

RESOLUÇÃO CGTIC Nº 02, DE 09 DE OUTUBRO DE 2020

Aprova o Plano de Gestão de Riscos de TIC do IFSC.

O PRESIDENTE DO COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, no uso das atribuições que lhe foram conferidas pelo pelo Art. 5º, inciso II e Art. 6º deste comitê.

RESOLVE:

Art. 1º Aprovar, o Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação do IFSC em atendimento a Norma Complementar do GSIPR 04/IN01/DSIC/GSIPR de 14/08/2009, a Resolução do Conselho Superior 052/2016 que aprova a Política de Segurança da Informação e Comunicação, a Resolução do Conselho Superior 034/2017 que aprova a Política de Governança de TIC do IFSC.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

ANDRÉ DALA POSSA

Autorizado conforme despacho no documento n.º 23292.039857/2020-13



**INSTITUTO
FEDERAL**
Santa Catarina

Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação

PGR - TIC

Outubro/2020



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

Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação

PGR - TIC

Versão 1.0

Florianópolis – Outubro/2020



Reitor

André Dala Possa

Pró-Reitor Desenvolvimento Institucional

Egon Sewald Junior

Diretor de Tecnologia da Informação e Comunicação

Benoni de Oliveira Pires

Coordenador de Governança de TIC

Farleir Luís Minozzo

Elaboração do PGR-TIC

Aline Pacheco Primão

Sumário

HISTÓRICO DE VERSÕES	7
PLANEJAMENTO DE EXECUÇÃO	8
TERMOS E ABREVIações	9
APRESENTAÇÃO	11
INTRODUÇÃO	11
PLANO DE GESTÃO DE RISCOS DE TIC	12
FERRAMENTAS E METODOLOGIA DE TRABALHO	13
FERRAMENTAS	13
METODOLOGIA	13
DOCUMENTOS DE REFERÊNCIA	13
VIGÊNCIA	14
ABRANGÊNCIA	14
REVISÕES	14
APROVAÇÃO E PUBLICAÇÃO	14
VALIDAÇÃO DO PLANO	15
SETORES ENVOLVIDOS NO PLANO	15
OBJETIVO	16
CONCEITOS E DEFINIÇÕES	16
PROCEDIMENTOS	18
Identificação dos Processos de TIC	19
Análise/Avaliação de Riscos	30
Identificação dos Riscos de TIC	31
Avaliação de Consequências	31
Estimativa do Risco	32
Tratamento dos Riscos	34
Monitoramento e Análise Crítica	35
Aceitação do Risco	35
Comunicação do Risco	36
PAPÉIS E RESPONSABILIDADES	37
AUTORIDADES RESPONSÁVEIS	37
REFERÊNCIAS	38
Anexo I	39
Anexo II	65

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
30/04/2020	Versão 1.0	Versão Inicial do Plano de Gestão de Riscos de TIC: Infraestrutura de TIC - Reitoria Infraestrutura de Apoio à TIC - Reitoria Armazenamento e Processamento de Dados - Reitoria Sistemas - Reitoria Segurança de Redes - Reitoria Recursos Humanos de TIC - Reitoria Processos de Negócio de TIC - Reitoria

PLANEJAMENTO DE EXECUÇÃO

Data	Descrição
30/08/2020	Versão Inicial do Plano de Gestão de Riscos - Banco de Dados - Reitoria
30/08/2020	Versão Inicial do Plano de Gestão de Riscos - Recursos Humanos de TIC - Câmpus
30/09/2020	Plano de Gestão de Riscos - Riscos do Câmpus Urupema
30/10/2020	Plano de Gestão de Riscos - Riscos do Câmpus São Lourenço do Oeste
30/11/2020	Plano de Gestão de Riscos - Riscos do Câmpus São Miguel do Oeste
30/12/2020	Plano de Gestão de Riscos - Riscos do Câmpus São Carlos
30/02/2021	Plano de Gestão de Riscos - Riscos do Câmpus Canoinhas
30/03/2021	Plano de Gestão de Riscos - Riscos do Câmpus Palhoça Bilíngue
30/04/2021	Plano de Gestão de Riscos - Riscos do Câmpus Cerfead
30/05/2021	Plano de Gestão de Riscos - Riscos do Câmpus Xanxerê
30/07/2021	Plano de Gestão de Riscos - Riscos do Câmpus Tubarão
30/09/2021	Plano de Gestão de Riscos - Riscos do Câmpus Araranguá
30/11/2021	Plano de Gestão de Riscos - Riscos do Câmpus Jaraguá do Sul - Centro
30/01/2022	Plano de Gestão de Riscos - Riscos do Câmpus Jaraguá do Sul - Rau
30/03/2022	Plano de Gestão de Riscos - Riscos do Câmpus Gaspar
30/05/2022	Plano de Gestão de Riscos - Riscos do Câmpus Caçador
30/07/2022	Plano de Gestão de Riscos - Riscos do Câmpus Garopaba
30/09/2022	Plano de Gestão de Riscos - Riscos do Câmpus Itajaí
30/12/2022	Plano de Gestão de Riscos - Riscos do Câmpus Criciúma
30/03/2023	Plano de Gestão de Riscos - Riscos do Câmpus Florianópolis - Continente
30/06/2023	Plano de Gestão de Riscos - Riscos do Câmpus Chapecó
30/09/2023	Plano de Gestão de Riscos - Riscos do Câmpus Lages
30/12/2023	Plano de Gestão de Riscos - Riscos do Câmpus Joinville
30/04/2024	Plano de Gestão de Riscos - Riscos do Câmpus São José
30/08/2024	Plano de Gestão de Riscos - Riscos do Câmpus Florianópolis
30/12/2024	Revisão Geral do Plano de Gestão de Riscos de TIC

TERMOS E ABREVIações

CIR - Coordenadoria de Infraestrutura de Redes

CISSP - Comissões Internas de Saúde do Servidor Público

CGTI - Coordenadoria de Governança de Tecnologia da Informação

CODIR - Colégio de Dirigentes

CONSUP - Conselho Superior

CGTIC - Comitê Gestor de Tecnologia da Informação e Comunicação

CTIC - Coordenação de Tecnologia da Informação e Comunicação dos Câmpus do IFSC

DSI - Departamento de Sistemas de Informação

DTIC - Diretoria de Tecnologia da Informação e Comunicação

EGD - Estratégia Governança Digital

ESR - Escola Superior de Redes

FORTIC - Fórum de Tecnologia da Informação e Comunicação do IFSC

IFSC - Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina

PDI - Plano de Desenvolvimento Institucional

PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação

PETIC - Planejamento Estratégico de Tecnologia da Informação e Comunicação

POSIC - Política de Segurança da Informação

SISP - Sistema de Administração de Recursos de Tecnologia da Informação

SETIC - Secretaria de Tecnologia da Informação e Comunicação

TIC - Tecnologia da Informação e Comunicação

PDCA - *Plan, Do, Check, Act* (Planejar, Fazer, Checar, Agir)

TCU - Tribunal de Contas da União

TI - Tecnologia da Informação

POP-SC - Ponto de Presença de Santa Catarina

REMEP - Rede Metropolitana

RNP - Rede Nacional de Pesquisa

ABNT - Associação Brasileira de Normas Técnicas

CAFe - Comunidade Acadêmica Federada

NBR - Norma Brasileira

Câmpus

ARU Campus Araranguá

CAN Campus Canoinhas

CDR Campus Caçador

CCO Campus Chapecó

CRI Campus Criciúma
CTE Campus Florianópolis Continente
FLN Campus Florianópolis
GPB Campus Garopaba
GAS Campus Gaspar
ITJ Campus Itajaí
JAR Campus Jaraguá do Sul
JGW Campus Jaraguá do Sul Geraldo Werninghaus
JLE Campus Joinville
LGS Campus Lages
PHB Campus Palhoça Bilíngue
REI Reitoria
SCA Campus São Carlos
SJE Campus São José
SLO Câmpus Avançado São Lourenço do Oeste
SMO Campus São Miguel do Oeste
TUB Campus Tubarão
URP Campus Urupema
XXE Campus Xanxerê
CERFEAD Centro de Referência em Ensino a Distância

REITORIA

PROAD Pró-Reitoria de Administração
PRODIN Pró-Reitoria de Desenvolvimento Institucional
PROEN Pró-Reitoria de Ensino
PROEX Pró-Reitoria de Extensão e Relações Externas
PROPPi Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação

APRESENTAÇÃO

INTRODUÇÃO

Os riscos de segurança de informação podem ser definidos como uma forma em que determinada ameaça consegue explorar uma vulnerabilidade de um ativo ou conjunto de ativos de informação, prejudicando assim, a organização.

Um conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos à que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos (GSIPR04, 2009).

A gestão de riscos é considerada um artefato importante do planejamento estratégico de uma organização e que deve ser feita por toda a empresa. Ela propõe atividades ordenadas para controlar uma determinada organização quando se refere a riscos.

O processo de gestão de riscos de segurança da informação compreende as etapas: definição do contexto, análise/avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco e monitoramento e análise crítica de riscos:

- ✓ Definição do Contexto – esta fase tem o objetivo de conhecer o ambiente da organização, realizando um levantamento de todas as informações relevantes que caracterizam a empresa/setor em que será executada a análise de riscos e contribuem para o seu desenvolvimento. Também é na definição de contexto que é definido o escopo e limites do projeto, sua abrangência, seus resultados e suas entregas;
- ✓ Análise/avaliação de Riscos – identificação dos riscos e assim, determinar ações necessárias para reduzir o risco para um nível aceitável.
- ✓ Tratamento do Risco – esta fase é utilizada para responder aos riscos identificados. No tratamento de riscos é possível obter quatro opções, dependendo da viabilidade técnica e financeira, eficácia dos controles, eficiência do tratamento e características do negócio da organização, as quais são: redução do risco, retenção do risco, evitar o risco e transferência do risco;
- ✓ Aceitação do Risco – nesta fase é feita uma análise do plano de tratamento de riscos, a qual os gestores da organização decidem a aceitação de riscos. É feito um documento formal chamado Declaração de Aplicabilidade, em que nele serão apresentados controles não aplicáveis e justificativos de não serem contemplados;
- ✓ Comunicação do Risco – fase permanente durante todo o processo de gestão de riscos. É a troca interativa da informação e conhecimentos de como os riscos devem ser gerenciados;
- ✓ Monitoramento e Análise Crítica – fase permanente durante todo o processo de gestão de riscos. Ocorre o registro de atividades e ações da gestão de riscos.

A *Figura 1* apresenta o processo de gestão de riscos de segurança da informação, com as suas respectivas etapas. O fluxo inicia na definição do contexto, partindo para análise/avaliação de riscos; se a avaliação do risco for satisfatória passa para a etapa de tratamento do risco, caso contrário volta para a definição do contexto; se o tratamento do risco for satisfatório passa para a fase de aceitação do risco, caso contrário pode voltar para o tratamento do risco ou definição do contexto. As fases de monitoramento do risco e monitoramento e análise crítica de riscos devem ser realizadas durante todas as fases do processo. Esse processo segue um fluxo contínuo e podem ser realizados vários ciclos.

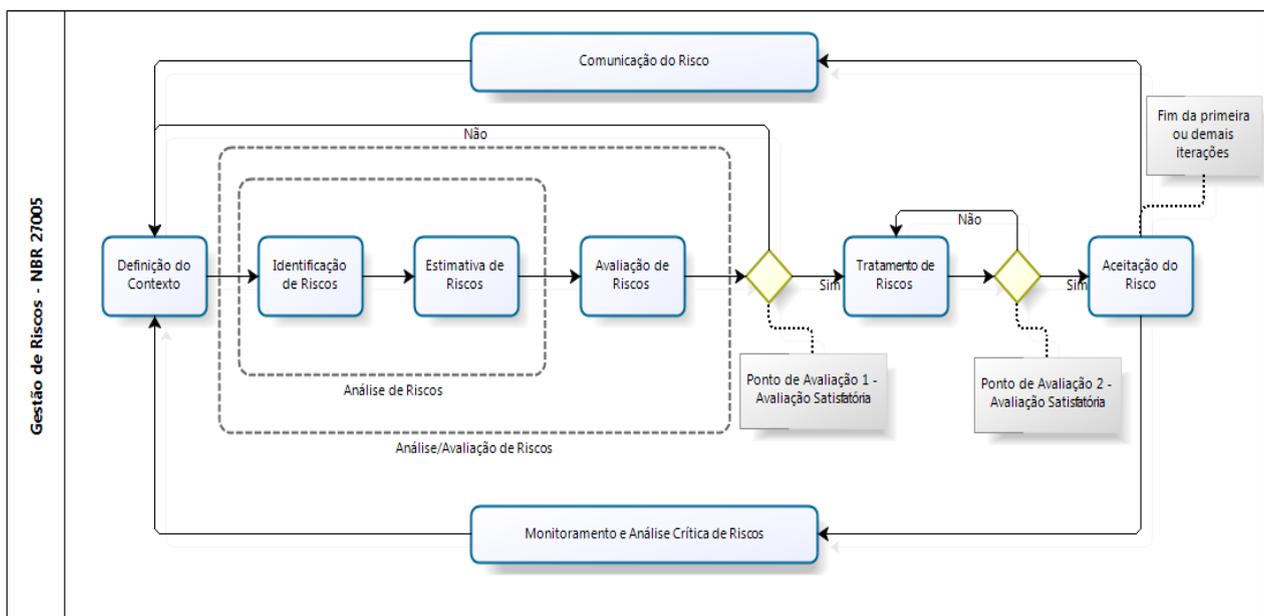


Figura 1 – Processo de Gestão de Riscos de Segurança da Informação

Fonte: NBR ISO/IEC 27005

PLANO DE GESTÃO DE RISCOS DE TIC

O Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação (PGR-TIC) é o instrumento de diagnóstico, planejamento e gestão dos riscos de TIC do IFSC.

Nesta primeira versão foi realizada apenas a gestão de risco da Reitoria. Nas versões posteriores serão incluídos os Câmpus do IFSC permitindo que todos os ativos sejam analisados e que todos os riscos sejam tratados.

No Anexo I, é disposto o Plano de Tratamento de Riscos com sua definição e a análise do risco residual, bem como a identificação de controles para reduzir, reter, evitar ou transferir os riscos. O plano apresenta ainda a Declaração de Aceitabilidade com a justificativa para os riscos aceitos.

FERRAMENTAS E METODOLOGIA DE TRABALHO

FERRAMENTAS

O processo de elaboração do Plano de Gestão de Riscos de TIC segue as normas NBR 27005 e NBR 31000. Também foram utilizadas as planilhas de Riscos da Escola Superior de Redes (ESR). Este documento segue os princípios e diretrizes do Sistema de Governança de TIC do IFSC e está alinhado com o Planejamento Estratégico Institucional e o Planejamento Estratégico de Tecnologia da Informação e Comunicação Institucional.

METODOLOGIA

A Diretoria de Tecnologia da Informação e Comunicação através da sua Coordenadoria de Governança de TIC iniciou o desenvolvimento do Plano de Gestão de Riscos de TIC.

A partir da cadeia de valores e os macroprocessos institucionais a DTIC desenvolveu os seus processos. Em seguida foram feitos os levantamentos de ativos de TIC sob o controle da DTIC.

Com os ativos categorizados, catálogo e portfólio de serviços publicados, iniciou-se o processo de identificação/análise dos riscos e controles existentes. Após a definição dos riscos foi efetuado o plano de tratamento de riscos, no qual são definidas as ações, controles a serem realizados para cada risco encontrado e também riscos residuais.

DOCUMENTOS DE REFERÊNCIA

Fonte	Documento
DSIC	Norma Complementar de Gestão de Riscos de Segurança da Informação e Comunicação – GSIPR. 04/IN01/DSIC/GSIPR de 14/08/2009.
DSIC	Guia do Gestor
ABNT	ABNT NBR ISO/IEC 27005:2008, Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação.
ABNT	ABNT NBR ISO/IEC 31000:2009, Gestão de Riscos – Princípios e Diretrizes
ABNT	ABNT NBR ISO/IEC 31010:2012, Gestão de Riscos – Técnicas para o processo de Avaliação de Riscos
IFSC	Sistema de Governança de TIC
IFSC	Política de Segurança da Informação e Comunicação
IFSC	Consulta aos câmpus – Mapeamento dos ativos institucionais.
SISP	Guia de Governança de Tecnologia da Informação e Comunicação
SISP	Metodologia de Gestão de Riscos de SIC do SISP
ESR	Planilha de Gestão de Riscos

Tabela 1 – Documentos de referência

VIGÊNCIA

Este PGR-TIC têm abrangência de 4 (quatro) anos, podendo ser revisado anualmente, caso necessário.

