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

PROCESSO DE GESTÃO DE DADOS

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
05/01/2024	1	Elaboração do processo de gestão de dados.

1. INTRODUÇÃO

O processo de gestão de dados envolve uma série de etapas inter-relacionadas que visam garantir que os dados sejam coletados, armazenados, processados, protegidos, utilizados e eliminados de maneira eficiente e segura ao longo do seu ciclo de vida. Este processo envolve o planejamento e estratégia para o uso de dados, a coleta, armazenamento, processamento, análise, compartilhamento, gestão da qualidade, segurança e privacidade, monitoramento, melhoria contínua, educação e conscientização e eliminação segura dos dados.

O objetivo central da gestão de dados no IFTO é utilizar de forma estratégica as informações disponíveis para aprimorar os processos educacionais, administrativos e de tomada de decisões, além de garantir a segurança e conformidade com as regulamentações. Este processo é considerado fundamental para garantir que a informação seja gerenciada de forma protegida contra riscos e utilizada de forma a agregar valor aos objetivos de uma organização. Ele se adapta a mudanças nas necessidades, regulamentações e avanços tecnológicos ao longo do tempo.

Dentro do contexto apresentado, este documento está estruturado em uma breve introdução, definições, gestão de dados, papéis e responsabilidades, matriz RACI, indicador de desempenho, processos relacionados, práticas recomendadas e referências.

1.1. Escopo

O escopo do processo de gestão de dados abrange várias áreas-chave do IFTO. Ele envolve os seguintes elementos:

a) dados dos alunos: inclui informações de matrícula, desempenho acadêmico, presença, informações pessoais, histórico escolar, feedback de professores, entre outros;

b) dados do corpo docente e técnicos administrativos: informações sobre professores, funcionários administrativos e pessoal de apoio, como registros de emprego, histórico de treinamento, informações pessoais, etc;

c) sistemas de gerenciamento acadêmico: isso envolve o uso de sistemas de informação específicos para gerenciar dados acadêmicos, como sistemas de gestão de aprendizado (LMS), sistemas de informação de alunos (SIS), sistemas de gestão de cursos, entre outros;

d) operações administrativas: inclui dados relacionados à gestão financeira, contabilidade, recursos humanos, infraestrutura física da instituição (instalações, equipamentos), compras e contratos;

e) pesquisa e desenvolvimento acadêmico: dados provenientes de projetos de pesquisa, publicações acadêmicas, atividades de desenvolvimento curricular, programas acadêmicos e atividades extracurriculares;

f) comunicação e interação: dados relacionados à comunicação entre alunos, professores, pais e administração, incluindo e-mails, plataformas de mensagens, registros de reuniões, entre outros;

g) segurança e conformidade: considerações de segurança de dados, políticas de acesso, conformidade com regulamentações de privacidade e proteção contra ameaças cibernéticas;

h) análise e relatórios: capacidade de analisar dados para identificar tendências, medir o desempenho institucional, fazer previsões e criar relatórios para auxiliar na tomada de decisões estratégicas;

i) integração de sistemas: assegurar que diferentes sistemas utilizados na instituição se integrem de forma eficiente para garantir a consistência e acessibilidade dos dados;

j) treinamento e educação em dados: fornecer treinamento e desenvolvimento contínuo para a equipe da instituição para garantir a compreensão dos procedimentos de gestão de dados e a importância da segurança da informação.

1.2. **Objetivos**

O objetivo geral deste processo é garantir que os dados do IFTO sejam gerenciados de forma estruturada, eficiente e segura ao longo de seu ciclo de vida. Para que este objetivo seja alcançado são definidos os seguintes objetivos específicos:

a) precisão e qualidade dos dados: garantir a precisão, integridade, consistência e confiabilidade dos dados, assegurando que estejam livres de erros e sejam úteis e confiáveis para tomada de decisão informadas;

b) acesso seguro e restrito: controlar o acesso aos dados, garantindo que apenas usuários autorizados tenham permissão para acessar informações sensíveis ou críticas;

c) privacidade e segurança: proteger os dados contra acessos não autorizados, garantindo a privacidade dos dados pessoais e a segurança das informações confidenciais;

d) padronização e normalização: padronizar formatos, estruturas e definições de dados para facilitar a compreensão, a integração e a interoperabilidade entre diferentes sistemas e departamentos;

e) governança de dados: estabelecer políticas, processos e responsabilidades para garantir o uso correto e ético dos dados, alinhando-se aos objetivos estratégicos da organização;

f) conformidade: cumprir com regulamentações e leis relacionadas à proteção de dados e privacidade, evitando riscos legais e protegendo a reputação da instituição;

