atendimento ao previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Essa legislação estabelece que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve adotar medidas de segurança, técnicas e administrativas capazes de resguardar 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 Elaboração de uma Política de Gestão de Ativos visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

2. O objetivo desta política é definir e garantir que os ativos de tecnologia da informação sejam identificados adequadamente de acordo com as principais normas, princípios, objetivos e diretrizes em relação à gestão de ativos de TI, no âmbito do IFRO, para garantir o nível de segurança da informação, privacidade e proteção aos dados determinados pela legislação competente.

3. Para manter a segurança e continuidade do negócio do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), 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 risco da organização. Auxiliando também na recuperação de incidentes.

4. Os ativos de TIC do IFRO devem ser classificados a fim de permitir a definição de níveis de segurança para eles. Cada ativo de TIC deverá ter um "responsável", o qual realizará a classificação do ativo e deverá ser registrado em uma base de dados gerenciada de forma centralizada.

DO ESCOPO

5. Esta política se aplica a todos os ativos de TIC, aos sistemas de informação, à infraestrutura de tecnologia de informação e ainda aos dados digitais corporativos do IFRO de forma direta ou indireta, incluindo ativos do órgão armazenados em serviços de nuvem públicas e privadas.

VIGÊNCIA, VALIDADE E ATUALIZAÇÃO

6. Esta Política passa a vigorar a partir da data de sua publicação e deverá ser atualizada a cada três anos. A comissão, a fim de que a e/ou seus instrumentos normativos, não fiquem ultrapassados ou desatualizados, deve revê-la periodicamente ou quando se fizer necessário.

TERMOS DE DEFINIÇÕES

7. A presente política considera as definições do Glossário apresentadas na Portaria GSI/PR nº 93, de 18 de outubro de 2021 – Glossário de Segurança da Informação do Gabinete de Segurança Institucional da PRESIDÊNCIA DA REPÚBLICA e outras definições.

I. ACESSO: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;
II. AMEAÇA: conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;
III. AGENTE RESPONSÁVEL: servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta e indireta, que se enquadre em qualquer das opções seguintes:
    1. execute o tratamento de informação classificada;
    2. possua credencial de segurança;
    3. seja responsável por um posto de controle de um órgão de registro; e
    4. utilize dispositivos que tenham embarcado criptografia de Estado.
IV. AUTENTICIDADE: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
V. AMBIENTE DE INFORMAÇÃO: agregado de indivíduos, organizações ou sistemas que coletam, processam e disseminam informação;
VI. AMEAÇA: conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;
VII. 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;
VIII. ATIVO: tudo que tenha valor para a organização, material ou não;
IX. ATIVO DE REDE: equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores;
X. CONFIDENCIALIDADE: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

XI. CPALM: Coordenação de Patrimônio e Almoxarifado;
XII. 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 (PSN);
XIII. DADO PESSOAL: informação relacionada à pessoa natural identificada ou identificável;
XIV. DISPONIBILIDADE: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;
XV. INCIDENTE DE SEGURANÇA: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
XVI. INTEGRIDADE: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
XVII. INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
XVIII. MEDIDAS DE SEGURANÇA: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;
XIX. SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
XX. SETOR DE TIC: Setor responsável pela gestão da Tecnologia de Informação, composto pelas coordenações da Reitoria e dos *campi*;
XXI. TRATAMENTO: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; e
XXII. TIC: sigla de tecnologia da informação e comunicação.

