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

PROCESSO DE RECUPERAÇÃO/RESTAURAÇÃO DE DADOS

HISTÓRICO DE VERSÕES

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

1. INTRODUÇÃO

O processo de recuperação/restauração de dados tem como objetivo principal restaurar informações perdidas, danificadas ou corrompidas para um estado funcional e utilizável. Este processo deve garantir que as informações perdidas sejam recuperadas de forma eficaz, garantindo a continuidade dos negócios e minimizando os impactos adversos decorrentes da perda de dados.

O processo de recuperação/restauração de dados definido pelo IFTO garante que a informação seja gerenciada de maneira eficaz, protegida contra riscos e utilizada de forma a agregar valor aos objetivos estratégicos propostos nos planos institucionais. Este processo visa proteger a confidencialidade, integridade e disponibilidade dos dados, além de garantir a conformidade com regulamentos e políticas de proteção de dados.

Dentro do contexto apresentado, este documento apresenta uma breve introdução, definições, recuperação/restauração de dados, papéis e responsabilidades, matriz RACI, indicador de desempenho, práticas recomendadas e referências. A partir da execução deste processo espera-se recuperar/restaurar os dados em menor tempo possível para que não se comprometa as atividades finalísticas do IFTO.

1.1. Escopo

O processo de recuperação/restauração de dados abrange todas as fases relacionadas à recuperação de dados envolvendo recursos, sistemas e serviços de Tecnologia da Informação. Ele abrange todos os aspectos do ciclo de vida dos dados e pode variar de acordo com regulamentações aplicáveis no contexto da administração pública federal.

1.2. Objetivos

O objetivo geral do processo de recuperação/restauração de dados é recuperar dados perdidos, seja por exclusão acidental, falhas no sistema ou *software*, corrupção de

arquivos, ou mesmo desastres naturais ou cibernéticos. Para que este objetivo seja alcançado são definidos os seguintes objetivos específicos:

a) recuperar dados perdidos ou danificados: recuperar dados que foram perdidos devido a exclusões acidentais, falhas de hardware, ataques de malware, corrupção de arquivos, entre outros incidentes;

b) restaurar a integridade dos dados: garantir que os dados recuperados estejam íntegros e não corrompidos é essencial. Isso significa restaurar os dados para um estado onde possam ser acessados e usados sem erros ou falhas;

c) minimizar a interrupção nos processos de negócios: minimizar a perda de dados críticos para a operação de sistemas e processos de negócios;

d) recuperar rapidamente dados críticos: ajudar a reduzir o tempo de inatividade e a manter a continuidade de negócios;

e) assegurar a disponibilidade de dados: garantir que os dados estejam prontamente disponíveis para uso após a restauração;

f) proteger e preservar a informação: preservar a confidencialidade, integridade e disponibilidade dos dados. Isso significa proteger os dados recuperados contra novos incidentes de perda ou corrupção;

g) reduzir o impacto financeiro e operacional: minimizar os custos associados à perda de informações críticas, seja através de perda de produtividade, danos à reputação ou perda de oportunidades de negócios; e

h) aprender com incidentes passados: cada incidente de perda de dados oferece uma oportunidade para aprender e melhorar os procedimentos de backup e recuperação. A análise pós-restauração pode ajudar a identificar áreas de melhoria para evitar problemas similares no futuro.

1.3. **Abrangência**

O processo de recuperação/restauração de dados abrange diversas áreas para garantir a restauração de informações perdidas. Ele envolve os seguintes aspectos:

a) identificação de todas as fontes potenciais onde os dados podem residir, incluindo dispositivos de armazenamento, servidores, sistemas de *backup*, nuvem, entre outros;

b) compreende a análise da natureza e do escopo da perda de dados, determinando se os dados foram corrompidos, excluídos, se houve falhas de *hardware* ou *software*, ou se foram afetados por desastres naturais ou cibernéticos;

c) inclui a escolha dos métodos e técnicas apropriados para recuperar os dados perdidos;

d) envolve o desenvolvimento de um plano detalhado para a recuperação/restauração, determinando a sequência de ações a serem realizadas, considerando prioridades, recursos necessários e procedimentos a serem seguidos;

e) implementação do plano de recuperação/restauração, realizando as etapas necessárias para recuperar os dados perdidos de acordo com as estratégias estabelecidas; e

f) verificação da integridade e a precisão dos dados recuperados para garantir que estão em condições utilizáveis e que correspondem às expectativas.

