Coordenadoria da TIC do TRT24

Processo Gerenciar Riscos de TIC

Aguardando aprovação

HISTÓRICO DO DOCUMENTO

Seq.	DATA	DESCRIÇÃO
01	11/03/2015	Desenho do processo
02	27/10/2015	Revisão dos indicadores
03	23/09/2016	Alinhamento ao COBIT 5.0
04	08/08/2017	Revisão do alinhamento ao COBIT 5.0 e ao indicador do PETIC
05	23/08/2018	Alinhamento à nova versão do processo Gerenciar Segurança da Informação

EQUIPE DE DOCUMENTAÇÃO

Seq.	Nome	Cargo
01	João Carlos Ferreira Filho	Chefe da Seção de Governança de TIC

Aguardando aprovação

Sumário

1 OBJETIVO 4

2 ABRANGÊNCIA 4

3 DEFINIÇÕES 4

4 PROCESSO GERENCIAR RISCOS DE TI 5

4.1 Papéis e responsabilidades 5
4.2 Fluxo do processo 6
4.2.1 Fluxo do processo Gerenciar Riscos de TIC 6
4.3 Descrição do processo 7
4.3.1 Descrição de processo Gerenciar Riscos de TIC 7

5 TABELA RACI 9

5.1 Processo Gerenciar Riscos de TIC 9

6 CONTROLES DO PROCESSO 10

6.1 Indicadores 10
6.2 Descrição dos indicadores 11

7 DIVULGAÇÃO DE RESULTADOS 14

8 ANEXO I – ÍNDICE DE AUDITORIAS 15

9 ANEXO II – ÍNDICE DE ATIVOS DE TI INCLUÍDOS NA ANÁLISE DE RISCOS (RISK PROFILE) 15

10 ANEXO III – ÍNDICE DE TRATAMENTO DE RISCOS 16

11 ANEXO IV - ÍNDICE DE RISCO DE ATIVOS 16

Aguardando aprovação

1 Objetivo

Atender às demandas de avaliação de riscos de ativos de TI, baseando-se no manual "Módulo Risk Manager – Software para Automação de GRC – Governança, Riscos e Compliance", na publicação "The Risk IT Practitioner Guide" (ISBN 978-1-60420-116-1), produzido pela Information Systems Audit and Control Association (ISACA), baixado do site http://www.colmich.edu.mx/computo/files/MAAGTIC/RiskIT_PG_30June2010_Research.pdf, em 04/03/2015 e na Norma ABNT NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação.

2 Abrangência

Coordenadoria de Tecnologia de Informação e Comunicações.

3 Definições

- **Ameaça:** ação de origem humana (intencional ou acidental) ou ambiental, que explora uma vulnerabilidade presente num ativo e provoca impactos na organização.
- **Ativo:** qualquer recurso que possui valor para a organização e cujo risco precisa ser controlado e gerenciado. Pode ser uma operação, uma atividade, um projeto, um programa, um serviço, um processo, um objetivo estratégico...
- **Controle**: políticas, práticas, procedimentos, estruturas organizacionais, dispositivos de hardware e funções de software, que visam eliminar vulnerabilidades ou minimizar os impactos causados por incidentes.
- **Impacto:** consequência sobre os ativos e negócios de uma organização, caso uma ameaça venha a se efetivar. Pode ser tangível (exemplo: perdas financeiras) ou intangíveis (exemplo: perda de credibilidade). Corresponde ao produto "S" (severidade) por "R" (relevância).
- **Incidente de segurança:** materialização de uma ameaça. Um incidente de segurança provoca danos a um ou mais ativos, além de impactos ao negócio.
- **Perfil de risco:** uma descrição geral dos riscos de TI (identificados) a que uma organização está exposta.
- **Probabilidade:** possibilidade de concretização de uma ameaça. Pode variar de 1-Muito baixa a 5-Muito alta.
- **PSR:** é uma indicação numérica do nível de vulnerabilidade relativo a um risco. Pode variar de 1 a 125 e é o resultado da multiplicação de três grandezas: Probabilidade; Severidade; e Relevância.
- **Relevância:** grau de importância do ativo para o negócio da organização. Pode variar de 1-Muito baixa a 5-Muito alta.
- **Risco:** é a combinação da probabilidade de que algum incidente ocorra e sua conseqüência.
- **Risco inerente:** é o nível de risco (PSR), sem levar em conta os controles aplicados ou poderiam ter sido aplicados pela organização.
- **Risco residual:** é o nível de risco (PSR) remanescente após a organização ter aplicado ações de controle do risco.
- **Severidade:** medida do grau em que um ativo será afetado, caso uma ameaça venha a se efetivar. Pode variar de 1-Muito baixa a 5-Muito alta
- **Vulnerabilidade:** fragilidade de um ativo que pode ser explorada por uma ameaça.

