Secretaria de TIC do TRT24

ALEX SANDRO PONTES DA SILVA
03/10/2024 16:33

Processo Gerenciar Eventos

Histórico do Documento

	Data	Descrição
01	27/09/2024	Elaboração do documento

Secretaria de TIC do TRT da 24ª Região

Documento de Descrição de Processo de Trabalho

Processo Gerenciar Eventos

27/09/2024

Equipe de Documentação

	Nome	Cargo
01	Alex Sandro Pontes da Silva	Chefe do Setor de Apoio a Processos e Iniciativas Nacionais
02	Alessander Monteiro Silva	Chefe da Divisão de Infraestrutura de TIC

Sumário

1. Objetivo

Estabelecer o processo de gerenciamento de eventos para assegurar que métodos e procedimentos padronizados sejam usados para, a partir do monitoramento de eventos, detectar desvios da operação normal ou esperada de um serviço de TI ou item de configuração, recomendando a ação de controle apropriada.

2. Abrangência

Secretaria de Tecnologia da Informação e Comunicações (SETIC).

3. Definições

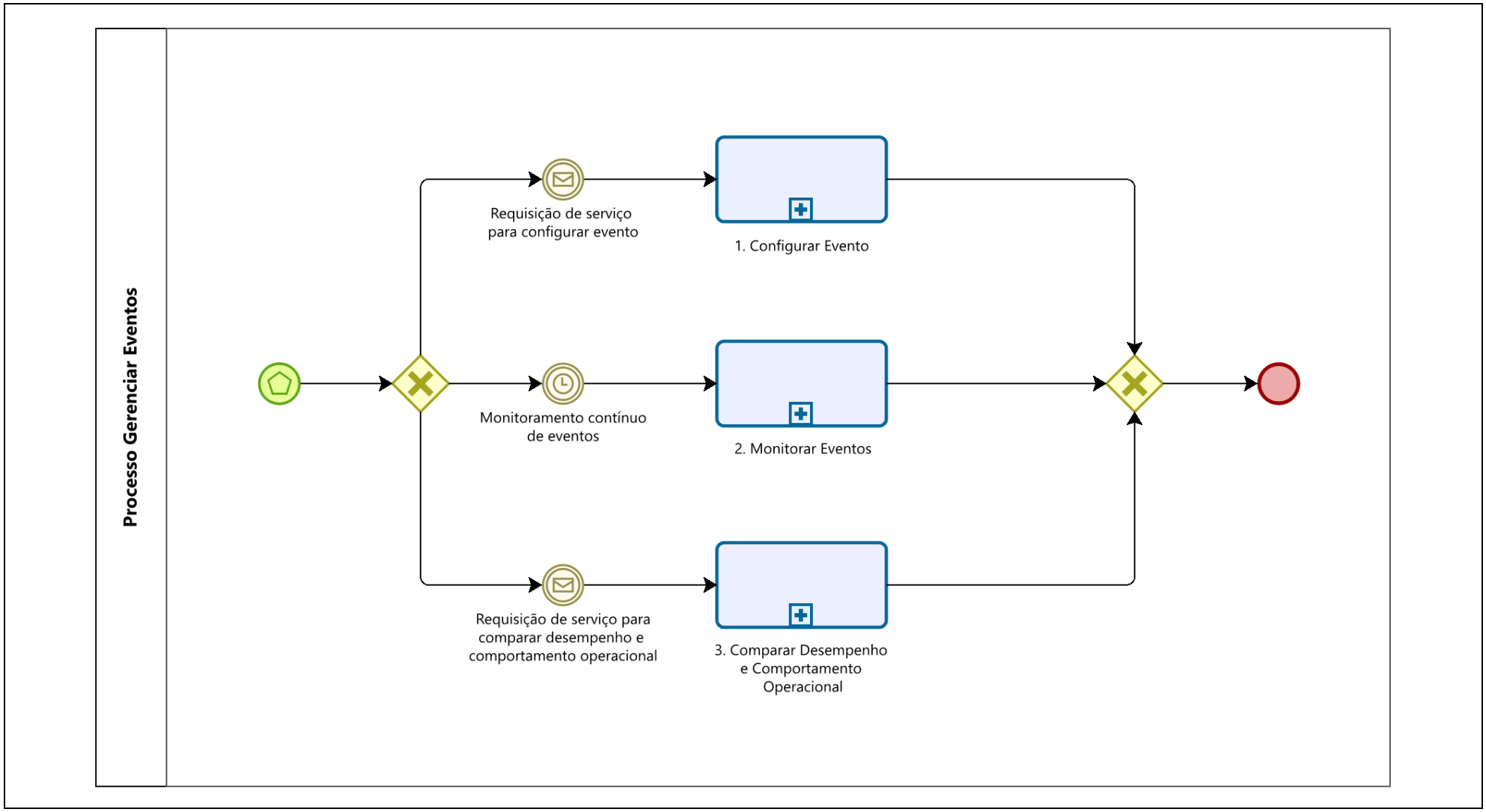
- **ANO:** Acordo de Nível Operacional
- **ANS:** Acordo de Nível de Serviço
- **Evento:** Qualquer mudança de estado que tenha significado para o gerenciamento de um serviço de TI ou item de configuração (IC). Os eventos podem ser divididos em três categorias:
  - **Informativo**: evento que não requer uma ação específica, mas precisa ser registrado a título de conhecimento. Ex: *jobs* executados com êxito, *backups* automáticos realizados com sucesso, rotinas de segurança concluídas com sucesso;
  - **Alerta**: evento gerado quando a operação de um serviço de TI ou IC está próxima a uma situação limite para tomada de providências. Ex: percentual de capacidade ocupada em *storage*, limites de capacidade de processamento de servidores;
  - **Exceção**: evento que identifica que uma determinada situação predefinida não está funcionando conforme o previsto. Ex: falha na realização de *backup*, tempo de execução de *job* muito acima do usual.
- **Ferramenta de monitoramento:** Aplicação utilizada para o monitoramento de eventos da infraestrutura de TI
- **Ferramenta ITSM:** Aplicação utilizada para o gerenciamento de serviços de TIC (CITSmart)
- **IC:** Item de Configuração

