IBM Systems - iSeries

Gestão de Sistemas - Planear uma estratégia de cópia de segurança e recuperação

Versão 5 Edição 4

IBM Systems - iSeries

Gestão de Sistemas - Planear uma estratégia de cópia de segurança e recuperação

Versão 5 Edição 4

Obs.

Antes de usar estas informações e o produto a que se referem, não deixe de ler as informações em "Avisos", na página 21.

Sétima Edição (Fevereiro de 2006)

Esta edição aplica-se à versão 5, edição 4, modificação 0 do IBM i5/OS (número de produto 5722-SS1) e a todas as edições e modificações subsequentes até indicação em contrário em novas edições. Esta versão não se pode executar em todos os modelos RISC (reduced instruction set computer) nem em modelos CISC.

Índice

Planear uma estratégia de cópia de segurança e recuperação

Este tópico dxescreve o que fazer em caso de necessidade de cópias de segurança perante perda de informações no sistema.

Os computadores em geral e os servidores IBM eServer 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, o possível impacto aumenta. As empresas são cada vez mais dependentes dos computadores e das informações neles armazenadas. As informações que são guardadas em 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, irá precisar de utilizar as suas cópias de segurança das informações. Todos os sistemas devem restaurar algumas ou todas as informações que contêm em 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 estudar o calendário de cópia de segurança e recuperação, estará preparado(a) para começar a planear a sua estratégia. Siga estes passos:

1. Saber o que guardar e com que frequência.
2. Determinar o tempo atribuído à salvaguarda.
3. Escolher opções de disponibilidade.
4. Testar a estratégia escolhida.

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

Este tópico contém informações sobre planeamento de uma estratégia e selecção de opções necessárias para configurar o sistema para cópia de segurança, recuperação e disponibilidade. Para mais informações sobre a execução real das tarefas relacionadas com estes tópicos, consulte o manual Cópia de Segurança e Recuperação e o tópico Cópia de segurança do servidor. O tópico Roteiro de disponibilidade inclui informações sobre os tipos comuns de falhas que podem ocorrer.

Conceitos relacionados

Cópia de segurança do servidor

Roteiro de disponibilidade do servidor iSeries

PDF para impressão

Utilize esta opção para ver e imprimir um ficheiro PDF destas informações.

Para ver ou descarregar a versão em PDF deste documento, seleccione Planear uma estratégia de cópia de segurança e recuperação (cerca de 317 KB).

Guardar ficheiros PDF

Para guardar um PDF na estação de trabalho para visualizar ou imprimir:

1. Clique com o botão direito do rato no PDF no seu browser (clique com o botão direito do rato na ligação acima).
2. Clique na opção que guarda o PDF localmente.
3. Navegue até ao directório no qual pretende guardar o PDF.
4. Clique em **Save** (Guardar).

Descarregar o Adobe Acrobat Reader

É necessário o programa Adobe Reader instalado no sistema para ver ou imprimir estes ficheiros PDF. Pode descarregar uma cópia grátis no sítio da Adobe na Web (www.adobe.com/products/acrobat/readstep.html) .

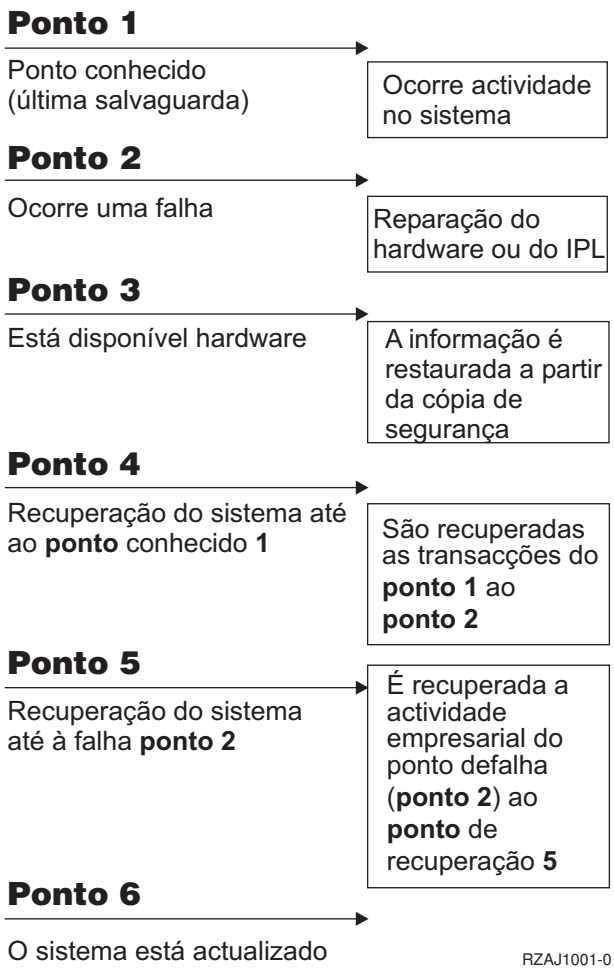
Calendário de cópia de segurança e recuperação

