SUMÁRIO

1. Equipe de Elaboração e Revisão do Manual

- Breno Moreno Luna;
- Carlos Alberto Araújo Correia Filho;
- Ewerton Leandro da Costa Araújo;
- Wilberto Rodrigues de Oliveira.

2. Objetivo

O objetivo do presente documento é definir o Processo de Gerenciamento de Eventos implantado pela Secretaria de Tecnologia da Informação e Comunicação (SETIC) do Tribunal Regional do Trabalho da 13ª Região .

3. Propósito do processo

O processo tem o propósito de monitorar e gerar alertas ou notificações de um serviço de TIC ou Item de configuração(IC).

4. Escopo

Este processo é aplicável a todas as ações e projetos executados pela SETIC, devendo ser de observação obrigatória por todos os servidores responsáveis pelo monitoramento de serviços e ICs de TIC.

5. Definições e Abreviações

- Processo: Conjunto de atividades interdependentes, ordenadas no tempo e espaço de forma encadeada, as quais ocorrem como resposta a eventos e possuem objetivo, inicio, fim, entradas e saídas bem definidas;
- Gerente do processo: Responsável pelos resultados do processo, coleta de indicadores e melhorias;
- Evento: indica que algo não está de acordo com a operação normal do serviço ou descumprindo um nível de serviço acordado;
- Incidente: Uma interrupção não planejada ou uma redução da qualidade de um serviço de TI;
- Item de configuração(IC): qualquer componente ou ativo de serviço que precise ser gerenciado de forma a entregar um serviço de TIC. Por exemplo: servidor, roteador, software, documentos formais, etc;
- Requisição de mudança(RDM): pedido formal, devidamente registrado, para realizar uma mudança.

6. Benefícios Esperados

- Padronização no monitoramento de serviços e ICs de TIC;
- Aumento na eficiência, eficácia e efetividade no monitoramento de eventos ;

7. Regras Gerais

7.1 Processo de Gerenciamento de eventos

Link para o diagrama: Processo de Gerenciamento de Eventos de TIC

7.1.1 Atividade: Monitoramento

- Objetivo: Monitorar o status e tendências dos Serviços de TI ou ICs e configurar alertas ;
- Entrada: Dados de monitoramento dos ICs e serviços;
- Saídas: Dados de monitoramento dos ICs e Serviços Registrados;
- Descrição: A equipe responsável pelo monitoramento deve monitorar o status e tendências dos serviços de TIC e configurar alertas para identificar possíveis incidentes, isso tudo feito por meio de uma ferramenta de monitoramento.
    - Exemplos de eventos que podem ser monitorados:
        - Detecção de intrusão na rede;
        - Alerta de vírus;
        - Performance de sistema de aplicações, banco de dados, rede;
        - Alerta de falhas em ICs;
        - Condições predeterminadas como identificação de erros em Log ou Jobs que não rodaram em determinado momento.

7.1.2 Atividade: Detecção de eventos

- Objetivo: Detectar possíveis eventos por meio de uma ferramenta de monitoramento;
- Entrada: Dados de monitoramento dos ICs e Serviços Registrados e correlacionados ;
- Saídas: Notificações de possíveis eventos ;
- Descrição: Deve-se identificar se é um evento ou não, caso não seja deve-se descartar a notificação, caso seja a ferramenta de monitoramento deve ter a capacidade de concentrar eventos coletados e interpretar o significado .

7.1.3 Atividade: Classificação do Eventos

- Objetivo: Decidir se o evento deve ser comunicado à operação de TIC ou se deve ser ignorado.
- Entrada: Evento;
- Saída: Evento classificado;
- Descrição: Decidir se o evento deve ser comunicado à operação de TIC ou se deve ser ignorado. Se for ignorado, será registrado em uma base de informações sobre eventos e nenhuma ação será tomada. Caso o evento seja tratado deve-se fazer a significância do evento com base em duas categorias descritas abaixo:
    - Aviso/Informativo
        - Informativo: Eventos que não requerem ações, são armazenados e mantidos por um período determinado, são normalmente utilizados para para verificar o status de IC. Também podem ser utilizados como insumos para monitorar a performance dos ICs. Deve-se passar para atividade correlacionar o evento com algum IC
        - Aviso: Evento gerado quando um serviço ou IC está se aproximando de uma situação limite . Deve-se enviar para o setor responsável tomar as providências. Deve-se passar para atividade correlacionar o evento com algum IC
    - Evento Crítico

- Identifica que uma situação pré definida que não está funcionando conforme previsto. A equipe de monitoramento deve identificar se o evento crítico é um incidente ou uma mudança.

