Plano de Manutenção do Banco de Dados - Sistema SIGA

Corpo de Bombeiros Militar de Mato Grosso (CBM MT)
Sistema Integrado de Gestão de Almoxarifado
Data: 18 de junho de 2025
Autor: SD Walingson 4°BBM MT

Sumário Executivo

Este documento apresenta o plano abrangente de manutenção para o banco de dados PostgreSQL do Sistema Integrado de Gestão de Almoxarifado (SIGA) do Corpo de Bombeiros Militar de Mato Grosso. O plano foi atualizado para incorporar as novas funcionalidades implementadas, incluindo gestão de custódia em campo, vinculação a eventos operacionais, sistema de avaliação de materiais e registro de ocorrências.

O plano de manutenção é estruturado em rotinas diárias, semanais, mensais, trimestrais e anuais, cada uma com objetivos específicos para garantir a performance, integridade, segurança e disponibilidade do sistema. As rotinas foram projetadas considerando as características específicas do ambiente operacional do CBM MT, incluindo picos de demanda durante emergências e a necessidade de disponibilidade contínua para operações críticas.

A implementação deste plano garante que o sistema mantenha performance otimizada mesmo com o crescimento dos dados, que a integridade dos dados seja preservada através de verificações regulares, que backups sejam realizados de forma consistente e confiável, e que potenciais problemas sejam identificados e resolvidos antes de impactar as operações.

1. Rotinas de Manutenção Diária

1.1. Verificação de Integridade e Consistência

As rotinas diárias de verificação de integridade constituem a primeira linha de defesa contra problemas que podem comprometer a confiabilidade do sistema. Estas verificações são executadas automaticamente durante períodos de baixa atividade, tipicamente entre 02:00 e 04:00, quando o impacto nas operações é mínimo.

A verificação de integridade referencial é executada diariamente para garantir que todas as relações entre tabelas estejam consistentes. Esta verificação é particularmente importante para as novas funcionalidades implementadas, como as ligações entre operações de cautela e transferências de custódia em campo, ou entre operações e eventos operacionais. O sistema verifica se todos os registros de `custodia_campo` referenciam operações de cautela válidas e se todas as associações em `operacao_evento` apontam para eventos existentes.

A verificação de consistência de estoque é executada comparando as quantidades registradas na tabela `estoque_atual` com os somatórios calculados a partir das operações registradas. Esta verificação inclui agora as quantidades em custódia externa, garantindo que o total de materiais cautelados corresponda exatamente aos registros de custódia em campo. Discrepâncias são automaticamente reportadas para investigação imediata.

A verificação de integridade de partições garante que todas as partições necessárias existam e estejam corretamente configuradas. O sistema verifica se existem partições para o mês corrente e os próximos dois meses para todas as tabelas particionadas (`operacao`, `historico_estoque`, `log_auditoria`, `notificacao`), criando automaticamente partições ausentes conforme necessário.

1.2. Monitoramento de Performance

O monitoramento diário de performance inclui a coleta e análise de métricas críticas que indicam a saúde geral do sistema. As métricas de tempo de resposta são coletadas para consultas representativas de cada módulo do sistema, incluindo consultas de estoque, rastreabilidade de custódia, análise de eventos e geração de relatórios.

A análise de consultas lentas identifica queries que excedem limites de tempo estabelecidos, permitindo otimizações proativas antes que problemas de performance impactem os usuários. O sistema mantém um histórico de performance que permite identificar tendências de degradação e correlacionar problemas de performance com eventos específicos como picos de operações ou crescimento de dados.

O monitoramento de utilização de recursos inclui CPU, memória, espaço em disco e I/O. Alertas são gerados quando qualquer recurso excede 80% de utilização, permitindo ações preventivas antes que limitações de recursos afetem a disponibilidade do sistema. O monitoramento é especialmente importante para o espaço em disco, considerando o crescimento contínuo das tabelas particionadas.

A verificação de locks e bloqueios identifica situações onde transações estão sendo bloqueadas por períodos excessivos, o que pode indicar problemas de concorrência ou

transações mal otimizadas. Esta verificação é particularmente importante durante períodos de alta atividade, como durante grandes operações de emergência quando múltiplos usuários estão registrando movimentações simultaneamente.