Aguardando aprovação

4 Processo Gerenciar Riscos de TI

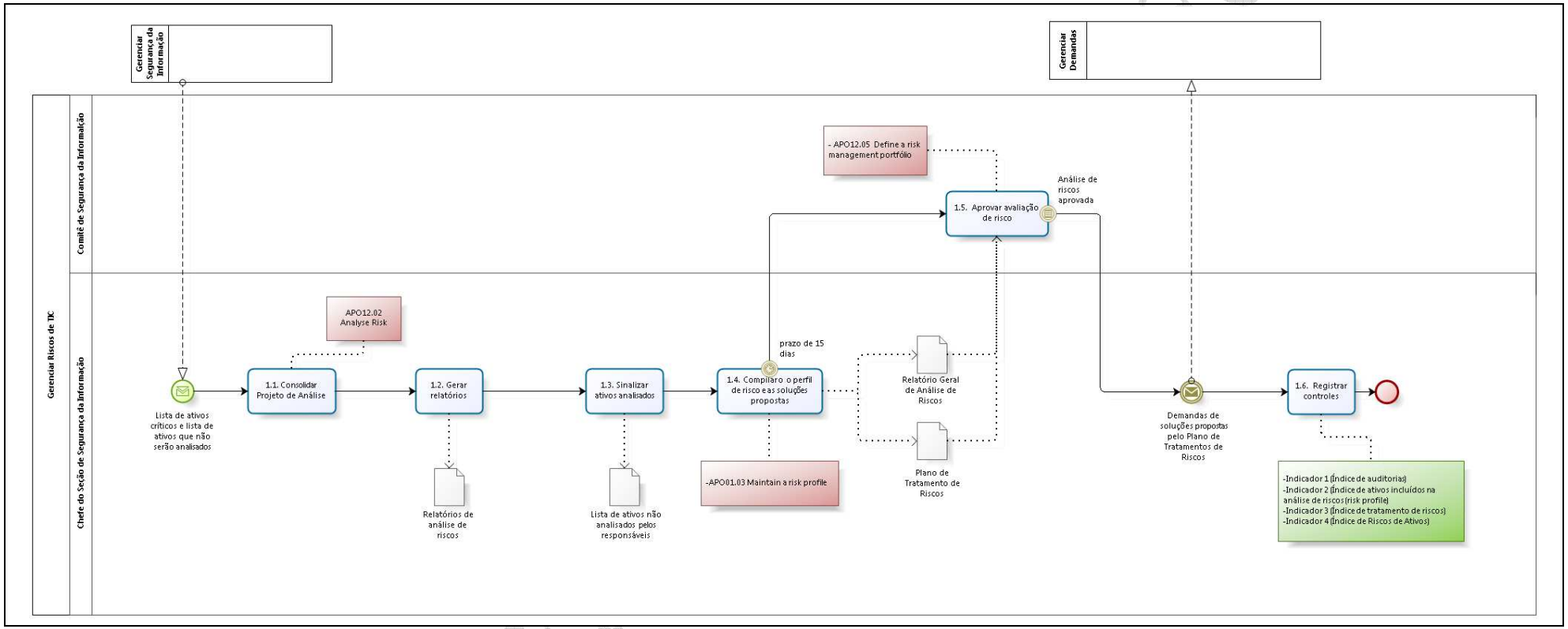
4.1 Papéis e responsabilidades

Papel	Responsabilidades	Responsável
Dono Processo	· Buscar a qualidade e eficiência gerais do processo · Assegurar que todos os envolvidos na execução do processo sejam informados das mudanças e suporte efetuados	Diretor(a) da Coordenadoria de Tecnologia da Informação e Comunicações
Gerente do Processo	· Busca a eficiência e a efetividade do processo · Produzir informações gerenciais (indicadores gerenciais) · Promover a execução das atividades do processo · Registrar os controles do processo · Manter o desenho e indicadores do processo atualizados, garantindo que estejam adequados aos propósitos da organização	Chefe da Seção de Segurança da Informação
Comitê Técnico de Segurança da Informação	· Aprovar o Relatório Geral de Análise de Riscos	Coordenador do Comitê Técnico de Segurança da Informação

