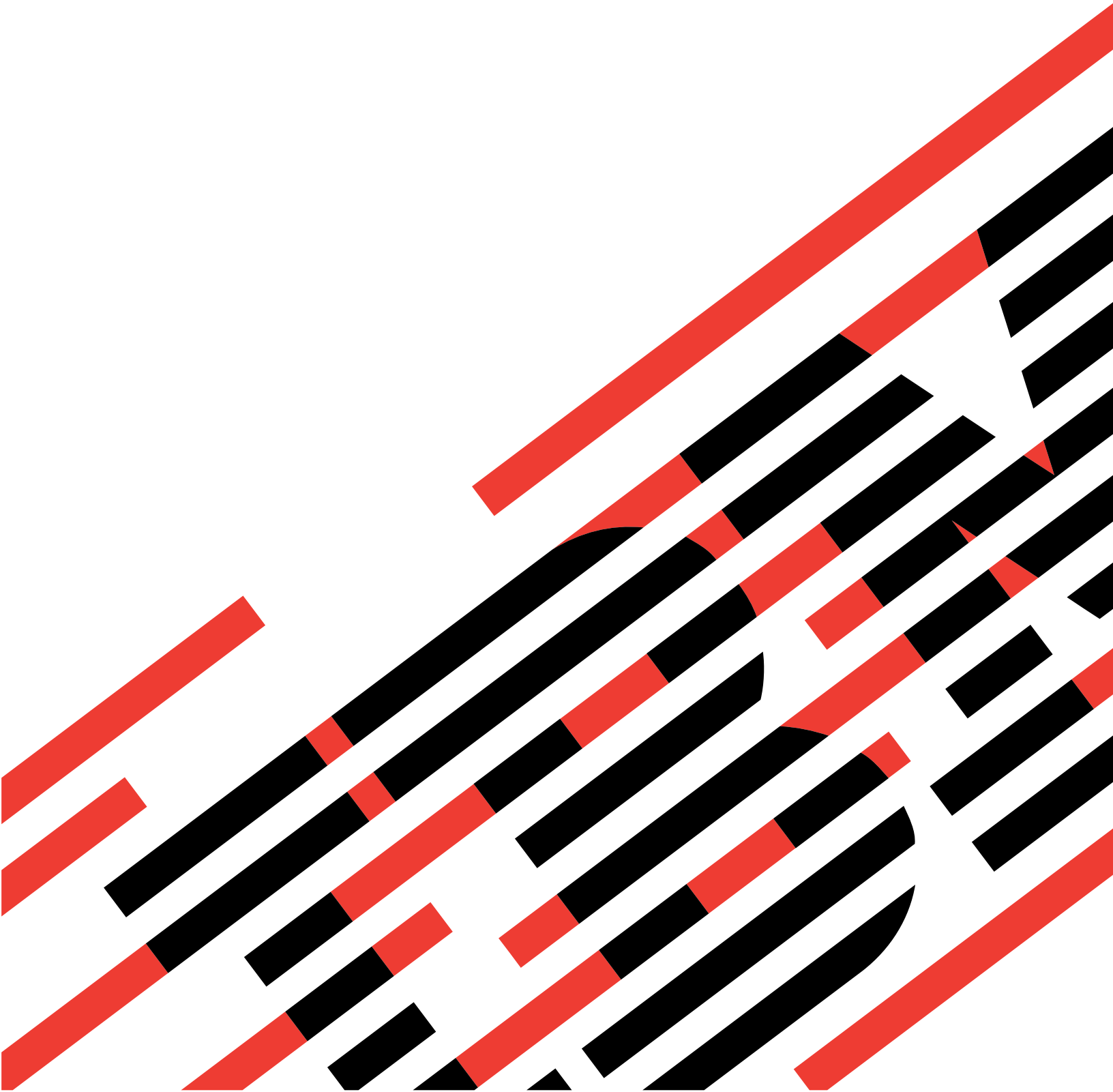
IBM

eserver

iSeries

Planear uma estratégia de cópia de segurança e recuperação



IBM

@server

iSeries

Planear uma estratégia de cópia de segurança e recuperação

Índice

Parte 1. Planear uma estratégia de cópia de segurança e recuperação 1

Capítulo 1. Calendário de cópia de segurança e recuperação 3

Capítulo 2. Saber o que guardar e com que frequência 5

Capítulo 3. Determinar a sua janela de salvaguarda 7
Estratégia de salvaguarda simples 7
Estratégia de salvaguarda média 8
Guardar objectos alterados 8
Registar objectos em diário e guardar receptores de diário 9
Estratégia de salvaguarda complexa 9

Capítulo 4. Escolher as opções de disponibilidade 11

Capítulo 5. Testar a estratégia 13

Capítulo 6. Plano de recuperação de desastres—modelo 15
Plano de Recuperação de Desastres 15
Descrição da imagem 24

Parte 1. Planear uma estratégia de cópia de segurança e recuperação

Os computadores em geral e os servidores iSeries™ em particular, são extremamente fiáveis. Pode trabalhar no sistema durante meses, ou mesmo anos, sem ter quaisquer problemas que ponham em risco as informações contidas no sistema. No entanto, ao mesmo tempo que diminui a ocorrência destes problemas, aumenta o seu possível impacto. As empresas são cada vez mais dependentes dos computadores e das informações neles armazenadas. As informações que são guardadas no computador podem não existir em mais lado nenhum.

Guardar informações no sistema consome tempo e requer disciplina. Porque motivo deve fazê-lo? Porque motivo deve gastar tempo no respectivo planeamento e avaliação?

Porque pode ocorrer um problema. Nesse caso, **vai** precisar de utilizar as suas cópias de segurança das informações. Cada sistema tem de restaurar algumas ou todas as informações que contém numa determinada altura.

O Calendário de cópia de segurança e recuperação fornece uma descrição geral detalhada dos eventos que ocorrem durante o processo de cópia de segurança e recuperação.

