



TRIBUNAL DE JUSTIÇA
DO ESTADO DO PARÁ
SECRETARIA DE INFORMÁTICA

PGE

Processo de
Gerenciamento de Eventos

2021

Conforme Pinkverify
ITSM 12º Processo ITIL 4



Membros Envolvidos na Construção do Processo GE – 12º ITSM

Secretário Adjunto de Informática - TJPA

Miguel Pernambuco – Requisitante

Coordenadoria de Atendimento Ao Usuário - TJPA

Felipe Moraes Freitas – Avaliador

Serviço de Registro e Execução ao Atendimento - TJPA

Ramon Santos Nascimento – Avaliador

Coordenador de Nível de Serviços - LANLINK

James Mormax Jr. – Liberação

Gestor de Processos e Equipe Técnica - LANLINK

Alexander Quaresma Tschertasch – Projetista

Analista de Capacitação e Implementação de Soluções - LANLINK

Kelly Bruna Nascimento de Oliveira – Análise ortográfica



Histórico de Versões

DATA	VERSÃO	DESCRIÇÃO	PROJETISTA	APROVADOR
08/10/2021	1.0	Elaboração	ALEXANDER TSCHERTASCH	RAMON NASCIMENTO



SUMÁRIO

1. Introdução.....	05
1.1. Objetivo.....	06
1.2. Definições.....	06
2. Entradas.....	07
3. Subprocessos.....	08
3.1. Ocorrência do Evento.....	08
3.2. Notificação do Evento.....	08
3.3. Detecção do Evento.....	08
3.4. Filtro do Evento.....	09
3.5. Significância do Evento.....	09
3.6. Correlação do Evento.....	09
3.7. Direcionar.....	09
3.8. Selecionar Reação.....	10
4. Saídas.....	10
5. Responsabilidades dos Gerentes dos Serviços de TI.....	10
6. Níveis de Gerenciamento de Eventos.....	11
7. Fluxo Grama do Gerenciamento de Eventos.....	12
8. Gerenciamento de Impacto e Probabilidade.....	12
9. Matriz de Potencialidade.....	14
10. Recomendações.....	17

1. INTRODUÇÃO

Um evento pode ser definido como uma ocorrência ou mudança de estado que possui relevância para o gerenciamento de um serviço de TI ou IC. Muitos eventos acontecem no ambiente da TI. O monitoramento ativo desses eventos serve para precaver-se de incidentes, garantir o cumprimento do ANS e verificar se o serviço está sendo executado de acordo com sua operação normal.

No ciclo de Desenho do serviço de TI, devem ser definidos quais eventos serão monitorados.

Os eventos podem ser divididos em 05 categorias:

CATEGORIA	IDENTIFICAÇÃO
INFORMAÇÃO	Evento REGULAR
ADVERTÊNCIA	Evento NÃO TÃO USUAL
MODERADO	Evento conhecido como NORMAL
ELEVADO	Evento que indica ALTO IMPACTO
TRÁGICO	Evento com criticidade MAIS ALTA

Plan. 01

INFORMATIVO: Não requerem ação. Para cada serviço devem ser definidos que eventos precisam ser registrados a título informativo. Ex: backups automáticos do APT realizados com sucesso, rotinas de segurança de redes concluídas com sucesso.

ADVERTÊNCIA: É um evento não tão usual. Quando o IC está operando próximo do limite definido como aceitável.

MODERADO: Evento gerado quando um serviço ou IC está próximo a uma situação limite para tomada de providências. No ciclo de Desenho devem ser definidos os limites (threshold) para cada serviço. Ex: percentual de capacidade ocupada em storage, limites de capacidade de processamento de servidores.

ELEVADO: 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.



TRÁGICO: É o evento com criticidade mais alto, indicando que o ambiente está totalmente afetado, ou seja, operação parada. Este é o pior cenário possível dentro das classificações de eventos e indica que o IC, ou, conjunto de ICs que geraram o evento estão indisponíveis.

1.1. Objetivo

O objetivo do processo de Gerenciamento de Eventos é monitorar e gerar alertas ou notificações de um Serviço de TI ou item de Configuração considerados relevantes para os processos de gerenciamento de serviços de TI e para cumprimento dos ANS.

