Arquitetura de Alta Disponibilidade  
e Disaster Recovery

Diretoria de Infraestrutura

Gerência de Soluções e Planejamento

Gerência de Soluções de Infraestrutura

Setembro/2009

**Sumário**

[1 Objetivo 3](#_Toc241915136)

[2 Definições 3](#_Toc241915137)

[2.1 Disaster Recovery 3](#_Toc241915138)

[2.2 Alta Disponibilidade 4](#_Toc241915139)

[2.3 Cluster 4](#_Toc241915140)

[2.4 Ambiente 5](#_Toc241915141)

[3 Modelos Propostos 6](#_Toc241915142)

[3.1.1 DR - Modelo 1 - Backup Off-site 7](#_Toc241915143)

[3.1.2 DR - Modelo 2 - Replicação de armazenamento off-site 8](#_Toc241915144)

[3.1.3 HA - Modelo 3 - Contingência Local 10](#_Toc241915145)

[3.1.4 HA – Modelo 4 Contingência off-site 12](#_Toc241915146)

[3.1.5 Composto - Modelo 5 - Réplica de armazenamento off-site e Contingência local 12](#_Toc241915147)

[3.1.6 Composto - Modelo 6 - Réplica de armazenamento off-site e contingência remota 12](#_Toc241915148)

[4 Recomendações 12](#_Toc241915149)

[4.1 Geral 12](#_Toc241915150)

[4.2 Site Remoto 12](#_Toc241915151)

[4.3 Aplicações Web 12](#_Toc241915152)

[4.4 Aplicações Cliente/Servidor 12](#_Toc241915153)

[4.5 Banco de Dados 12](#_Toc241915154)

[4.6 Armazenamento 12](#_Toc241915155)

[4.7 Infraestrutura de Rede 12](#_Toc241915156)

# Objetivo

O Objetivo deste documento é propor modelos de referência para implantação de alta disponibilidade (HA) e Disaster Recovery (DR) em ambientes críticos para o negócio e operação da OI.

Não é escopo deste documento abordar as questões relativas a um Plano de Continuidade de Negócios (PCN) no que tange aos processos e procedimentos necessários à ativação de um plano de DR.

# Definições

## Disaster Recovery

Disaster Recovery é um conjunto de processos, políticas e procedimentos, que permite manter operacional a infra-estrutura de TI essencial para o negócio da Empresa, em caso de desastres naturais ou por falhas humanas.

As diretrizes de Disaster Recovery devem estar contidas no PCN e devem conter todas as premissas para manutenção de aplicações, dados, equipamentos e redes de comunicação em caso de desastre.

**Tipos de desastre**

* Natural
  + Provocado ou não por fenômeno natural, como enchentes, terremotos e incêndios.
  + Difícil de ser previsto, porém precauções podem ser tomadas.
* Humano
  + Provocado por erro humano, intencional ou não, que acarreta em sucessivas falhas, tornando o negócio inoperante.
  + Nestes casos ainda podemos mencionar acidentes, sabotagens, greves, roubos, vírus e invasões.

## Alta Disponibilidade

A Alta Disponibilidade (HA) é a capacidade de manter um serviço operacional, mesmo em caso de falha de algum dos equipamentos que compõem o ambiente e sem percepção por parte do usuário final.

A implantação se faz através da criação de uma camada de abstração, dotada de inteligência para gerir os recursos abaixo dela e garantindo assim o perfeito funcionamento do serviço para o ambiente externo.

Existem duas formas de implantação para Alta Disponibilidade, uma é a redundância ativa, ou seja, que participa ativamente no provimento do serviço e assume a carga residual em caso de falha de um dos elementos, e outra é a redundância passiva ou failover, elemento secundário que permanece em estado de espera para o caso de falha do elemento principal.

## Cluster

Cluster é um conjunto de computadores que trabalham coordenadamente em uma determinada atividade. É um modelo computacional concebido da necessidade de aproveitar computadores de pequeno porte, para executarem atividades somente possíveis em plataformas de grande porte. O ganho desse modelo deriva da capacidade de distribuir as demandas de processamento entre os diversos computadores que compõem o cluster.

