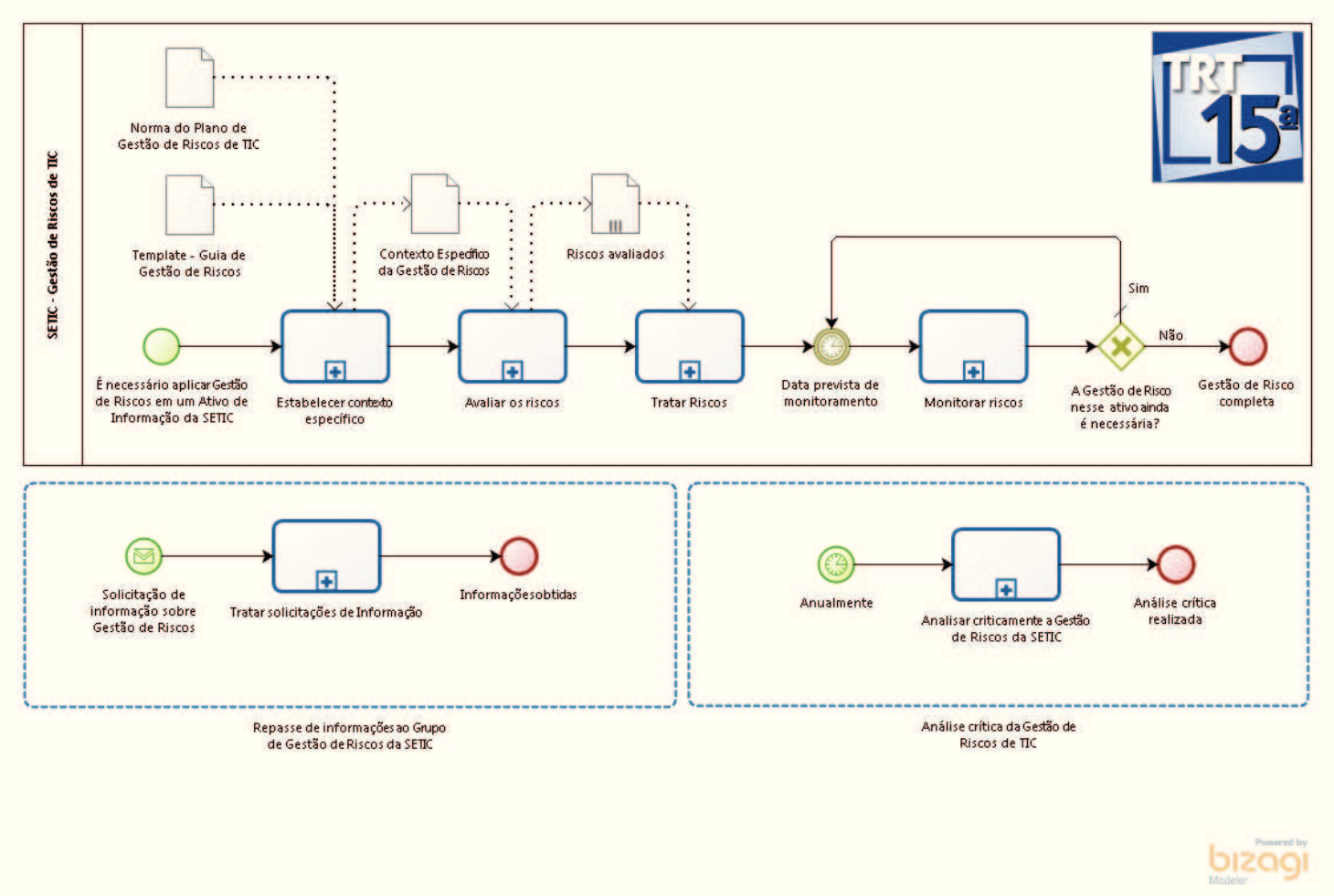
Otimização do Processo

Gestão de Riscos de TIC

Versão 1.0

CGTIC / SETIC / TRT15


SETIC - Gestão de Riscos de TIC
Norma do Plano de Gestão de Riscos de TIC
Template - Guia de Gestão de Riscos
Contexto Específico da Gestão de Riscos
Riscos avaliados
É necessário aplicar Gestão de Riscos em um Ativo de Informação da SETIC
Estabelecer contexto específico
Avaliar os riscos
Tratar Riscos
Data prevista de monitoramento
Monitorar riscos
A Gestão de Risco nesse ativo ainda é necessária?
Sim
Não
Gestão de Risco completa
Solicitação de informação sobre Gestão de Riscos
Tratar solicitações de Informação
Informações obtidas
Repasse de informações ao Grupo de Gestão de Riscos da SETIC
Anualmente
Analisar criticamente a Gestão de Riscos da SETIC
Análise crítica realizada
Análise crítica da Gestão de Riscos de TIC
Powered by bizagi Modeler

Versão: 1.0

S E T I C - G E S T Ã O D E R I S C O S D E T I C

ELEMENTOS DO PROCESSO

Estabelecer contexto específico

Objetivo

Definir o propósito do Ativo de Informação, as necessidades/expectativas das partes interessadas e as questões internas e externas que afetam a capacidade da Instituição para alcançar os resultados pretendidos.