1.2. Definições

- **AGENTES DE MONITORAMENTO OU PROGRAMAS DE MONITORAMENTO:** São programas instalados nos ICs para coletar seus eventos e gerar alertas específicos.
- **ANS:** Acordo de nível de serviço.
- **CENTRAL DE SERVIÇOS:** Função definida na ITIL Versão 3. É o ponto único de contato para os usuários de TI. Tem por objetivo restaurar a operação normal dos serviços o mais rápido possível.
- **EVENTO:** Qualquer ocorrência considerada relevante no serviço de TI.
- **DONO DO PROCESSO:** É o chefe da seção responsável pelo serviço de tecnologia da informação definido no portfólio de processos.
- **REQUISIÇÃO DE SERVIÇO:** Pedido de informação para uma mudança ou para acessar um serviço de TI. Geralmente não requer uma requisição de Mudança (RDM).
- **ALERTA:** Aviso ou advertência sobre uma meta, mudança ou falha que ocorreu. Controlado por ferramentas de gerenciamento de sistemas e pelo processo de gerenciamento de Evento. Exemplo: Uso de memória RAM do servidor de e-mail ultrapassou 75%, não é registrado como um incidente é apenas um aviso.



- **INCIDENTE:** É uma interrupção inesperada ou redução na qualidade de um serviço de TI. Falha de um IC.
- **PROBLEMA:** Causada por um ou mais incidente.
- **SOLUÇÃO DE CONTORNO (WORKAROUND):** Meio temporário de resolver questões ou dificuldades. Ex : Reiniciar o servidor. Essas soluções para incidentes que não tem um registro de problema associado são documentadas dentro do próprio registro de incidente. Para soluções de contorno para problemas são registradas e documentadas nos registros de erros conhecidos.
- **ERRO CONHECIDO (KNOWN ERROR):** É um problema que tem causa, raiz documentada e uma solução de contorno identificada. Erros conhecidos são colocados no processo de gerenciamento de Problema
- **BASE DE ERROS CONHECIDOS:** Local onde se registram erros conhecidos. Esses registros são utilizados pelo processo de gerenciamento de incidente para resolver incidentes. Faz parte de gerenciamento do conhecimento de serviço. Esta base pode ser disponibilizada para usuários fazerem autoatendimento via Catálogo de Serviços.

2. ENTRADAS

COMPETÊNCIA	ORIGEM	INFORMAÇÃO
CAU	Central de Serviços	Incidentes Reportados
CAU	Gerenciamento de Catálogo de Serviço	Serviços de Negócios
CAU	Gerenciamento de Configuração	Serviço de TI e ICs em produção
CAU	Gerenciamento de Nível de Serviço	Acordo de Nível de Serviço
CST	Gerenciamento de Disponibilidade	Monitoramento de Disponibilidade
CST	Gerenciamento de Capacidade	Monitoramento de Capacidade
CST	Gerenciamento de Segurança da Informação	Informações de Segurança

Plan. 02



3. SUBPROCESSOS

3.1. Ocorrência do Evento

Objetivo: Definir os eventos dos serviços que precisam ser detectados.

Responsabilizado: Secretário da informática (SECINFO).

Atividades:

- No ciclo de Desenho do serviço definir quais eventos precisam ser monitorados. Para isto, definir quais serviços de TI e quais IC terão seus eventos monitorados. Ex: PJE, servidores de internet, servidores de arquivos e outros.
- No ciclo de Operação atualizar a relação de eventos que precisam ser monitorados de acordo com histórico de incidentes, BDEC, problemas e ocorrências que possam comprometer a operação normal do serviço, inclusive na sua interação com outros serviços da TI. Exemplos: alteração da política de segurança, mudanças ocorridas após o ciclo de Desenho.

3.2. Notificação do Evento

Objetivo: Esse subprocesso ocorre no Ciclo de Transição do serviço e tem por objetivo definir como será feito o monitoramento do serviço para detectar os eventos definidos no subprocesso anterior.