1.3. Backup Incremental

O sistema de backup incremental diário garante que todas as alterações realizadas nas últimas 24 horas sejam preservadas de forma segura. O backup incremental é executado utilizando a funcionalidade de WAL (Write-Ahead Logging) do PostgreSQL, capturando todas as transações desde o último backup completo ou incremental.

Os backups incrementais são armazenados em múltiplas localizações para garantir redundância: armazenamento local para recuperação rápida, armazenamento em rede para proteção contra falhas de hardware local, e armazenamento em nuvem para proteção contra desastres que possam afetar as instalações físicas. Cada backup é verificado automaticamente após a conclusão para garantir sua integridade.

O sistema mantém um histórico de 30 dias de backups incrementais, permitindo recuperação point-in-time para qualquer momento dentro deste período. Esta capacidade é crucial para situações onde problemas são descobertos dias após sua ocorrência, permitindo recuperação precisa sem perda significativa de dados.

A documentação de cada backup inclui informações sobre tamanho, duração, verificação de integridade e localização de armazenamento. Esta documentação é essencial para planejamento de capacidade e para procedimentos de recuperação de desastres.

1.4. Verificação de Alertas e Notificações

A verificação diária do sistema de alertas e notificações garante que todos os mecanismos de comunicação estejam funcionando corretamente. Esta verificação inclui o teste dos canais LISTEN/NOTIFY do PostgreSQL, que são utilizados para notificações em tempo real sobre estoque crítico, documentação irregular e novas ocorrências.

O sistema verifica se todas as notificações geradas nas últimas 24 horas foram adequadamente processadas e entregues aos destinatários apropriados. Notificações não entregues são reprocessadas automaticamente, e falhas persistentes são escaladas para investigação manual.

A verificação inclui também o teste dos alertas automáticos de estoque crítico, simulando condições que deveriam gerar alertas e verificando se as notificações são geradas corretamente. Esta verificação é essencial para garantir que situações críticas sejam comunicadas imediatamente aos responsáveis.

O sistema mantém estatísticas sobre a efetividade das notificações, incluindo tempos de entrega, taxas de leitura e ações tomadas em resposta aos alertas. Estas estatísticas são utilizadas para otimizar continuamente o sistema de notificações e garantir sua relevância e efetividade.

2. Rotinas de Manutenção Semanal

2.1. Análise Detalhada de Performance

A análise semanal de performance proporciona uma visão mais abrangente das tendências de utilização do sistema, permitindo identificar padrões que não são visíveis nas verificações diárias. Esta análise inclui a revisão de todas as métricas coletadas durante a semana, identificando picos de utilização, consultas que apresentaram degradação de performance e recursos que se aproximaram de limites críticos.

A análise de consultas inclui a identificação de queries que, embora não sejam individualmente problemáticas, consomem recursos significativos devido à alta frequência de execução. Estas consultas são candidatas para otimização através de ajustes de índices, reescrita de queries ou criação de views materializadas.

O sistema analisa padrões de acesso às partições, identificando partições que recebem mais acessos que o esperado ou partições antigas que ainda estão sendo consultadas frequentemente. Esta informação orienta decisões sobre estratégias de arquivamento e otimização de índices.

A análise de crescimento de dados projeta tendências futuras baseadas no crescimento observado durante a semana. Esta projeção é essencial para planejamento de capacidade e para identificar quando será necessário expandir recursos de armazenamento ou processamento.

2.2. Manutenção de Índices

A manutenção semanal de índices garante que todos os índices estejam otimizados para as consultas atuais do sistema. Esta manutenção inclui a reconstrução de índices que apresentaram fragmentação significativa, a análise de utilização de índices para identificar índices subutilizados que podem ser removidos, e a identificação de oportunidades para criação de novos índices.

A análise de fragmentação é particularmente importante para índices em tabelas com alta rotatividade de dados, como as tabelas de operações e notificações. Índices fragmentados podem impactar significativamente a performance de consultas, especialmente em operações de range scan que são comuns em consultas por período.