Depois de compreender porque precisa de um calendário de cópia de segurança e recuperação, está pronto para começar a planear a sua estratégia. Siga estes passos:
1. Saber o que guardar e com que frequência
2. Determinar a sua janela de salvaguarda
3. Escolher as opções de disponibilidade
4. Testar a estratégia

O Modelo do plano de recuperação de desastres também pode ser útil como recurso de planeamento.

Este tópico contém informações sobre como planear a sua estratégia e seleccionar as opções necessárias à medida que configura o sistema para cópia de segurança, recuperação e disponibilidade. Para obter mais informações sobre como executar realmente as tarefas relacionadas com estes tópicos,

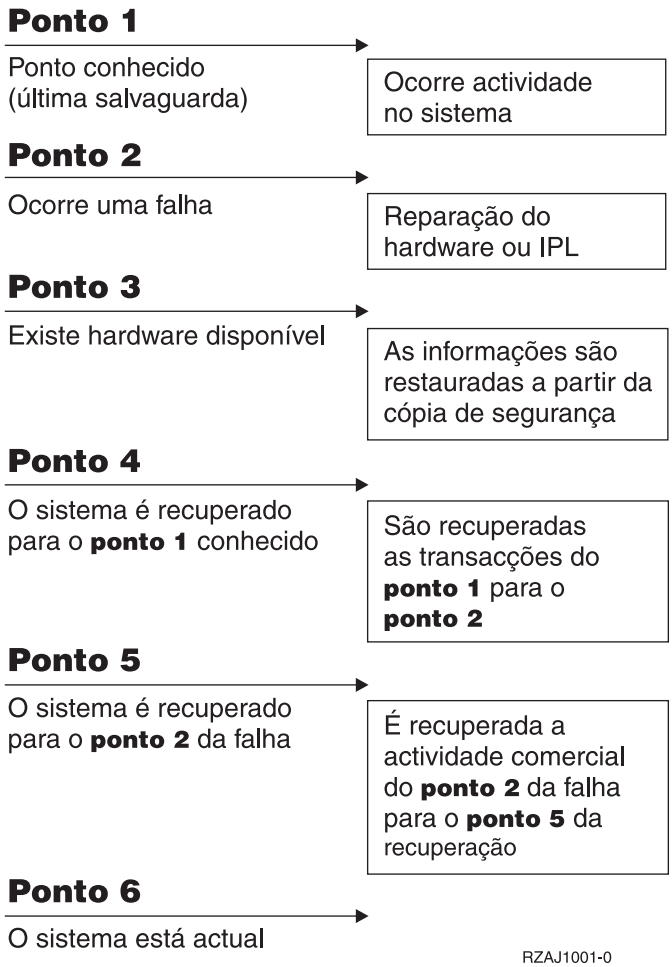
consulte o manual Cópia de Segurança e Recuperação  e o tópico Cópia de segurança do servidor. O tópico Guia de consulta rápida disponível para o servidor iSeries fornece informações sobre os tipos comuns de falhas que podem ocorrer.

Capítulo 1. Calendário de cópia de segurança e recuperação

O calendário de cópia de segurança e recuperação começa quando guarda as informações e termina quando o sistema recupera totalmente após uma falha. Consulte este calendário enquanto lê estas informações e toma decisões. As suas estratégias de salvaguarda e disponibilidade determinam o seguinte:

- Se pode concluir cada etapa do quadro com êxito
- O tempo que demorará a concluir cada etapa

À medida que for lendo, use o quadro para desenvolver exemplos específicos. E se o ponto conhecido (1) for domingo à noite e o ponto da falha (2) for quinta-feira à tarde? Quanto tempo demorará a voltar ao ponto conhecido? Quanto tempo demorará a voltar ao ponto actual (6)? E é possível com a estratégia de salvaguarda que planeou?



Capítulo 2. Saber o que guardar e com que frequência

Deve guardar todo o conteúdo do sistema com a maior frequência possível. Pode não estar preparado para recuperar de uma perda de local ou de determinados tipos de falhas de disco se não guardar tudo com regularidade. Se guardar as partes correctas do servidor iSeries, poderá recuperar até ao ponto 4 (a última salvaguarda) apresentado no calendário de cópia de segurança e recuperação. Deve guardar as partes do sistema que são alteradas diariamente. Deve guardar as partes do sistema que não são alteradas frequentemente todas as semanas.

Partes do sistema que são alteradas com frequência

Esta tabela mostra as partes do sistema que são alteradas com frequência e que, por isso, devem ser guardadas diariamente:

Tabela 1. Itens a guardar diariamente: Partes do sistema alteradas com frequência

Descrição do Item	Fornecido pela IBM®?	Quando Ocorrem as Alterações
Informações de segurança (perfis de utilizador, autoridades privadas, listas de autorização)	Alguns	Regularmente, à medida que são adicionados novos utilizadores e objectos ou as autoridades são alteradas[1]
Objectos de configuração na QSYS	Não	Regularmente, quando são adicionadas ou alteradas descrições de dispositivo ou quando utiliza a função Gestor de Serviço de Hardware para actualizar as informações de configuração[1]
Bibliotecas fornecidas pela IBM que contêm dados de utilizador (QGPL, QUSRSYS)	Sim	Regularmente
Bibliotecas de utilizador que contêm dados de utilizador e programas	Não	Regularmente
Arquivadores e documentos	Alguns	Regularmente, se utilizar estes objectos
Distribuições	Não	Regularmente, se utilizar a função de distribuição
Directórios de utilizador	Não	Regularmente

1 Estes objectos podem também ser alterados quando actualiza programas licenciados.

Partes do sistema que não são alteradas com frequência

Esta tabela mostra as partes do sistema que não são alteradas com frequência; pode guardá-las semanalmente.

