POLÍTICA

TECNOLOGIA DA INFORMAÇÃO

RIO BRASIL TERMINAL

GOVERNANÇA DE SISTEMAS DE TI

IT SYSTEMS GOVERNANCE

RIO BRASIL TERMINAL

An ICTSI Group Company

Código:	PL TI - 012
Área:	Tecnologia da Informação
Revisão:	2
Data Revisão:	19/04/2025

Elaborador:	André Eudes S. dos Santos	Analista de Governança
Revisor:	Neuza Maria Balassiano Hauben	Coordenadora de Sistemas
Aprovador:	Rodrigo Almeida de Abreu	Gerente de TI

Sumário

1. OBJETIVO 4
2. APLICAÇÃO 4
3. ITENS OBRIGATÓRIOS NA GOVERNANÇA DE SISTEMAS 5
3.1 DOCUMENTO DE ESCOPO 6
3.2 ARQUITETURA DE TI 7
3.3 APROVAÇÃO 7
3.4 DESENVOLVIMENTO / TESTES 8
3.5 IMPLANTAÇÃO / PÓS-GO-LIVE 10
4. RESPONSABILIDADES 10
5. DIRETRIZES GERAIS 11
PLTI-013 - POLITICAS DE REVISÃO_CONTROLE DE ACESSOS_TI_V2.pdf 11
PLTI-008 - GESTÃO DE MUDANÇA_V3.docx 12
6. TERMOS UTILIZADOS 12
7. DOCUMENTOS RELACIONADOS 13
8. VIGÊNCIA 14
9. REVISÃO 14
10. ANEXOS 14
11. HISTÓRICO DE REVISÃO 14

Código:	PL TI - 012
Área:	Tecnologia da Informação
Revisão:	2
Data Revisão:	19/04/2025

1. OBJETIVO

Esta política estabelece diretrizes para a governança dos sistemas de Tecnologia da Informação (TI), criando o programa de **Application Lifecycle Management (ALM)** visando garantir a segurança da informação, conformidade regulatória, eficiência, continuidade dos serviços e alinhamento estratégico dos sistemas com os objetivos organizacionais da Rio Brasil Terminal, iTracker e CLIA Pouso Alegre do grupo ICTSI, pela aderência a boas práticas, como as Políticas Globais da ICTSI, ITIL, COBIT, LGPD e ISO 20000/27001.

2. APLICAÇÃO

A definição de **Sistema** no contexto da informática, refere-se a processos digitais automatizados que aproveitam as ferramentas da computação e da eletrônica para realizar sua complexa série de processos e operações, que podem exercer qualquer um dos processos descritos a seguir como: coleta, armazenamento, processamento, recuperação, transformação e apresentação de dados.

Independente da família de linguagem desenvolvida, seja ela de baixo ou alto nível, o que inclui as chamada liguagens “low-code” ou “no-code”, estes sistemas interagem e usufruem de infraestrutura de hardware e/ou redes para desempenhar sua função, exigindo uma avaliação abrangente de sua aplicabilidade, tecnologia empregada, segurança, adequação de infraestrutura e rede necessária e custos associados.

É dever da Equipe de TI e seus parceiros Fábricas de Software prezar pela tríade da CIA: Confidentiality, Integrity, Availability (Confidencialidade, Integridade e Disponibilidade), como meio de garantir a segurança da informação e a continuidade do negócio. Para atingir este objetivo a Política de Governança de Sistemas é uma peça fundamental e precisa da participação de todos nesta busca de um ambiente onde a informação é confiável, íntegra e disponível.

Esta política aplica-se a todos os sistemas corporativos, ou seja, utilizados pela organização seja em nível setorial ou geral, incluindo hardware, software, redes, dados e serviços que os suportam, bem como a todos os colaboradores, prestadores de serviço e demais partes interessadas que utilizem ou gerenciem recursos de TI da Rio Brasil Terminal, iTracker e CLIA Pouso Alegre.

