



**RESOLUÇÃO CGD Nº 05, DE 04 DE JUNHO DE 2021**

Dispõe sobre o Sistema de Governança de Tecnologia da Informação e Comunicação (SGTIC) com sua estrutura, políticas e os desdobramentos.

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 Publicar o conjunto de políticas de TIC denominado Sistema de Governança de Tecnologia da Informação e Comunicação (SGTIC) com sua estrutura, políticas e os desdobramentos.

Art. 2º Esta Resolução entra em vigor na data de 01 de julho de 2021.

Obs.: Súmula da reunião do CGD disponível em:

<https://sigrh.ifsc.edu.br/sigrh/downloadArquivo?idArquivo=1771878&key=78f88f14d29001442983819d758327f3>

## *SISTEMA DE GOVERNANÇA 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**

**Sistema de Governança de TIC**

**SGTIC**

**2021 – 2025**

## **COMITÊ DE GOVERNANÇA DIGITAL**

### **Presidência**

André Dala Possa – Reitor Pró Tempore

Juarez Pontes – Diretor Executivo

### **Secretário-Executivo**

Benoni de Oliveira Pires – Diretor de TIC

### **Membros do CGD**

#### **Titulares**

Fabiana Besen Santos – Pró-reitora de Administração

Egon Sewald Júnior – Pró-reitor de Desenvolvimento Institucional

Luiz Otávio Cabral – Pró-reitor de Ensino

Rafael Nilson Rodrigues – Pró-reitor de Extensão e Relações Externas

Ailton Durigon – Pró-reitor 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)

## **Equipe de Elaboração do Sistema de Governança**

### **Coordenador**

Benoni de Oliveira Pires

### **Membros**

Farleir Luís Minozzo

Aline Pacheco Primão

## Sumário

HISTÓRICO DE VERSÕES	6
TERMOS E ABREVIações	7
APRESENTAÇÃO	8
O DOCUMENTO	8
ESCOPO	8
VIGÊNCIA	8
ABRANGÊNCIA	8
APROVAÇÃO E PUBLICAÇÃO	8
POLÍTICAS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	9
CONCEITOS	9
PRINCÍPIOS	10
DIRETRIZES	11
RESPONSABILIDADES	13
ESTRUTURA NORMATIVA	16
ANEXO I	18
ANEXO II	21



## ***HISTÓRICO DE VERSÕES***

<b>Data</b>	<b>Versão</b>	<b>Descrição</b>
08/2019	Versão 1.0	Versão inicial – Aprovado CGTIC 14/06/2019;
06/2021	Versão 1.1	Versão atualizada – Aprovado CGD 04/06/2021



## ***TERMOS E ABREVIações***

**CGD** – Comitê de Governança Digital

**CGTIC** – Comitê Gestor de Tecnologia da Informação e Comunicação

**CGTI** Coordenadoria de Governança de TI

**CIR** Coordenadoria de Infraestrutura de Redes

**CTIC** Coordenadoria de Tecnologia de Informação e Comunicação

**DSI** Departamento de Sistemas da Informação

**DTIC** Diretoria de Tecnologia da Informação e Comunicação

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

**PDTIC** Plano Diretor de Tecnologia da Informação e Comunicação

**PETIC** Planejamento Estratégico de Tecnologia da Informação e Comunicação

**PRODIN** Pró-Reitoria de Desenvolvimento Institucional

**SGTIC** Sistema de Governança de Tecnologia da Informação e Comunicação

**SISP** Sistema de Administração de Recursos de Tecnologia da Informação

**TIC** Tecnologia da Informação e Comunicação

## **APRESENTAÇÃO**

### **O DOCUMENTO**

Este documento tem por finalidade apresentar o Sistema de Governança de Tecnologia da Informação e Comunicação (SGTIC) com sua estrutura, políticas e os desdobramentos destas.

### **ESCOPO**

Este documento tratará da estrutura de governança de TIC, das políticas que a compõem e indicará o formato das normas e os tipos de planos a serem elaborados.

### **VIGÊNCIA**

O SGTIC terá vigência de 5 anos a partir de sua publicação. As revisões serão realizadas sempre que necessário com solicitação encaminhada e avaliada pelo Comitê de Governança Digital (CGD).