DOS PRINCÍPIOS

8. A concepção, desenvolvimento e operação dos ativos de TIC do IFRO devem ser realizados atendendo a boa-fé e respeitando os seguintes princípios:

I. FINALIDADE**:** realização do tratamento para propósitos legítimos, específicos e explícitos, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II. ADEQUAÇÃO**:** compatibilidade do tratamento com as finalidades e objetivos, de acordo com o contexto de tratamento;
III. NECESSIDADE**:** limitação das ações do tratamento ao mínimo necessário para realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades e objetivos; do tratamento de dados;
IV. SEGURANÇA**:** utilização de medidas técnicas e administrativas aptas a proteger os ativos de informação e dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração e comunicação ou difusão não autorizada por legislação ou por ordem judicial, durante o processo de tratamento;
V. PREVENÇÃO**:** adoção de medidas para prevenir a ocorrência de danos decorrentes do processo de tratamento de dados;
VI. LEGALIDADE**:** utilização lícita de ativos de TI para finalidades relacionadas ao vínculo do usuário com o Instituto; e
VII. ECONOMICIDADE**:** utilização de ativos de TI para obtenção do resultado esperado com o menor custo possível, com precaução, celeridade e qualidade na prestação do serviço ou no trato com os bens públicos.

DOS PRINCÍPIOS GERAIS

9. Os princípios gerais são:

I. A Política de Gestão de Ativos de informação deve estar alinhada com a Política de Segurança da Informação (POSIC) do IFRO;
II. A Política de Gestão de Ativos de informação deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional;
III. 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 risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação;
IV. As rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação da organização, a fim de manter o escopo da organização mapeado e documentado;
V. O processo de mapeamento de ativos de informação deve considerar, preliminarmente, os objetivos estratégicos da organização, seus processos internos, os requisitos legais e sua estrutura organizacional; e
VI. O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter: 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 contêiners de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.

GESTÃO DE ATIVOS DE TIC

10. A política de Gestão de Ativos de Tecnologia da Informação e Comunicação do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO) tem como principal objetivo instituir a gestão de ativos de informação, através de procedimentos que visam garantir a disponibilidade e a integridade dos ativos de TIC no IFRO para o uso adequado na prestação de serviços durante todo o seu ciclo de vida.

11. As fases do ciclo de vida dos ativos de TIC são: planejamento, aquisição, implantação, gerenciamento e descarte.

I. PLANEJAMENTO**:** revisão dos ativos de TIC em uso e análise da necessidade e do custo de novas aquisições;
II. AQUISIÇÃO**:** definição de especificações, fornecedores e contratos;
III. IMPLANTAÇÃO**:** configuração, instalação e distribuição dos ativos adquiridos ou contratados;
IV. GERENCIAMENTO**:** controle, monitoramento e manutenção dos ativos; e
V. DESCARTE**:** processo de desfazimento de ativos por motivos de obsolescência, perda de característica, inservibilidade ou excedência.

12. Os ativos de informação são divididos em ativos de *hardware*, de *software* e de dados:

I. São considerados ativos de *hardware*: equipamentos de escritório, como computadores de mesa e portáteis, discos rígidos, monitores, impressoras, dispositivos de armazenamento móveis, etc.; de infraestrutura, como servidores, *storages*, *switches*, roteadores, *access points, firewall*, controladoras, etc.;
II. São considerados ativos de *software*: aplicações desenvolvidas pelo IFRO, aplicações desenvolvidas por outros órgãos públicos e hospedados no IFRO, aplicações de *software* livres e licenças de aplicações e *softwares* de terceiros adquiridas; e
III. São considerados ativos de dados: dados armazenados em sistemas de informação no formato lógico, elétrico, magnético, óptico, que podem ainda ser classificados como dados pessoais, de interesse e propriedade do usuário, ou dados corporativos, de interesse e propriedade ou sob a guarda do IFRO.

13. Os ativos de TIC serão considerados inservíveis, conforme Decreto nº 9.373, de 11 de maio de 2018:

I. OCIOSO: bem móvel que se encontra em perfeitas condições de uso, mas não é aproveitado;
II. RECUPERÁVEL: bem móvel que não se encontra em condições de uso e cujo custo da

recuperação seja até cinquenta por cento do seu valor de mercado ou cuja análise de custo e benefício demonstre ser justificável a sua recuperação;

III. ANTIECONÔMICO: bem móvel cuja manutenção seja onerosa ou cujo rendimento seja precário, em virtude de uso prolongado, desgaste prematuro ou obsoletismo; ou

IV. IRRECUPERÁVEL: bem móvel que não pode ser utilizado para o fim a que se destina devido à perda de suas características ou em razão de ser o seu custo de recuperação mais de cinquenta por cento do seu valor de mercado ou de a análise de seu custo benefício demonstre ser injustificável a sua recuperação.