Responsabilizado: Dono do Processo.

Atividades:

- Pesquisar a existência de agentes de monitoramento proprietários dos fabricantes dos ICs utilizados no serviço. Se não houver, pesquisar outros agentes, inclusive baseados em software livre.
- Implementar e testar as ferramentas de monitoramento e notificação escolhidas.

3.3. Detecção do Evento

Objetivo: Receber as notificações emitidas no subprocesso anterior e interpretá-las.

Responsabilizado: Dono do Processo.

Atividades:

- Definir e implementar a forma como serão recebidas as notificações e alertas. Ex: por e-mail, por mensagem de celular, relatórios diários, logs.
- Definir quem serão os responsáveis pelo monitoramento e as ações a serem tomadas após a detecção do evento.



3.4. Filtro do Evento

Objetivo: Discriminar quais eventos serão notificados e quais serão ignorados.

Responsabilizado: Dono do Processo.

Atividades:

- Analisar em cada IC ou serviço de TI, sob o Gerenciamento de Eventos, como será realizado o filtro de eventos. Assim, serão discriminados os eventos que serão notificados daqueles que serão ignorados.
- Definir o tempo de vida útil dos eventos registrados. Eles deverão ser excluídos após esse período, para economicidade de espaço em disco. Definir quem serão os responsáveis pelo monitoramento e as ações a serem tomadas após a detecção do evento.

3.5. Significância do Evento

Objetivo: Definir a categoria do evento.

Responsabilizado: Dono do Processo.

Atividades:

- Categorizar os eventos monitorados em informativo, aviso ou exceção;

3.6. Correlação do Evento

Objetivo: Relacionar o evento aos níveis de serviço e aos riscos para o negócio.

Responsabilizado: Dono do Processo.

Atividades:

- 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 a priorização do evento para os serviços.

3.7. Direcionar

Objetivo: Indicar para quem ou para onde os Eventos devem ser informados de acordo com a correlação.

Responsabilizado: Dono do Processo.

Atividades:

- Definir os setores ou pessoas que deverão tomar conhecimento sobre a ocorrência do evento para providências.
- Implementar resposta automática a eventos quando cabível. Ex: scripts para reiniciar processos ou executar Jobs.



3.8. Selecionar Reação

Objetivo: Definir as providências que serão tomadas para tratamento do evento.

Responsabilizado: Dono do Processo.

Atividades:

- SELECIONAR ENTRE AS OPÇÕES POSSÍVEIS DE REAÇÃO:
 - Se o evento é informativo, registrar em um arquivo de log para fins de análise;
 - Se já houver ação automatizada prevista para o evento, implementar resposta automática, tal como: iniciar um job, reiniciar uma aplicação, aplicar uma rotina, acionar software de segurança;
 - Se for um alerta, solicitar intervenção humana para tratamento;
 - Se for uma exceção ou indicativo de falha, encaminhar para a Central de Serviços via abertura de Registro de Incidente e informar o gerente do serviço.

4. SAÍDAS

DESTINO	INFORMAÇÃO
Todos os processos	Informações sobre eventos para gerenciamento, ações preventivas, análise de riscos, análise de tendências em ICs e serviços da TI.
Gerenciamento de Incidentes e Central de serviços	Abertura de Registro de Incidentes

Plan. 03

5. RESPONSABILIDADES DOS DONOS DOS PROCESSOS DE TI

Não é previsto no framework ITIL o papel de Gerente de Eventos, devido ao contexto amplo que se estende por todas as áreas da TI. Cada gerente de Serviço de TI em conjunto com o diretor da SETIC deverá definir os eventos relevantes na sua área e executar as demais atividades do processo. O Framework ITIL prevê a seguinte estrutura organizacional:



FUNÇÃO	PAPEL NO PROCESSO
Central de Serviços	Informações sobre eventos para gerenciamento, ações preventivas, análise de riscos, análise de tendências em ICs e serviços da TI.
Gerenciamento de Operações de TI	Monitorar eventos e fornecer suporte inicial
Gerenciamento Técnico e da Aplicação	Definir e gerenciar os eventos

