Secretaria da TIC do TRT24

GESLAINE
PEREZ
MAQUERTE
10/09/2024 14:58

Processo Gerenciar Riscos de TIC

HISTÓRICO DO DOCUMENTO

	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
06	30/06/2022	Readequar o processo às recomendações do CSJT e alinhar à nova metodologia
07	28/02/2024	Revisão do Processo

Secretaria de TIC do TRT da 24ª Região

Documento de Descrição de Processo de Trabalho

Processo Gerenciar Riscos de TIC

28/02/2024

EQUIPE DE DOCUMENTAÇÃO

	Nome	Cargo
01	João Carlos Ferreira Filho	Chefe da Divisão de Governança de TIC
02	Geslaine Perez Maquerte	Chefe da Divisão de Proteção de Dados e Segurança da Informação
03	Alex Sandro Pontes da Silva	Chefe do Setor de Apoio a Processos e Iniciativas Nacionais

SUMÁRIO

1 OBJETIVO 4

2 ABRANGÊNCIA 4

3 DEFINIÇÕES 4

4 PROCESSO GERENCIAR RISCOS DE TIC 5

4.1 Papéis e Responsabilidades 5
4.2 Fluxo do Processo 6
4.3 Descrição de Processo 7

5 TABELA RACI 9

5.1 Processo Gerenciar Riscos de TIC 9

6 INDICADORES DO PROCESSO 10

6.1 Descrição dos Indicadores 10

7 DIVULGAÇÃO DE RESULTADOS 11

8 ANEXO I – ÍNDICE DE ATIVOS DE TI INCLUÍDOS NA ANÁLISE DE RISCOS (*RISK PROFILE*) 12

9 ANEXO II - ÍNDICE DE RISCO DE ATIVOS 13

1 Objetivo

Atender às demandas de avaliação de riscos de ativos de TI, baseando-se na Norma ABNT NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação - que implemente no mínimo os controles CIS versão 8.1 ou superior (https://seginfo.com.br/2021/09/10/cis-controls-v8-versao-em-portugues-disponivel-para-download/).

2 Abrangência

Secretaria de Tecnologia de Informação e Comunicações.

3 Definições

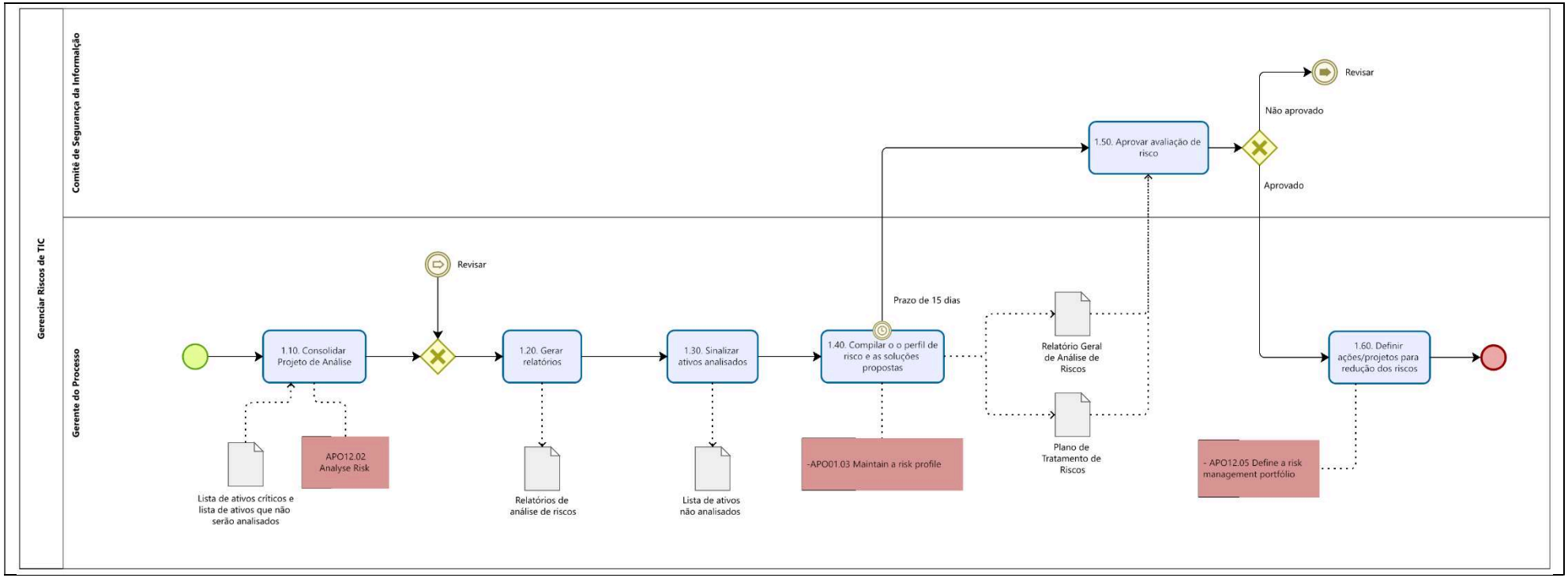
- **Ameaça:** ação de origem humana (intencional ou acidental) ou ambiental, que explora uma vulnerabilidade presente num ativo e provoca impactos na organização.
- **Ativo:** qualquer recurso que possui valor para a organização e cujo risco precisa ser controlado e gerenciado. Pode ser uma operação, 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.

