RESOLUÇÃO Nº 05, DE 30 DE SETEMBRO DE 2022,

DO COMITÊ DE GOVERNANÇA DIGITAL

Dispõe sobre o Plano de Gestão de Mudanças de TIC do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

O PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, no uso das atribuições que lhe foram conferidas pelo Art. 6º, inciso IV e Art. 9º, deste comitê.

RESOLVE:

Art. 1º Aprovar o Plano de Gestão de Mudanças de TIC do Instituto Federal de Santa Catarina.

Art. 2º Esta Resolução entra em vigor na data de 01 de novembro de 2022.

IFSC
Documento assinado digitalmente
JESUE GRACILIANO DA SILVA
Data: 27/10/2022 08:24:45-0300
CPF: 110.559.078-07
Verifique as assinaturas em https://v.ifsc.edu.br

Jesué Graciliano da Silva

Presidente do Comitê de Governança Digital

Súmula da reunião do CGD disponível em: https://sigrh.ifsc.edu.br/sigrh/downloadArquivo?idArquivo=2825847&key=1f546b9deb9b38d3c5a9bf9f59bbdb43

PLANO DE GESTÃO DE MUDANÇAS DE TIC

INSTITUTO FEDERAL
Santa Catarina

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA

Plano de Gestão de Mudanças de TIC
PGMS - TIC

Florianópolis – Novembro/2022

COMITÊ DE GOVERNANÇA DIGITAL

Presidência

Jesué Graciliano da Silva

Pró-reitor de Desenvolvimento Institucional

Secretário-Executivo

Benoni de Oliveira Pires – Diretor de TIC

Membros do Comitê de Governança Digital

Titulares

Aloísio da Silva Júnior – Pró-reitor de Administração

Jesué Graciliano da Silva – Pró-reitor de Desenvolvimento Institucional

Adriano Larentes da SIlva – Pró-reitor de Ensino

Valter Vander da Silveira – Pró-reitor de Extensão e Relações Externas

Flavia Maia Moreira – Pró-reitora de Pesquisa, Pós-Graduação e Inovação

Tiago Semprebom – Colégio de Dirigentes (São José)

Daniel Fernando Carossi – Colégio de Dirigentes (São Lourenço do Oeste)

Evaristo Marcos de Quadros Júnior – Encarregado do Tratamento dos Dados Pessoais

Suplentes

Eliana Cristina Bar – Colégio de Dirigentes (Palhoça)

José Roberto Machado – Colégio de Dirigentes (Jaraguá do Sul)

Sumário

TERMOS E ABREVIAÇÕES

DSI - Departamento de Sistemas

MOC - Management of Change (Gestão de Mudanças)

PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação

PETIC - Planejamento Estratégico de Tecnologia da Informação e Comunicação

PGR/TIC - Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação

PO - Product Owner

SGCN/TIC - Sistema de Gestão de Continuidade de Negócios de Tecnologia da Informação e Comunicação

RDM - Requisição de Mudança

TAEs - Técnicos-Administrativos em Educação

TIC - Tecnologia da Informação e Comunicação

GLOSSÁRIO

Mudança - Acréscimo, modificação ou remoção de qualquer coisa que possa afetar os Serviços de TI;

Gestão de Mudanças - Atividades coordenadas para dirigir e controlar uma organização no que se refere a mudanças.

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
09/2022	Versão 1.0	Gestão de Mudanças de Segurança da Informação

APRESENTAÇÃO

O DOCUMENTO

O Plano de Gestão de Mudanças de Segurança de TIC (PGMS TIC), tem seu escopo inicialmente limitado ao atendimento da Instrução Normativa 03 de 28 de Maio de 2021, publicada pelo Gabinete de Segurança Institucional da Presidência da República.

Sua implementação tem por objetivo preparar e adaptar o Instituto Federal de Santa Catarina - IFSC 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.