Avaliar os riscos

Objetivo

Gerar uma lista de riscos categorizados quanto ao atendimento dos Critérios de Riscos da Instituição.

Tratar Riscos

Objetivo

Elaborar e executar um **Plano de Ações de Tratamento de Riscos** que conduza o **Nível de Risco** do **Ativo de Informação** para um estado aceitável de acordo com o **Apetite de Risco** da Instituição.

Monitorar riscos

Objetivo

Revisar o estado dos **Riscos** e aprimorar o **Plano de Tratamento de Riscos** para garantir a manutenção do **Nível de Risco** do **Ativo de Informação** em um estado aceitável de acordo com o **Apetite de Risco** da Instituição.

Contexto Específico da Gestão de Riscos

Aba "Contexto" do "Guia de Gestão de Riscos" preenchido.

Riscos avaliados

Lista de riscos categorizados quanto ao atendimento dos Critérios de Riscos da SETIC.

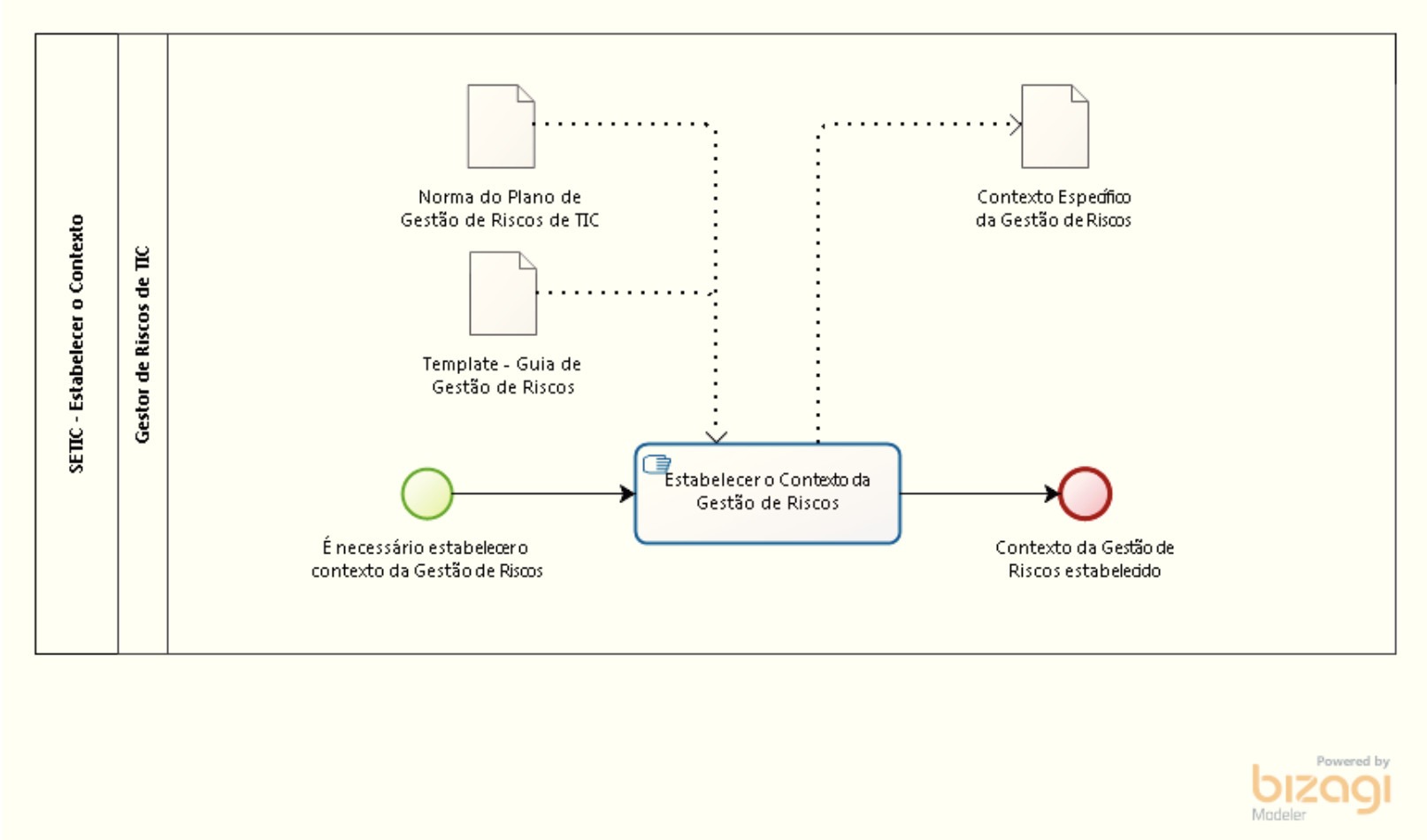
Template - Guia de Gestão de Riscos

Documento da Metodologia de Gestão de Riscos que guia o Gestor de Riscos na execução de atividades necessárias para a realização de uma Gestão de Riscos eficaz.