g) gestão do ciclo de vida dos dados: gerenciar eficientemente o ciclo de vida dos dados desde a sua criação até o arquivamento ou exclusão, assegurando sua relevância e utilidade;

h) análise e tomada de decisão: disponibilizar dados de qualidade e confiáveis para análises, relatórios e tomadas de decisão estratégicas, acadêmicas e administrativas precisas e informadas;

i) redução de redundância e dispersão: minimizar a redundância de dados e a dispersão

desorganizada, evitando múltiplas fontes de informação e garantindo consistência;

j) melhoria de processos: identificar oportunidades de melhoria nos processos de negócios por meio da análise e entendimento dos dados, permitindo otimizações e inovações;

k) facilitação da colaboração: promover a colaboração entre equipes e departamentos, facilitando o compartilhamento de informações relevantes de maneira eficaz;

l) resiliência e continuidade de negócios: garantir que os dados estejam protegidos contra perdas e sejam recuperáveis em caso de desastres, assegurando a continuidade das operações;

m) eficiência operacional: utilizar dados para otimizar processos e operações, reduzir redundâncias, identificar áreas de melhoria e aumentar a eficiência global da instituição;

n) melhoria contínua: usar análises de dados para identificar tendências, pontos fortes e áreas que precisam de aprimoramento, promovendo a melhoria contínua dos serviços educacionais oferecidos;

o) inovação educacional: utilizar dados para impulsionar a inovação no ensino e na aprendizagem, adaptando os métodos de ensino às necessidades dos alunos e ao ambiente educacional em constante mudança; e

p) segurança da informação: proteger os dados contra ameaças de segurança cibernética, como ataques de *hackers*, vazamentos de informações ou acesso não autorizado.

1.3. **Abrangência**

A gestão de dados abrange várias áreas e atividades, considerando diferentes aspectos ao longo do ciclo de vida dos dados dentro do IFTO, desde a coleta até a eliminação, assegurando que os dados sejam um ativo valioso e útil para o IFTO. Este processo abrange:

a) coleta de dados: inclui a identificação e a aquisição de dados relevantes para a organização, provenientes de diversas fontes, como sistemas internos, sensores, interações com clientes, entre outros;

b) armazenamento e gerenciamento de dados: envolve a organização, armazenamento seguro e eficiente dos dados em sistemas de gerenciamento de bancos de dados ou em plataformas de armazenamento, garantindo a acessibilidade e a integridade;

c) processamento e transformação: consiste em processar os dados, aplicar transformações e limpezas para garantir sua consistência, qualidade e utilidade para análises e tomadas de decisão;

d) padronização e normalização: estabelecimento de padrões e estruturas comuns para os dados, facilitando a integração entre sistemas e a compreensão dos dados por diferentes usuários;

e) governança de dados: definição de políticas, normas e diretrizes para garantir o uso ético, seguro e eficaz dos dados, incluindo definição de responsabilidades e procedimentos;

f) segurança e privacidade: implementação de medidas de segurança para proteger os dados contra acessos não autorizados, além de garantir a privacidade e o cumprimento de regulamentações;

g) análise e visualização: utilização de ferramentas e técnicas para analisar os dados e transformá-los em insights acionáveis, por meio de visualizações e relatórios;

h) compartilhamento e colaboração: facilitação do compartilhamento seguro e controlado de

dados entre diferentes áreas e equipes, permitindo a colaboração e a utilização eficiente das informações;

i) backup e recuperação: implementação de procedimentos de *backup* e planos de recuperação de desastres para garantir a disponibilidade e a continuidade dos dados em situações adversas;

j) gerenciamento do ciclo de vida dos dados: acompanhamento e gestão do ciclo de vida completo dos dados, desde sua criação, uso, retenção até a exclusão ou arquivamento; e

k) educação e conscientização: promover a conscientização e a educação dos usuários sobre práticas adequadas de gestão e uso de dados.

1.4. **Benefícios esperados**

A gestão de dados traz uma série de benefícios importantes que impactam diretamente a eficiência, a qualidade educacional e a tomada de decisões. Dentre eles tem-se:

a) tomada de decisão informada: os dados precisos e atualizados ajudam os líderes educacionais a tomarem decisões embasadas em evidências, seja na alocação de recursos, na melhoria dos programas educacionais ou na identificação de áreas de aprimoramento;

b) melhoria da qualidade educacional: a análise dos dados acadêmicos pode identificar padrões de desempenho dos alunos, permitindo a implementação de estratégias específicas de ensino para melhorar o aprendizado e o sucesso acadêmico;

c) personalização do aprendizado: o uso de dados permite a criação de abordagens personalizadas de ensino, adaptando o currículo às necessidades individuais dos alunos, promovendo um ambiente de aprendizado mais eficaz;