ABRANGÊNCIA

A primeira versão contempla apenas a reitoria. Esta foi dividida em oito (8) subfases:

1. Infraestrutura de TIC: Controladoras Wireless, Switches Core e Distribuição, Firewall e Central Telefônica;
2. Infraestrutura de Apoio à TIC: Link de Internet, No-break, Gerador e Ar condicionado;
3. Armazenamento e Processamento de Dados: Computadores Desktops, Storage, Servidor Rack e Servidor de modelos *blade*;
4. Sistemas: SIG, Sophia, PAEVS, Helios, Aplicativos Móveis, Liferay, VEEAM, Windows Server, Prime Cisco, Volare e VMWare;
5. Segurança de Redes: Sistema de Detecção de Intrusão e Políticas de Controle de Acesso, Ferramentas de Detecção de Ameaças e Vulnerabilidades, entre outros;
6. Banco de Dados: Oracle DB, PostgreSQL e MySQL;
7. Recursos Humanos: Analistas de TIC, Técnicos de TIC e Laboratoristas de TIC; e
8. Processos de Negócios de TIC.

A partir da segunda versão serão contemplados o Cerfead (Centro de Referência EAD) e todos os demais Câmpus do IFSC. Este projeto tem a perspectiva de ser finalizado no ano de 2024.

REVISÕES

A revisão do Plano é realizada nas seguintes situações:

1. Em no máximo 4 (quatro) anos;
2. Nos momentos em que o CGTIC julgar necessário; ou
3. Em função dos resultados dos testes realizados; ou
4. Após ocorrência de algum evento ou mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes; ou
5. Sempre que finalizado uma nova etapa dentro o planejamento.

APROVAÇÃO E PUBLICAÇÃO

O PGR - TIC foi submetido para apreciação e aprovação ao Comitê Gestor de Tecnologia da Informação e Comunicação. O PGR - TIC deverá ser publicado no Portal do IFSC nos seguintes endereços: <<http://www.ifsc.edu.br/tecnologia-da-informacao>>.

VALIDAÇÃO DO PLANO

O Plano de Gestão de Riscos de TIC será validado em reuniões do CGTIC (Comitê Gestor de Tecnologia da Informação e Comunicação), em reuniões específicas para esse fim.

SETORES ENVOLVIDOS NO PLANO

Os setores que deverão estar envolvidos na Gestão de Riscos de TIC (Figura 2) são:

Alta Gestão:

- Reitor(a);
- Pró-reitores(as);
- Diretor(a)-executivo(a).

Setores e seus titulares:

- Diretor de TIC
 - Chefe do Departamento de Sistemas (DSI);
 - Coordenador(a) de Infraestrutura e Redes (CIR);
 - Coordenador(a) de Governança de TIC (CGovTIC).

Representantes delegados:

- Comitê Gestor de TIC (CGTIC);

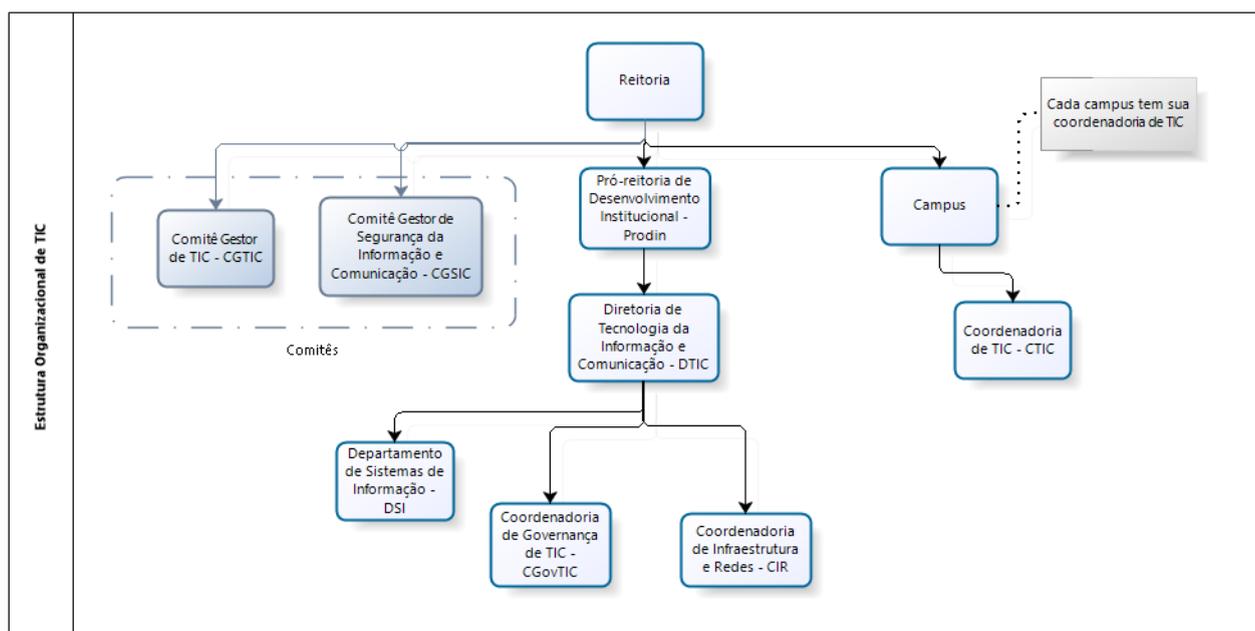


Figura 2 - Estrutura Organizacional da TIC - IFSC

OBJETIVO

Este plano tem como objetivo detalhar os processos de gestão de riscos previstos no Sistema de Governança de TIC do Instituto Federal de Santa Catarina.

CONCEITOS E DEFINIÇÕES

Alta Administração: agentes públicos ou políticos responsáveis pela Governança de TIC nos órgãos e entidades do SISP, a saber: Reitor(a); Colégio de Dirigentes; Conselho Superior;

Ameaça: é todo e qualquer evento que possa explorar uma vulnerabilidade;

Análise do Risco: uso sistemático de informações para identificar fontes e estimar o risco;

Ativo: Qualquer elemento de valor à organização, isto é, qualquer item tangível ou intangível, recursos ou habilidade que tenha valor crítico à existência da organização, e que por consequência necessite de proteção;

Ativo de Informação: meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e pessoas que têm acesso a estes ativos.

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

Avaliação de Riscos: processo de comparar o risco estimado com critérios de riscos predefinidos para determinar a importância do risco;

Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC): órgão colegiado de natureza consultiva e de caráter permanente em conformidade com as orientações emanadas pela Secretaria de Tecnologia da Informação e Comunicação do Ministério do Planejamento, Desenvolvimento e Gestão (SETIC/MPDG) e pelo Sistema de Administração e Recursos de Informação e Informática (SISP). O CGTIC é responsável por alinhar os investimentos de Tecnologia da Informação com os objetivos estratégicos e apoiar a priorização de projetos a serem desenvolvidos;

Compartilhamento do risco: compartilhar com outra entidade o ônus da perda ou benefício do ganho associado a um risco.

Comunicação do risco: troca ou compartilhamento de informações sobre o risco entre o tomador de decisão e outras partes interessadas.

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

Diretoria de Tecnologia da Informação e Comunicação (DTIC): cabe o planejamento, a coordenação, a organização e o controle, em nível central, dos recursos de tecnologia da informação e comunicação no âmbito do IFSC;

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

Estimativa de riscos: processo utilizado para atribuir valores à probabilidade e consequência de um risco.

Evento: ocorrência gerada com base em fontes internas ou externas que pode causar impacto negativo, positivo ou ambos.

Evitar o risco: decisão de não se envolver ou agir de forma a mitigar uma situação de risco.

Fórum de Servidores de Tecnologia da Informação e Comunicação do IFSC (FORTIC): Fórum colaborativo

dos servidores de TIC do IFSC.

Gerenciamento de Riscos: processo contínuo, que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar eventos capazes de afetar os objetivos, processos de trabalho e projetos da organização, positiva ou negativamente, nos níveis estratégico, tático e operacional;

Gestão de Riscos: o conjunto de ações direcionadas ao desenvolvimento, disseminação e implementação de metodologias de gerenciamento de riscos institucionais, objetivando apoiar a melhoria contínua de processos de trabalho, projetos e a alocação e utilização dos recursos disponíveis, contribuindo para o cumprimento dos objetivos da organização;

Gestão de Riscos de Segurança da Informação e Comunicação: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

Governança de TIC: conjunto de ações e mecanismos pelo qual o uso atual e futuro da TIC é dirigido e controlado, mediante avaliação e direcionamento do uso da TIC para dar suporte à organização e monitorar seu uso para realizar os planos, incluída a estratégia e as políticas de uso da TIC dentro da organização;

Identificação do risco: processo para localizar, listar e caracterizar elementos de risco. Por menor que seja a probabilidade de ocorrência de um risco, pode ser determinada que a incerteza ocorra e explore uma vulnerabilidade, concretizando uma ameaça.

Impacto: mudança adversa no nível obtido dos objetivos. Consequência avaliada dos resultados com a ocorrência de um evento em particular, em que determinada vulnerabilidade foi explorada, uma ameaça ocorreu e o risco se concretizou;

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

Modificação do risco: ações tomadas para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco.

Monitoramento e análise crítica: são as atividades de acompanhamento dos resultados, implementação dos controles e de análise crítica para a melhoria contínua do processo de gestão de riscos.

Probabilidade: é a chance do risco acontecer, estabelecida a partir de uma escala predefinida de probabilidades possíveis.

Retenção de risco: aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco.

Risco: combinação da probabilidade de um evento indesejado ocorrer e de suas consequências para a organização;

Sistema de Governança de TIC: sistema de políticas que dá os princípios, diretrizes legais para a governança de TIC do Instituto Federal de Santa Catarina.

Tecnologia da Informação e Comunicação (TIC): ativo estratégico que suporta processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;

Transferir Risco: uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

Tratamento dos Riscos: processo e implementação de ações de segurança da informação e

comunicações para evitar, reduzir, reter ou transferir um risco; e

Vulnerabilidade: é qualquer fraqueza que possa ser explorada para comprometer a segurança da informação;

PROCEDIMENTOS

Para análise/avaliação do risco foi utilizada a planilha disponibilizada pela Escola Superior de Redes (ESR), para o curso de Gestão de Riscos de TI - NBR 31000 e NBR 27005.

Definição de Contexto

A definição do contexto leva em consideração as normas e regulamentos institucionais, delimitando o âmbito de atuação. Pode abranger a instituição como um todo, um segmento, um processo, um sistema, um recurso ou um ativo de informação.

No caso do IFSC, por ser disperso em vinte e dois (22) Câmpus, o Centro de Referência EAD (Cerfead) e Reitoria, será necessário dividir o escopo. Inicialmente será avaliado os riscos de TIC da reitoria, após validado será realizado nos demais Câmpus, começando pelos menores e finalizando nos maiores. A *Tabela 2* apresenta o cronograma de execução do plano.

VERSÕES		
Versão	Data	Abrangência
1.0	30/05/2020	Infraestrutura de TIC Reitoria
1.0	30/05/2020	Infraestrutura de Apoio à TIC Reitoria
1.0	30/05/2020	Armazenamento e Processamento de Dados Reitoria
1.0	30/05/2020	Sistemas Reitoria
1.0	30/05/2020	Segurança de Redes
1.0	30/05/2020	Processos de Negócios de TIC Reitoria
1.0	30/05/2020	Recursos Humanos de TIC Reitoria
1.1	30/07/2020	Banco de dados Reitoria
2.0	30/09/2020	Urupema
2.1	30/10/2020	São Lourenço do Sul
2.2	30/11/2020	São Miguel do Oeste
2.3	30/12/2020	São Carlos
2.4	30/02/2021	Canoinhas
2.5	30/03/2021	Palhoça Bilingue
2.6	30/04/2021	Cerfead
2.7	30/05/2021	Xanxerê
2.8	30/07/2021	Tubarão
2.9	30/09/2021	Araranguá
2.10	30/11/2021	Jaraguá do Sul - Centro

2.11	30/01/2022	Jaraguá do Sul - Rau
2.12	30/03/2022	Gaspar
2.13	30/05/2022	Caçador
2.14	30/07/2022	Garopaba
2.15	30/09/2022	Itajaí
2.16	30/12/2022	Criciúma
2.17	30/03/2023	Florianópolis Continente
2.18	30/06/2023	Chapecó
2.19	30/09/2023	Lages
2.20	30/12/2023	Joinville
2.21	30/04/2024	São José
2.22	30/08/2024	Florianópolis
3.0	30/12/2024	Revisão Geral - Reitoria e Câmpus

Tabela 2 - Cronograma do Plano de Gestão de Riscos.

Identificação dos Processos de TIC

A primeira etapa da elaboração de gestão de riscos é a identificação e mapeamento dos processos de TIC e a definição do nível de criticidade, considerando seu impacto e relevância para os objetivos estratégicos da instituição.

A partir dos macroprocessos institucionais foram definidos os processos de TIC do IFSC. A partir desses processos foram definidos pela DTIC os processos gerais.

A definição dos processos de TIC são de suma importância, pois é a partir deles que serão verificados os processos críticos e a que se deve dar maior relevância na Gestão de Riscos de TIC. A *Tabela 3* fornece os macroprocessos em que a TIC atua e processos definidos de cada setor.

#	Processo	Dono /Responsável	Setores Envolvidos	Descrição	Escopo
01	Gestão da Governança (gestão de riscos)	Colégio de Dirigentes	IFSC	Macroprocesso	Governança Institucional
02	Gestão de TI (Gestão de demandas de TI)	Diretor de TI	DTIC	Macroprocesso	Demandas gerais junto a DTIC
03	Gestão de TI (Desenvolvimento de soluções de TI)	Chefe do Depto Sistemas	DTIC	Macroprocesso	Desenvolvimento de sistemas/funcionalidades ou outras soluções solicitadas à DTIC
04	Gestão de TI (Implantação de soluções de TI)	Coordenador de Infraestrutura e Redes	DTIC	Macroprocesso	Implantar soluções prontas de TIC
05	Gestão de TI (Manutenção e suporte)	Coordenador de Infraestrutura e	DTIC	Macroprocesso	Manter soluções prontas implantadas

	de soluções de TI)	Redes			
06	Gestão de TI (Gestão da governança de TI)	Coordenador de Governança de TIC	DTIC	Macroprocesso	Todos os documentos devem ser desenvolvidos seguindo os processos de governança de TIC
07	Comunicação DTIC - Externo	Diretor de TI	DTIC	Processo	Sistema de Chamados para a DTIC, todas as coordenadorias e departamento
08	Gerenciamento de contas de email - CIR	Coordenador de Infraestrutura e Redes	DTIC/CIR	Processo	Gerenciamento de contas de e-mails
09	Criar/alterar/excluir Listas - CIR	Coordenador de Infraestrutura e Redes	DTIC/CIR	Processo	Gerenciamento de listas de e-mails
10	Criação de Contas de email - CIR	Coordenador de Infraestrutura e Redes	DTIC/CIR	Processo	Criação de contas de e-mails
	Manutenção de infraestrutura - CIR	Coordenador de Infraestrutura e Redes	DTIC/CIR	Processo	Complemento do processo de Comunicação DTIC
14	Priorização de demanda - DSI	Chefe do Depto Sistemas	DTIC/DSI	Processo	Priorização das demandas de desenvolvimento de sistemas
15	Deploy sistema em produção - DSI	Chefe do Depto Sistemas	DTIC/DSI	Processo	Deploy dos sistemas DTIC em produção
16	Elaboração/Manutenção de Planos de TIC - CGovTIC	Coordenador de Governança de TIC	DTIC/CGovTIC	Processo	Elaboração de planos gerais de TIC (não inclui PETIC e PDTIC)
17	Elaboração/Manutenção de Políticas de TIC - CGovTIC	Coordenador de Governança de TIC	DTIC/CGovTIC	Processo	Elaboração das Políticas de TIC
18	Elaboração/Manutenção PDTIC - CGovTIC	Coordenador de Governança de TIC	DTIC/CGovTIC	Processo	Elaboração do Plano Diretor de Tecnologia da Informação e Comunicação
19	Elaboração/Manutenção PETIC - CGovTIC	Coordenador de Governança de TIC	DTIC/CGovTIC	Processo	Elaboração do Plano Estratégico de Tecnologia da Informação e Comunicação
20	Aquisição de TIC - CGovTIC	Coordenador de Governança de TIC	DTIC/CGovTIC	Processo	Compras de TIC com Pregão Eletrônico
21	Desenvolvimento de Aplicações - DSI	Chefe do Depto Sistemas	DTIC/DSI	Processo	Desenvolvimento de aplicações
22	Especificação de Requisitos - DSI	Chefe do Depto Sistemas	DTIC/DSI	Processo	Especificação de requisitos de sistemas/ desenvolvimento - alteração

Tabela 3 - Macroprocessos/Processos TIC

Comunicação/Chamados Externos - DTIC: este processo é para qualquer solicitação realizada junto à DTIC, vinda de qualquer servidor, para todas as coordenações/departamento. A *Figura 3* ilustra este processo.

