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

PROCESSO DE GESTÃO DE MUDANÇAS

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
19/04/2021	1	Elaboração do processo de gerenciamento de mudanças.
08/01/2023	2	Atualização do processo para conformidade com Instrução Normativa PR/GSI nº 3, de 28 de maio de 2021.

1. INTRODUÇÃO

A gestão de mudanças nos aspectos de segurança da informação refere-se ao conjunto de práticas e processos utilizados para gerenciar e controlar as alterações nos sistemas, processos e procedimentos relacionados à segurança da informação em uma organização. No IFTO esse processo visa garantir que as mudanças implementadas não comprometam a segurança dos dados, sistemas e ativos de TI.

A implementação do processo de gestão de mudanças nos aspectos de segurança da informação tem por objetivo preparar e adaptar o IFTO para as mudanças decorrentes da evolução de processos e de tecnologias da informação, visando à obtenção de mudanças eficazes e eficientes e à mitigação de eventuais resistências. Este processo deve ser respaldado pelas informações levantadas no relatório de identificação, análise e avaliação de riscos de segurança da informação e no relatório de tratamento de riscos de segurança da informação (BRASIL, 2021).

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

1.1. Escopo

O escopo do processo de gestão de mudanças nos aspectos de Segurança da Informação abrange várias áreas-chave para garantir a integridade, confidencialidade e disponibilidade dos dados e sistemas. Faz parte do escopo deste processo:

a) mudanças nos sistemas de TI e infraestrutura de segurança: inclui alterações nos sistemas, redes, aplicativos, hardware, software e outras infraestruturas relevantes para a segurança da informação;

b) atualizações de políticas e procedimentos de segurança: envolve a revisão e atualização contínua das políticas, diretrizes e procedimentos de segurança para refletir as mudanças nas necessidades do IFTO e os novos desafios de segurança;

c) implementação e migração de novas tecnologias: abrange a introdução de novas tecnologias, ferramentas ou processos de segurança para melhorar a postura de segurança do IFTO;

d) mudanças nos controles de acesso e privacidade: inclui alterações nos níveis de acesso, permissões, autenticação e medidas de privacidade para garantir a proteção adequada dos dados;

e) patches e atualizações de segurança: envolve a aplicação de patches, atualizações de software e correções de segurança para mitigar vulnerabilidades conhecidas nos sistemas;

f) alterações nas configurações de segurança: inclui ajustes nas configurações de *firewalls*, controles de segurança, políticas de criptografia e outras configurações relevantes para a segurança;

g) mudanças nos procedimentos de resposta a incidentes: abrange ajustes nos procedimentos de resposta a incidentes para lidar com novos tipos de ameaças ou cenários de segurança;

h) integração de novos requisitos de conformidade: inclui a implementação de mudanças para atender a novos requisitos regulatórios e normativos relacionados à segurança da informação;

i) gestão de fornecedores e terceiros: envolve alterações nas relações com fornecedores externos para garantir que eles atendam aos padrões de segurança da organização; e

j) auditoria e monitoramento de mudanças: abrange a revisão, auditoria e monitoramento das mudanças implementadas para garantir que estejam em conformidade com os requisitos de segurança.

1.2. **Objetivos**

Os objetivos do processo de gestão de mudanças nos aspectos de segurança da informação são essenciais para garantir a integridade, confidencialidade e disponibilidade dos dados e sistemas, enquanto se adaptam às necessidades da organização e às demandas do ambiente de ameaças em constante evolução. Dentre eles tem-se:

a) minimizar riscos de segurança: garantir que todas as mudanças implementadas não introduzam novas vulnerabilidades ou aumentem os riscos de segurança existentes nos sistemas;

b) assegurar a conformidade regulatória: implementar mudanças para atender aos requisitos regulatórios e normativos em constante evolução, mantendo a conformidade legal;

c) manter a disponibilidade dos sistemas: garantir que as mudanças não comprometam a disponibilidade dos sistemas críticos para a organização;

d) garantir a integridade dos dados: certificar-se de que as mudanças não afetem a integridade dos dados armazenados e transmitidos;

e) melhorar a eficiência das medidas de segurança: implementar mudanças que melhorem a eficiência das medidas de segurança existentes, sem comprometer sua eficácia;

f) avaliar impactos e mitigar ameaças emergentes: identificar e avaliar novas ameaças de segurança emergentes e implementar mudanças para mitigar esses riscos;

g) reduzir incidentes e brechas de segurança: diminuir a probabilidade de incidentes de segurança e brechas, adotando práticas proativas de gestão de mudanças;

h) melhorar a capacidade de resposta a incidentes: implementar mudanças que fortaleçam a capacidade de resposta a incidentes e a resiliência dos sistemas de segurança;

i) garantir o alinhamento com objetivos de negócios: certificar-se de que as mudanças em segurança estejam alinhadas com os objetivos e estratégias gerais da organização; e

j) promover a conscientização e treinamento: educar os colaboradores sobre as mudanças de segurança implementadas, suas implicações e ações adequadas a serem tomadas.

1.3. **Abrangência**

A abrangência do processo de gestão de mudanças nos aspectos de Segurança da Informação é ampla e engloba diversas áreas críticas para garantir a eficácia e a integridade das medidas de segurança. Este processo abrange:

a) sistemas e infraestrutura de TI: inclui mudanças em *hardware, software*, redes e sistemas críticos para garantir que todas as alterações mantenham ou aprimorem a segurança da infraestrutura de TI;

b) políticas e procedimentos de segurança: abrange a revisão e atualização contínua das políticas, diretrizes e procedimentos de segurança para atender às demandas emergentes de ameaças e requisitos regulatórios;

c) controles de acesso e privacidade: envolve alterações nos controles de acesso, permissões, autenticação e medidas de privacidade para garantir a proteção adequada dos dados e sistemas;

d) atualizações de segurança e patches: inclui a aplicação de patches, atualizações de software e correções de segurança para mitigar vulnerabilidades conhecidas e garantir a segurança dos sistemas;

e) configurações e configurações de segurança: abrange ajustes nas configurações de segurança, políticas de firewall, criptografia e outras configurações relevantes para manter a postura de segurança;

f) processos de resposta a incidentes: inclui ajustes nos procedimentos de resposta a incidentes para lidar com novos tipos de ameaças ou cenários de segurança;

g) gestão de riscos e auditoria de segurança: envolve a integração da gestão de mudanças à gestão de riscos de segurança, garantindo uma avaliação contínua dos riscos e auditorias de conformidade;

h) relações com fornecedores e terceiros: abrange a implementação de mudanças para garantir que os fornecedores externos atendam aos padrões de segurança da organização;

i) monitoramento e revisão contínua: inclui a monitorização contínua das mudanças implementadas para identificar quaisquer problemas ou anomalias e revisões regulares para avaliar sua eficácia; e

j) treinamento e conscientização: envolve educar a equipe sobre as mudanças de segurança implementadas, suas implicações e procedimentos adequados a serem seguidos.

1.4. **Benefícios esperados**

O processo de gestão de mudanças nos aspectos de Segurança da Informação traz uma série de benefícios significativos para as organizações, ajudando a manter a integridade, confidencialidade e disponibilidade dos dados e sistemas. Dentre eles tem-se:

a) redução de riscos de segurança: ajuda a minimizar os riscos associados às mudanças implementadas nos sistemas, reduzindo a probabilidade de brechas de segurança e ameaças;

b) maior conformidade regulatória: auxilia na manutenção da conformidade com as regulamentações de segurança e normas de conformidade, mitigando o risco de não conformidade;

c) melhoria na eficiência dos processos de segurança: implementa mudanças que melhoram a eficiência das medidas de segurança sem comprometer sua eficácia;

d) maior resiliência contra ameaças emergentes: adaptação rápida e eficaz às novas ameaças de segurança por meio de mudanças bem gerenciadas nos sistemas e procedimentos;

e) disponibilidade contínua dos sistemas críticos: garante que as mudanças implementadas não interrompam a disponibilidade dos sistemas e serviços essenciais;

f) redução de incidências de segurança: diminui a probabilidade de incidentes de segurança, minimizando a exposição a vulnerabilidades introduzidas por mudanças mal gerenciadas;

g) maior controle sobre as alterações de segurança: estabelece um processo estruturado para gerenciar e controlar as mudanças de segurança, garantindo que sejam autorizadas e rastreadas adequadamente;

h) melhoria da resposta a incidentes: reforça os procedimentos de resposta a incidentes para lidar efetivamente com alterações e incidentes de segurança relacionados;

i) adaptação às necessidades de negócios em evolução: permite ajustes contínuos nos controles de segurança para atender às mudanças nas necessidades e demandas do negócio; e

j) promoção da consciência e educação em segurança: educa e conscientiza a equipe sobre as mudanças de segurança implementadas, fortalecendo a cultura de segurança no IFTO.