Atualmente a definição de cluster não se limita apenas a capacidade de processamento paralelo para uma determinada atividade. Existem modelos de alta disponibilidade e balanceamento de carga que são classificados pelo mercado como clusters, como por exemplo, Web Farms. No caso de soluções mais especializadas e comerciais, podemos citar Oracle RAC, Microsoft Cluster Server, Veritas Cluster Server e outros.

## Ambiente

Para a definição do modelo mais adequado de DR e HA, é recomendado que se faça a divisão dos serviços em camadas. Neste documento optou-se por utilizar quatro camadas, a saber: apresentação, aplicação, banco de dados e armazenamento.

A adoção de algum dos modelos deverá ser condicionada ao tipo de serviço que cada camada provê e ao nível de criticidade que ela representa no contexto do negócio. Os modelos adotados para cada caso podem ser mistos de HA e DR.



# Modelos Propostos

Os modelos propostos não se referem diretamente a um serviço nas camadas já mencionadas, e sim modelos de referência para a guarda da informação de forma segura e manutenção de serviços.

**Modelos de DR**

* **Modelo 1 - Backup off-site**
  + Procedimento de backup realizado remotamente através de robôs e fitas, em site distinto da origem dos dados.
* **Modelo 2 – Réplica de armazenamento off-site**
  + Procedimento de cópia entre subsistemas de armazenamento localizados em sites distintos.

**Modelos de HA**

* **Modelo 3 - Contingência local**
  + Infraestrutura redundante para execução das aplicações em site local.
* **Modelo 4 - Contingência off-site**
  + Infraestrutura redundante para execução das aplicações em site remoto.

**Modelos compostos de DR + HA**

* **Modelo 5 – Réplica de armazenamento off-site e contingência local** 
  + Procedimento de cópia entre subsistemas de armazenamento localizados em sites distintos com contingência local.
* **Modelo 6 – Réplica de armazenamento off-site e contingência remota** 
  + Infraestrutura com backup off-site e contingência em site remoto.

### DR - Modelo 1 - Backup Off-site

Modelo que estabelece a realização de backup em fitoteca robotizada em ambiente remoto, ou seja, envio dos dados críticos para uma localidade diferente do site principal. Ambiente focado na proteção das informações quando não houver necessidade de retorno imediato do serviço.



**Funcionamento**

Após o término do backup no site local, os dados serão duplicados em um robô localizado no site remoto por meio da rede SAN. Além da réplica dos dados das aplicações no site remoto, também será realizada a cópia do catalogo do servidor de backup.

Em caso de perda do site local, um servidor de backup será instalado, utilizando o respectivo catalogo replicado, permitindo assim a devida restauração em caso de desastre dos dados replicados na fitoteca remota.

**Recursos**

* Infraestrutura Remota
  + Robô de backup;
* Comunicação
  + Adequação da transmissão ao volume de dados transferidos pela SAN no procedimento de backup;
  + Roteamento entre redes SAN de backup, mantendo desta forma o isolamento das redes SAN de backup locais;

**Considerações**

* Sempre que possível, a cópia do backup deve ser armazenada em sala cofre.
* Deve ser realizado backup off-site do catalogo do servidor de backup;
* Opcionalmente, caso a infraestrutura não permita a realização de backup remoto conforme proposto, poderá ser adotada a estratégia de transporte das cópias das mídias de backup entre os sites.

|  |
| --- |
| Características |
| Guarda dos dados em sites geograficamente distribuídos |
| RTO – **\*** horas/dias |
| RPO – último backup realizado |

\* Depende do volume de dados em backup.

### DR - Modelo 2 - Replicação de armazenamento off-site

Modelo que estabelece a réplica de discos em sites geograficamente distribuídos, buscando garantir a proteção dos dados em caso de falha do site principal. Este modelo permite uma recuperação dos dados mais rápida em relação ao modelo de *Backup off-site.*



**Funcionamento**

No site remoto será disponibilizado um storage com capacidade para réplica dos volumes de dados do storage do site principal. Será implantado o roteamento SAN entre o site principal e o remoto. Através do recurso de cópia remota será realizada uma replicação periódica dos volumes do site principal no storage do site remoto. Poderão ser utilizados métodos de réplicas síncronos ou assíncronos, devendo ser analisados caso a caso.

Para garantir a existência da cópia remota durante o processo de replicação, devem ser utilizadas técnicas de snapshot da cópia remota.