Plan. 04

6. NÍVEIS DE GERENCIAMENTO DE EVENTOS

NÍVEL	IDENTIFICAÇÃO
SUPERFICIAL	Inicialmente considerando apenas na fase de implantação com disposição à abrangência.
NESSÁRIO	Uma perspectiva aos índices de monitoramento dos eventos de criticidades pertinentes com disposição à abrangência.
RECOMENDADO	Planejamento, automação, participação dedicada de proprietário do processo no monitoramento continuado dos impactos e probabilidades existente ao negócio do cliente com disposição à abrangência.
APRIMORADO	Aplicabilidade das práticas no definidas no processo de certificação ITSM 12º Processo PinkVerify.

Plan. 05

7. FLUXO GRAMA DO GERENCIAMENTO DE EVENTOS

O diagrama em questão faz relação ao NÍVEL SUPERFICIAL, onde deve ser inicialmente considerando apenas na fase de implantação com disposição à abrangência.

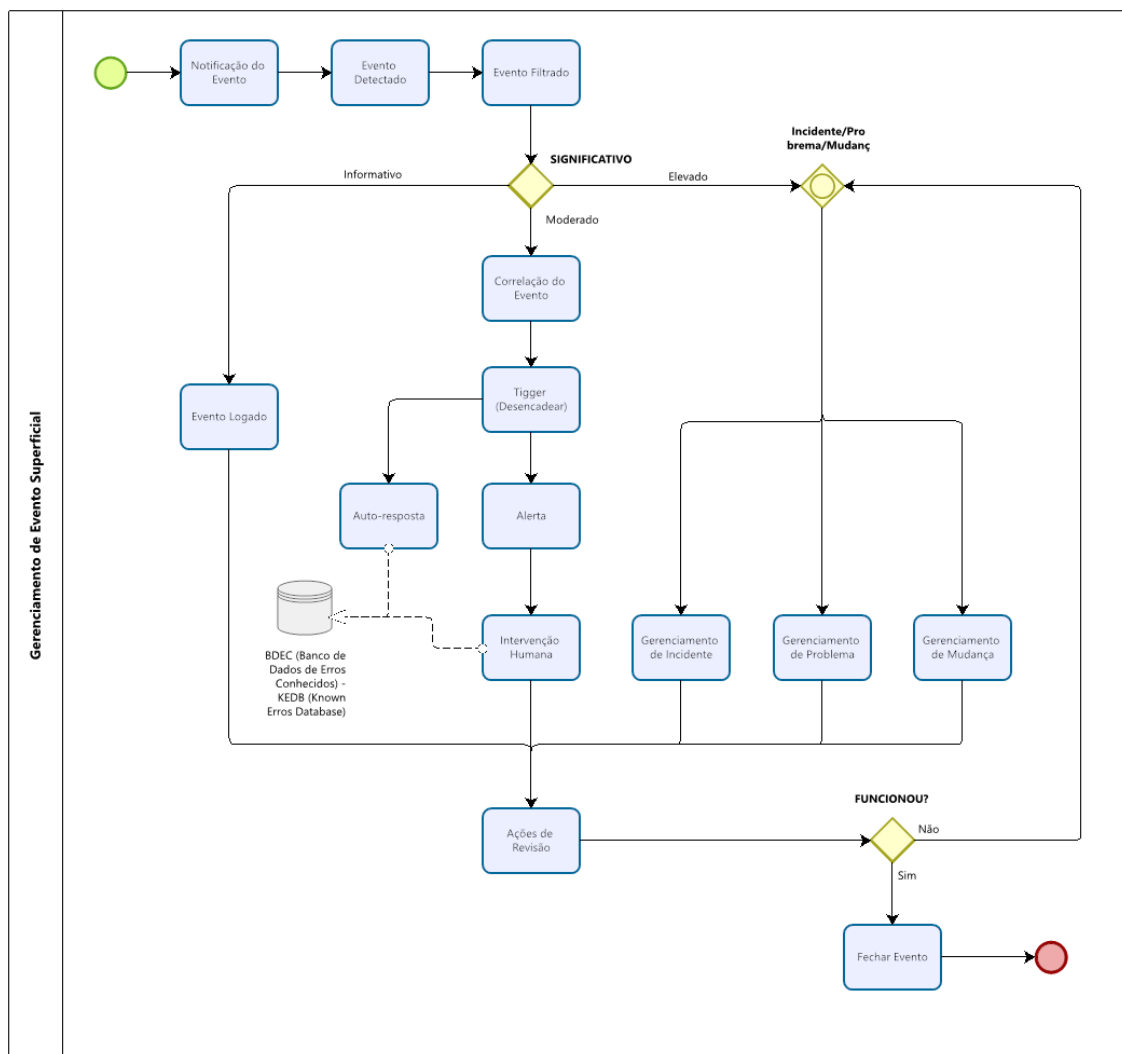


Fig. 01

8. MATRIZ DE IMPACTO E PROBABILIDADE

A Matriz de Riscos ou Matriz de Probabilidade, aqui a utilizaremos para representar as categorias quanto a sua criticidade dentro do Gerenciamento de eventos, sobretudo com o intuito de visarmos também o gerenciamento de riscos que permite de forma visual identificar quais são os riscos que devem receber mais atenção. Essa Acurácia parametrizada está em conformidade com impactos e probabilidade observando principal atividade do cliente.



IMPACTO	Trágico	5	Risco Moderado	Risco Alto	Risco Crítico	Risco Crítico	Risco Crítico
	Elevado	4	Risco Moderado	Risco Alto	Risco Alto	Risco Crítico	Risco Crítico
	Moderado	3	Risco Pequeno	Risco Moderado	Risco Alto	Risco Alto	Risco Crítico
	Advertência	2	Risco Pequeno	Risco Moderado	Risco Moderado	Risco Alto	Risco Alto
	Informação	1	Risco Pequeno	Risco Pequeno	Risco Pequeno	Risco Moderado	Risco Moderado
			1	2	3	4	5
			PROBABILIDADE				
			Muito Baixo	Baixo	Possível	Alto	Muito Alto

Fig. 02