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 em dano para um sistema ou organização;

b) análise de incidentes: consiste em examinar todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento. O propósito dessa análise é identificar o escopo do incidente, sua extensão, sua natureza e os prejuízos causados. Também faz parte da análise do incidente propor estratégias de contenção e recuperação;

c) análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco;

d) ativo: tudo que tenha valor para a organização, material ou não;

e) ativo de rede: equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores;

f) 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;

g) avaliação de risco: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

h) BDGC: banco de dados de gerenciamento de configuração;

i) evento: qualquer mudança de estado que tenha significância para o gerenciamento de um serviço de TI ou outro item de configuração. O termo também pode ser usado para significar

um alerta ou notificação criada por qualquer serviço de TI, item de configuração ou uma ferramenta de monitoramento. Qualquer requisição que é feita de uma maneira automática para o setor de TI, ou seja, para ser considerado evento, não se pode haver qualquer intervenção seja de um usuário ou até mesmo de um técnico especializado. Pode ser considerado um evento: link de internet com consumo próximo a contratado junto a operadora, disco rígido de um servidor cheio, alto consumo de memória RAM;

j) gestão de mudanças nos aspectos relativos à segurança da informação: aplicação de um processo estruturado e de um conjunto de ferramentas de gerenciamento de mudanças, de modo a aumentar a probabilidade de sucesso e fazer com que as mudanças transcorram com mínimos impactos no âmbito de órgão da APF, visando viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação;

k) gestão de riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

l) gestão de segurança da informação: ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

m) incidente: interrupção não planejada (imprevista) de um serviço ou redução na qualidade de um serviço. Qualquer evento que cause ou possa causar uma interrupção ou uma redução da qualidade do serviço prestado. Qualquer acontecimento que ocorre com algum componente que tenha alguma ligação com um serviço já prestado pelo departamento de TI e que não faça parte do comportamento padrão de usabilidade causando assim a redução na qualidade do serviço de TI ou até mesmo a interrupção do serviço como um todo, como por exemplo: internet lenta, indisponibilidade para acessar uma pasta na rede, e-mail não enviando mensagens e impressora não funcionando;

n) mudança: Modificação ou remoção de qualquer processo, arquitetura, ferramenta, métrica, documentação e outros itens de configuração que possam afetar os serviços de TI. Adição, alteração ou remoção de componentes de serviços de TI, bem como intervenções em ambiente operacional de TI que precisam ser gerenciadas;

o) mudança de serviço: mudança num serviço existente ou a introdução de um serviço novo, ou ainda a adição, modificação ou remoção de serviço autorizado, planejado ou suportado ou componente de serviço e sua documentação associada;

p) RdM: requisição de mudança. Comunicação formal que busca uma alteração em um ou mais itens de configuração, pode assumir várias formas, como a requisição de serviço, chamada na central de serviço, documento de início de projeto. Todos os processos podem emitir requisições de mudança (RdMs) para modificações necessárias que melhorem a eficiência de serviços de TI; e

q) Requisição: é quando tudo esta funcionando perfeitamente nos serviços de TI, porém o usuário precisa da mão de obra do departamento de tecnologia para a criação de um recurso ou desenvolvimento de uma nova ferramenta de trabalho. Exemplo de requisição: criação de um e-mail, mudança da instalação de um computador, desenvolvimento de um novo relatório no sistema.

3. GERENCIAMENTO DE MUDANÇAS

Mudança é um evento evolutivo nas organizações. Ela transforma o estado atual dos serviços de TI, em uma situação nova. A mudança pode ser antecipada ou inesperada, com motivações internas ou externas e acontece em todos os lugares.

Uma mudança pode aparecer devido a um incidente ou devido a ações proativas para beneficiar o negócio da instituição, como a redução de custos ou a melhoria dos serviços. As mudanças podem surgir não somente de forma reativa em resposta às exigências impostas externamente ou problemas ocorridos, como também podem surgir de forma proativa em busca de melhorias na prestação dos serviços de TI.

Para Melendez Filho (2011), uma requisição de mudança de TI pode abranger, desde situações simples, como trocas de pontos de rede e pequenas atualizações de sistemas até o desejo da implementação de melhorias nos serviços. Estas melhorias podem ser obtidas através de indicadores de nível de serviço, substituições de componentes de serviços para outros de maior capacidade e menor risco de descontinuidade.

Cada mudança é categorizada em um tipo. O tipo de mudança indica a extensão do risco que uma determinada mudança pode causar no ambiente, levando em consideração sua natureza, complexidade, pessoas envolvidas, esforço de preparação, exposição a falhas e quantidade de usuários. Este processo considera três tipos de mudança, cada um gerenciado de maneiras diferentes.

a) **mudança normal (proativa):** mudança eventual que descreve as adições, modificações ou desativações de serviços ou de seus componentes. A mudança é considerada normal quando inclui qualquer mudança de serviço que não seja padrão ou emergencial. É aquele tipo de mudança que precisa ser programada através do registro em uma requisição de mudança (RdM), avaliada e autorizada antes de ser implementada. Qualquer solicitação de mudança com atividades não rotineiras pode ser considerada uma mudança normal. Este tipo de mudança é decorrente de melhorias que foram planejadas para o ambiente, geralmente não são vinculadas com incidentes e sim com eventos recorrentes que podem representar riscos para o negócio. Alguns exemplos:

- liberar uma nova versão de um aplicativo de negócio;
- migrar um aplicativo para outro servidor;
- alterar algum atributo em um serviço existente;
- ampliação do parque computacional;
- obsolescência prevista de equipamentos e processos; e
- necessidade de adoção de novas tecnologias.

b) **mudança padrão (rotineira):** mudança que segue um padrão de procedimentos e métodos formais preestabelecidos. É um tipo de mudança pré-aprovada que tem baixo risco, é relativamente comum e segue um procedimento ou instrução de trabalho. É um tipo de mudança em que a equipe técnica já possui elevado grau de conhecimento e discernimento necessário para realizar a atividade. Toda mudança padrão pode ter um modelo de mudança que defina os passos a serem seguidos, incluindo como a mudança deve ser registrada, gerenciada e implementada. Alguns exemplos:

- recuperação de senha;
- fornecimento de um PC para um novo funcionário;
- upgrade de sistema operacional;
- atualização de infraestrutura de tecnologia da informação;
- serviços de tecnologia da informação com periodicidade habitual que impliquem mudanças de um ou mais aspectos de segurança; e
- alteração de local de uma impressora.

c) **mudança emergencial**: mudanças com prazo curto para iniciar e normalmente pouco prazo para concluir. Este tipo de mudança tem a finalidade de reparar falhas ou restabelecer interrupções em serviços que têm impacto no negócio do IFTO. É um tipo mudança não prevista de alto impacto e que ocorre, geralmente, em função de:

- incidente grave ou modificação nos fatores de risco com alto impacto para os processos da organização;

- incidente grave ou modificação nos fatores de risco com alto impacto para os processos da organização;

- alteração normativa de aplicação imediata;

- necessidade de modificação significativa imediata nos ativos de informação;

- necessidade de modificação significativa imediata nos ativos de informação; e

- outros eventos similares;

O gerenciamento de mudanças é um processo que visa controlar e gerenciar as alterações realizadas em um sistema, projeto ou processo. Ele ajuda a garantir que as mudanças sejam implementadas de forma planejada, com o mínimo de impacto possível no ambiente e nos processos existentes. Para garantir que as mudanças não aumentem a exposição a ameaças ou vulnerabilidades este processo deve ser integrado aos processos de gestão de riscos e vulnerabilidades.

