MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO CEARA

RESOLUÇÃO Nº 06/CATI, DE 27 DE JANEIRO DE 2025

Institui a Política de Gestão de Ativos no âmbito da Universidade Federal do Ceará (UFC).

O REITOR DA UNIVERSIDADE FEDERAL DO CEARÁ, no uso de suas atribuições legais e estatutárias, em atendimento à recomendação expressa do Comitê Administrativo de Tecnologia da Informação e Governança Digital (CATI), em sua reunião de 27 de janeiro de 2025, e considerando a documentação apresentada por meio do processo administrativo SEI nº 23067.002563/2026-19,

RESOLVE:

Art. 1º Instituir a Política de Gestão de Ativos, no âmbito da Universidade Federal do Ceará (UFC), na forma do Anexo desta Resolução.

Art. 2º Esta Resolução entra em vigor na data de sua aprovação.

Reitoria da Universidade Federal do Ceará, em 27 de janeiro de 2025.

CUSTÓDIO LUÍS SILVA DE ALMEIDA
Reitor

Documento assinado eletronicamente por **CUSTODIO LUIS SILVA DE ALMEIDA**, **Reitor**, em 29/01/2026, às 18:59, 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.ufc.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6128464** e o código CRC **BAC47BB2**.

Av. da Universidade, 2853 - (85) 3366-7305
CEP 60020-181 - Fortaleza/CE - http://ufc.br/

UNIVERSIDADE FEDERAL DO CEARÁ

Política de Gestão de Ativos

Versão 1.0

Fortaleza – Janeiro - 2025

Data	Versão	Descrição	Autor
27/01/2025	1.0	Política de Gestão de Ativos	Superintendência de Tecnologia da Informação

Sumário

1 INTRODUÇÃO 6
2 OBJETIVO 7
3 ESCOPO 7
4 TERMOS E DEFINIÇÕES 8
5 REFERÊNCIA LEGAL E DE BOAS PRÁTICAS 10
6 DOS PRINCÍPIOS GERAIS 11
7 DIRETRIZES 12
8 PAPÉIS E RESPONSABILIDADES 15
9 CLASSIFICAÇÃO DOS ATIVOS 16
9.1 Criticidade do ativo de informação 16
9.2 Classificação de Nível de Acesso das Informações: 16
9.3 Manipulação de mídia: 17
9.4 Uso aceitável 17
9.5 Uso não aceitável 18
10 NÃO CONFORMIDADE 19

UNIVERSIDADE FEDERAL DO CEARÁ

POLÍTICA DE GESTÃO DE ATIVOS

Responsável	Superintendência de Tecnologia da Informação
Aprovado por:	Comitê Administrativo de Tecnologia da Informação e Governança Digital da UFC
Políticas Relacionadas	Política de Segurança da Informação e Comunicação - POSIC (UFC)
Localização de armazenamento	https://sti.ufc.br/documentos/politicas-normas-e-resolucoes/politicas-de-privacidade-e-seguranca/
Data de Aprovação	27/01/2025
Data de revisão	
Versão	1.0

1 INTRODUÇÃO

De acordo com a norma NBR ISO 55000, a gestão de ativos é a atividade coordenada de uma instituição para obter valor a partir de seus ativos. Isso envolve equilibrar custos, riscos, oportunidades e benefícios de desempenho para maximizar o valor ao longo do tempo e o retorno sobre o investimento em ativos. Em outras palavras, a gestão de ativos busca encontrar um equilíbrio entre esses fatores para obter o melhor desempenho possível dos ativos e, consequentemente, da instituição como um todo. A obtenção de valor não se limita apenas ao aspecto financeiro, mas também inclui a melhoria da qualidade dos serviços prestados e a satisfação dos usuários.

Considerando a importância estratégica da gestão de ativos, e o vasto conjunto de ativos físicos e intangíveis (que incluem instalações, equipamentos, sistemas de tecnologia da informação, propriedade intelectual, dentre outros) as diretrizes aqui estabelecidas visam garantir que os ativos desta universidade sejam mantidos e atualizados regularmente para que se obtenha o máximo de valor.

Hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.

Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no art.46. da Lei Geral de Proteção de Dados, sancionada em 14 de agosto de 2018:

"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."

A gestão de ativos institucionais é o processo de aquisição, identificação, rastreamento, manutenção e descarte de um ativo de propriedade de uma empresa. A política de gestão de ativos fornece 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.

2 OBJETIVO

O objetivo desta política é garantir que os ativos de informação sejam identificados adequadamente e que os controles de proteção recomendados para estes ativos de informação estejam em vigor.

É essencial mapear e monitorar todos os ativos de informação para aumentar o controle da instituição, facilitar a aplicação de atualizações, implementar controles de segurança e gerenciar riscos, além de auxiliar na recuperação de incidentes.