Norma do Plano de Gestão de Riscos de TIC

Esta publicação tem por objetivo detalhar o processo de Gestão de Riscos a fim de auxiliar sua implantação.

ESTABELECER CONTEXTO ESPECÍFICO



Versão: 1.0

S E T I C - E S T A B E L E C E R O C O N T E X T O

Executantes

Gestor de Riscos de TIC

ELEMENTOS DO PROCESSO

Estabelecer o Contexto da Gestão de Riscos

Objetivo

Esta atividade visa definir o propósito do Ativo de Informação, as necessidades/expectativas das partes interessadas e as questões internas e externas que afetam a capacidade da Instituição para alcançar os resultados pretendidos pelo Ativo de Informação.

Detalhamento

Em reunião entre o Gestor de Riscos e Partes Interessadas, é necessário definir todas as informações solicitadas na aba "Contexto" do "Guia de Gestão de Riscos".

Contexto Específico da Gestão de Riscos

Aba "Contexto" do "Guia de Gestão de Riscos" preenchido.

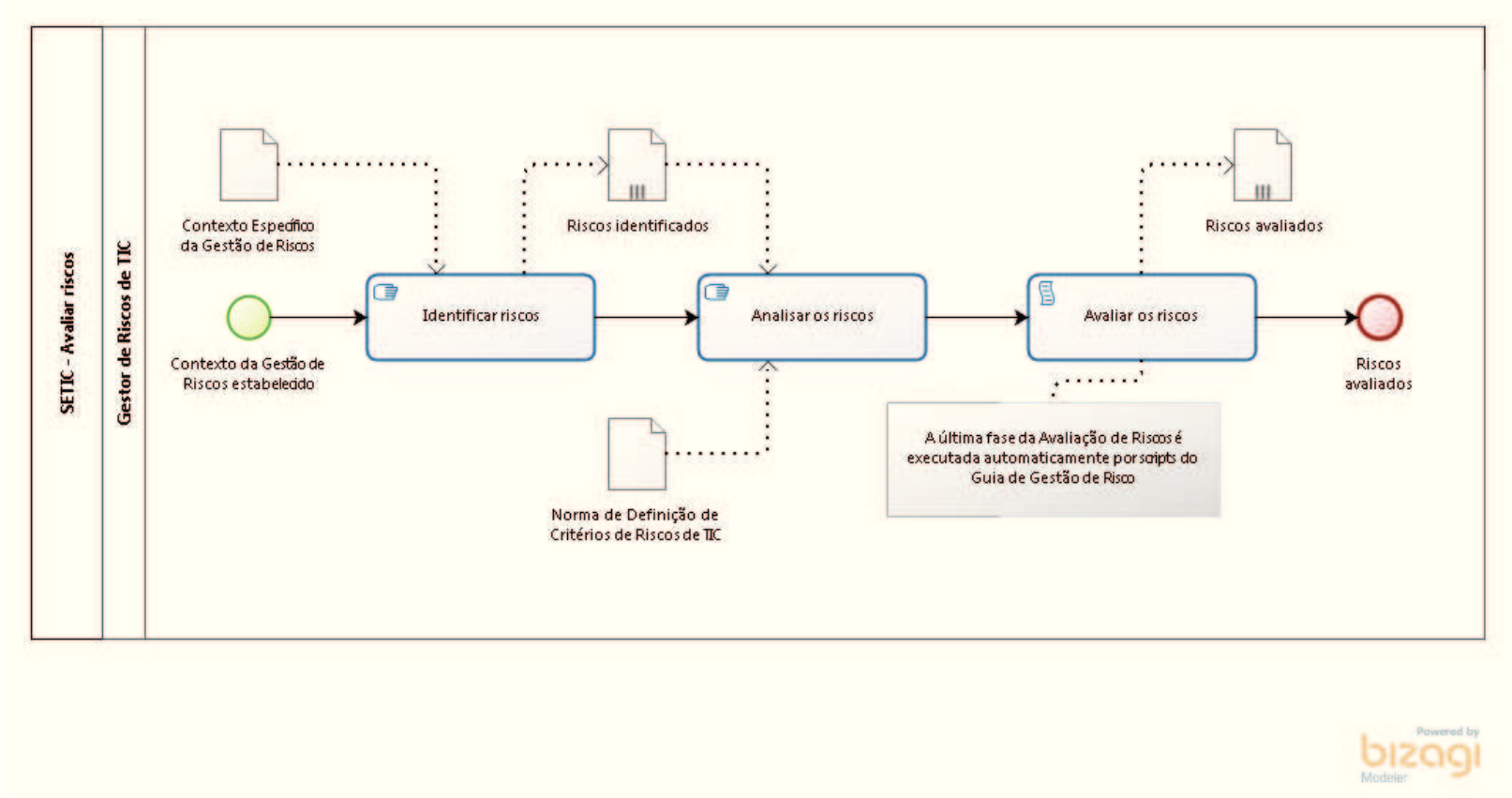
Norma do Plano de Gestão de Riscos de TIC

Esta publicação tem por objetivo detalhar o processo de Gestão de Riscos a fim de auxiliar sua implantação.