Objetivo do PGMS-TIC

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 e deverá observar as informações levantadas no Relatório de identificação, análise e avaliação de riscos de segurança da informação e também no Relatório de tratamento de riscos de segurança da informação, desenvolvidos pelo CSIRT.

Legislação de Referência

Instrução Normativa GSI/PR Nº 03, 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.

CLASSIFICAÇÃO DAS MUDANÇAS

As mudanças devem ser classificadas de acordo com quatro momentos distintos.

Emergencial

Para que uma mudança seja classificada como emergencial, deve existir uma justificativa importante, caracterizada pela perda de dados ou parada de algum serviço em produção, necessitando portanto uma imediata intervenção. ocorre, geralmente, em função de:

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

b. alteração normativa de aplicação imediata;

c. necessidade de modificação significativa imediata nos ativos de informação;

d. outros eventos similares;

Eventuais mudanças necessárias neste estágio, devem ser submetidas aos responsáveis competentes, de acordo com Sistema de Gestão de Continuidade de Negócios (SGCN - IFSC).

Rotineira

Mudanças de níveis contínuos, devem obedecer ritos e procedimentos já estabelecidos pelas áreas de tecnologia voltadas para programação e implantação de sistemas. A equipe técnica já possui elevado grau de conhecimento e discernimento necessário para realizar a atividade e que ocorre, geralmente, em função de:

a. atualização da infraestrutura de tecnologia da informação;

b. serviços de tecnologia da informação com periodicidade habitual que impliquem mudanças de um ou mais aspectos de segurança; e

c. outros eventos similares;

Nestas, se faz necessário um elevado nível de conhecimento da estrutura atualmente em funcionamento, para garantir sua continuidade com o menor nível possível de riscos.

Para correta classificação do tipo de mudança neste nível, deve-se utilizar o Plano de Gestão de Riscos (PGR - IFSC), no qual deverá ser apontado e mitigados eventuais riscos.

Proativa

Mudanças proativas devem ser abordadas sempre que houver visão de oportunidade de melhoria, economicidade, aumento de eficiência ou eventual redução de riscos. Se busca trazer maior eficiência para a organização e que ocorre geralmente em função de:

a. ampliação do parque computacional;

b. obsolescência prevista de equipamentos e processos;

c. necessidade de adoção de novas tecnologias; e

d. outros eventos similares.

Eventos estes, nos quais pode-se antever obsolescência tecnológica, encerramentos de contratos (por vencimento ou não), adoção de novas tecnologias ou novas oportunidades de melhoria.

Reversão

Atividades a serem executadas para desfazer a mudança e voltar para o estado inicial.

Esta possibilidade deverá sempre ser avaliada quando o procedimento de mudança não ocorreu como esperado ou deixou-se de existir o fato gerador da mudança.

Cabe ainda adotar a reversão da mudança, sempre que alguma regulamentação ou demanda demonstrar essa necessidade.

PAPÉIS E RESPONSABILIDADES

Demandante

Este ator é o dono do processo, e deve ser o encarregado pela área demandante e tem a responsabilidade de:

I. Ser responsável pela especificação do processo de gestão da mudança e garantir a execução do mesmo;

II. Dar assessoria ao gestor de segurança da informação e ao setor responsável pela mudança, sempre que lhe for solicitado;

III. Garantir a execução do processo pela estrutura organizacional;

IV. Realizar as mudanças necessárias na especificação da Gestão de Mudanças quando couber.

V. Testar e avaliar as mudanças implementadas pelas áreas de TIC.

Gestor de segurança da informação

Cabe ao gestor de segurança da informação, com relação ao processo de gestão de mudanças nos aspectos de segurança da informação:

I. coordenar a gestão de mudanças;

II. designar o agente responsável pela gestão de mudança, dentre os servidores efetivos do órgão;

III. analisar e encaminhar o documento de descrição e aprovação de mudança para apreciação da alta administração do órgão, à qual cabe a decisão de aprovar ou indeferir a mudança; e

IV. proporcionar a interação constante entre as equipes de gestão de mudanças em aspectos de segurança da informação, de gestão de riscos de segurança da informação e de gestão de continuidade de negócios em segurança da informação.