4 Processo Gerenciar Riscos de TIC

4.1 Papéis e Responsabilidades

Papel	Responsabilidades	Responsável
Dono Processo	● Assegurar que todos os envolvidos na execução do processo sejam informados das mudanças e suporte efetuados ● Aprovar as atualizações do processo ● Buscar a qualidade e eficiência do processo	Secretário de Tecnologia de Informação e Comunicações
Gerente do Processo	● Buscar a eficiência e a efetividade do processo ● Manter o desenho e indicadores do processo atualizados, garantindo que estejam adequados aos propósitos da organização ● Produzir informações gerenciais (indicadores) ● Promover a execução das atividades do processo	Chefe da Divisão de Proteção de Dados e Segurança da Informação
Comitê de Segurança da Informação	● Aprovar o Relatório Geral de Análise de Riscos	Coordenador do Comitê de Segurança da Informação e Proteção de Dados

4.2 Fluxo do Processo



4.3 Descrição de Processo

Id	Atividade	Responsável	Descrição
1.10	Consolidar Projeto de Análise	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** informações da lista de ativos críticos e lista de ativos que não serão analisados
			Processamento: • Concluir projeto de análise, reunindo todos os dados recebidos e informando aos proprietários que novas informações serão incluídas no próximo ciclo. • Gerar resultados conforme fórmulas da metodologia aplicada, utilizando-se da ferramenta escolhida.
			Saídas: somatório dos valores PSR (Probabilidade/Severidade/Relevância) dos riscos de cada ativo
1.20	Gerar Relatórios	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Entradas:** dados da análise de riscos com a aplicação da metodologia de cálculo
			Processamento: • Gerar relatórios executivos, gerenciais e operacionais, que guiarão as ações de tratamento dos riscos.
			Saídas: relatórios de análise de riscos
1.30	Sinalizar ativos analisados	Chefe da Divisão de Proteção de Dados e 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
1.40	Compilar o perfil de risco e as soluções propostas	Chefe da Divisão de Proteção de Dados e 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. **Observação**: 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
1.50	Aprovar avaliação de risco	Coordenador do Comitê de Segurança da Informação e Proteção de Dados	**Entradas:** Relatório Geral de Análise de Riscos
			Processamento: • Avaliar a análise de riscos realizada e aprovar ou não.
			Saídas: relatório de análise de riscos validado
1.60			**Entradas:** relatórios produzidos durante a análise de riscos

Id	Atividade	Responsável	Descrição
	Definir ações/projetos para redução de riscos	Chefe da Divisão de Proteção de Dados e Segurança da Informação	**Processamento**: • Definir um portfólio de ações/projetos de redução dos riscos de TIC a um nível aceitável para o TRT. A conclusão do relatório irá embasar algumas das próximas ações da segurança da informação
			Saídas: lista de ações/projetos para redução de riscos

5 Tabela RACI

5.1 Processo Gerenciar Riscos de TIC

	Atividade	Comitê de Segurança da Informação	Chefe da Divisão de Proteção de Dados e Segurança da Informação
1.10	Consolidar Projeto de Análise	**I**	**R**
1.20	Gerar Relatórios		**R**
1.30	Sinalizar ativos analisados		**R**
1.40	Compilar o perfil de risco e as soluções propostas		**R**
1.50	Aprovar avaliação de risco	**R**	**C**
1.60	Definir ações/projetos para redução de risco	**C**	**R**

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

6 Indicadores do Processo

6.1 Descrição dos Indicadores

Nome de indicador	**Índice de ativos de TI incluídos na análise de riscos (risk profile)**
Origem	• COBIT 5.0 ○ *Enabling process*: APO12.03 ○ *Process Assessment Model* ▪ *Outcome* APO12-02 ▪ *Base pratice* APO12-BP3
Objetivo	Medir a atualização e adequação dos itens incluídos na análise de riscos
Meta	90%
Periodicidade	Anual
Fórmula de cálculo	Total de ativos analisados / Total de ativos
Fonte	• Planilha do ANEXO I ○ Total de ativos analisados: ver a soma de valores da coluna “Nº de ativos analisados” ○ Total de ativos: ver a soma dos valores da coluna “Nº de ativos”
Observação	• Acumular valores

Nome de indicador	**Índice de risco de ativos**					
Origem	• COBIT 5.0 ○ *Enabling process*: APO12.02/04 ○ *Process Assessment Model* ▪ *Outcome* APO12-04 ▪ *Base pratice* APO12-BP2/BP4					
Objetivo	Medir se as ações de gerenciamento de riscos são efetivamente implementadas					
Meta	2022	2023	2024	2025	2026	2027
	82,9%	60%	50%	40%	30%	20%
Periodicidade	Anual					

Fórmula de cálculo	Total de controles com PSR “Alto” ou “Muito Alto” / Total de controles

Fonte	• Planilha do ANEXO II
	  ○ 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’ ”
	  ○ Total de controles: ver o último valor registrado na coluna “Nº de controles”

7 Divulgação de resultados

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

8 Anexo I – 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"

9 Anexo II - 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