Tabela 2. Itens a guardar semanalmente: Partes do sistema que não são alteradas frequentemente

Descrição do Item	Fornecido pela IBM?	Quando Ocorrem as Alterações
Código Interno Licenciado	Sim	PTFs ou nova edição do sistema operativo
Objectos do sistema operativo na biblioteca QSYS	Sim	PTFs ou nova edição do sistema operativo
Bibliotecas opcionais do Operating System/400 (QHLPSYS, QUSRTOOL)	Sim	PTFs ou nova edição do sistema operativo
Bibliotecas de programas licenciados (QRPG, QCBL, Qxxxx)	Sim	Actualizações de programas licenciados
Arquivadores de programas licenciados (Qxxxxxxx)	Sim	Actualizações de programas licenciados

Tabela 2. Itens a guardar semanalmente: Partes do sistema que não são alteradas frequentemente (continuação)

Descrição do Item	Fornecido pela IBM?	Quando Ocorrem as Alterações
Directórios de programas licenciados (/QIBM/ProdData, /QOpenSys/QIBM/ProdData)	Sim	Actualizações de programas licenciados

Capítulo 3. Determinar a sua janela de salvaguarda

Na realidade, o momento em que executa procedimentos de salvaguarda, o modo como os executa e os itens que guarda dependem do tamanho da sua janela de salvaguarda. A sua **janela de salvaguarda** é a quantidade de tempo que o sistema pode não estar disponível para os utilizadores enquanto as operações guardar são executadas. Para simplificar a recuperação, necessita de guardar quando o sistema se encontrar num ponto conhecido e os dados não estiverem a ser alterados.

Quando seleccionar uma estratégia de salvaguarda, deve equilibrar aquilo que os utilizadores consideram uma janela de salvaguarda aceitável com o valor dos dados que pode perder e a quantidade de tempo pode demorar a recuperar.

Se o sistema for tão importante para a sua empresa de modo a que já não seja possível gerir a janela de salvaguarda, é provável que também não tenha capacidade para uma desactivação não marcada. Deve avaliar seriamente todas as opções de disponibilidade do servidor iSeries, incluindo conjuntos de unidades. O tópico Guia de consulta rápida disponível para o servidor iSeries contém informações adicionais sobre as opções disponíveis.

Escolha uma das seguintes estratégias de salvaguarda, com base no tamanho da sua janela de salvaguarda. A seguir, avalie novamente a sua decisão com base no modo como a sua estratégia de salvaguarda o posiciona para uma recuperação.

- Estratégia de salvaguarda simples
  Tem uma janela de salvaguarda grande, o que significa que dispõe diariamente de um período de 8 a 12 horas sem actividade do sistema (incluindo trabalho batch).
- Estratégia de salvaguarda média
  Tem uma janela de salvaguarda média, o que significa que dispõe diariamente de um período de tempo mais reduzido (4 a 6 horas) sem actividade do sistema.
- Estratégia de salvaguarda complexa
  Tem uma janela de salvaguarda pequena, o que significa que dispõe de pouco ou nenhum tempo quando o sistema não está a ser utilizado para trabalho interactivo ou batch.

Estratégia de salvaguarda simples

A estratégia de salvaguarda mais simples é guardar tudo todas as noites (ou fora do horário de expediente). Pode utilizar a opção 21 (Todo o sistema) do menu Guardar para efectuar esta acção. Pode marcar a execução da opção 21 sem ser necessário um operador (não assistida), para ser iniciada a uma determinada hora.

Pode também utilizar este método para guardar todo o sistema após a actualização para uma nova edição ou aplicar correcções temporárias de programa (PTFs).

Pode concluir que não tem tempo suficiente ou capacidade de unidade de bandas suficiente para executar a opção 21 sem um operador. Mesmo assim, poderá empregar uma estratégia simples:

Diária	Guardar tudo aquilo que é alterado frequentemente.
Semanal	Guardar aquilo que não é alterado frequentemente.

A opção 23 (Todos os dados do utilizador) do menu Guardar guarda os itens que são alterados com regularidade. A opção 23 pode ser programada para execução não assistida. Para executar esta operação sem assistência, tem de ter capacidade de suporte de cópia de segurança online suficiente.

Se o seu sistema tiver um longo período de inactividade durante o fim-de-semana, a sua estratégia de salvaguarda pode assemelhar-se ao seguinte:

Sexta-feira à noite	Opção 21 do menu Guardar
Segunda-feira à noite	Opção 23 do menu Guardar
Terça-feira à noite	Opção 23 do menu Guardar
Quarta-feira à noite	Opção 23 do menu Guardar
Quinta-feira à noite	Opção 23 do menu Guardar
Sexta-feira à noite	Opção 21 do menu Guardar

Estratégia de salvaguarda média

Pode concluir que não tem uma janela de salvaguarda suficientemente longa para utilizar uma estratégia de salvaguarda simples. Talvez possa executar grandes trabalhos batch no seu sistema à noite. Também pode ter ficheiros muito grandes que demoram muito tempo a guardar. Se for o caso, pode ter de desenvolver uma estratégia de salvaguarda média, o que significa que a complexidade da operação guardar e recuperar é média.

Quando desenvolver uma estratégia de salvaguarda média, aplique o seguinte princípio: quanto mais frequentes forem as alterações, mais frequentes devem ser as operações guardar. Basta avaliar com mais detalhe a frequência com que são feitas alterações do que o faz quando utiliza uma estratégia simples.

Estão disponíveis várias técnicas a utilizar numa estratégia de salvaguarda média. Pode utilizar uma destas técnicas ou uma combinação das mesmas.
- Guardar objectos alterados
- Registar em diário objectos e guardar os receptores de diário

Guardar objectos alterados

Pode utilizar vários comandos para guardar apenas informações que tenha alterado desde a última operação guardar ou desde uma data e hora específica.

Pode utilizar o comando Guardar Objectos Alterados (SAVCHGOBJ) para guardar apenas os objectos que tenham sido alterados desde a última vez que uma biblioteca ou grupo de bibliotecas foi guardado. Isto pode ser particularmente útil numa situação em que os programas e dos ficheiros de dados se encontram na mesma biblioteca. Normalmente, os ficheiros de dados são alterados frequentemente e os programas são alterados pouco frequentemente. Pode utilizar o comando SAVCHGOBJ para guardar apenas os ficheiros que são alterados.