Para manter a segurança e continuidade do negócio da Universidade Federal do Ceará (UFC), 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.

Os ativos de informação da UFC devem ser classificados 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.

3 ESCOPO

Esta política é aplicável a todos os ativos de informação, incluindo aqueles armazenados em serviços de nuvem, pertencentes à Universidade Federal do Ceará, considerando as normativas que regem a Administração Pública Federal. Os ativos de informação compreendidos nesse contexto são essenciais para a instituição e o escopo desta política poderá ser revisado quando necessário.

4 TERMOS E DEFINIÇÕES

Para fins desta política, as seguintes definições serão adotadas:

a) **Ativo** - Algo ou entidade com valor real ou potencial para uma instituição, incluindo consideração de riscos e passivos. Pode ser tangível ou intangível, físico ou não físico, positivo ou negativo. Os ativos físicos são equipamentos, estoques e propriedades, enquanto os ativos intangíveis incluem contratos, marcas e direitos de propriedade intelectual. Um sistema de ativo também pode ser considerado um ativo;

b) **Ativo 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;

c) **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;

d) **Ciclo de vida do Ativo -** período compreendido a partir da criação do ativo até o fim da vida do ativo;

e) **Competência -** capacidade de aplicar conhecimentos e habilidades para alcançar os resultados pretendidos;

f) **Conformidade ou *Compliance*** - cumprimento de um requisito;

g) **Contêiner dos Ativos De Informação** - local onde se encontra o ativo de informação. Geralmente, um contêiner descreve algum tipo de ativo tecnológico -*hardware, software* ou sistema de informação (mas também pode se referir a pessoas ou mídias como papel, CD-ROM ou DVD-ROM). Um contêiner, portanto, é qualquer tipo de ativo dentro do qual um ativo de informação é armazenado, transportado ou processado. Ele pode ser um único ativo tecnológico (como um servidor), uma coleção de ativos tecnológicos (como uma rede) ou uma coletânea de mídias digitais, entre outros;

h) **Informação documentada -** informações exigidas a serem controladas e mantidas por uma instituição e o meio no qual ela está contida;

i) **Eficácia -** extensão na qual as atividades planejadas são realizadas e os resultados planejados, alcançados;

j) **Gestão de ativos -** atividade coordenada de uma instituição para obter valor a partir dos ativos;

k) **Melhoria contínua -** atividade recorrente para aumentar o desempenho;

l) **Monitoramento -** determinação da condição de um sistema, um processo ou uma atividade;

m) **Não conformidade -** não atendimento de um requisito;

n) **Instituição -** pessoa ou grupo de pessoas que tem suas próprias funções com responsabilidades, autoridades e relacionamentos para atingir os seus objetivos;

o) **Objetivo organizacional -** objetivo abrangente que define o contexto e direção para as atividades de uma instituição;

p) **Plano organizacional -** informação documentada que especifica os programas para atingir os objetivos organizacionais;

q) **Política -** intenções e diretrizes de uma instituição, conforme formalmente expresso pela sua alta direção;

r) **Processo -** conjunto de atividades inter-relacionadas ou interativas que transformam entradas em saídas;

s) **Requisito -** necessidade ou expectativa que é expressa, geralmente, de forma implícita ou obrigatória;

t) **Risco -** efeito da incerteza nos objetivos;

u) **Sistema de gestão de ativos -** sistema de gestão para a gestão de ativos cuja função é estabelecer a política de gestão de ativos e os objetivos da gestão de ativos;

v) **Terceirizar -** fazer um acordo onde uma instituição externa executa parte de uma função ou de um processo de uma instituição;

5 REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Orientação	Secção
Decreto Nº 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo Art.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
Guia do Framework de Privacidade e Segurança da Informação	Controles 1 e 2
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	Gestão da Segurança da Informação
Guias Operacionais SGD	Todos
Instrução Normativa Nº 01/GSI/PR, de 27 de maio de 2020	Art.12, Inciso IV, alínea d
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo II
Instrução Normativa Nº 05/GSI/PR, de 30 de agosto de 2021	Anexo
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
NIST SP 800-53 v4	AC-3, AC-4, AC-16, AC-20, CM-8, CM-9, MP-2, MP-3, PL-4, PM-5, PS-6, RA-2, SC-16
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos;	A.8 (A.8.1., A.8.2., A.8.3.)
Norma Complementar nº 20/IN01/DSIC/GSIPR, (Revisão 01) - Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.	Em sua íntegra
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Enterprise Asset Management Policy Template CIS v8	Em sua íntegra
Software Asset Management Policy Template CIS v8 - November 2022	Em sua íntegra

6 DOS PRINCÍPIOS GERAIS

a) Esta política está alinhada com a Política de Segurança da Informação e Comunicação (POSIC) da UFC.

b) A Política de Gestão de Ativos de informação está alinhada com uma gestão de continuidade de negócios em nível organizacional.

c) 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.

d) As rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação da UFC, a fim de manter o escopo da instituição mapeado e documentado.

e) 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.

f) 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.

g) Os demais planos e normas que tratam da aquisição, gestão, uso e descarte dos ativos de informação deverão estar alinhados com esta política.

h) A gestão de riscos deve ter como escopo a política de gestão de riscos e plano de gestão de riscos da Universidade Federal do Ceará.