O sistema analisa estatísticas de utilização de índices coletadas pelo PostgreSQL, identificando índices que não foram utilizados durante a semana. Índices não utilizados consomem espaço de armazenamento e recursos durante operações de escrita sem proporcionar benefícios, sendo candidatos para remoção após análise cuidadosa.

A identificação de oportunidades para novos índices é baseada na análise de consultas que apresentaram performance subótima durante a semana. O sistema sugere índices que poderiam melhorar a performance destas consultas, considerando o impacto no overhead de manutenção e no espaço de armazenamento.

2.3. Verificação de Backup e Recuperação

A verificação semanal de backup inclui testes de recuperação que garantem que os backups estão funcionais e que os procedimentos de recuperação estão operacionais. Estes testes são executados em um ambiente separado para não impactar as operações de produção.

O teste de recuperação point-in-time verifica a capacidade de recuperar o banco de dados para um momento específico durante a semana anterior, utilizando a combinação de backup completo e backups incrementais. Este teste valida não apenas a integridade dos backups, mas também a funcionalidade dos procedimentos de recuperação.

A verificação de integridade dos backups arquivados inclui a validação de checksums e a verificação de que todos os arquivos necessários para recuperação estão presentes e acessíveis. Backups corrompidos ou incompletos são identificados e substituídos por cópias de backup secundárias.

O sistema testa também a recuperação de componentes específicos, como tabelas individuais ou partições específicas, validando procedimentos que podem ser necessários em cenários de recuperação parcial. Esta capacidade é importante para situações onde apenas parte dos dados foi afetada por problemas.

2.4. Análise de Segurança

A análise semanal de segurança inclui a revisão de logs de acesso, identificação de padrões de uso anômalos e verificação de que todas as políticas de segurança estão sendo adequadamente aplicadas. Esta análise é crucial para manter a integridade e confidencialidade dos dados do sistema.

A revisão de logs de auditoria identifica atividades suspeitas, como tentativas de acesso não autorizado, alterações de dados fora do horário normal de trabalho, ou padrões de acesso que desviam significativamente do comportamento normal dos usuários.

Atividades suspeitas são investigadas e, se necessário, escaladas para as autoridades competentes.

A verificação de permissões garante que todos os usuários tenham apenas as permissões necessárias para suas funções, seguindo o princípio do menor privilégio. O sistema identifica usuários com permissões excessivas e sugere ajustes para reduzir riscos de segurança.

A análise inclui também a verificação de que todas as conexões ao banco de dados estão utilizando criptografia adequada e que não há conexões não autorizadas ou de origens não reconhecidas. Esta verificação é essencial para manter a confidencialidade dos dados durante a transmissão.

3. Rotinas de Manutenção Mensal

3.1. Backup Completo e Verificação

O backup completo mensal constitui a base do sistema de recuperação de desastres, capturando o estado completo do banco de dados em um momento específico. Este backup é executado durante um período de manutenção programada, quando o sistema pode ser temporariamente colocado em modo de leitura apenas para garantir consistência total.

O processo de backup completo inclui não apenas os dados das tabelas, mas também todos os objetos do banco de dados como índices, views, procedures, triggers e configurações. Esta abordagem garante que uma recuperação completa possa restaurar não apenas os dados, mas toda a funcionalidade do sistema.

A verificação do backup completo inclui a restauração em um ambiente de teste e a execução de uma bateria de testes que validam a integridade dos dados e a funcionalidade de todos os componentes do sistema. Esta verificação é essencial para garantir que o backup seja utilizável em uma situação real de recuperação de desastres.

O backup completo é armazenado em múltiplas localizações geográficas para proteção contra desastres regionais. Cópias são mantidas em instalações locais, em data centers remotos e em serviços de armazenamento em nuvem, garantindo que pelo menos uma cópia esteja sempre acessível mesmo em cenários de desastre extremo.

3.2. Análise de Crescimento e Planejamento de Capacidade

A análise mensal de crescimento proporciona uma visão abrangente das tendências de utilização de recursos e crescimento de dados, permitindo planejamento proativo de

expansão de capacidade. Esta análise inclui projeções baseadas em dados históricos e consideração de fatores sazonais que podem afetar o crescimento.

