**SENAI - SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL**

**DESENVOLVIMENTO DE SISTEMAS – DESI 2023/2**

****

PROJETO DE MANUTENÇÃO DE SISTEMA

Cesar Glufke Zanellato

# Florianópolis, 12 de novembro de 2023.

**SUMÁRIO**

1. Introdução;

2. Gerenciamento de Eventos;

2.1. Detecção e Monitoramento;  
2.2. Classificação e Priorização;   
2.3. Análise e Resposta;  
2.4. Comunicação e Documentação;

3. Gerenciamento de Incidentes e Problemas;  
  
 3.1. Detecção e Registro;

3.2. Classificação e Priorização;  
 3.3. Investigação e Diagnóstico;  
 3.4. Resolução e Recuperação;  
 3.5. Comunicação e Encerramento;

4. Referencias;

# 

# 1 INTRODUÇÃO

A manutenção de sistemas é uma prática vital para as empresas modernas que dependem de tecnologia da informação para operar eficientemente. A expansão rápida e significativa da empresa, que agora conta com 360 agências em 21 estados do Brasil, trouxe consigo desafios operacionais substanciais para a área de TI. Diante dessa realidade, a manutenção adequada dos sistemas tornou-se imperativa para garantir a continuidade dos serviços bancários e a satisfação dos clientes.

Este documento técnico tem como objetivo abordar a importância da manutenção de sistemas para empresas, destacando a necessidade de utilizar um plano de gerenciamento de eventos de TI e um plano de gerenciamento de incidentes e problemas, conforme as orientações do ITIL. O Information Technology Infrastructure Library (ITIL) é um conjunto de boas práticas globalmente aceito para o gerenciamento de serviços de TI, fornecendo diretrizes para melhorar a eficiência e eficácia do serviço de TI em organizações.

# 2 GERENCIAMENTO DE EVENTOS

O plano de gerenciamento de eventos de TI é essencial para detectar, registrar, avaliar e responder a eventos que possam impactar as operações da empresa. A implementação de ferramentas avançadas de monitoramento e alertas proativos é fundamental para identificar problemas em tempo real. A padronização de procedimentos operacionais e a definição de acordos de nível de serviço claros garantem uma resposta rápida e eficaz aos eventos, minimizando interrupções nos serviços.  
  
 **2.1. Detecção e Monitoramento:**

* Implementar ferramentas avançadas de monitoramento para detectar eventos em tempo real.
* Estabelecer alertas proativos para atividades incomuns ou falhas nos sistemas.

**2.2. Classificação e Priorização:**

* Classificar eventos com base na gravidade e no impacto nos negócios.
* Priorizar eventos de acordo com sua urgência e relevância para a operação da empresa.

**2.3. Análise e Resposta:**

* Realizar análises detalhadas para entender a causa raiz dos eventos.
* Implementar soluções temporárias imediatas para minimizar o impacto.
* Desenvolver e aplicar soluções definitivas para evitar recorrências.

**2.4. Comunicação e Documentação:**

* Manter uma comunicação transparente com as partes interessadas, informando sobre o status e as ações tomadas para resolver o evento.
* Documentar detalhes do evento, incluindo análises, soluções aplicadas e lições aprendidas para referência futura.

|  |  |  |
| --- | --- | --- |
| **Classificação** | **Área** | **Descrição** |
| **Normal** | Sistema | Funcionamento regular do sistema sem anomalias detectadas. |
| **Alerta de Hardware** | Sistema | Sinaliza problemas em componentes de hardware, como falhas de disco rígido ou RAM, que podem afetar o desempenho do sistema. |
| **Alerta de Espaço em Disco** | Sistema | Indica a aproximação da capacidade máxima do disco, alertando para a necessidade de liberação de espaço para evitar problemas de armazenamento. |
| **Alerta de Aplicação** | Sistema | Notificação sobre falhas em uma aplicação específica, indicando possíveis bugs ou incompatibilidades. |
| **Alerta de Atualização de Software** | Sistema | Notificação indicando a disponibilidade de atualizações importantes para o software, alertando para a necessidade de manter o sistema seguro e atualizado. |
| **Alerta de Uso Excessivo da CPU** | Sistema | Indica um alto consumo de recursos da CPU, alertando para possíveis gargalos no sistema que podem levar a falhas ou lentidão. |
| **Crítico de Segurança** | Login | Tentativas de login suspeitas ou atividades de acesso não autorizadas, indicando uma possível violação de segurança. |
| **Não Usual de Login** | Login | Atividades de login que não seguem padrões usuais, como múltiplas tentativas de login em curtos intervalos, indicando possíveis tentativas de acesso não autorizado. |
| **Alerta de Performance** | Rede | Alerta indicando deterioração na performance da rede, sinalizando possíveis congestionamentos. |
| **Alerta de Conectividade** | Rede | Indica problemas de conectividade de rede, como quedas frequentes, que afetam a comunicação entre sistemas e usuários. |
| **Crítico de Segurança de Rede** | Rede | Indica atividades suspeitas na rede, como tentativas de intrusão ou tráfego incomum, alertando para possíveis ameaças de segurança. |
| **Alerta de Utilização de Banda Larga** | Rede | Indica um aumento significativo no consumo de largura de banda na rede, alertando para possíveis atividades de transferência de dados não autorizadas ou tráfego malicioso. |
| **Alerta de Backup** | Backup | Notificação indicando falha ou sucesso incompleto no processo de backup, alertando sobre possíveis perdas de dados. |
| **Crítico de Banco de Dados** | Banco de Dados | Indica falhas ou erros críticos no banco de dados, sinalizando potencial perda de dados ou interrupção nos serviços relacionados. |
| **Não Usual de Relatórios** | Relatórios | Indica discrepâncias ou erros nos relatórios que não correspondem aos padrões esperados, sinalizando problemas de precisão ou integridade dos dados. |