O calendário de cópia de segurança e recuperação começa quando se guardam 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 ou não concluir satisfatoriamente cada etapa do quadro
- O tempo que demorará a concluir cada etapa

Utilize o seguinte calendário 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 será possível com a estratégia de salvaguarda que planeou?



Segue-se uma descrição da imagem do calendário:

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

Conceitos relacionados

"Testar a estratégia" na página 9
Se a situação implicar uma estratégia de salvaguarda média ou complexa, também irá implicar uma revisão regular.

Referências relacionadas

"Saber o que guardar e com que frequência"
Deve guardar todo o conteúdo do sistema com a maior frequência possível.

Saber o que guardar e com que frequência

Deve guardar todo o conteúdo do sistema com a maior frequência possível.

Poderá não estar preparado(a) para recuperar de uma perda no 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. O que guardar diariamente

Descrição do elemento	Fornecido pela IBM?	Quando ocorrem alterações
Informações de segurança (perfis de utilizador, autoridades privadas, listas de autorização)	Alguns	Regularmente, à medida que são adicionados novos utilizadores e objectos ou são alteradas autoridades[1]
Objectos de configuração na QSYS	Não	Regularmente, quando são adicionadas ou alteradas descrições de dispositivo ou quando se utiliza a função Hardware Service Manager 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
Pastas 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 se actualizam programas licenciados.

Partes do sistema que não são alteradas com frequência

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

Tabela 2. O que guardar semanalmente

Descrição do elemento	Fornecido pela IBM?	Quando ocorrem alterações
Código Interno Licenciado (LIC)	Sim	PTFs (Program Temporary Fixes - correcções temporárias de programas) ou nova edição do sistema operativo
Objectos do sistema operativo na biblioteca QSYS	Sim	PTFs ou nova edição do sistema operativo
Bibliotecas opcionais da IBM i5/OS (QHLPSYS, QUSRTOOL)	Sim	PTFs ou nova edição do sistema operativo
Bibliotecas de programas licenciados (QRPG, QCBL, Qxxxx)	Sim	Actualizações de programas licenciados
Pastas de programas licenciados (Qxxxxxxx)	Sim	Actualizações de programas licenciados
Directórios de programas licenciados (/QIBM/ProdData, /QOpenSys/QIBM/ProdData)	Sim	Actualizações de programas licenciados

Conceitos relacionados

"Calendário de cópia de segurança e recuperação" na página 2
O calendário de cópia de segurança e recuperação começa quando se guardam as informações e termina quando o sistema recupera totalmente após uma falha.

Referências relacionadas

"Estratégia de salvaguarda simples"
Dispõe de um tempo considerável atribuído à salvaguarda, o que significa que dispõe diariamente de um período de 8 a 12 horas sem actividade do sistema (incluindo trabalho batch). A estratégia de salvaguarda mais simples é guardar tudo todas as noites ou fora do horário de expediente.

Determinar o tempo atribuído à salvaguarda

O momento de execução de procedimentos de salvaguarda, o modo de execução destes e os artigos que se guardam dependem da extensão do tempo atribuído à salvaguarda.

O **tempo atribuído à salvaguarda** é a quantidade de tempo que o sistema pode não estar disponível para os utilizadores enquanto as operações de salvaguarda 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.

Ao seleccionar uma estratégia de salvaguarda, deve considerar aquilo que os utilizadores consideram um tempo aceitável atribuído à salvaguarda, o valor dos dados que poderá perder e a quantidade de tempo que pode demorar a recuperação.

Se o sistema for tão crucial para a empresa a ponto de não ter um tempo atribuído à salvaguarda que se possa gerir, é provável que também não se possa obviar a uma perda de energia não programada. Deverá avaliar seriamente todas as opções de disponibilidade do servidor iSeries, incluindo a utilização de conjuntos de unidades. O tópico Roteiro de disponibilidade do servidor iSeries contém informações adicionais sobre as opções de disponibilidade.