### **ABRANGÊNCIA**

A estrutura apresentada abrange toda a instituição devendo ser implantada pela DTIC em parceria com as CTICs.

### **APROVAÇÃO E PUBLICAÇÃO**

Este plano foi submetido para apreciação nos seguintes fóruns e colegiados, nesta ordem:

1. CGTIC – 14 de junho de 2019.
2. CGD – 04 de junho de 2021.



## ***POLÍTICAS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO***

### ***CONCEITOS***

#### ***Governança de TIC***

Governança é o sistema pelo qual, a atual e a futura utilização da TIC, é dirigida e controlada, envolvendo avaliar e direcionar sua utilização para apoiar a instituição e o acompanhamento deste uso para realizar planos, incluindo a estratégia e as políticas de utilização de TIC dentro da instituição.

#### ***Gestão de TIC***

A gestão de TIC é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades de TIC em consonância com a direção definida pelo Comitê de Governança Digital a fim de atingir os objetivos institucionais. Compreende a gestão dos recursos de TIC quer sejam processos, serviços, sistemas, infraestrutura e pessoas.

#### ***Capacidade de TIC***

Tem por objetivo assegurar que a capacidade da infraestrutura de TIC esteja alinhada com as necessidades do IFSC, suportando assim todos os processos que necessitam da TIC, dentro de um custo aceitável.

#### ***Gestão de Riscos de TIC***

Tem por objetivo levantar o desenvolvimento, disseminação e implementação de metodologias de gerenciamento de riscos institucionais, apoiando a melhoria contínua de processos de trabalho, projetos e a alocação e utilização dos recursos disponíveis, contribuindo para o cumprimento dos objetivos da instituição.

#### ***Continuidade de Negócios de TIC***

Tem por objetivo impedir a interrupção das atividades do negócio e proteger os processos críticos contra defeitos, falhas ou desastres, garantindo a retomada em tempo hábil, caso necessário.

#### ***Gestão de Dados***

Compreende a guarda segura, cópia de segurança e a restauração dos dados institucionais com garantia de confidencialidade, disponibilidade, integridade e autenticidade.

## PRINCÍPIOS

### Gerais

- **Foco nas Partes Interessadas:** as estruturas de governança e gestão, bem como as estratégias, os planos, projetos e serviços de TIC, deverão ser desenvolvidos tendo como principal insumo as necessidades das principais partes envolvidas no uso das tecnologias da informação e comunicação (alunos e sociedade), alinhadas aos objetivos do Governo Digital;
- **Gestão por Resultados:** as ações relacionadas à governança deverão ser implantadas considerando mecanismos para a medição e o monitoramento das metas, permitindo que a função de governança possa validar, direcionar, justificar e intervir nas estratégias e ações de TIC da organização, realizando benefícios com otimização de custos e riscos;
- **Conformidade:** as ações relacionadas à governança de TIC deverão contribuir para que se cumpram obrigações regulamentares, legislativas, legais e contratuais aplicáveis.
- **Transparência:** o desempenho, os custos, os riscos e os resultados das ações empreendidas pela área de TIC deverão ser medidos pela gestão de TIC e reportados à alta administração da organização e à sociedade por meio de canais de comunicação adequados, provendo transparência à aplicação dos recursos públicos em iniciativas de TIC e propiciando amplo acesso e divulgação das informações;
- **Prestação de Contas e Responsabilização:** os papéis e responsabilidades acerca das tomadas de decisão que envolvem os diversos aspectos de TIC deverão ser definidos, compreendidos e aceitos de maneira clara e sem ambiguidade, de forma a assegurar a adequada prestação de contas das ações, bem como a responsabilização pelos atos praticados;
- **TIC como Ativo Estratégico:** a governança deve ser implantada buscando o papel estratégico da TIC para contribuir, de maneira eficaz, com a sustentação dos serviços públicos providos pela organização e com a viabilização de novas estratégias;
- **Gestão por Processos:** a gestão deve ser guiada por processos de negócios congruentes com a instituição. Estes são modelados e controlados através da análise, definição e monitoramento, os quais devem ser revisados e otimizados de forma a permitir melhoria contínua;
- **Liderança:** a gestão deverá ser exercida através do alinhamento das equipes com a missão e visão de TIC alinhada à missão e visão institucional. O foco da gestão deverá estar nas pessoas como agentes de transformação e inovação;
- **Trabalho em Equipe:** Equipes de trabalho apresentam maiores e melhores resultados do que entes isolados; O trabalho em equipe intercampus deve ser fomentado trazendo ganhos institucionais e regrido a definição das capacitações a serem realizadas para as equipes de TIC;
- **Melhoria Contínua:** a gestão deve adotar práticas de pequenas mudanças e/ou incrementais, de forma a atingir resultados cada vez melhores, seja na entrega de serviços e soluções, ou em seus processos internos.