# 3 GERENCIAMENTO DE INCIDENTES E PROBLEMAS

O gerenciamento de incidentes e problemas, de acordo com as práticas do ITIL, visa estabelecer uma central de atendimento eficiente, analisar causas raiz, implementar soluções definitivas e realizar mudanças controladas. Ao criar uma equipe dedicada para o gerenciamento de problemas e investir em treinamento contínuo, a empresa pode identificar e resolver problemas recorrentes, melhorando a estabilidade e confiabilidade dos sistemas.

**3.1. Detecção e Registro:**

* Implementar um sistema de registro centralizado para documentar todos os incidentes.
* Estabelecer um canal de comunicação dedicado para relatórios de incidentes por parte dos usuários.

**3.2. Classificação e Priorização:**

* Classificar incidentes com base na severidade e impacto nos negócios.
* Priorizar incidentes de acordo com as orientações de SLA (Service Level Agreement).

**3.3. Investigação e Diagnóstico:**

* Realizar investigações detalhadas para identificar a causa raiz de cada incidente.
* Utilizar técnicas como a análise de causa raiz (RCA) para identificar falhas e implementar correções definitivas.

**3.4. Resolução e Recuperação:**

* Implementar soluções temporárias (workarounds) para restaurar os serviços rapidamente.
* Desenvolver e implementar soluções definitivas para evitar recorrências.

**3.5. Comunicação e Encerramento:**

* Manter os usuários informados sobre o status e a resolução dos incidentes.
* Documentar detalhes do incidente, solução e lições aprendidas antes de encerrar o incidente no sistema.

|  |  |  |
| --- | --- | --- |
| **Incidente** | **Tipo** | **Descrição** |
| **Acesso Negado** | Segurança da Informação | Um usuário é impedido de acessar determinados recursos ou áreas do sistema sem autorização adequada, indicando possíveis violações de política de segurança ou falhas de autenticação. |
| **Conteúdo Abusivo** | Segurança da Informação | Identificação de conteúdo inapropriado, como spam, phishing ou conteúdo ofensivo, que pode comprometer a segurança da rede e a reputação da empresa. |
| **Erro de Autenticação** | Segurança da Informação | Usuários enfrentam problemas ao tentar se autenticar no sistema, indicando possíveis problemas no banco de dados de usuários ou falhas de autenticação. |
| **Ataque de Malware** | Segurança da Informação | Identificação de atividades maliciosas relacionadas a malware, como ransomware ou trojans, que podem comprometer a segurança dos sistemas e dados da empresa. |
| **Uso Impróprio de Recursos** | Suporte | Um usuário utiliza indevidamente os recursos do sistema, como armazenamento excessivo de dados ou consumo excessivo de largura de banda, impactando negativamente o desempenho para outros usuários. |
| **Notificação do Sistema** | Suporte | Recebimento de alertas ou mensagens de erro do sistema, indicando possíveis falhas ou comportamentos anômalos que requerem investigação e resolução. |
| **Perda de Conexão de Rede** | Suporte | Os usuários ou sistemas perdem a conexão com a rede, impedindo o acesso a recursos online ou sistemas remotos, o que pode ser causado por falhas de hardware ou configuração de rede. |
| **Inclusão de Relatório Incorreto** | Desenvolvimento | Relatórios gerados pelo sistema contêm informações incorretas, prejudicando a precisão e integridade dos dados, geralmente relacionado a falhas no código ou lógica de processamento. |
| **Falha de Aplicação Crítica** | Desenvolvimento | Uma aplicação crítica para as operações da empresa falha, impedindo o uso normal do sistema, geralmente relacionado a bugs de software ou incompatibilidades. |
| **Sobrecarga de Servidor** | Desenvolvimento | Um aumento repentino no tráfego do site ou na demanda de aplicativos sobrecarrega o servidor, levando a uma resposta lenta ou à indisponibilidade dos serviços online. |

# 4 REFERENCIAS Livro de Didático: SÉRIE TI - SOFTWARE MANUTENÇÃO DE SISTEMAS - 2022. SENAI – Departamento Nacional