A probabilidade (eixo vertical) consiste na medição de o quão provável é a ocorrência do risco. Em outras palavras, na probabilidade deve-se analisar o quão fácil ou difícil é que determinado risco aconteça, por exemplo, medir o quão provável é que chova hoje? A probabilidade deve ser medida em níveis, por exemplo: muito baixo, baixo, moderado, alto e muito alto. Essas probabilidades também podem ser convertidas em números (porcentagens) para facilitar o entendimento, sendo:

muito baixo = 1 a 10%;

baixo = 11% a 30%;



moderado = 31% a 50%;

alto = 51% a 70%;

muito alto = 71% a 90%.

O impacto (eixo horizontal) se refere às consequências do risco caso ele vier a ocorrer, ou seja, quais serão os prejuízos ou danos causados caso o risco incida de fato. O impacto pode ser negativo por exemplo, prejuízo financeiro, perda de clientes, dano à equipamento, etc; ou ainda, positivo, como novas oportunidades de negócio, utilização de uma nova tecnologia, redução de taxas ou impostos, etc. O impacto também é medido em níveis, por exemplo: muito baixo, baixo, moderado, alto e muito alto.

Relação Probabilidade e Impacto na Matriz de Riscos

É importante destacar que tanto para o impacto quanto para a probabilidade é possível definir a quantidade de níveis que desejar. Como explicado acima e pode ser visto na Figura 2, a matriz apresentada é composta por 5 níveis verticais (probabilidade) e 5 horizontais (impacto).

Em relação à definição dos níveis das dimensões, é necessário se atentar para que a quantidade de níveis para probabilidade e impacto sejam as mesmas, por exemplo, se for decidido que a probabilidade será apenas baixa, média e alta (3 níveis) o impacto pode ser insignificante, moderado ou catastrófico, ou seja, 3 níveis também

9. MATRIZ DE POTENCIALIDADE

Matriz de potencialidade é uma ferramenta que contribui para que os membros de uma equipe visualizem de forma mais clara os seus papéis e responsabilidades dentro de um determinado projeto.