d) eficiência operacional: a gestão eficaz de dados pode otimizar processos administrativos, reduzir custos, minimizar a burocracia e melhorar a eficiência geral da instituição;

e) engajamento dos alunos: ao acompanhar o desempenho dos alunos e entender suas necessidades, a instituição pode oferecer suporte personalizado, aumentando o engajamento e a retenção dos estudantes;

f) identificação de tendências e oportunidades: a análise de dados pode revelar tendências educacionais, demandas do mercado de trabalho e oportunidades de desenvolvimento de novos programas ou cursos;

g) avaliação e melhoria contínua: a coleta e análise de dados permitem avaliar constantemente a eficácia dos métodos de ensino, do currículo e dos programas, facilitando a adaptação e melhoria contínua;

h) transparência e prestação de contas: a gestão de dados transparente ajuda a construir confiança com os alunos, pais, funcionários e partes interessadas, demonstrando a responsabilidade da instituição no uso e proteção dos dados;

i) conformidade com regulamentações: manter uma gestão adequada de dados ajuda a garantir a conformidade com leis de privacidade e proteção de dados, evitando riscos legais e danos à reputação da instituição; e

j) inovação educacional: o uso estratégico de dados pode inspirar a inovação no ensino, na aprendizagem e no desenvolvimento de novas abordagens educacionais.

2. **DEFINIÇÕES**

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

a) agentes de tratamento: o controlador e o operador;

b) alta administração: representa o mais alto nível estratégico e decisório de um órgão ou entidade, seja ela parte da administração pública federal;

c) banco de dados:conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

d) consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

e) controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

f) 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;

g) dado: elemento bruto e não processado, muitas vezes representando fatos, valores ou observações. Dados podem ser números, palavras, imagens, sons, etc. Por si só, os dados podem não ter um significado claro ou contexto;

h) dados pessoal: informação relacionada a pessoa natural identificada ou identificável;

i) dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

j) encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

k) 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;

l) informação: conjunto de dados que foram processados e organizados para obter significado e contexto. A informação é o resultado da interpretação dos dados, tornando-os úteis e relevantes para tomar decisões ou entender situações;

m) operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

n) TI: Tecnologia da Informação;

o) titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

p) tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; e

q) 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 DADOS

A gestão de dados é um processo composto por fases que envolve a coleta, armazenamento, processamento, análise, compartilhamento, armazenamento, reutilização e eliminação de dados. Ela garante que os dados sejam gerenciados de forma eficiente, segura e em conformidade com os objetivos do IFTO e as regulamentações pertinentes.

Este processo visa tratar os dados como um ativo valioso, aproveitando seu potencial para tomar decisões informadas, melhorar a eficiência operacional, inovar e atender às necessidades dos usuários, enquanto também protege a integridade, confidencialidade e disponibilidade desses dados. Neste contexto, a figura 1 apresenta as 7 (sete) fases que envolvem a gestão de dados no IFTO.

