PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO

PROCESSO DE GERENCIAMENTO DE EVENTOS DE TIC

SUMÁRIO

1. OBJETIVO

Este documento tem por objetivo estabelecer o Processo de Gerenciamento de Eventos de TIC no âmbito do Tribunal Regional do Trabalho da 16ª Região (TRT16), a fim de representar e descrever as atividades necessárias para detectar eventos que possam comprometer a prestação de serviços de TIC e a segurança da informação do Tribunal.

2. APLICABILIDADE

Tem aplicabilidade nas atividades de planejamento e monitoramento dos eventos gerados pelos serviços de TIC e pelos itens de configurações (IC's) no âmbito do Tribunal Regional do Trabalho da 16ª Região (TRT16).

3. TERMOS E DEFINIÇÕES

- Evento: indica um comportamento de um serviço ou IC que não está funcionando de forma normal;
- IC: Item de configuração. Qualquer componente que precisa ser configurado para entregar um serviço de TIC;
- Incidente: qualquer acontecimento que não seja parte da operação padrão de um serviço e que causa, ou pode causar, uma interrupção ou redução na qualidade daquele serviço;
- Incidente de Segurança da Informação: é um tipo específico de incidente relacionado à segurança da informação, que comprometa a confidencialidade, integridade e disponibilidade da informação;

- Proprietário de Serviço: chefe da unidade de TIC responsável pela implantação e gerenciamento do serviço;
- Ferramenta de Monitoramento: soluções tecnológicas especializadas que realizam a supervisão contínua dos variados serviços prestados pelo Tribunal, incluindo os (IC's).
- RACI: matriz de responsabilidade;
- SETIC: Secretaria de Tecnologia de Informação e Comunicação;
- Software Livre: software que pode ser copiado, executado, modificado e distribuído livremente, sem necessidade de pagar pela aquisição;
- TIC: Tecnologia de Informação e Comunicações.