DIRETRIZES

14. As Diretrizes são:

I. Informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado;
II. A categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade competente;
III. A organização empregará o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo *hardware* ou *software;*
IV. A organização deve assegurar que os ativos de informação inventariados possuam contrato de suporte em vigor;
V. A organização empregará o uso de ferramentas de descoberta ativa e/ou passiva para identificar dispositivos institucionais conectados à rede da instituição e automaticamente atualizar o inventário de ativos;
VI. A organização utilizará ferramentas de inventário de *software*, quando possível, em toda a organização para automatizar a descoberta e documentação do *software* instalado;
VII. A organização utilizará controles técnicos em todos os ativos para garantir que apenas *software* autorizado seja executado;
VIII. A organização utilizará ferramenta de gerenciamento de endereços IP - ex.: Dynamic Host Configuration Protocol (DHCP) - para atualizar o inventário de ativos da instituição;
IX. O inventário também deverá incluir atualizações ou remoções dos *softwares*, bem como dos sistemas de informação;
X. As atualizações e novas versões de *softwares* devem ser avaliadas e aprovadas antes da instalação;
XI. Cada ativo de informação (por exemplo, *desktops, laptops*, servidores, *tablets*), quando aplicável, deve ter uma etiqueta afixada ao dispositivo com esse identificador; e
XII. Registre o identificador de ativos da informação juntamente com outras informações relevantes no inventário de TI. Isso inclui:
    a. Identificador de ativos;
    b. Descrição do item;
    c. Fabricante;
    d. Número do modelo;
    e. Número de série;
    f. Localização física do ativo, quando aplicável;
    g. Endereço físico (controle de acesso à mídia (MAC));
    h. Endereço de Protocolo de Internet (IP); e
    i. Data de validade da garantia/vida útil.

15. No caso de *softwares* instalados na organização deve ser registrado no inventário informações como:

I. Título do *software*;
II. Desenvolvedor ou editor de *software*;
III. Data de aquisição;
IV. Data de instalação;
V. Duração do uso;
VI. Versões;
VII. Data de fim do suporte, se conhecida;
VIII. Qualquer informação de licenciamento relevante; e
IX. Data de descomissionamento.

16. Das atribuições do responsável pelo processo de gestão de ativos de TIC (recomenda-se a leitura ao art. 9º da Instrução Normativa GSI nº 3, de 28 de maio de 2021):

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. 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;
VI. Os processos em torno do gerenciamento de mudança e de configuração também serão estabelecidos e monitorados; e
VII. Todos os ativos de informação devem ser devolvidos após o desligamento do órgão.

17. Criticidade do ativo de informação:

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

I. Requisitos legais;
II. Pelo valor financeiro;
III. Pelo seu potencial de agregar valor ao negócio; e
IV. Por sua vida útil.

18. Classificação de Nível de Acesso das Informações:

18.1. 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;

18.2. As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação do IFRO, 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;

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

18.4. 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.

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

19. Manipulação de mídia (A):

19.1. As mídias internas e removíveis também devem ser gerenciadas pelo mesmo procedimento de classificação de ativos de informação usado pela organização;

19.2. As mídias devem ser protegidas contra acesso não autorizado e uso indevido durante o uso e em trânsito, e deve ser descartada com segurança, usando os procedimentos apropriados; e

19.3. As mídias contendo informações confidenciais e internas do IFRO devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

20. USO ACEITÁVEL: 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.

20.1. Os seguintes itens devem ser cobertos nas diretrizes de uso aceitáveis:

I. Uso do computador e dos sistemas de informação;
II. Uso de *softwares* e dados; e
III. Uso da *Internet* e e-mail.

20.2. Como requisito de acesso ao ativo de informação e como componente do treinamento de conscientização de segurança, todos os usuários dos ativos de informação, sejam funcionários ou terceiros, serão obrigados a fornecer aceitação assinada das diretrizes de uso aceitáveis.