4. Processo Gerenciar Eventos

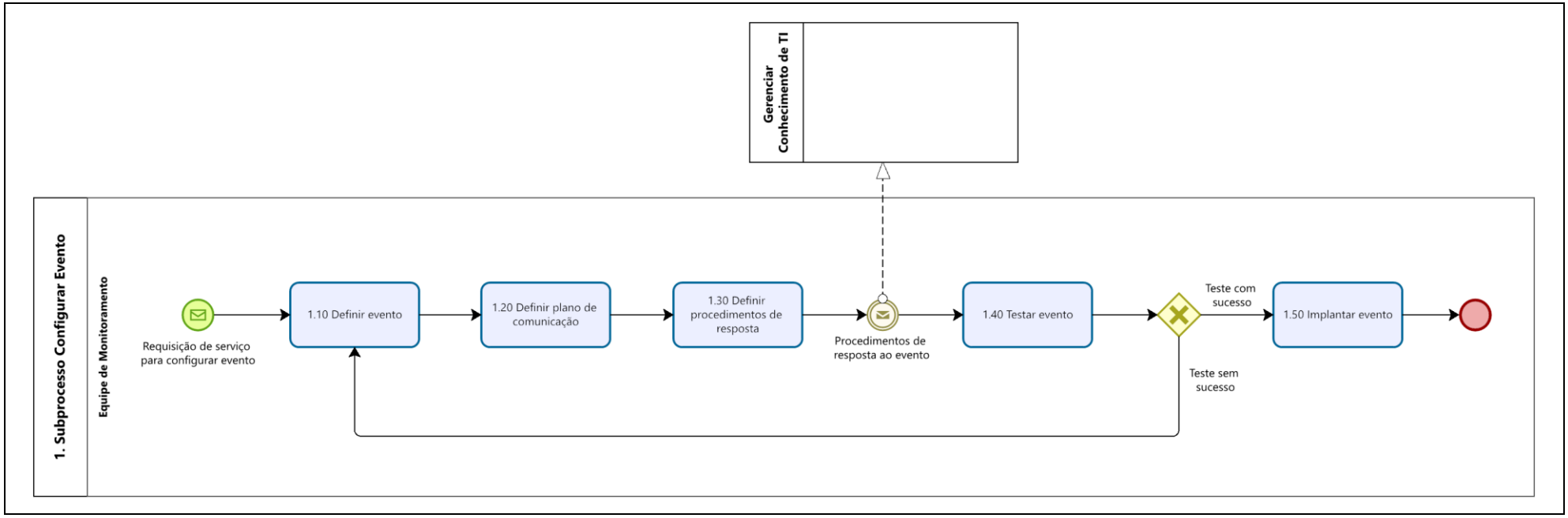
4.1 Papéis e Responsabilidades

Papel	Responsabilidades	Responsável
Dono do Processo	• Aprovar as atualizações do processo • Assegurar que todos os envolvidos na execução do processo sejam informados das mudanças e suporte efetuados • Buscar a qualidade e eficiência gerais do processo	Secretário de Tecnologia da 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 Infraestrutura de TIC