Os seguintes ativos de informação devem ser considerados no processo de mapeamento de ativos de informação:

a) Hardware;
b) Software;
c) Ativos de redes de computadores.

7 DIRETRIZES

a) Informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado;

b) A categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade de autorização;

c) A organização empregará o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo hardware ou software;

d) A organização deve assegurar que os ativos de informação inventariados possuam contrato de suporte em vigor;

e) A organização empregará 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;

f) A organização utilizará ferramentas de inventário de software, quando possível, em toda a organização para automatizar a descoberta e documentação do software instalado;

g) A organização assegurará que exista um processo semanal para lidar com ativos não autorizados;

h) A organização utilizará controles técnicos em todos os ativos para garantir que apenas software autorizado seja executado, sendo estes reavaliados semestralmente ou com mais frequência;

i) A organização utilizará controles técnicos para garantir que apenas bibliotecas e scripts autorizados, e assinados digitalmente tenham permissão para serem executados;

j) A organização utilizará ferramenta de gerenciamento de endereços IP - ex.: *Dynamic Host Configuration Protocol* (DHCP) - para atualizar o inventário de ativos da instituição;

k) O inventário também deverá incluir atualizações ou remoções dos softwares, bem como dos sistemas de informação;

l) As atualizações e novas versões de softwares devem ser avaliadas e aprovadas antes da instalação;

m) Registre o identificador de ativos da informação juntamente com outras informações relevantes no inventário de TI. Isso inclui:

1. Identificador do ativo;
2. Configuração do ativo;
3. Fabricante;
4. Número do modelo;
5. Número de série;
6. Nome do usuário responsável pelo ativo, função ou unidade de negócios, quando aplicável.
7. Localização física do ativo na UFC
8. Endereço físico (controle de acesso à mídia (MAC))
9. Endereço de Protocolo de Internet (IP)
10. Qualquer informação de licenciamento relevante
11. No caso de softwares instalados na organização deve ser registrado no inventário informações como:

    a) Título do software;
    b) Desenvolvedor ou editor de software;
    c) Data de instalação;
    d) Versões;
    e) Data de fim do suporte, se conhecida;
    f) Qualquer informação de licenciamento relevante;
    g) Data de descomissionamento.

7.1 Descarte

O descarte envolve o processo de baixa patrimonial 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, devendo considerar:

a) 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 irrecuperáveis;

b) 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;

c) 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;

d) O setor de TI presumirá que o backup de dados armazenados nos ativos de TI foi feito pelo responsável antes de repasse e descarte;

e) 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;

f) Métodos de exclusão de dados confiáveis, como formatação segura devem ser utilizados;

g) Equipamentos entregues diretamente na Superintendência de Tecnologia da Informação (STI) e que sejam considerados irrecuperável/inservível **(DESCARTES)** terão um prazo de 30 dias para que seja realizada sua retirada pelo responsável acompanhado de parecer técnico;

h) Decorridos 30 dias para retirada dos equipamentos sem consertos os mesmos serão considerados **"DESCARTE"** com a retirada de possíveis peças para reutilização, constando no relatório do chamado todo histórico dos procedimentos realizados (***Peças para reuso***);

i) Após a retirada do material a ser reutilizado o equipamento vai ser encaminhado para o setor responsável proceder à baixa patrimonial.

8 PAPÉIS E RESPONSABILIDADES

a) **Gestor de segurança da informação** - Coordenar o processo de mapeamento de ativos de informação, bem como designar um agente responsável pela gestão dos ativos de informação, dentre os servidores efetivos do órgão ou da entidade;

b) **Agente responsável pelo mapeamento dos ativos de informação** - Empregar os mecanismos automatizados para identificar e registrar os ativos de informação, classificar os ativos de informação por nível de criticidade segundo a Política de Classificação da Informação da UFC e Realizar monitoramento dos ativos de informação.

c) **Responsável pelo setor a ser inventariado** - Viabilizar o processo de inventário dos ativos de informação e validar o processo resultante do inventário dos ativos de informação.

d) **Indicado(a) da área de Governança de TI da STI** - monitorar as ações e assegurar a entrega de benefícios.

e) **Usuários** - 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;

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

9 CLASSIFICAÇÃO DOS ATIVOS

9.1 Criticidade do ativo de informação

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

a) Requisitos legais;
b) Pelo valor financeiro;
c) Pelo seu potencial de agregar valor ao negócio;
d) Por sua vida útil

9.2 Classificação de Nível de Acesso das Informações:

a) 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;

b) As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação da Universidade Federal do Ceará, 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;

c) 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;

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

e) 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.