Agente responsável pela gestão de mudança

Cabe ao agente responsável pela gestão de mudança nos aspectos de segurança da informação:

I. recomendar à alta administração da instituição de um grupo técnico de mudança, composto por servidores das áreas afetadas e da área de segurança da informação para a elaboração do documento de avaliação e aprovação de mudança;

II. elaborar, juntamente com o grupo técnico de mudança, o documento de avaliação e aprovação de mudança e submetê-lo à análise do gestor de segurança da informação;

III. acompanhar, juntamente com o grupo técnico de mudança, os testes da mudança aprovada pelo documento de avaliação e aprovação de mudança;

IV. acompanhar, juntamente com o grupo técnico de mudança, a implementação da solução aprovada no documento de avaliação e aprovação de mudança;

V. assegurar, juntamente com o grupo técnico de mudança, registro de auditoria contendo todas as informações relevantes relacionadas com a mudança; e

VI. informar ao gestor de segurança da informação sobre o andamento e a conclusão do processo.

MODELOS DE DOCUMENTOS

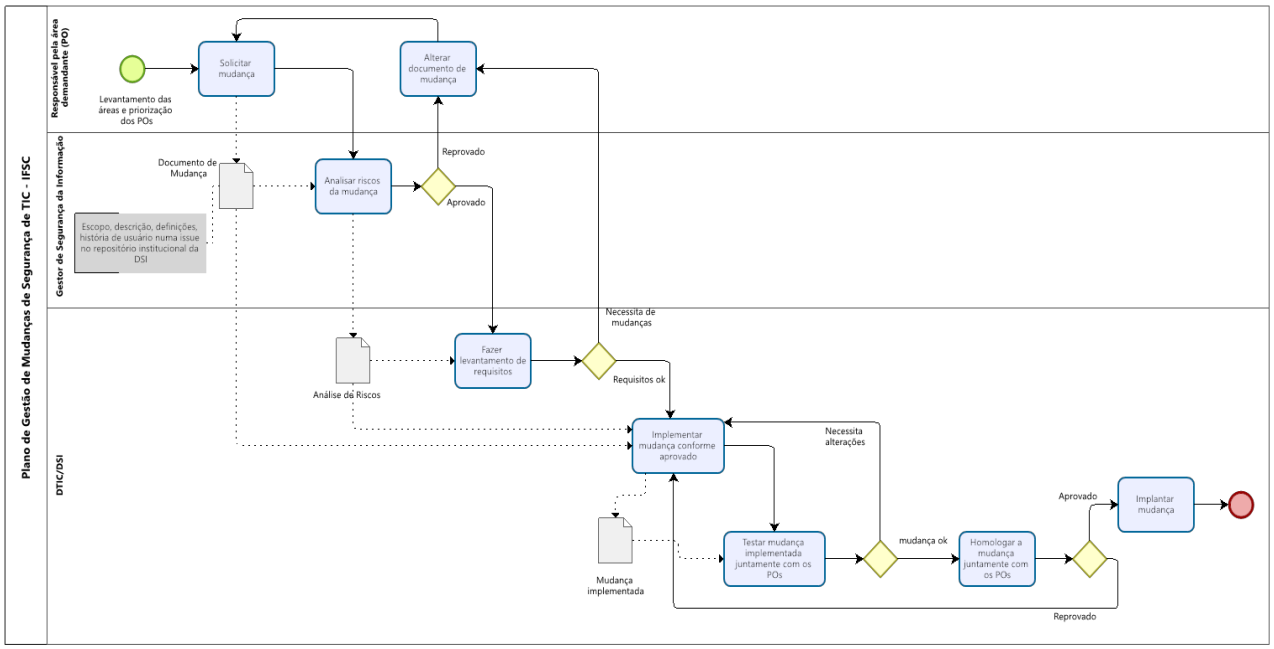
As requisições de mudanças (RDMs), devem ter um escopo claramente definido e documentado. Para tal, deve ser registrado através de instrumento específico, contendo no mínimo os dados elencados nos modelos do Anexo I e II.

