1. **Procedimentos de backup, segurança e contingência**

**1.1. Objetivo**

A importância de realizar backups na administração de sistemas é essencial, pois em cenários de invasão, falha acidental ou aplicações críticas onde a mesma opera 24 horas por dia, 7 dias por semana e 365 dias por ano, uma manutenção no ambiente de produção pode deixar a Empresa vulnerável a diversos fatores negativos, tais como: prejuízo financeiro, credibilidade da empresa, perda de patrimônio (embora os dados não sejam físico), roubo de informações e etc.

O presente documento estabelece uma política de proteção de dados, que inclui tolerância a falhas, cópias de segurança (backup) e restauração de arquivos digitais armazenados pela empresa. O modo como isto deverá ser feito está descrito logo abaixo e irá fazer parte do plano de contingência.

O plano de contingência tem por finalidade criar um planejamento de riscos a fim de descrever as medidas a serem tomadas pela empresa em casos urgentes em que precise retomar de maneira mais rápida possível o sistema da organização. Nele são criados planos que visam garantir um nível de serviço mínimo que permita dar continuidade nos serviços vitais da empresa sem que esta sofra maiores prejuízos de imagem ou financeiros. O plano de contingência é integrado por um plano de backup e pelo plano de tolerância a falhas. Deve ser desenvolvido envolvendo todas as áreas sujeitas as catástrofes. Será de responsabilidade da área de infraestrutura de TI manter a operacionalização e funcionalidade do plano.

**1.2. Requisitos**

Os centros de processamento de dados onde são concentrados os equipamentos de processamento e armazenamento de dados da empresa, deverão ser projetados para serem extremamente seguros, protegidos de acessos indevidos e deverão utilizar componentes redundantes e tecnologias de tolerância a falhas (como clusters de servidor e espelhamento de software ou hardware) para garantir a alta disponibilidade com a replicação de dados cruciais.

Porém, para que os problemas de corrupção ou invasão de dados sejam menos impactantes, é necessário um formato de arquivamento em que deverá abranger os dados transacionais do sistema, como por exemplo, para fins de auditoria jurídica ou de necessidade da empresa. Portanto, é necessário ter uma estratégica de proteção de dados que inclua um esquema de backup e recuperação abrangente para proteger os dados contra qualquer tipo de interrupção ou desastre imprevisto.

**1.3. Tolerância a Falhas**

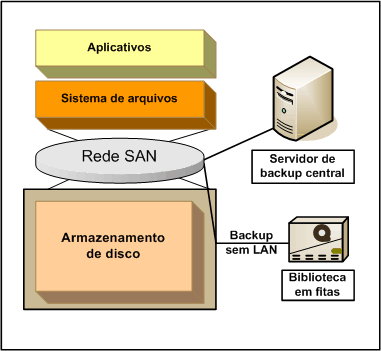
Diante da necessidade de possuir um sistema de recuperação de dados mais veloz e com mais segurança, o sistema de transporte BIBI irá utilizar o sistema RAID10. Aliando ganho de desempenho no acesso, redundância em caso de falhas em um dos discos e facilidade na recuperação do conteúdo perdido, este conjunto é um dos mais indicados nos casos onde se necessita aliar performance e redundância.

A implementação do RAID 10 será via software, onde o sistema operacional gerencia o RAID através da controladora de discos, sem a necessidade de um controlador de RAIDs, tornando-a mais barata.

Nesse tipo de implementação, todo o processamento necessário para o gerenciamento do RAID é feito pela CPU. Toda movimentação de dados(leitura e escrita) é feita por uma camada de *software* que faz a abstração entre a operação lógica (RAID) e os discos físicos, e é controlada pelo sistema operacional.