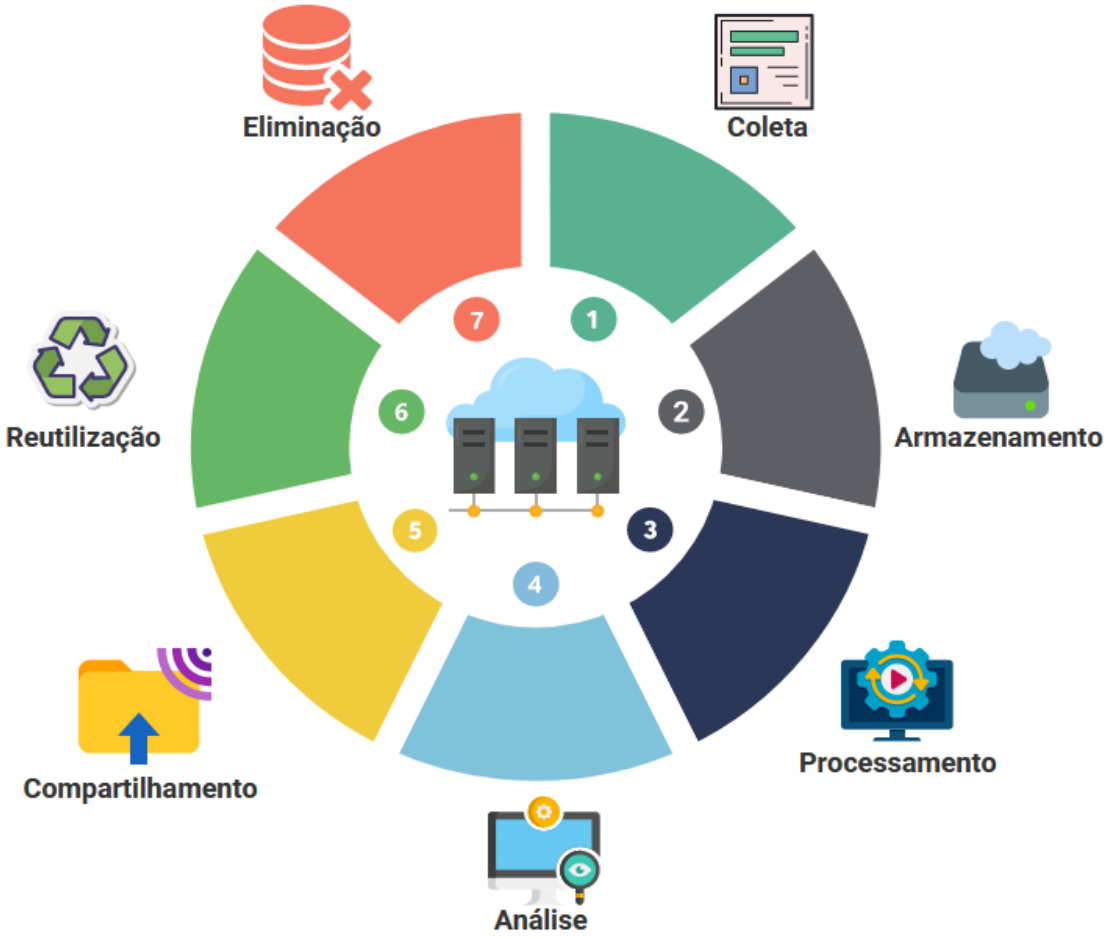

Figura 1 - Gestão de dados

3.1. Processo de gestão de dados

O processo de gestão de dados é um conjunto organizado de fases, atividades e práticas que visam garantir que os dados sejam coletados, armazenados, processados, organizados e utilizados de maneira eficiente, segura e em conformidade com os objetivos institucionais. Esse processo abrange todas as fases do ciclo de vida dos dados, desde a coleta até a eliminação, e envolve a implementação de estratégias para otimizar a qualidade, acessibilidade e segurança dos dados. A tabela 1 apresenta a entrada, fases e saída do processo de gestão de dados.

Tabela 1 - Processo de gestão de dados

Processo de gestão de dados	
Entrada	Dado.
Fases	1. Coleta. 2. Armazenamento. 3. Processamento. 4. Análise. 5. Compartilhamento. 6. Reutilização. 7. Eliminação.
Saída	Informações.

3.1.1. Coleta

Fase responsável por identificar e coletar dados de fontes internas e externas, de acordo com os requisitos e objetivos da organização. Esta fase deve ser executada observando que os dados devem obedecer ao princípio da necessidade e da finalidade (BRASIL, 2018; ENAP, 2022).

A coleta de dados reuni informações relevantes para as operações educacionais e administrativas que auxiliam a tomada de decisões no IFTO. Nesta fase poderão ser executadas as seguintes atividades:

a) identificar as fontes primárias de dados dentro da instituição, como sistemas de informação acadêmico (SUAP), sistemas de gestão de aprendizado (Moodle), registros acadêmicos, entre outros;

b) definir claramente os objetivos da coleta de dados, identificando quais informações são necessárias para apoiar processos educacionais, administrativos, pesquisas ou tomada de decisões;

c) estabelecer procedimentos e protocolos padronizados para coletar dados de forma consistente, garantindo a uniformidade e qualidade das informações;

d) escolher os métodos adequados para coletar dados, que podem incluir questionários, entrevistas, observações, análise de registros existentes, entre outros, dependendo do tipo de informação desejada;

e) identificar os indicadores-chave ou métricas a serem coletadas para medir o desempenho acadêmico, o progresso dos alunos, eficiência administrativa, entre outros aspectos relevantes;

f) implementar mecanismos para garantir a precisão, integridade e consistência dos dados coletados, evitando erros ou duplicações que possam comprometer sua utilidade;

g) assegurar que a coleta de dados seja realizada de acordo com as regulamentações de privacidade e obtenção de consentimento quando necessário, especialmente ao lidar com informações pessoais de alunos, servidores, prestadores de serviço, estagiários e voluntários;

h) estabelecer sistemas seguros para armazenar os dados coletados, protegendo as informações contra acessos não autorizados e garantindo sua integridade e confidencialidade;

i) manter registros detalhados sobre os dados coletados, incluindo informações sobre a fonte, o método de coleta, datas e quaisquer particularidades relevantes para garantir a rastreabilidade e transparência; e

j) revisar periodicamente os processos de coleta de dados para garantir que continuem

alinhados com as necessidades da instituição, fazendo ajustes conforme necessário para melhorar a eficiência e relevância.