Consoante a duração do tempo de salvaguarda, escolha uma das seguintes estratégias: simples, média ou complexa. A seguir, avalie novamente a sua decisão com base no posicionamento de recuperação que a estratégia de salvaguarda lhe permite.

Conceitos relacionados

Roteiro de disponibilidade do servidor iSeries

Estratégia de salvaguarda simples

Dispõe de um tempo considerável atribuído à salvaguarda, o que significa que dispõe diariamente de um período de 8 a 12 horas sem actividade do sistema (incluindo trabalho batch). 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).

Poderá 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 artigos 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 sistema tiver um longo período de inactividade durante o fim-de-semana, a 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

Referências relacionadas

"Saber o que guardar e com que frequência" na página 3
Deve guardar todo o conteúdo do sistema com a maior frequência possível.

Estratégia de salvaguarda média

Dispõe de um tempo médio atribuído à salvaguarda, o que significa que dispõe diariamente de um período de tempo de 4 a 6 horas sem actividade no sistema. Utilize esta estratégia se concluir que não tem um tempo suficientemente longo atribuído à salvaguarda para utilizar uma estratégia de salvaguarda simples.

Talvez execute grandes trabalhos batch no sistema à noite. Também poderá dar-se o caso de ter ficheiros muito grandes e que demoram muito tempo a guardar. Se assim for, poderá ter de desenvolver uma estratégia de salvaguarda média, o que significa que a complexidade da operação de salvaguarda e recuperação 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 de salvaguarda. Basta avaliar em mais detalhe a frequência com que são feitas alterações do que o que 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 de salvaguarda ou desde uma data e hora específica.

Pode utilizar o comando Save Changed Objects (SAVCHGOBJ) para guardar apenas os objectos que tenham sido alterados desde a última vez que uma biblioteca ou um grupo de bibliotecas tiver sido guardado. Tal poderá ser particularmente útil numa situação em que os programas e os ficheiros de dados se encontram na mesma biblioteca. Regra geral, 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 Save Document Library Object (SAVDLO) para guardar apenas os documentos e as pastas que foram alterados. Da mesma forma, pode utilizar o comando Save (SAV) para guardar objectos em directórios que tenham sido alterados a partir de determinado ponto.

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

Dia	Volume de trabalho batch	Operação de salvaguarda
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 de salvaguarda 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 guardará 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 opção melhor.

Quando se registam objectos em diário, o sistema grava uma cópia de todas as alterações efectuadas no objecto num receptor de diário. Quando se guarda um receptor de diário, guarda-se 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:

Tabela 3. Estratégia de salvaguarda exemplo

Dia	Volume de trabalho batch	Operação de salvaguarda
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, deverá 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 Save Library (SAVLIB) ou Save Object (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.

Conceitos relacionados

Gestão de diários

Estratégia de salvaguarda complexa

Dispõe de um curto tempo atribuído à salvaguarda, o que significa que dispõe de pouco ou nenhum tempo quando o sistema não está a ser utilizado para trabalho interactivo ou batch. Um tempo muito curto atribuído à salvaguarda 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, poderá ser necessário guardar ficheiros essenciais específicos a horas específicas do dia ou da semana. Poderá também considerar a utilização de uma ferramenta, como por exemplo, o IBM 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 de guardar activo (SAVACT) é suportado nos seguintes comandos:

- Save Library (SAVLIB)
- Save Object (SAVOBJ)
- Save Changed Objects (SAVCHGOBJ)
- Save Document Library Object (SAVDLO)
- Save (SAV)

Se utilizar o suporte guardar-enquanto-activo, poderá reduzir significativamente a quantidade de tempo em que os ficheiros estarão indisponíveis. Quando o sistema tiver estabelecido um ponto de verificação para todos os objectos que estão a ser guardados, estes poderão ficar disponíveis para utilização. É possível utilizar o suporte 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, deverá utilizar registo em diário para simplificar a recuperação. Se utilizar o valor *SYSDFN com o parâmetro SAVACT, deverá utilizar controlo de consolidações, caso a biblioteca que está a guardar tiver objectos de base de dados relacionados entre si. Se optar por utilizar o suporte 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 poderá reduzir o tempo de indisponibilidade dos ficheiros executando operações guardar em mais de um dispositivo de cada vez ou executando *operações de salvaguarda simultâneas*. Por exemplo, pode guardar bibliotecas num dispositivo, pastas noutro e directórios num terceiro dispositivo. Também pode guardar diferentes conjuntos de bibliotecas ou objectos em dispositivos diferentes.