Pode utilizar o comando Guardar Objecto da Biblioteca de Documentos (SAVDLO) para guardar apenas os documentos e arquivadores que foram alterados. Da mesma forma, pode utilizar o comando Guardar (SAV) para guardar objectos em directórios que tenham sido alterados a partir de um ponto determinado.

Também pode optar por guardar objectos alterados se o seu volume de trabalho batch for maior em determinadas noites. Por exemplo:

Dia	Volume de Trabalho do Batch	Operação Guardar
Sexta-feira à noite	Parcial	Opção 21 do menu Guardar
Segunda-feira à noite	Completo	Guardar apenas as alterações[1]
Terça-feira à noite	Parcial	Opção 23 do menu Guardar
Quarta-feira à noite	Completo	Guardar apenas as alterações[1]
Quinta-feira à noite	Completo	Guardar apenas as alterações[1]
Sexta-feira à noite	Parcial	Opção 21 do menu Guardar

1 Utilize uma combinação dos comandos SAVCHGOBJ, SAVDLO e SAV.

Registar objectos em diário e guardar receptores de diário

Se as operações guardar dos ficheiros de base de dados demorarem demasiado porque os ficheiros são demasiado grandes, a salvaguarda de objectos alterados poderá não ser útil. Se tiver um membro de ficheiro com 100.000 registos e 1 registo for alterado, o comando SAVCHGOBJ guarda o membro de ficheiro completo. Nesta situação, o registo em diário de ficheiros de base de dados e a salvaguarda dos receptores de diário pode ser uma solução melhor, mesmo que a recuperação seja mais complexa.

Um princípio semelhante é aplicável a objectos de sistema de ficheiros integrados e áreas de dados. Se as operações de salvaguarda de objectos de sistemas de ficheiros integrados e de áreas de dados for demasiado demorada, pode optar por registar em diário os objectos de modo a tornar estas operações mais eficazes. A salvaguarda de receptores de diário poderá ser uma melhor opção.

Quando regista objectos em diário, o sistema escreve uma cópia de todas as alterações efectuadas no objecto para um receptor de diário. Quando guarda um receptor de diário, está a guardar apenas as partes alteradas do objecto, e não o objecto na sua totalidade.

Se registar os objectos em diário e se o volume de trabalhos batch for variável, a estratégia de salvaguarda pode ter o seguinte aspecto:

Dia	Volume de Trabalho do Batch	Operação Guardar
Sexta-feira à noite	Parcial	Opção 21 do menu Guardar
Segunda-feira à noite	Completo	Guardar receptores de diário
Terça-feira à noite	Parcial	Opção 23 do menu Guardar
Quarta-feira à noite	Completo	Guardar receptores de diário
Quinta-feira à noite	Completo	Guardar receptores de diário
Sexta-feira à noite	Parcial	Opção 21 do menu Guardar

Notas:

1. Para tirar partido da protecção fornecida pelo registo em diário, deve desligar e guardar receptores de diário regularmente. A frequência com que os guarda depende do número de alterações registadas em diário que ocorrem. Guardar os receptores de diário várias vezes ao dia pode ser adequado ao seu caso. O modo como guarda os receptores de diário depende de estarem ou não numa biblioteca separada. Poderá utilizar o comando Guardar Biblioteca (SAVLIB) ou Guardar Objecto (SAVOBJ).
2. Deve guardar os objectos novos antes de poder aplicar entradas de diário ao objecto. Se as aplicações adicionarem novos objectos regularmente, deve considerar a utilização da estratégia SAVCHGOBJ isoladamente ou em combinação com o registo em diário.

No tópico Gestão de diário pode obter mais informações sobre diários.

Estratégia de salvaguarda complexa

Uma janela de salvaguarda de dimensões muito pequenas requer uma estratégia complexa de salvaguarda e recuperação. Utilize as mesmas ferramentas e técnicas descritas para uma estratégia de salvaguarda média, mas a um nível de detalhe superior. Por exemplo, pode ser necessário guardar ficheiros críticos específicos a horas específicas do dia ou da semana. Pode também considerar a utilização de uma ferramenta como, por exemplo, o Backup Recovery and Media Services for iSeries (BRMS).

Guardar o sistema enquanto está activo é muitas vezes necessário numa estratégia de salvaguarda complexa. O parâmetro Guardar Activo (SAVACT) é suportado nos seguintes comandos:

- Guardar Biblioteca (SAVLIB)
- Guardar Objecto (SAVOBJ)
- Guardar Objectos Alterados (SAVCHGOBJ)
- Guardar Objecto da Biblioteca de Documentos (SAVDLO)

- Guardar (SAV)

Se utilizar o suporte de guardar enquanto activo, pode reduzir significativamente a quantidade de tempo durante o qual os ficheiros não estarão disponíveis. Quando o sistema tiver estabelecido um ponto de verificação para todos os objectos que estão a ser guardados, os objectos poderão ficar disponíveis para utilização. É possível utilizar o suporte de guardar enquanto activo em conjunto com o registo em diário e o controlo de consolidações para simplificar o procedimento de recuperação. Se utilizar os valores *LIB ou *SYNCLIB com o parâmetro SAVACT, deve utilizar o registo em diário para simplificar a recuperação. Se utilizar o valor *SYSDFN com o parâmetro SAVACT, deve utilizar o controlo de consolidações caso a biblioteca que está a guardar tiver objectos de base de dados relacionados. Se optar por utilizar o suporte de guardar enquanto activo, certifique-se de que compreende o processo e até que nível os pontos de controlo estão a ser bem estabelecidos no sistema.

Também pode reduzir o período de tempo que os ficheiros não estão disponíveis executando operações guardar em mais de um dispositivo de cada vez ou executando **operações guardar simultâneas**. Por exemplo, pode guardar bibliotecas num dispositivo, arquivadores noutro e directórios num terceiro dispositivo. Também pode guardar diferentes conjuntos de bibliotecas ou objectos em dispositivos diferentes.