As políticas de backup no site principal não sofrem nenhuma alteração e no site remoto não será realizado backup em fita.

Em caso de perda do storage do site principal, a aplicação poderá montar a cópia do volume remotamente, até que o volume principal seja re-estabelecido.

**Recursos**

* Infraestrutura Local
  + Licença de réplica remota de dados no storage;
* Infraestrutura Remota
  + Storage com capacidade para receber a replicação;
  + Licença de réplica remota de dados no storage;
  + Licença de snapshot no storage;
* Comunicação
  + Adequação da transmissão ao volume de dados transferidos pela SAN no procedimento de sincronização de volumes;
  + Roteamento para redes SAN;

**Considerações**

* O modelo apresentado não permite à restauração dos dados no site remoto em data retroativa, pois representa uma cópia do presente.
* A adoção de um intervalo maior de sincronizações de dados entre os storages permite também a recuperação dos dados do site principal em caso de falha lógica, adicionalmente à falha física, objetivo principal deste modelo.
* No caso da infraestrutura não permitir a adoção do modelo proposto, opcionalmente poderá ser disponibilizado um storage adicional no site local para realização da replicação de discos, agregando desta forma uma proteção em caso de perda do storage principal. Ou seja, neste caso não haverá proteção em caso de perda do site principal;

|  |
| --- |
| Características |
| Cópia do volume de produção em site remoto |
| RTO – minutos/horas |
| RPO – última sincronização dos dados |

### HA - Modelo 3 - Contingência Local

Modelo que especifica a disponibilização de ambiente de contingência em site local e é destinado a aplicações onde há impacto nas operações da empresa.

Fornece proteção aos serviços em caso de falha de componentes de hardware e software que compõe a solução. Não garante a disponibilidade em caso de desastre no site local.



**Funcionamento**

Um ou mais servidores fornecerão redundância física e lógica de forma transparente para o cliente. Os servidores poderão operar em dois modos, distribuição de carga ou failover. A distribuição de carga consiste na divisão das requisições direcionadas ao serviço entre os servidores que compõem a solução. Failover é um modo onde o servidor secundário só entra em operação caso o principal esteja indisponível.

No caso da perda de um dos servidores, o impacto no funcionamento dos serviços prestados por ele será minimizado, pois outro servidor assumirá as atividades de forma automática. Para que ocorra a distribuição automática de carga é necessário que se tenha um software especializado como o Heartbeat, o suporte nativo na aplicação como no caso do Oracle RAC ou balanceadores de carga.

No caso da utilização de balanceadores de carga, serão eles os responsáveis por gerenciar a distribuição do tráfego e o contingenciamento em caso de falha.

No caso do armazenamento, o volume principal será compartilhado para todos os servidores da solução, dessa forma a perda de um dos servidores não impacta na disponibilidade dos dados.

**Recursos**

* Infraestrutura Local
  + Disponibilização de servidor(es) secundário(s) para contingência ativa ou passiva dimensionado para sustentar o serviço em caso de perda do servidor principal;
  + Disponibilização de conectividade Ethernet redundante;
  + Disponibilização de conectividade SAN redundante;
  + Balanceador de carga; (caso necessário)
  + Solução de cluster (Ex. Veritas Cluster); (caso necessário)

**Considerações**

* É importante salientar que o modelo não garante a manutenção dos serviços em caso de perda do site principal;
* Não fornece disponibilidade para a camada de armazenamento. Se houver necessidade de se prover proteção aos dados, o modelo pode ser complementado com o de Backup off-site ou Replicação de armazenamento off-site.

|  |
| --- |
| Características |
| Redundância de comunicação |
| Contingência em caso de perda do servidor principal |
| **\*** RTO – segundos/minutos |
| **\*** RPO – segundos |

\* Não compreende falhas na camada de armazenamento.

### HA – Modelo 4 Contingência off-site

Modelo que estabelece contingência geograficamente distribuída, podendo ser ativa ou passiva e com infraestrutura independente. Permite a proteção aos dados e garantia de alta disponibilidade dos serviços.