O gerenciamento de mudanças é o processo responsável por garantir que métodos e procedimentos padronizados sejam usados, de maneira eficiente, para avaliar, aprovar, implantar e revisar todas as mudanças na infraestrutura e no desenvolvimento de TI, a fim de minimizar o impacto relacionado aos serviços e aos clientes (TRT7, 2016). A gestão de mudanças considerando os aspectos de segurança da informação é crucial para garantir que as alterações nos sistemas, processos ou políticas não comprometam a segurança dos dados e sistemas da organização. Este processo envolve: avaliação de impacto, análise de riscos, planejamento e controle, comunicação e treinamento, testes e monitoramento, revisão, atualização e conformidade A figura 1 apresenta as 4 (quatro) macro fases deste processo.

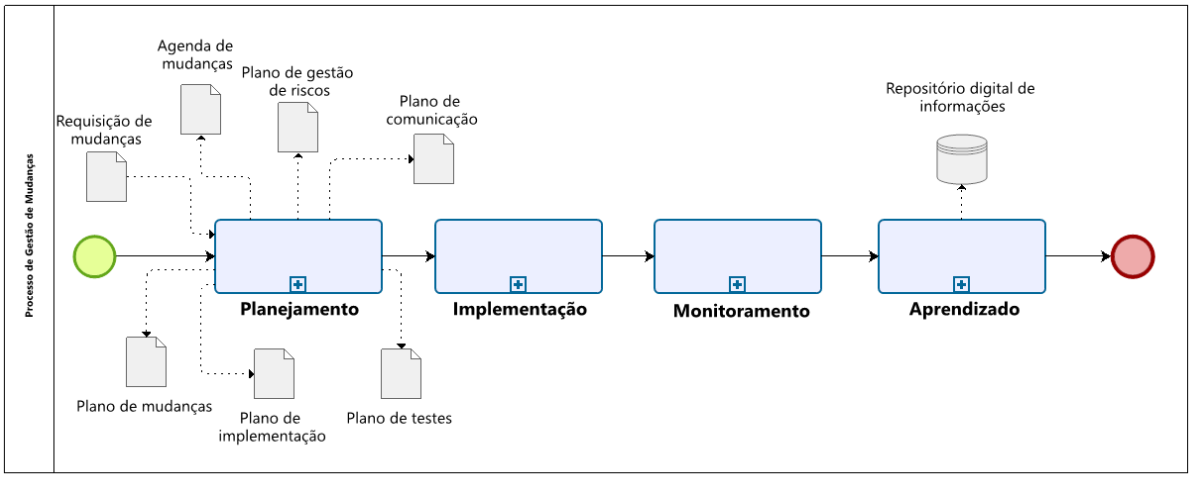


Figura 1 - Processo de gerenciamento de mudanças

Conforme apresenta a figura 1 o processo de gerenciamento de mudanças é composto por 4 (quatro) macro fases: planejamento, implementação, monitoramento e aprendizado. A tabela 1 detalha este processo com suas fases, entrada e saídas.

Tabela 1 - Detalhamento do processo de gerenciamento de mudanças

Processo de gerenciamento de mudanças	
Entrada	Requisição de mudança.
Fases	1. Planejamento. 2. Implementação. 3. Monitoramento.

	4. Aprendizado.
Saídas	- Lista de prioridades. - Agenda de mudanças. - Plano de gestão de riscos. - Plano de mudanças. - Plano de testes. - Plano de implementação. - Plano de comunicação. - Relatório de acompanhamento de mudanças. - Lições aprendidas. - Termo de encerramento.

Fonte: Diretoria de Tecnologia da Informação

A tabela 1 mostra o processo de gerenciamento de mudanças de forma resumida. As próximas seções apresentam o detalhamento das atividades que compõem cada fase deste processo.

3.1. **Planejamento**

A fase de planejamento é responsável pela análise de todas as requisições de mudança que chegam à TI. Cada mudança deve ser precedida de planejamento e testes. Esta fase apresenta detalhes das ações que deverão ser tomadas para efetuar a mudança por meio da lista de prioridades, agenda de mudanças e dos planos: mudanças, gestão de riscos, implementação, testes e comunicação.

Nesta fase são definidas a priorização da requisição de mudança aprovada, quais as datas de execução e dos testes, os responsáveis pela execução das mudanças e testes. A fase está detalhada na figura 2.

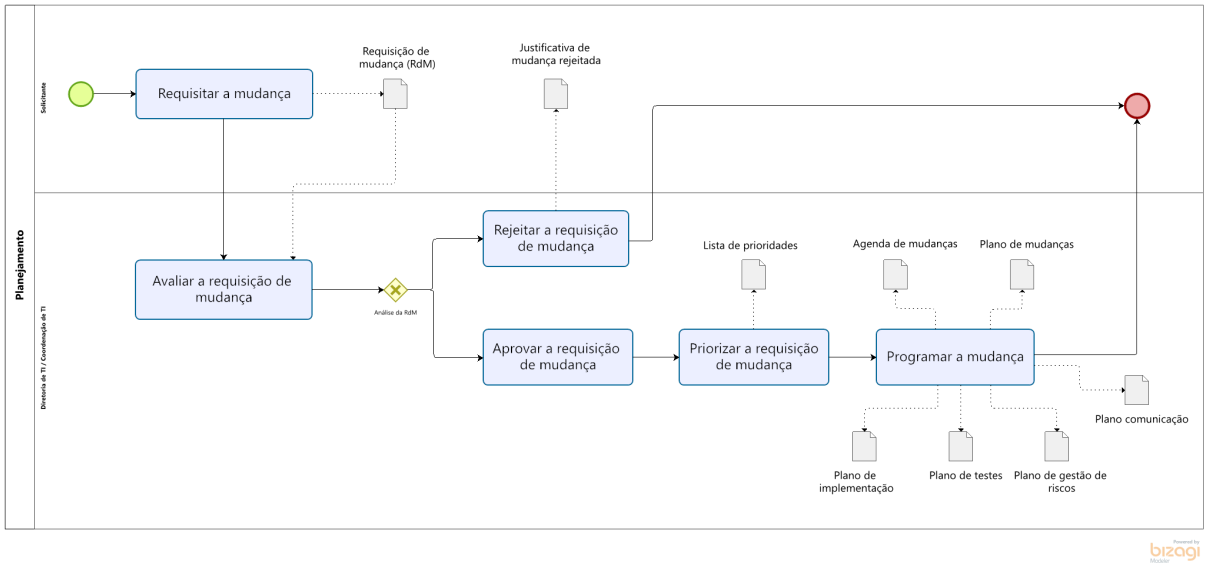


Figura 2 - Planejamento

Conforme pode ser verificado na figura 2 a fase de planejamento é composta por 6 (seis) atividades. Estas atividades serão detalhadas nas próximas seções.

3.1.1. **Requisitar a mudança**

Esta atividade é realizada pelo solicitante que descreve detalhadamente a necessidade de mudança, justifica e sugere o prazo para a sua implementação. A requisição da mudança inicia o processo de gestão de mudanças e nele deverão estar diversos detalhes

desta mudança, como por exemplo: evento ou incidente que foi a origem desta solicitação, itens de configuração afetados pela mudança, aprovadores, impactos, agendamento, riscos e ações necessárias.

A requisição de mudança deve ser acompanhada da justificativa ou proposta da mudança, explicando os benefícios ou problemas que serão resolvidos com a mudança. Todas as mudanças registradas devem ser categorizadas em tipos diferentes de mudança: normal, padrão e emergencial. Este documento deve conter basicamente: agente demandante, unidade de origem, descrição da mudança, tipo de mudança, objetivo(s) da mudança com os fatores que levaram a esta necessidade e benefícios esperados.

O registro da mudança permitirá rastrear as alterações de um serviço prestado pela área de TI e também evidenciar a execução de mudanças sem aprovação. Todos os registros mencionados ou relacionados com a requisição da mudança devem ser atualizados e verificados antes do encerramento das atividades do processo.

3.1.2. **Avaliar a requisição de mudança**

Esta atividade é responsável por avaliar a mudança de forma ampla, abrangendo riscos e impactos para o negócio. Nesta atividade são identificados os serviços e ativos de TI que possam ser afetados pela mudança, de modo a avaliar impactos em níveis de serviços acordados com as áreas de negócios.

