

UNIVERSIDADE FEDERAL DO TOCANTINS  
CONSELHO UNIVERSITÁRIO - CONSUNI

Secretaria dos Conselhos Superiores (Socs)  
Bloco IV, Segundo Andar, Câmpus de Palmas  
(63) 3229-4067 | (63) 3229-4238 | socs@uft.edu.br



**RESOLUÇÃO Nº 115, DE 29 MAIO DE 2024 – CONSUNI/UFT**

Estabelece a Política de Gestão de Ativos de Tecnologia da Informação com as diretrizes de orientação, monitoramento e avaliação no âmbito da Universidade Federal do Tocantins (UFT).

O Egrégio Conselho Universitário (Consuni) da Universidade Federal do Tocantins (UFT), reunido em sessão ordinária realizada no dia 29 de maio de 2024, no uso de suas atribuições legais e estatutárias, e

**CONSIDERANDO**, que os riscos decorrentes de falhas na gestão da segurança da informação são de toda ordem e podem representar desde problemas relacionados à integridade de dados públicos e pessoais, passando pelo vazamento de informações sigilosas, confidenciais e pessoais, bem como podendo provocar impactos econômicos negativos em caso de indisponibilidade de serviços ou falhas em sistemas e bases de dados;

**CONSIDERANDO**, o Decreto nº 10.332/2020, que institui a Estratégia de Governo Digital 2020-2022;

**CONSIDERANDO**, a Lei nº 12.527/2011, Lei de Acesso à Informação (LAI);

**CONSIDERANDO**, o art. 46 da Lei Geral de Proteção de Dados, Lei nº 13.709/2018, de 14 de agosto de 2018, que prevê que “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”;

**CONSIDERANDO**, o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação (PNSI), que dispõe sobre a governança da segurança da informação, no âmbito da administração pública federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional;

**CONSIDERANDO**, os incisos I, II e III do Decreto nº 9.573/2018, que aprovou a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC);

**CONSIDERANDO**, os itens 2.3.4 e 2.3.5 do Decreto nº 10.222/2020 -

Estratégia Nacional de Segurança Cibernética (E-CIBER), que tratam da elevação dos níveis de proteção das infraestruturas críticas;

**CONSIDERANDO**, o inciso XXIII, art 2º do Decreto nº 10.046/2019, que trata da Governança no Compartilhamento de Dados (GCD), em especial, das ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

**CONSIDERANDO**, o Capítulo IV da Instrução Normativa nº 03/GSI/PR, de 28 de maio de 2021, que apresenta itens obrigatórios da Segurança da Informação na Administração Pública Federal;

**RESOLVE:**

**Art. 1º** Aprovar a Política de Gestão de Ativos de Tecnologia da Informação com as diretrizes de orientação, monitoramento e avaliação da Universidade Federal do Tocantins (UFT), conforme anexo desta Resolução.

**Art. 2º** A Política de Gestão de Ativos da Universidade Federal do Tocantins observará os princípios, objetivos e diretrizes estabelecidos nesta Política, bem como às disposições constitucionais, legais e regimentais vigentes.

**Art. 3º** As determinações desta política aplicam-se às diretrizes a serem seguidas para a realização da gestão dos ativos de tecnologia da informação, realizadas a partir da vigência deste instrumento, os quais precisam estar adequados a essas determinações.

**Art. 4º** Esta Resolução entra em vigor na data de sua publicação, conforme dados do processo nº 23101.004778/2023-50.

LUÍS EDUARDO BOVOLATO  
Reitor



UNIVERSIDADE FEDERAL DO TOCANTINS

---

**POLÍTICA DE GESTÃO DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO  
COM AS DIRETRIZES DE ORIENTAÇÃO, MONITORAMENTO E  
AVALIAÇÃO NO ÂMBITO DA UNIVERSIDADE FEDERAL DO TOCANTINS  
(UFT).**

Anexo da Resolução nº 115/2024 - Consuni  
Aprovada pelo Conselho Universitário em 29 de maio de 2024.

Palmas-TO,  
2024.



UNIVERSIDADE FEDERAL DO TOCANTINS

ANEXO DA RESOLUÇÃO Nº 115/2024 – CONSUNI

**POLÍTICA DE GESTÃO DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO  
COM AS DIRETRIZES DE ORIENTAÇÃO, MONITORAMENTO E AVALIAÇÃO  
NO ÂMBITO DA UNIVERSIDADE FEDERAL DO TOCANTINS (UFT).**