4. PAPÉIS E RESPONSABILIDADES

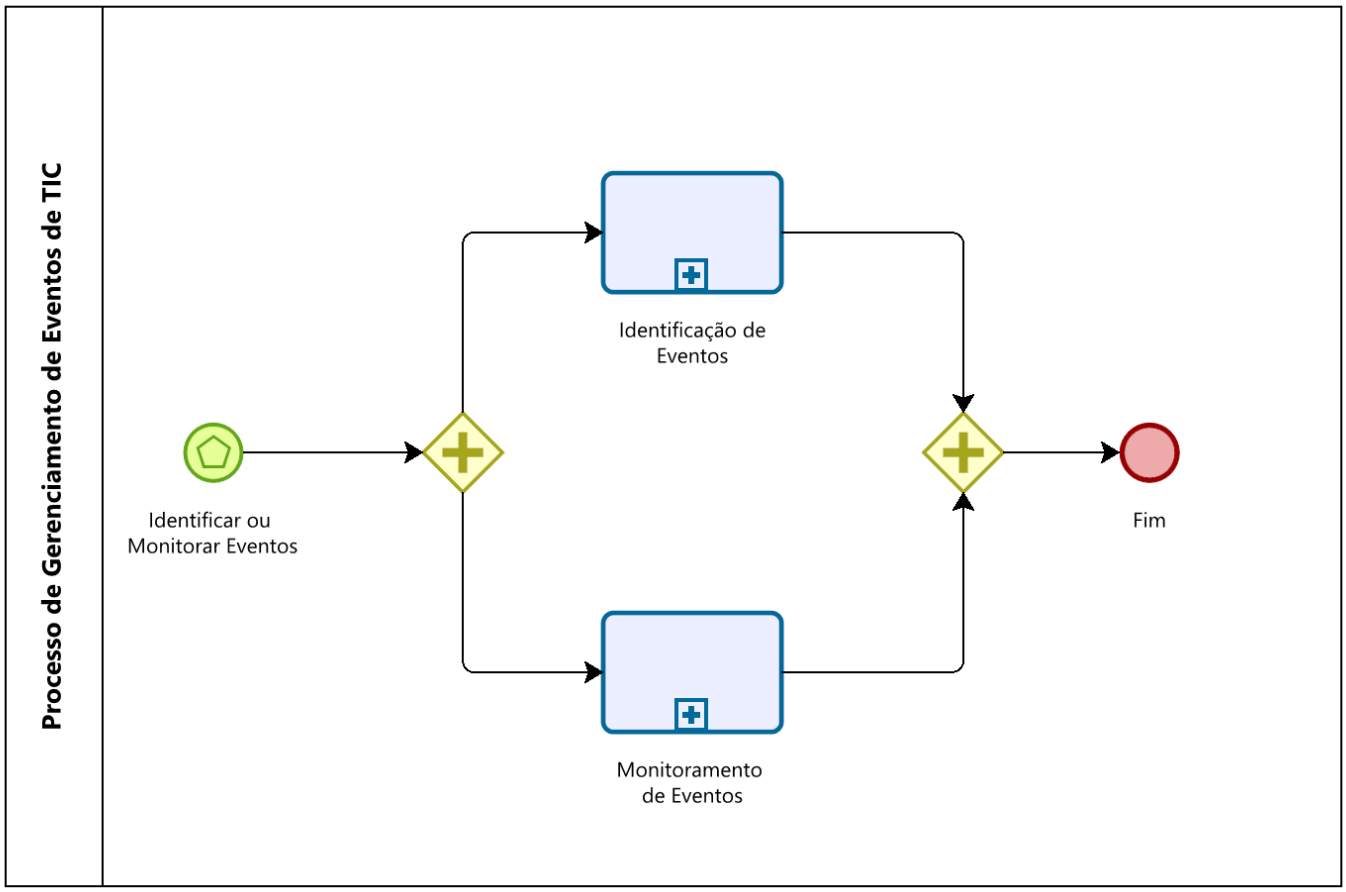
PAPEL	RESPONSABILIDADE	RESPONSÁVEL
Dono do Processo	• Buscar a qualidade e eficiência geral do processo; • Atuar na gestão de conflitos com as partes interessadas da demanda; • Aprovar os eventos que devem ser monitorados para cada serviço de TIC ou IC.	Chefe da Divisão de Infraestrutura e Segurança da Informação
Gerente do Processo	• Buscar a eficiência e a efetividade do processo; • Promover a execução das atividades do processo; • Definir as ferramentas que serão usadas no monitoramento; • Coordenar testes de monitoramento.	Chefe da Divisão de Infraestrutura e Segurança da Informação
Proprietário do Serviço ou IC	• Auxiliar na definição dos eventos que devem ser monitorados; • Definir equipe para tratar o evento; • Automatizar respostas para eventos corriqueiros; • Acionar o processo de tratamento de incidente; • Acionar o processo de tratamento de incidente de segurança da informação	Unidade técnica do serviço ou IC
Monitor de Evento	• Monitorar os eventos definidos e gerados pela ferramenta; • Classificar os tipos de eventos; • Fornecer um suporte inicial.	Servidor da Divisão de Infraestrutura e Segurança da Informação