PROCESSO

MUDANÇAS DE SOFTWARE DESENVOLVIDOS PELA DSI

O processo de mudanças de softwares desenvolvidos no âmbito do Departamento de Sistemas segue, de forma geral, o seguinte fluxo:

1. Solicitação da mudança pela área demandante;
2. Análise de riscos da mudança;
3. Levantamento de requisitos com os POs;
4. Inserção do escopo, descrição, definições, história de usuário numa issue no repositório institucional da DSI;
5. Desenvolvimento da mudança de software;
6. Homologação da mudança pelo PO e desenvolvedores;
7. Disponibilização da mudança pela DSI.



A solicitação de mudança pode ser encaminhada para a DSI das seguintes formas:

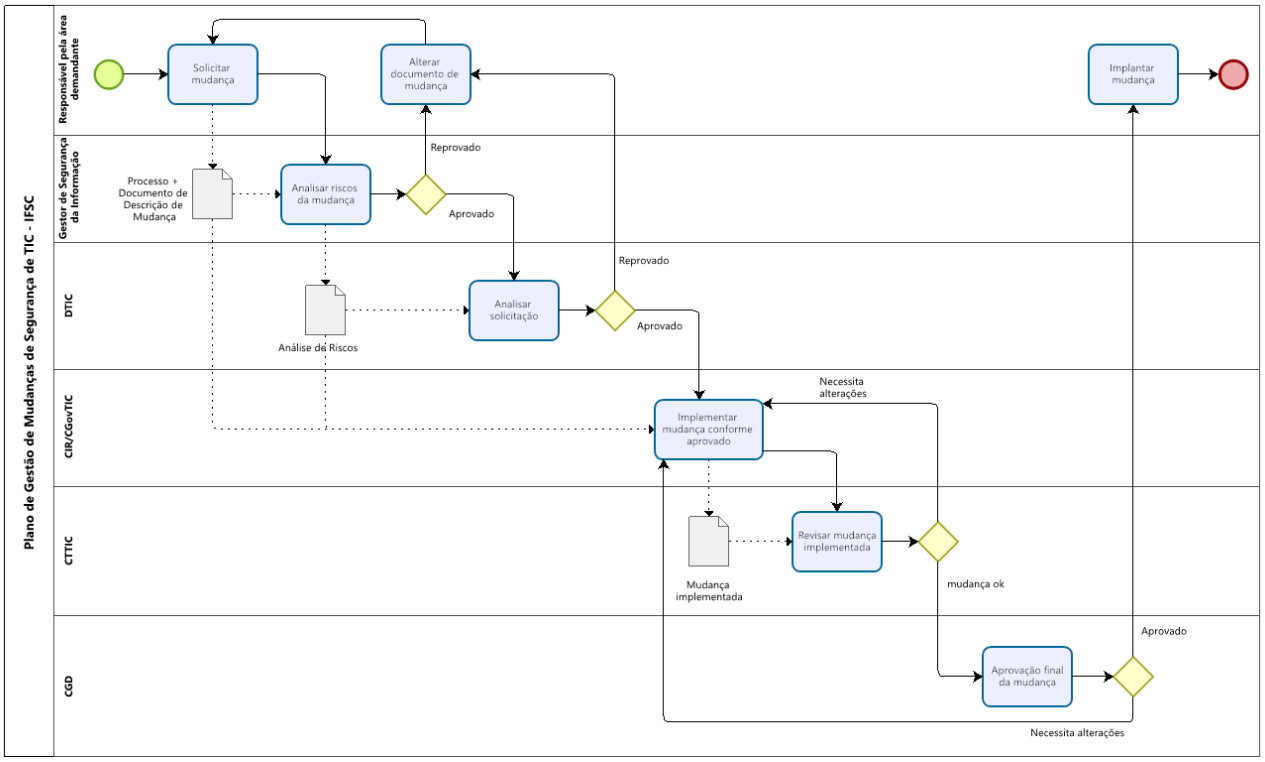
1. Reunião de priorização realizada quinzenalmente com representantes das Pró-Reitorias, que coletam e encaminham, no âmbito das Pró-Reitorias e instituição, as respectivas necessidades;
2. Solicitação pela Diretoria de Tecnologia da Informação, pelo Pró-Reitor de Desenvolvimento Institucional ou para o atendimento de demandas legais;
3. Notificação pelo CSIRT, CIR, DSI, CGovTI de vulnerabilidade ou incidente.

