Processo de Gerenciamento de Eventos de TIC

SETIC - Secretaria de Tecnologia da Informação e Comunicação

Gestor do Processo: Coordenador de Infraestrutura e Serviços
Área responsável: Coordenadoria de Infraestrutura e Serviços

JOENIR JOSE DELLA FLORA
11/09/2023 10:31

ROMULO VALENTE FERREIRA
11/09/2023 11:28

OBJETIVO

Definir os procedimentos para o monitoramento e o tratamento de eventos relacionados à tecnologia da informação e comunicação, através da descrição das atividades correspondentes ao processo de gerenciamento de eventos de TIC.

DEFINIÇÕES GERAIS PARA A ADEQUADA EXECUÇÃO DESTE PROCESSO

Para o gerenciamento de Eventos de TIC, há dois conceitos básicos fundamentais que sustentam suas atividades:

Agentes de Monitoramento: Os Agentes de Monitoramento são softwares instalados nos componentes de infraestrutura de TIC (servidores, roteadores, switches, sistemas operacionais, entre outros), sendo responsáveis pela coleta de dados sobre o estado, desempenho e eventos desses componentes, armazenando informações sobre uso de recursos, disponibilidade, erros, tempos de resposta e muito mais. Quando um agente de monitoramento detecta um evento, ele o registra localmente e, dependendo da sua configuração, pode enviar esse evento para um sistema centralizado que realiza o gerenciamento de eventos, podendo acionar alertas para as equipes de suporte e monitoramento de recursos de infraestrutura.

Banco de Dados de Gestão de Configuração (BDGC): é uma base de dados centralizada, responsável por armazenar informações detalhadas sobre todos os ativos de serviço e componentes da infraestrutura de TIC. Ele mantém registros sobre a configuração, relacionamentos e histórico de mudanças relacionado a cada ativo registrado, fornecendo uma visão abrangente da infraestrutura de TIC e seus componentes. O BDGC é de grande importância para o gerenciamento de mudanças, resolução de incidentes, análise de problemas e planejamento de capacidade.

Em conjunto, os Agentes de Monitoramento e o Banco de Dados de Gestão de Configuração desempenham um papel fundamental no monitoramento proativo da infraestrutura de TIC, na detecção de eventos relevantes, na resposta a incidentes e na manutenção precisa das informações de configuração, permitindo que os responsáveis pela sua gestão, operem de maneira eficiente, identificando problemas e tomando medidas corretivas de forma ágil.

O Gerenciamento de Eventos de TIC desempenha uma função crucial no fornecer informações em tempo real sobre o estado e o comportamento dos serviços e infraestrutura de TIC. Isso afeta diretamente vários outros processos de gerenciamento de serviços de TIC, permitindo realizar uma operação mais eficiente e também uma identificação precoce de problemas, a fim de manter níveis de serviço de alta qualidade.

INTERFACE COM DEMAIS PROCESSOS

- **Gerenciamento de Incidentes de TIC:** Os incidentes são detectados por meio de eventos, e esses eventos podem acionar a abertura de chamados. Além disso, o processo de gerenciamento de eventos pode fornecer informações úteis para a resolução rápida de incidentes.

- **Gerenciamento da Capacidade de TIC:** O Gerenciamento de Eventos auxilia o Gerenciamento da Capacidade, fornecendo informações sobre o comportamento do sistema e possíveis mudanças na demanda ou desempenho, auxiliando na identificação de padrões de uso e na previsão de necessidades futuras de capacidade.

- **Gerenciamento de Disponibilidade de TIC:** Através do monitoramento de eventos que podem indicar indisponibilidade ou interrupções nos serviços, o processo de gerenciamento de eventos contribui para a garantia de alta disponibilidade dos serviços de TIC.

- **Gerenciamento da Configuração e Ativos de Serviço:** O processo de gerenciamento de eventos fornece informações sobre as alterações e os estados dos ativos de serviços e componentes de infraestrutura. Assim, esses eventos são registrados no banco de dados de gerenciamento da configuração, auxiliando na manutenção de registros atualizados sobre a configuração e ativos.