3.1.2. Armazenamento

Fase responsável por armazenar dados podendo ser em diretórios, bancos de dados, planilhas, documentos entre outros. O armazenamento deve ser realizado de forma organizada e segura, garantindo que sejam facilmente acessíveis quando necessário.

Os dados pessoais devem ser armazenados e mantidos por prazos definidos, ou seja, até que a finalidade seja alcançada ou deixem de ser necessários ou pertinentes ao alcance da finalidade (BRASIL, 2018; ENAP, 2022). O armazenamento de dados é essencial para manter a integridade, segurança e disponibilidade dos dados armazenados no IFTO, garantindo que estejam prontamente acessíveis quando necessários e protegidos contra ameaças externas. Nesta fase poderão ser realizadas as seguintes atividades:

a) escolher a infraestrutura adequada para armazenar os dados, como bancos de dados, servidores locais, armazenamento em nuvem ou uma combinação de várias soluções, considerando capacidade, segurança e acessibilidade;

b) estabelecer estratégias para organizar e estruturar os dados de maneira lógica e eficiente, utilizando sistemas de gerenciamento de banco de dados e estratégias de arquivamento;

c) implementar medidas de segurança robustas, como criptografia, *firewalls*, controle de acesso e *backups* regulares, para proteger os dados contra acessos não autorizados, perda ou corrupção;

d) adotar padrões de nomenclatura e metadados para facilitar a identificação e organização dos dados, permitindo uma recuperação eficiente quando necessário;

e) estabelecer políticas claras sobre quanto tempo os dados serão armazenados e quando eles devem ser excluídos ou arquivados, em conformidade com regulamentações de privacidade e retenção de dados;

f) monitorar regularmente o desempenho do armazenamento de dados, verificando a capacidade utilizada, a velocidade de acesso e a eficiência do sistema para garantir um ambiente operacional adequado;

g) implementar procedimentos de *backup* regularmente programados para garantir a recuperação dos dados em caso de falhas no sistema, catástrofes ou perda acidental;

h) manter documentação detalhada sobre os sistemas de armazenamento de dados, incluindo procedimentos de manutenção, atualizações e modificações feitas;

i) estabelecer controles de acesso precisos para garantir que apenas pessoas autorizadas tenham permissão para acessar e modificar dados sensíveis; e

j) garantir que o armazenamento de dados esteja em conformidade com as regulamentações de privacidade e segurança e outras legislações locais aplicáveis.

3.1.3. Processamento

Fase responsável realizar o tratamento de dados. O processamento de dados só poderá ser realizado se o tratamento estiver enquadrado no Art. 7º da LGPD (BRASIL, 2018; ENAP, 2022).

O processamento de dados envolve diversas atividades que transformam e utilizam os dados coletados em informações úteis e acionáveis, permitindo que o IFTO tome decisões informadas e melhore seus processos educacionais e administrativos. Nesta fase

poderão ser realizadas as seguintes atividades:

a) limpar os dados, identificando e corrigindo erros, removendo duplicações e garantindo que os dados estejam prontos para serem processados e analisados;

b) combinar dados de diferentes fontes, transformá-los em formatos comuns e integrá-los em um único conjunto de dados para análise e uso consistente;

c) realizar análises estatísticas dos dados para identificar tendências, padrões e correlações que possam fornecer *insights* para tomada de decisões ou melhorias na instituição;

d) dividir os dados em categorias ou segmentos específicos para compreender melhor grupos de alunos, tendências de desempenho, necessidades educacionais, entre outros;

e) desenvolver relatórios e *dashboards* visuais que apresentem de forma clara e acessível as informações extraídas dos dados, permitindo uma compreensão rápida e eficaz;

f) utilizar modelos de aprendizado de máquina para previsões, recomendações ou detecção de padrões mais complexos nos dados;

g) automatizar tarefas repetitivas e rotineiras usando os dados, como a geração de relatórios regulares ou o envio de notificações com base em certos critérios;

h) verificar a precisão e confiabilidade dos resultados obtidos do processamento de dados para garantir que estejam alinhados com a realidade e sejam úteis para a tomada de decisões;

i) utilizar os dados para personalizar experiências educacionais, adaptando métodos de ensino, conteúdos ou intervenções para atender às necessidades individuais dos alunos; e

j) monitorar continuamente o desempenho dos processos baseados em dados e coletar *feedback* para refinamento e melhoria contínua do uso dos dados na instituição.