DA FINALIDADE

21. Os ativos de TIC devem ser usados estritamente para fins institucionais e por usuários com vínculo institucional que autoriza a utilização da infraestrutura e serviços de TIC.

22. A solicitação de acesso à infraestrutura e serviços de TIC para pessoas sem vínculo deve ser feita apenas pelo gestor do setor interessado, que deverá apresentar justificativa de necessidade para a concessão de tal acesso, juntamente com o Termo de Responsabilidade assinado pelo usuário sem vínculo.

23. A concessão de acesso à infraestrutura e serviços de TIC para usuários sem vínculo fica a critério do setor responsável pelo serviço.

24. Os ativos de *hardware* podem ser compartilhados, mas só podem ser acessados com autenticação individual quando houver requisição de login.

25. A instalação e execução de *softwares* em ativos de *hardware* se restringe a *softwares* autorizados pelo setor de TIC.

26. Em caso de necessidade de instalação de *softwares* adicionais em qualquer ativo de TIC, este deve ser realizado apenas pelo setor de TIC mediante apresentação de solicitação e justificativa.

27. Usuários com permissão de administrador ficam restritos a servidores e terceirizados do setor de TIC, podendo haver concessão da permissão, a critério do setor de TIC, a usuários não integrantes do mesmo.

28. A solicitação de permissão de administrador deve ser feita apresentando a necessidade justificada e, em caso de aprovação, o solicitante deve assinar Termo de Responsabilidade se comprometendo a não instalar *softwares* não autorizados em ativos de TIC sob sua responsabilidade e em ativos que não estão sob sua responsabilidade.

DAS COMPETÊNCIAS DO SETOR DE TIC

29. As Competências do Setor de TIC são:

I. Planejar a aquisição de ativos de TIC, conforme demandas da instituição e observando as orientações da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022;
II. Realizar a conferência dos ativos de TIC a serem recebidos, oriundos de processos de aquisição ou doação, e assinar o termo de recebimento provisório do bem;
III. Realizar toda a configuração necessária em ativos de TIC para plena utilização dos equipamentos e execução das atividades pelos usuários finais;
IV. Garantir que o acesso a ativos de *hardware* seja feito apenas através de autenticação individual quando houver requisição de login, como forma de proteção ao sigilo de dados;
V. Realizar manutenção e dar suporte aos ativos de *hardware* e *software* quando possível e necessário; e
VI. Manter a segurança de informações contidas em discos de armazenamento em casos de descarte ou desfazimento, baixas patrimoniais, ou envios para consertos em empresas externas.

DAS OBRIGAÇÕES DO USUÁRIO

30. As obrigações do Usuário são:

I. Respeitar e seguir as cláusulas ou diretrizes presentes nesta política.
II. Fazer o *backup* de dados não compartilhados nos diretórios em rede, nas máquinas de sua utilização de forma periódica, ou quando houver necessidade de solicitação de suporte, considerando que o *backup* de arquivos pessoais salvos no sistema é de total responsabilidade de seu proprietário, e não do setor de TIC.
III. Não repassar, emprestar, ou entregar ativos de TIC, ou componentes de ativos de TIC, a pessoas sem autorização.
IV. Não realizar por conta própria nenhum tipo de manutenção, formatação ou conserto em ativos de *hardware*.
V. Não realizar o remanejamento de equipamentos de TI sem o consentimento da CPALM ou do setor competente.
VI. Acionar e encaminhar o ativo de TIC para o setor de TIC diante de necessidade de algum tipo de suporte.