## Quanto a Gestão de Riscos

- Agregar valor e proteger a organização;
- Gestão dinâmica, interativa e capaz de reagir a mudanças;
- Ser parte integrante dos processos organizacionais;
- Ser parte da tomada de decisões;
- Abordar explicitamente a incerteza;
- Apoiar a melhoria contínua da organização.

## Quanto a Gestão de Dados

- **Confidencialidade:** garantir que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;
- **Disponibilidade:** garantir que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido;
- **Integridade:** garantir a não violação das informações, com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital;
- **Autenticidade:** assegurar a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria.

## *DIRETRIZES*

### Gerais

- Desenvolver e implantar a governança de TIC, levando em consideração as especificidades e o nível de maturidade atual do IFSC e observando as orientações e práticas definidas no documento Estratégia Brasileira para a Transformação Digital – e-Digital;
- Oferecer serviços por meios de canais digitais orientados pela perspectiva dos alunos e cidadãos;
- Estar alinhada a Estratégia Brasileira para a Transformação Digital: e-Digital;

- Promover o reúso de dados abertos pelos diferentes setores da sociedade, com o objetivo de estimular a transparência ativa de informações;
- Manter a capacidade da infraestrutura de TI alinhada com as necessidades do negócio dentro de um custo aceitável;
- Planejar as contratações de TIC;
- Fomentar a integração visando o compartilhamento e a otimização dos recursos de TIC entre as unidades do IFSC;
- Promover a segurança da informação;
- Avaliar e Monitorar os riscos de TIC para o cenário atual e futuro.

### ***Quanto a Continuidade de Negócios***

- Identificar e documentar os riscos que possam comprometer a continuidade das atividades críticas do IFSC;
- Identificar, documentar e avaliar os possíveis impactos à continuidade das atividades críticas, caso tais riscos se concretizem;
- Definir, implementar e manter um processo formal e documentado para a Análise de Impacto nos Negócios, incluindo:
  - Identificação das atividades que suportam os negócios críticos do IFSC;
  - Avaliação dos impactos de não realização das atividades críticas ao longo do tempo;
  - Fixação dos prazos de forma priorizada para a retomada das atividades, em um nível mínimo de execução tolerável, levando em consideração o tempo em que os impactos da interrupção tornem-se inaceitáveis;
  - Identificação de interdependências e recursos que suportam as atividades, incluindo fornecedores, terceiros e demais partes interessadas relevantes.
- Determinar uma estratégia de continuidade de negócios adequada para proteger, estabilizar, continuar, retomar e recuperar as atividades prioritárias, bem como suas interdependências e recursos de apoio;
- Estabelecer níveis adequados de autoridade e competência, no intuito de assegurar a comunicação efetiva às partes interessadas, bem como assegurar a continuidade das atividades críticas;
- O Plano de Continuidade de Negócios deve viabilizar a continuidade e a recuperação das atividades críticas, em caso de interrupção;
- Treinamentos e avaliações do SGCN devem ser realizados periodicamente para garantir a manutenção e o bom funcionamento dos planos de continuidade.

