



Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Reitoria

PROCESSO DE GESTÃO DE ATIVOS DE INFORMAÇÃO

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
04/01/2024	1	Elaboração do processo de gestão de ativos de informação.

1. INTRODUÇÃO

O processo de gestão de ativos de informação tem o objetivo de estruturar e manter um registro de ativos de informação, destinado a subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação (BRASIL, 2021). Este processo envolve a identificação, classificação, avaliação, proteção e controle desde a aquisição do ativo de informação até o seu descarte final. Ele deve considerar os objetivos estratégicos do IFTO, seus processos internos, requisitos legais e estrutura organizacional.

Dentro do contexto apresentado, este documento apresenta uma breve introdução, definições, gestão de ativos de informação, papéis e responsabilidades, matriz RACI, indicador de desempenho, processos relacionados, práticas recomendadas e referências. A partir da execução deste processo espera-se gerenciar os ativos de informação com segurança e em conformidade com a legislação no âmbito do administração pública federal.

1.1. Escopo

O processo de gestão de informação abrange uma série de atividades relacionadas à administração e ao controle dos ativos de tecnologia da informação ao longo de seu ciclo de vida, tais como: inventário de ativos, aquisição e provisionamento, gerenciamento de configuração, monitoramento e manutenção, atualizações e upgrades, conformidade e segurança, desativação, disposição e descarte do ativo de TI.

1.2. Objetivos

O processo de gestão de ativo de informação tem o objetivo de estruturar e manter um registro de ativos de informação, destinado a subsidiar os processos de gestão de riscos, de gestão de continuidade e

de gestão de mudanças nos aspectos relativos à segurança da informação. Para que este objetivo seja alcançado são definidos os seguintes objetivos específicos:

- a) rastreamento e inventário: manter um inventário detalhado e preciso de todos os ativos de informação para garantir sua localização, status, propriedade e informações relevantes;
- b) otimização de custos: maximizar o valor dos ativos de informação, procurando reduzir custos desnecessários, seja através da padronização, renegociação de contratos, ou eliminação de ativos obsoletos;
- c) otimização do uso de recursos: garantir que os ativos de informação sejam utilizados de maneira eficiente e eficaz para atender às necessidades do negócio, evitando subutilização ou desperdício de recursos;
- d) redução de custos: gerenciar os ativos de informação de forma a minimizar despesas desnecessárias, seja por meio da otimização de licenciamento de *software*, controle de estoque de *hardware* ou manutenção adequada;
- e) garantia de conformidade: assegurar que os ativos de informação estejam em conformidade com regulamentações, políticas internas e requisitos legais, mitigando riscos de não conformidade;
- f) melhoria da produtividade e desempenho: garantir que os ativos de informação estejam em pleno funcionamento e com desempenho otimizado para manter a produtividade dos usuários;
- g) gestão de riscos: identificar e mitigar os riscos relacionados à segurança, integridade e disponibilidade dos ativos de informação, protegendo a organização contra possíveis ameaças;
- h) planejamento estratégico de tecnologia: auxiliar na tomada de decisões estratégicas sobre a aquisição, atualização ou substituição de ativos de informação, alinhando-os às metas e objetivos organizacionais;
- i) acompanhamento do ciclo de vida dos ativos de informação: gerenciar desde a aquisição até a disposição final dos ativos de informação, garantindo que seu ciclo de vida seja monitorado e otimizado;
- j) maximização do ciclo de vida dos ativos: estender a vida útil dos ativos por meio de manutenção preventiva, atualizações e implementação de práticas de obsolescência gerenciada;
- k) apoio à tomada de decisão estratégica: fornecer informações e dados relevantes para apoiar decisões estratégicas sobre investimentos, atualizações e migrações tecnológicas;
- l) melhoria na produtividade e eficiência: garantir que os ativos de informação estejam disponíveis e funcionando eficientemente para apoiar as operações diárias da organização;
- m) suporte à continuidade do negócio: assegurar que os ativos críticos estejam disponíveis e em pleno funcionamento mesmo diante de eventos imprevistos ou crises;
- n) gestão de fornecedores e contratos: gerenciar efetivamente relacionamentos com fornecedores para garantir que os contratos sejam cumpridos e que a organização receba o melhor valor possível;

- o) melhoria contínua: implementar práticas e processos que permitam a melhoria contínua na gestão dos ativos de informação, adaptando-se às mudanças tecnológicas e às necessidades do negócio; e
- p) conformidade: garantir que os ativos estejam em conformidade com regulamentações e políticas internas, minimizando riscos de segurança, conformidade e financeiros.