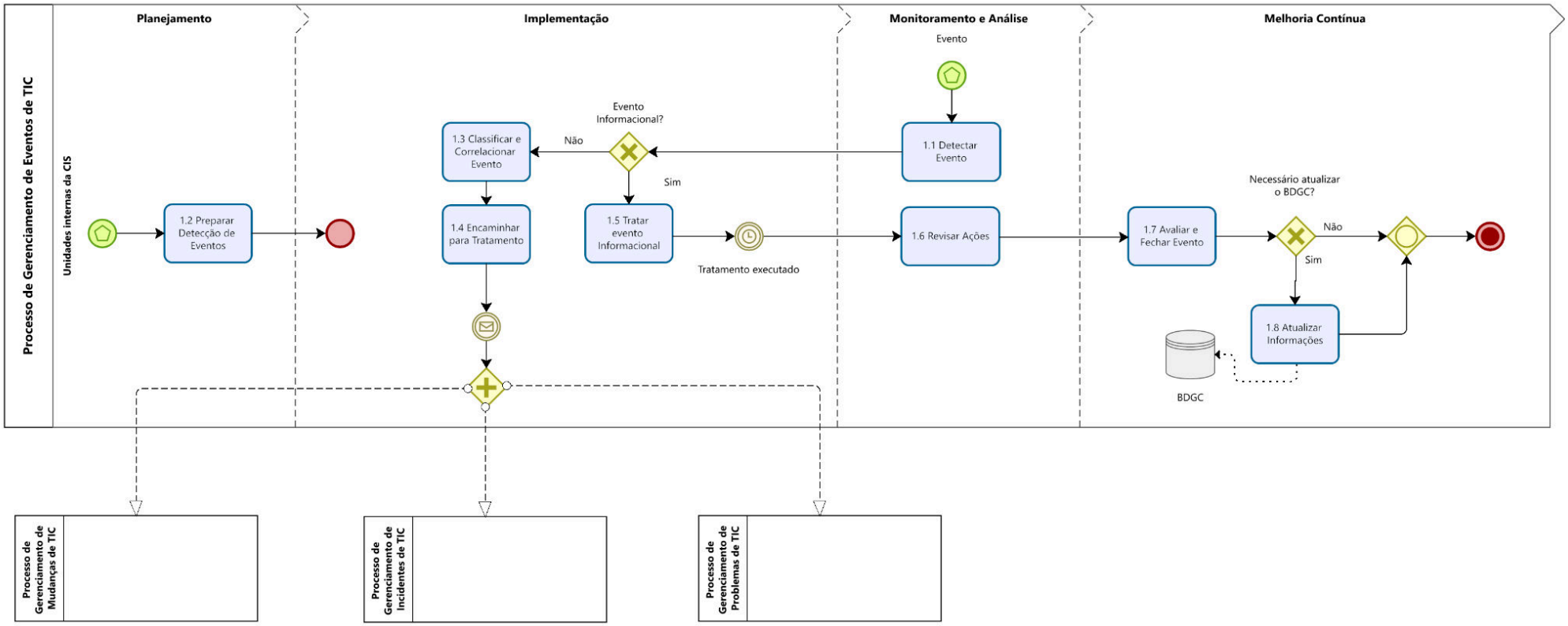
- **Gerenciamento de Nível de Serviço:** Uma vez que eventos relacionados ao desempenho, disponibilidade e qualidade dos serviços podem impactar diretamente os níveis acordados de serviço, monitorar eventos ajuda a identificar desvios dos níveis de serviço esperados.

- **Gerenciamento de Problemas:** Fornecer informações sobre eventos repetitivos, recorrentes ou críticos. Esses eventos podem ser indicativos de problemas subjacentes na infraestrutura ou nos serviços, ajudando o analista de problemas a investigar e resolver problemas de forma proativa.

FLUXOGRAMAS DESTE PROCESSO

Processo 1.0. Gerenciamento de Eventos de TIC

Fluxo principal do Processo de Gerenciamento de Eventos de TIC



DESCRIÇÃO DAS ATIVIDADES DO FLUXOGRAMA 1.0. GERENCIAMENTO DE PROBLEMAS DE TIC			
Nome da atividade	**Objetivo**	**Responsável**	**Tarefas / Ações**
1.1 Detectar Evento	Identificar e registrar um evento	Unidades internas da CIS	**Entrada:** Notificação de evento **Tarefas:** ● Uma vez que uma notificação de evento tenha sido gerada, o evento será detectado por um agente de monitoramento, que interpretará o seu significado. **Saída:** Evento detectado
1.2 Preparar Detecção de Eventos	Realizar a análise e planejamento para a detecção de eventos	Unidades internas da CIS	**Entrada:** Plano de Capacidade e Disponibilidade; Solicitação de monitoramento **Tarefas:** ● Identificar e analisar os Planos de monitoramento de Capacidade, os Planos de monitoramento de Disponibilidade, histórico de incidentes e problemas e outras solicitações de monitoramento para determinar os serviços e itens de configuração a serem monitorados. ● Pesquisar a existência de agentes de monitoramento proprietários dos fabricantes dos ICs. Se não houver, pesquisar outros agentes, inclusive baseados em software livre ou métodos para detectar os eventos identificados. ● Implementar e testar as ferramentas de monitoramento e notificação escolhidas. ● Discriminar quais os eventos que serão notificados e quais serão ignorados, e determinar quem será notificado nos casos apropriados. ● Definir o tempo de vida útil dos eventos registrados. Eles deverão ser excluídos após esse período, para economicidade de espaço em disco. **Saída:** Detecção de evento preparada.
1.3 Classificar e Correlacionar Evento	Classificar, priorizar e correlacionar ao tratamento correspondente ao evento	Unidades internas da CIS	**Entrada:** Evento detectado **Tarefas:** ● É sugerido que os eventos sejam colocados em três categorias básicas: ○ **Informacionais**: eventos que indicam uma operação normal, ou seja, indicam que o serviço está funcionando; ○ **Alertas**: eventos que indicam uma operação anormal, como quando o usuário tenta entrar na aplicação e não