**COMITÊ DE GOVERNANÇA DIGITAL (CGD)**

**Luís Eduardo Bovolato**

Reitor

**Marcelo Leineker Costa**

Vice-Reitor

**Eduardo José Cezari**

Pró-Reitor de Graduação

**Maria Santana Ferreira dos Santos Milhomem**

Pró-Reitora de Extensão

**Rafhael Sanzio Pimenta**

Pró-Reitor de Pesquisa e Pós-Graduação

**Kherlley Caxias Batista Barbosa**

Pró-Reitor de Assuntos Estudantis

**Eduardo Andrea Lemus Erasmo**

Pró-Reitor de Avaliação e Planejamento

**Ary Henrique Morais de Oliveira**

Pró-Reitor de Tecnologia da Informação e Comunicação

**Michelle Matilde Semiguen Lima Trombini Duarte**

Pró-Reitora de Gestão e Desenvolvimento de Pessoas

**Carlos Alberto Moreira de Araújo Júnior**

Pró-Reitor de Administração e Finanças

**COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CGTIC)**

**Ary Henrique Morais de Oliveira**

Pró-Reitor de Tecnologia da Informação e Comunicação

**Olivia Tozzi Bittencourt**

Diretora de Infraestrutura Tecnológica

**Glauco Batista Sousa**

Coordenador de Segurança da Informação

**Werley Reinaldo Teixeira**

Diretor de Soluções Digitais

**Anna Paula de Sousa Parente Rodrigues**

Coordenadora de Soluções para a Educação

**Samuel Barbosa Costa da Silva**

Coordenador de Soluções para a Gestão

**EQUIPE DE APOIO TÉCNICO**

**Aislan Max Gomes Coelho**

Analista em Tecnologia da Informação

**Jefferson Victor Araújo**

Analista em Tecnologia da Informação

**Juliano Alves Rios**

Analista em Tecnologia da Informação

**Junior Fernandes de Oliveira**

Técnico em Tecnologia da Informação

**Luis Ferreira de Oliveira Junior**

Técnico em Tecnologia da Informação

**Marluzio da Silva Leite**

Analista em Tecnologia da Informação

**Controle de versões:**

1.0	05/06/2023	Coordenação de Segurança da Informação	Versão Inicial do Documento
1.1	28/08/2023	Comitê de Segurança da Informação	Análise e correção do documento
1.2	28/08/2023	Ary Henrique Morais de Oliveira	Análise e correção do documento
1.3	28/08/2023	Comitê Gestor de Tecnologia da Informação e Comunicação	Aprovação no CGTIC

1.4	26/02/2024	Comitê de Governança Digital	Aprovação no CGD
1.5	28/05/2024	Comissão de Legislação e Normas	Aprovação na CLN/CONSUNI
1.6	29/05/2024	Conselho Universitário	Aprovação no Consuni

#### **Contatos:**

Glauco Batista de Sousa	(63) 3229-4032	internet@uft.edu.br
Ediane Dias dos Santos	(63) 3229-4032	protic@uft.edu.br

### **PRINCÍPIOS**

**Art. 1º** Estabelecer padrões para gerenciar ativamente (inventariar, rastrear e corrigir) todos os ativos institucionais conectados à rede, com o objetivo de identificar precisamente quais necessitam ser monitorados e/ou protegidos dentro da instituição, mapeando todos os ativos não autorizados para uma possível remoção ou remediação futura.

**Art. 2º** Atribuir papéis e responsabilidades aos envolvidos nas ações de gestão dos ativos institucionais.

**Art. 3º** Prover a gestão de ativos institucionais pelo processo de aquisição, identificação, rastreamento, manutenção e descarte de um ativo de propriedade de uma instituição.

**Art. 4º** Fornecer os processos e procedimentos para governar o ciclo de vida da gestão dos ativos institucionais enquanto uma instituição estiver usando um ativo. Um inventário deve ser criado e mantido para apoiar a missão da instituição. Este inventário deve ser atual e refletir os ativos atuais de propriedade e operados pela instituição.

**Art. 5º** Manter a continuidade do negócio da UFT, em sua missão como instituição de ensino, pesquisa e extensão, é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de perdas que estão sujeitas a ocorrer de diversas formas, tais como: erro humano, ataques externos, incêndios, falhas de hardware, catástrofes naturais dentre outras.

### **PROPÓSITO**

**Art. 6º** 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. 7º** Manter a segurança da informação da Universidade Federal do Tocantins - UFT, 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.

**Art. 8º** Classificar os ativos de informação da UFT a fim de permitir a definição de níveis de segurança para eles. Cada ativo de informação deverá ter um responsável, no qual realizará a classificação do ativo de informação e deverá ser registrado em uma base de dados gerenciada de forma centralizada.

## **ESCOPO**

**Art. 9º** Esta Política de Gestão de Ativos se aplica a todos os processos de negócios e dados, sistemas de informação e componentes, pessoal e áreas físicas da UFT, para garantir o nível de segurança da informação, privacidade e proteção aos dados determinados pela legislação competente.

**Art. 10.** Esta política se aplica a todos os ativos de informação da UFT, incluindo ativos fora da Instituição, armazenados em um serviço de nuvem. Ativos de informação neste contexto, incluem documentos, base de dados, contratos, documentação de sistemas, procedimentos, manuais, logs de sistemas, planos, guias, programas de computador, servidores, computadores, e-mail, arquivos pessoais e compartilhados, bancos de dados e conteúdo da web específicos.