Também poderá utilizar vários dispositivos em simultâneo executando uma *operação de salvaguarda paralela*. Para executar uma operação de salvaguarda paralela, necessita do Backup Recovery and Media Services ou de uma aplicação que lhe permita criar objectos de definição de suportes de dados.

Para mais informações sobre o suporte guardar-enquanto-activo, operações de salvaguarda simultâneas e operações de salvaguarda paralelas, consulte as informações Criar uma cópia de segurança do servidor.

Conceitos relacionados

IBM Backup Recovery and Media Services for iSeries

Enquanto activo

Mais de um dispositivo

Cópia de segurança do servidor

Controlo de consolidação

Gestão de diários

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 recuperação após uma falha. Em certos casos, com opções de disponibilidade poderá ser desnecessário executar uma recuperação.

Para justificar o custo de utilização de opções de disponibilidade, terá de considerar o seguinte:

- O valor fornecido pelo sistema.
- O custo de um estado de inactividade programado ou não programado.
- Quais são os requisitos de disponibilidade.

Segue-se uma lista das opções de disponibilidade que pode utilizar para complementar a sua estratégia de salvaguarda:

- A gestão de diários permite recuperar as alterações efectuadas em objectos desde a última salvaguarda completa.
- A protecção de caminhos de acesso permite reproduzir 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 é necessário recuperar aos dados do conjunto de discos da unidade em falha.
- A protecção por paridade de dispositivos permite reconstruir dados perdidos; o sistema pode continuar em execução enquanto os dados estiverem a ser reconstruídos.
- A protecção por replicação ajuda a manter os dados disponíveis porque existem duas cópias dos dados em duas unidades de discos separadas.
- A repartição por conjuntos de unidades permite manter alguns dados ou mesmo a totalidade de dados em dois sistemas; o sistema secundário pode assumir programas de aplicação fulcrais se o sistema principal falhar.

O tópico Roteiro de disponibilidade do servidor iSeries contém informações que podem ser utilizadas para implementar uma solução de disponibilidade para o servidor iSeries.

Conceitos relacionados

Roteiro de disponibilidade do servidor iSeries

Referências relacionadas

Valores especiais para o comando SAVLIB

Testar a estratégia

Se a situação implicar uma estratégia de salvaguarda média ou complexa, também irá implicar uma revisão regular.

A revisão regular será a seguinte:

- Está a guardar **tudo** ocasionalmente?
- O que necessita de fazer para recuperar até ao ponto conhecido (4) no Calendário de cópia de segurança e recuperação?
- Está a utilizar opções como registar em diário ou guardar objectos alterados para ajudar a recuperar do ponto de falha (5)? Sabe como recuperar utilizando estas opções?
- Foram adicionadas novas aplicações? As novas bibliotecas, pastas e novos 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 do comando SAVLIB enumera 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 satisfatoriamente, poderá perder informações quando tentar restaurar.

Existem várias organizações que prestam serviços de testes de recuperação. Os IBM Continuity and Recovery Services constituem uma organização que pode ajudar a realizar testes de recuperação.

Conceitos relacionados

"Calendário de cópia de segurança e recuperação" na página 2
O calendário de cópia de segurança e recuperação começa quando se guardam as informações e termina quando o sistema recupera totalmente após uma falha.

Planear a recuperação de acidentes

Este tópico fornece directrizes para as informações e os procedimentos que são necessários para recuperar de um acidente.

O objectivo de um plano de recuperação de acidentes é garantir uma boa resposta a um acidente ou de qualquer outra emergência que afecte os sistemas de informação e assim minimizar o impacto no funcionamento da empresa. 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 acidentes. 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 acidentes

Este tópico faculta informações sobre a criação de um plano de recuperação de acidentes.

Secção 1. Principais objectivos deste plano

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

Secção 2. Pessoal

Tabela 4. Pessoal

Pessoal de processamento de dados			
Nome	**Cargo**	**Endereço**	**Contacto**

Tabela 4. Pessoal (continuação)

Pessoal de processamento de dados			
Nome	**Cargo**	**Endereço**	**Contacto**

Nota: Junte uma cópia do organigrama 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.

Tabela 5. Perfil da aplicação

Perfil da aplicação				
Nome da aplicação	**Fulcral? Sim/Não**	**Recurso fixo? Sim/Não**	**Fabricante**	**Comentários**
				Legenda de comentários:
				1. Executada diariamente _____.
				2. Executada semanalmente à/ao _____.
				3. Executada mensalmente à/ao _____.