Equipe de Monitoramento	• Estabelecer e manter atualizadas as estratégias de monitoramento do ambiente operacional para detecção, classificação e resposta adequada a eventos de TI significativos • Executar procedimentos que permitam comparar o desempenho e comportamento operacional atual com os que foram planejados para os serviços de TI ou itens de configuração	Servidores da Divisão Infraestrutura de TIC

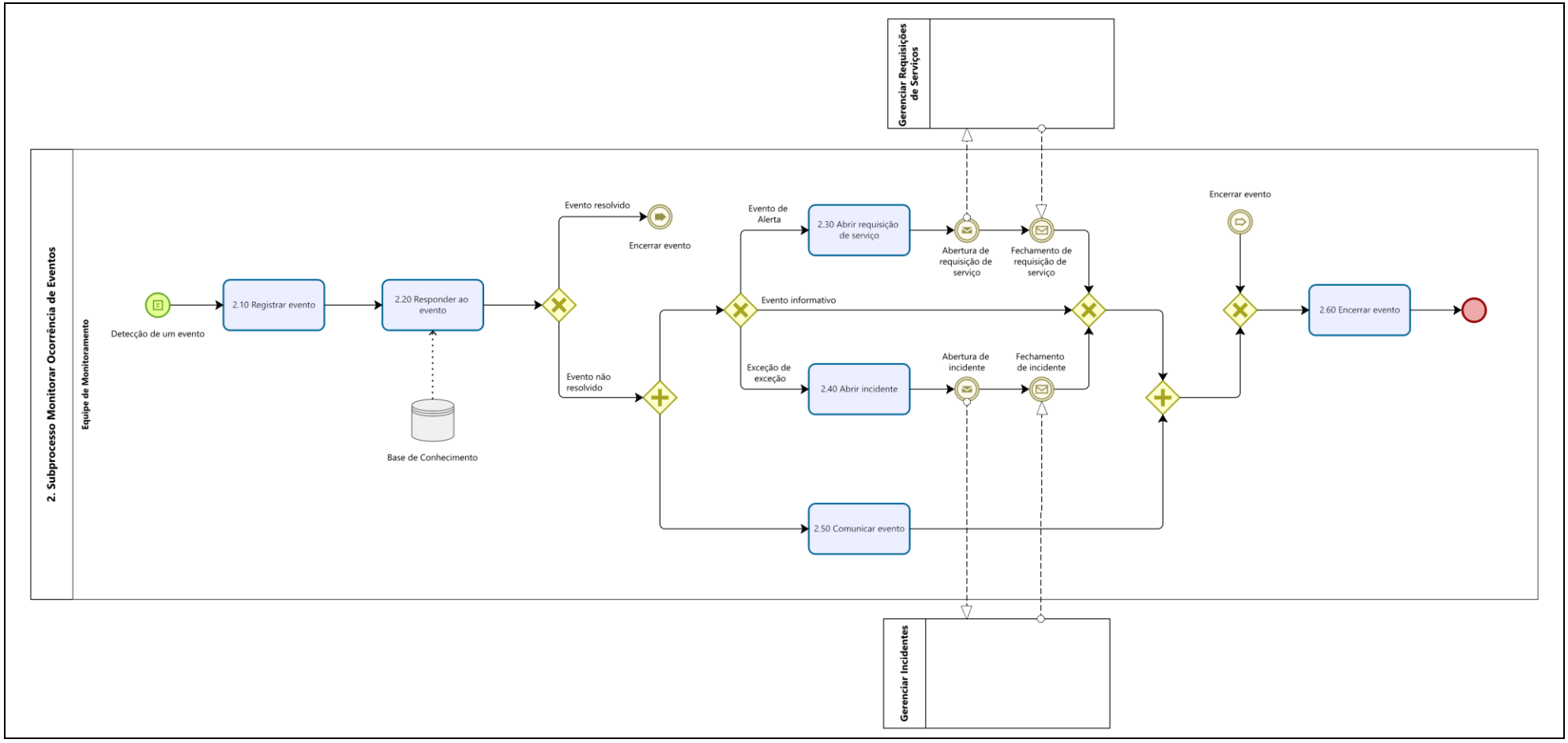
4.2 Fluxo Macro do Processo Gerenciar Eventos