O crescimento de dados é analisado por tabela e por partição, identificando áreas do sistema que estão crescendo mais rapidamente que o esperado. Esta análise é particularmente importante para as novas funcionalidades como registros de custódia em campo e avaliações de materiais, que podem ter padrões de crescimento diferentes das funcionalidades tradicionais.

A análise de utilização de recursos inclui tendências de CPU, memória, armazenamento e I/O, correlacionando estas métricas com o crescimento de dados e o aumento de usuários. Esta correlação permite projeções mais precisas sobre quando será necessário expandir recursos de hardware.

O planejamento de capacidade inclui recomendações específicas sobre quando e como expandir recursos, considerando fatores como lead time para aquisição de hardware, janelas de manutenção disponíveis e impacto nas operações. As recomendações incluem também estratégias alternativas como otimização de consultas ou arquivamento de dados antigos.

3.3. Manutenção de Partições

A manutenção mensal de partições inclui a criação de partições futuras, o arquivamento de partições antigas e a otimização de partições ativas. Esta manutenção é essencial para manter a performance do sistema conforme os dados crescem ao longo do tempo.

A criação de partições futuras garante que o sistema continue operando sem interrupções mesmo durante períodos de alta atividade quando a criação automática de partições poderia causar contenção. O sistema cria partições para os próximos três meses, garantindo disponibilidade contínua.

O arquivamento de partições antigas move dados históricos para armazenamento de longo prazo, liberando espaço no armazenamento principal e melhorando a performance de consultas que não precisam acessar dados históricos. Partições com mais de dois anos são movidas para armazenamento de arquivo, onde permanecem acessíveis mas não impactam operações correntes.

A otimização de partições ativas inclui a reconstrução de índices fragmentados, a atualização de estatísticas para o otimizador de consultas e a verificação de que todas as partições estão adequadamente configuradas. Esta otimização garante que as partições mais utilizadas mantenham performance ideal.

3.4. Análise de Utilização e Otimização

A análise mensal de utilização examina padrões de uso do sistema, identificando funcionalidades subutilizadas, consultas ineficientes e oportunidades de otimização. Esta análise é baseada em dados coletados durante todo o mês e proporciona insights valiosos para melhorias contínuas.

A análise de funcionalidades identifica módulos do sistema que são utilizados com menos frequência que o esperado, permitindo investigação sobre possíveis problemas de usabilidade ou necessidades de treinamento adicional. Funcionalidades como o sistema de avaliação de materiais podem precisar de promoção adicional para alcançar adoção completa.

A identificação de consultas ineficientes inclui não apenas consultas individuais lentas, mas também padrões de consultas que, em conjunto, consomem recursos significativos. Esta análise pode revelar oportunidades para otimização através de views materializadas, índices especializados ou reestruturação de dados.

A análise de oportunidades de otimização considera também aspectos funcionais, como a identificação de processos manuais que poderiam ser automatizados ou relatórios que poderiam ser pré-calculados para melhorar a experiência do usuário.

4. Rotinas de Manutenção Trimestral

4.1. Revisão Abrangente de Segurança

A revisão trimestral de segurança constitui uma análise aprofundada de todos os aspectos de segurança do sistema, incluindo controles de acesso, auditoria, criptografia e conformidade com políticas organizacionais. Esta revisão é executada por uma equipe especializada e pode incluir consultores externos para garantir objetividade.

A auditoria de controles de acesso verifica que todos os usuários tenham permissões apropriadas para suas funções atuais, identificando contas órfãs de funcionários que mudaram de função ou deixaram a organização. O sistema de Row Level Security (RLS) é testado para garantir que usuários só possam acessar dados apropriados para sua unidade e função.

A análise de logs de auditoria inclui a identificação de padrões que podem indicar tentativas de acesso não autorizado, uso inadequado de privilégios ou outras atividades suspeitas. Esta análise utiliza ferramentas automatizadas para identificar anomalias em grandes volumes de dados de auditoria.