Antes de implementar qualquer alteração nos sistemas ou procedimentos de segurança, é fundamental avaliar o impacto potencial dessas mudanças. Isso envolve entender como as alterações podem afetar a segurança existente e identificar possíveis pontos de vulnerabilidade. Para realizar a análise e avaliação de risco, importância e benefícios da mudança, deve ser utilizado o conceito dos 7 R's, o que tornará a análise assertiva. Para isso, serão realizadas 7 perguntas:

a) quem requisitou a mudança? (*raise*);

b) qual é a razão da mudança? (*reason*);

c) qual é o retorno requerido a partir da mudança? (*return*);

d) quais os riscos envolvidos na mudança? (*risks*);

e) quais os recursos necessários para entregar a mudança? (*resources*);

f) quem é o responsável por construir, testar e implantar a mudança? (*responsible*); e

g) qual é a relação entre esta mudança e outras mudanças? (*relationship*).

As seguintes perguntas deverão ser respondidas no momento da submissão da mudança para revisão e aprovação:

a) haverá indisponibilidade de algum dos itens de configuração relacionados durante a mudança?

b) haverá degradação do desempenho dos serviços relacionados durante a mudança?

c) há previsão de impacto para os clientes após a conclusão da mudança? Por exemplo: lentidão por retenção de processamento, atrasos de *jobs* e etc?

d) após a implementação, a forma de trabalho do cliente será alterada?

e) será necessário atualizar algum item de configuração relacionado ao final da mudança?

f) será necessário atualizar algum procedimento de monitoração ao final da mudança?

g) será necessário atualizar algum registro de conhecimento ao final da mudançaApós a implementação das mudanças, monitorar continuamente os sistemas de segurança para identificar quaisquer problemas ou anomalias resultantes das alterações.?

Em caso de urgência deverão ser realizadas as seguintes perguntas:

a) a mudança está relacionada com o tratamento de algum incidente ou problema em andamento?

b) o adiamento da mudança provocará aumento do impacto de incidentes relacionados?

c) a mudança está relacionada com algum requisito de negócio que possua data limite específica para entrega? Por exemplo: Leis, regulamentos, portarias, contratos, normas e etc.

d) a mudança depende de recursos com disponibilidade limitada?

e) a mudança está relacionada com a mitigação ou eliminação de riscos identificados de maneira proativa?

A criticidade da mudança é determinada pela soma dos valores relacionados com as respostas de impacto e urgência. De acordo com o valor alcançado na análise de criticidade a mudança será realizada.

Nesta atividade será determinado se a mudança vai ser ou não implementada. Uma mudança pode ser rejeitada ou aprovada. Independente do tipo de mudança, ela deve ser avaliada de forma que seja realizado o planejamento da execução da mudança. O documento de avaliação e aprovação de mudança tem o objetivo de: analisar as mudanças demandadas, recomendar quais mudanças devem ser aprovadas; e sugerir as alternativas para a implementação das mudanças. Esta atividade é responsável por identificar os serviços e ativos de TI que possam ser afetados pela mudança, de modo a também serem avaliados os impactos em níveis de serviços acordados.

3.1.3. **Rejeitar a requisição de mudança**

Atividade responsável por cancelar a mudança solicitada e informar ao solicitante o motivo pelo qual a mudança não será realizada.

3.1.4. **Aprovar a requisição de mudança**

A aprovação da requisição de mudança deve ser realizada a partir de um processo de autorização e controle de mudanças nos sistemas e políticas de segurança. Isso inclui a definição de responsabilidades claras para aprovar, revisar e implementar alterações.

De acordo com a análise de riscos e o planejamento de comunicação realizado pela equipe de TI, a Coordenação de TI juntamente com a Diretoria de Tecnologia da Informação aprova a realização da mudança. A autorização garante que a mudança foi devidamente avaliada, documentada e aprovada pelas partes interessadas. A aprovação de mudanças, inclusive quanto ao tratamento de casos de exceção (mudanças emergenciais) baseiam-se nos seguintes critérios:

a) tipo de mudança;

b) categoria da mudança;

c) impacto para usuários e áreas demandantes;

d) gravidade da mudança;

e) urgência para a realização da mudança; e

f) capacidade técnica da equipe para a realização da mudança.

O documento de avaliação e aprovação de mudança deve conter, no mínimo:

a) alternativas para implementação da mudança, com a descrição básica dos procedimentos necessários para sua execução;

b) recomendações, em ordem de prioridade, das alternativas a serem adotadas;

c) relação entre a mudança pretendida e outras alterações que, eventualmente, possam ocorrer simultaneamente;

d) análise de risco dos ativos de informação que serão afetados pela mudança;

e) avaliação do impacto do adiamento da realização da mudança;

f) definição da alternativa a ser implementada ou indeferimento da mudança proposta pela alta administração do órgão ou da entidade; e

g) análise crítica das consequências de mudanças não previstas e de ações propostas para mitigação das eventuais consequências negativas.

No momento da aprovação caso seja verificado se tratar de mudança emergencial que impacte várias áreas de negócios esta mudança terá prioridade em relação as demais.

3.1.5. **Priorizar a requisição de mudança**

A priorização das mudanças passa por uma análise de impacto x urgência que irá eleger as mudanças que possuem alto impacto, geralmente a mudança emergencial afeta grande parte dos usuários do negócio e alta urgência, que necessitam de ação imediata, como prioritárias. Esta atividade deve detalhar como será dividido o esforço para atender às demandas urgentes sem deixar de atender às demais solicitações do negócio.

3.1.6. **Programar a mudança**

A definição do dia e horário para a execução de uma solicitação de mudança depende do planejamento e de um acordo entre as áreas técnicas e de negócio. Aspecto como impacto, risco, prazo requerido e urgência são levados em conta. A programação é feita com base na lista de prioridades para execução de mudanças. Nesta atividade são atualizados a agenda de mudanças, planos de mudanças, implementação, testes, gestão de riscos e comunicação. Esta atividade e responsável pela criação do plano de testes para a realização da mudança.

3.2. **Implementação**

A fase implementação é responsável por acompanhar a execução da mudança. As atividades que compõem esta fase estão detalhadas na figura 3.

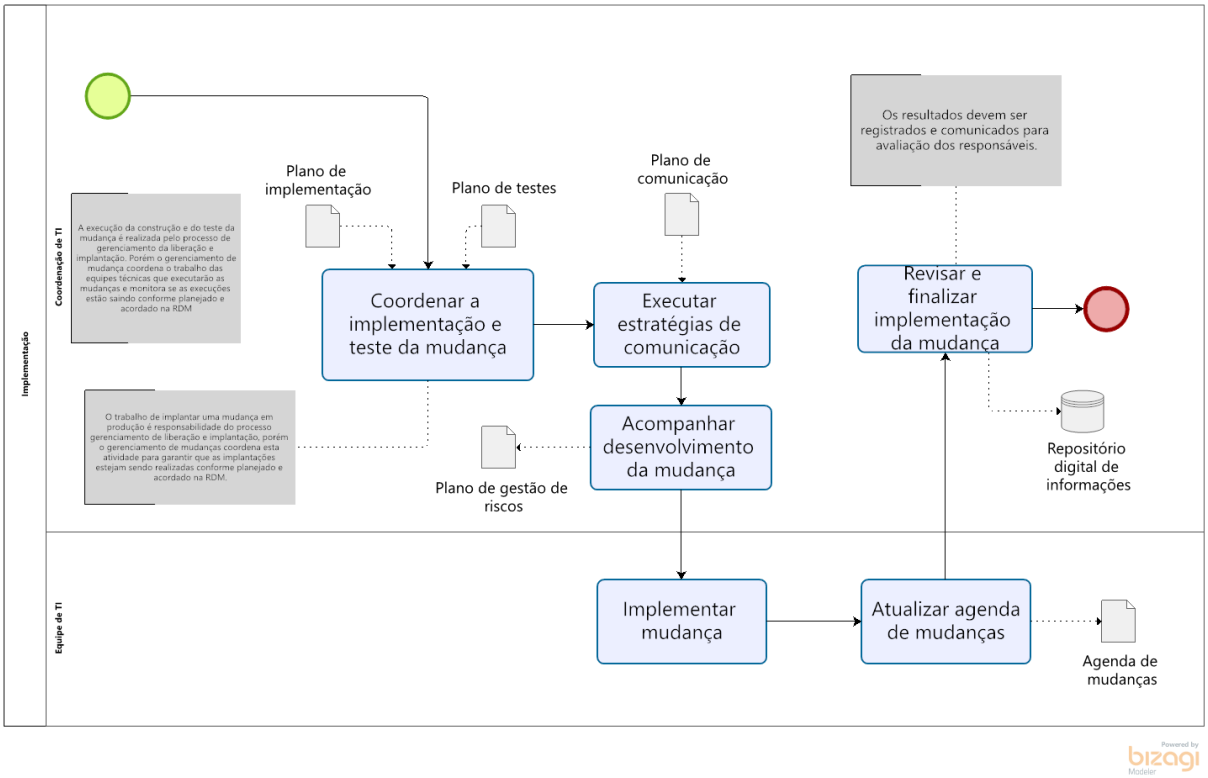


Figura 3 - Implementação

Conforme demonstra a figura 3 a fase de implementação é composta por 8 (oito) atividades que serão detalhadas nas próximas seções.