Esta política é aplicável e obrigatória para:

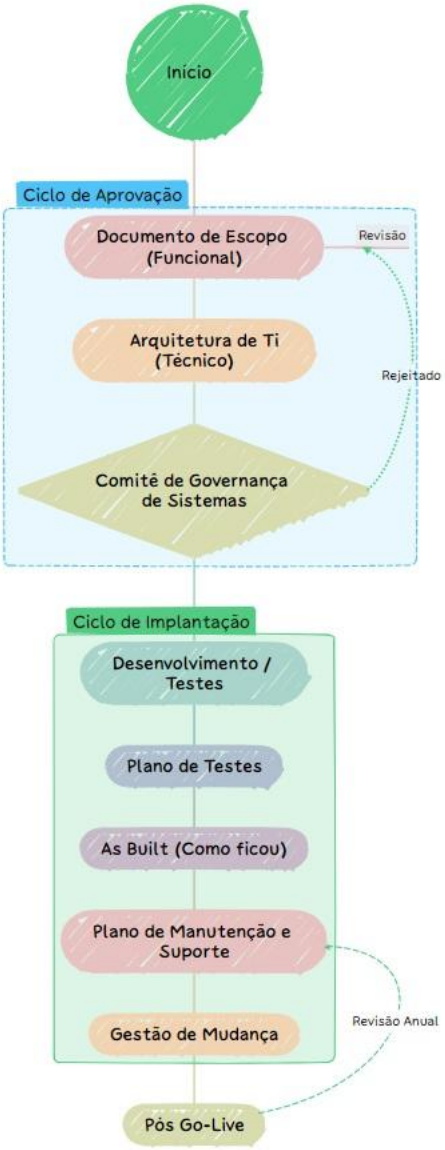
- **Fábricas de Softwares:** Será considerado e aplicado este conceito a qualquer equipe que desenvolva Sistema, conforme definição de sistema descrita deste capítulo, independente de ser parte da Equipe de TI, externos, ou demais áreas. Aplica-se à:
  - Desenvolvedores da Equipe de TI
  - Desenvolvedores, consultores, especialistas externos que forneçam ou desenvolvam software.
  - Demais equipes, independente da área ou cargo que desenvolvam software.
- **Áreas que demandam sistemas para uso corporativo.**

Esta política é aplicável e **obrigatória** a sistemas já existentes, novos sistemas que serão propostos e eventualmente criados ou contratados ou novas versões, módulos e funcionalidades, que devem ser cadastrados junto à Equipe de TI para iniciar o processo de regularização de conformidade de acordo com a nova política, conforme os itens descritos abaixo.

3. ITENS OBRIGATÓRIOS NA GOVERNANÇA DE SISTEMAS

Quando falamos de desenvolvimento de software, devemos contemplar todas as fases do **Ciclo de vida de desenvolvimento de software (SDLC)**, conforme etapas descritas abaixo.

Para softwares de mercado, muito do core do software é considerado segredo do comercial, porém o fornecedor deve fornecer as informações necessárias para entendimento da solução e sua interação com demais sistemas, infraestrutura e rede da ICTSI.



3.1 DOCUMENTO DE ESCOPO

Este documento possui natureza mais analítica e funcional e é necessário para descrever a necessidade original de negócio (processos **"As is'**), criticidade do conjunto de processos, volume, o objetivo que o sistema se propõe a cumprir (**"To be"**), contingências, quem são os patrocinadores do projeto, quais os recursos necessários (infraestrutura, licenças, fornecedores, pessoas), como o sistema vai atingir o objetivo proposto, indicar se tratará dados pessoais, qual o esforço, custo associado e ROI (Retorno sobre o Investimento). Este processo e

documentação associada, é necessária para novos sistemas, sistemas existentes, assim como novas funcionalidades ou módulos que serão adicionados.

Este documento dará subsídios para avaliar urgência, risco, custo e direcionar prioridades, assim como garantir que a proposta será de fato efetiva e que não há sobreposição de ações de equipes diferentes para o mesmo assunto.

3.2 ARQUITETURA DE TI

A Arquitetura de Ti é um documento com viés mais técnico e deve descrever (**"To be"**) as tecnologias que serão utilizadas, a arquitetura do sistema, mapeamento e tecnologia das integrações, uso de licenciamento, produtos ou componentes de terceiros, gestão de acessos, contingências, a fábrica de software responsável pelo desenvolvimento e sustentação, os requisitos de hardware, backup e rede. Este processo e documentação associada, é necessária para novos sistemas, sistemas existentes, assim como novas funcionalidades ou módulos que serão adicionados.

Os sistemas devem contemplar os aspectos mandatórios da Política de Senha Global da ICTSI (ICTSI Password Policy) e da Política Global de Controle de Acesso da ICTSI (Access Control Policy).