1.4. **Benefícios**

A implementação do processo de recuperação/restauração de dados acarreta os seguintes benefícios:

a) garante a continuidade das operações ao recuperar/restaurar dados essenciais perdidos. Isso evita interrupções prolongadas que poderiam afetar negativamente a produtividade e os serviços prestados;

b) reduz as perdas financeiras associadas à perda de dados críticos. A rápida recuperação/restauração de informações pode evitar custos significativos relacionados à interrupção dos negócios ou à perda de dados sensíveis;

c) auxilia na conformidade com regulamentações e leis que exigem a recuperação e retenção de dados por determinados períodos;

d) recupera dados importantes, como estratégias de negócios, informações de clientes, registros financeiros e outros ativos valiosos para o IFTO;

e) permite reconstruir históricos de transações, registros de usuários e arquivos importantes que são fundamentais para a tomada de decisões e análises futuras;

f) ajuda a preservar a reputação da organização ao evitar perdas de dados que possam comprometer a confiança dos clientes, parceiros e partes interessadas;

g) proporciona a oportunidade de aprender com incidentes passados para melhorar os processos de *backup*, segurança e prevenção de perda de dados no futuro;

h) assegura que os dados recuperados sejam confiáveis e estejam em condições utilizáveis, mantendo a integridade e a precisão das informações; e

i) minimiza o tempo de inatividade dos sistemas e aplicativos, restaurando rapidamente as funcionalidades normais e reduzindo o impacto nas operações diárias.

2. DEFINIÇÕES

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

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

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

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

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

e) 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;

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

g) 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;

h) 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);

i) 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;

j) 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;

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

l) TI: Tecnologia da Informação;

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

n) 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

o) técnicos administrativos, professores, estudantes e prestadores de serviço.

3. RECUPERAÇÃO/RESTAURAÇÃO DE DADOS

A perda de informações críticas armazenadas nos recursos, sistemas e serviços críticos de Tecnologia da Informação pode acarretar consequências graves para o IFTO, incluindo interrupção das operações, perda de produtividade e danos à reputação do instituto. As principais razões que causam a perda de dados dentro das organizações são: falhas no *hardware*, erro humano, queda do dispositivo, queda de energia, curto-circuito e ataques cibernéticos com *ransomware (*DATASTORAGE, 2023).

A recuperação/restauração de dados é um processo utilizado para recuperar/restaurar dados perdidos, corrompidos ou danificados, de uma variedade de dispositivos e mídias de armazenamento digital em razão de falha de *hardware*, erro humano, ataque de *malware*, vírus ou outros fatores externos (DATASTORAGE, 2023). Nesse sentido, a recuperação/restauração de dados é uma parte crítica da segurança da informação, uma vez que envolve um processo de recuperar dados que, por algum motivo, estão indisponíveis para o usuário, sistema ou instituição.

No mercado existem várias soluções para recuperação de dados danificados ou perdidos como *softwares* que realizam a recuperação direta no computador e serviços de recuperação em laboratórios de discos rígidos que apresentam falhas. Estas soluções são capazes de recuperar dados de discos rígidos, unidades *flash*, cartões de memória e outros dispositivos de armazenamento.

A solução escolhida para a recuperação/restauração de dados dependerá do diagnóstico prévio realizado pelos especialista em recuperação de dados. Após esta análise um plano de recuperação de dados ajuda a minimizar o tempo de inatividade, reduz os custos e mantem a confiança dos usuários.

A recuperação/restauração de dados em um ambiente de TI envolve uma série de etapas para recuperar informações perdidas, corrompidas ou danificadas, tais como:

a) identificação do problema: o primeiro passo é identificar a natureza do problema. Isso pode ser causado por exclusão acidental, corrupção de dados, ataque de *malware*, falha de *hardware*, entre outros;

b) avaliação do backup: se houver um sistema de *backup* em vigor, é essencial verificar a integridade, a data e a disponibilidade dos *backups*. Isso determinará a fonte dos dados para restauração;

c) isolamento do problema: se possível, isolar a causa do problema para evitar que se espalhe e cause mais danos aos dados;

d) planejamento da restauração: com base na análise do problema e na disponibilidade dos *backups*, é hora de elaborar um plano para restaurar os dados. Isso inclui decidir quais dados precisam ser restaurados, quais sistemas estão envolvidos e qual é a melhor abordagem para a recuperação;

e) restauração dos dados: execute o procedimento de restauração conforme planejado. Isso pode envolver diferentes métodos dependendo do tipo de *backup* (incremental, completo, diferencial) e das ferramentas disponíveis. Geralmente, isso é feito por meio de *software* especializado ou por processos manuais, dependendo da complexidade do sistema;