## Quanto a Gestão de Riscos

- Identificar, analisar, avaliar, tratar e monitorar os riscos de TIC de forma contínua;
- Promover a cultura de gestão de riscos como fator essencial para implantar as estratégias e planos de TIC, tomada de decisão e exercer os objetivos relacionados à TIC;
- Analisar o impacto que os riscos de TI têm sobre outras organizações públicas e demais partes interessadas, com consulta e compartilhamento de informações entre envolvidos;
- Estar alinhada à Política de Segurança da Informação e Comunicação do IFSC.

## Quanto a Gestão de Dados

- Criar condições favoráveis para gestão de espaço de armazenamento dos dados institucionais;
- Assegurar cópia dos dados institucionais;
- Disponibilizar dados institucionais aos usuários;
- Garantir autonomia ao usuário no uso dos dados sob sua responsabilidade;
- Gerar economia nos câmpus, com redução dos custos de aquisição de equipamentos e software de armazenamento e backup.

## **RESPONSABILIDADES**

### Governança

- O Comitê de Governança Digital é o órgão responsável pela Governança de TIC no IFSC;
- A Coordenadoria de Governança de Tecnologia da Informação e Comunicação, subordinada à DTIC é a responsável pela elaboração e execução da estratégia de governança de TIC do IFSC;
- As Coordenadorias de Tecnologia da Informação e Comunicação localizadas nos Câmpus do IFSC e as Coordenadorias ligadas à DTIC são unidades promotoras da estratégia de governança de TIC.

### Gestão

- Da Diretoria de Tecnologia da Informação e Comunicação:
  - Disponibilizar e manter os serviços e soluções de TIC hospedados nesta diretoria;
  - Planejar, desenvolver, implantar e evoluir os sistemas de informação hospedados nesta diretoria;

- Planejar, desenvolver, executar e monitorar as ações de TIC cuja abrangência se estenda a todos os Câmpus e reitoria do IFSC e estejam em alinhamento com o Plano Estratégico Institucional;
- Planejar, desenvolver, executar e monitorar o plano de capacitação dos servidores de TIC do IFSC;
- Gerenciar os recursos financeiros disponibilizados para a TIC;
- Realizar a gestão de risco em todas as áreas de TIC em consonância com a legislação vigente.
- Da Coordenadoria de Tecnologia da Informação e Comunicação:
  - Planejar, desenvolver, executar e monitorar os recursos de TIC circunscritos aos câmpus do IFSC;
  - Participar da elaboração do Plano Anual de Trabalho – PAT para as aquisições de TIC;
  - Realizar a gestão de risco em todas as áreas de TIC em consonância com a legislação vigente;

### Capacidade

- A DTIC é responsável por planejar, desenvolver, executar o plano de capacidade de TIC em âmbito institucional;
- O CGD é responsável por aprovar e monitorar o cumprimento do plano de capacidade de TIC;
- As CTICs são responsáveis por executar o plano de capacidade de TIC no âmbito dos câmpus.

### Gestão de Riscos

- Da Diretoria de Tecnologia da Informação e Comunicação:
  - Elaborar e executar o Plano de Gestão de Riscos de TIC;
  - Monitorar e tratar continuamente os riscos de TIC;
  - Determinar medidas mitigadoras, monitoramento e comunicação de ações e situações;
  - Divulgar, atualizar e gerenciar questões envolvendo a gestão de riscos;
  - Garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da Instituição.
- Do Comitê de Governança Digital:
  - Aprovar e acompanhar a execução do Plano de Gestão de Riscos de TIC;
  - Assegurar que o risco seja gerenciado de acordo com a política de gestão de riscos;
  - Monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a Política de Gestão de Riscos.

- Do Proprietário do Risco:
  - Monitorar, no âmbito de sua atuação, os riscos mapeados;
  - Comunicar sobre situações que envolvam risco;
  - Aplicar medidas de mitigação necessária;
  - Documentar artefatos que comprovem o monitoramento do risco.