3.1.4. Análise

Fase responsável por analisar os dados para extrair informações relevantes, *insights* e conhecimentos que auxiliem na tomada de decisões. Na análise de dados devem ser obedecidos os princípios de tratamento, com propósito legítimo, específico e explicito (BRASIL, 2018; ENAP, 2022). Nesta fase poderão ser realizadas as seguintes atividades:

a) identificar os objetivos específicos da análise de dados, como melhorar o desempenho acadêmico, entender padrões de comportamento dos alunos, otimizar processos administrativos, entre outros;

b) reunir dados de várias fontes, limpar, validar e preparar esses dados para análise, garantindo que estejam prontos para serem processados;

c) utilizar técnicas de análise exploratória para examinar os dados, identificar tendências, padrões e relações iniciais entre variáveis relevantes;

d) descrever os dados de maneira detalhada, incluindo estatísticas básicas, resumos, distribuições e visualizações para entender o estado atual dos aspectos acadêmicos e operacionais do IFTO;

e) aplicar modelos estatísticos ou de aprendizado de máquina para prever tendências futuras, como a probabilidade de sucesso de um aluno ou a demanda por determinados cursos;

f) utilizar dados para sugerir ações específicas, como recomendações de intervenções educacionais ou mudanças nos processos administrativos para otimização;

g) agrupar dados semelhantes para identificar segmentos específicos de alunos ou padrões de comportamento que possam direcionar estratégias mais eficazes;

h) avaliar dados para compreender as taxas de retenção de alunos, níveis de engajamento e fatores que impactam a permanência dos alunos na instituição;

i) analisar a eficácia de programas educacionais, métodos de ensino, processos administrativos, identificando áreas para melhorias e refinamentos; e

j) comunicar os insights obtidos por meio de relatórios, visualizações e apresentações acessíveis e compreensíveis para os interessados, como administradores, professores e pessoal acadêmico.

3.1.5. Compartilhamento

Fase responsável por fornecer acesso controlado aos dados, permitindo que as partes interessadas apropriadas os utilizem de acordo com suas funções e responsabilidades. O compartilhamento de dados deve ser consentido pelos seus titulares (BRASIL, 2018; ENAP, 2022). Para garantir que o compartilhamento de dados seja feito de maneira responsável, segura e em conformidade com as regulamentações, promovendo a utilidade e integridade dos dados compartilhados, o IFTO poderá realizar as seguintes atividades:

a) definir quem terá acesso aos dados e como eles serão compartilhados internamente e com partes externas, se necessário;

b) avaliar quais dados são necessários para serem compartilhados, seja entre departamentos da instituição, com outras instituições educacionais, órgãos governamentais ou para pesquisa acadêmica;

c) implementar medidas de segurança robustas para proteger os dados durante o processo de compartilhamento, como criptografia, autenticação de usuário e uso de redes seguras;

d) estabelecer acordos formais ou contratos que definam os termos e condições do compartilhamento de dados, incluindo os propósitos, restrições de uso e responsabilidades das partes envolvidas;

e) garantir que os dados sejam compartilhados em formatos compatíveis e utilizando protocolos adequados para facilitar a integração e compreensão dos dados por parte do receptor;

f) verificar se o compartilhamento de dados está em conformidade com as regulamentações de privacidade, leis de proteção de dados e outras leis aplicáveis antes de compartilhar qualquer informação;

g) educar os funcionários sobre as políticas e procedimentos de compartilhamento de dados, garantindo que entendam a importância da segurança e privacidade das informações compartilhadas;

h) realizar monitoramento constante das atividades de compartilhamento de dados para garantir que estejam alinhadas com as políticas estabelecidas e realizar auditorias para verificar conformidade e identificar possíveis problemas;

i) implementar sistemas que permitam o controle de permissões de acesso aos dados compartilhados, garantindo que apenas pessoas autorizadas tenham acesso às informações específicas; e

j) revisar periodicamente as políticas e procedimentos de compartilhamento de dados para garantir que estejam alinhados com as mudanças nas regulamentações, necessidades

institucionais e tecnologias emergentes.

3.1.6. Reutilização

Fase responsável por reutilizar dados já coletados pelo IFTO. Um novo consentimento deve ser solicitado sempre houver mudança de finalidade (BRASIL, 2018; ENAP, 2022). Esta fase permite que os dados sejam aplicados de maneira eficiente em diferentes contextos e para múltiplos fins, como por exemplo: projetos de ensino, pesquisa e extensão do IFTO. Nesta fase poderão ser realizadas as seguintes atividades:

a) identificar conjuntos de dados existentes que possam ser relevantes e úteis para novos propósitos, além daqueles para os quais foram originalmente coletados;

b) verificar a qualidade e a adequação dos dados para a nova finalidade, garantindo que estejam atualizados, consistentes e precisos para uso adicional;