f) verificação da integridade: após a restauração, é fundamental verificar se os dados restaurados estão íntegros e funcionando corretamente. Testes e verificações são realizados para garantir que os dados recuperados sejam utilizáveis e não estejam corrompidos;

g) implementação e monitoramento: depois que os dados são restaurados com sucesso, é necessário reintegrar o sistema ao ambiente de produção. O monitoramento contínuo é crucial para garantir que não ocorram problemas adicionais após a restauração; e

h) revisão pós-restauração: realize uma revisão do incidente para entender a causa raiz, identificar possíveis melhorias no processo de backup e restauração e documentar lições aprendidas para evitar problemas semelhantes no futuro.

Dentro do panorama apresentado, este processo pode ser realizado por meio de *software*, serviços especializados e meio de *backup* (CIS, 2023). No IFTO a recuperação/restauração de dados é realizada através da execução de um ciclo básico, contendo minimamente 5 (cinco) fases conforme apresenta a figura 1.

Figura 1 - Recuperação de dados

3.1. Processo de recuperação/restauração de dados

O processo de recuperação;restauração de dados é um conjunto organizado de fases, atividades e práticas para restaurar informações perdidas, corrompidas ou inacessíveis de forma a garantir que os dados sejam recuperados em menor tempo possível. A tabela 1 apresenta o resumo do processo.

Tabela 1 - Processo de recuperação/restauração de dados

Processo de recuperação/restauração de dados	
Entrada	Dispositivo de armazenamento danificado.
Fases	1. Avaliação. 2. Diagnóstico. 3. Recuperação. 4. Verificação. 5. Entrega.
Saída	Dados recuperados.

A execução do processo de recuperação/restauração de dados pode variar dependendo da causa da perda dos dados e do tipo de dispositivo envolvido. Todo o processo de recuperação/restauração de dados exige técnica e equipamentos adequados assim como também *softwares e* técnicas específicas.

3.1.1. Avaliação

Esta fase analisa o dispositivo para determinar a causa da perda de dados e a extensão do dano. No IFTO esta fase é realizada pelo profissional de TI que realiza a análise de viabilidade da recuperação dos dados, se realmente existe alguma possibilidade de recuperação dos dados. Nesta fase pode ser realizada a seguinte atividade:

a) identificar a natureza do problema: exclusão acidental, corrupção de dados, ataque de malware, falha de hardware, entre outros.

3.1.2. Diagnóstico

Esta fase é responsável por identificar falhas de *hardware* e *software* em dispositivos de armazenamento de dados. Com base no diagnóstico realizado pelo profissional de TI escolhe o método de recuperação de dados seja ele envolvendo *hardware* ou *software*. Nesta fase pode ser realizada a seguinte atividade:

a) verificar a integridade, a data e a disponibilidade dos *backups*;

b) determinar a fonte dos dados para a restauração dos dados; e

c) definir o método de recuperação como restauração a partir de *backups*, uso de *software* de recuperação de dados, recuperação de sistemas de arquivos corrompidos, entre outros.

3.1.3. Recuperação

Esta fase é executada dependendo do método selecionado no diagnóstico do dispositivo de armazenamento de dados. Na recuperação por *software*, um programa é usado para escanear o dispositivo em busca de dados perdidos e, em seguida, recuperá-los para o usuário. Já na recuperação *hardware* os profissionais de TI usam equipamentos e técnicas avançadas para reparar o dispositivo e recuperar os dados.

Nesta fase, os procedimentos de recuperação de dados são executados por meio de *softwares* especializados e manutenção física caso seja indicada, como por exemplo:

a) troca de componentes do dispositivo, motor e cabeças de leitura para que seja possível uma leitura forçada;

b) recuperação de dados de discos rígidos danificados por meio de técnicas especializadas com uso de softwares especializados; e

c) recuperação de informações a partir de registros, documentos físicos e outras fontes.

3.1.4. Verificação

Após realizar a fase de recuperação, é importante verificar se os arquivos recuperados estão íntegros e completos. Isso pode envolver a abertura dos arquivos e a comparação com os arquivos originais para garantir que nenhum dado tenha sido perdido durante o processo de recuperação. Nesta fase pode ser realizada a atividade:

a) verificar se os dados restaurados estão íntegros e não corrompidos, pode ser feito por meio de verificações manuais ou automáticas.