## Continuidade de Negócios

- Compete ao Comitê de Governança Digital promover e coordenar o Sistema de Gestão de Continuidade de Negócios de TIC;
  - O Comitê de Governança Digital poderá indicar servidores de TIC dos Câmpus, que terão atribuições de implementar, manter e aprimorar o Sistema de Gestão de Continuidade de Negócios.
- Compete à alta administração zelar pela implementação e execução do Sistema de Gestão de Continuidade de Negócios de TIC.
- Compete à DTIC coordenar o Sistema de Gestão de Continuidade de Negócios, promovendo, implementando, mantendo e aprimorando o SGCN, conforme a Política de Continuidade de Negócios de TIC instituída para o IFSC.
- Compete ao Comitê de Governança Digital o gerenciamento de incidentes.

## Gestão de Dados

- A Diretoria de Tecnologia da Informação e Comunicação é o setor responsável pela gestão de armazenamento, cópia e restauração de dados armazenados no *data center* sob sua responsabilidade no IFSC ou em serviço de nuvem (cloud) sendo observada as normas contratuais;
- A Coordenadoria de Infraestrutura de Redes é o setor responsável pela elaboração e execução do Plano de Armazenamento, Cópia e Restauração de dados;
- Os dados institucionais do IFSC deverão estar armazenados em infraestrutura sob a responsabilidade da Diretoria de Tecnologia da Informação e Comunicação;
- Dados armazenados na infraestrutura dos Câmpus são de responsabilidade da Direção Geral dos Câmpus.

## **ESTRUTURA NORMATIVA**

A partir das políticas de TIC deverão ser elaborados os seguintes documentos:

### **Normas**

- Estabelecem os conceitos, detalhando os passos a serem executados, e as obrigações a serem observadas para o cumprimento da Política; As normas serão publicadas como Resoluções ou Instruções Normativas.

### **Planos**

- Instrumentalizam o disposto nas normas ou políticas, permitindo sua direta aplicação no âmbito do IFSC. Planos Resultantes das políticas de TIC:
  - Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC): Este documento tem por finalidade orientar o planejamento e o monitoramento dos objetivos estratégicos de TI e de suas respectivas metas e indicadores, de maneira a consolidar a importância da gestão de TI e garantir seu alinhamento às áreas de negócio da Instituição. O PETIC deverá estar alinhado ao PDI e EGD;
  - Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC): instrumento de diagnóstico, planejamento e gestão dos recursos de Tecnologia da Informação (TI). O PDTIC representa um instrumento de gestão para a execução das ações de TI da organização, possibilitando justificar os recursos aplicados em TI, minimizar o desperdício, garantir o controle, aplicar recursos naquilo que é considerado mais relevante e, por fim, melhorar o gasto público e o serviço prestado ao cidadão. O PDTIC deverá estar alinhado ao PETIC e PAT;
- Plano de Gestão de Riscos TIC (PGR): 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 instituição;
- Plano de Gestão de Capacidade de Negócio de TIC (PGCN): Instrumento cujo objetivo é avaliar a capacidade atual de TIC e as necessidades atuais e futuras das partes interessadas, avaliando eliminando as lacunas existentes;
- Sistema de Gestão de Continuidade de Negócios de TIC (SGCN): Inclui estruturas organizacionais, políticas, atividades de planejamento, responsabilidades, procedimentos, processos e recursos. Este instrumento fornece normas e padrões para que a instituição consiga recuperar, retomar e dar continuidade aos seus processos de negócios mais cruciais, evitando que eles sofram danos maiores. O SGCN é dividido em quatro (4) planos, que são:
  - Plano de Contingência (PC): Define as necessidades e ações mais imediatas. Deve ser utilizado somente quando todas as prevenções tiverem falhado;

- Plano de Administração ou Gerenciamento de Crises (PAC): Define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência;
- Plano de Recuperação de Desastres (PRD): Determina o planejamento para que, uma vez controlada a contingência e passada a crise, sejam retomados os níveis originais de operação;
- Plano de Continuidade Operacional (PCO): Seu objetivo é restabelecer o funcionamento dos principais ativos que suportam as operações da instituição, reduzindo o tempo de queda e os impactos provocados por um eventual incidente.
- Plano de Gestão de Dados: Instrumento cujo objetivo é o detalhamento das atividades e seus responsáveis em relação a preservação do dado institucional;
- Plano de Capacitação de Servidores de TIC: Documento que definirá a necessidade de capacitação de acordo com as competências necessárias para a execução das atividades de TIC, bem como o percentual dos valores financeiros a serem aplicados;
- Plano de Uso dos Recursos de TIC: Documento que definirá quais são os recursos de TIC e como se dará seu uso, bem como os responsáveis pelos mesmos;
- Plano de Atividades de TIC: Documento que definirá as atividades de TIC de acordo com as competências levantadas para cada área e demais instrumentos que normatizam as atividades do setor.