Este documento dará subsídios para entender o impacto do sistema no ecossistema de infraestrutura e sistemas da ICTSI, gestão de capacidade de infraestrutura e rede, visando garantir estabilidade, resiliência e prontidão, inclusive em situações adversas e de desastre e recuperação.

3.3 APROVAÇÃO

Todo investimento em construção, contratação de sistemas ou componentes de sistema, assim como a adoção de componentes "free" ou open source de sistemas devem ser submetidos para o **Comitê de Governança de Sistemas**, formado por:

- **Gerente de TI**
- **Coordenador de Sistemas**
- **Coordenador de Infraestrutura**

Para iniciar o processo, deve ser aberto um chamado no Jira (System Governance) com pelo menos 72 horas de antecedência da reunião semanal do Comitê de Governança de Sistemas. Para situações emergenciais, submeter com 24hs de antecedência. Na abertura, já deve ser submetido as documentações dos itens 3.1 e 3.2 que são obrigatórias.

Caso existam custos associados, a Gerência de TI vai buscar aprovação orçamentária/financeira da Diretoria e abertura de Ordens Internas de CAPEX ou OPEX junto à Equipe de Planejamento Financeiro.

Se o projeto não for priorizado para execução no mesmo ano, ele poderá ser incluído na proposta orçamentária para o ano seguinte pela área de Ti junto ao Planejamento Financeiro e Diretoria.

Caso seja necessário assinar propostas e contratos de Software e hardware, a Gerência de Ti vai liderar do processo de revisão contratual e coleta de assinaturas junto ao jurídico, abertura de requisição de compra e pedido no ERP.

3.4 DESENVOLVIMENTO / TESTES

O ciclo de desenvolvimento deve conter um cronograma de atividade e fases mapeados de entrega, seguido de ciclos de desenvolvimento em ambiente apropriado e previamente acordado com a Equipe de TI para testes, versionamento de código fonte no versionador centralizado oficial da ICTSI, com coleta de evidências para submissão ao processo de Gestão de Mudança via chamado no Jira, para que a mudança seja aplicada em ambiente de homologação.

Na fase de homologação, os usuários devem ser convidados a executar um roteiro de testes previamente definido no ambiente de homologação (QA) chamado de User Acceptance Testing (UAT), em um cenário muito próximo do esperado de acontecer em produção.

Este roteiro deve conter os cenários de testes, a distribuição das atividades entre os usuários envolvidos nos testes e os resultados esperados, e toda a evidência de testes deve ser preservada, seja ela positiva ou não. Os cenários reprovados devem ser revistos pela fábrica de software responsável a fim de disponibilizar nova versão para testes.

Concluído o ciclo de testes, deve ser realizado o versionamento de código fonte no versionador centralizado oficial da ICTSI.

Nesta etapa, a Fábrica de Software deve entregar a documentação do **“As built”**, trazendo todas as atualizações funcionais e técnicas realizadas de fato, em relação aos documentos entregues referentes ao “As is” e “To be” (documento de Escopo e Arquitetura) previamente entregues. Para atender à Lei Geral de proteção de Dados (LGPD), neste documento deve conter a lista completa de campos que podem conter dados pessoais, dados pessoais sensíveis, qual a base legal de tratamento do dado, política de retenção do dado, identificar se poderá haver dados de menores de idade, especificar em qual País os dados são tratados/armazenados e com quais

parceiros externos com os quais eles poderão ser compartilhados ou acessíveis. Para fins de LGPD, “tratamento de dados” significa qualquer ação de coleta, acesso, manipulação, armazenagem, alteração, correção, exclusão do dado.

Também deverá ser entregue o **Plano de Manutenção e Suporte da Aplicação**, que deverá conter:

- Identificação das Equipes de Suporte Nível 1 e Nível 2, horário de atendimento baseado na criticidade da aplicação, plantonista para acionamento após o horário de atendimento e escalação. O canal oficial do grupo ICTSI para chamados para Sistemas é o Jira.
- Definição de SLA de atendimento de incidente e solicitações de catálogo de serviço para configuração no Jira.
- Plano de gestão de acessos à Aplicação, definição de perfis caso aplicável.
- Plano regular de arquivamento e expurgo de dados.
- Gestão de dados pessoais conforme política de LGPD.
- Expectativa de crescimento de usuários e dados para os próximos 5 anos para adequação da infraestrutura.
- Reavaliação anual do Plano de Manutenção e Suporte da Aplicação, com análise da tecnologia empregada para análise de obsolescência e necessidade de evolução tecnológica.