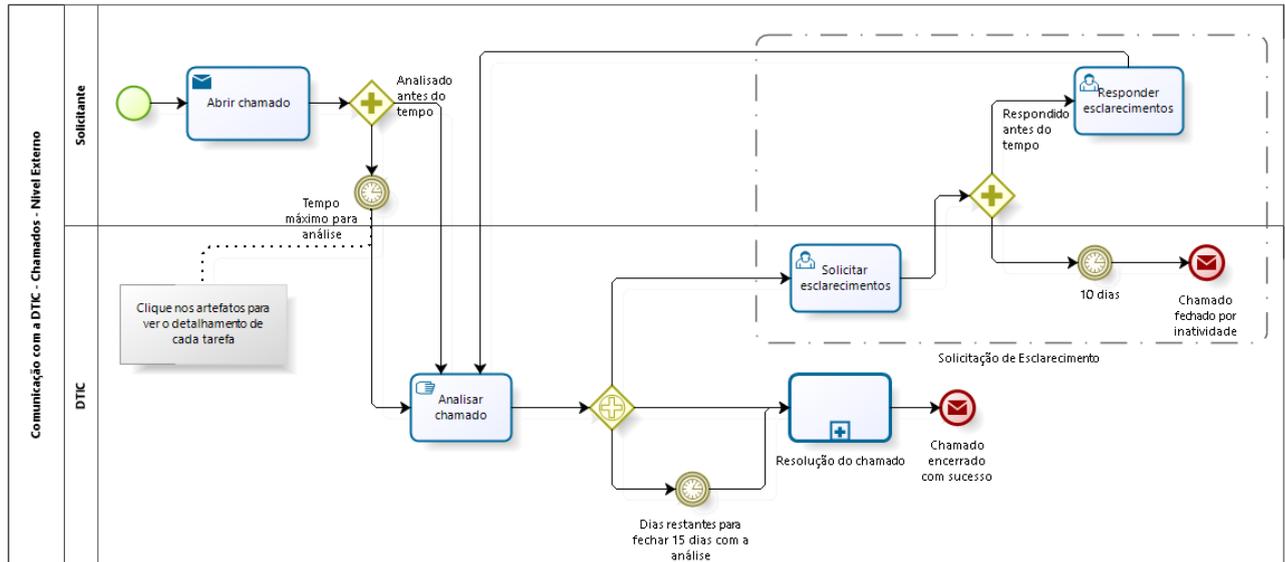


Figura 3 - Processo de Comunicação/Chamados Externos - DTIC

Gerenciamento de Contas de E-mail - CIR: processo realizado pela Coordenadoria de Infraestrutura e Redes. Este processo fornece a solicitação e recuperação de senhas e logins de servidores, bolsistas, tutores e alunos. A *Figura 4* apresenta o processo mencionado.

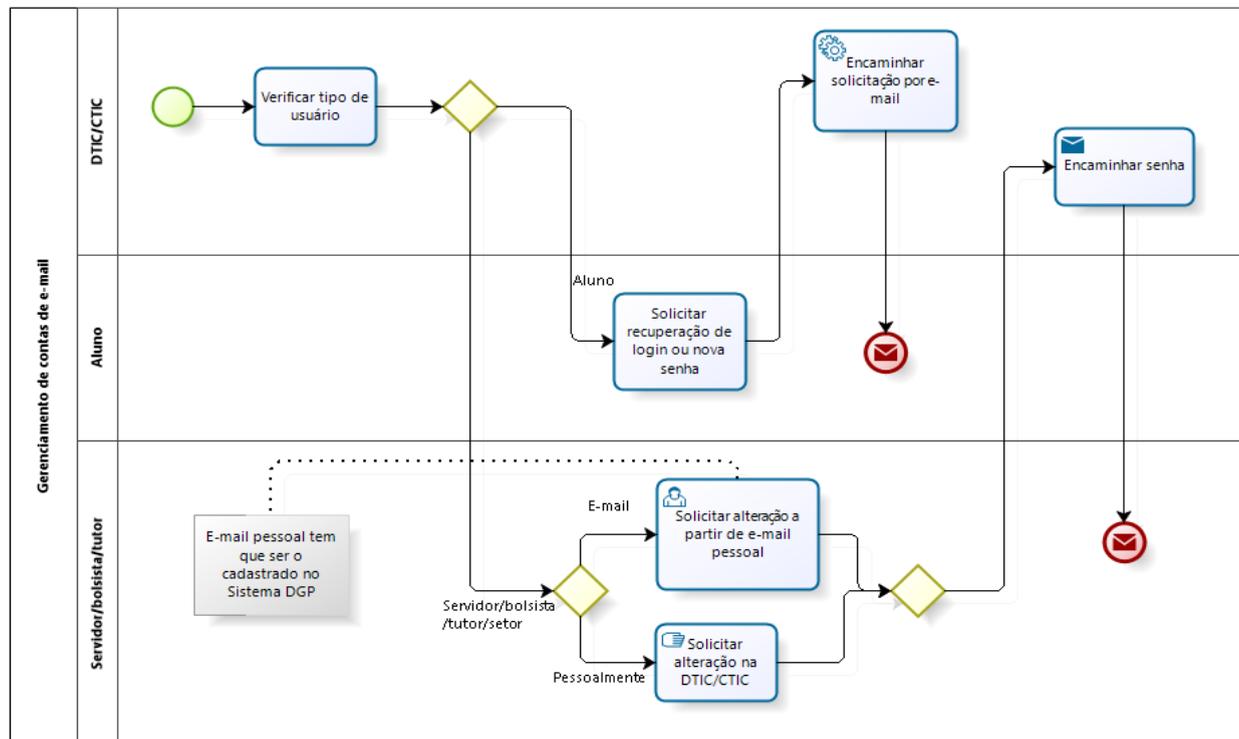


Figura 4 - Processo de Gerenciamento de Contas de E-mail - CIR

Criação de Listas de E-mail - CIR: este processo é interno à coordenação de Redes e Infraestrutura, quando um servidor solicita a criação de uma lista (via processo de comunicação/chamados DTIC). O gerenciamento da lista é realizado pelo servidor responsável pela lista. A *Figura 5* ilustra este processo.

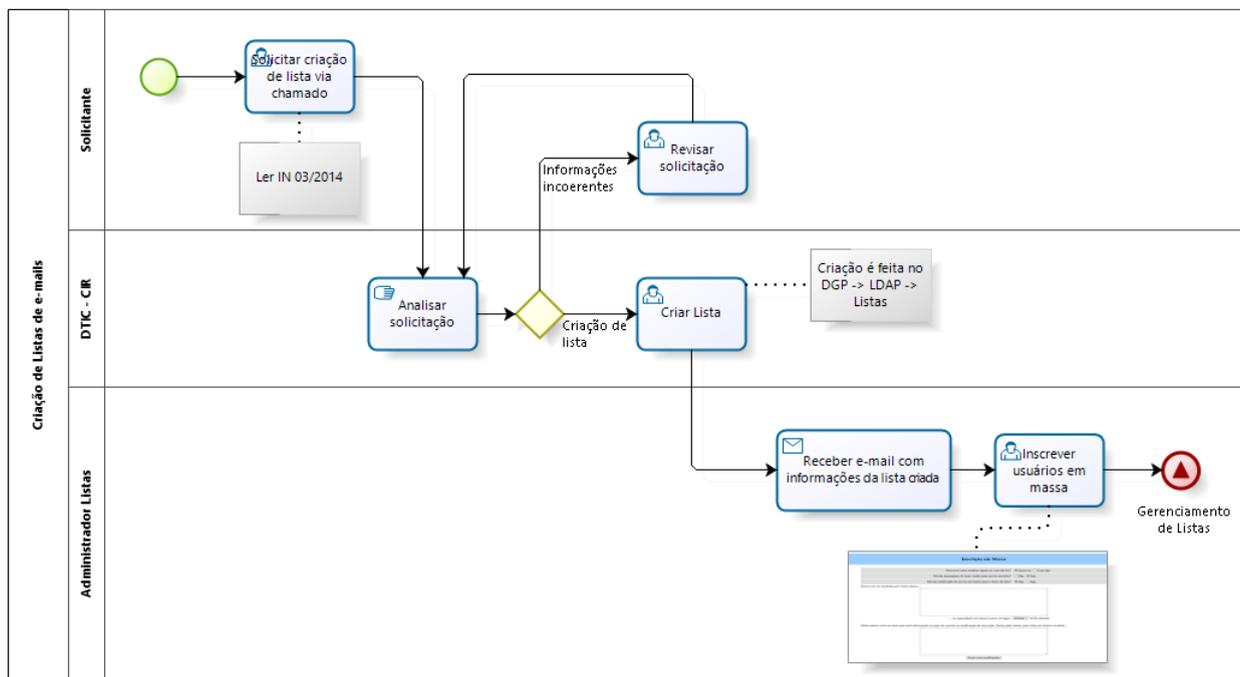


Figura 5 - Processo de Criação de Listas de E-mail - CIR

Criação de Contas de E-mail - CIR: processo gerenciado pela Coordenadoria de Redes e Infraestrutura, representa a criação de contas de e-mail para servidores (realizado pelo DGP), criação de e-mail para aluno (gerenciado pelos RAs) e criação de e-mail para bolsistas/tutores/institucionais (gerenciado pela DTIC). A *Figura 6* ilustra o processo em questão.

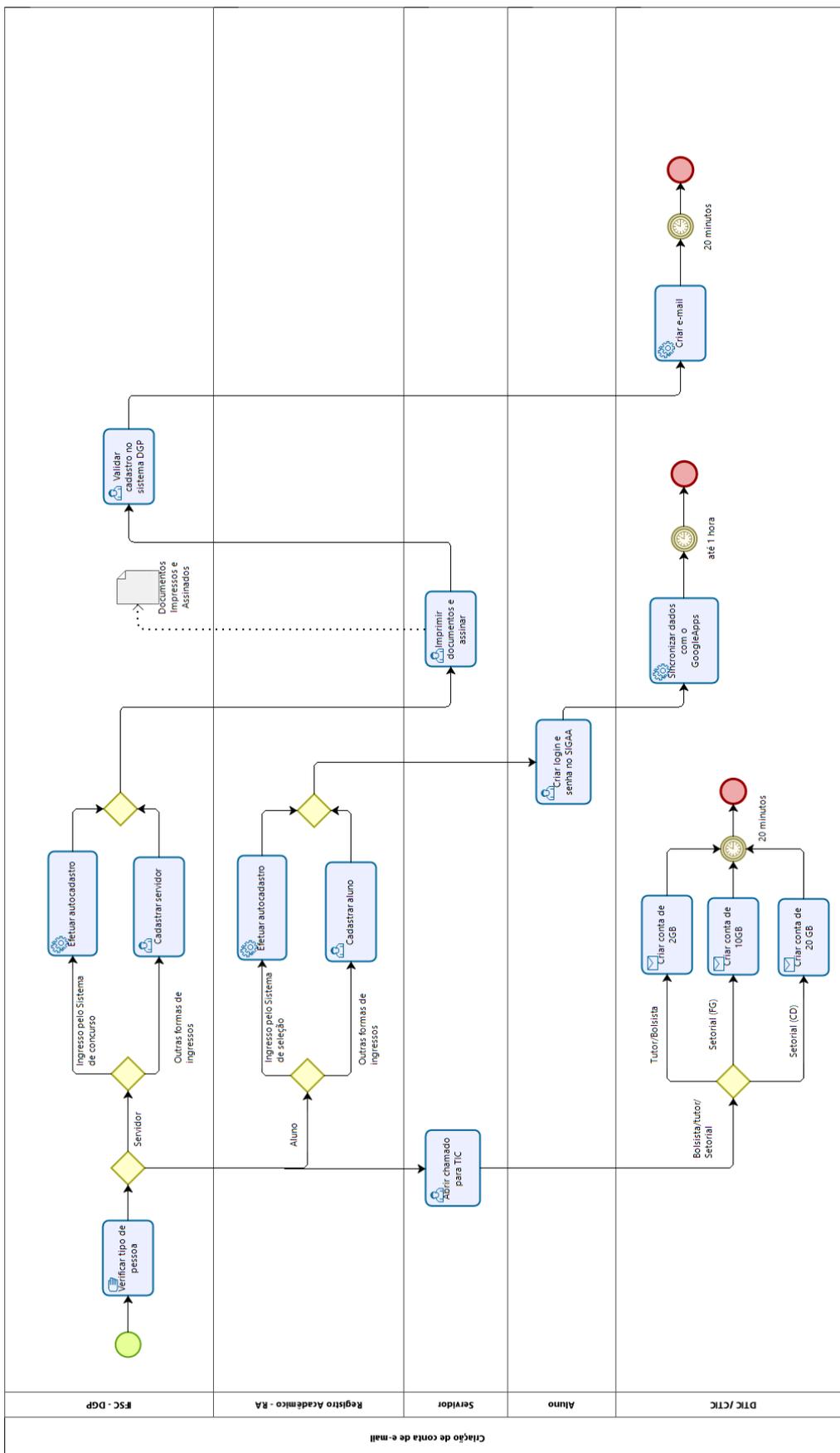


Figura 6 - Processo de Criação de Contas de E-mail - CIR

Manutenção de Infraestrutura - CIR: Este processo é um subprocesso “Resolução de Chamados” de Comunicação DTIC é interno à Coordenação de Infraestrutura e Redes. A *Figura 7* representa o processo.

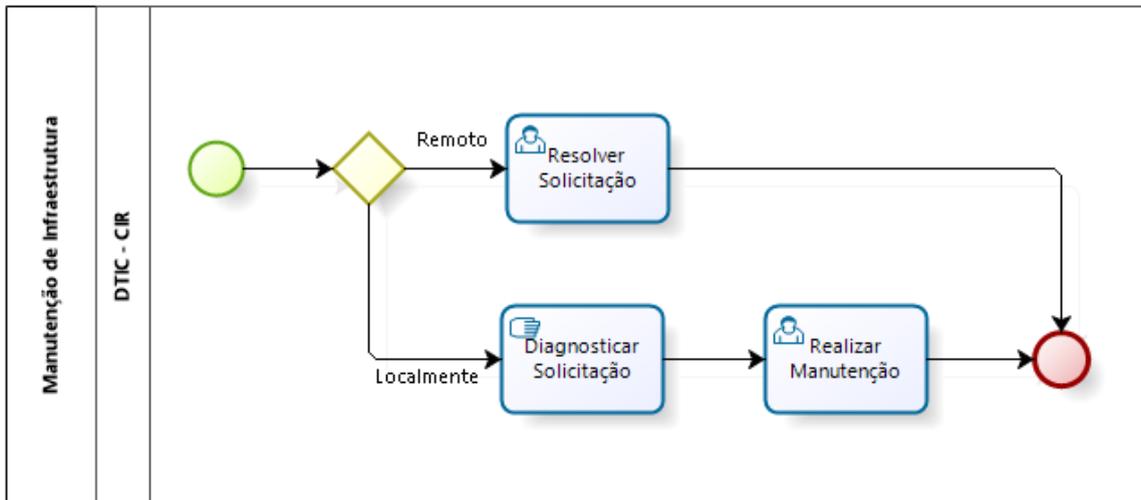
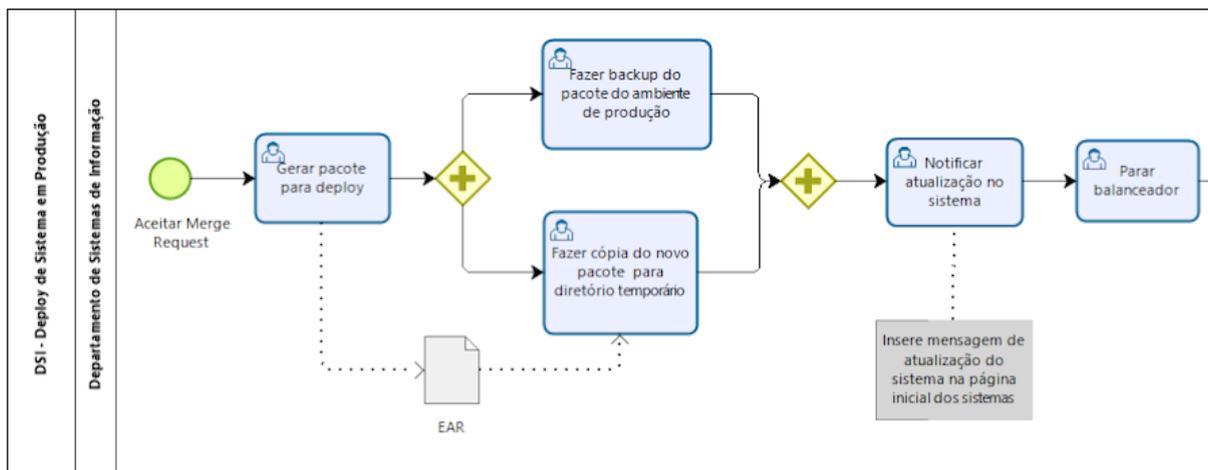


Figura 7 - Processo de Manutenção de Infraestrutura - CIR

Deploy de Sistemas em Produção - DSI: este processo é interno ao Departamento de Sistemas de Informação e ele é realizado cada vez em que uma atualização é feita nos sistemas. A *Figura 8* fornece o processo de Deploy.