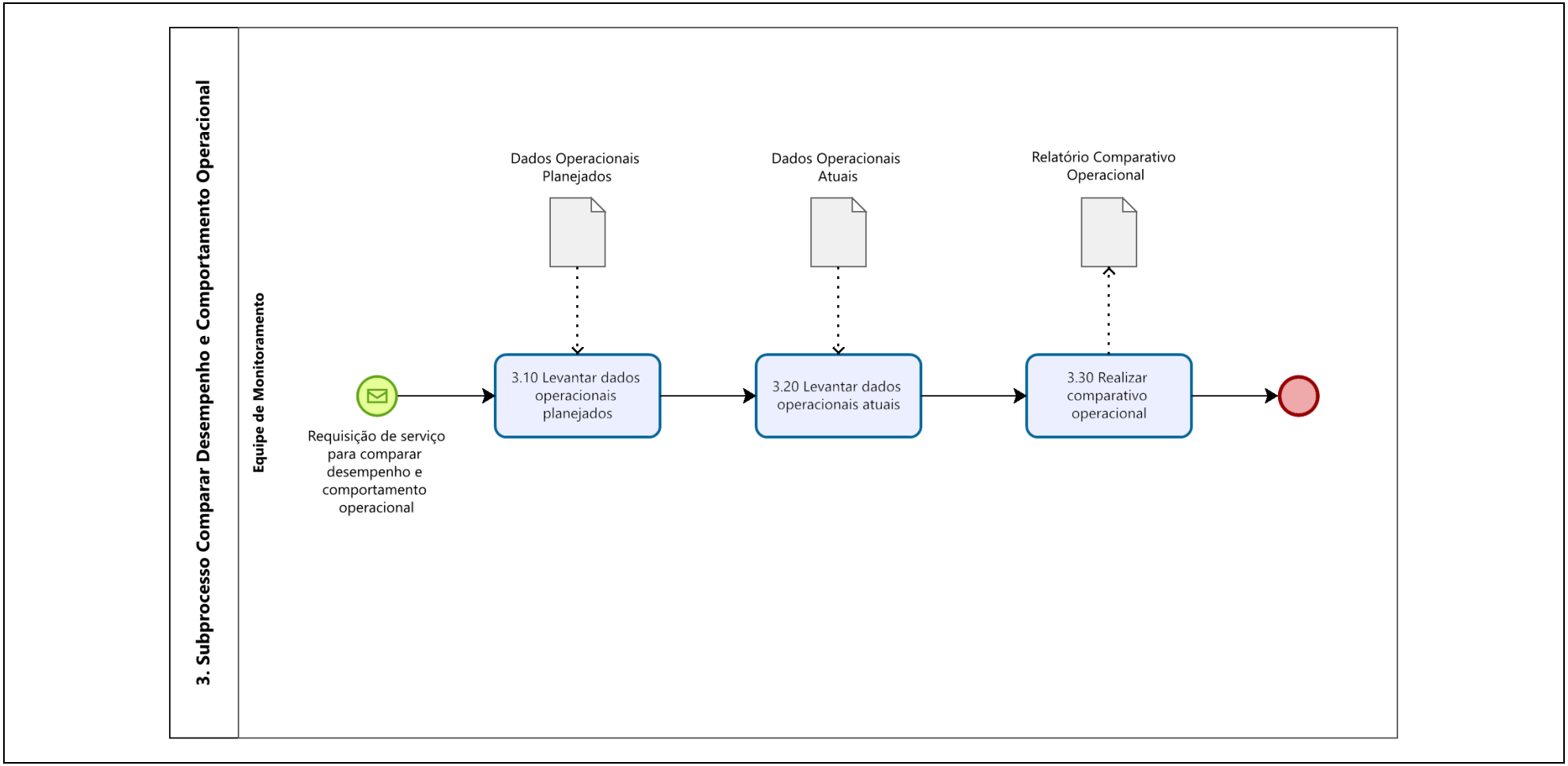
4.2.1. Fluxo do Subprocesso Configurar Evento