Aguardando aprovação

4.2 Fluxo do processo

4.2.1 Fluxo do processo Gerenciar Riscos de TIC



Aguardando Aprovação

4.3 Descrição do processo

4.3.1 Descrição de processo Gerenciar Riscos de TIC

Id	Atividade	Objetivo	Responsável	Descrição
1.1	Consolidar análise de riscos	• Encerrar a fase de preenchimento de questionários	Chefe da Seção de Segurança da Informação	**Entradas:** todos os questionários preenchidos na base do Risk Manager, lista de ativos críticos e lista de ativos que não serão analisados
				Processamento: concluir projeto de análise, colocando-o na situação "fechada" no Risk Manager. Observe-se que nesse momento estaremos compilando as informações que embasarão as decisões relacionadas ao tratamento dos riscos de TIC. (COBIT 5, processo APO12, prática chave de gerenciamento APO12.02 Analyse risk.)
				Saídas: somatório dos valores PSR (Probabilidade/Severidade/Relevância) dos riscos de cada ativo
1.2	Gerar Relatórios	• Gerar relatórios da avaliação dos riscos do ativo	Chefe da Seção de Segurança da Informação	**Entradas:** projeto na situação “fechada”
				Processamento: gerar relatórios executivos, gerenciais e operacionais, que guiarão as ações de tratamento dos riscos.
				Saídas: relatórios de análise de riscos
1.3	Sinalizar ativos analisados	• Controlar a lista de ativos a serem avaliados	Chefe da Seção de Segurança da Informação	**Entradas:** relatório de análise de riscos
				Processamento: a partir da análise executada relacionar os ativos que não foram analisados pelos respectivos responsáveis.
				Saídas: lista de ativos não analisados pelos responsáveis
1.4	Compilar o perfil de risco e as soluções propostas	• Preparar resposta à demanda de avaliação de risco	Chefe da Seção de Segurança da Informação	**Entradas:** relatórios de análise de riscos
				Processamento: compilar os documentos de saída da(s) avaliação(ões) de risco feita(s). O chefe do SSI deve apresentar recomendações explícitas quanto às soluções de segurança a serem implementadas.

Aguardando aprovação

Id	Atividade	Objetivo	Responsável	Descrição
				Observe-se que esse documento corresponde a um inventário atualizado dos riscos conhecidos, com seus respectivos potenciais de dano e as respostas propostas. (COBIT 5, processo APO12, prática chave de gerenciamento APO12.03 Maintain a Risk Profile). **Saídas:** Relatório Geral de Análise de Riscos e Plano de Tratamento de Riscos
1.5	Aprovar avaliação de risco	• Validar análise de risco	Coordenador do Comitê de Segurança da Informação	**Entradas:** Relatório Geral de Análise de Riscos **Processamento**: Avaliar a análise de riscos realizada e aprovar ou não, notadamente a relação entre as recomendações oriundas do Risk Manager e as soluções de segurança recomendadas pelo SSI. Observe-se que essa atividade equivale à definição de um portfólio de ações/projetos de redução dos riscos de TIC a um nível aceitável para o TRT. (COBIT 5, processo APO12, prática chave de gerenciamento APO12.05 Define a risk management action portfolio.) **Saídas:** relatório de análise de riscos validado
1.6	Registrar Controles	• Controlar a execução do processo	Chefe da Seção de Segurança da Informação	**Entradas:** relatórios produzidos durante a análise de riscos **Processamento**: • Registrar Indicadores 1,2,3 e 4 conforme as planilhas dos ANEXOS I, II, III e IV, respectivamente **Saídas:** dados dos indicadores registrados nas planilhas

Aguardando aprovação

5 Tabela RACI

5.1 Processo Gerenciar Riscos de TIC

	Atividade	Comitê de Segurança da Informação	Chefe da Seção de Segurança da Informação
1.1	Consolidar Projeto de Análise		**R**
1.2	Gerar Relatórios		**R**
1.3	Sinalizar ativos analisados		**R**
1.4	Compilar o perfil de risco e as soluções propostas		**R**
1.5	Aprovar avaliação de risco	**R**	**C**
1.6	Registrar Controles		**R**

Legenda: Responsável (R), Consultado (C), Informado (I)

Aguardando aprovação

6 Controles do processo

O controle do processo é realizado por meio de indicadores obtidos através da coleta de dados relacionados ao processo, sendo que, quando os resultados esperados não forem alcançados, devem ser estabelecidas ações para tratamento dos desvios encontrados.

6.1 Indicadores

Id	Objetivo do controle	Origem	Indicador
1	Os riscos de TI são identificados, analisados, gerenciados e reportados	COBIT 5.0	Índice de auditorias
2	Há um relatório de perfil de riscos atualizado e completo		Índice de ativos de TI incluídos na análise de riscos (risk profile)
3	Ações de gerenciamento de risco importantes são gerenciadas e controladas		Índice de tratamento de riscos
4	Ações de gerenciamento de riscos são efetivamente implementadas		Índice de Risco de Ativos

Aguardando aprovação

6.2 Descrição dos indicadores

1) Índice de auditorias

Origem	• COBIT 5.0 o Enabling process: APO12.01 o Process Assessment Model ▪ Outcome APO12-01 ▪ Base pratice APO12-BP1
Periodicidade	Anual
Meta	90%
Fórmula de cálculo	Total de auditorias realizadas / total de auditorias previstas
Fonte	• Planilha do ANEXO I o Total de auditorias realizadas: ver a soma dos valores da coluna “Nº de auditorias realizadas” o Total de auditorias previstas: ver a soma dos valores da coluna “Nº de auditorias previstas”
Observação	Acumular valores