30.1. A requisição de equipamentos de TIC será realizada de acordo com o **Fluxograma de Solicitação de Equipamentos de TIC**, constante no ANEXO I desta política.

DAS COMPETÊNCIAS DE GESTORES DE SETORES ADMINISTRATIVOS

31. As competências de Gestores e Setores Administrativos são:

I. Respeitar e seguir as cláusulas ou diretrizes presentes nesta política.
II. Zelar pela guarda, integridade físicas e condições de uso dos ativos de TIC sob sua responsabilidade e de propriedade patrimonial do IFRO.
III. Limitar a utilização de ativos de TIC sob sua responsabilidade a pessoas autorizadas.

31.1. Os equipamentos de TIC, a exemplo de Impressoras, *Switches*, Roteadores e *Access Point* que estiverem instalados dentro de salas que estão fora do espaço físico da TI, ficam sob responsabilidade do gestor da unidade.

DA POLÍTICA DE DESCARTE DE ATIVOS DE TIC

32. A Política de Descarte de ativos tem como objetivo definir processos de descarte de ativos de TIC de modo a garantir a segurança e não divulgação dos dados armazenados nos ativos.

33. Os ativos de dados poderão ser descartados ou destruídos durante o processo de manutenção que inclui formatação para devolução ou realocação do ativo, sendo o *backup* um procedimento de responsabilidade do usuário proprietário ou responsável pelos dados em questão.

34. O setor de TIC sempre presumirá que o *backup* foi realizado pelo responsável antes da submissão do equipamento para descarte, desfazimento ou doação e por isso não fará nenhum tipo de confirmação junto ao responsável acerca da execução do procedimento de *backup*.

35. O processo de formatação ou destruição é aplicado independentemente de o dispositivo em questão estar armazenando dados pessoais ou corporativos.

36. Todos os dispositivos que armazenam ativos de dados serão formatados pelo setor de TIC antes de repasse e descarte, caso o dispositivo possa realizar novas gravações, ou fisicamente destruídos, caso o dispositivo não possa realizar novas gravações.

37. As licenças digitais de aplicações cedidas pelos fabricantes para utilização no instituto não são aptas a sofrer nenhum processo de descarte.

38. As licenças de aplicações obtidas pelo instituto e armazenadas em CDs e DVDs das fabricantes poderão ser descartadas por inservibilidade mediante Relatório de Bem Inservível emitido por técnico do setor de TIC.

39. Os ativos de *hardware* podem ser descartados mediante avaliação do estado do bem e emissão de Relatório de Bem Inservível, ambos feitos por técnicos do setor de TIC.

DAS RESPONSABILIDADES DA COORDENAÇÃO DE PATRIMÔNIO E ALMOXARIFADO

40. É de responsabilidade da CPALM efetuar o recolhimento de bens inservíveis e gerenciar o seu destino de forma a melhor atender os interesses do instituto com base nas normas vigentes.

41. Os bens considerados inservíveis seguirão as políticas de descarte e/ou doação definidas pela CPALM.

DAS DISPOSIÇÕES FINAIS

42. Os pedidos de substituição de ativos de TIC somente serão considerados se estiverem inventariados e possuírem laudo comprovando bem inservível produzido pelo setor de TIC.

43. Unidades em desconformidade com esta política estão impossibilitadas de receber novos equipamentos.

44. O descumprimento a alguma norma desta Política sujeita o usuário infrator a processo administrativo disciplinar.

45. Propostas de alteração desta Política devem ser encaminhadas ao setor de TIC.

46. Esta política deverá ser revisada anualmente pela comissão e atualizada conforme a necessidade.

47. A utilização dos serviços e recursos de TIC no âmbito do IFRO implica na aceitação desta política e de normas complementares e no comprometimento com sua preservação.

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

ANEXO I

FLUXOGRAMA DE SOLICITAÇÃO DE EQUIPAMENTOS DE TIC