Template - Guia de Gestão de Riscos

Documento da Metodologia de Gestão de Riscos que guia o Gestor de Riscos na execução de atividades necessárias para a realização de uma Gestão de Riscos eficaz.

AVALIAR OS RISCOS



Versão: 1.0

S E T I C - A V A L I A R R I S C O S

Executantes

Gestor de Riscos de TIC

ELEMENTOS DO PROCESSO

Identificar riscos

Objetivo

Consiste na busca, reconhecimento e descrição de riscos, mediante a identificação das fontes de risco, eventos, suas causas e suas consequências potenciais.

Detalhamento

O propósito da identificação de riscos é determinar eventos que possam causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer.

Convém que a identificação de riscos inclua os riscos cujas fontes estejam ou não sob controle da organização, mesmo que a fonte ou a causa dos riscos não seja evidente.

Em termos práticos, é necessário preencher as colunas referentes à Identificação de Riscos na aba "Avaliação de Riscos" do "Guia de Gestão de Riscos".

Existem diversas ferramentas que podem auxiliar o Gestor de Riscos na identificação de riscos. A norma ABNT NBR ISO27005 apresenta que a Identificação de Riscos pode ser dividida em 5 passos:

- Identificação de Ativos.
- Identificação de Ameaças.
- Identificação de Controles.
- Identificação de Vulnerabilidades.
- Identificação das Consequências.
-

A publicação PMBok 5ª Ed. apresenta as seguintes ferramentas para Identificação de Riscos:

- Revisões de documentação existente.
- Técnicas de coleta de informações.
- Análise de listas de verificação.
- Análise de premissas.
- Técnicas de diagramas.
- Análise de forças, fraquezas, oportunidades e ameaças (SWOT).
- Opinião especializada.

Quaisquer mecanismos que permitam a identificação de riscos é válido para essa atividade.

ATENÇÃO: É importante não gastar tempo agora com a análise sobre a probabilidade ou impacto dos riscos identificados. O importante mesmo é gerar uma lista abrangente das possibilidades de riscos.

Analisar os riscos

Objetivo

Para cada risco identificado é necessário compreender a natureza do risco e determinar seu nível de risco residual.

Detalhamento

Em termos práticos, é necessário preencher as colunas referentes à Análise de Riscos na aba "Avaliação de Riscos" do "Guia de Gestão de Riscos".

O primeiro passo dessa atividade é **Avaliar o Risco Inerente**, que deve determinar o nível do risco desconsiderando quaisquer controles já implantados. Para cada risco identificado é necessário registrar seu impacto com base na **Escala de Impacto** e registrar sua probabilidade com base na **Escala de Probabilidade**.

O Segundo passo é descrever os controles relevantes para cada risco identificado e que já estão implantados. A eficácia dos controles será determinada pela **Escala de Eficácia de Controles**.

Ao final desses passos, para cada risco identificado, será calculado automaticamente seu **Risco Residual**.

Avaliar os riscos

Objetivo

Comparar os **Riscos Residuais** com os **Critérios de Riscos** para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.

Detalhamento

O esforço executado nesta atividade é realizado automaticamente por scripts do **Guia de Gestão de Risco**.

Riscos identificados

Lista de riscos identificados e registrados na Aba "Avaliação de Riscos" do "Guia de Gestão de Riscos".

Norma de Definição de Critérios de Riscos de TIC

Termos de referência contra os quais a significância de um risco é avaliada. Dentro deste documento estão descritas, entre outras:

- A Escala de Probabilidade.
- A Escala de Impactos.
- A Escala de Eficácia de Controles.