2) Índice de ativos de TI incluídos na análise de riscos (risk profile)

Origem	• COBIT 5.0 o Enabling process: APO12.03 o Process Assessment Model ▪ Outcome APO12-02 ▪ Base pratice APO12-BP3
Periodicidade	Anual
Meta	90%
Fórmula de cálculo	Total de ativos analisados / Total de ativos

Aguardando aprovação

Fonte	• Planilha do ANEXO II o Total de ativos analisados: ver a soma de valores da coluna “Nº de ativos analisados” o Total de ativos: ver a soma dos valores da coluna “Nº de ativos”
Observação	• Acumular valores

3) Índice de tratamento de riscos

Origem	• COBIT 5.0 o Enabling process: APO12.05 o Process Assessment Model ▪ Outcome APO12-03 ▪ Base pratice APO12-BP5
Periodicidade	Anual
Meta	60%
Fórmula de cálculo	Coeficiente de tratamento / Total de demandas de soluções propostas
Fonte	• Planilha do ANEXO III o Coeficiente de tratamento: ver a soma de valores da coluna “Coeficiente de tratamento” o Total de demandas de soluções propostas: ver o total de demandas registradas na planilha
Observação	Acumular valores

4) Índice de Risco de Ativos

Origem	• COBIT 5.0 o Enabling process: APO12.02/04 o Process Assessment Model ▪ Outcome APO12-04 ▪ Base pratice APO12-BP2/BP4

Aguardando aprovação

Periodicidade	Anual					
Meta	2015	2016	2017	2018	2019	2020
	87%	60%	50%	40%	30%	20%
Fórmula de cálculo	Total de controles com PSR “Alto” ou “Muito Alto” / Total de controles					
Fonte	• Planilha do ANEXO IV o Total de controles com PSR “Alto” ou “Muito Alto”: ver o último valor registrado na coluna “Nº de controles com PSR ‘Alto’ ou ‘Muito Alto’ ” o Total de controles: ver o último valor registrado na coluna “Nº de controles”					

Aguardando aprovação

7 Divulgação de resultados

Os resultados do processo serão demonstrados através dos indicadores de desempenho disponibilizados no site de governança de TIC da Coordenadoria de Tecnologia da Informação e Comunicações, menu Indicadores, item Indicadores Gerenciais, processo Gerenciar Riscos de TIC.

Aguardando aprovação

8 Anexo I – Índice de auditorias

Data do registro	Nº de auditorias realizadas	Nº de auditorias previstas

Onde:

- **Para cada execução do processo:**
  - **Data do registro:** data de referência do registro
  - **Nº de auditorias realizadas**: nº acumulado de análises de riscos realizadas conforme o fluxo do processo
  - **Nº de auditorias previstas:** nº acumulado de análises de riscos previstas até o momento (considerar no mínimo 2 análises de risco por ano)

9 Anexo II – Índice de ativos de TI incluídos na análise de riscos (risk profile)

Data do registro	Nº de ativos analisados	Nº de ativos

Onde:

- **Para cada execução do processo:**
  - **Data do registro:** data de referência do registro
  - **Nº de ativos analisados:** nº de ativos da “Lista de ativos a serem analisados” que foram efetivamente analisados
  - **Nº de ativos**: nº de ativos da “Lista de ativos críticos”

Aguardando aprovação

10 Anexo III – Índice de tratamento de riscos

Data do registro	Descrição da demanda	Coeficiente de tratamento
	Demanda 1	0
	Demanda 2	1
	...	
	Demanda n	0,5

Onde:

- **Para cada execução do processo:**
  - **Data do registro:** data de referência do registro
  - **Descrição da demanda**: descrição da demanda conforme listado no Plano de Tratamento de Riscos
  - **Coeficiente de tratamento:** "0" para as demandas não atendidas, "0,5" para as demandas em atendimento e "1" para as demandas atendidas.

Observação: listar as demandas acumuladas dos Planos de Tratamentos de Risco (evitar repetições)

11 Anexo IV - Índice de Risco de Ativos

Data do registro	Nº de controles com PSR "Alto" ou "Muito Alto"	Nº de controles

Onde:

- **Para cada execução do processo:**
  - **Data do registro:** data de referência do registro
  - **Nº de controles com PSR "Alto" ou "Muito Alto":** somatório do nº de controles com PSR "Alto" ou "Muito Alto" obtido do relatório de análise de riscos
  - **Nº de controles:** total de controles obtido do relatório de análise de riscos

Aguardando aprovação