3.1.5. Entrega

Na fase entrega os dados recuperados/restaurados devem ser armazenados em um local seguro para evitar uma perda futura. Isso pode incluir a criação de *backups* adicionais ou a transferência dos dados para um dispositivo mais seguro, podendo ser um disco, e-mail, pendrive ou nuvem. Nesta fase pode ser necessária a realização de uma revisão do incidente para entender a causa raiz, identificar possíveis melhorias no processo de backup e restauração e documentar lições aprendidas para evitar problemas semelhantes no futuro. Esta fase pode envolver as seguintes atividades:

a) reintegração dos dados recuperados/restaurados ao sistema, garantindo que estejam disponíveis para uso;

b) realização de testes extensivos para garantir que os sistemas e os dados recuperados funcionem conforme o esperado; e

c) monitoramento contínuo para detectar possíveis problemas.

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 Direta ou Indireta. Cabe ao representante deste nível as seguintes responsabilidades:

a) prover a orientação e o apoio necessário às ações de recuperação de dados, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes; e

b) disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução de ações de recuperação/restauração de dados no âmbito do IFTO.

4.2. Comitê de Segurança da Informação

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

a) avaliar e aprovar o processo de recuperação/restauração de dados; e

b) propor melhorias para o processo de recuperação/restauração 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, processo e plano para recuperação/restauração de dados;

b) coordenar o processo de recuperação/restauração de dados; e

c) designar um agente responsável pela recuperação/restauração 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, procedimentos e controles sobre recuperação/restauração de dados.

4.5. Setor de TI (Diretoria de TI e demais setores de TI na unidades do IFTO)

Agente responsável pela recuperação/restauração de dados institucionais. Compete a este setor as seguintes responsabilidades:

a) identificar a causa e a extensão da perda de dados;

b) investigar se a perda foi por exclusão acidental, corrupção de arquivos, falha de hardware, entre outros;

c) determinar quais dados foram perdidos ou danificados e sua importância para o funcionamento normal do sistema ou organização;

d) verificar a existência, integridade e atualização dos backups;

e) decidir a melhor abordagem para a recuperação/restauração de dados;

f) recuperar/restaurar dados a partir de backups, uso de software de recuperação de dados, entre outros métodos;

g) utilizar técnicas avançadas de recuperação de dados por *software* especializado;

h) verificar se os dados restaurados estão íntegros e funcionando corretamente;

i) garantir que os dados recuperados sejam utilizáveis e não estejam corrompidos;

j) reintegrar dados ao sistema ou ambiente de produção;

k) realizar testes extensivos para garantir que os dados restaurados estejam funcionando corretamente ou detectar possíveis problemas após a recuperação; e

l) documentar o processo de recuperação e realizar uma análise pós-recuperação para identificar causas raiz, melhorar os procedimentos de *backup* e recuperação e aprender com a experiência para evitar problemas futuros.

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
Avaliação	A	I	I	C	R	I
Seleção	A	I	I	C	R	I
Recuperação	A	I	I	C	R	I
Verificação	A	I	I	C	R	I
Armazenamento	A	I	I	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: Usuário.

6. INDICADOR DE DESEMPENHO

O processo de recuperação/restauração 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 3 - Indicador de desempenho

Indicador	Número de recuperação/restauração de dados ocorridas durante o ano.
Descrição	Quantificar as recuperações/restaurações de dados ocorridas durante o ano.
Objetivo	Acompanhar a execução do processo de recuperação/restauração de dados ocorrida durante o ano.
Fonte	DTI
Periodicidade	Anual.
Fórmula	Total de recuperações/restaurações de dados ocorridas durante o ano.
Meta	Diminuir a quantidade de recuperações/restaurações de dados ocorridas durante o ano.