5. INTERFACES COM OUTROS PROCESSOS

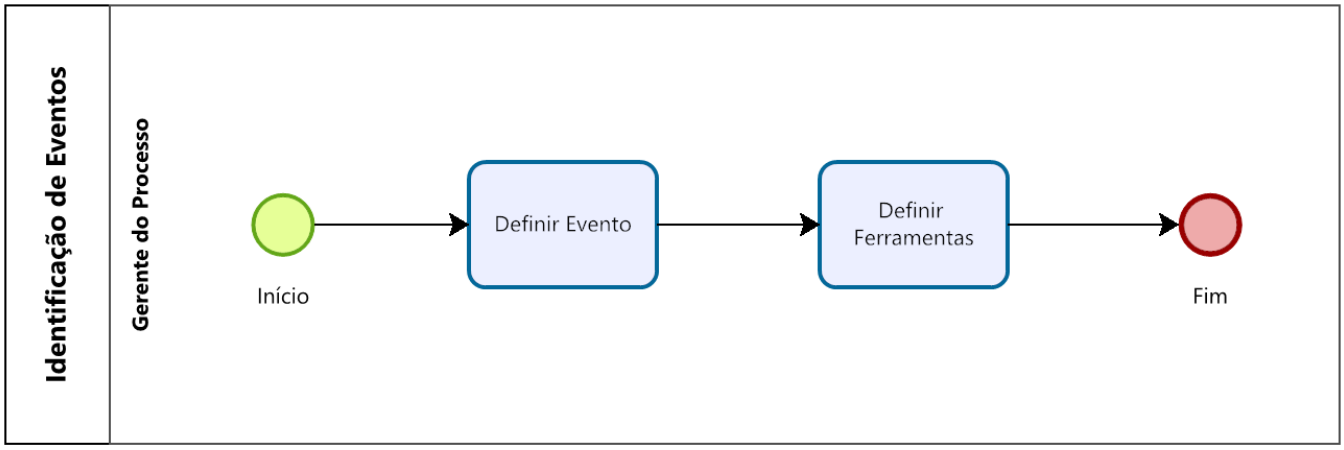
A seguir são descritas as principais interfaces do Processo de Gerenciamento de Evento de TIC com os outros processos de gestão de TIC do TRT16:

- Processo de Gerenciamento de Incidentes de TIC: esse processo é acionado quando um evento for classificado do tipo crítico, mas que não comprometa a segurança da informação ou cibernética deste Tribunal;
- Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação: esse processo é acionado quando um evento for classificado do tipo crítico e que comprometa a segurança da informação ou cibernética deste Tribunal.