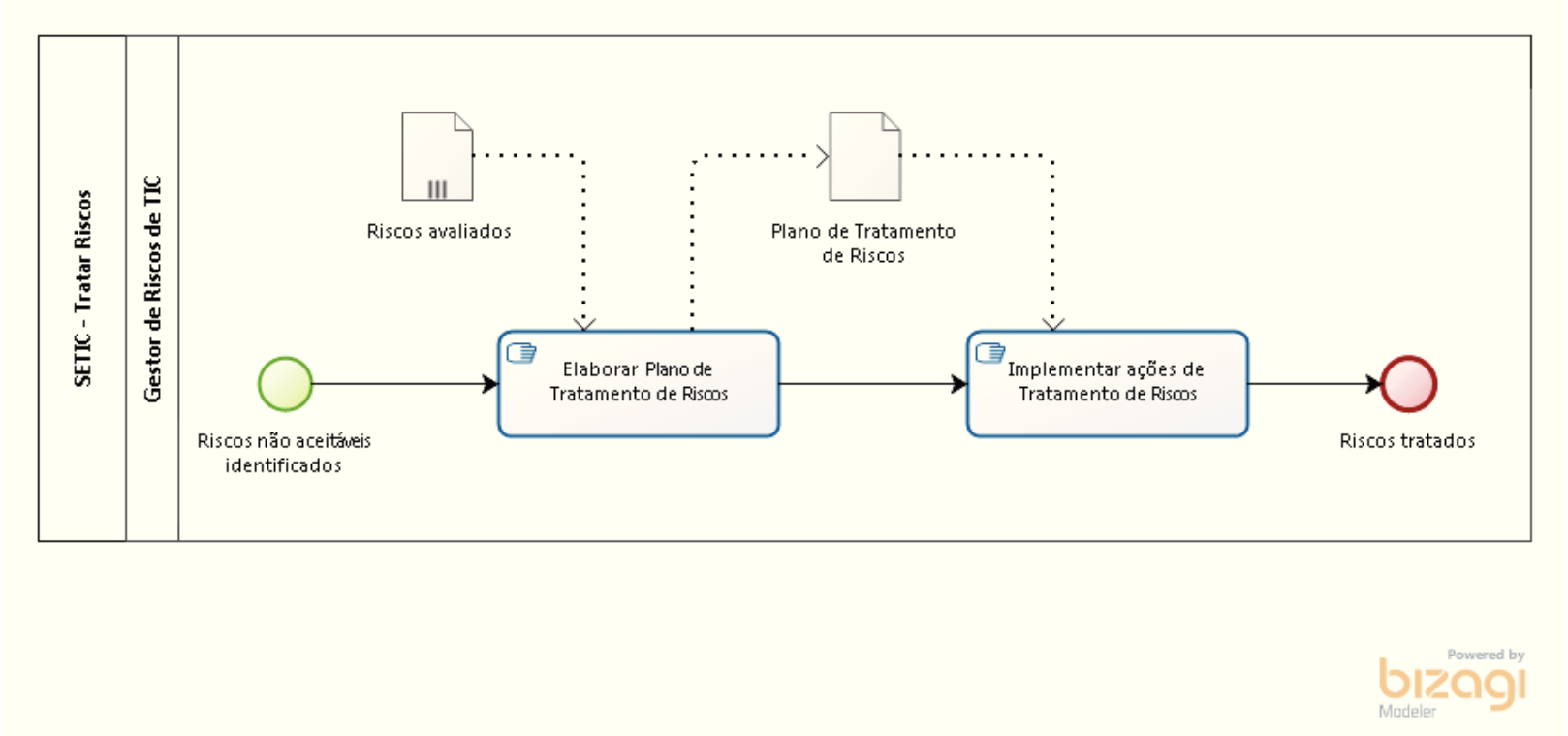
Riscos avaliados

Lista de riscos categorizados quanto ao atendimento dos **Critérios de Riscos** da Instituição.

Contexto Específico da Gestão de Riscos

Aba "Contexto" do "Guia de Gestão de Riscos" preenchido.

TRATAR RISCOS



Versão: 1.0

S E T I C - T R A T A R R I S C O S

Executantes

Gestor de Riscos de TIC

ELEMENTOS DO PROCESSO

Elaborar Plano de Tratamento de Riscos

Objetivo

Elaborar um **Plano de Ações de Tratamento de Riscos** que conduza o **Nível de Risco** do **Ativo de Informação** para um estado aceitável de acordo com o **Apetite de Risco** da Instituição.

Implementar ações de Tratamento de Riscos

Objetivo

Executar o **Plano de Ações de Tratamento de Riscos** elaborado anteriormente, visando garantir que ele conduza o **Nível de Risco** do **Ativo de Informação** para um estado aceitável de acordo com o **Apetite de Risco** da Instituição.