7. PROCESSOS RELACIONADOS

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

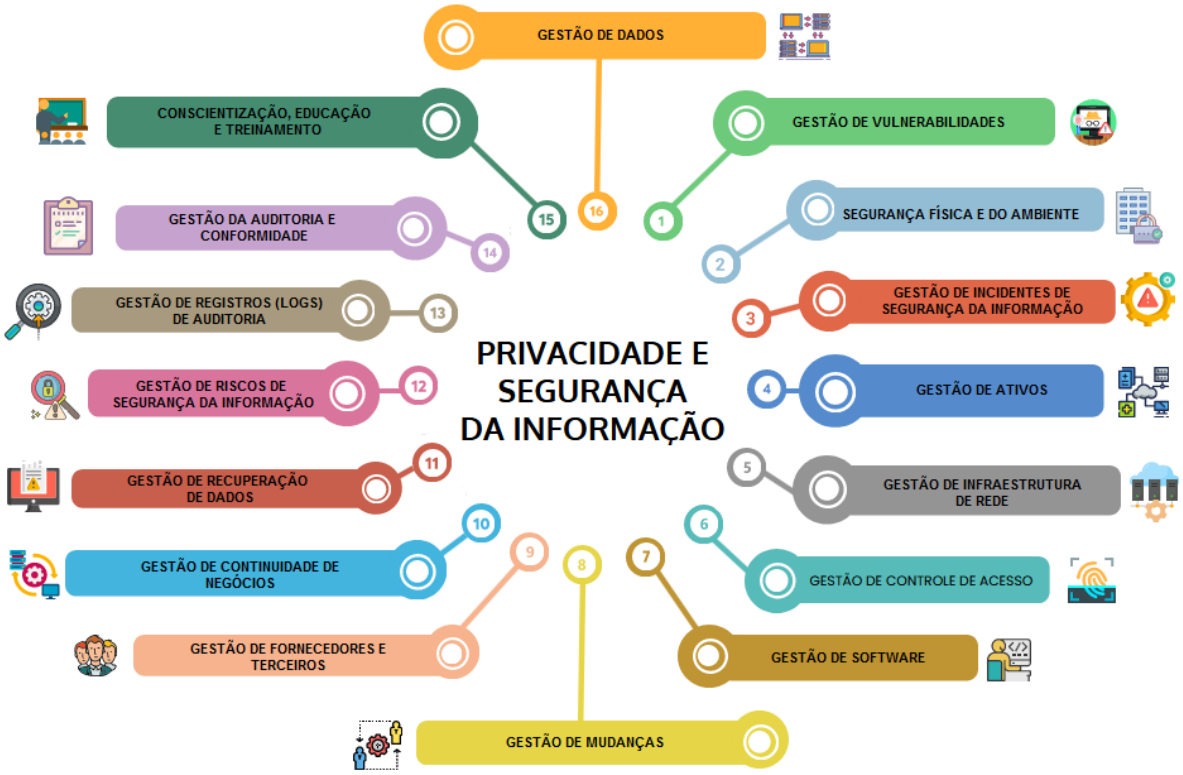

Figura 2 - Processos que compõem o SGSI-IFTO

8. PRÁTICAS RECOMENDADAS

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

1. Um processo de recuperação/restauração de dados deve ser estabelecido e mantido de forma a descrever em seu escopo as atividades de recuperação/restauração de dados, priorização da recuperação e a atividade de segurança dos dados de *backup*.

2. O IFTO deve realizar periodicamente uma revisão e/ou atualização do processo de recuperação/restauração, assim como em casos específicos quando ocorrerem mudanças significativas na organização que venham impactar a organização de forma significativa.

3. O IFTO deve garantir que todos os dados dos sistemas tenham cópias de segurança (backups) realizadas automaticamente e de forma regular.

4. O IFTO deve criar e manter pelo menos uma instância isolada dos dados de recuperação/restauração. Alguns exemplos deste tipo de implementação são controle de versão de destinos de *backup* por meio de sistemas e serviços *offline* (*backup offline*, não acessível por meio de uma conexão de rede), em nuvem, ou em datacenter separado do site local.

5. O IFTO deve realizar o teste de integridade dos dados na mídia de *backup* regularmente, executando um processo de restauração/restauração de dados para garantir que o *backup* esteja funcionando corretamente.

6. Sempre que possível o IFTO deve garantir que os dados de recuperação/restauração sejam protegidos adequadamente por meio de segurança física ou criptografia quando são

armazenados, bem como quando são movidos pela rede. Isso inclui *backups* remotos e serviços em nuvem.

7. O IFTO deve estabelecer controles que garantam que os dados de recuperação/restauração sejam equivalentes aos dados originais.

9. REFERÊNCIAS

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Portaria nº 852, de 28 de março de 2023: dispõe sobre o programa de privacidade e segurança da informação** - PPSI. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908 Acesso em: 6 de dez. 2023.

CENTER FOR INTERNET SECURITY. **Controle 11: recuperação de dados.** Disponível em: https://www.cisecurity.org/ Acesso em: 5 dez. 2023.

SEAGATE. **Quando ocorre perda de dados.** SEAGATE, 2012. Disponível em: https://www.seagate.com/files/www-content/services-software/pt-br/docs/data-loss-faq-tp-638-1-1206-pt.pdf Acesso em: 4 dez. 2023.

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 05/01/2024, às 18:15, 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 **2237362** e o código CRC **E7B74DF9**.

Referência: Processo nº 23235.021942/2023-78 SEI nº 2237362