A verificação de conformidade garante que o sistema continue atendendo a todas as regulamentações aplicáveis, incluindo leis de proteção de dados, regulamentos de segurança da informação e políticas internas da organização. Esta verificação inclui a documentação de todos os controles implementados e evidências de sua efetividade.

4.2. Teste de Recuperação de Desastres

O teste trimestral de recuperação de desastres simula cenários realistas de falha para validar que os procedimentos de recuperação são efetivos e que os objetivos de tempo de recuperação (RTO) e ponto de recuperação (RPO) podem ser atendidos. Estes testes são executados em ambiente separado para não impactar as operações de produção.

O teste de recuperação completa simula a perda total do sistema de produção, validando a capacidade de restaurar completamente o sistema a partir de backups. Este teste inclui não apenas a restauração dos dados, mas também a reconfiguração de todos os componentes do sistema e a validação de que todas as funcionalidades estão operacionais.

O teste de recuperação parcial simula cenários onde apenas parte do sistema é afetada, como a corrupção de uma partição específica ou a falha de um subsistema. Estes testes validam procedimentos de recuperação granular que podem ser mais apropriados para certos tipos de problemas.

A validação de procedimentos inclui a verificação de que toda a documentação de recuperação está atualizada e que todos os membros da equipe responsável pela recuperação estão adequadamente treinados. O teste identifica lacunas na documentação ou no treinamento que precisam ser corrigidas.

4.3. Análise de Performance e Otimização

A análise trimestral de performance proporciona uma visão de longo prazo das tendências de utilização do sistema, permitindo identificar padrões sazonais e planejar otimizações estratégicas. Esta análise inclui correlação entre performance e eventos operacionais, como grandes emergências que podem impactar significativamente a utilização do sistema.

A análise de tendências de performance identifica degradações graduais que podem não ser visíveis em análises de curto prazo. Por exemplo, consultas que se tornam progressivamente mais lentas conforme os dados crescem podem ser identificadas e otimizadas antes que se tornem problemáticas.

A avaliação de arquitetura examina se a estrutura atual do banco de dados ainda é adequada para os padrões de uso observados. Esta avaliação pode recomendar

mudanças estruturais como redistribuição de dados, criação de novos índices especializados ou implementação de novas estratégias de particionamento.

A análise inclui também a avaliação de novas funcionalidades do PostgreSQL que podem beneficiar o sistema, como novos tipos de índices, funcionalidades de paralelização ou melhorias no otimizador de consultas. A adoção de novas funcionalidades é planejada cuidadosamente para minimizar riscos.

4.4. Revisão de Procedimentos e Documentação

A revisão trimestral de procedimentos garante que toda a documentação operacional esteja atualizada e que os procedimentos reflitam as melhores práticas atuais. Esta revisão é especialmente importante após a implementação de novas funcionalidades ou mudanças significativas no sistema.

A atualização de procedimentos operacionais inclui a incorporação de lições aprendidas durante o trimestre, ajustes baseados em mudanças no ambiente operacional e melhorias identificadas através da experiência prática. Procedimentos para as novas funcionalidades como gestão de custódia em campo são refinados baseados no uso real.

A revisão de documentação técnica garante que todas as especificações, diagramas e manuais estejam atualizados e reflitam o estado atual do sistema. Esta documentação é essencial para manutenção efetiva e para treinamento de novos membros da equipe.

A validação de procedimentos de emergência inclui a verificação de que todos os procedimentos para situações críticas estão atualizados e que todos os membros da equipe estão familiarizados com suas responsabilidades. Esta validação pode incluir simulações de cenários de emergência para testar a efetividade dos procedimentos.

5. Rotinas de Manutenção Anual

5.1. Revisão Estratégica Completa

A revisão anual constitui uma avaliação abrangente de todos os aspectos do sistema, incluindo arquitetura, performance, segurança, conformidade e alinhamento com objetivos organizacionais. Esta revisão é conduzida por uma equipe multidisciplinar que inclui administradores de banco de dados, arquitetos de sistemas, especialistas em segurança e representantes dos usuários finais.