4.2.2. Fluxo do Subprocesso Monitorar Eventos



4.2.3. Fluxo do Subprocesso Comparar Desempenho e Comportamento Operacional



4.3 Descrição do Subprocesso Configurar Evento

Id	Atividade	Responsável	Descrição
1.10	Definir evento	Equipe de Monitoramento	**Entrada:** Requisição de serviço para configurar evento
			Processamento: • Baseando-se em considerações de risco e desempenho, determinar quais eventos referentes à operação do serviço ou IC são significativos e devem ser registrados • Verificar a existência de relacionamento de dependência com demais ICs e serviços e avaliar a necessidade de monitoramento deles • Na ferramenta de monitoramento, categorizar o evento a ser monitorado (informativo, alerta ou exceção) e definir os seus atributos relevantes
			Saída: Evento definido
1.20	Definir plano de comunicação	Equipe de Monitoramento	**Entrada:** Evento definido
			Processamento: • Definir um plano de comunicação na ferramenta de monitoramento, determinando quem, como, quando e as mensagens de notificação sobre o evento
			Saída: Plano de comunicação definido
1.30	Definir procedimentos de resposta	Equipe de Monitoramento	**Entrada:** Evento e plano de comunicação definidos
			Processamento: • Determinar os procedimentos técnicos que são adequados para responder ao evento definido e registrá-los na base de conhecimento de TI
			Saída: Procedimentos de resposta ao evento definidos
1.40	Testar evento	Equipe de Monitoramento	**Entrada:** Evento e procedimentos de resposta ao evento definidos
			Processamento: • Testar o funcionamento da rotina de monitoramento, comunicação e os respectivos procedimentos de resposta ao evento
			Saída: Evento testado
			Se o teste for executado **com sucesso**, seguir para “Implantar evento”
			Se o teste for executado **sem sucesso**, seguir para “Definir evento”

Id	Atividade	Responsável	Descrição
1.50	Implantar evento	Equipe de Monitoramento	**Entrada:** Evento testado
			Processamento: • Implantar a rotina de monitoramento do evento no ambiente adequado
			Saída: Evento implantado