3.2.1. Coordenar a implementação e teste da mudança

As requisições de mudanças autorizadas devem ser passadas para a equipe de TI executar a mudança. A gestão de mudança apenas controla e coordena as atividades mas são executa as atividades de implementação de mudanças. O processo responsável por estas atividades é o gerenciamento de liberação e implantação. Para a execução desta atividade é necessário que seja observado o plano de testes.

Antes de implementar mudanças significativas nos sistemas de segurança, realizar testes e validações para garantir que essas mudanças não introduzam novas vulnerabilidades ou problemas de segurança.

3.2.2. Executar estratégias de comunicação

A área de TI deve previamente comunicar aos usuários e áreas de negócios afetadas sobre a programação das requisições de mudanças aprovadas. Esta atividade poderá ocorrer através de agenda de mudanças ou envio de mensagem eletrônica para orientação, explicar as razões e atividades que serão realizadas, ou informar indisponibilidade de serviços críticos.

3.2.3. Acompanhar desenvolvimento da mudança

A Coordenação de TI deve analisar e avaliar o desenvolvimento da mudança a fim de verificar se a mesma atingiu o objetivo proposto. As mudanças executadas devem ser

rastreáveis e monitoradas, com vistas à avaliação de sua efetividade e para permitir ações corretivas, no caso de ocorrência de efeitos não identificados nas fases de planejamento e testes. Entre os aspectos que devem ser rastreados e monitorados tem se:

a) as causas de sucesso ou fracasso ao atingir o objetivo proposto;

b) alterações ou desvios do planejamento inicial;

c) comprometimento dos envolvidos;

d) falhas nas estimativas de tempo e recursos, na execução, na comunicação ou no processo;

e) impactos do tempo de indisponibilidade ou de degradação do serviço nas atividades dos usuários; e

f) lições aprendidas e oportunidades de melhorias.

3.2.4. **Implementar mudança**

Atividade responsável por executar todos os procedimentos que foram previamente planejados para liberação, atentando para questões como serviços afetados, plano de contingência e realização dos testes.

3.2.5. **Atualizar agenda de mudanças**

Atividade responsável por realizar a atualização da agenda de mudanças, conforme a implementação da mudança realizada.

3.2.6. **Revisar e finalizar implementação da mudança**

Após a implementação da mudança, os resultados devem ser registrados e comunicados para avaliação dos responsáveis pela coordenação da implantação da mudança e para a Diretoria de Tecnologia da Informação e partes interessadas. Se a mudança foi concluída com êxito, devem ser concluídos também todos os registros associados à mudança como incidentes e problemas e devem ser solicitadas as atualizações de informações do sistema de gerenciamento da configuração para o processo de gerenciamento de configuração.

3.3. **Monitoramento**

A fase de monitoramento é responsável pela análise e a verificação dos resultados alcançados na mudança realizada. O principal objetivo desta fase é detectar eventuais erros ou falhas não identificados nas fases de planejamento e testes de forma a saná-las o mais breve possível. A figura 4 detalha as atividades que compõem esta fase.

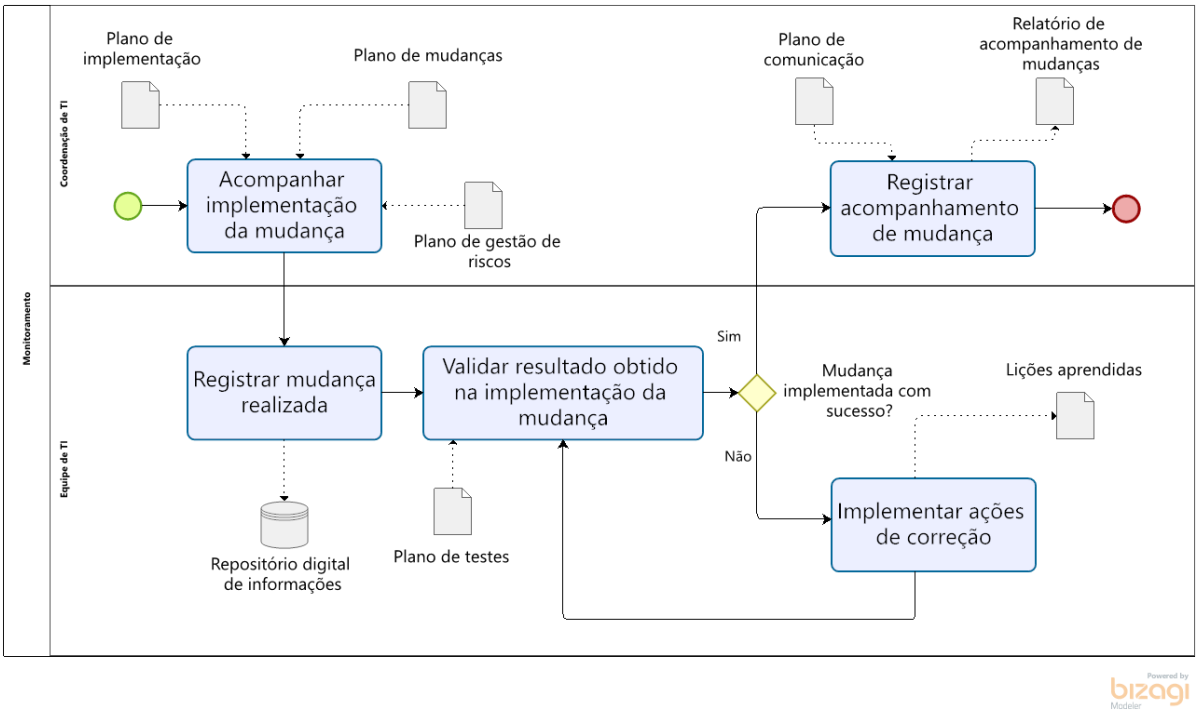


Figura 4 - Monitoramento

Conforme demonstra a figura 4 a fase de monitoramento é composta por entradas, 5 (cinco) atividades e saídas que serão detalhadas nas próximas seções.

3.3.1. **Acompanhar implementação da mudança**

Atividade responsável por acompanhar/rastrear a implementação da mudança de acordo com os planos: gestão de mudanças, implementação e gestão de riscos.

3.3.2. **Registrar mudança realizada**

O IFTO deve manter registros detalhados de todas as mudanças realizadas nos sistemas de segurança. Isso incluir documentar o motivo da mudança, quem a autorizou, quais sistemas foram afetados e como a mudança foi implementada. Todos os registros mencionados ou relacionados com a requisição da mudança devem ser atualizados e verificados antes do encerramento das atividades do processo. Esta atividade deve ser feita através do repositório digital de informações.

Não haverá encerramento automático de registros de incidentes, problemas ou requisições devido à finalização da mudança. Os registros dos itens de configuração, associados à mudança, devem ser atualizados se necessário.

Para garantir a consistência das informações, o processo de gerenciamento da configuração e ativos de TI deve ser acionado para a conferência ou atualização dos itens de configuração ao final de toda mudança. Em casos de falhas durante a implantação da mudança, planos de remediação devem ser utilizados.

3.3.3. **Validar resultado obtido na implementação da mudança**

A partir do plano de testes definido pela Coordenação de TI, a equipe deve validar o resultado obtido na implementação da mudança. É recomendável que esta

validação seja documentada através de lições aprendidas de forma que possa auxiliar a implementação de novas mudanças.

3.3.4. **Implementar ações de correção**

De acordo com os resultados apresentados pela atividade "validar o resultado obtido na implementação da mudança", a equipe de TI deve implementar ações de correção com a finalidade de obtenção dos resultados planejados. Após a implementação das ações de correção, as lições aprendidas devem ser registradas.