Se estiver a utilizar a V4R4 ou uma edição posterior, também pode utilizar múltiplos dispositivos em simultâneo executando uma **operação guardar paralela**. Para executar uma operação guardar paralela, necessita do Backup Recovery and Media Services ou de uma aplicação que lhe permita criar objectos de definição de suportes.

Para obter mais informações sobre o suporte de guardar enquanto activo, operação guardar simultâneas e operações guardar paralelas, consulte as informações Criar uma cópia de segurança doo servidor. O tópico Controlo de consolidações contém informações mais detalhadas sobre o controlo de consolidações. O tópico Gestão de diário contém informações mais detalhadas sobre registo em diário.

Capítulo 4. Escolher as opções de disponibilidade

As opções de disponibilidade são um complemento de uma boa estratégia de salvaguarda, mas não a substituem. As opções de disponibilidade podem reduzir significativamente o tempo que demora a recuperar após uma falha. Em alguns casos, as opções de disponibilidade podem impedi-lo de executar uma recuperação.

Para justificar o custo de utilização de opções de disponibilidade, tem de compreender:
- O valor fornecido pelo sistema.
- O custo de um estado de inactividade programado ou não programado.
- Quais são os seus requisitos de disponibilidade.

Seguem-se as opções de disponibilidade que pode utilizar para completar a sua estratégia de salvaguarda:
- A gestão de diário permite recuperar as alterações efectuadas em objectos desde a última salvaguarda completa.
- A protecção de caminhos de acesso permite-lhe recriar a ordem pela qual os registos de um ficheiro de base de dados são processados.
- Os conjuntos de discos limitam a quantidade de dados que tem de recuperar aos dados do conjunto de discos da unidade em falha.
- A protecção por paridade de dispositivos permite-lhe reconstruir dados perdidos; o sistema pode continuar em execução enquanto os dados estiverem a ser reconstruídos.
- A protecção por replicação ajuda-o a manter os dados disponíveis porque tem duas cópias dos dados em duas unidades de discos separadas.
- A repartição por conjuntos de unidades permite-lhe manter alguns dados ou mesmo a totalidade de dados em dois sistemas; o sistema secundário pode assumir os programas de aplicação se o sistema principal falhar.

O tópico Guia de consulta rápida disponível para o servidor iSeries contém informações que podem ser utilizadas para implementar uma solução disponível para o servidor iSeries.

Capítulo 5. Testar a estratégia

Se a sua situação requerer uma estratégia de salvaguarda média ou complexa, também irá requerer uma revisão regular, do seguinte modo:

- Está a guardar **tudo** ocasionalmente?
- O que necessita de fazer para recuperar para o ponto conhecido (4) no calendário de cópia de segurança e recuperação?
- Está a utilizar opções como registar em diário ou guardar objectos alterados para o ajudar a recuperar do ponto de falha (5)? Sabe como recuperar utilizando estas opções?
- Foram adicionadas novas aplicações? As novas bibliotecas, os novos arquivadores e directórios estão a ser guardados?
- Está a guardar as bibliotecas fornecidas pela IBM que contêm dados de utilizador (por exemplo, QGPL e QUSRSYS)?

  Nota: O tópico Valores especiais para o comando SAVLIB apresenta todas as bibliotecas fornecidas pela IBM que contêm dados de utilizador.
- A recuperação foi testada?

A melhor forma de testar a estratégia de salvaguarda é testar uma recuperação. Apesar de poder testar uma recuperação no seu próprio sistema, levá-la a cabo pode ser arriscado. Se não tiver guardado tudo com êxito, poderá perder informações quando tentar restaurar.

Existem várias organizações que prestam serviços de testes de recuperação. IBM Continuity and Recovery Services  é uma organização que pode ajudá-lo nos testes de recuperação.

Capítulo 6. Plano de recuperação de desastres—modelo

O objectivo de um plano de recuperação de desastres é garantir uma forma de estar preparado para recuperar de um desastre ou de qualquer outra emergência que afecte os sistemas de informação e, assim, minimizar o efeito no funcionamento da empresa. Este tópico fornece as directrizes para o tipo de informações e procedimentos que são necessários para recuperar de um desastre. Quando tiver preparado as informações descritas neste tópico, guarde o documento num local seguro e acessível, fora das instalações.

Segue-se um modelo a utilizar na criação do seu plano de recuperação de desastres. Pode consultar este modelo aqui; para o imprimir, transfira-o para o computador e imprima o ficheiro PDF relativo a este tópico.

Plano de Recuperação de Desastres

Secção 1. Principais objectivos deste plano

Os principais objectivos deste plano são:
- Minimizar interrupções nas operações normais.
- Limitar a extensão da interferência e dos danos.
- Minimizar o impacto económico da interrupção.
- Estabelecer antecipadamente meios alternativos de operação.
- Formar técnicos nos procedimentos de emergência.
- Proporcionar uma reposição simples e rápida do serviço.

Secção 2. Pessoal

Pessoal de processamento de dados			
Nome	**Posição**	**Endereço**	**Telefone**

Nota: Junte uma cópia do organograma da sua empresa a esta secção do plano.

Secção 3. Perfil da aplicação

Utilize o comando Ver Recursos de Software (DSPSFWRSC) para preencher esta tabela.

Perfil da aplicação				
Nome da Aplicação	**Crítica? Sim/Não**	**Activa? Sim/Não**	**Fabricante**	**Comentários**

Legenda de comentários:

1. Utilizada diariamente às _____.
2. Utilizada semanalmente às _____.
3. Utilizada mensalmente às _____.

Secção 4. Perfil do inventário

Utilize o comando Trabalhar com Produtos de Hardware (WRKHDWPRD) para preencher esta tabela. Esta lista deve incluir os seguintes elementos:

- Unidades de processamento
- Unidades de discos
- Modelos
- Controladores de estação de trabalho
- Computadores pessoais
- Estações de trabalho de reserva
- Telefones
- Ar condicionado ou aquecimento
- Impressora do sistema
- Unidades de bandas e de disquetes
- Controladores
- Processadores de I/O
- Comunicações de dados gerais
- Monitores de reserva
- Bastidores
- Humidificador ou desumidificador

Perfil do inventário					
Fabricante	**Descrição**	**Modelo**	**Número de Série**	**Próprio ou Alugado**	**Custo**

Perfil do inventário					
Fabricante	**Descrição**	**Modelo**	**Número de Série**	**Próprio ou Alugado**	**Custo**
Nota: Deve ser feita uma auditoria desta lista de _____ em _____ meses.					