7.1.4 Atividade: Correlacionar o Evento ao(s) IC(s) associados

- Objetivo: Correlacionar o evento com algum IC;
- Entrada: Evento classificado como Aviso/Informativo;
- Saída: Evento correlacionado ao IC;
- Descrição: A equipe de monitoramento com auxílio da ferramenta de monitoramento deve relacionar o evento com algum item de configuração(IC). Caso não seja possível, deve seguir o processo normalmente informando ao setor responsável sobre a não identificação do IC.

7.1.5 Atividade: Direcionar o evento para o setor responsável

- Objetivo: Direcionar o evento para o setor responsável;
- Entrada: Evento correlacionado ao IC;
- Saída: Evento direcionado para o setor responsável;
- Descrição: A equipe de monitoramento deve direcionar o evento, se possível relacionado com algum IC, para o setor responsável o qual deve ficar em alerta sobre o evento.

7.1.6 Atividade: Analisar Evento Crítico

- Objetivo: Analisar o evento crítico e selecionar a melhor reação ;
- Entrada: evento ;
- Saída: Seleção da reação ao evento;
- Descrição: Selecionar a reação entre as opções disponíveis:
  - Abrir registro de incidente quando for identificada uma exceção ou quando uma considerável quantidade de avisos indica uma falha iminente;
  - Abrir uma requisição de mudança quando a exceção indica que é necessária uma mudança imediata, geralmente abre-se um incidente, mas pode ser que seja de fato uma mudança urgente.

7.1.7 Atividade: Ir para o processo de incidente e enviar para o setor responsável

- Objetivo: Enviar para o processo de incidente e para o setor responsável;
- Entrada: Evento;
- Saída: Ir para o processo de incidente ;
- Descrição: Caso o evento seja um incidente deve-se abrir um chamado do tipo incidente e no chamado informar qual o setor responsável pelo tratamento.

7.1.8 Atividade: Ir para o processo de mudança e enviar para o setor responsável

- Objetivo: Enviar para o processo de mudança e para o setor responsável;
- Entrada: Evento;
- Saída: Ir para o processo de mudança;
- Descrição: Caso a reação seja uma abertura de uma requisição de mudança(RDM) deve-se seguir para o processo de mudança e abrir a RDM via sistema.

8. Entradas e Saídas

8.1 Entradas

- Dados de monitoramento dos ICs e Serviços;

8.2 Saídas

- Evento encaminhado para o setor responsável;
- Abertura de incidente;
- Ir para o processo de mudança;

9. Papéis e responsabilidades

Papel	Quem exerce o papel	Responsabilidades
Dono do Processo	Servidor da área de TIC formalmente designado	• Analisar relatórios e indicadores de desempenho; • Coletar os indicadores do processo; • Propor mudanças no processo; • Autorizar mudanças no processo; • Remover impedimentos para a execução do processo; • Prover recursos para a execução das atividades do processo.
Unidade Responsável pelo Monitoramento	NITIC / NAU	• Monitoramento • Detecção de evento; • Classificação do evento; • Correlacionar o Evento ao(s) IC(s) associados; • Direcionar o evento para o setor responsável; • Analisar evento crítico; ; • Ir para o processo de incidente e enviar para o setor responsável; • Ir para o processo de mudança e enviar para o setor responsável;

10. Indicadores de desempenho

10.1 Percentual de Ativos que tenham monitoramento ativado

- Objetivo: medir a percentual de ativos que estejam sendo monitorados;
- Fonte: ferramenta de monitoramento;
- Periodicidade da medição: mensal;
- Regra de cálculo: (quantidade de ativos monitorados/quantidade total de ativos);
- Meta: 95%;
- Polaridade: quanto maior melhor;
- Responsável pela coleta : dono do processo;

11. Melhorias Futuras

- Analisar a possibilidade de criação de novos indicadores para monitorar a execução deste processo;
- Incluir indicador para percentual de Incidentes Identificados no Monitoramento
- Revisões futuras no processo.