3.3.5. **Registrar acompanhamento de mudança**

Após a implementação das mudanças, o IFTO deve monitorar continuamente os sistemas de segurança para identificar quaisquer problemas ou anomalias resultantes das alterações. Deve-se realizar uma revisão pós implementação para avaliar o impacto das mudanças na segurança. Isso permite identificar problemas e ajustar os processos conforme necessário.

O gerenciamento de mudança tem como foco o controle, e garante que as mudanças sejam implantadas e testadas dentro do cronograma. Para isso é preciso o registro para acompanhamento da mudança em relatório de apropriado. Durante o registro da mudança deve ser declarada a necessidade de atualização de registros de conhecimento e dos itens de configuração.

3.4. **Aprendizado**

Esta fase garante o registro da execução de cada nova requisição de mudança a fim de economizar tempo de planejamento e implantação em futuras solicitações semelhantes. Ela é responsável por registrar o aprendizado obtido na implantação da mudança de forma a aprimorar o processo (lições aprendidas). A figura 5 apresenta o detalhamento desta fase.

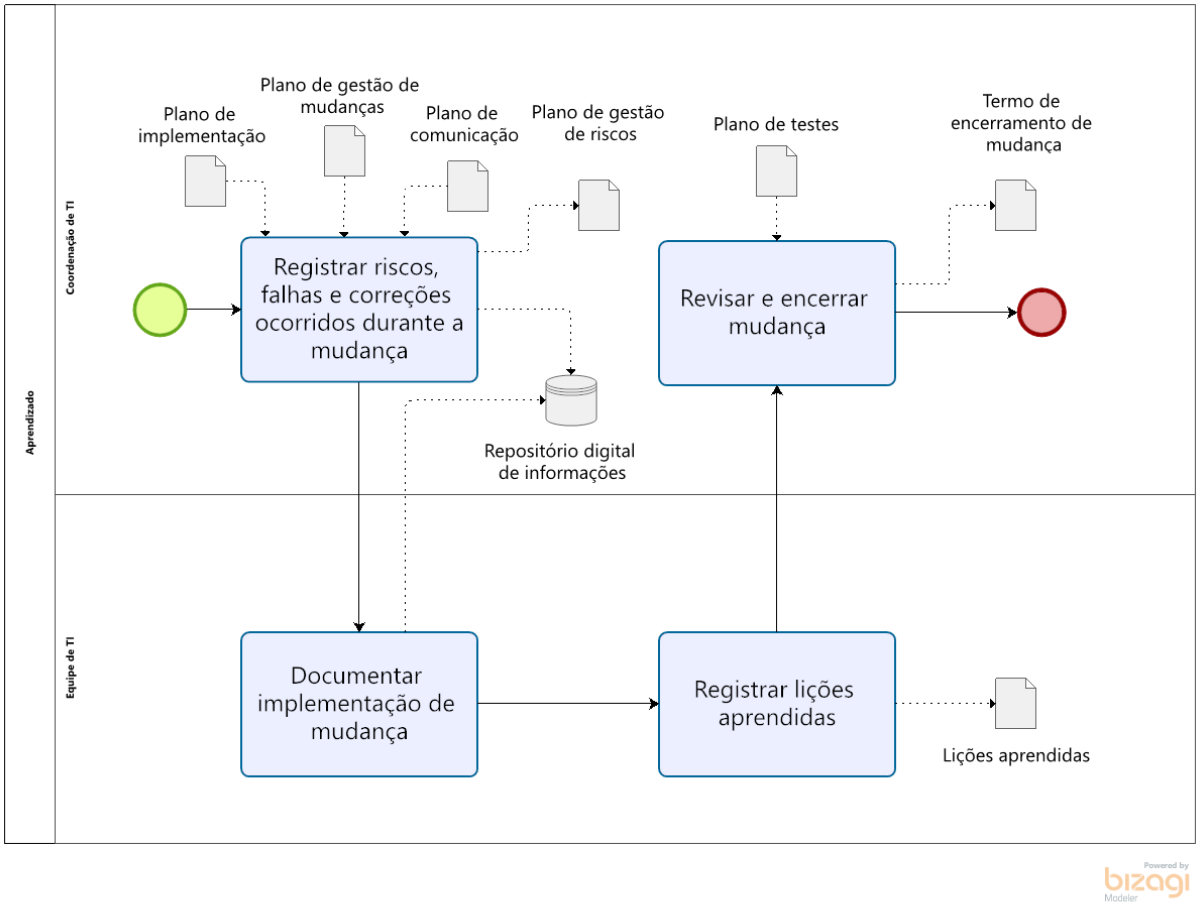


Figura 5 - Aprendizado

Conforme demonstra a figura 5 a fase de aprendizado é composta por entradas, 4 (quatro) atividades e saídas que serão detalhadas nas próximas seções.

3.4.1. Registrar riscos, falhas e correções ocorridos durante a mudança

A Coordenação de TI é responsável por registrar riscos, falhas e correções ocorridos durante a mudança. Os artefatos utilizados por esta atividade são: planos de implementação, gestão de mudanças, comunicação, gestão de riscos, repositório digital de informações e mapa de riscos. Esta atividade é responsável por avaliar a efetividade da mudança realizada. A partir dele é possível identificar ações corretivas, no caso de ocorrência de efeitos não identificados nas fases de planejamento e implementação (testes).

3.4.2. Documentar a implementação da mudança

Esta atividade é responsável por registrar a implementação da mudança. Este registro é feito através do repositório digital de informações. A equipe de TI deverá comunicar as mudanças planejadas à equipe de segurança e a outras partes interessadas relevantes. Além disso, garantir que a equipe esteja ciente das implicações de segurança das mudanças implementadas.

3.4.3. Registrar lições aprendidas

Atividade responsável pelo registro do aprendizado durante a execução da mudança. Recomenda-se que todos os membros da equipe de TI que participaram da

implementação da mudança devem registrar as lições aprendidas de forma que o processo possa ser aprimorado cada vez mais.

3.4.4. **Revisar e encerrar a mudança**

As mudanças implantadas, com exceção das mudanças padrões, precisam ser avaliadas após certo tempo. Esta atividade realiza a revisão da mudança ocorrida. Para isso, deve ser utilizado o plano de testes como artefato de revisão. Os resultados obtidos com a execução desta atividade deverão ser registrados no termo de encerramento da mudança. Esta atividade deverá responder os seguintes questionamentos:

a) A mudança cumpriu com seu objetivo?

b) Os usuários ficaram satisfeitos com o resultado?

c) Ocorreu algum efeito colateral?

d) Os custos e esforços estimados excederam?

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. A seguir são apresentados os papéis envolvidos no processo de gerenciamento de mudança proposto para a área de TI.

4.1. **Alta Administração**

Este papel representa o mais alto nível estratégico e decisório do IFTO, 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 mudanças, 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, norma interna complementar e processo de gestão de mudanças no âmbito do IFTO.

4.2. **Comitê de Segurança da Informação**

Este grupo de pessoas representam áreas finalísticas do IFTO. Compete a este grupo de pessoas a seguinte responsabilidade:

a) avaliar e aprovar a política, norma interna complementar e processo de gestão de mudanças.

4.3. **Gestor de Segurança da Informação**

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

a) propor a política, norma interna complementar e processo para gestão de gestão de mudanças;

b) elaborar e coordenar o processo de gestão de gestão de mudanças; e

c) designar um agente responsável pela execução das atividades referentes ao processo de gestão de mudanças, dentre os servidores efetivos do IFTO.

4.4. **Equipe de Tratamento e Resposta a Incidentes Cibernéticos**

Este grupo de pessoas é 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 a política, norma interna complementar, processo, plano, procedimentos e atividades sobre gestão de mudanças.