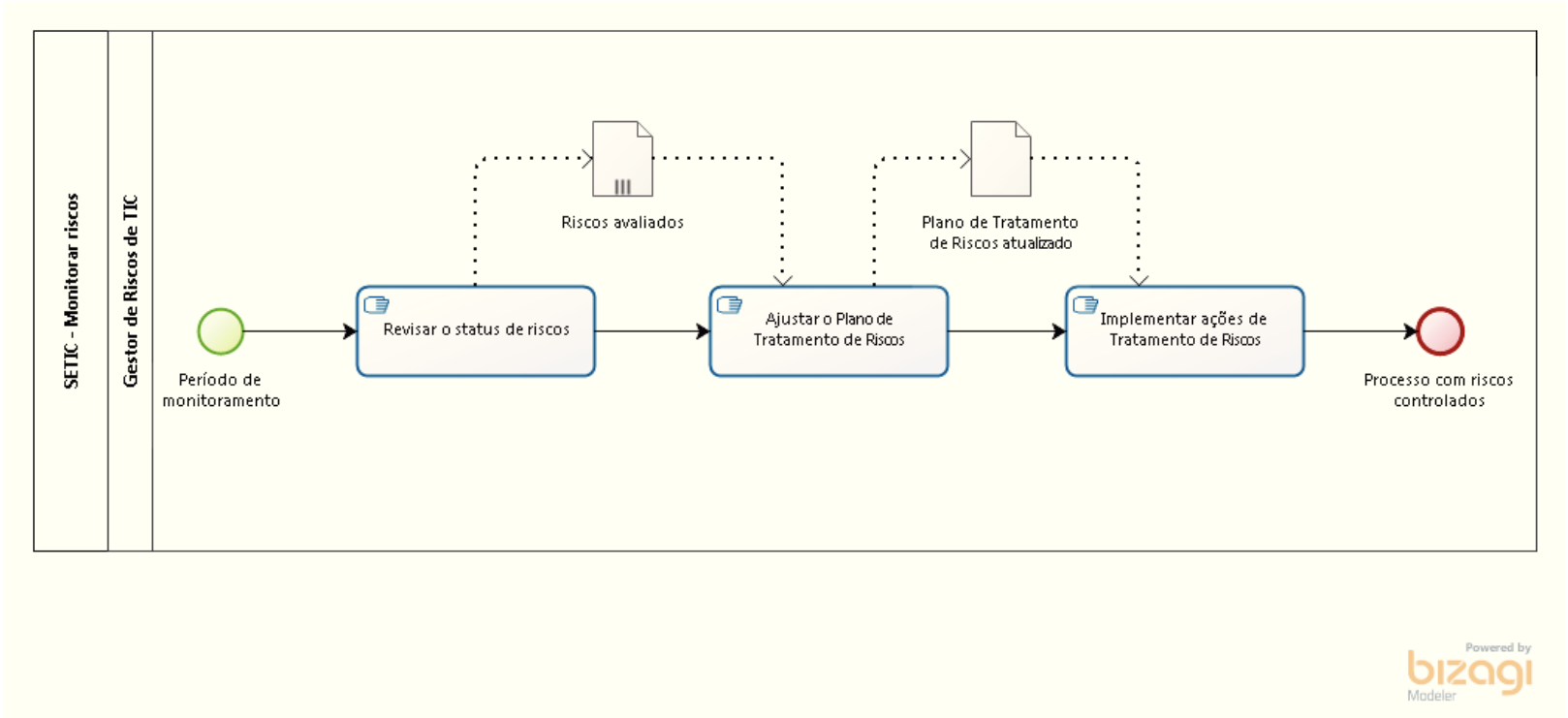
Plano de Tratamento de Riscos

Conjunto de ações de Tratamento de Risco que conduzirão o **Nível de Risco** do **Ativo de Informação** para um estado aceitável de acordo com o **Apetite de Risco** da Instituição.

Riscos avaliados

Lista de riscos categorizados quanto ao atendimento dos **Critérios de Riscos** da Instituição.

MONITORAR RISCOS



Versão: 1.0

S E T I C - M O N I T O R A R R I S C O S

Executantes

Gestor de Riscos de TIC

ELEMENTOS DO PROCESSO

Revisar o status de riscos

Objetivo

Verificar se existe alguma mudança na exposição de riscos.

Detalhamento

Quanto à Identificação de riscos, é necessário:

- Verificar se os riscos existentes ainda estão ativos.
- Remover do Guia de Gestão de Riscos aqueles que estão inativos.
- Identificar novos riscos e registrá-los no Guia de Gestão de Riscos.

Quanto à Análise de riscos, é necessário:

- Verificar se o Nível de Riscos dos riscos existentes é coerente.
- Verificar se a eficácia dos controles estabelecidos é coerente.
- Realizar a Análise de Riscos para os novos riscos.
- Garantir que o Guia de Gestão de Riscos está plenamente preenchido e representa o momento atual.

Os ajustes devem ser realizados diretamente na aba "Avaliação de Riscos" do Guia de Gestão de Riscos.

Ajustar o Plano de Tratamento de Riscos

Objetivo

Ajustar o **Plano de Ações de Tratamento de Riscos** que mantenha o **Nível de Risco** do **Ativo de Informação** em um estado aceitável de acordo com o **Apetite de Risco** da Instituição.

Detalhamento
Um ponto de atenção importante é garantir que sejam registradas ações de remoção de controles de riscos quando esses forem classificados como inativos.