			consegue e um log é registrado com esta informação; ○ **Exceção**: eventos que sinalizam uma operação não usual, mas que não é excepcional. Esses eventos, em geral, geram uma notificação de incidente, problema ou RdM. ● Ao fazer a correlação, apontando detalhes do evento, é necessário que se determine o nível e o tipo de impacto no negócio. Pode-se dizer que se um evento é significativo, ele deve ser registrado e uma ação precisa ser tomada. **Saída:** Evento classificado e correlacionado.
1.4 Encaminhar para Tratamento	Realizar o encaminhamento para tratamento do evento	Unidades internas da CIS	**Entrada:** Evento classificado e correlacionado. **Tarefas:** ● A resposta aos eventos informacionais são feitas automaticamente através de scripts ou dos sistemas de monitoramento. Exemplos de auto resposta: reboot de um dispositivo; reinicialização de serviço; submissão de job; mudança de configuração de dispositivo; bloqueio de dispositivo ou aplicação contra acessos não autorizados. Neste caso, o evento será tratado na atividade 1.4. ● Caso o evento gerado seja uma exceção, após ser classificado e correlacionado, os responsáveis pelo monitoramento devem encaminhar o evento para seu respectivo processo de tratamento, conforme sua classificação (Processo de Gerenciamento de Incidentes de TIC, Processo de Gerenciamento de Mudanças de TIC; Processo de Gerenciamento de Problemas de TIC). ● **Saída:** Evento encaminhado
1.5 Tratar Evento Informacional	Tratar o evento não classificado como exceção	Unidades internas da CIS	**Entrada:** Evento encaminhado **Tarefas:** ● A resposta aos eventos informacionais devem ser feitas automaticamente através de scripts ou dos sistemas de monitoramento. Exemplos de auto resposta: reboot de um dispositivo; reinicialização de serviço; submissão de job; mudança de configuração de dispositivo; bloqueio de dispositivo ou aplicação contra acessos não autorizados. **Saída:** Evento informacional encaminhado
1.6 Revisar Ações	Verificar se o evento foi tratado	Unidades internas da CIS	**Entrada:** Evento encaminhado; Evento informacional encaminhado **Tarefas:** ● Caso o evento for do tipo informacional, verificar se as ações de tratamento foram suficientes para tratá-lo.

			• Caso o evento tenha sido encaminhado para outro processo para tratamento, deve-se verificar se o evento foi tratado pelo seu processo correspondente, após o prazo informado por seu respectivo gestor. • Após aguardar o tratamento do evento, encaminha para o fechamento deste. **Saída:** Evento revisado
1.7 Avaliar e Fechar Evento	Encaminhar para finalização do tratamento do Evento	Unidades internas da CIS	**Entrada:** Evento revisado **Tarefas:** No gerenciamento de eventos de TIC, para comparar o desempenho e o comportamento operacional atual com os padrões de desenho e Acordos de Nível de Serviço (SLAs), é necessário implementar procedimentos e práticas específicas, dessa forma, isso ajudará a garantir que os serviços de TIC estejam operando de acordo com as expectativas e requisitos acordados. As tarefas que ajudam a realizar esse alinhamento são: • **Documentar Desvios e Ações Corretivas:** Caso haja desvios em relação aos padrões de desenho ou SLAs, é necessário realizar a documentação detalhada e iniciar ações corretivas para abordar esses problemas. • **Implementar Melhorias Contínuas:** Identificar áreas de melhorias após a coleta das informações relacionadas ao evento em questão. Essas melhorias podem ser implementadas no processo de gerenciamento de eventos ou em outras áreas relacionadas. • **Relatórios de Conformidade:** Gerar relatórios periódicos que destaquem o alinhamento ou a falta deste, entre o desempenho atual e os padrões de desenho e SLAs. **Saída:** Evento tratado
1.8 Atualizar Informações	Atualizar as informações relacionadas ao evento no BDGC	Unidades internas da CIS	**Entrada:** Evento tratado **Tarefas:** • Atualizar o BDGC com as informações registradas durante o ciclo de tratamento do evento. **Saída:** informações atualizadas