4.4 Descrição do Subprocesso Monitorar Eventos

Id	Atividade	Responsável	Descrição
	Detecção de um evento		Através de ferramentas de monitoramento ou de verificação pessoal, é realizada a inspeção do funcionamento do ambiente operacional. O evento é considerado detectado quando seus critérios de identificação forem satisfeitos
2.10	Registrar evento	Equipe de Monitoramento	**Entrada:** Evento detectado
			Processamento: • O evento detectado deve ser registrado na ferramenta ITSM e, de acordo com suas características, ser classificado em informativo, alerta ou exceção • Sempre que possível, correlacionar o evento aos serviços e ICs associados
			Saída: Evento registrado
2.20	Responder ao evento	Equipe de Monitoramento	**Entrada:** Evento registrado
			Processamento: • Executar a ação (manual ou automática) prevista nos procedimentos técnicos de resposta ao evento, tal como: iniciar um *job*, reiniciar uma aplicação, aplicar uma rotina, acionar *software* de segurança • Verificar o resultado da resposta executada (resolvido ou não resolvido)
			Saída: Resposta ao evento executada
			Se o evento estiver **resolvido**, seguir para “Encerrar evento”
			Se o evento **não** estiver **resolvido** e for um **alerta**, seguir para “Abrir requisição de serviço” e “Comunicar evento”
			Se o evento **não** estiver **resolvido** e for **informativo**, seguir para “Comunicar evento” e “Encerrar evento”
			Se o evento **não** estiver **resolvido** e for uma **exceção**, seguir para “Abrir incidente” e “Comunicar evento”
2.30	Abrir requisição de serviço	Equipe de Monitoramento	**Entrada:** Evento de alerta não resolvido
			Processamento: • Para evento classificado como **alerta** deve ser aberto um chamado do tipo “requisição de serviço” na ferramenta ITSM, onde devem ser informados os dados que identificam o evento • O atendimento da requisição de serviço será tratado pelo processo Gerenciar Requisições de Serviços
			Saída: Requisição de serviço aberta

Id	Atividade	Responsável	Descrição
			Abertura de requisição de serviço
			Fechamento de requisição de serviço
2.40	Abrir incidente	Equipe de Monitoramento	**Entrada:** Evento de exceção não resolvido
			Processamento: • Para evento classificado como **exceção** deve ser aberto um chamado do tipo "incidente" na ferramenta ITSM, onde devem ser informados os dados que identificam o evento • O atendimento do incidente será tratado pelo processo Gerenciar Incidentes
			Saída: Incidente aberto
			Abertura de incidente
			Fechamento de incidente
2.50	Comunicar evento	Equipe de Monitoramento	**Entrada:** Evento não resolvido
			Processamento: • Comunicar a existência do evento conforme definido no plano de comunicação do evento
			Saída: Evento não resolvido comunicado
2.60	Encerrar evento	Equipe de Monitoramento	**Entrada:** Evento registrado

			Processamento:
			• Registrar o encerramento do evento na ferramenta ITSM conforme a seguir:
			  ○ Se os procedimentos executados **produziram os efeitos esperados**, encerrar o evento como **resolvido**
			  ○ Se os procedimentos executados **não produziram os efeitos esperados**, encerrar o evento como **não resolvido**
			  ○ Caso o evento represente um **falso positivo**, encerrar o evento como **improcedente** e registrar seus detalhes para a correção e melhoria do monitoramento
			  ○ Eventos com ação **automática** ou classificados como **informativos** podem ser encerrados de **forma automática**