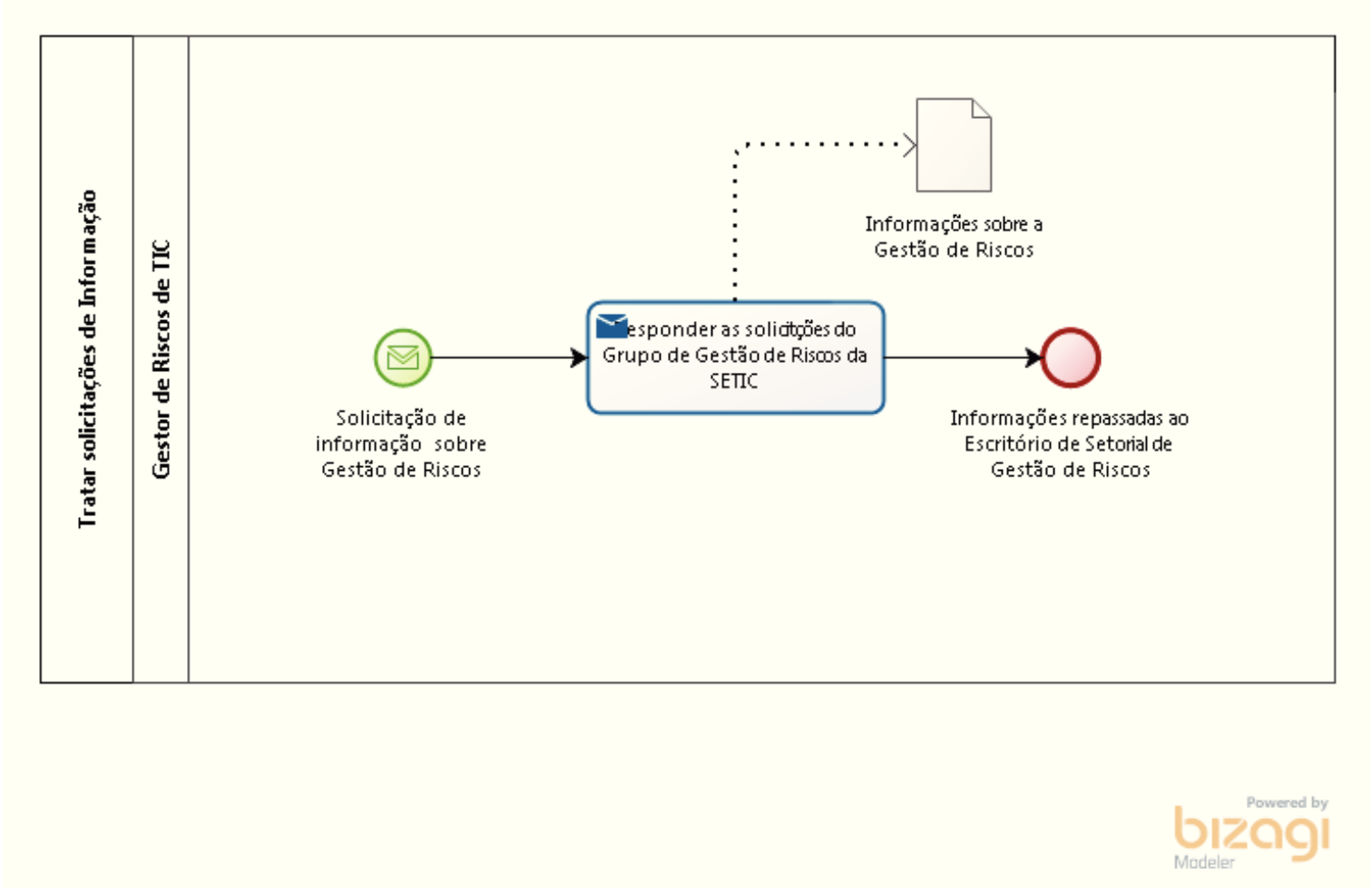
Implementar ações de Tratamento de Riscos

Objetivo
Executar o **Plano de Ações de Tratamento de Riscos** elaborado anteriormente, visando garantir que ele que conduza o **Nível de Risco** do **Ativo de Informação** para um estado aceitável de acordo com o **Apetite de Risco** da Instituição.

Plano de Tratamento de Riscos atualizado
Atualização do conjunto de ações de Tratamento de Risco que manterão o **Nível de Risco** do **Ativo de Informação** em um estado aceitável de acordo com o **Apetite de Risco** da Instituição.

Riscos avaliados
Lista de riscos categorizados quanto ao atendimento dos Critérios de Riscos da SETIC.