**Funcionamento**

No caso deste modelo, a distribuição de servidores para redundância passa a ser geográfica. O(s) servidor(es) presente(s) no site remoto passam a garantir a disponibilidade dos serviços mesmo em caso de perda do site principal. As requisições para os serviços serão distribuídas entre os dois sites, no caso da contingência ativa ou apenas para o site principal no caso de contingência passiva. Para o caso de contingência ativa, serão disponibilizados balanceadores com suporte a GLB (Global Load Balancing) para realizarem a distribuição de tráfego entre o site principal e o remoto. No caso de contingência passiva, a solução pode ser implantada por meio de software especializado (Ex. Veritas) ou por suporte nativo da aplicação.

Em termos de armazenamento, só haverá um volume em produção por vez, devendo ele ser replicado para o site remoto através do modelo de Replicação de armazenamento off-site. Em caso de perda do servidor principal, não haverá necessidade de montagem do volume replicado no site remoto, pois o servidor secundário já possui o volume do site principal montado. No caso de perda total do site principal ou do storage principal, o volume replicado será montado em produção para que o servidor do site remoto passe a atender os serviços imediatamente.

**Recursos**

* Infraestrutura Local
  + Disponibilização de conectividade ethernet redundante;
  + Disponibilização de conectividade SAN redundante;
  + Disponibilização de balanceador de carga com suporte a GLB; (caso necessário)
  + Solução de cluster; (caso necessário)
* Infraestrutura Remota
  + Servidor(es) secundário(s) ativos ou passivos capazes de assumir toda a demanda do site principal;
  + Disponibilização de conectividade Ethernet redundante;
  + Disponibilização de conectividade SAN redundante;
  + Disponibilização de balanceador de carga com suporte a GLB; (caso necessário)
  + Solução de cluster; (caso necessário)
* Comunicação
  + Roteamento para redes SAN;
  + Implantação de balanceamento entre os sites pelo uso de Global Load Balance (GLB); (caso necessário)

**Considerações**

* Caso ocorra a perda do volume em produção no site principal e o volume replicado no site remoto seja ativado, é necessário estabelecer os devidos procedimentos operacionais de sincronização de dados antes do retorno ao site principal quando a falha estiver normalizada.
* No caso de banco de banco de dados Oracle, pode ser adotada a solução de sincronização DataGuard , que mantém uma base replicada em standby com sincronismo automático com a produção, permitindo assim um rápido failover em caso de falha;

|  |
| --- |
| Características |
| Redundância de comunicação |
| Contingência em caso de perda do servidor principal |
| Contingência em caso de perda do site principal |
| RTO – segundos/minutos/horas |
| RPO – segundos/minutos |

### Composto - Modelo 5 - Réplica de armazenamento off-site e Contingência local

Composição de referência que faz uso dos modelos de *Réplica de armazenamento off-site* e *Contingência local*, com ou sem o uso de balanceadores de carga. O recurso de contingência local pode ser ativado manual ou automaticamente, através do uso de balanceadores de carga.



**Funcionamento**

Será disponibilizada contingência local física e lógica para o(s) servidor(es) e uma replicação dos volumes de produção em storage remoto através da rede SAN de produção. Os servidores poderão possuir em sua camada de rede equipamentos para balanceamento de carga e operar em modo failover manual.

No caso de perda do storage principal, o(s) servidor(es) poderão acessar o volume replicado no site remoto para manter o serviço operacional. A mudança de volume deverá ser realizada manualmente. No caso de perda total do site principal os dados de produção estarão disponíveis no volume replicado no storage do site remoto. O procedimento de backup no site principal permanece inalterado.

**Recursos**

* Infraestrutura Local
  + Disponibilização de servidor(es) secundário(s) para contingência passiva, dimensionado para sustentar o serviço em caso de perda do servidor principal;
  + Disponibilização de conectividade ethernet redundante;
  + Disponibilização de conectividade SAN redundante;
  + Licença de réplica remota de dados no storage;
* Infraestrutura Remota
  + Storage com capacidade para receber a replicação;
  + Licença de réplica remota de dados no storage;
  + Licença de snapshot no storage;
* Comunicação
  + Adequação da transmissão ao volume de dados transferidos pela SAN no procedimento de sincronização de volumes;
  + Roteamento para redes SAN;

**Considerações**

* O modelo apresentado, não permite à restauração dos dados no site remoto baseado em uma data inferior a última sincronização;
* É importante salientar que o modelo não garante a manutenção dos serviços em caso de perda do site principal;

|  |
| --- |
| Características |
| Redundância de comunicação |
| Contingência em caso de perda do servidor principal |
| Réplica do volume em produção no site remoto |
| RTO – minutos |
| RPO – \* N/A |

\* Depende da última sincronização realizada.