Inventário diverso		
Descrição	**Quantidade**	**Comentários**

Nota: Esta lista deve incluir os seguintes elementos:
- Bandas
- Software de PC (por exemplo, DOS)
- Documentação ou conteúdo dos armários de arquivo
- Conteúdo do cofre das bandas
- Disquetes
- Pacotes de emulação
- Software de linguagens (por exemplo, COBOL e RPG)
- Consumíveis de impressora (por exemplo, papel e impressos)

Secção 5. Procedimentos de cópia de segurança dos serviços de informação

- Servidor iSeries
  - Os receptores de diário são alterados diariamente às _____ e às _____.
  - Os objectos alterados são guardados diariamente nas seguintes bibliotecas às _____:
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____

    Este procedimento também guarda os diários e os receptores de diário.
  - No dia _____ às _____ é efectuada uma salvaguarda de todo o sistema.
  - Todos os suportes de salvaguarda são armazenados fora da empresa, num cofre, na localização _____.
- Computador Pessoal
  - É aconselhável fazer cópias de segurança de todos os computadores pessoais. As cópias dos ficheiros de PC devem ser transferidas para o servidor no dia _____ (data) às _____ (hora), imediatamente antes de uma salvaguarda completa. Em seguida, é guardado com o procedimento normal para guardar o sistema. Isto possibilita uma cópia de segurança mais segura de sistemas relacionados com o computador pessoal, em que um desastre de área local pode destruir importantes sistemas de PC.

Secção 6. Procedimentos de recuperação de desastres

Em todos os planos de recuperação de desastres, os seguintes elementos devem ser tidos em consideração.

Procedimentos de Resposta de Emergência
Para documentar as respostas de emergência apropriadas a incêndios, desastres naturais ou quaisquer outras actividades, de forma a proteger vidas humanas e a diminuir os danos materiais.

Procedimentos de Operações de Cópia de Segurança
Para garantir que as tarefas essenciais de processamento de dados podem continuar a ser efectuadas após a interrupção.

Procedimentos de Acções de Recuperação
Para facilitar a rápida reposição de um sistema de processamento de dados a seguir a um desastre.

Lista de verificação de acções em caso de desastre

1. Início do Plano
   a. Informar a administração da empresa
   b. Contactar e atribuir tarefas à equipa de recuperação de desastres
   c. Determinar a extensão do desastre
   d. Implementar um plano adequado de recuperação de aplicações, de acordo com a extensão do desastre (consulte a Secção 7. Plano de recuperação—unidade móvel)
   e. Supervisionar a evolução dos acontecimentos
   f. Contactar o local de cópia de segurança e estabelecer marcações
   g. Contactar todo o restante pessoal necessário—tanto utilizadores como técnicos de processamento de dados
   h. Contactar os fornecedores—tanto de hardware como de software
   i. Informar os utilizadores de que houve interrupção dos serviços
2. Lista de Verificação de Acompanhamento
   a. Fazer uma lista das equipas e respectivas tarefas
   b. Reunir numerário de emergência e programar o transporte de e para as instalações alternativas, se necessário.
   c. Preparar alojamentos, caso seja necessário
   d. Preparar instalações para refeitórios, conforme necessário
   e. Fazer uma lista de todo o pessoal e dos respectivos números de telefone
   f. Estabelecer um plano de participação para os utilizadores
   g. Preparar a entrega e recepção do correio
   h. Estabelecer os fornecimentos de emergência do escritório
   i. Alugar ou adquirir equipamento, conforme necessário
   j. Determinar quais as aplicações que devem ser executadas e a respectiva sequência
   k. Identificar o número de estações de trabalho necessárias
   l. Verificar quais as necessidades de equipamento autónomo para cada aplicação
   m. Verificar o tipo de papel necessário para cada aplicação
   n. Verificar todos os dados que vão ser levados para as instalações alternativas antes de sair e deixar um perfil de inventário nas instalações centrais
   o. Definir fornecedores principais para assistência a problemas que ocorram durante a emergência
   p. Planear o transporte de itens adicionais necessários nas instalações alternativas
   q. Tomar direcções (definir correspondências) para criar uma cópia de segurança do local
   r. Procure bandas adicionais, se necessário
   s. Levar cópias do sistema e documentação sobre funcionamento e manuais de procedimentos.

t. Certificar-se de que todo o pessoal envolvido sabe quais são as suas tarefas

u. Informar as companhias de seguros

Procedimentos de arranque da recuperação para utilização após um desastre

1. Notificar _____, Serviços de Recuperação de Desastres, da necessidade de utilizar o serviço e da selecção do plano de recuperação.

   Nota: A contagem decrescente do tempo para entrega garantida começa no momento em que _____ é notificado da selecção do plano de recuperação.

   a. Números de contacto em caso de desastre

      _____ ou _____

   Estes números de telefone estão disponíveis das _____ às _____, de segunda a sexta-feira.

2. Número de contacto em caso de desastre: _____

   Este número de telefone está disponível em caso de desastre fora do horário de expediente, nos fins-de-semana e nos feriados. Só deve utilizar este número para comunicar a ocorrência efectiva de um desastre.

3. Fornecer a _____ um endereço para a entrega do equipamento (se for o caso), um contacto, um contacto alternativo para a coordenação do serviço e números de telefone em que seja possível contactá-lo 24 horas por dia.
4. Contactar as companhias da electricidade e dos telefones e programar as ligações de assistência necessárias.
5. Notificar imediatamente _____ caso seja necessário alterar algum dos planos relacionados.