Atendimentos de demandas que sejam correspondentes a *bugs* podem ser reportados através do sistema de chamados institucional.

OUTRAS MUDANÇAS

O processo de requisição e aprovação de mudanças deve seguir o seguinte fluxo:

1. Solicitação de mudança pelas áreas demandantes;
2. Análise de riscos pelo Gestor de Segurança da Informação;
3. Aprovação inicial pela chefia DTIC;
4. Implementação da mudança pela área de Redes ou Governança;
5. Revisão pelo CTTIC (Comitê Técnico de Tecnologia da Informação e Comunicação);
6. Aprovação final pelo CGD (Comitê de Governança Digital);
7. Implantação da Mudança.



ANEXO I

DOCUMENTO DE DESCRIÇÃO DE MUDANÇA

O documento de descrição de mudança tem o objetivo de identificar o tipo de alteração pretendida, de forma a adequar a organização às transformações nos contextos interno e externo.

Os titulares das unidades demandantes da mudança são responsáveis pela elaboração e aprovação do documento* mencionado, o qual deverá ser remetido ao agente responsável pela gestão de mudanças nos aspectos de segurança da informação.

Descrição	Área responsável
I - agente demandante;	
II - unidade de origem;	
III - descrição da mudança;	
IV - tipo de mudança;	
V - objetivo(s) da mudança com os fatores que levaram a esta necessidade;	
VI - Elementos de segurança da informação envolvidos?	
VII - benefícios esperados.	

*No caso de softwares, pode-se substituir este documento pelo de uso de softwares de controle de versão e repositórios, que resulta em uma série de benefícios para a organização. Recomenda-se que o documento de descrição de mudança esteja em formato de issue ou comentário que contenha, de forma geral, o conteúdo abaixo no corpo do texto. A alternativa é a elaboração individual de um documento para cada mudança.

ANEXO II

DOCUMENTO DE AVALIAÇÃO E APROVAÇÃO DE MUDANÇA

O documento de avaliação e aprovação de mudança tem o objetivo de:

I. analisar as mudanças demandadas;

II. recomendar quais mudanças devem ser aprovadas; e

III. sugerir as alternativas para a implementação das mudanças.

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

Descrição	Mudança
I - alternativas para implementação da mudança, com a descrição básica dos procedimentos necessários para sua execução;	
II - recomendações, em ordem de prioridade, das alternativas a serem adotadas;	
III - relação entre a mudança pretendida e outras alterações que, eventualmente, possam ocorrer simultaneamente;	
IV - análise de risco dos ativos de informação que serão afetados pela mudança;	
V - avaliação do impacto do adiamento da realização da mudança;	
VI - definição da alternativa a ser implementada ou indeferimento da mudança proposta pela alta administração do órgão ou da entidade;	
VII - análise crítica das consequências de mudanças não previstas e de ações propostas para mitigação das eventuais consequências negativas.	

*No caso de softwares, pode-se substituir este documento pelo de uso de softwares de controle de versão e repositórios, que resulta em uma série de benefícios para a organização. Recomenda-se que o documento de descrição de mudança esteja em formato de issue ou comentário que contenha, de forma geral, o conteúdo abaixo no corpo do texto.

REFERÊNCIAS

I - Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.