c) avaliar a relevância dos dados para a nova finalidade, determinando se podem ser aplicados de maneira eficaz em um novo contexto ou para atender a novos requisitos;

d) quando necessário, anonimizar ou proteger dados sensíveis para garantir conformidade com regulamentações de privacidade antes de reutilizá-los em novos contextos;

e) padronizar formatos e preparar os dados para serem compatíveis com os requisitos do novo projeto ou finalidade para garantir sua integração e utilidade;

f) documentar claramente os dados reutilizados, incluindo informações sobre a fonte, a finalidade original, as transformações aplicadas e quaisquer considerações importantes para os novos usos;

g) integrar os dados reutilizados com os sistemas ou processos existentes, garantindo sua acessibilidade e utilidade para os usuários finais;

h) fornecer orientação e treinamento para os usuários sobre como interpretar e usar os dados reutilizados de maneira eficaz para seus propósitos específicos;

i) monitorar regularmente o desempenho e a relevância dos dados reutilizados para garantir que continuem sendo úteis e sejam atualizados conforme necessário; e

j) coletar *feedback* dos usuários sobre a utilidade e qualidade dos dados reutilizados e utilizar essas informações para melhorar os processos de reutilização de dados futuros.

3.1.7. Eliminação

Fase responsável por eliminar dados após o término de seu tratamento. Os dados pessoais devem ser eliminados após o término de seu tratamento (BRASIL, 2018; ENAP, 2022). Esta fase trata a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Nesta fase são estabelecidos processos para descartar de maneira segura dados obsoletos ou não necessários. Esta fase garante que os dados sejam eliminados de maneira segura e em conformidade com as regulamentações, minimizando riscos de segurança e protegendo a privacidade dos dados do IFTO. Nesta fase poderão ser realizadas as seguintes atividades:

a) avaliar regularmente os dados armazenados para determinar se ainda são necessários para as operações atuais ou se podem ser eliminados com segurança;

b) identificar conjuntos de dados que se tornaram obsoletos, irrelevantes ou duplicados e que não são mais necessários para os propósitos da instituição;

c) verificar as políticas internas e regulamentações externas relacionadas à retenção de dados para determinar os prazos de retenção e os critérios para eliminação;

d) estabelecer procedimentos claros e documentados para a eliminação segura e permanente de dados, incluindo métodos apropriados de destruição;

e) Quando possível, desidentificar ou anonimizar dados sensíveis antes da eliminação para garantir a conformidade com regulamentações de privacidade;

f) garantir que a eliminação de dados seja autorizada pelos responsáveis e de acordo com as políticas internas da instituição;

g) utilizar métodos seguros para eliminar os dados, como a destruição física de mídias ou o uso de *softwares* especializados para eliminar dados digitais;

h) manter registros detalhados sobre quais dados foram eliminados, quando e por quê, incluindo informações sobre quem autorizou o processo;

i) realizar auditorias e revisões periódicas para garantir que os processos de eliminação de dados estejam alinhados com as políticas e regulamentações; e

j) comunicar apropriada e transparentemente sobre a eliminação de dados aos envolvidos, garantindo que todos entendam os motivos e os procedimentos envolvidos.

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 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 dados, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes; e

b) disponibilizar os recursos (humanos, tecnológicos e financeiros) para a execução da política e processo de gestão de dados 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) avaliar e aprovar política e processo para gestão de dados; e

b) propor melhorias para a política e processo de gestão de dados.

4.3. Gestor de Segurança da Informação

Servidor designado para gerir a segurança da informação. Compete à esta pessoa as seguintes responsabilidades:

a) propor a política e processo para gestão de dados;

b) coordenar o processo de gestão de dados; e

c) designar um agente responsável pela gestão de dados, dentre os servidores efetivos do IFTO.

4.4. Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR

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 a seguinte responsabilidade:

a) avaliar política, norma, processo, planos, procedimentos e controles sobre gestão de dados.

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

Agente responsável pela gestão de dados. Compete a este setor as seguintes responsabilidades:

a) identificar e classificar dados e informações por nível de criticidade;

b) identificar potenciais ameaças aos dados e informações;

c) coletar dados;

d) processar dados;

e) analisar dados;

f) compartilhar dados;

g) armazenar dados;

h) reutilizar dados; e

i) eliminar dados.