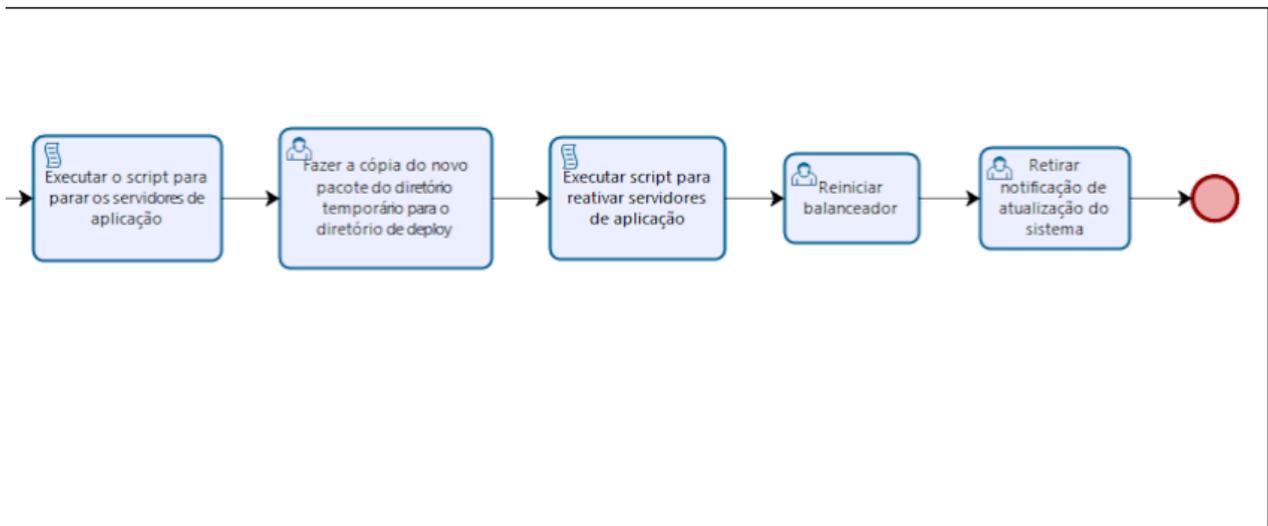
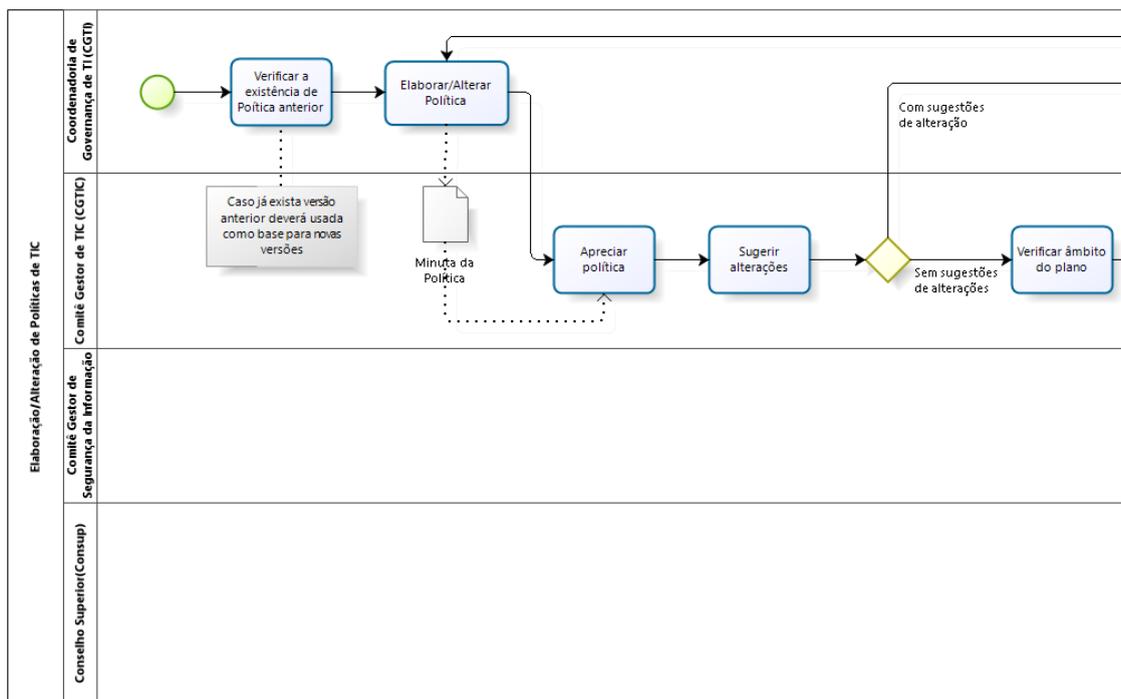


Figura 8 - Processo de Deploy de Sistemas em Produção - DSI

Elaboração de Políticas de TIC - CGovTIC: processo atendido pela Coordenadoria de Governança de Tecnologia da Informação e Comunicação. Aplicado a elaboração/alteração de políticas de TIC. A Figura 9 ilustra este processo.



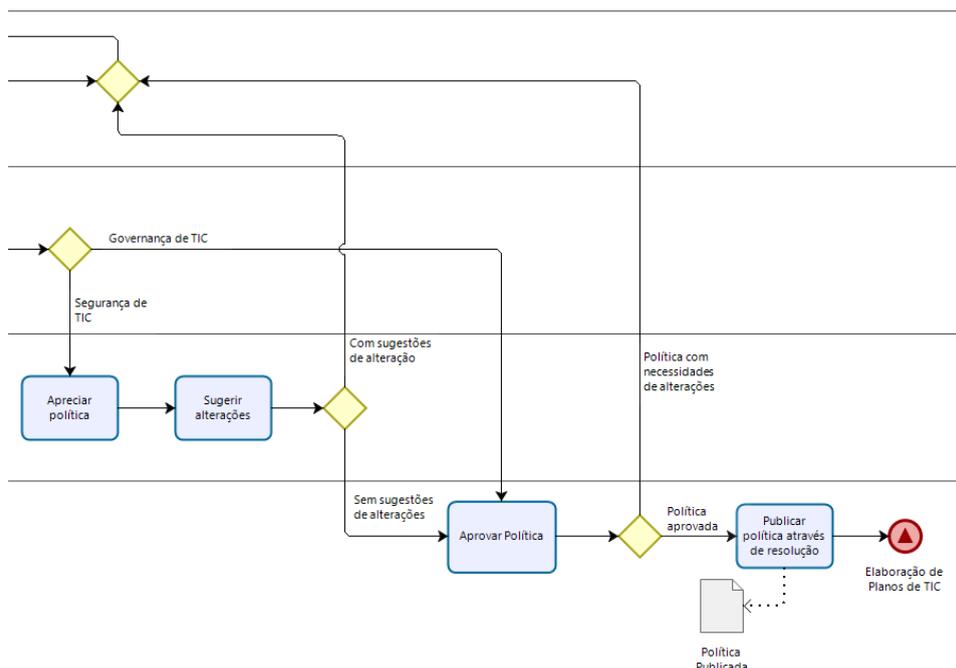
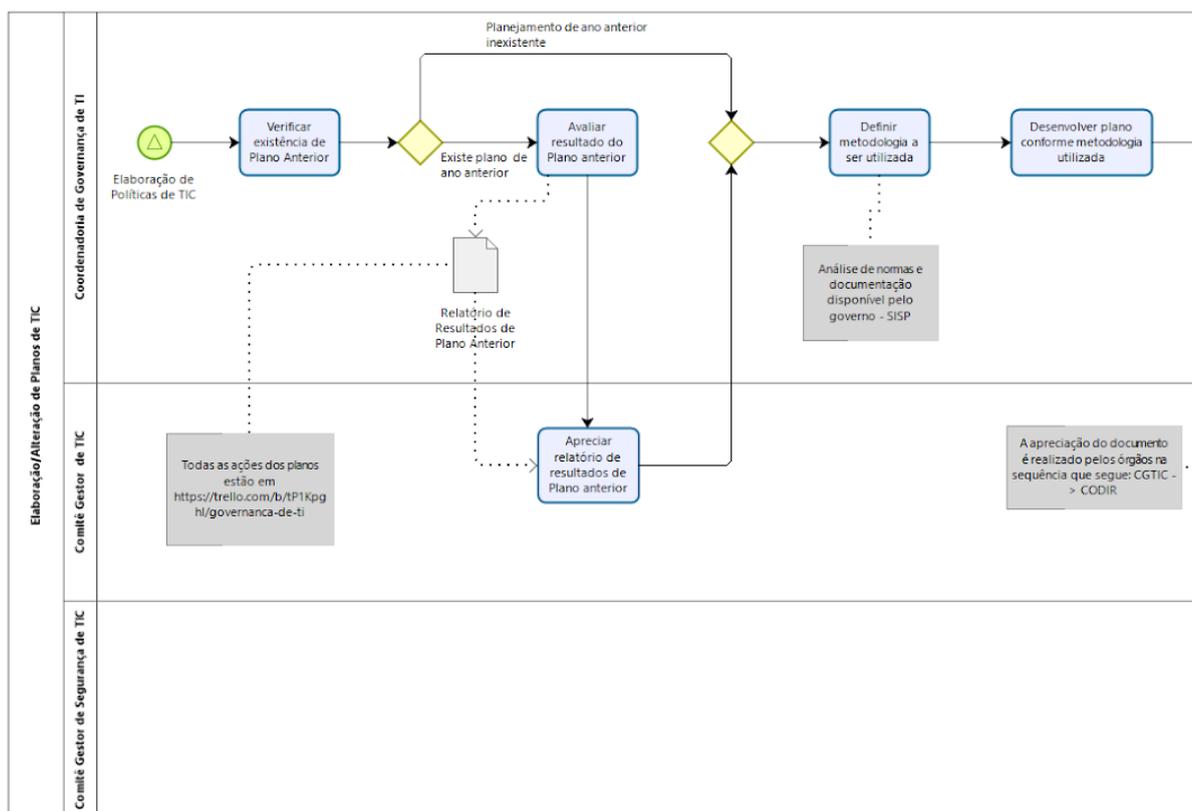


Figura 9 - Processo de Elaboração de Políticas de TIC - CGovTIC

Elaboração de Planos de TIC - CGovTIC: processo atendido pela Coordenadoria de Governança de Tecnologia da Informação e Comunicação. Aplicado a elaboração/alteração de planos de TIC. A Figura 10 ilustra este processo.



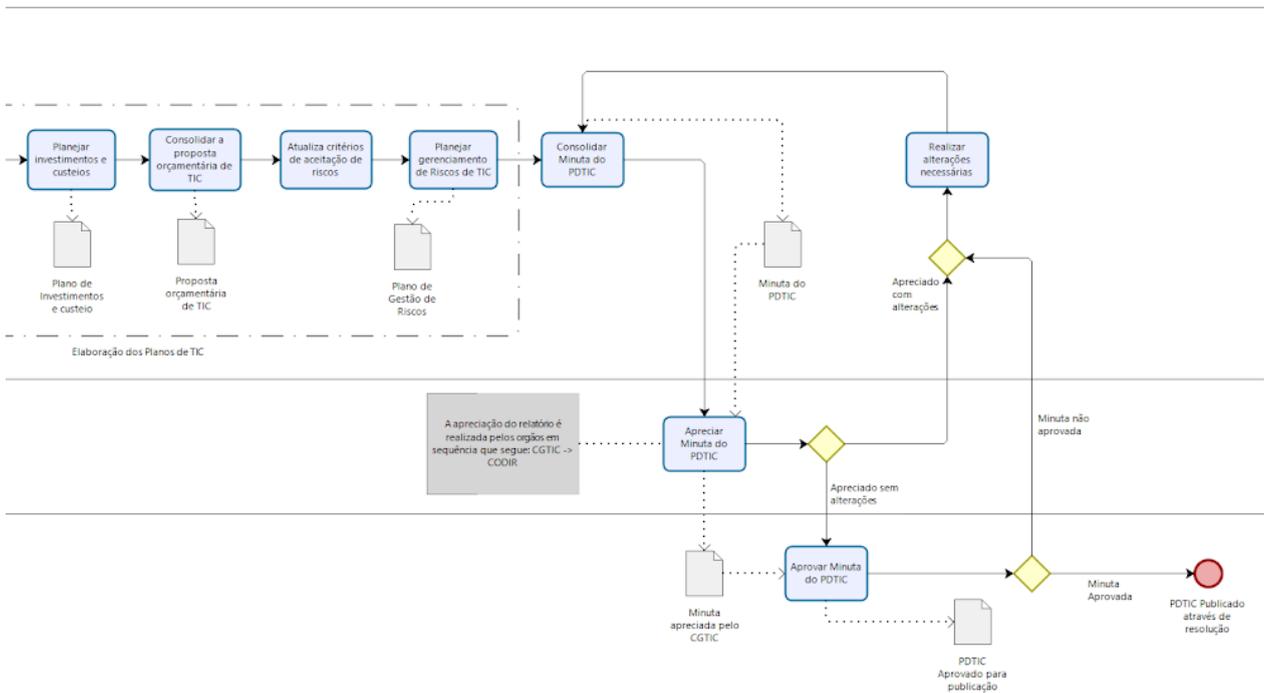
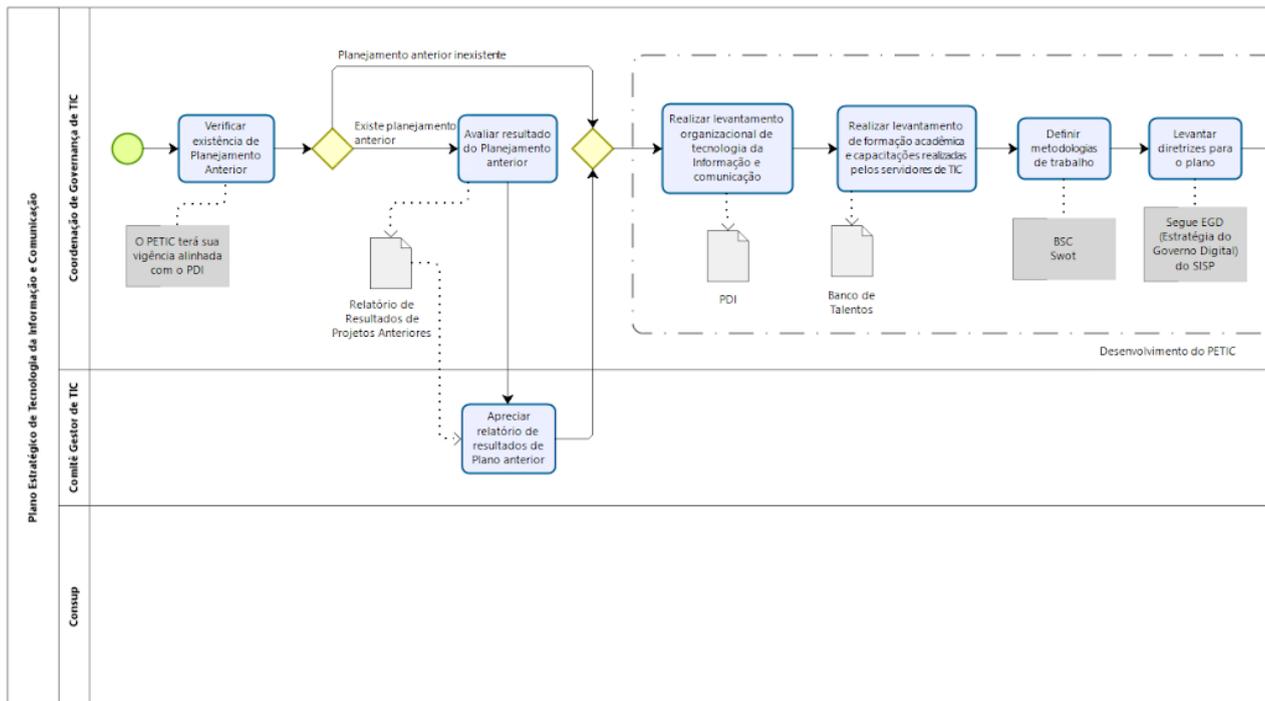


Figura 11 - Processo de Elaboração/Alteração do PDTIC - CGovTIC

PETIC - CGovTIC: processo atendido pela Coordenadoria de Governança de Tecnologia da Informação e Comunicação. Esse plano, juntamente com o PDTIC, por serem planos institucionais, seguem um processo mais amplo que os demais. A *Figura 12* ilustra este processo.