A ideia é evitar possíveis falhas na distribuição das tarefas ou dúvidas sobre a quem pertence cada atividade. Problemas como esses podem não só comprometer a



gestão de pessoal, mas também impactar negativamente no desenvolvimento e na entrega dos resultados.

CONDICIONAM RE/PR	GLPI	POWER BI R S	ZABBIX	**POT	*REF MED DE POT
APROVEITAMENTO	40%	27,5%	20%	29,16%	90%
DISPONIBILIDADE	60%	62,5%	45%	55,83%	95%
SUORTE CERTIFICADO	X%	X%	X%	X%	85% (RMMP)
ACESSO	X%	X%	X%	X%	100%
MONITOR CONT	100%	100%	100%	100%	100%
TOMADA DE DECISÃO AUTOMATIZADA	0%	0%	0%	0%	25%
RELEVÂNCIA TÉCNICA	80%	55%	70%	68,33%	100%

Plan. 06

8.1. Formulas de Matiz de Potencialidade

Formula **POT

** : POTENCIALIDADE

$$\frac{SPFM}{QFM} = ** PFM$$

SPFM: SOMA DOS PERCETUAIS DAS FERRAMENTAS DE MONITORAMENTO

QFM: QUANTIDADE DE FERRAMENTAS DE MONITORAMENTO

PFM: POTENCIALIADE DA FERRAMENTE DE MONITORAMENTO

Formula *RMMP

* : REFERENCIA MÉDIA DE MÉDCIA DE POTENCIALIDADE



SPFM = ** PFM QFM

RMP: VALOR DE REFERENCIA COMO INDICADOS APROPRIADO SUGERIDO

QFM: QUANTIDADE DE FERRAMENTAS DE MONITORAMENTO

PFM: POTENCIALIADE DA FERRAMENTE DE MONITORAMENTO

Os principais pontos considerados são:

- **APROVEITAMENTO:** O quando está se fazendo uso dos recursos disponibilizados pela solução;
- **DISPONIBILIDADE:** Quanto tempo a solução está e pode permanecer e constante funcionalidade sem interrupção;
- **SUPORTE PROPRIETÁRIO/CONTRATADO:** Quais serviços foram contratados para manutenção da solução, serviços certificados e qualificados.
- **ACESSO:** Qual disponibilidade de acesso está colocada ao quadro técnico relevante;
- **MONITORAMENTO:** Quais recursos estão disponíveis para o monitoramento, como dashboard, disparos automáticos de alertar destinado a e-mail, SMS, ligação, sistema sonoro e demais configurações possíveis;
- **TOMADA DE DECISÃO AUTOMATIZADA:** Configuração previamente estabelecida pela recomendações do fabricante, boas práticas identificadas via networks e experiências registradas no CS anteriormente obtidas (antes do evento);
- **RELEVÂNCIA TÉCNICA:** Qual nível de relevância técnica atribuída pela infraestrutura local ao negócio da empresa.



10. CONCLUSÕES

Para o avanço conclusivo da primeira etapa de implementação do PGE – 12º ITSM torna-se indispensável a resolução das seguintes interrogações.

- a. Apresentar análise conclusiva de todos os EVENTOS que ocorrem na infraestrutura de TI, sobretudo as que possam ser automatizadas, a fim de garantir a continuidade do serviço.
- b. Apresentar o fluxo de valor no negócio do cliente (TJPA).
- c. Listar Recursos computacionais e humano existente no monitoramento existentes.
- d. Construção e homologação da Matriz de Impacto e Probabilidade.
- e. Construção e homologação da Matriz de Responsabilidade.
- f. Construção e homologação da Matriz de Funcionalidade junto a Infraestrutura de TI, como: APROVEITAMANETO, DISPONIBILIDADE (ÁREA MONITORAMENTO), SUPORTE PROPRIETÁRIO, ACESSO AO QUADRO TÉCNICO RELEVANTE), MONITORAMENTO CONTINUADO, TOMADA DE DECISÃO AUTOMATIZADA E RELEVÂNCIA TÉCNICA.