6. MACROFLUXO DO PROCESSO

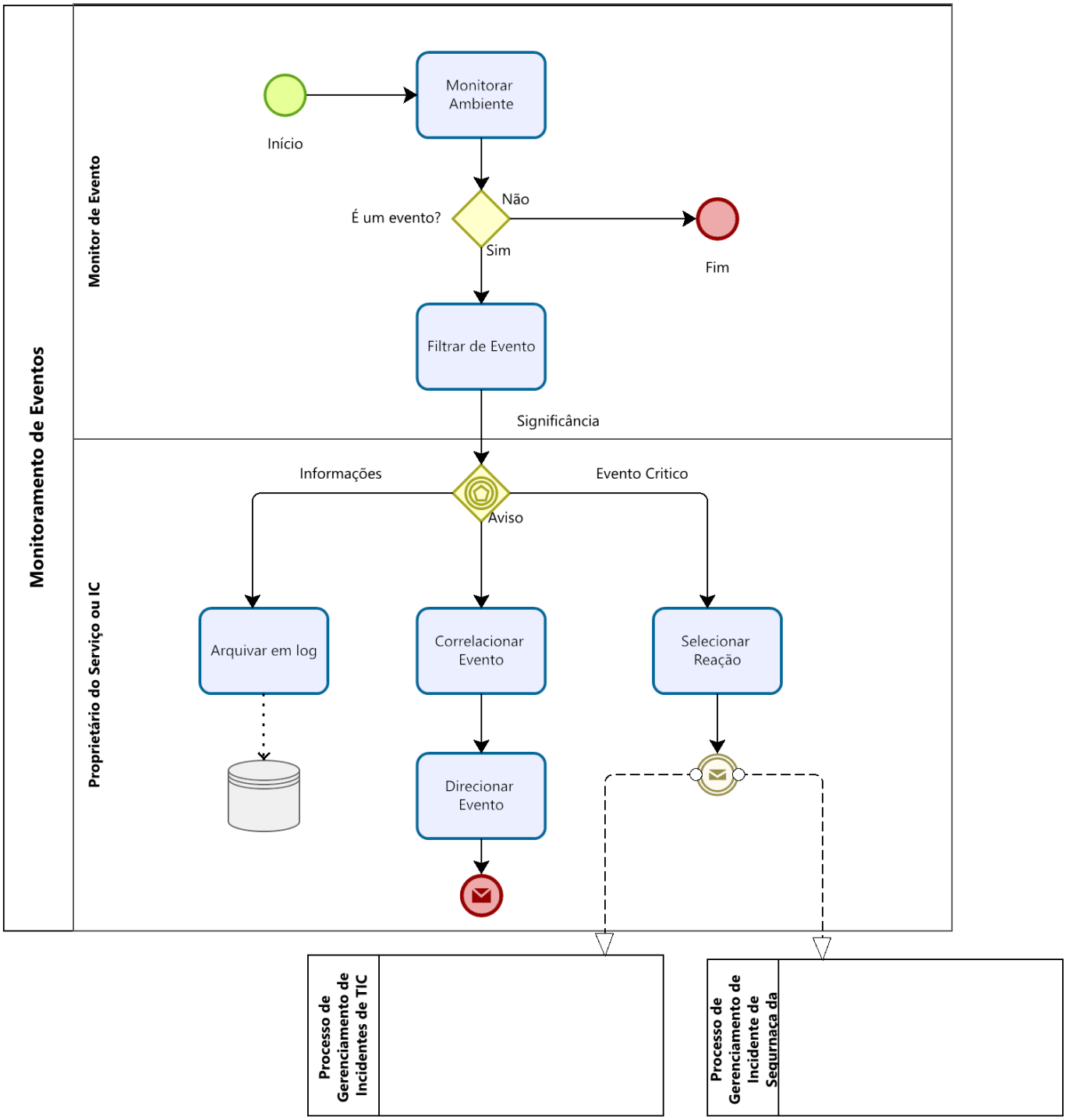


6.1. Identificação de Eventos



ATIVIDADE	RESPONSÁVEL	DETALHAMENTO
Definir Evento	Gerente do processo	Objetivo: Definir os eventos de serviços e IC'S que precisam ser monitorados. Entrada: Informações sobre o Serviço de TIC ou IC Descrição: • Definir quais eventos devem ser monitorados para o Serviço de TIC ou IC; • Baseado nas informações de Operação de Serviço, atualizar a relação de eventos que precisam ser monitorados de acordo com o histórico dos incidentes, problemas e ocorrências que comprometem a operação normal do serviço. Saídas: Eventos associados ao Serviço de TIC ou IC registrados.
Definir Ferramentas	Gerente do processo	Objetivo: Definir as ferramentas que irão monitorar os eventos definidos. Entradas: Eventos associados ao Serviço de TIC ou IC registrados. Descrição: • Analisar se a ferramenta de monitoramento em produção é capaz de monitorar os eventos definidos para Serviço de TIC ou IC; • Caso a ferramenta em produção não seja capaz de monitorar os novos eventos definidos, pesquisar por agentes de monitoramento da solução proprietária ou ainda procurar por uma solução baseada em software livre; • Configurar a ferramenta para monitorar os novos eventos; • Realizar testes de monitoramento. Saídas: Ferramenta escolhida, Eventos do Serviços de TIC e IC registrados na ferramenta.

6.2. Monitoramento de Eventos



ATIVIDADE	RESPONSÁVEL	DETALHAMENTO
Monitorar Ambiente	Monitor de Evento	Objetivo: Identificar eventos que tenham alguma significância, pois as ferramentas de gerenciamento acabam coletando muitos eventos sem importância. Entradas: Eventos do Serviços de TIC e IC escolhidos e registrados na ferramenta.Descrição: • Analisar os alertas gerados pela ferramenta; • Verificar se alerta recebido tem alguma significância; Saída: Evento que apresenta significância.