Secção 7. Plano de recuperação–unidade móvel

1. Notificar _____ da natureza do desastre e da necessidade de seleccionar o plano para a unidade móvel.
2. Confirmar por escrito o conteúdo da comunicação telefónica com _____ num prazo de 48 horas da mesma.
3. Confirmar todos os suportes de segurança necessários disponíveis para instalar na máquina de reserva.
4. Preparar uma ordem de compra que contemple a utilização do equipamento de reserva.
5. Notificar _____ dos planos de obtenção de uma caravana e do respectivo posicionamento (do lado _____ de _____). (Consulte o plano de instalação da unidade móvel nesta secção.)
6. Dependendo das necessidades de comunicação, notificar a companhia dos telefones (_____) de possíveis alterações de linhas de emergência.
7. Iniciar a instalação da electricidade e das comunicações às _____.
   a. A electricidade e as comunicações devem estar preparadas para serem ligadas à caravana.
   b. No local onde as linhas telefónicas entram no edifício (_____), cortar o sistema de ligação actual aos controladores de administração (_____). Essas linhas são reencaminhadas para as linhas que estão ligadas à unidade móvel. Estas linhas são ligadas a modems na unidade móvel.

      As linhas que vão actualmente de _____ para _____ devem ser ligadas à unidade móvel através de modems.
   c. Provavelmente, será necessário que _____ reencaminhe as linhas do complexo _____ para uma área mais segura em caso de desastre.
8. Quando a caravana chegar, fazer as ligações à corrente e efectuar as verificações necessárias.
9. Fazer as ligações às linhas de comunicações e efectuar as verificações necessárias.

10. Iniciar o carregamento do sistema a partir das cópias de segurança (consulte a Secção 9. Restaurar Todo o Sistema).
11. Iniciar as operações normais assim que for possível:
    a. Trabalhos diários
    b. Salvaguardas diárias
    c. Salvaguardas semanais
12. Estabelecer um plano para fazer uma cópia de segurança do sistema, de forma a poder restaurá-lo para um computador das instalações centrais quando já houver instalações disponíveis. (Utilizar procedimentos regulares de cópia de segurança do sistema).
13. Proteger a unidade móvel e distribuir as chaves necessárias.
14. Manter um registo de manutenção do equipamento móvel.

Plano de instalação da unidade móvel

Inclua aqui o plano de instalação da unidade móvel.

Plano das comunicações em caso de desastre

Inclua aqui o plano das comunicações em caso de desastre, incluindo os diagramas do sistema de ligações.

Assistência eléctrica

Inclua aqui o diagrama da assistência eléctrica.

Secção 8. Plano de recuperação–centro de emergência

A assistência para a recuperação de desastres dispõe de um centro de emergência. Esse centro tem um sistema de segurança (reserva) para utilização temporária enquanto as instalações centrais estiverem a ser restabelecidas.

1. Notificar _____ da natureza do desastre e da necessidade de um centro de emergência.
2. Solicitar transporte aéreo dos modems para _____ para as comunicações. (Consulte _____ para comunicações para o centro de emergência.)
3. Confirmar por escrito o conteúdo da comunicação telefónica com _____ num prazo de 48 horas da mesma.
4. Começar a tomar as medidas necessárias para a deslocação da equipa de operações até às instalações.
5. Confirmar se todas as bandas necessárias estão disponíveis e empacotadas para serem enviadas para se fazer o restauro no sistema de segurança.
6. Preparar uma ordem de compra que contemple a utilização do sistema de segurança.
7. Reveja a lista de verificação de todos os materiais necessários antes de passar para o site mais visitado.
8. Certificar-se de que a equipa de recuperação de desastres que está no local tem as informações necessárias para começar a restaurar as instalações. (Consulte a Secção 12. Reconstrução das instalações do desastre).
9. Encarregar-se das despesas de viagem (ter dinheiro disponível).

10. Depois de chegar ao centro de emergência, contactar a instalação central para estabelecer os procedimentos de comunicação.
11. Rever se os materiais transportados para o centro de emergência estão completos.
12. Começar a carregar o sistema a partir das bandas de salvaguarda.
13. Iniciar as operações normais assim que for possível:
    a. Trabalhos diários
    b. Salvaguardas diárias
    c. Salvaguardas semanais
14. Estabelecer um plano para fazer uma cópia de segurança do sistema do centro de emergência, de forma a poder restaurá-lo para o computador das instalações centrais.

Configuração do sistema do centro de emergência

Inclua aqui a configuração do sistema do centro de emergência.

Secção 9. Restaurar todo o sistema

Para repor o sistema como estava antes do desastre, utilize os procedimentos de recuperação após uma perda total do sistema do manual *Cópia de Segurança e Recuperação*, SC17-5326-06.

Antes de Começar: Procure as seguintes bandas, equipamento e informações no cofre de bandas que está na empresa ou nas instalações externas de armazenamento:

- Se instalar a partir do dispositivo de instalação alternativo, precisa do suporte de bandas e do suporte de CD-ROM que contém o Código Interno Licenciado (LIC).
- Todas as bandas da operação de salvaguarda completa mais recente
- As bandas mais recentes onde estão guardados os dados de segurança (SAVSECDTA ou SAVSYS)
- As bandas mais recentes onde está guardada a configuração, caso seja necessário
- Todas as bandas que contêm diários e receptores de diário guardados desde a operação guardar diária mais recente
- Todas as bandas da operação guardar diária mais recente
- Lista de PTFs (armazenada com as bandas de salvaguarda completa mais recentes, bandas de salvaguarda semanais ou ambas)
- Lista das bandas da operação guardar integral mais recente
- Lista das bandas da operação guardar semanal mais recente
- Lista das bandas das operações guardar diárias
- Registo do histórico da operação guardar integral mais recente
- Registo do histórico da operação guardar semanal mais recente
- Registo do histórico das operações guardar diárias
- O manual *Instalação de Software*
- O manual *Cópia de Segurança e Recuperação*
- Lista telefónica
- Manual do modem
- Caixa de ferramentas

Secção 10. Processo de reconstrução

A equipa de gestão tem de ter acesso aos danos e começar a reconstrução de um novo centro de dados.