A Equipe de Ti da ICTSI poderá, a qualquer momento, mesmo sem aviso prévio, executar análise de risco de cibersegurança da aplicação e trazer recomendações obrigatórias para adequação

Após a conclusão das etapas acima citadas, as evidências e as documentações devem ser submetidas ao processo de Gestão de Mudança via chamado no Jira, para que a mudança seja aplicada em ambiente de produção. Todas as atividades prévias para a mudança devem ser previamente mapeadas, sejam elas executadas pela Equipe de Ti ou a Fábrica de Software.

Não é permitido adicionar sistemas, novos módulos ou funcionalidades ou infraestrutura no ambiente de Tecnologia da ICTSI sem a anuência do Comitê de Governança de Sistemas, e não seguindo os passos descritos nesta política, sob o risco de pôr em risco a estabilidade da operação e a continuidade do negócio.

Para sistemas comerciais de terceiros, dependendo da extensão do sistema, pode ser avaliado realização de um processo simplificado (a ser avaliado) com uso de uma prova de conceito (POC) antes da contratação para execução de ciclo de testes.

3.5 IMPLANTAÇÃO / PÓS-GO-LIVE

Após a implantação do novo sistema, a Fábrica de Software deverá priorizar acompanhar ativamente junto a Equipe de TI pelo período assistido de 60 dias corridos, onde deve ser priorizado a resolução de quaisquer incidentes itens de alto impacto e/ou criticidade que possar aparecer, independentemente de sua natureza.

A Equipe de Ti da ICTSI poderá, a qualquer momento, mesmo sem aviso prévio, executar análise de risco de cibersegurança da aplicação e trazer recomendações obrigatórias para adequação no prazo limite de 14 dias corridos, conforme nível de serviço (SLA) definido pela Equipe Global de Cibersegurança.

O desempenho do sistema (tempo de resposta), desempenho das integrações com outros sistemas de produção, uso excessivo de recursos de infraestrutura e rede será avaliado e pode gerar ações de adequação.

Qualquer alteração nos parâmetros do **Plano de Manutenção e Suporte da Aplicação** deverá ser comunicado à Equipe de Ti com antecedência de 30 dias.

Qualquer sistema que apresente risco de cibersegurança, risco de estabilidade da produção ou de continuidade do negócio sem que as ações de correção apontadas sejam corrigidas em tempo hábil pela Fábrica de Software responsável, poderá o sistema ser sumariamente descontinuado ou substituído por outra solução definida pela Equipe de Ti.

A Equipe de TI é responsável pela estabilidade dos sistemas e dos ambientes de infraestrutura da ICTSI, enquanto a segurança da informação é de responsabilidade de todos, cada um dentro de suas responsabilidades.

Serão realizadas por parte da Equipe de Ti, aferições, auditorias e acompanhamento, a qualquer momento e sem aviso prévio, sobre qualquer um dos itens contemplados por esta política, de forma a identificar não conformidades que resultarão em uma atividade para a área contratante do software ou à Fábrica de Software para regularização em prazo de 14 dias.

4. RESPONSABILIDADES

- **Diretoria Executiva:** Aprovar e garantir a implementação da política.
- **Comitê de Governança de Sistemas:** Implementar e monitorar o cumprimento das diretrizes.

- **Gestão da área de negócio:** Seguir a política de Governança de Sistemas, cadastrar e regularizar softwares existentes e comunicar necessidades de tecnologia ou software para avaliação, aprovação e o desenvolvimento/contratação de sistemas de TI.
- **Fábricas de Software:** Seguir a política de Governança de Sistemas, cadastrar e regularizar softwares existentes.
- **Usuários:** Cumprir as normas estabelecidas, presar pela segurança da informação e relatar incidentes de segurança;

5. DIRETRIZES GERAIS

• GESTÃO DE ACESSOS

O acesso a sistemas deve ser controlado e restrito com base no princípio do privilégio mínimo. A autenticação multifator deve ser aplicada sempre que aplicável.