ATIVIDADE	RESPONSÁVEL	DETALHAMENTO
Filtrar de Evento	Monitor de Evento	Objetivo: Definir a partir de uma filtragem, a forma que o evento deve ser tratado. Entradas: Evento com significância.Descrição: • Categorizar o evento em 3 tipos: informação, aviso ou evento crítico; ◦ informativo: evento que não requer ações, porém precisa ser registrado. ◦ aviso: evento gerado quando um serviço está próximo do seu limite; ◦ evento crítico: Um determinado serviço ou configuração de IC não está funcionando como o previsto. • Encaminhar evento categorizado para o proprietário do serviço ou IC. Saída: Eventos encaminhados.
Arquivar em log	Proprietário do Serviço ou IC	Objetivo: Registrar os eventos informativos. Não requer uma ação. Entradas: Evento do Tipo Aviso Descrição: • Registrar o evento em um arquivo de log para fins de análise. Saídas: Evento registrado.
Correlacionar Evento	Proprietário do Serviço ou IC	Objetivo: Correlacionar o evento em relação aos níveis de serviços, categorias de riscos e impactos para o negócio. Entradas: Evento do tipo aviso Descrição: • Atribuir informações sobre o impacto do evento nos níveis de serviço; • Atribuir informações sobre o impacto do evento nos riscos para o negócio; • Atribuir informações sobre priorização do evento para os serviços. Saídas: Evento correlacionado.
Direcionar Evento	Proprietário do Serviço ou IC	Objetivo: Indicar para quem ou para onde o evento deve ser informado. Entrada: Evento correlacionado. Descrição: • Informar o(s) setor(es) ou pessoa(s) que deverão trabalhar na solução do evento; • Automatizar respostas àqueles eventos passíveis de serem tratados de tal forma. Saída: Evento direcionado.

ATIVIDADE	RESPONSÁVEL	DETALHAMENTO
Selecionar Reação	Proprietário do Serviço ou IC	Objetivo: Definir as providências que serão tomadas para tratar o evento crítico. Entrada: Evento crítico. Descrição: • Registrar um chamado de incidente quando for identificada uma exceção ou quando uma considerável quantidade de avisos indicar uma falha iminente; • Registrar um chamado de incidente de segurança da informação quando for identificada uma exceção que comprometa um dos tripés da segurança da informação, Confidencialidade, Disponibilidade e Integridade. Saída: Chamados registrados.

7. MATRIZ RACI

ATIVIDADE	Dono do Processo	Gerente do Processo	Proprietário do Serviço ou IC	Monitor de Evento
IDENTIFICAÇÃO DE EVENTOS				
Definir Evento	R/A	C	C	-
Definir Ferramentas	I	R/A	I	C
MONITORAMENTO DE EVENTOS				
Monitorar Ambiente	-	I	-	R
Filtrar Evento	-	-	-	R
Arquivar em log	-	-	R	C
Correlacionar Evento	I	I	R	-
Direcionar Evento	-	I	R	-
Selecionar Reação	I	I	R	-

8. INDICADORES

1 - Taxa de Detecção de Eventos	
Objetivo	Medir a eficácia do sistema de monitoramento de eventos em identificar e detectar eventos relevantes dentro da rede corporativa.
Periodicidade	Semestral
Forma de cálculo	(Número de Eventos Significantes/Número Total de Eventos) x 100
Fonte	Ferramentas de Detecção de Eventos do Tribunal e Alertas oriundos de outras entidades.

1 - Taxa de Detecção de Eventos	
Meta	> 70%

9. DIVULGAÇÃO DOS RESULTADOS

Os resultados do processo, indicadores e relatórios, serão demonstrados na página de Governança de TIC do Tribunal.

Documento assinado eletronicamente por **RAFAEL ROBINSON DE SOUSA NETO**, **Secretário de Tecnologia da Informação e Comunicação**, em 08/02/2024, às 14:19, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site Autenticar Documentos informando o código verificador **0102137** e o código CRC **65403569**.