1.3. Abrangência

A gestão de ativos de informação abrange um espectro amplo e diversificado de componentes, processos e práticas. Ela engloba todos os ativos relacionados à tecnologia da informação ao longo de seus ciclos de vida, desde a aquisição até o descarte final. Portanto, este processo abrange:

- a) hardware: inclui todos os dispositivos físicos, como servidores, computadores, dispositivos de rede, impressoras, entre outros;
- b) software: envolve todos os sistemas, aplicativos e programas utilizados pela organização, incluindo licenciamento, atualizações, e controle de versões;
- c) dados: refere-se aos ativos de informação, como bancos de dados, informações confidenciais, arquivos de clientes, entre outros, e seu gerenciamento, proteção e conformidade;
- d) recursos humanos: considera as habilidades, conhecimentos e treinamentos necessários para gerenciar, manter e utilizar efetivamente os ativos de informação;
- e) processos e procedimentos: envolve as práticas e políticas estabelecidas para a gestão, utilização e manutenção dos ativos de informação, garantindo conformidade, segurança e eficiência operacional;
- f) gestão financeira: inclui a análise de custos, orçamentos e investimentos relacionados aos ativos de informação, visando a otimização dos recursos financeiros;
- g) segurança da informação: engloba a proteção dos ativos de informação contra ameaças, violações de segurança, e a implementação de medidas de segurança para preservar a integridade, confidencialidade e disponibilidade dos dados;
- h) gestão de mudanças: refere-se à capacidade de gerenciar alterações nos ativos de informação de forma controlada e eficiente, minimizando impactos negativos nos serviços e operações; e
- i) relacionamento com fornecedores: envolve a gestão de contratos, acordos de nível de serviço (SLAs), negociações com fornecedores de *hardware*, *software* e serviços relacionados à TI.

1.4. Benefícios esperados

A execução eficaz do processo de gestão de ativos de informação oferece uma série de benefícios significativos para o IFTO,

tais como:

- a) redução de custos: otimiza o uso de recursos, evita gastos desnecessários, controla licenciamento de *software* e permite uma melhor alocação financeira, resultando em economia de custos;
- b) aumento da eficiência operacional: melhora a produtividade ao garantir que os ativos de informação estejam disponíveis e funcionando adequadamente, reduzindo interrupções e tempo de inatividade;
- c) melhoria na tomada de decisão: fornece dados precisos e atualizados sobre o inventário de ativos, permitindo decisões mais informadas sobre investimentos, atualizações e substituições;
- d) conformidade e mitigação de riscos: assegura conformidade com regulamentações e políticas, além de minimizar riscos de segurança, financeiros e legais associados aos ativos de informação;
- e) aumento da segurança da informação: garante a implementação de práticas de segurança adequadas, protegendo os ativos de informação contra ameaças e vulnerabilidades;
- f) maximização do valor dos ativos: acompanha o ciclo de vida dos ativos para garantir que sejam utilizados da melhor forma possível e prolonga sua vida útil quando apropriado;
- g) melhoria na gestão de fornecedores: facilita negociações mais eficazes, garantindo que os fornecedores de TI cumpram acordos e contratos, melhorando os relacionamentos comerciais;
- h) suporte à estratégia de negócios: alinha os ativos de informação com os objetivos e metas organizacionais, facilitando a inovação e a adaptação às mudanças do mercado;
- i) aprimoramento da gestão de mudanças: facilita a implementação de mudanças de maneira mais controlada e eficiente, minimizando impactos negativos nos serviços; e
- j) melhoria na satisfação do cliente interno e externo: garante que os serviços oferecidos pela TI sejam confiáveis, consistentes e atendam às necessidades dos usuários finais e clientes da organização.

2. DEFINIÇÕES

Para fins de compreensão dos termos utilizados neste processo serão utilizados os seguintes conceitos e definições:

- a) ameaça: conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;
- b) alta administração: representa o mais alto nível estratégico e decisório de um órgão ou entidade, seja ela parte da Administração Pública Federal Direta ou Indireta.
- c) 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;
- d) ativo: tudo que tenha valor para a organização, material ou não;

e) 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;

f) *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;

g) 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;

h) 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;

i) 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;

j) 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;

k) 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;

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

m) 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;

n) 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;

o) descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

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

q) documento: unidade de registro de informações, qualquer que seja o suporte ou o formato;

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

s) eliminação: exclusão de dado ou conjunto de dados, armazenados em banco de dados, independentemente do procedimento empregado;

t) 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;

u) 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;

v) 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;

x) 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;

w) 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;

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

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

a1) internet: rede global, composta pela interligação de inúmeras redes;

b1) medidas de segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

c1) política: intenções e diretrizes globais formalmente expressas pela direção;

d1) 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;

e1) 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;

f1) 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;

g1) recursos de processamento da informação: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem;

h1) 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;

i1) 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;

j1) segurança da informação: preservação da confidencialidade, integridade, disponibilidade, adicionalmente outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

k1) 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;

l1) SI: sigla de segurança da informação;

m1) 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;

n1) 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

o1) 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.

3. GESTÃO DE ATIVOS DE INFORMAÇÃO

A gestão de ativos de informação é o processo de identificação, classificação e proteção de ativos de informação críticos do IFTO. No IFTO este processo é um conjunto de práticas e procedimentos para identificar, avaliar, classificar, proteger, armazenar, preservar e dispor de informações de valor para o instituto.