PLTI-013 - POLITICAS DE REVISÃO CONTROLE DE ACESSOS TI V2.PDF

• POLÍTICAS GLOBAIS DE TECNOLOGIA DE INFORMAÇÃO DO GRUPO ICTI

Todos os sistemas devem estar aderentes às políticas globais de Tecnologia da Informação do grupo ICTSI, disponíveis no link abaixo:

Global Corporate Hub - Global Corporate Information Technology - All Documents

Regularmente a equipe global executa auditorias dos cumprimentos das diretrizes de tecnologia e a adequação é mandatória.

• GESTÃO DE MUDANÇAS

Toda modificação nos sistemas deve seguir um processo formal de gestão de mudanças. Deve haver registros e aprovação formal para alterações programadas, pré-aprovadas e críticas.

- **CONTINUIDADE DE NEGÓCIOS**

Planos de continuidade devem ser desenvolvidos, testados e atualizados periodicamente. Backups devem ser realizados regularmente e armazenados de forma segura.

- **CAPACITAÇÃO E CONSCIENTIZAÇÃO**

Todos os colaboradores que são parte do suporte devem receber treinamentos periódicos sobre a aplicação e sobre boas práticas de segurança e governança de TI.

- **ACESSO JIRA PARA GOVERNANÇA DE SISTEMS**

https://ictsi.atlassian.net/jira/core/projects/RITSG/form/109 - Cadastro de um sistema já existente (regularização).

https://ictsi.atlassian.net/jira/core/projects/RITSG/form/76 - Comitê de Sistemas, para submeter um novo sistema ou novo pedido de sistemas.

- **MONITORAMENTO E AUDITORIA**

Os sistemas devem ser monitorados continuamente para detectar atividades suspeitas. Auditorias periódicas devem ser conduzidas para avaliar a conformidade e segurança.

6. TERMOS UTILIZADOS

MFA: (Multi-Factor Authentication): É um método de segurança que exige que o usuário forneça duas ou mais formas de verificação. Múltiplo Fator de Autenticação.

ITIL: (Information Technology Infrastructure Library): Concentra-se nas melhores práticas para a gestão de serviços de TI, visando melhorar a qualidade e a eficiência dos serviços prestados.

COBIT: (Control Objectives for Information and Related Technologies): Oferece um modelo abrangente para o gerenciamento e a governança de TI, com foco no alinhamento dos objetivos de TI com os do negócio.

ISSO/IEC 27001: ISO/IEC 27001: Padrão internacional que especifica os requisitos para estabelecer, implementar, manter e melhorar um sistema de gestão de segurança da informação.

LGPD: Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados, que dispõe sobre a proteção de dados pessoais e altera o Marco Civil da Internet.

7. DOCUMENTOS RELACIONADOS

- **Documento de Escopo (As is / To be)**
- **Arquiterura de Ti (To be)**
- **Roteiro de Testes**
- **Evidências de Testes**
- **As Built**
- **Plano de Manutenção e Suporte da Aplicação**
- **ICTSI Password Policy**
- **Access Control Policy**
- **PLTI-013 - POLITICAS DE REVISÃO_CONTROLE DE ACESSOS_TI_V2.pdf**
- **Global Corporate Hub - Global Corporate Information Technology - All Documents**
- **PLTI-009 - Política de Produção e Provisão de Serviço_V4.docx**

8. VIGÊNCIA

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado.

9. REVISÃO

A gestão de governança da Rio Brasil Terminal, iTracker e CLIA Pouso Alegre deverá avaliar a necessidade de revisar esta política, ao menos uma vez por ano, expressando seu entendimento e sugestões nas reuniões das áreas envolvidas.

10. ANEXOS

- **Documento de Escopo (As is / To be)**
- **Arquiterura de Ti (To be)**
- **Roteiro de Testes**
- **Evidências de Testes**
- **As Built**
- **Plano de Manutenção e Suporte da Aplicação**
- **ICTSI Password Policy**
- **Access Control Policy**
- **PLTI-013 - POLITICAS DE REVISÃO_CONTROLE DE ACESSOS_TI_V2.pdf**
- **Global Corporate Hub - Global Corporate Information Technology - All Documents**

11. HISTÓRICO DE REVISÃO

Revisão	Vigência	Motivo da revisão

RIO BRASIL TERMINAL
An ICTSI Group Company

Código:	PL TI - 012
Área:	Tecnologia da Informação
Revisão:	2
Data Revisão:	19/04/2025

00	02/04/2025	Emissão do documento.
01	11/04/2025	Cadastro dos endereços do Jira
02	19/04/2025	Inclusão do fluxo