### Composto - Modelo 6 - Réplica de armazenamento off-site e contingência remota

Composição de referência que faz uso dos modelos de *Réplica de armazenamento off-site* e *Contingência Remota*, com ou sem o uso de balanceadores de carga. O recurso de contingência remota pode ser ativado manual ou automaticamente, através do uso de balanceadores de carga.



**Funcionamento**

Em relação ao modelo anterior, a distribuição de servidores para redundância passa a ser geográfica. O(s) servidor(es) presente(s) no site remoto passam a garantir a disponibilidade dos serviços mesmo em caso de perda do site principal. As requisições para os serviços poderão ser direcionadas preferencialmente para o site principal ou para ambos os sites. O servidor réplica no site remoto será dimensionado para assumir o processamento do principal, com uma pequena degradação de desempenho.

Em termos de armazenamento, só haverá um volume em produção por vez, através do modelo de *Replicação de armazenamento off-site*. Em caso de perda do servidor principal, não haverá necessidade de montagem do volume replicado no site remoto, podendo o servidor réplica no site remoto acessar diretamente o volume em produção no site principal. No caso de perda total do site principal, o volume replicado será montado em produção para que o servidor do site remoto passe a atender os serviços imediatamente. Vale salientar que caso não se opte pelo uso de balanceadores de carga, a ativação da contingência será realizada manualmente e apenas em caso de desastre. O backup será realizado individualmente em cada site com infra-estrutura própria, ou seja, o site principal do volume em produção e o site remoto do volume replicado.

**Recursos**

* Infraestrutura Local
  + Disponibilização de conectividade ethernet redundante;
  + Disponibilização de conectividade SAN redundante;
  + Licença de réplica remota de dados no storage;
* Infraestrutura Remota
  + Servidor(es) secundário(s) passivos capazes de assumir toda a demanda do site principal;
  + Disponibilização de conectividade Ethernet redundante;
  + Disponibilização de conectividade SAN redundante;
  + Storage com capacidade para receber a replicação;
  + Licença de réplica remota de dados no storage;
  + Licença de snapshot no storage;
* Comunicação
  + Adequação da transmissão ao volume de dados, levando em consideração e sincronismo de volumes de dados;
  + Roteamento para redes SAN;
  + Uso do recurso de Cópia Remota de discos (Ex. Metro Mirror);

**Considerações**

* Caso ocorra a perda do volume em produção no site principal, é importante lembrar que o volume replicado sofrerá alterações em decorrência de sua montagem para produção, por esse motivo é necessário que se sincronize novamente os discos antes de levantar o volume de produção do site principal novamente;
* No caso de banco de banco de dados Oracle, pode ser adotada a solução de sincronização DataGuard , que mantém uma base replicada em standby com sincronismo automático com a produção, permitindo assim um rápido failover em caso de falha;

|  |
| --- |
| Características |
| Redundância de comunicação |
| Contingência em caso de perda do servidor principal |
| Contingência em caso de perda do site principal |
| Recuperação imediata em caso de desastre |
| RTO – minutos |
| RPO – minutos |

# Recomendações

## Geral

Deve-se avaliar antes de se escolher um modelo, o tempo de interrupção para cada plataforma segundo o impacto no negócio, ou seja, é necessário definir o SLA requerido da infraestrutura.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Tipo** | | **Retorno operacional** | | | **Disponibilidade** | | | **Custo** | | |
| **Modelos** | **DR** | **HA** | **minutos** | **horas** | **dias** | **Alta** | **Média** | **Baixa** | **Alto** | **Médio** | **Baixo** |
| **1** | **x** |  |  | **x** | **x** |  |  | **x** |  |  | **x** |
| **2** | **x** |  | **x** | **x** |  |  | **x** |  |  | **x** |  |
| **3** |  | **x** | **x** |  |  |  | **x** |  |  | **x** |  |
| **4** |  | **x** | **x** |  |  | **x** |  |  | **x** |  |  |
| **5** | **x** | **x** | **x** |  |  |  | **x** |  |  | **x** |  |
| **6** | **x** | **x** | **x** |  |  | **x** |  |  | **x** |  |  |

Tabela de classificação de disponibilidade

## Site Remoto

No caso de utilização de site remoto é recomendado que o mesmo se encontre a uma distância mínima do site principal, essa distância varia de acordo com o risco presente na localidade principal.