3.1. Processo de gestão de ativos de informação

A gestão de ativos de informação envolve várias fases para

garantir a eficiente administração dos recursos tecnológicos ao longo de seu ciclo de vida. Este processo envolve atividades para a identificação dos ativos, inventário, classificação e categorização, avaliação e valoração, monitoramento e controle, manutenção e atualização, gestão de mudanças, garantia de conformidade e disposição adequada dos ativos de informação. A figura 1 apresenta as 5 (cinco) fases que compõem este processo.

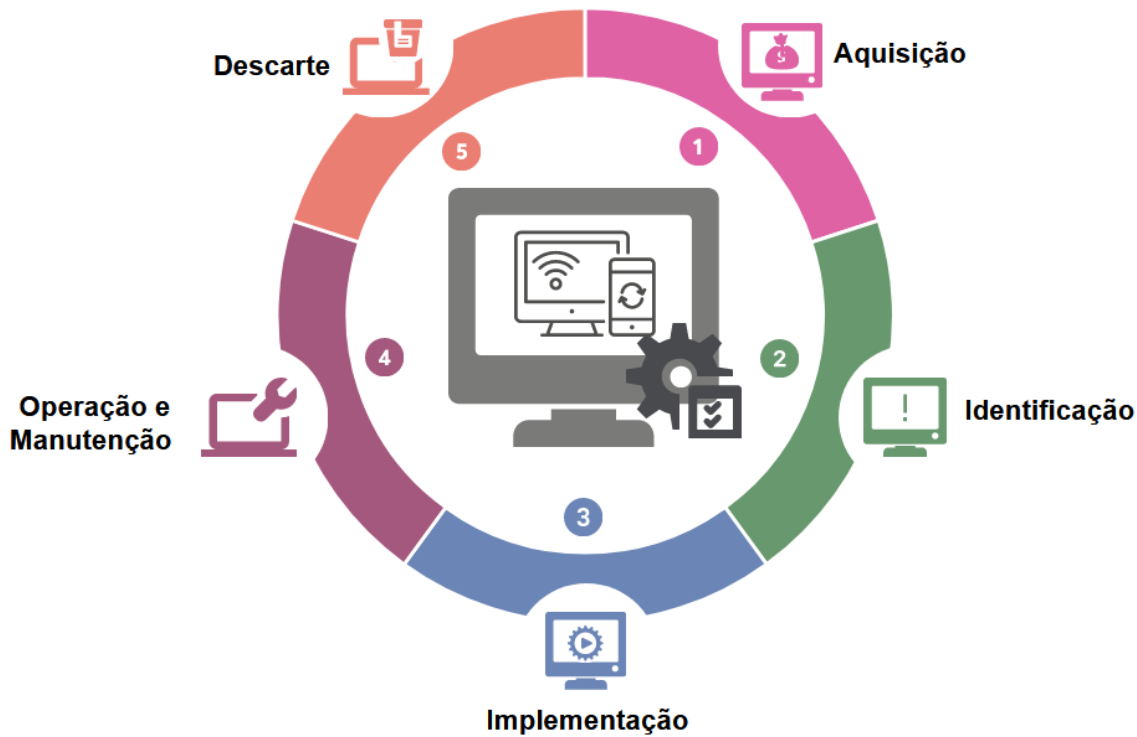


Figura 1 - Processo de gestão de ativos de informação

A figura 1 apresenta a entrada, fases e saída do processo de gestão de ativos de informação do IFTO. A tabela 1 faz o resumo do processo de gestão de ativos de informação.

Tabela 1 - Detalhamento do processo de gestão de ativos de informação

Processo de gestão de ativos de informação	
Descrição	Processo responsável pela gestão de ativos de informação.
Entrada	Ativo de Informação.
Fases	1. Aquisição. 2. Identificação 3. Implementação. 4. Operação e manutenção. 5. Descarte.
Saída	Inventário de ativos de informação.

Fonte: Diretoria de Tecnologia da Informação

3.1. Aquisição

Esta fase refere-se ao processo de obtenção e incorporação de ativos de informação relevantes para o IFTO. Esta fase contribui para a

construção de uma base sólida de recursos de informação que impulsionam a tomada de decisões e o desempenho organizacional. Nesta fase podem ser realizadas as seguintes atividades:

- a) identificar as necessidades de TI da organização, estabelecer requisitos para os ativos, determinar orçamentos e definir prazos para aquisição;
- b) compreender as necessidades operacionais e estratégicas para determinar as especificações técnicas dos ativos de TI a serem adquiridos;
- c) analisar o mercado para identificar fornecedores potenciais que ofereçam os produtos ou serviços que atendam aos requisitos definidos;
- d) comparar diferentes opções de produtos ou serviços, considerando critérios como desempenho, custo, suporte pós-venda, prazos de entrega e adequação às necessidades da organização;
- e) definir cláusulas de contratos, termos de pagamento, garantias e condições de suporte com os fornecedores escolhidos;
- f) selecionar fornecedores;
- g) executar o processo de aquisição/contratação; e
- h) realizar testes preliminares para garantir que atendam aos requisitos e estejam em conformidade com regulamentações, normas internas e externas, mitigando riscos de não conformidade.