Id	Atividade	Responsável	Descrição
			Saída: Evento encerrado

4.5 Descrição do Subprocesso Comparar Desempenho e Comportamento Operacional

Id	Atividade	Responsável	Descrição
3.10	Levantar dados operacionais planejados	Equipe de Monitoramento	**Entrada:** Requisição de serviço para avaliar desempenho e comportamento operacional; e dados operacionais planejados
			Processamento: • Levantar junto ao solicitante da requisição de serviço os dados operacionais **planejados** sobre os serviços ou ICs que serão objetos de comparação (p. ex. dados sobre desempenho, capacidade, disponibilidade, segurança, ANS/ANO)
			Saída: Dados de desempenho e comportamento operacional planejados
3.20	Levantar dados operacionais atuais	Equipe de Monitoramento	**Entrada:** Dados de desempenho e comportamento operacional planejados
			Processamento: • Com o auxílio das rotinas de monitoramento de eventos, levantar os dados operacionais **atuais** (reais) sobre os serviços ou ICs que serão objetos de comparação
			Saída: Dados de desempenho e comportamento operacional atuais
3.30	Realizar comparativo operacional	Equipe de Monitoramento	**Entrada:** Dados de desempenho e comportamento operacional planejados; Dados de desempenho e comportamento operacional atuais
			Processamento: • Produzir relatório que apresente o comparativo dos dados de desempenho e comportamento operacionais atuais (reais) com os que foram planejados para os serviços ou ICs
			Saída: Relatório Comparativo Operacional

5. Tabela RACI

5.1 Subprocesso Configurar Evento

Id	Atividade	Equipe de Monitoramento
1.10	Definir evento	**R**
1.20	Definir plano de comunicação	**R**
1.30	Definir procedimentos de resposta	**R**
1.40	Testar evento	**R**
1.50	Implantar evento	**R**

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

5.2 Subprocesso Monitorar Eventos

Id	Atividade	Equipe de Monitoramento
2.10	Registrar evento	**R**
2.20	Responder ao evento	**R**
2.30	Abrir requisição de serviço	**R**
2.40	Abrir incidente	**R**
2.50	Comunicar evento	**R**
2.60	Encerrar evento	**R**

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

5.3 Subprocesso Comparar Desempenho e Comportamento Operacional

Id	Atividade	Equipe de Monitoramento
3.10	Levantar dados operacionais planejados	**R**
3.20	Levantar dados operacionais atuais	**R**
3.30	Realizar comparativo operacional	**R**

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

6. Controles do Processo

6.1 Descrição do Indicador

Nome da Métrica/Indicador	Percentual de ICs Críticos com Monitoramento de Eventos

Origem	***COBIT 5 – DSS01 Manage Operations*** (Gerenciar Operações)
	• ***Process Goals and Metrics***
	  ○ ***Process Goal****: Operations are monitored, measured, reported and remediated.*
	  ○ ***Related Metrics****: Percent of critical operational event types covered by automatic detection systems*

Objetivo	Medir o percentual de ICs (Itens de Configuração) críticos que possuem monitoramento de eventos
Meta	Pelo menos 80% de ICs críticos com monitoramento de eventos
Periodicidade	Semestral
Forma de cálculo	(Total de ICs Críticos com Monitoramento / Total de ICs Críticos)

Fonte	• Tabela do ANEXO I
	  ○ **Total de ICs Críticos com Monitoramento**: ver coluna “Total de ICs Críticos com Monitoramento”;
	  ○ **Total de ICs Críticos**: ver coluna “Total de ICs Críticos”.

Observação	• Não acumular valores • Polaridade positiva

7. Divulgação dos Resultados

Os resultados do processo serão demonstrados através dos dados de métricas e indicadores registrados no processo administrativo autuado com o fim específico de acompanhar as atividades desse processo de trabalho, bem como no site de governança da SETIC, menu Indicadores, item Indicadores Gerenciais, processo Gerenciar Eventos.

8. ANEXO I – Indicador Percentual de ICs Críticos com Monitoramento de Eventos

Período da apuração	Total de ICs Críticos com Monitoramento	Total de ICs Críticos	Percentual de ICs Críticos com Monitoramento de Eventos
Janeiro a Junho 2024	90	100	90,00%
Julho a Dezembro 2024	95	100	95,00%

Onde:

- Para cada apuração:
  - **Período da apuração**: período de datas (início e fim) em que os dados estão sendo apurados.
  - **Total de ICs Críticos com Monitoramento**: informar a quantidade de ICs classificados como críticos que possuem algum evento monitorado.
  - **Total de ICs Críticos**: informar a quantidade de ICs classificados como críticos.