TRATAR SOLICITAÇÕES DE INFORMAÇÃO



Versão: 1.0

T R A T A R S O L I C I T A Ç Õ E S D E I N F O R M A Ç Ã O

Executantes

Gestor de Riscos de TIC

ELEMENTOS DO PROCESSO

Responder as solicitações do Grupo de Gestão de Riscos da SETIC

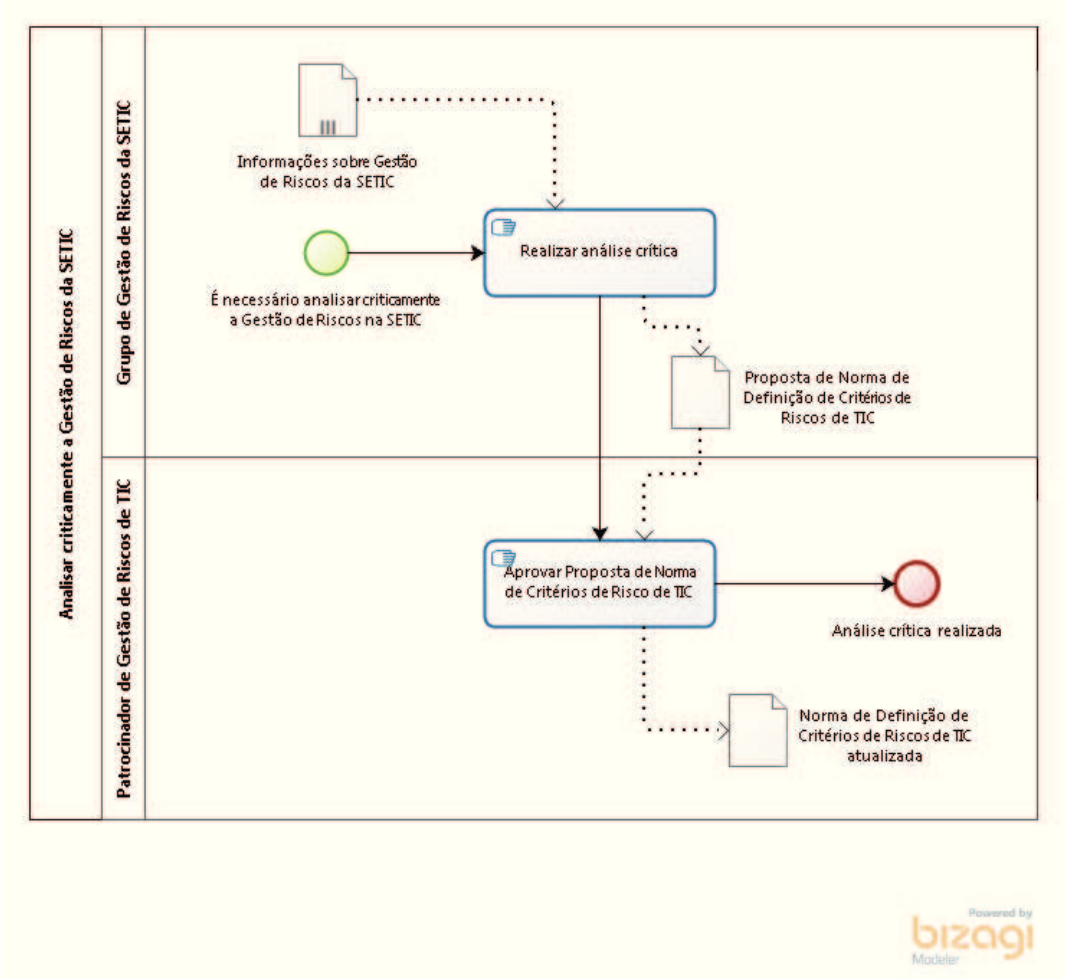
Objetivo

Atender às requisições de informações do Grupo de Gestão de Riscos da SETIC com o objetivo de apoiar as atividades de Gestão de Riscos, em especial, a Análise Crítica da Gestão de Riscos na SETIC.

Informações sobre a Gestão de Riscos

Informações sobre a execução da Gestão de Riscos.

ANALISAR CRITICAMENTE A GESTÃO DE RISCOS DA SETIC



Versão: 1.0

A N A L I S A R C R I T I C A M E N T E A G E S T Ã O D E R I S C O S D A S E T I C

Executantes

Grupo de Gestão de Riscos da SETIC

ELEMENTOS DO PROCESSO

Realizar análise crítica

Objetivo

Garantir alinhamento contínuo da Gestão de Riscos com os objetivos de negócios da organização e com os Critérios de Riscos.

Detalhamento

Deve-se revisar o estado da Gestão de Riscos de TIC e, com foco em manter o alinhamento contínuo da Gestão de Riscos com os objetivos de negócios da organização, deve-se atualizar a **Norma de Definição de Critérios de Riscos de TIC**.

Informações sobre Gestão de Riscos da SETIC

Informações coletadas das diversas Gestões de Riscos que são/foram executadas na SETIC.

Proposta de Norma de Definição de Critérios de Riscos de TIC

Proposta de nova versão da **Norma de Definição de Critérios de Riscos de TIC** que foi atualizada como resposta à análise crítica realizada sobre a Gestão de Riscos de TIC.

Norma de Definição de Critérios de Riscos de TIC atualizada

Nova versão da **Norma de Definição de Critérios de Riscos de TIC** que foi atualizada como resposta à análise crítica realizada sobre a Gestão de Riscos de TIC.

Aprovar Proposta de Norma de Critérios de Risco de TIC

Objetivo

Revisar e aprovar a proposta de nova versão da **Norma de Definição de Critérios de Riscos de TIC** que foi atualizada como resposta à análise crítica realizada sobre a Gestão de Riscos de TIC.