A avaliação de arquitetura examina se a estrutura atual do sistema ainda é adequada para as necessidades da organização, considerando mudanças nos requisitos

operacionais, crescimento de dados e evolução tecnológica. Esta avaliação pode recomendar mudanças significativas na arquitetura para melhorar performance, escalabilidade ou manutenibilidade.

A análise de alinhamento estratégico verifica se o sistema continua atendendo aos objetivos organizacionais e se há oportunidades para melhor suporte às operações do CBM MT. Esta análise considera mudanças na missão da organização, novos requisitos regulamentares e evolução das melhores práticas na área.

A avaliação de tecnologia examina novas tecnologias e funcionalidades que podem beneficiar o sistema, incluindo novas versões do PostgreSQL, ferramentas de monitoramento, soluções de backup e tecnologias de alta disponibilidade. A adoção de novas tecnologias é planejada considerando benefícios, riscos e recursos necessários.

5.2. Planejamento de Capacidade de Longo Prazo

O planejamento anual de capacidade projeta necessidades de recursos para os próximos três a cinco anos, baseado em tendências históricas, planos organizacionais e projeções de crescimento. Este planejamento é essencial para garantir que o sistema possa suportar o crescimento futuro sem degradação de performance.

A projeção de crescimento de dados considera não apenas tendências históricas, mas também mudanças planejadas nas operações da organização, como expansão de unidades, implementação de novas funcionalidades ou mudanças nos procedimentos operacionais. Estas projeções orientam decisões sobre expansão de armazenamento e arquivamento de dados.

O planejamento de recursos de processamento considera o crescimento esperado no número de usuários, aumento na complexidade das consultas e implementação de novas funcionalidades que podem impactar a utilização de CPU e memória. Este planejamento inclui estratégias para escalabilidade horizontal e vertical.

A análise de custo-benefício avalia diferentes estratégias para atender às necessidades futuras de capacidade, considerando fatores como custo de hardware, licenciamento de software, custos operacionais e impacto na disponibilidade do sistema. Esta análise orienta decisões de investimento de longo prazo.

5.3. Atualização de Versão e Modernização

A revisão anual inclui a avaliação de atualizações de versão do PostgreSQL e outros componentes do sistema, considerando benefícios de performance, segurança e funcionalidade versus riscos e esforço de migração. Atualizações de versão são planejadas cuidadosamente para minimizar impacto nas operações.

A avaliação de benefícios de atualização inclui melhorias de performance, novas funcionalidades que podem beneficiar o sistema, correções de segurança e melhor suporte para hardware moderno. Estes benefícios são quantificados sempre que possível para facilitar decisões de investimento.

A análise de riscos de atualização considera compatibilidade de aplicações, necessidade de retreinamento de equipe, potencial impacto na disponibilidade durante a migração e riscos de problemas não identificados durante testes. Estratégias de mitigação são desenvolvidas para todos os riscos identificados.

O planejamento de migração inclui cronograma detalhado, procedimentos de rollback, critérios de sucesso e planos de contingência. A migração é testada extensivamente em ambiente de desenvolvimento antes da implementação em produção.

5.4. Revisão de Conformidade e Auditoria

A auditoria anual constitui uma revisão abrangente de todos os aspectos de conformidade do sistema, incluindo aderência a regulamentações, políticas organizacionais e melhores práticas da indústria. Esta auditoria pode ser conduzida por auditores internos ou externos, dependendo dos requisitos organizacionais.

A verificação de conformidade regulamentária garante que o sistema continue atendendo a todas as leis e regulamentos aplicáveis, incluindo proteção de dados, segurança da informação e requisitos específicos para organizações públicas. Esta verificação inclui documentação de todos os controles implementados.

A auditoria de segurança examina todos os aspectos de segurança do sistema, incluindo controles de acesso, criptografia, auditoria, backup e recuperação. Esta auditoria identifica vulnerabilidades potenciais e recomenda melhorias para fortalecer a postura de segurança.

A revisão de procedimentos operacionais verifica que todos os procedimentos estão sendo seguidos adequadamente e que são efetivos para seus propósitos. Esta revisão pode identificar oportunidades para simplificação de procedimentos ou automação de tarefas manuais.