4.6. Usuário

Pessoa que utiliza os dados e informações processados pelo IFTO. Compete aos usuários as seguintes responsabilidades:

a) respeitar os princípios da finalidade e uso de ativos de TI estabelecido nas políticas e normas de segurança da informação do IFTO;

b) utilizar os dados e informações no IFTO prioritariamente para a realização das atividades desempenhadas nos limites da ética, razoabilidade e legalidade;

c) realizar backup de dados e informações periodicamente ou quando houver necessidade

de formatação do Sistema Operacional, das informações contidas em computadores sob sua responsabilidade;

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

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

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;

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
Coleta.	A	C	C	C	R	I
Armazenamento.	A	C	C	C	R	I
Processamento.	A	C	C	C	R	I
Análise.	A	C	C	C	R	I
Compartilhamento.	A	C	C	C	R	I
Reutilização.	A	C	C	C	R	I
Eliminação.	A	C	C	C	R	I

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 unidades do IFTO).

U: Técnicos Administrativos, professores, estudantes, voluntários e prestadores de serviço.

6. INDICADOR DE DESEMPENHO

O processo de gestão de dados será monitorado e medido através de indicador de desempenho. Esse relatório 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 4 - Indicador de desempenho

Indicador	Número de sistemas de informação que tratam dados no IFTO.
Descrição	Quantificar os sistemas de informação que tratam dados no IFTO.
Objetivo	Quantificar os sistemas de informação que tratam dados no IFTO.
Fonte	DTI.
Periodicidade	Anual.
Fórmula	Total de sistemas de informação que tratam dados no IFTO.
Meta	Aumentar a segurança da informação nos sistemas que tratam dados no IFTO.

7. PROCESSOS RELACIONADOS

Para que o processo de gestão de dados seja eficiente, ele se relaciona com outros processos relacionados à privacidade e segurança da informação, conforme apresenta na figura 2.

Figura 2 - Processos que compõem o SGSI-IFTO

8. PRÁTICAS RECOMENDADAS

Para que este processo possa ser executado com eficiência faz-se necessária a

observação das seguintes recomendações:

1. O IFTO deve desenvolver uma estratégia de gestão de dados que abranja objetivos, metas, responsabilidades e recursos para a gestão de dados.

2. O IFTO deve definir políticas claras e diretrizes para determinar quem pode acessar, usar e compartilhar dados, definindo os tipos de dados que podem ser compartilhados e os protocolos para compartilhamento.

3. O IFTO deve identificar os tipos de dados que a organização coleta e classifique-os com base em sua sensibilidade e importância.

4. O IFTO deve criar políticas claras e abrangentes que definam como os dados serão coletados, armazenados, usados e protegidos.

5. O IFTO deve usar padrões consistentes para formatos e nomenclatura de dados, facilitando a organização e a recuperação.

6. O IFTO deve definir níveis de acesso aos dados com base nas funções dos usuários e aplique autenticação e autorização rigorosas.

7. O IFO deve utilizar medidas de segurança, como criptografia, *firewalls* e monitoramento de ameaças, para proteger os dados contra acessos não autorizados.

8. O IFTO deve realizar *backups* regulares dos dados e teste a capacidade de recuperação para garantir a disponibilidade dos dados em caso de falhas.

9. O IFTO deve definir políticas para a retenção de dados, bem como os procedimentos de descarte seguro quando os dados não forem mais necessários.

10. O IFTO deve treinar os funcionários sobre as políticas de gestão de dados, segurança e práticas recomendadas para reduzir erros humanos.

11. O IFTO deve realizar avaliações de impacto de privacidade para avaliar riscos e garantir a conformidade com regulamentos de privacidade.

12. O IFTO deve implementar sistemas de monitoramento para rastrear o acesso e as atividades relacionadas aos dados.

13. O IFTO deve realizar auditorias periódicas para verificar a conformidade com as políticas e regulamentações de gestão de dados.

14. O IFTO deve promover uma cultura organizacional que valorize a qualidade, precisão e segurança dos dados.

15. O IFTO deve avaliar regularmente as práticas de gestão de dados, identificando áreas de melhoria e implementando mudanças conforme necessário.

9. **REFERÊNCIAS**

BRASIL. PRESIDÊNCIA DA REPÚBLICA. SECRETARIA-GERAL. SUBCHEFIA PARA ASSUNTOS JURÍDICOS. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 4 dez. 2023.

FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA. Escola Nacional de Administração Pública. **Governança de Dados na transformação digital: introdução à gestão de dados.** Disponível em: https://repositorio.enap.gov.br/jspui/bitstream/1/7093/4/M%C3%B3dulo%201%20-%20Introdu%C3%A7%C3%A3o%20%C3%A0%20Gest%C3%A3o%20de%20Dados.pdf Acesso em: 4 dez. 2023.

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 05/01/2024, às 11:47, 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.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2236371** e o código CRC **A3E0CD9E**.

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.ifto.edu.br — reitoria@ifto.edu.br

Referência: Processo nº 23235.018468/2023-05 SEI nº 2236371