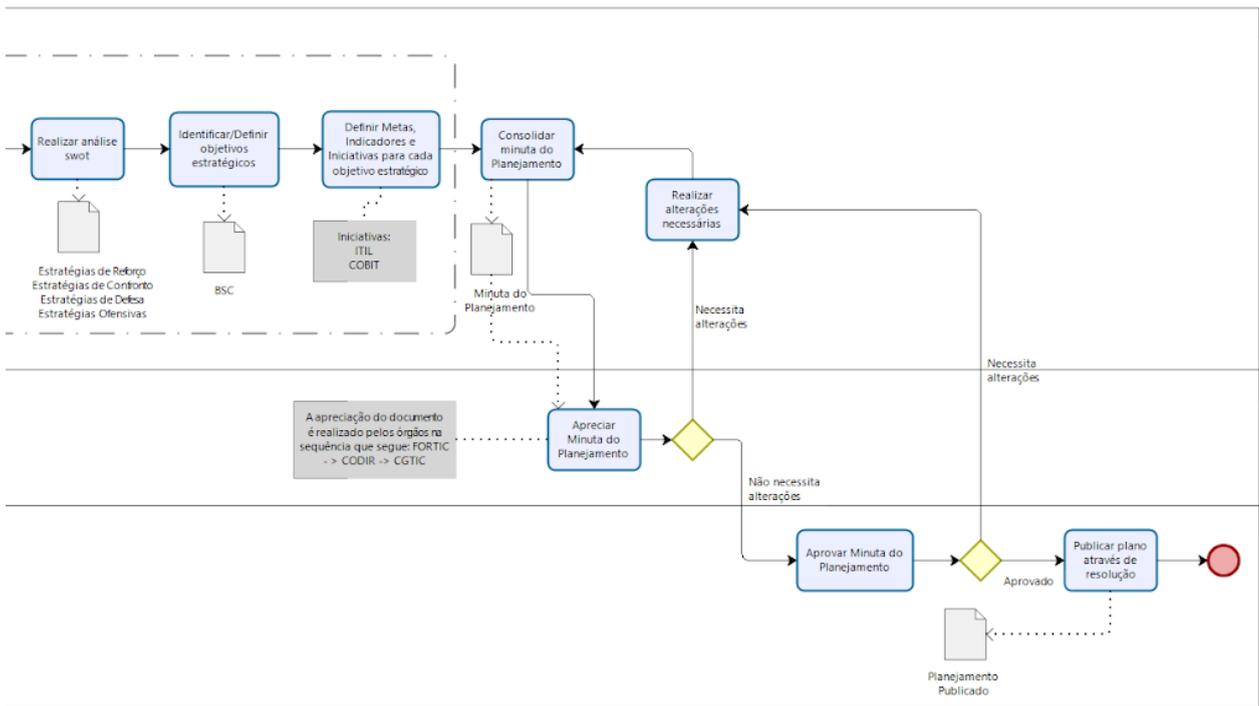
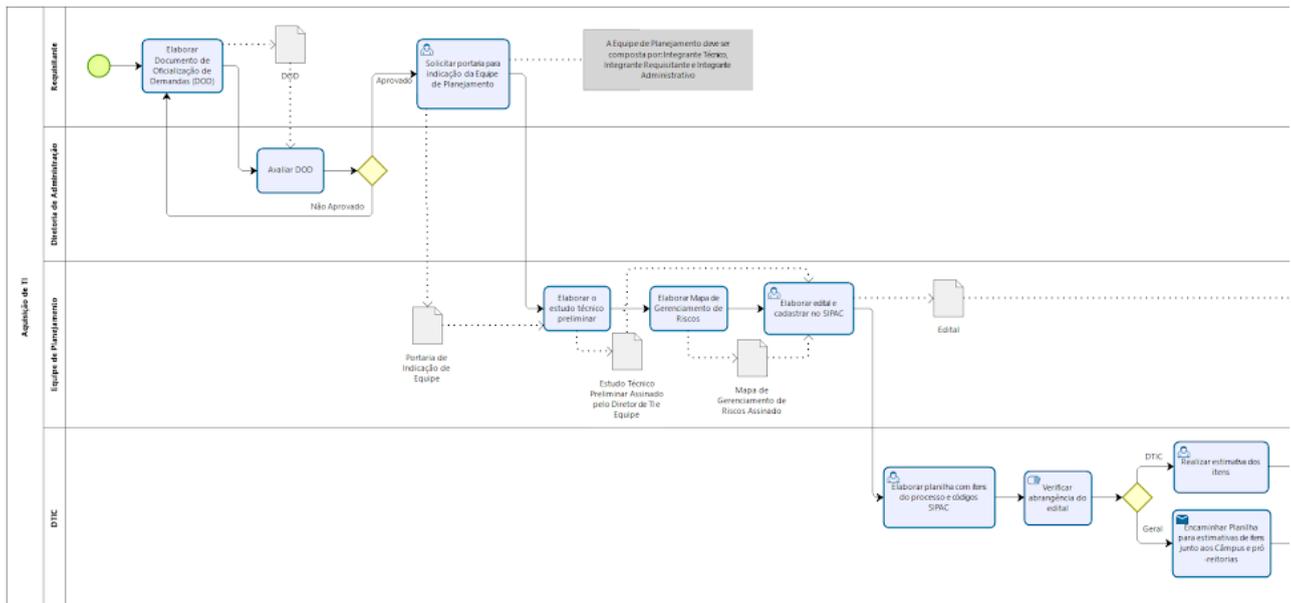


Figura 12 - Processo de Elaboração/Alteração do PETIC - CGovTIC

Aquisição de TI - CGovTIC: processo atendido pela coordenadoria de governança de TIC. Aplicado para todas as compras relacionadas às TICs. A Figura 13 ilustra este processo.



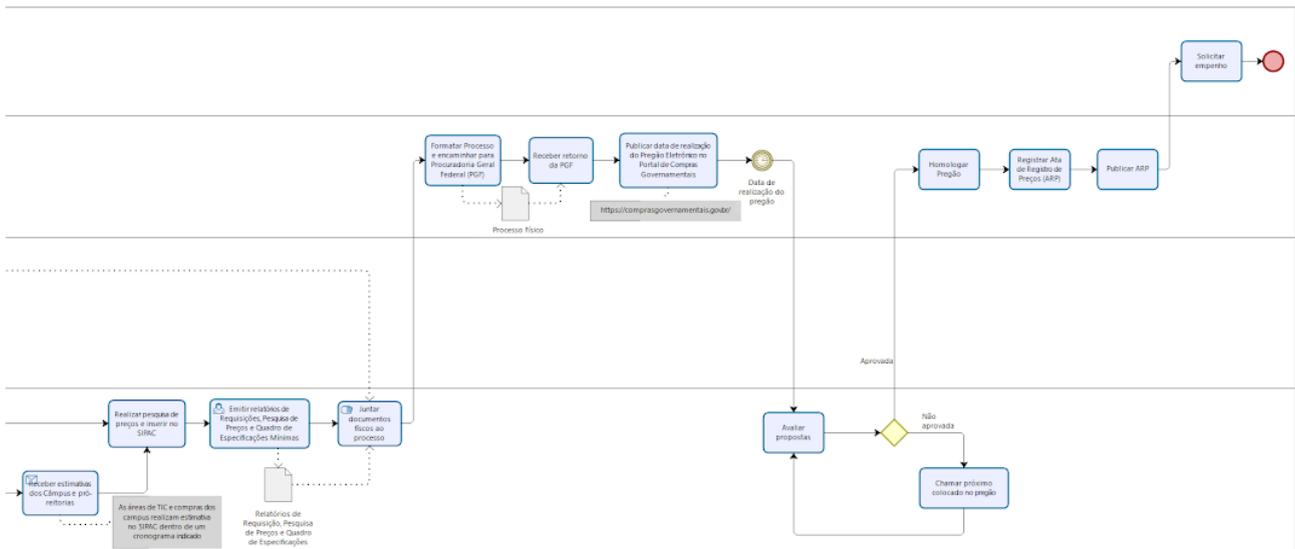


Figura 13: Processo de Aquisição de TIC

Análise/Avaliação de Riscos

Uma vez definido o escopo, os limites e a organização do processo de gestão de riscos de segurança da informação, é possível então, passar para a fase de análise/avaliação de riscos. Nesta fase são identificadas as ameaças, os controles existentes e que devem ser implementados, as vulnerabilidades e ameaças relacionadas. Assim que as ameaças e vulnerabilidades são levantadas é possível identificar e categorizar os riscos envolvidos e realizar o planejamento de tratamento necessário.

Com os resultados da Análise/Avaliação de riscos será possível direcionar e determinar ações gerenciais e prioridades para a gestão de riscos de segurança da informação, e assim, conseguir implementar controles para proteção para estes riscos. Esta deverá ser repetida periodicamente para conseguir contemplar mudanças que podem influenciar nos resultados.

A Figura 14 fornece o Processo de Análise/Avaliação de Riscos apresentado na Norma ISO/IEC 27005:2008. Este processo é dividido em três fases (identificar riscos, estimar riscos dentro da análise de riscos e avaliar os riscos).

A Identificação dos Riscos determinam os eventos que possam causar perda para a organização. A identificação consiste de 5 (cinco) etapas:

1. Identificar Ativos: ativo é considerado algo de valor para a organização e que, conseqüentemente, precisa ser protegido. A identificação dos ativos geralmente é feita por entrevista, no final obtêm-se uma lista de componentes e responsáveis.
2. Identificar Ameaças: esta fase tem o objetivo de verificar incidentes passados, identificando ameaças e suas fontes.
3. Identificar Controles Existentes: identificar controles planejados evitando custos e retrabalhos com duplicação de controles, e assegurando que estes controles estejam funcionando adequadamente.
4. Identificar Vulnerabilidades: tem como objetivo criar uma lista de vulnerabilidades associada aos

ativos, ameaças e controles.

5. Identificar Consequências: analisar consequências e prejuízos caso um incidente venha a ocorrer.

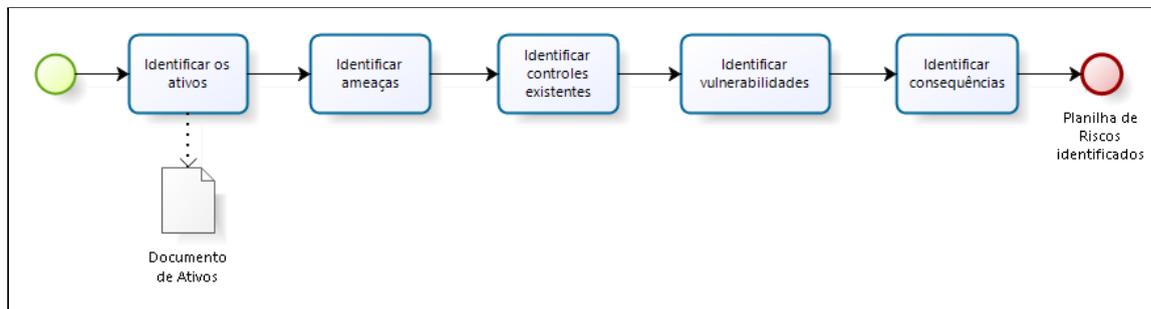


Figura 14 - Processo de Análise/Avaliação de Riscos

Identificação dos Riscos de TIC

Identificação de Ativos, Ameaças, Vulnerabilidades, Controles Existentes e Consequências:

Nesta fase, primeiramente foi feita a identificação dos ativos institucionais de TIC, para isso é criado um formulário e repassado para todas as TICs dos Câmpus, CERFEAD e coordenadores das áreas de TIC da Reitoria. Neste formulário foi solicitado para que os Profissionais de TIC preenchessem nos Câmpus, declarante do ativo, função do declarante, tipo de ativo, nome do ativo, quantidade, nome do responsável pelo ativo, função do responsável pelo ativo ou da chefia imediata, ameaças, vulnerabilidades, controles existentes para o ativo e consequência caso ocorra.

Após a coleta de informações sobre os ativos fez-se uma sintetização de todos os dados, padronizando os ativos. A partir disso, foram identificados 410 ativos e para cada ativo foram levantadas as vulnerabilidades, ameaças, controles existentes e consequências. Estes dados constam na Planilha de levantamento de ativos do Anexo I. No Anexo II, constam o levantamento de vulnerabilidades, ameaças, controles existentes e consequências.

Avaliação de Consequências

Esta fase tem o objetivo de avaliar os impactos sobre os negócios da instituição levando em conta as consequências de uma violação de segurança.

Esta etapa tem como entrada os cenários de incidentes, incluindo ativos afetados, vulnerabilidades e consequências para os ativos do negócio. A ação é o desenvolvimento de atividades de avaliação das consequências sobre o negócio da instituição e como saída obtivemos a lista de consequências referentes a um cenário de incidente, estando relacionada aos ativos e critérios de impacto.

Critérios de Priorização: a priorização das necessidades foi feita por meio da matriz Gravidade, Urgência e Tendência (GUT). Pela gravidade ou impacto que produzem quando não atendidas ou decorrente do seu atendimento. Pela urgência no seu atendimento. Pela tendência de agravamento do problema ou de perda da oportunidade, enquanto a necessidade não for atendida. Cada campo da matriz

GUT pode receber um valor de 1 a 5, conforme indicado na *Tabela 4*.

Valor	Gravidade	Urgência	Tendência
1	Sem gravidade	Sem urgência (acima de dois anos)	O cenário não irá piorar (acima de dois anos)
2	Pouco grave	Pode aguardar um pouco (em dois anos)	Irá piorar a longo prazo (em dois anos)
3	Grave	O mais breve possível (até um ano e seis meses)	Irá piorar a médio prazo (até um ano e seis meses)
4	Muito grave	Alguma urgência (em um ano)	Irá piorar a curto prazo (em um ano)
5	Extremamente grave	É necessário uma ação imediata (em até seis meses)	Irá piorar rapidamente (em até seis meses)

Tabela 4 - Critérios de priorização: Gravidade, Urgência e Tendência

Esta seção apresenta as necessidades priorizadas de acordo com a matriz Gravidade, Urgência e Tendência (GUT). O valor para prioridade foi constituído a partir do produto atribuído as colunas G, U e T.

Estimativa do Risco

A Estimativa do Risco consiste de 4 (quatro) etapas:

- ✓ Etapa 1: Avaliar Estimativas: atribuir valores aos ativos, ameaças, vulnerabilidades e consequências, e colocar os riscos em ordem de prioridade.
 - Quantitativa: para calcular valores para cada componente coletados durante a etapa de identificação de riscos. Utiliza dados exatos, valores numéricos inteiros.
 - Qualitativa: avaliar a intensidade de consequências e a probabilidade de ocorrência de riscos de atributos qualificadores e descritivos. É uma estimativa subjetiva, que utiliza a escala fornecida na *Tabela 5* para estimar os riscos de TIC.

ESCALA PARA ANÁLISE DOS RISCOS		
Nível do Risco	Sinal	Pontuação
Muito Alto		5
Alto		4
Médio		3
Baixo		2
Muito Baixo		1

Tabela 5 - Escala para Análise dos Riscos

- ✓ Etapa 2: Avaliar Consequências: avaliar o impacto de um incidente para a organização.

- ✓ Etapa 3: Avaliar Probabilidade dos Incidentes: avaliar probabilidade de cada cenário e o impacto.

A *Tabela 6* fornece os critérios de avaliação da probabilidade, histórico de ocorrência de um risco acontecer.

CRITÉRIOS DE AVALIAÇÃO DE PROBABILIDADE - HISTÓRICO DE OCORRÊNCIA (HI)			
Nível		Frequência	Descrição
5	Muito Alto	<i>Ocorreu mais de três vezes em um ano</i>	<i>É praticamente certo que ocorra novamente</i>
4	Alto	<i>Ocorreu três vezes em um ano.</i>	<i>Grande possibilidade de ocorrer</i>
3	Médio	<i>Ocorreu duas vezes em um ano.</i>	<i>Talvez ocorra novamente</i>
2	Baixo	<i>Ocorreu uma vez em um ano.</i>	<i>Pouco Provável que ocorra novamente</i>
1	Muito Baixo	<i>Não ocorreu em um ano ou não se tem registro</i>	<i>Provavelmente não ocorra novamente</i>

Tabela 6 - Critérios de Avaliação de Probabilidade - Histórico de Ocorrências

A *Tabela 7* fornece os critérios de avaliação da probabilidade com os fatores contribuintes para que um determinado risco ocorra.

CRITÉRIOS DE AVALIAÇÃO DE PROBABILIDADE - FATORES CONTRIBUINTES (FC)		
Nível		Fatores Contribuintes (FC)
5	Alto	<p><i>Não existem procedimentos de controle ou registro.</i></p> <p><i>Vulnerabilidade Técnica com exploração de dificuldade Baixa (CVSS).</i></p> <p><i>Vinte usuários ou mais por ativo.</i></p> <p><i>Inexistência de profissional qualificado na Tecnologia.</i></p> <p><i>Três ou mais agentes geradores da ameaça.</i></p> <p><i>Procedimento ocorre uma vez por mês ou mais.</i></p>
3	Médio	<p><i>Procedimentos de controle ou registro existem, mas não são auditados periodicamente.</i></p> <p><i>Vulnerabilidade Técnica com exploração de dificuldade Média (CVSS).</i></p> <p><i>De cinco a vinte usuários por ativo.</i></p> <p><i>Profissional em qualificação na Tecnologia.</i></p> <p><i>Dois agentes geradores da ameaça.</i></p> <p><i>Procedimento ocorre trimestralmente.</i></p>
1	Baixo	<p><i>Procedimentos controle ou registro existem e são auditados regularmente.</i></p> <p><i>Vulnerabilidade Técnica com exploração de dificuldade Alta. (CVSS).</i></p> <p><i>Menos de 5 usuários por ativo.</i></p> <p><i>Um ou mais profissionais qualificados na Tecnologia.</i></p> <p><i>Um agente gerador da ameaça.</i></p> <p><i>Procedimento ocorre anualmente ou em períodos maiores.</i></p>

Tabela 7 - Critérios de Avaliação de Probabilidade - Fatores Contribuintes

- ✓ Etapa 4: Estimar Nível do Risco: designar valores para probabilidade e consequências de um risco. A Figura 15 apresenta o processo de estimar níveis de risco.