6. Procedimentos de Emergência

6.1. Resposta a Falhas Críticas

Os procedimentos de emergência definem ações específicas para diferentes tipos de falhas críticas que podem afetar a disponibilidade ou integridade do sistema. Estes

procedimentos são projetados para minimizar o tempo de inatividade e preservar a integridade dos dados durante situações de crise.

Para falhas de hardware que afetam o servidor principal, o procedimento inclui avaliação rápida da extensão do problema, ativação de sistemas de backup se disponíveis, e início do processo de recuperação a partir de backups se necessário. O procedimento define claramente as responsabilidades de cada membro da equipe e os critérios para escalação.

Para corrupção de dados, o procedimento inclui isolamento imediato da área afetada para prevenir propagação do problema, avaliação da extensão da corrupção, e determinação da estratégia de recuperação mais apropriada. O procedimento considera diferentes cenários, desde corrupção de registros individuais até corrupção de partições inteiras.

Para ataques de segurança ou acesso não autorizado, o procedimento inclui isolamento imediato do sistema, preservação de evidências para investigação, avaliação da extensão do comprometimento, e implementação de medidas de contenção. O procedimento define também quando e como comunicar o incidente às autoridades competentes.

6.2. Comunicação de Emergência

Os procedimentos de comunicação de emergência garantem que todas as partes interessadas sejam informadas adequadamente sobre problemas críticos e sobre o progresso das ações de recuperação. Esta comunicação é essencial para manter a confiança dos usuários e para coordenar ações de resposta.

A lista de contatos de emergência inclui todos os membros da equipe técnica, gestores responsáveis, fornecedores críticos e autoridades relevantes. Esta lista é mantida atualizada e inclui múltiplos métodos de contato para garantir que as pessoas possam ser alcançadas mesmo fora do horário normal de trabalho.

Os modelos de comunicação definem mensagens padrão para diferentes tipos de emergência, garantindo que informações essenciais sejam comunicadas de forma clara e consistente. Estes modelos incluem informações sobre a natureza do problema, impacto esperado, ações sendo tomadas e estimativas de tempo para resolução.

O procedimento de escalação define quando e como escalar problemas para níveis superiores de gestão, considerando fatores como duração do problema, impacto nas operações e recursos necessários para resolução. A escalação garante que recursos adequados sejam mobilizados rapidamente para problemas críticos.

6.3. Recuperação e Validação

Os procedimentos de recuperação definem passos específicos para restaurar o sistema após diferentes tipos de falhas, garantindo que a recuperação seja executada de forma consistente e que a integridade dos dados seja preservada. Estes procedimentos são testados regularmente para garantir sua efetividade.

Para recuperação a partir de backups, o procedimento inclui seleção do backup apropriado, validação de sua integridade, execução da restauração, e verificação de que todos os dados foram recuperados corretamente. O procedimento considera diferentes cenários de recuperação, desde recuperação completa até recuperação de componentes específicos.

Para recuperação de falhas de hardware, o procedimento inclui instalação e configuração de hardware de substituição, restauração do sistema operacional e software, recuperação dos dados, e validação de que todas as funcionalidades estão operacionais. O procedimento define também como minimizar o tempo de inatividade durante a recuperação.

A validação pós-recuperação inclui testes abrangentes de todas as funcionalidades críticas do sistema, verificação de integridade dos dados, e confirmação de que a performance está dentro de parâmetros aceitáveis. Esta validação garante que o sistema esteja completamente funcional antes de retornar às operações normais.

7. Monitoramento e Alertas

7.1. Sistema de Monitoramento Contínuo

O sistema de monitoramento contínuo coleta métricas em tempo real sobre todos os aspectos críticos do sistema, incluindo performance, disponibilidade, integridade dos dados e segurança. Este monitoramento é essencial para identificar problemas antes que afetem os usuários e para manter visibilidade sobre a saúde geral do sistema.

As métricas de performance incluem tempo de resposta de consultas, utilização de CPU e memória, throughput de I/O e utilização de conexões. Estas métricas são coletadas continuamente e analisadas para identificar tendências que podem indicar problemas emergentes ou necessidades de otimização.