A política e planos de TIC deverão ser publicadas em portal institucional permitindo que seus conteúdos possam ser consultados pelo público em geral.

## **ANEXO I - DEFINIÇÕES**

- Acesso: permissão, privilégio ou capacidade de ler, registrar, atualizar, gerenciar ou administrar a consulta e/ou manipulação do acervo de dados e informações;
- Alta Administração: agentes públicos ou políticos responsáveis pela Continuidade de Negócios nos órgãos e entidades do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).
- Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- Análise de Impacto nos Negócios (*BIA – Business Impact Analysis*): processo de analisar as atividades e os efeitos que uma interrupção pode ter sobre elas;
- Armazenamento de Dados: consiste no armazenamento dos dados em local seguro com garantia de disponibilidade, autenticidade, integridade e confidencialidade.
- Atividades Críticas: são as atividades ou processos que devem ser realizados para entregar os principais produtos e serviços que permitirão que o IFSC alcance seus objetivos mais importantes e prioritários;
- 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.
- 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 CTI é responsável por alinhar os investimentos de Tecnologia da Informação com os objetivos estratégicos e apoiar a priorização de projetos a serem desenvolvidos.
- Comitê Gestor de Segurança da Informação (CGSI): é um órgão colegiado de natureza consultiva e propositiva que tem por finalidade planejar e coordenar as atividades de segurança da informação e colaborar com o Comitê de Tecnologia da Informação – CTI no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina – IFSC.
- Confidencialidade da Informação: Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Continuidade de Negócios: capacidade do IFSC de continuar a entrega de produtos ou serviços em um nível aceitável previamente definido após incidentes de interrupção;
- Dado: Qualquer elemento identificado em sua forma bruta e que, por si só, não conduz a uma compreensão de um fato ou situação.

- 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 da Informação: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- Estratégia de Continuidade de Negócios: abordagem do IFSC que garanta a recuperação e a continuidade de suas atividades diante da interrupção de suas atividades críticas decorrente de um desastre ou incidente;
- Estratégia de Governança Digital (EGD): Define objetivos estratégicos, metas, indicadores e iniciativas da Política de Governança de TIC e norteia programas, projetos, serviços, sistemas e atividades relacionadas. Este documento tem validade entre 2016 e 2019 para coincidir com a vigência do Plano Plurianual (PPA);
- Estratégia Brasileira de Transformação Digital: oferece um amplo diagnóstico dos desafios a serem enfrentados, uma visão de futuro, um conjunto de ações estratégicas que nos aproximam dessa visão, e indicadores para monitorarmos o progresso no atingimento de nossos objetivos;
- Gestão de Continuidade de Negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócios caso as ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a imagem do IFSC;
- Gestão de Riscos: 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 TIC: atividade responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades de TIC em consonância com a direção definida pela função de governança a fim de atingir os objetivos institucionais;
- Governança de TIC (GTIC): 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.
- Estimativa de Riscos: processo utilizado para atribuir valores à probabilidade e consequência de um risco.
- 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.
- Incidente: situação que pode representar ou levar à interrupção de negócios, perdas, emergências ou crises;

- **Integridade da Informação:** Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.
- **Interrupção:** evento, previsível ou imprevisível, que cause um desvio negativo, não planejado, das expectativas de entrega de produtos ou execução de serviços em relação aos objetivos do IFSC;
- **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.
- **Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETIC):** documento que fornece o planejamento estratégico de TIC em alinhamento ao Plano de Desenvolvimento Institucional da instituição, através dos recursos de tecnologia da informação e comunicação, permitindo que sejam definidos objetivos específicos para a TIC.
- **Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC):** documento de diagnóstico, planejamento e gestão de recursos e processos de TIC, que tem por objetivo atender as necessidades tecnológicas da instituição.
- **Risco:** Combinação da probabilidade de um evento indesejado ocorrer e de suas consequências para a organização.
- **Sistema de Gestão da Continuidade de Negócios (SGCN):** conjunto de elementos de gestão do IFSC que estabelece, implementa, opera, monitora, analisa criticamente, mantém e aprimora a continuidade de negócios;
- **Vulnerabilidade:** é qualquer fraqueza que possa ser explorada para comprometer a segurança da informação.