PAPÉIS E RESPONSABILIDADES		
Papel	**Responsabilidades**	**Responsável**
Dono do processo	• Conduzir todo o processo, dentro de todas as equipes de soluções. • Desenvolver e manter o processo; • Garantir a efetividade do Processo; • Possui a autoridade máxima em relação ao processo, garantindo sua especificação e execução.	Coordenador de Infraestrutura e Serviços
Central de Serviços	• Comunicar informações para quem for necessário, investigar e resolver eventos.	Servidor designado de TIC que presta suporte à Central de Serviços
Unidades internas da CIS	• Monitorar o ambiente; • Investigar os eventos; • Realizar o tratamento dos eventos.	Servidores lotados em unidades da Coordenadoria de Infraestrutura e Serviços da SETIC que monitoram a infraestrutura e os serviços de TIC

GLOSSÁRIO

Acordo de Nível Operacional (ANO): Um contrato entre um provedor de serviços de TI e outra parte da mesma organização, visando suporte para a entrega dos serviços de TI a clientes, definindo responsabilidades de ambas as partes.

Acordo de Nível de Serviço (ANS): Um contrato entre um provedor de serviços de TI e um cliente que descreve o serviço, documenta metas de nível de serviço e especifica as responsabilidades do provedor e do cliente.

Agente de monitoramento: Programas instalados nos ICs para coletar seus eventos e gerar alertas específicos.

Banco de Dados de Gerenciamento de Configuração (BDGC): Um banco de dados usado para armazenar os registros da configuração durante todo o seu ciclo de vida. O sistema de gerenciamento de configuração mantém um ou mais bancos de dados de gerenciamento de configuração, e cada banco de dados armazena atributos de itens de configuração (IC) e relacionamentos com outros itens de configuração.

Categoria: Um grupo nomeado de itens que tenham algo em comum. Categorias são usadas para agrupar itens similares. Por exemplo: categorias de incidente são usadas para agrupar tipos similares de incidentes, tipos de IC são usados para agrupar itens de configuração similares e assim por diante.

Classificação: O ato de associar uma categoria a algo, usada para garantir consistência no gerenciamento e nos relatórios. Itens de configuração, incidentes, problemas, mudanças, etc., são normalmente classificados.

Chamado: refere-se a um registro genérico, quando feito por um solicitante e registrado em ferramenta de gerenciamento de incidente pela Central de Serviços. Este chamado pode fazer referência a um incidente ou solicitação de serviço.

Evento: Uma mudança de estado que possui significado para o gerenciamento de um item de configuração ou serviço de TI. Evento também é o termo usado para quando um alerta ou notificação é criado por qualquer serviço de TI, item de configuração ou ferramenta de monitoração. Eventos geralmente requerem uma ação da equipe de operações de TI e às vezes podem levar à geração e registro de incidentes.

Incidente: Uma interrupção não planejada de um serviço de TI ou uma redução da qualidade de um serviço de TI. A falha de um item de configuração que ainda não afetou o serviço também é um incidente, por exemplo, a falha em um disco de um conjunto espelhado.

Indisponibilidade: O tempo em que um serviço de TI ou outro item de configuração não está disponível durante o tempo de serviço acordado. A disponibilidade de um serviço de TI normalmente é calculada a partir do tempo de serviço acordado e sua indisponibilidade.

Item de Configuração (IC): Qualquer componente ou outro ativo de serviço que precisa ser gerenciado de forma a entregar um serviço de TI. As informações sobre cada item de configuração são registradas em um registro de configuração no sistema de gerenciamento de configuração e é mantido por todo o seu ciclo de vida pelo Processo de Gerenciamento de Configuração e Ativo de Serviço. Os itens de configuração estão sob o controle do Processo de Gerenciamento de Mudança. Eles incluem tipicamente hardware, software, instalações, pessoas e documentos formais tais como documentação de processos e acordos de nível de serviço.

Prioridade: Uma categoria usada para identificar a importância relativa de um incidente, problema ou mudança. A prioridade é baseada em impacto e urgência, e é usada para identificar os tempos requeridos para que ações adequadas sejam tomadas.