Abaixo uma tabela que apresenta os riscos associados ao site principal e a distância ideal (aproximada) para uma contingência, segundo a ACP (Association of Contingency Planners).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risco | Dist. Site Remoto |  | Risco | Dist. Site Remoto |
| **Furação** | 168 km |  | **Incêndio Florestal** | 67 km |
| **Vulcão** | 120 km |  | **Torres de alta tensão** | 50 km |
| **Neve** | 109 km |  | **Tornado** | 46 km |
| **Terremoto** | 96 km |  | **Central Telefônica** | 45 km |
| **Tsunami** | 82 km |  | **Aeroporto** | 42 km |
| **Inundação** | 74 km |  | **Nenhum** | 34 km |
| **Instalação Militar** | 70 km |  |  |  |

## Aplicações Web

Aplicações Web devem preferencialmente adotar ambientes compartilhados em Web Farms (cluster), que possuam ao menos o modelo de contingência local, ativa ou passiva.

No caso da adoção de um modelo de *Contingência off-site*, faz-se necessária a adoção de um balanceador de carga em modo GLB (Global Load Balance) que tenha a capacidade de prover persistência de conexão e persistência ativa ou passiva de Cookies e SSL.

## Aplicações Cliente/Servidor

No caso de Servidores de aplicações que não possuam front-end em ambiente web, poderão ser adotados os modelos de *Contingência local* ou *off-site*.

Deverá ser utilizado um Load Balancer em modo de balanceamento de carga ou failover, com atuação até a camada 7. No caso de contingência remota, deverá ser adotado um Global Load Balancer, sendo que o equipamento deverá possuir redundância física e modo de recuperação de contexto (se aplicável).

É importante salientar que nem todas as aplicações conseguem operar com redundância tanto local quanto remota. É importante envolver o fornecedor da aplicação para alinhar as expectativas e estabelecer o modelo mais adequado para cada caso.

## Banco de Dados

Servidores de Banco de Dados considerados críticos devem adotar o modelo de *Contingência off-site* para assegurar a proteção dos dados em caso de desastre.

Preferencialmente, as bases de dados Oracle, devem adotar ambientes compartilhados em clusters, com escalabilidade horizontal como Oracle RAC. No caso de exceções, onde haja necessidade de ambiente dedicado, recomendamos a adoção dos modelos de *Replicação de armazenamento off-site.*

No caso de utilização de contingência remota, é necessário avaliar a capacidade de manutenção de instância remota on-line e seus requisitos no que tange o software de sincronização, como Oracle Data Guard.

## Armazenamento

Dados considerados críticos devem possuir cópia remota segundo os modelos de *Réplica de armaenamento off-site* e *Backup off-site*, com a finalidade de garantir a proteção aos dados em caso de desastre.

Para o caso de dados que tenha em sua camada de apresentação um ambiente de contingência, deverá ser disponibilizada uma réplica no site remoto onde se realiza a contingência. Considerar a aquisição de software de cópia remota de discos, tais como Metro Mirror, SRDF, etc

## Infraestrutura de Rede

A infraestrutura de rede deve ser configurada de acordo com as necessidades do ambiente de HA construído atendendo os seguintes requisitos:

* *Contingência Local*: utilizar ao menos 2 switches para conexão permitir que cada NIC do servidor seja conectada em switches diferentes, utilizando-se do recurso de NIC Team.
* *Contingência Off-site*: nos sistemas críticos utilizar switches com fonte e processamento redundante permitindo a conexão das NICs em módulos diferentes do mesmo switch.

É importante garantir que as conexões do Data Center com a rede corporativa seja feita de forma redundante para garantir o acesso do usuários aos sistemas instalados.

* Na transmissão recomenda-se o uso de caminhos físicos distintos.
* Requisitar do provedor de serviço de dados, acesso em equipamentos distintos na camada de distribuição/acesso.
* Utilizar protocolos de roteamento dinâmico para seleção automática de caminhos alternativos em caso de queda de enlaces.