**Art. 11.** A classificação dos ativos de informação e o escopo desta política serão revisados anualmente.

**Art. 12.** A regulamentação referente a equipamentos pessoais dos usuários, que são utilizados na rede lógica da UFT para fins acadêmicos ou administrativos, será definida em resolução específica.

## **TERMOS E DEFINIÇÕES**

**Art. 13.** Para melhor leitura e compreensão do documento, serão considerados os conceitos e definições constantes no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, apresentadas na PORTARIA GSI/PR nº 93, DE 18 DE OUTUBRO DE 2021.

## **DECLARAÇÕES DA POLÍTICA**

**Art. 14.** Esta política se aplica a todas as unidades e subunidades acadêmicas e administrativas; aos laboratórios de ensino, pesquisa e extensão; a todos os servidores, bolsistas, discentes, terceirizados e cedidos, ou com vínculo a órgãos parceiros da UFT, pautada dos princípios gerais:

I. a Política de Gestão de Ativos de informação deve estar alinhada com à Política de Segurança da Informação e Comunicação da UFT;

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;

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 contêineres de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.

**Art. 15.** Os seguintes ativos de informação devem ser considerados no processo de mapeamento de ativos de informação:

I. Ativos físicos: Equipamentos que compõem os recursos de TIC, como computadores, notebooks, dispositivos móveis, servidores, storages, switches, roteadores, impressoras, pontos de acesso, mídias removíveis, equipamentos de comunicação e conectividade, entre outros e suas respectivas instalações;

II. Ativos de softwares: Todos os sistemas/programas, banco de dados e utilitários desenvolvidos ou adquiridos para serem utilizados nas atividades acadêmicas e administrativas da UFT;

III. Ativos de informação: São os dados armazenados em banco de dados, que podem ser processados para gerar a informação necessária para ações de estratégia institucional.

## **DIRETRIZES**

**Art. 16.** Informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado como segue:

I. a categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade de autorização;

II. a instituição empregará o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo hardware ou software;

III. o inventário também deverá incluir atualizações ou remoções do sistema de informação;

IV. todos os ativos de propriedade da UFT ou que estejam nela instalados (oriundos de projetos, parcerias, etc.) deverão fazer parte do inventário;

V. quando apropriado, os ativos serão agrupados nas seguintes categorias para simplificar a definição das regras desta política:

a) computadores de laboratórios;

b) computadores de servidores técnico-administrativos, docentes e terceirizados.

**Art. 17.** As responsabilidades do proprietário do processo deverão seguir a conformidade do art. 9º da IN GSI/PR nº 3/2021:

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;

VII. todos os ativos de informação devem ser devolvidos após a rescisão do contrato de trabalho;

VIII. toda e qualquer modificação, configuração, atualização ou instalação de hardware ou software nos ativos de TIC, somente poderão ser executadas pelas equipes de TIC da Universidade ou por eles autorizadas mediante documentação pertinente assinada por ambas as partes, onde o autorizador se tornará corresponsável pelo bem.

## **CRITICIDADE DO ATIVO DE INFORMAÇÃO**

**Art. 18.** A criticidade dos ativos de informação críticos da organização é determinado pelo:

- I. requisitos legais;
- II. pelo valor financeiro;
- III. pelo seu potencial de agregar valor ao negócio;
- IV. por sua vida útil.

## **CLASSIFICAÇÃO DAS INFORMAÇÕES**

**Art. 19.** Todos os ativos de informação devem ser classificados de acordo com sua criticidade.

**Art. 20.** As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação da UFT devem ser classificados de acordo com a legislação pertinente (conforme recomendado pela Lei nº 12.527, de 18 de novembro de 2011), podendo ser classificado em uma das seguintes categorias:

I. **Ultrassecreta:** São passíveis de classificação como ultrassegredos, dentre outros, dados, informações ou documentos referentes à soberania e à integridade territorial nacionais, a planos e operações, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade ou do Estado;

II. **Secreta:** São passíveis de classificação como segredos, dentre outros, dados, informações ou documentos referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicas, cujo conhecimento não autorizado possa acarretar dano grave à segurança da UFT, da sociedade ou do Estado;

III. **Reservada:** São passíveis de classificação como confidenciais, dentre outros, dados, informações ou documentos que, no interesse da UFT, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança do UFT, da sociedade ou do Estado.

**Art. 21.** Os ativos de informação serão rotulados e manuseados com base nos procedimentos apropriados de classificação de informações usados pela organização.

## **USO ACEITÁVEL**

**Art. 22.** 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.

**Art. 23.** 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;

III. uso da Internet e e-mail;

IV. uso do telefone;

V. uso de equipamentos e materiais de escritório.

**Art. 24.** 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.

#### **DISPOSIÇÕES FINAIS**

**Art. 25.** Os casos omissos serão dirimidos pela Pró-Reitoria de Tecnologia da Informação e Comunicação e demais unidades envolvidas.

**Art. 26.** Esta Resolução entra em vigor na data de sua publicação conforme dados do processo nº 23101.004778/2023-50.