Registro de Incidente: Um registro contendo os detalhes de um incidente. Cada registro de incidente documenta o ciclo de vida de um incidente.

Requisição de Mudança (RDM): O acréscimo, modificação ou remoção de qualquer coisa que possa afetar serviços de TI. O escopo deve incluir mudanças a todos os processos, arquiteturas, ferramentas, métricas e documentação, além de mudanças em serviços de TI e outros itens de configuração.

Serviço de TI: Um serviço fornecido por um provedor de serviço de TI. Um serviço de TI é composto de uma combinação de tecnologia da informação, pessoas e processos. Um serviço de TI voltado para o cliente suporta diretamente os processos de negócio de um ou mais

clientes e convém que as suas metas de nível de serviço sejam definidas em um acordo de nível de serviço.

Solicitação de Serviço: Uma requisição formal de um usuário para algo a ser fornecido, por exemplo, uma requisição para informações, para redefinir uma senha ou para instalar uma estação de trabalho para um novo usuário. As solicitações de serviço são gerenciadas pelo processo de Cumprimento de Requisição, normalmente em conjunto com a Central de Serviço. As solicitações de serviço podem estar vinculadas a uma requisição para mudança como parte do cumprimento da requisição.

SETIC - Secretaria de Tecnologia da Informação e Comunicação do Tribunal Regional do Trabalho da 14a Região.

Tecnologia da Informação e Comunicação (TIC) - Compreende a infraestrutura e os componentes que viabilizam a computação moderna. São os elementos, que combinados, permitem às pessoas e organizações interagirem no mundo digital.

Urgência: Uma medida de quanto tempo um incidente, problema ou mudança irá levar até que tenha um impacto significativo no negócio. Por exemplo, um incidente de alto impacto pode ter urgência baixa se o impacto não afetar o negócio até o final do ano financeiro. O impacto e a urgência são usados para designar a prioridade.

Usuários: Magistrados, servidores, advogados, peritos, membros do Ministério Público, estagiários, terceirizados, pessoas que se encontrem a serviço da Justiça do Trabalho e qualquer outro usuário externo, desde que autorizados, que estejam acessando, em caráter temporário ou definitivo, os serviços e recursos tecnológicos oferecidos pelo TRT da 14ª Região.

INDICADORES E METAS

Indicador - Taxa de Falsos Positivos	
Descrição	Mede a precisão do sistema de detecção de eventos, avaliando quantos eventos falsos positivos (alertas incorretos) são gerados.
Responsável pela medição	Coordenador de Infraestrutura e Serviços
Local da medição	Coordenadoria de Infraestrutura e Serviços
Instrumento de captação	Banco de Dados da ferramenta de gerenciamento de serviços de TI; Agentes de Monitoramento
Periodicidade da medição	Anual
Fórmula	(Número de eventos de TIC identificados como Falsos Positivos / Número de eventos de TIC registrados) * 100

Meta	<20% OBS: As metas para os anos seguintes serão definidas na revisão deste documento, após a obtenção dos resultados do primeiro ciclo de execução do processo.

REFERÊNCIAS

Processo de Gerenciamento de Eventos de TIC do TRT13:
https://www.trt13.jus.br/institucional/gestao-estrategica/governanca/projetos-e-servicos/processos-de-tic/gestao-de-eventos/manual-do-processo-de-gerenciamento-de-eventos-de-tic.pdf

Processo de Gerenciamento de Eventos de TIC do TRT18:
https://www.trt18.jus.br/portal/arquivos/2023/03/Processo-de-Gerenciamento-de-Eventos-vs.0.0.pdf

Processo de Gerenciamento de Eventos de TIC do TRT22:
https://www.trt22.jus.br/arquivos_portal//downloads/Modelo%20do%20Processo%20de%20Gerenciamento%20de%20Eventos.pdf

Processo de Gerenciamento de Eventos de TIC do TRT23:
https://portal.trt23.jus.br/portal/sites/portal/files/groups/cic/governancatic/processo_de_gerenciamento_de_eventos_de_tic.pdf

DESTINAÇÃO DO PROCESSO

Servidores da Secretaria de Tecnologia da Informação e Comunicação.

OUTRAS INFORMAÇÕES DESTE PROCESSO

Elaboração: Rômulo Valente Ferreira	**Data:** 01/09/2023
Revisão: Joenir José Della Flora	**Data:** 01/09/2023
Data de aprovação formal:	

Histórico de Revisões			
Data	**Versão**	**Descrição**	**Responsável**
01/09/2023	1.0	Versão inicial do documento	Rômulo Valente Ferreira