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

Agente responsável pela execução das atividades referentes ao processo de gestão de mudanças. Setor responsável por assegurar a execução da política, norma interna complementar, processo e atividades de controle de acesso no âmbito do IFTO. Neste sentido, compete a este setor as seguintes responsabilidades:

a) receber, registrar e alocar as propriedades para todas as RDMs e rejeitar qualquer mudança que seja totalmente impraticável;

b) garantir a especificação e execução do processo;

c) definir hierarquia para autorização das requisições de mudança;

d) definir fluxo de tratamento das requisições de mudança;

e) trabalhar com outras áreas para garantir uma abordagem integrada do gerenciamento de mudanças nos serviços de TI;

f) manter o desenho e indicadores do processo, garantindo que estejam adequados aos propósitos da organização;

g) prover recursos para execução das atividades do processo;

h) garantir que as metas de desempenho e eficiência do processo sejam atingidas;

i) autorizar a solicitação de mudança;

j) publicar a programação de mudanças;

k) solicitar a atualização dos registros associados;

l) finalizar a solicitação de mudança;

m) treinar os atores do processo nos procedimentos e atividades;

n) acompanhar a qualidade do atendimento das solicitações de mudanças;

o) manter a documentação do processo atualizada;

p) gerenciar a implementação, bem como a execução do processo durante todo o seu ciclo de vida; e

q) fornecer os recursos necessários para a execução do processo.

4.6. **Coordenações de TI**

Este papel é realizado pelas coordenações de áreas de TI. Tem as seguintes responsabilidades:

a) verificar a conformidade da mudança;

b) devolver a requisição de mudança;

c) planejar e executar atividades relacionadas ao processo;

d) identificar, analisar e definir ações para os principais riscos que possam impactar o sucesso da mudança;

e) elaborar, manter e divulgar a agenda de mudanças;

f) gerenciamento operacional das atividades do processo, integração com outros processos e produção de relatórios gerenciais;

g) promover e garantir que o processo seja corretamente utilizado;

h) coordenar as interfaces entre o gerenciamento de mudanças e os outros processos, especialmente o gerenciamento de liberações e implantação e o gerenciamento da configuração e ativo de serviço;

i) aferir os indicadores de desempenho do processo;

j) elaborar e divulgar relatórios de desempenho da execução do processo;

k) manter o registro de melhorias do processo;

l) revisar a requisição de solicitação de mudança;

m) revisar mudança pós implantação;

n) avaliar e priorizar mudança em pauta;

o) coordenar a execução de solicitação de mudanças autorizadas;

p) garantir que a comunicação seja realizada durante o processo;

q) consolidar pauta de reunião;

r) comunicar a mudança aos envolvidos e impactados; e

s) encerrar a mudança.

4.7. **Equipe de TI**

Este papel é realizado por analistas de TI e técnicos de TI. Esta equipe tem as seguintes responsabilidades:

a) analisar, mudanças categorizadas como tipo planejada/normal;

b) validar, aprovar ou rejeitar mudanças emergenciais;

c) controlar o serviço e componentes de TI que foram alterados pela mudança, mantendo as informações de configuração precisas e confiáveis;

d) analisar os riscos das solicitações de mudanças;

e) implementar a solicitação de mudança;

f) dar atendimento às requisições, incidentes ou problemas encaminhados para abertura de solicitação de mudanças;

g) definir as atividades técnicas do plano de implementação e do plano de teste das solicitações de mudanças;

h) explicitar os riscos e benefícios da solicitação de mudanças;

i) executar as atividades programadas;

j) assegurar o registro adequado de todas as requisições de mudanças;

k) apoiar a classificação e priorização de todas as mudanças registradas;

l) comunicar com o líder da mudança sobre a execução das atividades;

m) fornecer *feedback* técnico a respeito das atividades, riscos e viabilidade das solicitações de mudança;

n) cooperar com a Coordenação de TI durante o planejamento da solicitação de mudança;

o) realizar o desenvolvimento, testes e implantação da mudança; e

p) elaborar e manter atualizado os artefatos do processo.

4.8. **Usuário (Solicitante)**

Pessoa responsável por abrir a requisição de mudança. Qualquer gestor ou usuário que necessite que requisite uma alteração no serviço de TI. Este papel tem as seguintes responsabilidades:

a) requisitar mudanças provenientes de requisições, incidentes, problemas, configuração, nível de serviço ou projetos para as áreas técnicas e fornecer informações complementares durante o processo de mudança;

b) solicitar alterações em funcionalidades de sistemas;

c) solicitar modificações de componentes de *hardware*;

d) solicitar alterações de versão de *software*;

e) solicitar atualização de equipamentos;

f) informar as suas necessidades de forma clara;

g) cooperar com o líder da mudança durante o planejamento da solicitação de mudança; e

h) fornecer resposta necessária para validação dos efeitos da mudança.

5. **MATRIZ RACI**

A matriz RACI apresentada na tabela 2 é um método utilizado para definir com clareza os papéis e responsabilidades de cada ator na execução da atividade relacionada ao 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; representa quem irá, de fato executar a tarefa. Deve haver ao menos um por tarefa;

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*; Define quem será responsável pelo sucesso da atividade. Fica encarregado de verificar se a atividade foi realizada com sucesso e dentro do prazo. Deve haver um, e apenas um, por atividade;

c) ***consulted (consultado):*** pessoa que deve ser consultada durante a execução da atividade; As informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade; Geralmente exercem papel de conselho na tomada de decisões;

d) ***informed (informado):*** pessoa que será informada acerca do progresso da execução da atividade.

Tabela 2 - Matriz de responsabilidades

Fase	AA	CSI	GSI	DTI	CTI	ETI	U
Planejamento	C	C	C	A	R	C	I
Implementação	C	C	C	A	R	C	I
Monitoramento	C	C	C	A	R	C	I
Aprendizado	C	C	C	A	R	C	I

Legenda:

AA: Alta Administração.

CSI: Comitê de Segurança da Informação.

GSI: Gestor de Segurança da Informação.

DTI: Diretoria de Tecnologia da Informação.

CTI: Coordenação de TI.

ETI: Equipe de TI.

U: Usuário (Solicitante).

6. INDICADOR DE DESEMPENHO

O processo de gestão de mudanças deve ser monitorado e avaliado periodicamente através de indicador de desempenho de forma a promover eventuais ajustes necessários e estar em conformidade com os padrões do mercado. Esta avaliação tem como objetivo acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. Para medir a eficiência deste processo foi definida a métrica operacional detalhada na tabela 3.

Tabela 3 - Indicador de desempenho

Indicador	Número de requisições atendidas.
Descrição	Índice de requisições atendidas durante o ano.
Objetivo	Medir a quantidade de requisições de mudanças atendidas durante o ano.
Periodicidade	Anual.
Fonte	SUAP.
Fórmula	Total de requisições atendidas durante o ano.
Unidade de medida	Crescente.
Meta	Acompanhar a resolução de requisições durante o ano.

Fonte: SUAP

7. PROCESSOS RELACIONADOS

Para que este processo seja executado de forma eficiente, ele interage com vários processos relacionados com a governança de TI, conforme demonstra a figura 6.

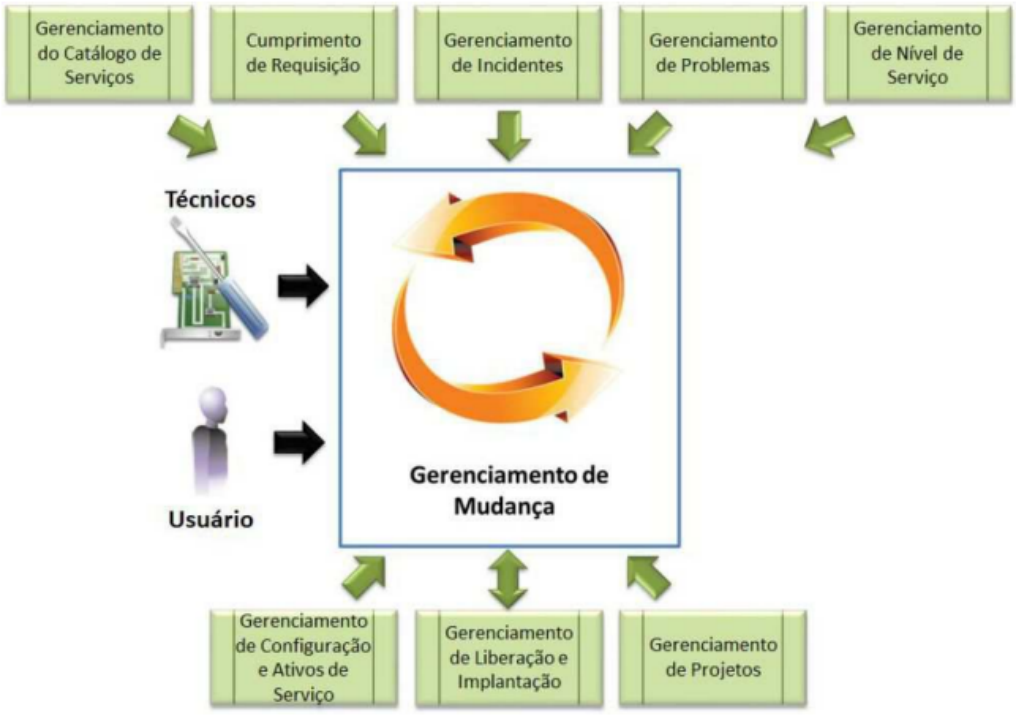


Figura 6 - Contexto do processo de gestão de mudanças (TRT7, 2016)

Além dos processos de governança de TI o processo de gestão de mudanças faz parte dos processos que compõem o sistema de gestão de segurança da informação do IFTO (SGSI-IFTO), conforme mostra a figura 7.