3.2. Identificação

Esta fase tem o objetivo principal de mapear e catalogar todos os ativos de informação do IFTO, desde *hardware*, *software*, até dados e recursos humanos relacionados à gestão desses ativos. A fase é essencial para estabelecer as bases sólidas necessárias para a gestão eficaz dos ativos de informação ao longo de seu ciclo de vida. Nesta fase podem ser realizadas as seguintes atividades:

- a) identificar e listar todos os ativos de informação existentes na organização, incluindo *hardware*, *software*, dados, redes, equipamentos, entre outros;
- b) classificar os ativos de acordo com categorias específicas, como equipamentos de rede, servidores, licenças de software, etc, para facilitar o gerenciamento e a compreensão;
- c) criar documentação detalhada para cada ativo, incluindo informações como número de série, especificações técnicas, localização física, status de propriedade e configurações;
- d) avaliar a importância de cada ativo para o funcionamento e os objetivos da organização, identificando os ativos críticos e aqueles que podem ser considerados menos prioritários;
- e) analisar como os ativos estão sendo utilizados, incluindo seu uso por departamentos ou equipes específicas, a frequência de uso e a eficiência do uso em relação aos objetivos organizacionais;
- f) identificar potenciais vulnerabilidades ou riscos associados a cada

ativo, seja em termos de segurança da informação, conformidade regulatória ou riscos operacionais;

g) determinar quem é responsável por cada ativo de informação, seja para sua manutenção, atualização, suporte ou operação diária;

h) utilizar *softwares* ou sistemas de gerenciamento de ativos de informação para facilitar o acompanhamento e a atualização contínua do inventário; e

i) realizar revisões periódicas do inventário de ativos para garantir que esteja sempre atualizado e refletindo a situação real dos recursos de TI da organização.

3.3. Implementação

Esta fase traduz os objetivos estratégicos e táticos da gestão de ativos de informação em ações concretas. Nesta fase, o IFTO começa a aplicar as medidas e controles necessários para gerenciar, proteger e utilizar eficientemente seus ativos de informação. Nesta fase podem ser realizadas as seguintes atividades:

a) desenvolvimento e implementação de políticas e procedimentos específicos para o gerenciamento de ativos de informação. Estas diretrizes estabelecem regras práticas que devem ser seguidas em relação à coleta, armazenamento, acesso, compartilhamento e descarte de informações;

b) condução de programas de educação e conscientização para garantir que os membros do IFTO compreendam a importância dos ativos de informação e estejam cientes das práticas recomendadas e das políticas de segurança;

c) implementação de controles de acesso adequados para garantir que apenas indivíduos autorizados tenham acesso aos ativos de informação. Isso pode envolver a utilização de sistemas de autenticação, autorização e monitoramento de atividades;

d) implementação de tecnologias e ferramentas necessárias para proteger os ativos de informação. Isso pode incluir *firewalls*, sistemas de detecção de intrusões, antivírus, criptografia e outras soluções de segurança da informação;

e) estabelecimento de processos robustos de *backup* e recuperação para garantir a disponibilidade contínua dos ativos de informação, mesmo em caso de falhas de sistemas, desastres naturais ou ataques cibernéticos;

f) implementação de sistemas de monitoramento contínuo e auditoria para rastrear atividades relacionadas aos ativos de informação. Isso ajuda a identificar comportamentos suspeitos, garantindo a detecção precoce de possíveis ameaças;

g) oferta de treinamento contínuo para os usuários, garantindo que eles estejam atualizados sobre as melhores práticas de segurança da informação e estejam cientes das últimas ameaças e vulnerabilidades;

h) implementação de processos de gestão de mudanças para garantir que qualquer modificação nos sistemas, processos ou procedimentos

relacionados aos ativos de informação seja realizada de maneira controlada e documentada;

- i) garantia de que as práticas de implementação estejam em conformidade com as regulamentações e normas relevantes do setor. Isso é crucial para evitar penalidades e garantir a reputação da organização; e
- j) desenvolvimento e implementação de planos de resposta a incidentes para lidar com qualquer violação de segurança ou evento adverso relacionado aos ativos de informação. Isso inclui ações coordenadas para minimizar o impacto e recuperar os sistemas afetados.

3.4. Operação e manutenção

Fase responsável pela execução diária das atividades relacionadas aos ativos de informação, garantindo sua segurança, integridade, disponibilidade e eficiência operacional. Ela é essencial para garantir que os ativos de informação permaneçam seguros, atualizados e alinhados com as necessidades operacionais do IFTO. Nesta fase podem ser realizadas as seguintes atividades:

- a) estabelecimento de sistemas de monitoramento contínuo para acompanhar a integridade e o desempenho dos ativos de informação. Isso inclui a vigilância de sistemas, redes e outros componentes para identificar possíveis anomalias ou ameaças;
- b) implementação de práticas de manutenção preventiva e atualização para garantir o funcionamento adequado dos ativos ao longo do tempo;
- c) implementação de procedimentos eficazes de gestão de incidentes para responder prontamente a qualquer violação de segurança, interrupção do serviço ou outro evento adverso que possa afetar os ativos de informação;
- d) realização de backups regularmente e testar os procedimentos de recuperação para garantir a pronta restauração dos ativos de informação em caso de perda de dados ou falhas no sistema;
- e) aplicação regular de atualizações de *software* e *patches* de segurança para garantir que os sistemas e aplicativos estejam protegidos contra vulnerabilidades conhecidas;
- f) controle rigoroso sobre as configurações dos sistemas, garantindo que apenas configurações seguras e aprovadas estejam em vigor. Isso reduz o risco de exploração de vulnerabilidades devido a configurações inadequadas;
- g) treinamento contínuo para os membros da equipe, mantendo-os atualizados sobre as últimas ameaças, práticas recomendadas de segurança e procedimentos operacionais relacionados aos ativos de informação;
- h) realização de avaliações regulares de riscos para identificar e mitigar novas ameaças ou mudanças nas condições operacionais que possam afetar os ativos de informação;
- i) revisão e atualização regular de políticas e controles de acesso para garantir que apenas usuários autorizados tenham acesso aos ativos de

informação conforme necessário para suas funções;

j) revisão periódica de políticas e procedimentos de segurança da informação para garantir que estejam alinhados com as mudanças nos ambientes operacionais e nas ameaças emergentes;

k) gerenciamento de alterações nos ativos, seja por atualizações, substituições ou novas aquisições, assegurando uma transição suave e minimizando impactos adversos; e

l) identificação de oportunidades de melhoria contínua nos processos, controles e práticas relacionadas aos ativos de informação. Isso pode envolver a implementação de melhores práticas da indústria, adoção de novas tecnologias ou ajustes nas políticas de segurança.

3.5. Descarte

Nesta fase os ativos de informação são adequadamente desativados, removidos e/ou eliminados. Essa fase é crítica para garantir a segurança da informação e o cumprimento de regulamentações relacionadas à privacidade e proteção de dados.

Descarte refere-se à eliminação adequada de informações confidenciais ou senhas de acesso em dispositivos eletrônicos, como computadores, smartphones, discos rígidos, entre outros, a fim de evitar o acesso não autorizado a dados sensíveis. Nesta fase podem ser realizadas as seguintes atividades:

a) avaliação do ciclo de vida de cada ativo de informação para determinar quando ele atinge o final de sua utilidade operacional. Isso pode envolver a definição de critérios específicos, como obsolescência tecnológica, irrelevância operacional ou expiração de regulamentações;

b) classificação dos ativos de informação com base em sua sensibilidade e na importância para a organização. Isso ajuda a determinar o nível de cuidado necessário durante o processo de descarte;

c) estabelecimento de procedimentos seguros para o descarte de diferentes tipos de ativos, considerando fatores como a destruição física de mídias, a exclusão segura de dados em sistemas eletrônicos e a documentação apropriada de todo o processo;

d) garantir que as mídias físicas que armazenam informações sensíveis sejam destruídas de maneira segura. Isso pode envolver a trituração de discos rígidos, a destruição de documentos físicos ou a certificação de que dispositivos de armazenamento não são reutilizados sem a devida sanitização;

e) implementação de procedimentos seguros para a exclusão de dados em sistemas eletrônicos, garantindo que as informações não possam ser recuperadas após o processo de descarte;

f) manutenção de registros detalhados de todos os ativos descartados, incluindo as razões para o descarte, os métodos utilizados e a data da eliminação. Essa documentação é valiosa para fins de conformidade regulatória e auditoria;

- g) garantia de que o processo de descarte esteja em conformidade com as regulamentações e leis locais e internacionais relacionadas à privacidade e proteção de dados;
- h) comunicação interna sobre os procedimentos de descarte seguro aos colaboradores para garantir que todos estejam cientes da importância de seguir as diretrizes estabelecidas;
- i) fornecimento de treinamento regular aos colaboradores sobre os procedimentos de descarte seguro, enfatizando a responsabilidade individual na preservação da segurança da informação; e
- j) realização de avaliações de riscos relacionadas ao descarte de ativos de informação para identificar possíveis ameaças e vulnerabilidades no processo.

4. PAPÉIS E RESPONSABILIDADES

Um papel é um conjunto de responsabilidades, atividades e autoridades definidas em um processo e atribuídas a uma pessoa, equipe ou função. Os papéis e responsabilidades envolvidos no processo de gestão de ativos de informação são:

4.1. Alta Administração

Representa o mais alto nível estratégico e decisório de um órgão ou entidade, seja ela parte da administração pública federal. Compete ao representante deste nível as seguintes responsabilidades:

- a) prover a orientação e o apoio necessário às ações de gestão de ativos de informação, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes; e
- b) destinar recursos (humanos, tecnológicos e financeiros) para a execução da gestão de ativos de informação no âmbito do IFTO.

4.2. Comitê de Segurança da Informação

Grupo de pessoas que representam áreas finalísticas do IFTO. Compete a este grupo de pessoas as seguintes responsabilidades:

- a) deliberar sobre política e norma interna complementar sobre gestão de ativos de informação;
- b) assessorar a implementação das ações de gestão de ativos de informação; e
- c) constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre gestão de ativos de informação.