9.3 Manipulação de mídia:

a) A mídia removível também deve ser gerenciada pelo mesmo procedimento de classificação de ativos de informação usado pela organização;

b) 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;

c) A mídia contendo informações confidenciais e internas da UFC devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

9.4 Uso aceitável

É considerado uso aceitável dos recursos de TI:

I. Garantir a segurança e integridade do recurso de TI em uso, mantendo-o nas condições originais. É de responsabilidade dos usuários zelar pela conservação e boas condições da infraestrutura e equipamentos.

II. Comunicar imediatamente ao setor de TI a ocorrência de qualquer anomalia no uso dos recursos de TI.

III. Notificar ao setor de TI quando ocorrerem alterações que venham a afetar o cadastro do usuário como unidade de exercício, ramal, cargo ou função.

IV. Efetuar a manutenção de suas áreas pessoais, como caixa de emails e pastas de armazenamento, evitando ultrapassar o limite estabelecido e garantindo o seu funcionamento contínuo.

V. Armazenar dados e informações da instituição em servidores seguros, conforme orientação do setor de TI para garantir a segurança dos dados, já que o backup é feito apenas nessas unidades. Não há garantia quanto aos dados salvos fora desses servidores. Os arquivos gravados em diretórios temporários das estações de trabalho podem ser acessados por todos os usuários que utilizarem a mesma, portanto não se pode garantir sua integridade e disponibilidade. Poderão ser alterados ou excluídos sem prévio aviso e por qualquer usuário que acessar a estação.

VI. Utilizar senhas que contenham, pelo menos, oito caracteres, compostos de letras, números e símbolos, evitando o uso de nomes, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com o usuário ou palavras constantes em dicionários. As senhas temporárias devem ser alteradas imediatamente. As senhas são sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese.

VII. Alterar as senhas no mínimo a cada trimestre.

9.5 Uso não aceitável

É considerado uso não aceitável dos recursos de TI:

I. Compartilhar informações sigilosas, classificadas ou proprietárias, inclusive senhas, com pessoas ou organizações não-autorizadas.

II. Utilizar para fins estranhos às suas atividades profissionais os recursos de TI colocados a sua disposição pelo Instituto. Esses recursos não devem ser utilizados para fins pessoais, incluindo entre estes o comércio, venda de produtos ou engajamento em atividades comerciais de qualquer natureza, de acordo com a legislação em vigor.

III. Fornecer informações reservadas a terceiros, exceto mediante autorização da administração.

IV. Fumar, comer ou beber próximo aos equipamentos de TI.

V. Difundir através dos recursos de TI, material ofensivo, obsceno, ilegal, antiético, comercial, pessoal, de propaganda, mensagens do tipo corrente, entretenimento, "spam" (envio de mensagem não solicitada), mensagens capazes de colocar em risco a segurança da instituição, propaganda política interna ou externa a UFC.

VI. Utilizar qualquer recurso de TI da UFC, para propagação de trotes, boatos, pornografia, propaganda comercial, religiosa ou político-partidária.

VII. Participar em Listas de Discussão, utilizando o serviço de emails da UFC, que possam abordar assuntos alheios à instituição, suas diretorias e suas gerências, exceto em casos de participação em Listas de Discussão sobre assuntos relacionados às atividades específicas desenvolvidos no órgão público;

VIII. Difundir malware (software malicioso) ou qualquer forma de rotinas de programação prejudiciais ou danosas às estações de trabalho e ao sistema de correio;

IX. Conduzir qualquer tipo de ataque ou atividade de fim malicioso que vise tornar um serviço indisponível, obter vantagem indevida, escalar privilégios, prejudicar outros usuários ou conseguir acesso às informações protegidas.

X. Instalar ou utilizar softwares nos equipamentos da UFC que não estejam devidamente licenciados. É vedada a utilização de softwares que não possuam licenças, sejam elas pagas, gratuitas ou temporárias e/ou que não estejam registrados no nome da instituição.

XI. Armazenar nas estações de trabalho, bem como na pasta pessoal, MP3, filmes, fotos, software(s) e outros arquivos com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria;

XII. Outras atividades que possam afetar de forma negativa a Universidade, servidores, discentes, fornecedores e parceiros.

10 NÃO CONFORMIDADE

Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.