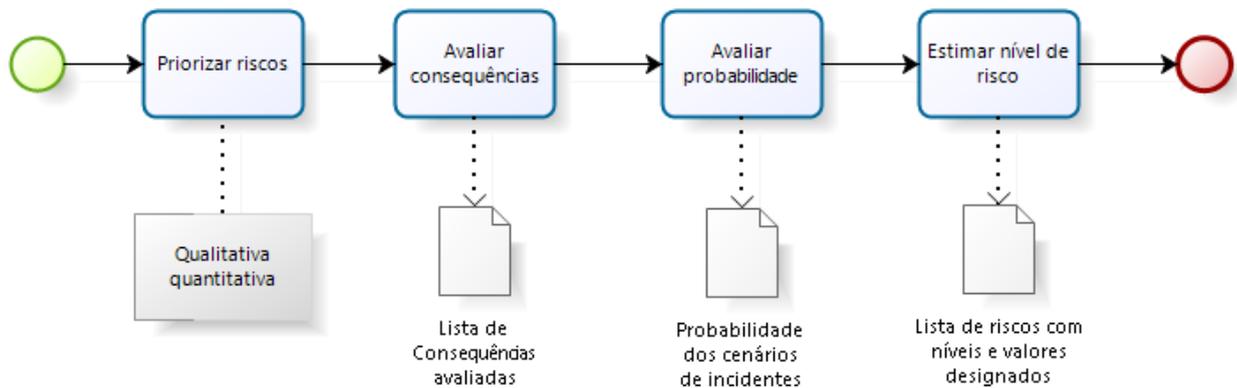


Figura 15 - Processo de Estimativa do Nível do Risco

Tratamento dos Riscos

Nesta fase, deve-se criar um plano de tratamento dos riscos, relacionando ações de segurança, responsáveis, prioridades e prazos para execução necessária para sua implantação. Para isso, deve-se observar requisitos legais, análise de custo/benefício e restrições organizacionais, técnicas e estruturais.

O Plano de Tratamento de Riscos deve determinar as formas de tratamento dos riscos identificados: reduzir, evitar, transferir ou reter. O Anexo III apresenta o plano de tratamento de riscos.

Na implementação do Plano de Tratamento de Riscos, serão executadas todas as ações de segurança de informação e comunicação incluídas no plano aprovado. Deve haver um acompanhamento do gestor em relação às ações, principalmente com relação aos prazos. A Figura 16 apresenta o processo do Plano de Tratamento de Riscos.

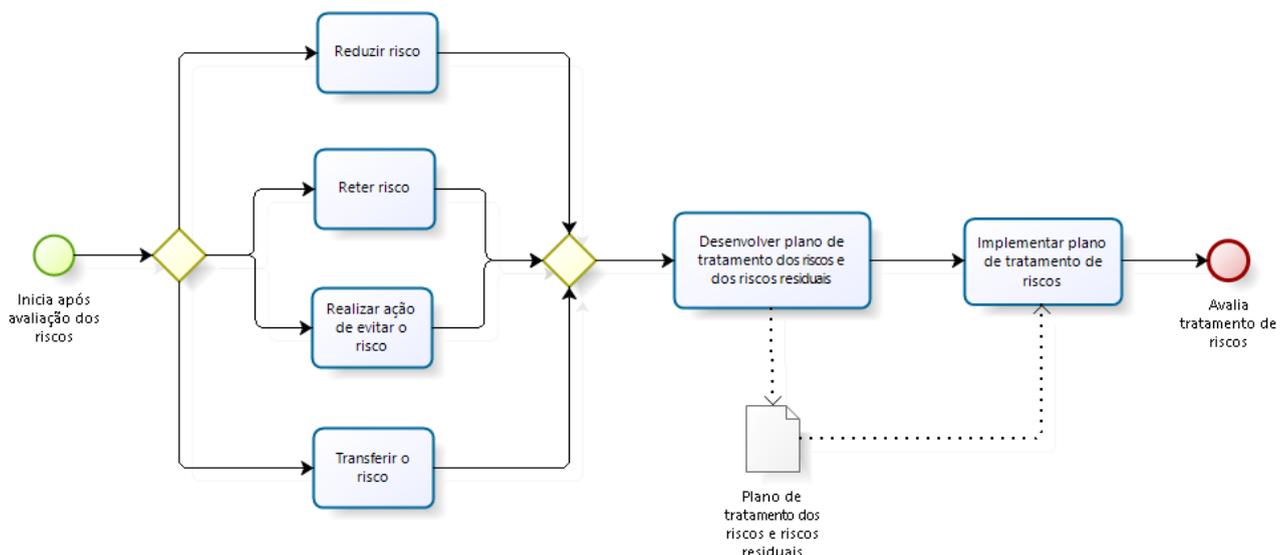


Figura 16 - Processo de Plano de Tratamento de Riscos

Monitoramento e Análise Crítica

Nesta etapa, é realizado o acompanhamento dos resultados, implementação dos controles, monitoramento de riscos residuais, identificação de novas ameaças e análise crítica visando a melhoria contínua do processo de gestão de riscos. Esta fase deve ser realizada pelo CGTIC, para verificar se a gestão de riscos está atendendo aos objetivos de negócio da organização.

O Monitoramento e Análise Crítica deve ser feito para:

1. Verificar se o tratamento está sendo implementado conforme planejado;
2. Novos ativos foram incluídos no escopo da gestão de riscos;
3. Verificar se os controles realizados ainda estão sendo eficazes;
4. Cenários de incidentes e probabilidades ainda são válidos;
5. Novos agentes capazes de explorar novos riscos;
6. Políticas e procedimentos estão sendo executados de forma adequada;
7. Ocorrência de novos incidentes relacionados a segurança de informação;
8. Novos riscos não identificados; e
9. Novos riscos que elevaram as consequências e impactos a um nível de risco inaceitável.

Esta fase tem como entrada todas as informações sobre os riscos obtidas nas atividades, a saída deve ser o alinhamento contínuo da gestão de riscos com os objetivos de negócio e com os critérios de risco, permitindo que a instituição analise seu processo de gestão de riscos e execute as melhorias necessárias ao processo.

Aceitação do Risco

Na fase de aceitação do risco é feita a análise do plano de tratamento de riscos. A partir desta análise será elaborado um documento formal com os riscos que serão aceitos, chamado de Declaração de Aplicabilidade, onde serão descritos os controles não aplicáveis e justificativa do fato de não serem contemplados. Esta aceitação cabe aos gestores por meio do CGTIC.

A Figura 17 apresenta a entrada para ação de aceitação do risco e a saída que ela provê.

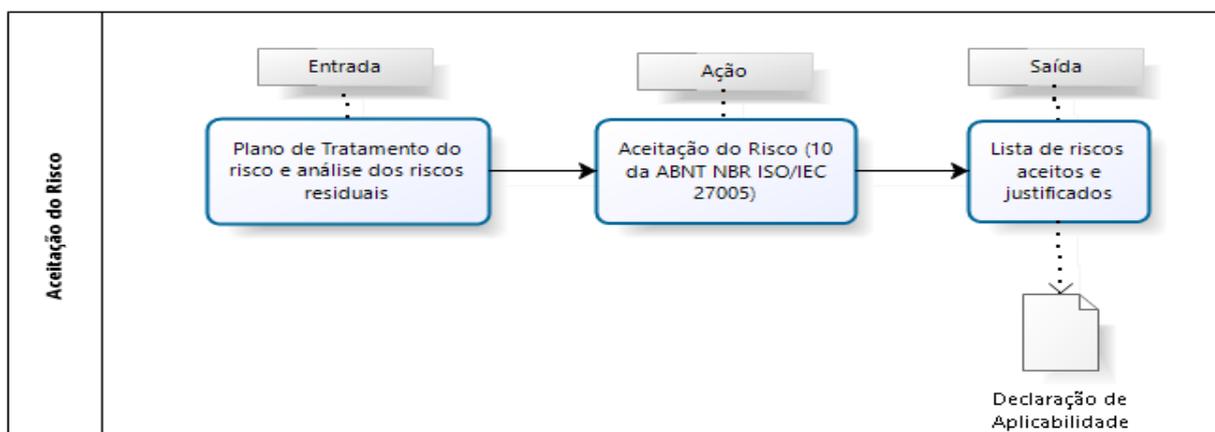


Figura 17 - Entradas e Saída da Aceitação de Riscos

Foram definidos critérios para análise de aceitação de riscos, assim, facilitando a decisão do CGTIC no momento em que for realizar a aceitação de riscos. Os critérios estão na Tabela 6.

CRITÉRIOS DE AVALIAÇÃO DE PROBABILIDADE - HISTÓRICO DE OCORRÊNCIA (HI)			
Nível		Freqüência	Descrição
5	Muito Alto	<i>Ocorreu mais de três vezes em um ano</i>	<i>É praticamente certo que ocorra novamente</i>
4	Alto	<i>Ocorreu três vezes em um ano.</i>	<i>Grande possibilidade de ocorrer</i>
3	Médio	<i>Ocorreu duas vezes em um ano.</i>	<i>Talvez ocorra novamente</i>
2	Baixo	<i>Ocorreu uma vez em um ano.</i>	<i>Pouco Provável que ocorra novamente</i>
1	Muito Baixo	<i>Não ocorreu em um ano ou não se tem registro</i>	<i>Provavelmente não ocorra novamente</i>

Tabela 6 - Critérios para Aceitação dos Riscos

Comunicação do Risco

A comunicação do risco é a troca de informações, conhecimentos e percepções sobre como os riscos devem ser gerenciados. É uma fase muito importante para o sucesso da gestão de riscos da segurança da informação. Todas as partes envolvidas antes do desenvolvimento, durante e após a conclusão precisam ser comunicadas, com apresentação de resultados alcançados e metas atingidas. Todos os integrantes da Gestão de Riscos devem compartilhar informações entre as partes interessadas e tomadores de decisões. Nesta fase, todas as mudanças que ocorrem na fase de monitoramento e análise crítica chegam ao conhecimento de todos os integrantes do processo. A Tabela 7 apresenta a Matriz de Riscos - Impacto X Probabilidade

MATRIZ DE RISCOS							
		IMPACTO					
		Nível	Muito Baixo (MB)	Baixo (B)	Médio (M)	Alto (A)	Muito Alto (MA)
PROBABILIDADE	Muito Alto (MA)		5	10	15	20	25
	Alto (A)		4	8	12	16	20
	Médio (M)		3	6	9	12	15
	Baixo (B)		2	4	6	8	10
	Muito Baixo (MB)		1	2	3	4	5

Tabela 7 - Matriz de Riscos - Impacto X Probabilidade

ESCOPO

A abrangência e foco deste plano são as equipes (recursos humanos), levando em conta os fatores físicos, estruturais e os ecossistemas.

PAPÉIS E RESPONSABILIDADES

Diretoria de Tecnologia da Informação e Comunicação (DTIC) - Diretoria responsável por orquestrar ações de suas coordenações durante eventuais interrupções e suas consequências.

Coordenadoria de Infraestrutura e Redes (CIR) - Responsável pelas ações de manutenção dos serviços de redes e infraestrutura do data center do IFSC, bem como configuração e instalação de sistemas em geral. Deve ser acionada sempre que houverem interrupções nos serviços de internet, intranet e aplicações indisponíveis.

Departamento de Sistemas da Informação (DSI) - Atua na parte de parametrização e programação de sistemas, bem como na manutenção de aplicações institucionais. Deve ser acionada no caso de bugs ou defeitos que impossibilitam o uso mínimo das ferramentas de software hospedadas no IFSC.

Coordenação de Governança de TI (CGovTIC) - Trabalha como setor de regulação e regulamentação, atuando na parte de planejamento e projetos de TI sempre que solicitada. Atende demandas de órgãos de controle, como auditorias externas e internas, referentes a planos ou políticas que dizem respeito à organização da TI.

Coordenadoria de TIC dos Câmpus (CTICs) - Equipe responsável pelas ações de manutenção dos serviços de voz/dados e computadores dos câmpus, bem como configuração e instalação de sistemas que eventualmente estão sob responsabilidade dos Câmpus.

AUTORIDADES RESPONSÁVEIS

As autoridades designadas neste plano seguirão a seguinte linha decisória:

1. Reitor(a);
2. Pró-Reitor(a) de Desenvolvimento Institucional (PRODIN);
3. Diretor(a) de TIC;
 - a. Coordenadoria de Governança de TI (CGovTIC);
 - b. Coordenadoria de Infraestrutura e Redes (CIR);
 - c. Departamento de Sistemas de Informação (DSI).

REFERÊNCIAS

Cestari Filho, Felício. ITIL V3 - Fundamentos/Felício Cestari Filho. - Rio de Janeiro: RNP/ESR, 2011.

Cestari Filho, Felício. Gerenciamento de Serviços/ Felício Cestari Filho. - Rio de Janeiro: RNP/ESR, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT ISO/IEC Guia 73:2009: Gestão de riscos – Vocabulário. Rio de Janeiro: ABNT, 2009a.

_____. NBR ISO 31000:2009 – Gestão de Riscos – Princípios e Diretrizes. Rio de Janeiro: ABNT, 2009b.

_____. ABNT NBR ISO/IEC 27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2008b.

Anexo I

PLANO DE TRATAMENTO DE RISCOS E RISCOS RESIDUAIS

O Tratamento de Riscos é utilizado para responder aos riscos identificados. Este plano conterá uma descrição prática, sequência de prioridade, recursos necessários, atribuições, prazos e informações importantes para medir o desempenho dos tratamentos de riscos.

Os Riscos Residuais são aqueles que restam após a implantação de controles para evitar, transferir ou mitigar os riscos. Após a implementação de um controle, pode ocorrer que o risco não tenha sido totalmente mitigado, estes devem ser tratados por meio da implementação de controles.

Reduzir Risco: ou mitigação do risco, significa implementar controles para reduzir os riscos a um nível aceitável, levando em conta custos de aquisição, implementação, administração, operação, monitoramento e manutenção de controles em relação ao valor do ativo que deve ser protegido. Deve ser escolhido um ou mais tipos de proteção para serem implantados, estes podem ser:

1. Correção: implementa controle a fim de corrigir qualquer anormalidade;
2. Eliminação: aplica controles a fim de excluir possíveis erros e vulnerabilidades, sem no entanto eliminar o risco, mas apenas reduzi-lo;
3. Prevenção: implementa controles com o intuito de prevenir e impedir a exploração de uma vulnerabilidade;
4. Minimização do Impacto: implementa controles a fim de reduzir ou limitar danos caso ocorra um incidente de segurança;
5. Dissuasão: ação, atividade ou medida de controle organizada e realizada a fim de fazer mudar opinião, intenção ou ideia;
6. Detecção: implementa controles realizados a fim de descobrir erros ou anormalidades;
7. Recuperação: implementa controle realizado a fim de voltar para uma situação de normalidade;
8. Monitoramento: aplica controles para acompanhar, observar, acompanhar desvios e perceber sinais de alerta de vulnerabilidades, ameaças e riscos a fim de tomar providências antecipadas; e
9. Conscientização: aplica controles e atividades de ensino para orientar sobre segurança de informação, fazendo com que todos os usuários saibam aplicar conhecimentos mostrados em sua rotina pessoal e profissional.

Reter Risco: a instituição aceita o risco sem fazer nada a respeito, ou seja, aceita correr o risco, incluindo ainda aqueles riscos que não tenham sido identificados. Deve ser feita de acordo com os critérios de aceitação dos riscos definidos pela instituição, esta definição deve ser embasada e registrada pela alta administração. É importante que seja criado um registro de riscos aceitos com justificativa e a relação de responsáveis pela aprovação (Declaração de Aplicabilidade - Aceitação de Riscos).

Realizar ação e Evitar Risco: realizar ações de mudança com o intuito de eliminar o risco. Quando a equipe de análise (CGTIC) identificar riscos em que os custos de implementação de controles são muito elevados ou que excedam os benefícios do negócio é possível decidir se o risco deve ser evitado.

Transferir Risco: também chamado de compartilhamento do risco, é quando a instituição opta por compartilhar com uma entidade externa o risco através de seguros que cubram as consequências da ocorrência de um incidente de segurança da informação. Também podem ser utilizados serviços parceiros (outsourcing) para a gestão de eventos de segurança de informação, de forma a transferir as operações de gestão do risco, porém a responsabilidade legal pelas consequências não é transferida.

A Figura 18 apresenta o processo de tratamento dos riscos.