## ***ANEXO II - REFERÊNCIAS***

- ABNT NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2006.
- AABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.
- ABNT NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. Rio de Janeiro: ABNT, 2008.
- COBIT 5.0
- Decreto nº 8.638, de 15 de Janeiro de 2016, que institui a Política de Governança Digital para os órgãos e entidades da administração pública federal direta, autárquica e fundacional.
- Diretoria de Tecnologia da Informação e Comunicação. <https://dtic.ifsc.edu.br/>
- Estratégia de Governança Digital do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal – EGD/SISP.
- Guia ABNT ISO GUIA 73:2009 – Risk Management – Concepts and Vocabulary. Recomendações para uso em normas.
- Guia da Governança de Tecnologia da Informação e Comunicação do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal – SISP.
- Guia do Comitê de Tecnologia da Informação do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal – SISP
- Portaria nº 19, de 29 de Maio de 2017, que dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal – SISP.
- Instrução Normativa nº 4, de 11 de Setembro de 2014, que dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP do Poder Executivo Federal.
- ISO 22301:2013 – Segurança da Sociedade – Sistema de Gestão de Continuidade de Negócios – Requisitos.

- ISO 22313:2015 – Segurança da Sociedade – Sistema de Gestão de Continuidade de Negócios – Orientações.
- Missão, Visão e Valores do Instituto Federal de Santa Catarina - IFSC. <http://www.ifsc.edu.br/menu-institucional>
- Modelo de Governança de Tecnologia da Informação – Levantamento Completo Realizado junto aos Órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo – SISP.
- Norma Complementar NC04/IN01/DSIC/GSI/PR.
- Norma Complementar nº06, do Departamento de Segurança da Informação e Comunicações/Gabinete de Segurança Institucional da Presidência da República, publicada no DOU no 223, Seção 1, de 23/11/2009.
- Norma Técnica ABNT ISO/IEC 31010:2009 - Gestão de riscos - Técnicas para o processo de avaliação de riscos.
- Norma Técnica ABNT NBR ISO/IEC 31000:2009, Gestão de Riscos - Princípios e Diretrizes.
- Norma Técnica ABNT NBR ISO/IEC 38500:2009, Governança Corporativa de Tecnologia da Informação, que fornece princípios para orientar os dirigentes das organizações (incluindo proprietários, membros do conselho de administração, diretores, parceiros, executivos seniores ou similares) sobre o uso eficaz, eficiente e aceitável da Tecnologia de Informação dentro das organizações.
- Política de Continuidade de Negócios do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). Portaria MCTIC nº 1.141, de 05.03.2018. Publicada no D.O.U. de 07.03.2018, Seção I, Pág. 18.
- Portaria nº 403 de 29 de Março de 2012 do Instituto Federal de Santa Catarina - IFSC, que institui o Comitê de Tecnologia da Informação (CTI) no âmbito do IFSC.
- Regimento do Comitê de Tecnologia da Informação – CTI do Instituto Federal de Santa Catarina – IFSC.
- Resolução CONSUP nº 19, de 23 de Maio de 2016 do Instituto Federal de Santa Catarina – IFSC, que retifica o regulamento do Comitê de Tecnologia da Informação do IFSC e dá outras providências.
- Resolução CONSUP nº 52, de 24 de Outubro de 2016, que institui a Política de Segurança da Informação no âmbito do Instituto Federal de Santa Catarina – IFSC.
- Resolução CONSUP nº 09, de 26 de Março de 2021, Aprova, ad referendum, a criação do Comitê de Governança Digital do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina e aprova seu regimento.