Figura 7 - Processos que compoẽm 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 processo de gestão de mudanças nos aspectos de segurança da informação deve ser respaldado pelas informações levantadas no relatório de identificação, análise e avaliação de riscos de segurança da informação e no relatório de tratamento de riscos de segurança da informação.

2. O processo de gestão de mudanças nos aspectos de segurança da informação além de promover o controle das mudanças planejadas, deve considerar a análise crítica das consequências de mudanças não previstas, atuando em ações para amenizar os efeitos adversos.

3. Para que uma mudança ocorra é necessária a existência de uma requisição. Toda requisição de mudança (RDM) deve ter associação com, pelo menos, um registro de incidente, de problema ou de requisição de serviço.

4. Toda e qualquer requisição de mudança obrigatoriamente deve estar registrada na Central de Serviços (SUAP).

5. Antes de implementar qualquer mudança, deve-se avaliar os possíveis impactos na segurança da informação. Deve-se identificar ameaças potenciais e avaliar os riscos associados.

6. O IFTO deve ter políticas claras de segurança da informação.

7. As mudanças devem ser avaliadas por pessoas que sejam capazes de compreender os riscos e os benefícios esperados.

8. As mudanças em sistemas de informação deverão ser acordadas com a área demandante antes de serem implantadas.

9. O IFTO deve documentar procedimentos para mudanças, incluindo aprovações necessárias e requisitos de segurança a serem considerados em todas as etapas.

10. Para a realização de mudanças deve-se estabelecer uma equipe composta por representantes de diferentes áreas para garantir uma visão abrangente.

11. Mudanças devem ser previamente comunicadas a todas as partes interessadas que possam ser afetadas. Todos os envolvidos devem estar cientes dos motivos, benefícios e possíveis impactos das mudanças na segurança da informação.

12. Testes de segurança devem ser realizados antes e após implementar as mudanças para identificar possíveis vulnerabilidades ou falhas de segurança.

13. Backups regulares de dados devem ser realizados.

Planos de contingência devem ser estabelecidos em caso de problemas durante e após a implementação das mudanças.

14. Um sistema de monitoramento contínuo deve ser estabelecido para acompanhar as mudanças implementadas e detectar quaisquer anomalias de segurança.

15. Após a implementação das mudanças, deve-se avaliar os resultados. Deve-se analisar se os objetivos de segurança foram alcançados e se há áreas que precisam ser melhoradas.

16. Revisões regulares das práticas de gestão de mudanças em segurança da informação devem ser realizadas para garantir que estejam alinhadas com as necessidades atuais e as melhores práticas.

17. A equipe responsável pela execução de mudanças deve receber treinamentos regulares sobre novas ameaças, técnicas de segurança e procedimentos de gestão de mudanças.

9. REFERÊNCIAS

BRASIL. Presidência da República. Gabinete de Segurança da Informação. **Instrução Normativa nº 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. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172 Acesso em: 4 jan 2024.

MELENDEZ Filho, Rubem. **Service Desk Corporativo: Solução com base na ITIL V3**. São Paulo: Novatec Editora, 2011.

Office of Government Commerce (OGC, 2007). **ITIL: The Official Introduction to the ITIL Service Lifecycle**. London: TSO (The Stationary Office), 2007. ISBN 9780113310616. Disponível em: <https://www.kornev-online.net/ITIL/The%20Official%20Introduction%20to%20the%20ITIL%20Service%20Lifecycle.pdf>. Acesso em: 10 jan. 2021.

TRIBUNAL REGIONAL DO TRABALHO da 7ª Região. **Processo de Gerenciamento de Serviços de TI.** Disponível em: https://www.trt7.jus.br/files/institucional/governanca_ti/processos/servicos/Processos-Servicos-TI.pdf. 2016. Acesso em: 27 jun. 2022.

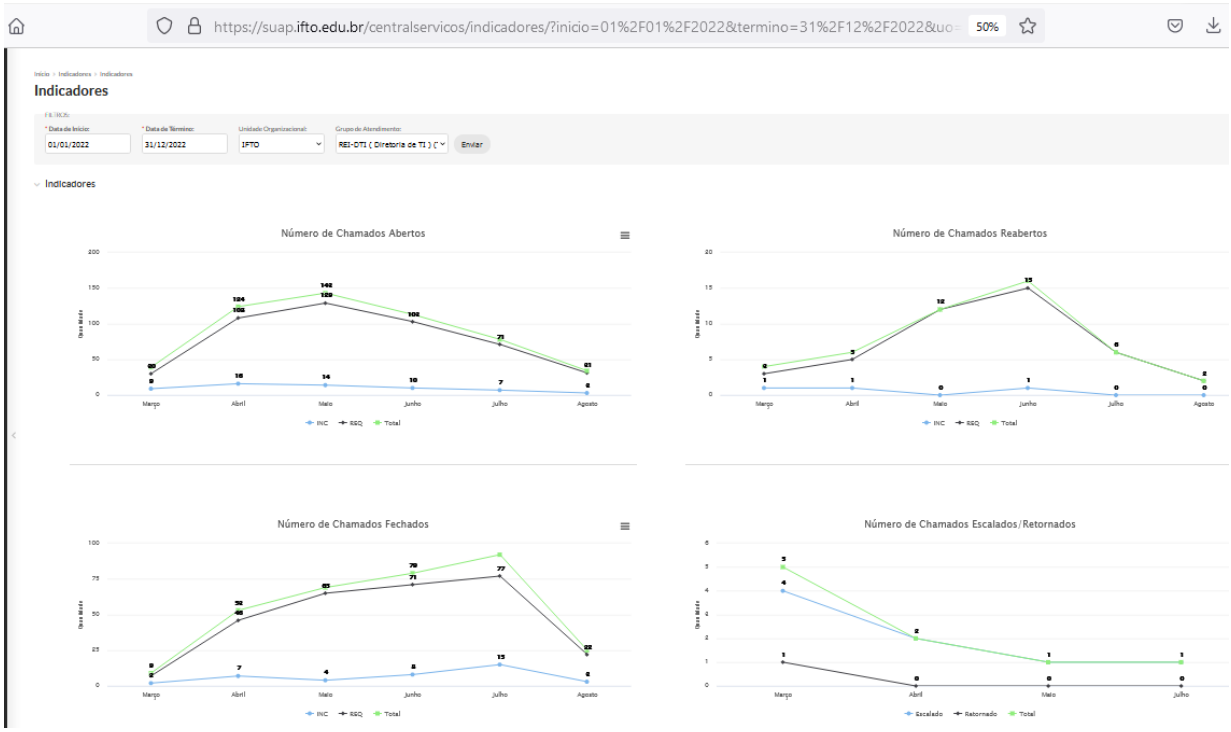
TRIBUNAL REGIONAL DO TRABALHO da 13ª Região. **Manual do processo de gerenciamento de mudanças.** Disponível em: https://www.trt13.jus.br/institucional/gestao-estrategica/governanca/publicacoes/trt-13/setic/escritorio-de-processos/processo-de-gerenciamento-de-mudancas/manual-do-processo-gerenciamento-de-mudancas.pdf. 2018. Acesso em: 16 set. 2022.

ANEXO I
Serviços e ativos de informação que podem ser afetados por mudança

Serviço/ativo de TI	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

ANEXO II
Indicadores de mudanças apresentados pela Central de Serviços - SUAP



Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 08/01/2024, às 15:37, 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 **2236360** e o código CRC **4B67EA8C**.

Referência: Processo nº 23235.000383/2021-09 SEI nº 2236360