4.3. Gestor de Tecnologia da Informação

Servidor designado para gerir a Tecnologia da Informação. Compete à esta pessoa a seguinte responsabilidade:

a) 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.

4.4. Gestor de Segurança da Informação

Servidor designado para gerir a segurança da informação. Compete ao Gestor de Segurança da Informação as seguintes responsabilidades:

a) coordenar a elaboração da política de gestão de ativos de informação e da norma interna de complementar, observadas a legislação pertinente exaradas pelo gabinete de segurança institucional da presidência da república;

b) assessorar a alta administração na implantação da política de gestão de ativos de informação associados à TI;

c) designar um agente responsável pela gestão de ativos de informação, dentre os servidores efetivos do IFTO;

d) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à gestão de ativos de informação;

e) propor recursos necessários às ações de gestão de ativos de informação;

f) verificar os resultados dos trabalhos de auditoria sobre a gestão de ativos de informação; e

g) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos relacionados à gestão de ativos de informação.

4.5. Equipe de Tratamento e Resposta à Incidentes Cibernéticos

Grupo de pessoas composto por servidores públicos civis ocupantes de cargo efetivo, com capacitação técnica compatível com as atividades dessa equipe. Compete à estas pessoas as seguintes responsabilidades:

a) deliberar sobre procedimentos internos para gestão de ativos de informação;

b) receber, analisar e responder às notificações e atividades relacionadas à ativos institucionais;

c) desenvolver as atividades de prevenção, tratamento e resposta a incidentes relacionados à ativos de informação; e

d) propor diretrizes e responsabilidades para a política e norma interna complementar de gestão de ativos de informação.

4.6. Setor de TI (Diretoria de Tecnologia da Informação e demais setores de TI das unidades do IFTO)

Agente responsável pela gestão dos ativos de informação. Compete à Diretoria de Tecnologia da Informação e demais setores de TI das unidades do IFTO as seguintes responsabilidades:

- a) definir características técnicas e funcionalidades de ativos de informação;
- b) conferir os ativos de informação a serem recebidos, oriundos de processos de aquisição ou doação e assinar os termos de recebimento provisório e definitivo;
- c) instalar e configurar os ativos de informação para o uso seguro;
- d) identificar e classificar os ativos de informação por nível de criticidade;
- e) identificar potenciais ameaças e vulnerabilidades aos ativos de informação;
- f) identificar vulnerabilidades dos ativos de informação;
- g) 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;
- h) avaliar os riscos relacionados aos ativos de informação ou do grupo de ativos de informação;
- i) proceder à análise e redistribuição de ativos de informação, considerando demanda setoriais e perfis de utilização de *hardware e software*;
- j) apoiar a alta administração no processo de disponibilização de bens e ativos de informação;
- k) realizar manutenções de *hardware e software* e dar suporte técnico operacional quando necessário em ativos de informação;
- l) homologar os *softwares* a serem utilizados em âmbito institucional;
- m) prover condições para que os *softwares* instalados em ativos de TI possam ser atualizados em suas respectivas versões mais recentes;
- n) proteger os ativos de informação contra violações de segurança da informação;
- o) prover a infraestrutura de inventário eletrônico automatizado dos equipamentos;
- p) definir as características da obsolescência de ativos de informação;
- q) definir as características de perfis de usuários correlacionando-os com os recursos mínimos de performance dos ativos de informação;
- r) definir taxa de renovação anual de ativos de informação considerando as demandas institucionais alinhadas como o Comitê Gestor de TI; e
- s) realizar a análise e, quando aplicável, emitir o laudo de constatação de bem inservível para ativos de informação;
- t) zelar pela segurança da informação contidas nos ativos de informação do IFTO por meio de:

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

II - 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.

4.7. Usuários

Pessoa que utiliza os ativos de informação. Compete aos usuários as seguintes responsabilidades:

- a) atender aos princípios e diretrizes contidos nesta política, incluindo norma interna complementar sobre gestão de ativos de informação;
- b) guiar-se pelos princípios de confidencialidade, autenticidade, integridade, não repúdio, conformidade, controle de acesso e disponibilidade no decorrer de suas atividades;
- c) utilizar os ativos institucionais prioritariamente para a realização das atividades desempenhadas nos limites da ética, razoabilidade e legalidade;
- d) realizar *backup* de dados pessoais armazenados em ativos de informação periodicamente ou quando houver necessidade de formatação do sistema operacional;
- e) não entregar os computadores, componentes internos, como HDs, e equipamentos em geral a pessoas sem autorização;
- f) não realizar por conta própria nenhum tipo de manutenção, formatação ou conserto em ativos de informação; e
- g) devolver todos os ativos de informação que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.

4.8. Responsáveis pelos setores do IFTO

Compete aos responsáveis pelos setores do IFTO as seguintes responsabilidades:

- a) zelar pela guarda, integridade física e condições de uso dos ativos institucionais sob sua responsabilidade e de propriedade patrimonial do IFTO;
- b) manter armazenamento seguro e fazer o *backup* periódico, ou quando houver necessidade de solicitação de suporte, de dados corporativos sob sua guarda; e
- c) limitar a utilização de ativos institucionais sob sua responsabilidade a pessoas autorizadas.