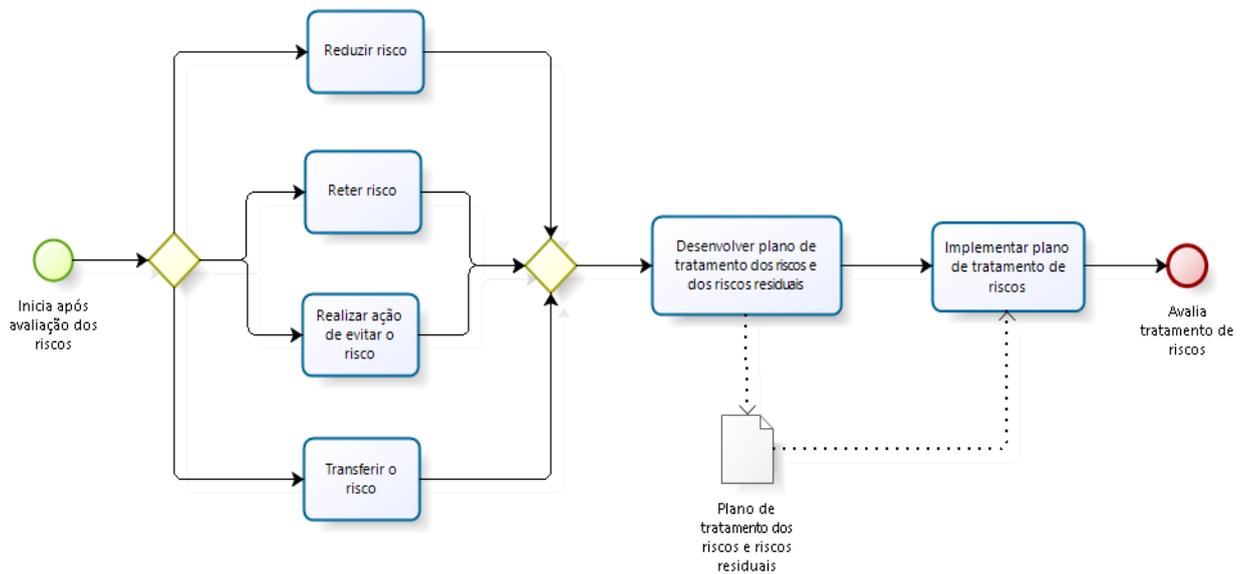


Figura 18 - Processo de Tratamento do Risco

PLANO DE TRATAMENTO DE RISCOS

A *Tabela 8* está contemplada com os riscos, níveis de risco, controles já existentes e controles a serem implantados.

1. RISCOS

Item 1.0 - Infraestrutura de TIC da Reitoria

ID RISCO-AMEAÇA	RISCO	NÍVEL	CONTROLE EXISTENTE	AÇÃO	CONTROLE A IMPLANTAR
R1 - 1.1.1	Indisponibilidade do sistema de rede sem fio em todos os Câmpus do IFSC	Baixo	C1 - Equipamento Redundante (in loco ou remoto)	Reduzir	C2 - Ativar contrato de garantia (manutenção física e atualização de firmware).
R1 - 1.1.2	Indisponibilidade do sistema de rede sem fio em todos os Câmpus do IFSC	Médio	-	Reduzir	C2 - Ativar contrato de garantia (manutenção física e atualização de firmware).
R1 - 1.2.1	Indisponibilidade do sistema de rede sem fio em todos os Câmpus do IFSC	Médio	-	Evitar	C3 - Substituição de equipamentos antigos (limitados a versão de firmware).
R2 - 2.1.1	Parada da rede interna de toda Reitoria	Médio	-	Reduzir	C4 - Substituição por novo equipamento com fonte redundante
R2 - 2.3.1	Parada da rede interna de toda Reitoria	Baixo	-	Reter/Aceitar	-
R3 - 3.1.1	Indisponibilidade das linhas telefônicas da Reitoria	Baixo	C5 - Serviço de telefonia celular corporativo	Reter/Aceitar	
R3 - 3.2.1	Indisponibilidade das linhas telefônicas da Reitoria	Médio	C6 - Serviço de telefonia celular corporativa	Reduzir	C7 - Contratação de central virtual
R8 - 7.1.1	Possibilidade de invasão e furto dos dados, alteração nos dados	Baixo	-	Reter/Aceitar	-

R13 - 10.1.1	Perda de dados gravados	Alto	8.1.1 Manter contrato vigente de manutenção de fibra ótica	Reduzir	C1 - Equipamento redundante (in loco ou remoto)
-----------------	-------------------------	------	--	---------	---

Tabela 8 - Riscos de TIC - Infraestrutura de TIC/Reitoria

Item 1.1 - Infraestrutura de Apoio à TIC/Reitoria

ID RISCO-AMEAÇA	RISCO	NÍVEL	CONTROLE EXISTENTE	AÇÃO	CONTROLE A IMPLANTAR
R4 - 4.1.1	Indisponibilidade de todos os serviços hospedados localmente	Baixo	-	Reter/Aceitar	-
R4 - 4.1.2	Indisponibilidade de todos os serviços hospedados localmente	Alto	C8 - Manter contrato vigente de manutenção de fibra ótica	Reduzir	C9 - Acompanhar toda obra de construção/reforma que coloque em risco a estrutura física de redes
R9 - 8.1.1	Interrupção na manutenção de energia	Médio	-	Evitar	C12 - Substituição por novo equipamento
R9 - 8.1.2	Interrupção na manutenção de energia	Médio	-	Evitar	C12 - Substituição por novo equipamento
R10 - 8.2.1	Interrupção manutenção de energia	Médio	C14 - Manutenção de ARP vigente para aquisição de materiais de consumo	Reter/Aceitar	-
R11 - 8.3.1	Interrupção do fornecimento de energia	Médio	C10 - Ativação de contrato de suporte e manutenção	Reter/Aceitar	-
R12 - 9.1.1	Superaquecimento do Data center	Médio	C10 - Ativação de contrato de suporte e manutenção	Reter/Aceitar	-
R12 - 9.1.2	Superaquecimento do data center	Médio	C10 - Ativação de contrato de suporte e manutenção	Reter/Aceitar	-

Tabela 9 - Riscos de TIC - Infraestrutura de Apoio à TIC/Reitoria

Item 1.2 - Armazenamento e Processamento de Dados/Reitoria

ID RISCO-AMEAÇA	RISCO	NÍVEL	CONTROLE EXISTENTE	AÇÃO	CONTROLE A IMPLANTAR
R5 - 5.1.1	Defeito de hardware impedir o funcionamento de todo o processamento de dados	Alto	C10 - Ativação de contrato de suporte e manutenção	Reduzir	C11 - Prover estrutura física equivalente que suporte o processamento atual
R6 - 6.1.1	Perda de dados de backup	Alto	-	Evitar	C12 - Substituição por novo equipamento
R7 - 6.1.2	Perda de dados de produção	Alto	-	Reduzir	C10 - Ativação de contrato de suporte e manutenção
R14 - 11.1.1	Perda de dados pelo pouco tempo de retenção	Alto	-	Reduzir	C15 - Elaborar Política de Gestão de Dados
R15 - 12.1.1	Perda de dados por falha de restore	Baixo	-	Reduzir	C15 - Elaborar Política de Gestão de Dados
R16 - 12.2.1	Impossibilidade da restauração dos dados nos sistemas informatizados	Baixo	-	Reduzir	C15 - Elaborar Política de Gestão de Dados
R16 - 12.3.1	Impossibilidade da restauração dos dados nos sistemas informatizados	Baixo	-	Reduzir	C15 - Elaborar Política de Gestão de Dados
R16 - 12.4.1	Impossibilidade da restauração dos dados nos sistemas informatizados	Baixo	-	Reduzir	C15 - Elaborar Política de Gestão de Dados

Tabela 10 - Riscos de TIC - Armazenamento e Processamento de Dados//Reitoria

Item 1.3 - Sistemas/Reitoria

ID RISCO- AMEAÇA	RISCO	NÍVEL	CONTROLE EXISTENTE	AÇÃO	CONTROLE IMPLANTAR
R17 - 13.1.1	Atraso na entrega da solução de TIC	Alto	-	Reduzir	C16 - Definição de cronograma de entrega com níveis de alarme ao ultrapassar os prazos por etapas
R17 - 13.1.2	Atraso na entrega da solução de TIC	Alto	-	Evitar	C17 - Elaboração de documento de aceite de funcionalidades pelas partes interessadas
R18 - 13.1.3	Comprometimento de funcionalidade não diretamente relacionadas	Alto	-	Evitar	C18 - Realização de reunião de validação de entregas parciais
R19 - 13.1.4	Não atendimento às necessidades dos usuários	Alto	-	Evitar	C18 - Realização de reunião de validação de entregas parciais
R19 - 13.1.5	Não atendimento às necessidades dos usuários	Alto	-	Evitar	C18 - Realização de reunião de validação de entregas parciais
R20 - 13.1.6	Atraso na manutenção e evolução da solução de TIC	Médio	-	Evitar	C19 - Sujeitar documentação final às partes interessadas
R21 - 13.2.1	Atraso no desenvolvimento da solução	Alto	-	Reduzir	C20 - Definição formal (portaria) da equipe de planejamento de soluções (incluindo dono do negócio, e substituto, e responsáveis pelo suporte comercial)
R21 - 13.2.2	Atraso no desenvolvimento da solução	Alto	-	Reduzir	C21 - Definição de canal oficial de comunicação entre as partes interessadas
R21 - 13.2.3	Atraso no desenvolvimento da solução	Alto	-	Reduzir	C22 - Definição de arbitragem entre as partes interessadas
R21 - 13.2.4	Atraso no desenvolvimento da	Alto	-	Evitar	C20 - Definição formal (portaria) da

	solução				equipe de planejamento de soluções (incluindo dono do negócio, e substituto, e responsáveis pelo suporte negocial)
R22 - 13.2.5	Sobrecarga no atendimento de chamados pela equipe de TIC	Alto	-	Evitar	C20 - Definição formal (portaria) da equipe de planejamento de soluções (incluindo dono do negócio, e substituto e responsáveis pelo suporte negocial)
R23 - 13.3.1	Não entrega de projetos importantes para a instituição	Alto	-	Reduzir	C23 - Elaboração de um plano de execução de tarefas evitando o acúmulo
R23 - 13.3.2	Não entrega de projetos importantes para a instituição	Alto	-	Evitar	C24 - Definição de projetos que serão desenvolvidos durante o ano (PDTIC)
R23 - 13.3.3	Não entrega de projetos importantes para a instituição	Alto	-	Evitar	C25 - Iniciar novo código somente após adequação de códigos antigos
R24 - 13.4.1	Inoperabilidade das soluções de TIC	Alto	-	Evitar	C26 - Definição de modelo de arquitetura para novos projetos
R24 - 13.4.2	Inoperabilidade das soluções de TIC	Alto	-	Evitar	C26 - Definição de modelo de arquitetura para novos projetos
R24 - 13.4.3	Inoperabilidade das soluções de TIC	Alto	-	Reduzir	C26 - Definição de modelo de arquitetura para novos projetos
R25 - 13.5.1	Entendimento de uso equivocado da funcionalidade	Alto	-	Evitar	C27 - Definição de gerenciamento de serviços de TIC - Entregas
R25 - 13.5.2	Entendimento de uso equivocado da funcionalidade	Alto	-	Reduzir	C27 - Definição de gerenciamento de serviços de TIC - Entregas
R26 -	Solução	Alto	-	Evitar	C28 - Revisão de

13.6.1	indisponível em momentos críticos				códigos antigos
R27 - 13.6.2	Furto e vazamento de dados	Alto	-	Evitar	C29 - Atualização de patches de segurança
R28 - 13.6.3	Sistemas sem integração aumentando o trabalho dos usuários na execução de uma tarefa	Alto	-	Evitar	C28 - Revisão de códigos antigos
R29 - 13.6.4	Comprometimento de funcionalidades	Alto	-	Evitar	C28 - Revisão de códigos antigos

Tabela 11 - Riscos de TIC - Sistemas//Reitoria

Item 1.4 - Segurança de Redes/Reitoria

ID RISCO-AMEAÇA	RISCO	NÍVEL	CONTROLE EXISTENTE	AÇÃO	CONTROLE A IMPLANTAR
R30 - 14.1.1	Máquina ou recursos de rede indisponível para seus usuários	Alto	-	Evitar	C30 - Implantar DS/IPS
R31 - 14.2.1	Lentidão no computador	Alto	-	Evitar	C31 - Implantar ferramenta de análise e detecção de vulnerabilidades
R32 - 14.2.1	Falhas no computador	Alto	-	Reduzir	C31 - Implantar ferramenta de análise e detecção de vulnerabilidades
R33 - 14.2.1	Furto de identidade para coletar informações e/ou dados pessoais do computador	Alto	-	Reduzir	C31 - Implantar ferramenta de análise e detecção de vulnerabilidades
R34 - 14.3.1	Implementação de alterações nos dados ou programa	Médio	-	Reduzir	C15 - Elaborar política de gestão de dados
R35 - 14.3.1	Furto de arquivo de dados	Médio	-	Reduzir	C15 - Elaborar política de gestão de dados
R36 - 14.3.1	Acesso a sites de downloads ilegais	Médio	-	Reduzir	C15 - Elaborar política de gestão de dados
R37 - 14.3.2	Perda de Produtividade: o uso indevido de recursos de	Médio	-	Reduzir	C31 - Implantar ferramenta de análise

	TI, como largura de banda de rede, pode causar tempo de resposta lento, atrasando atividades legítimas no computador que, em aplicativos críticos como a negociação de ações, podem ser muito caros				e detecção de vulnerabilidades
R38 - 14.4.1	Comprometimento dos serviços internamente	Baixo	-	Reduzir	C32 - Implantar solução de segurança física
R39 - 14.5.1	Falsificação de identidade	Médio	-	Reduzir	C33 - Implantar práticas de codificação segura (BD)
R40 - 14.5.1	Violação de dados existentes	Médio	-	Reduzir	C33 - Implantar práticas de codificação segura (BD)
R41 - 14.5.1	Divulgação completa de todos os dados no sistema	Médio	-	Reduzir	C33 - Implantar práticas de codificação segura (BD)
R42 - 14.5.1	Destruição ou indisponibilidade dos dados	Médio	-	Reduzir	C33 - Implantar práticas de codificação segura (BD)
R43 - 14.6.1	Ataques externos aos sistemas de TIC	Médio	-	Reduzir	C34 - Implantar solução de hardening

Tabela 12 - Riscos de TIC - Segurança de Redes//Reitoria

Item 1.6 - Recursos Humanos de TIC Reitoria

Nestes riscos estão incluídos todos os profissionais da DTIC. A fim de definição segue os dados dos servidores.

	NOME	FUNÇÃO	CÂMPUS	CARGO/OBS
1	Benoni de Oliveira Pires	Analista de TI	DTIC/Reitoria	Diretor de TI
2	Aline Pacheco Primão	Analista de TI	CGovTIC/DTIC/Reitoria	Horário mestrado
3	Farleir Luís Minozzo	Analista de TI	CGovTIC/DTIC/Reitoria	Coordenador de Governança de TI
4	Evaristo Marcos de Quadros Junior	Analista de TI	CIR/DTIC/Reitoria	Coordenador de Infraestrutura e Redes
5	Luiz Fernando Costa	Analista de Ti	CIR/DTIC/Reitoria	6H
6	Vinicius Teixeira Coelho	Analista de TI	CIR/DTIC/Reitoria	6H
7	Kari de Souza Soares	Técnico de TI	CIR/DTIC/Reitoria	-
8	Charles da Silva Pereira	Técnico de TI	CIR/DTIC/Reitoria	-
9	Gilberto José de Souza Coutinho	Técnico de TI	DSI/DTIC/Reitoria	Chefe do Departamento de Sistemas
10	Andrey Carmisini	Analista de TI	DSI/DTIC/Reitoria	-
11	Daniel Severo Estrazulas	Analista de TI	DSI/DTIC/Reitoria	-
12	Diogo Angeloni	Analista de TI	DSI/DTIC/Reitoria	-
13	Jaime Miranda Junior	Analista de TI	DSI/DTIC/Reitoria	licença doutorado (volta mar/2023)
14	Paulo Victor Rebouça Soares	Analista de TI	DSI/DTIC/Reitoria	-
15	Paulo Henrique Santini	Analista de TI	DSI/DTIC/Reitoria	6H
16	Samuel Bristot Loli	Analista de TI	DSI/DTIC/Reitoria	-
17	Sergio Nicolau da Silva	Analista de TI	DSI/DTIC/Reitoria	-
18	Esdras Rocha de Oliveira	Analista de TI	DSI/DTIC/Reitoria	-
19	Shirlei Aparecida de Chaves	Analista de TI	DSI/DTIC/Reitoria	-
20	Vanildo Santos	Analista de TI	DSI/DTIC/Reitoria	-
21	Victor Gonçalves	Analista de TI	DSI/DTIC/Reitoria	-

22	Carlos Eduardo Serpa de Sousa	Analista de TI	DSI/DTIC/Reitoria	licença por motivo particular (volta out/2020)
----	-------------------------------	----------------	-------------------	--