**1.4. Plano de Backup e Recuperação**:

* **Modo de Backup (online):** Serão realizados backups online do sistema, ou seja, os backups são feitos mesmo com o sistema em operação. Nesse período os usuários podem utilizar a aplicação ou a base de dados e executar ações normais, tais como a atualização e a recuperação dos dados com o sistema funcionando normalmente.
* **Mídia de Backup (disco magnético):** Serão utilizados discos magnéticos como mídia de backup, pois os mesmos são fáceis de configurar e manter.
* **Tipo de Backup:** Mensalmente, serão realizados backups completos, a fim copiar toda a base de dados e todos os arquivos envolvidos na aplicação, preferencialmente ás segundas-feiras, e diariamente serão realizados backups incrementais, cujo objetivo é copiar e salvar os dados que foram modificados desde o último backup completo ou incremental.
* **Topologia de Backup (SAN):** A capacidade de integração de subsistemas de espaço em disco ao backup e recuperação fornece várias opções para a implantação de soluções de proteção de dados em ambientes baseados em SAN. As SANs são projetadas para otimizar a eficiência das transferências de dados, possibilitando processos de backup e recuperação mais rápidos. O caminho entre o dispositivo de armazenamento e o dispositivo de backup não envolve o servidor, o que significa que a carga no servidor é reduzida. Em outras palavras, uma rede de área de armazenamento é uma rede de alta velocidade de dispositivos de armazenamento que também conecta os dispositivos de armazenamento com os servidores. As vantagens do backup e recuperação baseados em SAN são: a carga de servidor reduzida em que o caminho entre o dispositivo de armazenamento e o dispositivo de backup não envolve o servidor; os backups podem ser feitos sem exigir que os dados passem pela LAN; e as SANs são projetadas para otimizar a eficiência das transferências de dados, possibilitando processos de backup e recuperação mais rápidos.



**1.5. Escopo**

Este plano de contingência abrange todas ás áreas sujeitas a catástrofes, especialmente a área Administrativa e as áreas de Tecnologia da Informação, no que diz respeito aos equipamentos de aplicação de dados da plataforma do Sistema de Transporte BIBI. Para que este plano seja executado com sucesso é preciso ter a última atualização de backup do sistema (em caso de incidentes/desastres que venham a atingir o datacenter) e é necessário possuir um sistema de tolerância a falhas que reflita o estado atual do banco de dados da aplicação (em caso de falhas de discos rígidos). A área de infraestrutura deverá ser informada para dar cabo a este plano sempre que houver necessidade.

**1.6. Estratégia**

As estratégias de recuperação de dados serão adotadas de acordo com o tipo de situação e para isso é necessário o constante monitoramento dos equipamentos de redes e servidores de aplicação de dados, para que seja tomada a ação adequada. Em caso de falha de disco rígido, o sistema de Transporte BIBI não será afetado e a recuperação do sistema será transparente, uma vez que se substitua o disco falho por outro, e que o controlador RAID esteja executando nos servidores de aplicação. Se for necessário a recuperação do dados do sistema por backup, a recuperação será feita a partir da última cópia de segurança realizada de forma a obter todos os dados completos para ativação.

**1.6.1. Ativação das Medidas de Segurança**

Como medida de segurança o backup será testado e revisado periodicamente. Deste modo será possível descobrir problemas em dispositivos e locais de armazenamento, podendo assim evitar dificuldades na recuperação. Quando necessário, será realizado a substituição de disco rígido com defeito. Isso acontecerá toda vez que o controlador de RAIDs executado no sistema operacional apontar uma falha de disco em uma das unidades que rodam a aplicação. O responsável pelo monitoramento deverá efetuar a substituição imediatamente, esse incidente não afeta a execução do sistema uma vez que o controlador de RAIDs utiliza um sistema de replicação de dados e, portanto, é tolerante a falhas de discos. O encarregado deverá reportar a substituição dos discos para efeito de controle.

Sempre que for necessário, a ativação do plano de contingência será colocada em prática. Para isso o responsável pela área de infraestrutura deverá iniciar o procedimento de restauração por backup, utilizando para isso a última cópia de backup total do sistema.

**1.7. Quanto a Realização do Backup**

Deverá ser realizado um backup completo do banco de dados da plataforma depois de 1 mês de operação, na segunda-feira à partir das 0:00 hrs. Após a realização do primeiro backup completo, serão efetuados backups incrementais diários. Dessa forma os dados da aplicação estarão assegurados diariamente. Depois de concluído o procedimento de backup completo pelo servidor de backup central, será necessário a guarda dos discos de backup no centro de armazenamento de dados e segurança, devendo este se situar a uma distância suficiente das instalações da empresa a fim de evitar possíveis perdas totais de dados mediante sinistros ou desastres.

**1.8. Simulação de Emergência**

Treinamentos com simulações práticas são fundamentais para preparar a equipe responsável para tomar medidas rápidas e coerentes diante de uma situação emergencial. Por isso, semestralmente, sugere-se realizar simulados de emergência a fim de verificar a qualidade dos backups implantados, bem como a preparação da equipe responsável pela infraestrutura de TI para realizar planos de contingência em situações reais e a regularidade do sistema.