4.9. Responsáveis pelo setor de Patrimônio

Compete ao responsável pelo setor de Patrimônio as seguintes responsabilidades:

- a) 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
- b) realizar os procedimentos institucionais adequados para o descarte seguro de ativos institucionais.

5. MATRIZ RACI

A matriz RACI apresentada na tabela 2 é utilizada para definir com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades do processo. A sigla RACI significa, em inglês: *responsible, accountable, consulted e informed*.

a) responsible (responsável): pessoa, função ou unidade organizacional responsável pela execução de uma atividade no âmbito de um processo;

b) accountable (responsabilizado): dono da atividade, deverá fornecer os meios para que a atividade possa ser executada, e será responsabilizado caso a atividade não alcance os seus objetivos; cada atividade só pode possuir um *accountable*;

c) consulted (consultado): pessoas que deverão ser consultadas durante a execução da atividade; as informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade; e

d) informed (informado): pessoas que serão informadas acerca do progresso da execução da atividade.

Tabela 2 - Matriz de Responsabilidades

Fase	AA	CSI	GSI	ETIR	STI	U	RS	RP
Aquisição	A	C	C	C	R	I	I	I
Identificação	A	C	C	C	R	I	I	I
Implementação	A	C	C	C	R	I	I	I
Operação e Manutenção	A	C	C	C	R	I	I	I
Descarte	A	I	I	I	C	I	I	R

Fonte: Diretoria de Tecnologia da Informação

Legenda:

AA: Alta Administração.

CSI: Comitê de Segurança da Informação.

GSI: Gestor de Segurança da Informação.

ETIR: Equipe de Tratamento e Resposta a Incidentes Cibernéticos.

STI: Setor de Tecnologia da Informação (Diretoria de Tecnologia da Informação e setores de TI das demais unidades do IFTO).

U: Usuários.

RS: Responsáveis pelos setores do IFTO.

RP: Responsáveis pelo setor de Patrimônio.

6. INDICADOR DE DESEMPENHO

O processo deve ser monitorado e avaliado periodicamente através de indicador de desempenho de forma a realizar eventuais ajustes necessários. Esse monitoramento tem como objetivo acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. A tabela 3 apresenta o indicador de desempenho do processo.

Tabela 3 - Indicador de Desempenho

Indicador	Número de ativos de informação gerenciados a cada ano.
Descrição	Identificar a quantidade de ativos de informação são gerenciados pela DTI.
Objetivo	Gerenciar ativos de informação.
Periodicidade	Anual.
Fonte	GLPI
Fórmula	Total de ativos de informação.
Meta	Aumentar o número de ativos de informação gerenciados pelo GLPI.

Fonte: Diretoria de Tecnologia da Informação

7. PROCESSOS RELACIONADOS

Para que a abordagem de segurança da informação seja efetiva, o processo de gestão de ativos de informação está interligado à outros processos que compõem o Sistema de Gestão de Segurança da Informação (SGSI-IFTO). A figura 2 apresenta estes processos.



Figura 2 - Processos que compõem o SGSI-IFTO

8. PRÁTICAS RECOMENDADAS

Para que este processo possa ser executado em eficiência faz-se necessária a observação das seguintes recomendações:

1. O IFTO deve identificar as informações críticas que os ativos de informação armazenam, processam ou transmitem.
2. O IFTO deve estabelecer uma política de gestão de ativos de informação com o objetivo de garantir que os ativos de informação sejam identificados adequadamente e que os controles de proteção recomendados sejam implementados visando a garantia da disponibilidade e a integridade dos ativos de informação no IFTO para a plena e adequada prestação de serviços durante todo o seu ciclo de vida.
3. Uma norma sobre o uso seguro de recursos de TI deve ser estabelecida, documentada e analisada continuamente.
4. Regras e procedimentos para aquisição, uso, manutenção, transferência e descarte de ativos de informação devem ser identificadas, documentadas e implementadas para que sejam permitidos o uso de informações e de ativos associados aos recursos de processamento da informação.
5. A gestão de ativos de informação deve envolver 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.
6. O IFTO deve manter um inventário atualizado contendo todos os ativos

de informação, associados à informação, incluindo *hardware*, *software*, dados e dispositivos conectados à rede deve ser estabelecido, documentado e atualizado continuamente.

7. O processo de mapeamento de ativos de informação no IFTO deve considerar, preliminarmente os objetivos estratégicos do instituto, seus processos internos, os requisitos legais, planos institucionais e sua estrutura organizacional.

8. O IFTO deve implementar controles de acesso físicos e lógicos à informação e aos ativos associados à informação que são por ela gerenciados ou custodiados, com vistas a proteger adequadamente a confidencialidade das informações não públicas e a integridade e a disponibilidade das informações consideradas críticas para o negócio.

9. O processo de gestão de ativos de informação 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.

10. Um procedimento operacional padrão para operação e manutenção de ativos de informação deve ser estabelecido, documentado e analisado continuamente.