Se for necessário restaurar ou substituir as instalações originais, seguem-se alguns dos factores a considerar:

- Qual é a disponibilidade planeada de todo o equipamento informático necessário?
- Será mais eficaz e eficiente actualizar os sistemas informáticos com equipamento mais recente?
- Qual é o tempo considerado necessário para reparações ou construção das instalações dos dados?
- Existe algum local alternativo que possa ser mais facilmente preparado em termos de utilização de computadores?

Uma vez tomada a decisão de reconstruir o centro de dados, vá para a Secção 12. Reconstrução das instalações do desastre.

Secção 11. Testar o plano de recuperação de desastres

Num plano de contingências bem sucedido, é importante testar e avaliar o plano com regularidade. As operações de processamento de dados são de natureza volátil, causando alterações frequentes no equipamento, nos programas e na documentação. Estas acções fazem com que seja essencial considerar o plano como um documento em constante alteração. Utilize estas listas de verificação à medida que for seguindo o teste e decidindo quais são as áreas a testar.

Tabela 3. Efectuar um teste de recuperação

Item	Sim	Não	Aplicável	Não Aplicável	Comentários
Seleccionar a finalidade do teste. Que aspectos do plano estão a ser avaliados?					
Descrever os objectivos do teste. Como fará a avaliação do cumprimento desses objectivos?					
Reunir com a direcção e explicar o teste e os objectivos. Obter a sua concordância e apoio.					
Pedir à direcção que anuncie o teste e o tempo de conclusão esperado.					
Reunir os resultados do teste no final do período de teste.					
Avaliar os resultados. A recuperação foi bem sucedida? Se sim ou se não, qual a razão?					
Determinar as implicações dos resultados do teste. A recuperação bem sucedida num caso simples implica o sucesso da recuperação de todos os trabalhos essenciais no período de corte de energia tolerável?					
Fazer recomendações quanto a alterações. Pedir respostas até uma data indicada.					
Informar outras áreas dos resultados. Incluir utilizadores e auditores.					
Alterar o manual do plano de recuperação de desastres de acordo com as necessidades.					

Tabela 4. Áreas a testar

Item	Sim	Não	Aplicável	Não Aplicável	Comentários
Recuperação de sistemas de aplicações individuais utilizando ficheiros e documentação armazenados fora das instalações.					

Tabela 4. Áreas a testar (continuação)

Item	Sim	Não	Aplicável	Não Aplicável	Comentários
Novo carregamento de bandas do sistema e realização de um IPL utilizando ficheiros e documentação guardados fora das instalações.					
Capacidade de efectuar o processamento noutro computador.					
Capacidade da direcção para determinar a prioridade dos sistemas em caso de processamento limitado.					
Capacidade de recuperação e processamento bem sucedido sem as pessoas responsáveis.					
Capacidade do plano para clarificar as áreas de responsabilidade e a cadeia de comando.					
Eficácia das medidas de segurança e dos procedimentos para ignorar a segurança durante o período de recuperação.					
Capacidade para realizar a evacuação de emergência e respostas básicas de primeiros socorros.					
Capacidade dos utilizadores de sistemas de tempo real para suportar uma perda temporária das informações online.					
Capacidade dos utilizadores para continuar as operações diárias sem as aplicações ou os trabalhos que são considerados como não essenciais.					
Capacidade de contactar rapidamente os responsáveis ou os seus substitutos.					
Capacidade do pessoal encarregue da introdução de dados para fornecer o input a sistemas essenciais utilizando instalações alternativas e suportes de input diferentes.					
Disponibilidade de equipamento e processamento periférico, tal como impressoras e digitalizadores.					
Disponibilidade de equipamento de suporte, tal como aparelhos de ar condicionado e desumidificadores.					
Disponibilidade da assistência: fornecedores, transporte, comunicações.					
Distribuição do output produzido nas instalações de recuperação.					
Disponibilidade do stock de tipos de papel importantes.					
Capacidade de adaptação do plano a desastres menores.					

Secção 12. Reconstrução das instalações do desastre

- Planta do centro de dados.

- Determinar as necessidades actuais de hardware e as alternativas possíveis. (Consulte a Secção 4. Perfil do inventário.)
- Comprimento em metros quadrados, requisitos eléctricos e requisitos de segurança do centro de dados.
  - Comprimento em metros quadrados _____
  - Requisitos de eléctricos _____
  - Requisitos de segurança: área que é possível trancar, preferencialmente com fechadura com combinação numa porta.
  - Vigas de suporte
  - Detectores de calor, água, fumo, incêndio e movimento
  - Chão falso

Fornecedores

Planta das instalações

Inclua aqui uma cópia da planta proposta.

Secção 13. Registo de alterações ao plano

Mantenha o seu plano actualizado. Tenha registos das alterações da configuração, das aplicações e dos planos e procedimentos de cópia de segurança. Por exemplo, pode imprimir uma lista do hardware local actual, escrevendo:

```
DSPLCLHDW OUTPUT(*PRINT)
```

Descrição da imagem

A descrição da imagem do calendário é a seguinte:

1. Ponto 1: Ponto conhecido (última salvaguarda). Existe actividade no sistema.
2. Ponto 2: Ocorre uma falha. Existe uma reparação no hardware ou um IPL.
3. Ponto 3: O hardware está disponível. A informação é restaurada a partir da cópia de segurança.
4. Ponto 4: O sistema é recuperado para o ponto conhecido 1. São recuperadas as transacções do ponto 1 para o ponto 2.
5. Ponto 5: O sistema é recuperado para o ponto de falha 2. É recuperada a actividade do ponto de falha 2 para o ponto de recuperação 5.
6. Ponto 6: O sistema está actualizado.