O monitoramento de disponibilidade verifica continuamente que todos os componentes críticos do sistema estão funcionais e acessíveis. Este monitoramento inclui verificação de conectividade, responsividade de serviços e integridade de funcionalidades essenciais como backup e replicação.

O monitoramento de segurança inclui detecção de tentativas de acesso não autorizado, monitoramento de atividades suspeitas e verificação de que todos os controles de segurança estão funcionando adequadamente. Este monitoramento é integrado com sistemas de resposta a incidentes para garantir resposta rápida a ameaças.

7.2. Configuração de Alertas

O sistema de alertas é configurado para notificar automaticamente a equipe responsável sobre condições que requerem atenção imediata ou que podem indicar problemas emergentes. Os alertas são categorizados por severidade e configurados com diferentes métodos de notificação baseados na urgência.

Alertas críticos são configurados para condições que afetam imediatamente a disponibilidade ou integridade do sistema, como falhas de hardware, corrupção de dados ou ataques de segurança. Estes alertas são enviados imediatamente através de múltiplos canais para garantir resposta rápida.

Alertas de aviso são configurados para condições que podem se tornar problemáticas se não forem endereçadas, como utilização alta de recursos, degradação de performance ou aproximação de limites de capacidade. Estes alertas permitem ação proativa antes que problemas se tornem críticos.

Alertas informativos são configurados para eventos que devem ser registrados mas não requerem ação imediata, como conclusão de backups, criação de novas partições ou execução de manutenção programada. Estes alertas mantêm a equipe informada sobre atividades do sistema.

7.3. Dashboards e Relatórios

Os dashboards de monitoramento proporcionam visibilidade em tempo real sobre o status de todos os componentes críticos do sistema, permitindo que a equipe identifique rapidamente problemas e monitore tendências. Estes dashboards são acessíveis através de interfaces web e podem ser exibidos em monitores dedicados.

O dashboard principal inclui métricas de alto nível sobre performance, disponibilidade e utilização de recursos, proporcionando uma visão geral rápida da saúde do sistema. Este dashboard é projetado para permitir identificação rápida de problemas mesmo por pessoal não técnico.

Dashboards especializados proporcionam visões detalhadas de aspectos específicos do sistema, como performance de consultas, utilização de partições, efetividade de backups e atividade de segurança. Estes dashboards são utilizados pela equipe técnica para análise detalhada e troubleshooting.

Os relatórios automatizados são gerados periodicamente para documentar tendências de longo prazo, efetividade de procedimentos de manutenção e conformidade com objetivos de nível de serviço. Estes relatórios são utilizados para planejamento estratégico e para comunicação com gestão superior.

Conclusão

O plano de manutenção apresentado proporciona uma estrutura abrangente para garantir que o Sistema Integrado de Gestão de Almoxarifado do CBM MT mantenha performance, integridade, segurança e disponibilidade ideais ao longo de sua vida útil. A implementação consistente deste plano é essencial para o sucesso operacional do sistema e para a confiança dos usuários.

As rotinas de manutenção são projetadas para serem proativas, identificando e resolvendo problemas antes que afetem as operações. A combinação de verificações automatizadas e análises manuais garante que todos os aspectos críticos do sistema sejam adequadamente monitorados e mantidos.

A estrutura de emergência proporciona procedimentos claros para resposta a situações críticas, minimizando o impacto de problemas inesperados e garantindo recuperação rápida. A documentação detalhada e o treinamento regular da equipe são essenciais para a efetividade destes procedimentos.

O sistema de monitoramento contínuo e alertas garante visibilidade constante sobre a saúde do sistema e resposta rápida a condições que requerem atenção. Esta visibilidade é fundamental para manter a confiança dos usuários e para garantir que o sistema continue atendendo às necessidades operacionais da organização.

A implementação bem-sucedida deste plano de manutenção requer comprometimento organizacional, recursos adequados e treinamento contínuo da equipe. Com estes elementos em lugar, o sistema SIGA continuará proporcionando valor significativo para as operações do CBM MT por muitos anos.