11. A gestão dos os *softwares* (sistemas operacionais e aplicações) instalados na rede do IFTO 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.

12. A aquisição de ativos de informação deve ser pautada por normativa pertinente no âmbito da administração pública federal.

13. 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, documentado e atualizado.

14. O IFTO deve gerenciar (inventariar e controlar) os *softwares* instalados nos dispositivos conectados em sua rede.

15. O IFTO deve implementar configurações seguras em seus ativos de *software*, de *hardware* e de rede críticos para o negócio.

16. Um procedimento padronizado de configuração segura deve ser estabelecido, documentado e atualizado continuamente para todos os ativos de informação.

17. As rotinas de implementação e configuração de ativos de informação devem ser estabelecidas, padronizadas, documentadas e atualizadas continuamente.

18. O IFTO deve aplicar controles compensatórios para o uso de privilégios administrativos em seus ativos de *software*, de *hardware* e de rede críticos para o negócio.

19. Controles de acesso devem ser implementados e mantidos continuamente para limitar o acesso aos ativos de informação apenas a usuários autorizados.

20. Controles técnicos devem ser implementados em ativos de informação

para garantir que apenas *softwares* autorizados sejam executados e apenas bibliotecas e *scripts* autorizados, e assinados digitalmente tenham permissão para serem executados.

21. Serviços, *softwares* e aplicativos desnecessários devem ser desinstalados ou desativados nos ativos de informação.

22. Sempre que possível os ativos de informação devem ser testados para avaliar a eficácia e a resiliência dos controles de segurança da informação.

23. Medidas de segurança para ativos de informação 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.

24. O IFTO deve manter, monitorar e analisar logs de auditoria dos ativos de *software*, de *hardware* e de rede críticos para o negócio.

25. Sistemas de monitoramento contínuo para detectar atividades incomuns ou padrões de tráfego suspeitos nos ativos de informação devem ser implementados.

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

27. 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 de informação.

28. O IFTO deve gerenciar vulnerabilidades técnicas em seus ativos de *software*, de *hardware* e de rede críticos para o negócio.

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

30. Fornecer treinamento regular para os funcionários sobre práticas de segurança da informação, conscientizando-os sobre a importância de proteger os ativos de informação.

31. Implementar controles de acesso rigorosos para garantir que apenas usuários autorizados tenham acesso aos ativos de informação necessários para suas funções.

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

33. O IFTO deve implementar procedimentos seguros para o descarte de ativos de informação no final de seu ciclo de vida, garantindo que dados sensíveis sejam eliminados de maneira segura.

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

35. Manter documentação completa e precisa sobre todos os ativos de informação, seus proprietários, histórico de mudanças e eventos de segurança relevantes.

36. Buscar constantemente oportunidades de melhoria na gestão de ativos de informação, incorporando *feedback*, aprendizado com incidentes e atualizações tecnológicas.

9. REFERÊNCIAS

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa GSI/PR N 3, de 28 de maio de 2021.** Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

ANEXO I

Inventário de ativos de informação associados à informação

Ativo associado a informação	Informação crítica	Responsável
E-mail institucional	- Mensagens - Documentos Eletrônicos - Imagens - Vídeos	Diretoria de Tecnologia da Informação
Portal Institucional	- Documentos Eletrônicos - Imagens - Vídeos	Diretoria de Comunicação
Conferência web	- Vídeos	RNP
Eduplay	- Vídeos	RNP
Firewall	- Regras de segurança da rede	Área de Tecnologia da Informação
File Sender	- Documentos Eletrônicos	RNP
SUAP	- Documentos Eletrônicos - Base de dados	Diretoria de Tecnologia da Informação
SIGA-EPCT	- Documentos Eletrônicos - Base de dados	Diretoria de Tecnologia da Informação
SEI	- Documentos Eletrônicos - Base de dados	Diretoria de Tecnologia da Informação
Sistemas Integrados	- Documentos Eletrônicos - Base de dados	Diretoria de Tecnologia da Informação
Sophia Biblioteca	- Base de Dados	Diretoria de Tecnologia da Informação
Moodle	- Base de dados - Documentos Eletrônicos - Vídeos - Imagens	Diretoria de Tecnologia da Informação
Computadores	- Documentos Eletrônicos - Vídeos - Imagens	Área de Tecnologia da Informação
Notebooks	- Documentos Eletrônicos - Vídeos - Imagens	Área de Diretoria de Tecnologia da Informação

Netbooks	- Documentos Eletrônicos - Vídeos - Imagens	Área de Diretoria de Tecnologia da Informação
Tablets	- Documentos Eletrônicos - Vídeos - Imagens	Área de Diretoria de Tecnologia da Informação
Servidores	- Documentos Eletrônicos - Vídeos - Imagens	Área de Diretoria de Tecnologia da Informação



Documento assinado eletronicamente por **Fabiana Ferreira Cardoso, Gestora de Segurança da Informação**, em 04/01/2024, às 16:47, 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.iftto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2235382** e o código CRC **8C47B657**.

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
portal.iftto.edu.br — reitoria@iftto.edu.br

Referência: Processo nº
23235.004528/2023-02

SEI nº 2235382