Tabela 13 - Recursos Humanos de TIC/IFSC

ID RISCO-AMEAÇA	RISCO	NÍVEL	CONTROLE EXISTENTE	AÇÃO	CONTROLE A IMPLANTAR
R44 - 15.1.1	Perda de dados por soluções implantadas incorretamente	Médio	-	Reduzir	C44 - Capacitar servidores em especificação de requisitos
R45 - 16.1.1	Não atendimento aos princípios de gestão, governança e gerenciamento de serviços	Médio	-	Reduzir	C35 - Elaboração de plano de capacitação por competências
R46 - 17.1.1	Soluções de TIC não entregues ou entregue com falhas	Médio	-	Reduzir	C35 - Elaboração de plano de capacitação por competências
R47 - 18.1.1	Atendimento de suporte deficitário	Médio	-	Reduzir	C35 - Elaboração de plano de capacitação por competências
R48 - 19.1.1	Equipe trabalha o mínimo, sem visão de futuro, trazendo riscos ao desenvolvimento das estratégias institucionais	Médio	-	Reduzir	C35 - Elaboração de plano de capacitação por competências
R48 - 20.1.1	Equipe trabalha o mínimo, sem visão de futuro, trazendo riscos ao desenvolvimento das estratégias institucionais	Médio	-	Reduzir	C35 - Elaboração de plano de capacitação por competências
R48 - 21.1.1	Equipe trabalha o mínimo, sem visão de futuro, trazendo riscos ao desenvolvimento das estratégias institucionais	Médio	-	Reduzir	C35 - Elaboração de plano de capacitação por competências
R48 - 22.1.1	Equipe trabalha o mínimo, sem visão	Médio	-	Reduzir	C35 - Elaboração de plano de capacitação

	de futuro, trazendo riscos ao desenvolvimento das estratégias institucionais				por competências
--	--	--	--	--	------------------

Tabela 14 - Riscos em Recursos Humanos de TIC/IFSC

Item 1.7 - Processos de Negócio de TIC/Reitoria

ID RISCO-AMEAÇA	RISCO	NÍVEL	CONTROLE EXISTENTE	AÇÃO	CONTROLE A IMPLANTAR
R49 - 23.1.1	Chamados não atendidos por ficarem perdidos em relação ao tempo	Médio	-	Reduzir	C36 - Definir atendentes de nível 1 para os chamados
R50 - 24.1.1	Listas em desuso ativas	Médio	-	Reduzir	C37 - Definir controles de criação de email e lista
R51 - 25.1.1	Brechas abertas para invasão através de email que estão ativos, mas não são mais usados	Médio	-	Reduzir	C37 - Definir controles de criação de email e lista
R52 - 26.1.1	Serviços e sistemas indisponíveis	Baixo	-	Reduzir	C38 - Definição de ANS
R53 - 27.1.1	Perdas de tarefas em relação e aulas prejudicadas	Baixo	C39 - Definição de horário alternativo ao horário comercial	Reter/Aceitar	-
R54 - 28.1.1	Estratégias não executadas	Médio	-	Evitar	C40 - Criação de painel de indicadores para acompanhamento
R55 - 29.1.1	Atividades de gestão não executadas	Médio	-	Evitar	C40 - Criação de painel de indicadores para acompanhamento
R55 - 30.1.1	Atividades de gestão não executadas	Médio	-	Evitar	C40 - Criação de painel de indicadores para acompanhamento
R56 - 31.1.1	Não implantação de governança de TIC e distanciamento da estratégia institucional	Médio	-	Evitar	C40 - Criação de painel de indicadores para acompanhamento
R57 - 32.1.1	Desperdício do dinheiro público que poderia ser usado em outras demandas prioritárias para a instituição	Médio	-	Evitar	C41 - Consulta prévia ao planejamento de contratação com as áreas interessadas
R57 - 32.1.2	Desperdício do dinheiro público que poderia ser usado em	Médio	-	Evitar	C41 - Consulta prévia ao planejamento de contratação com as

	outras demandas prioritárias para a instituição				áreas interessadas
R58 - 33.1.1	Não atendimento às demandas institucionais	Médio	C42 - Uso de metodologias ágeis	Reduzir	C24 - Definição de projetos que serão desenvolvidas durante o ano (PDTIC)
R59 - 34.1.1	Excesso de integrações ao SIG com criação de aplicações “periféricas” ao mesmo	Médio	-	Reduzir	C43 - Atualização da arquitetura do SIG
R60 - 35.1.1	Solução desenvolvida não atende a demanda do solicitante	Médio	-	Reduzir	C44 - Capacitar servidores em especificação de requisitos

Tabela 15 - Riscos de TIC - Processos de Negócio de TIC/Reitoria

2. CONTROLES DE TIC

Os controles ajudam a proteger o ativo prevenindo fraudes, erros, desperdícios, assegurando o cumprimento de normas e planos de diretrizes institucionais. A *Tabela D* fornece os controles existentes e/ou controles a serem implantados pela TIC do IFSC.

CONTROLES	
Controle	Descrição do controle
C1	Equipamento redundante (<i>in loco</i> ou remoto)
C2	Ativação de contrato de garantia (manutenção física e atualização de firmware)
C3	Substituição de equipamentos antigos (limitados a versão de firmware)
C4	Substituição por novo equipamento com fonte redundante
C5	Fone@RNP
C6	Serviço de telefonia celular corporativa
C7	Contratação central virtual (VoIP)
C8	Manter contrato vigente de manutenção de fibra óptica
C9	Acompanhar toda obra de construção/reforma que coloque em risco a estrutura física de redes.
C10	Ativação de contrato de suporte e manutenção
C11	Prover estrutura física equivalente que suporte o processamento atual
C12	Substituição por novo equipamento
C13	Solução em software livre
C14	Manutenção de ARP vigente para aquisição de materiais de consumo
C15	Elaborar política de gestão de dados
C16	Definição de cronograma de entrega com níveis de alarme ao ultrapassar os prazos por etapas
C17	Elaboração de documento de aceite de funcionalidades pelas partes interessadas
C18	Realização de reunião de validação de entregas parciais
C19	Sujeitar documentação final às partes interessadas
C20	Definição formal (portaria) da equipe de planejamento da solução (incluindo dono do negócio, e substituto, e os responsáveis pelo suporte negocial).
C21	Definição de canal oficial de comunicação entre as partes interessadas
C22	Definição de arbitragem entre as partes interessadas
C23	Elaboração de um plano de execução de tarefas evitando o acúmulo
C24	Definição de projetos que serão desenvolvidos durante o ano (PDTIC)
C25	Iniciar novo código somente após adequação de códigos antigos
C26	Definição de modelo de arquitetura para novos projetos
C27	Definição de Gerenciamento de Serviço de TI - Entregas
C28	Revisão de códigos antigos
C29	Atualização de patches de segurança
C30	Implantar IDS/IPS
C31	Implantar ferramenta de análise e detecção de vulnerabilidades
C32	Implantar solução de segurança física

C33	Implantar práticas de codificação segura (BD)
C34	Implantação de solução de hardening
C35	Elaboração de plano de capacitação por competência
C36	Definir atendentes de nível 1 para os chamados
C37	Definir controles de criação de email e lista
C38	Definição de ANS
C39	Definição de horário alternativo ao horário comercial
C40	Criação de painel de indicadores para acompanhamento
C41	Consulta prévia ao planejamento de contratação com as áreas interessadas
C42	Uso de metodologias ágeis
C43	Atualização da arquitetura do SIG
C44	Capacitar servidores em especificação de requisitos

Tabela 16 - Controles de TIC

3. PRIORIZAÇÃO DOS RISCOS

Na *Tabela 17* será descrita, de forma priorizada, os riscos e prazos a serem cumpridos os controles.

PRIORIDADE	ID RISCO	NÍVEL DO RISCO	AÇÃO	ID CONTROLE IMP.	QUEM	PRAZO	ID RISCO RESIDUAL
1.0 - Infraestrutura de TIC/Reitoria							
1	R13 - 10.1.1	Alto	Reduzir	C1	DTIC/CIR		RR13
2	R1 - 1.2.1	Médio	Evitar	C3	DTIC/CIR		RR03
3	R1 - 1.1.2	Médio	Reduzir	C2	DTIC/CIR		RR02
4	R2 - 2.1.1	Médio	Reduzir	C4	DTIC/CIR		RR04
5	R3 - 3.2.1	Médio	Reduzir	C7	DTIC/CIR		RR05
6	R8 - 7.1.1	Médio	Reduzir	C12	DTIC/CIR		RR10
7	R1 - 1.1.1	Baixo	Reduzir	C2	DTIC/CIR		RR01
1.1 - Infraestrutura de Apoio à TIC/Reitoria							
1	R4 - 4.1.2	Alto	Reduzir	C9	DTIC/CIR		RR06
2	R9 - 8.1.1	Médio	Evitar	C12	DTIC/CIR		RR11
3	R9 - 8.1.2	Médio	Evitar	C12	DTIC/CIR		RR12
1.2 - Armazenamento e Processamento de Dados/Reitoria							
1	R5 - 5.1.1	Alto	Reduzir	C11	DTIC/CIR		RR07
2	R6 - 6.1.1	Alto	Evitar	C12	DTIC/CIR		RR08
3	R7 - 6.1.2	Alto	Reduzir	C10	DTIC/CIR		RR09
4	R14 - 11.1.1	Alto	Reduzir	C15	DTIC/CGOVTIC		RR14
5	R15 - 12.1.1	Baixo	Reduzir	C15	DTIC/CGOVTIC		RR15
6	R16 - 12.2.1	Baixo	Reduzir	C15	DTIC/CGOVTIC		RR16
7	R16 - 12.3.1	Baixo	Reduzir	C15	DTIC/CGOVTIC		RR17
8	R16 - 12.4.1	Baixo	Reduzir	C15	DTIC/CGOVTIC		RR18
1.3 - Sistemas/Reitoria							

1	R17 - 13.1.1	Alto	Reduzir	C16	DTIC/DSI		RR19
2	R17 - 13.1.2	Alto	Evitar	C17	DTIC/DSI		RR20
3	R18 - 13.1.3	Alto	Evitar	C18	DTIC/DSI		RR21
4	R19 - 13.1.4	Alto	Evitar	C18	DTIC/DSI		RR22
5	R19 - 13.1.5	Alto	Evitar	C18	DTIC/DSI		RR23
6	R21 - 13.2.1	Alto	Reduzir	C20	DTIC/DSI		RR25
7	R21 - 13.2.2	Alto	Reduzir	C21	DTIC/DSI		RR26
8	R21 - 13.2.3	Alto	Reduzir	C22	DTIC/DSI		RR27
9	R21 - 13.2.4	Alto	Evitar	C20	DTIC/DSI		RR28
10	R22 - 13.2.5	Alto	Evitar	C20	DTIC/DSI		RR29
11	R23 - 13.3.1	Alto	Reduzir	C23	DTIC/DSI		RR30
12	R23 - 13.3.2	Alto	Evitar	C24	DTIC/CGOVTIC		RR31
13	R23 - 13.3.3	Alto	Evitar	C25	DTIC/DSI		RR32
14	R24 - 13.4.1	Alto	Evitar	C26	DTIC/DSI		RR33
15	R24 - 13.4.2	Alto	Evitar	C26	DTIC/DSI		RR34
16	R24 - 13.4.3	Alto	Reduzir	C26	DTIC/DSI		RR35
17	R25 - 13.5.1	Alto	Evitar	C27	DTIC/DSI		RR36
18	R25 - 13.5.2	Alto	Reduzir	C27	DTIC/DSI		RR37
19	R26 - 13.6.1	Alto	Evitar	C28	DTIC/DSI		RR38
20	R27 -	Alto	Evitar	C29	DTIC/DSI		RR39

	13.6.2						
21	R28 - 13.6.3	Alto	Evitar	C28	DTIC/DSI		RR40
22	R29 - 13.6.4	Alto	Evitar	C28	DTIC/DSI		RR41
23	R20 - 13.1.6	Médio	Evitar	C19	DTIC/DSI		RR24
1.4 - Segurança de Redes/Reitoria							
1	R30 - 14.1.1	Alto	Evitar	C30	DTIC/CIR		RR42
2	R31 - 14.2.1	Alto	Evitar	C31	DTIC/CIR		RR43
3	R32 - 14.2.1	Alto	Reduzir	C31	DTIC/CIR		RR43
4	R33 - 14.2.1	Alto	Reduzir	C31	DTIC/CIR		RR43
5	R34 - 14.3.1	Médio	Reduzir	C15	DTIC/CGOVTIC		RR44
6	R35 - 14.3.1	Médio	Reduzir	C15	CTIC/CGOVTIC		RR44
7	R36 - 14.3.1	Médio	Reduzir	C15	CTIC/CGOVTIC		RR44
8	R37 - 14.3.2	Médio	Reduzir	C31	DTIC/CIR		RR45
9	R39 - 14.5.1	Médio	Reduzir	C33	DTIC/CIR		RR47
10	R40 - 14.5.1	Médio	Reduzir	C33	DTIC/CIR		RR47
11	R41 - 14.5.1	Médio	Reduzir	C33	DTIC/CIR		RR47
12	R42 - 14.5.1	Médio	Reduzir	C33	DTIC/CIR		RR47
13	R43 - 14.6.1	Médio	Reduzir	C34	DTIC/CIR		RR48
14	R38 - 14.4.1	Baixo	Reduzir	C32	DTIC/CIR		RR46
1.5 - Banco de Dados/Reitoria							
Próxim	Entrega						

a							
1.6 - Recursos Humanos/IFSC							
1	R44 - 15.1.1	Médio	Reduzir	C35	DTIC/CGOVTIC		RR49
2	R45 - 16.1.1	Médio	Reduzir	C35	DTIC/CGOVTIC		RR50
3	R46 - 17.1.1	Médio	Reduzir	C35	DTIC/CGOVTIC		RR51
4	R47 - 18.1.1	Médio	Reduzir	C35	DTIC/CGOVTIC		RR52
5	R48 - 19.1.1	Médio	Reduzir	C35	DTIC/CGOVTIC		RR53
6	R48 - 20.1.1	Médio	Reduzir	C35	DTIC/CGOVTIC		RR54
7	R48 - 21.1.1	Médio	Reduzir	C35	DTIC/CGOVTIC		RR55
8	R48 - 22.1.1	Médio	Reduzir	C35	DTIC/CGOVTIC		RR56
1.7 - Processos de Negócios/Reitoria							
1	R49 - 23.1.1	Médio	Reduzir	C36	DTIC		RR57
2	R50 - 24.1.1	Médio	Reduzir	C37	DTIC/CIR		RR58
3	R51 - 25.1.1	Médio	Reduzir	C37	DTIC/CIR		RR59
4	R54 - 28.1.1	Médio	Evitar	C40	DTIC		RR61
5	R55 - 29.1.1	Médio	Evitar	C40	DTIC		RR62
6	R55 - 30.1.1	Médio	Evitar	C40	DTIC		RR63
7	R56 - 31.1.1	Médio	Evitar	C40	DTIC		RR64
8	R57 - 32.1.1	Médio	Evitar	C41	DTIC		RR65
9	R57 - 32.1.2	Médio	Evitar	C41	DTIC		RR66
10	R58 -	Médio	Reduzir	C24	DTIC/DSI		RR67

	33.1.1						
11	R59 - 34.1.1	Médio	Reduzir	C43	DTIC/DSI		RR68
12	R60 - 35.1.1	Médio	Reduzir	C44	DTIC/DSI		RR69
13	R52 - 26.1.1	Baixo	Reduzir	C38	DTIC/CIR		RR60

Tabela 18 - Priorização dos Riscos

4. RISCOS RESIDUAIS

ID RISCO RESIDUAL	NÍVEL	STATUS	JUSTIFICATIVA
RR01	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR02	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR03	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR04	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR05	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR06	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR07	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR08	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR09	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR10	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR11	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR12	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR13	Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR14	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR15	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR16	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR17	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.

RR56	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR57	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR58	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR59	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR60	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR61	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR62	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR63	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR64	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR65	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR66	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR67	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR68	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
RR69	Muito Baixo	Reter/Aceitar	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.

Tabela 19 - Riscos Residuais

Anexo II

DECLARAÇÃO DE APLICABILIDADE

Aceitação dos Riscos

A declaração de aplicabilidade refere-se aos riscos que serão aceitos pela instituição. Neste documento, são descritos os controles não aplicáveis e justificativa do fato de não serem contemplados. Esta aceitação cabe aos gestores através do CGTIC.

ID RISCO	JUSTIFICATIVA
1.0 Riscos de Infraestrutura	
R2 - 2.3.1	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
R3 - 3.1.1	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
R8 - 7.1.1	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
1.1 Riscos de Infraestrutura de Apoio	
R4 - 4.1.1	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
R10 - 8.2.1	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
R11 - 8.3.1	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
R12 - 9.1.1	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
R12 - 9.1.2	O CGTIC entende que os controles são suficientes e o nível de risco, neste caso, é aceitável.
1.2 Armazenamento e Processamento de Dados	
-	
1.3 Sistemas	
-	
1.4 Segurança de Redes	
-	
1.5 Banco de Dados	
-	

1.6 Recursos humanos	
-	
1.7 Processos de Negócio	
-	

Tabela 20 - Aceitação de Riscos