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 disco
- 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 E/S
- Comunicação de dados geral
- Monitores de reserva
- Bastidores
- Humidificador ou desumidificador

Tabela 6. Perfil do inventário

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

Tabela 7. Inventário diverso

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

Tabela 7. Inventário diverso (continuação)

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 formulários)		

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 e directórios às _____:
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____

    Este procedimento também guarda os diários e os receptores de diário.
  - No dia _____ às _____ horas é efectuada uma salvaguarda de todo o sistema.
  - Todos os suportes de salvaguarda são armazenados fora da empresa, num cofre, em _____ (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 _____ às _____ horas, 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 acidente na área local pode destruir importantes sistemas de PC.

Secção 6. Procedimentos de recuperação de acidentes

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

Procedimentos de resposta de emergência
: Documentar as respostas de emergência apropriadas a incêndios, catástrofes naturais ou outras actividades, de forma a proteger vidas humanas e a diminuir os danos materiais.

Procedimentos de operações de cópia de segurança
: Garantir que as tarefas essenciais de processamento de dados podem continuar a ser efectuadas após a interrupção.

Procedimentos de acções de recuperação

Facilitar a rápida reposição de um sistema de processamento de dados a seguir a um acidente.

Lista de verificação de acções em caso de acidente

1. Iniciação ao Plano
   a. Informar a administração da empresa.
   b. Contactar e atribuir tarefas à equipa de recuperação de acidentes.
   c. Determinar a extensão do acidente.
   d. Implementar um plano adequado de recuperação de aplicações (consultar "Secção 7. Plano de recuperação de unidade móvel" na página 15).
   e. Supervisionar o avanço das operações.
   f. Contactar o local de cópia de segurança e estabelecer horários.
   g. Contactar todo o restante pessoal necessário, tanto utilizadores como técnicos de processamento de dados.
   h. Contactar revendedores, de hardware e 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 fundo de maneio 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 contacto.
   f. Estabelecer um plano de participação para os utilizadores.
   g. Preparar a entrega e recepção do correio.
   h. Estabelecer o economato 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 elementos adicionais necessários nas instalações alternativas.
   q. Reunir indicações (mapa) para o local de reserva.
   r. Verificar existência de bandas magnéticas 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 acidente

1. Avisar os Serviços de Recuperação de Acidentes _____ 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 avisado da selecção do plano de recuperação.

a. Números de contacto em caso de acidente

   _____ ou _____

   Estes números de telefone funcionam das _____ às _____ de Segunda a Sexta-feira.

2. Número de contacto em caso de acidente: _____

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

3. Facultar 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. Avisar _____ imediatamente caso seja necessário alterar algum dos planos relacionados.

Secção 7. Plano de recuperação de unidade móvel

1. Avisar _____ da natureza do acidente 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 dados de cópia 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. Avisar _____ dos planos de obtenção de uma caravana e do respectivo posicionamento (do lado _____ de _____). Consultar o plano de instalação da unidade móvel nesta secção.
6. Consoante as necessidades de comunicação, avisar 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 _____ a _____ 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 acidente.
8. Quando a caravana chegar, estabelecer as ligações à corrente e efectuar as verificações necessárias.
9. Estabelecer as ligações às linhas de comunicações e efectuar as verificações necessárias.
10. Começar o carregamento do sistema a partir das cópias de segurança (consulte “Secção 9. Restaurar todo o sistema” na página 17).
11. Começar 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-la num computador das instalações centrais quando já houver instalações disponíveis. (Utilize procedimentos regulares de cópia de segurança do sistema).
13. Proteger a unidade móvel e distribuir as chaves necessárias.

14. Manter registo da manutenção do equipamento móvel.

Plano de instalação da unidade móvel

Incluir aqui o plano de instalação da unidade móvel.

Plano das comunicações em caso de acidente

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

Assistência eléctrica

Incluir aqui o diagrama da assistência eléctrica.

Secção 8. Plano de recuperação do centro de emergência

A assistência para a recuperação de acidentes 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. Avisar _____ da natureza do acidente e da necessidade de um centro de emergência.
2. Solicitar transporte aéreo dos modems para _____ para fins de comunicações. (Consulte _____ para as 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. Rever a lista de verificação de todos os materiais necessários antes de passar para o centro de emergência.
8. Certificar-se de que a equipa de recuperação de acidentes que está no local tem as informações necessárias para começar a restaurar as instalações. (Consultar “Secção 12. Reconstrução das instalações do acidente.” na página 19).
9. Prover a despesas de viagem (fundo de maneio 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-la no computador das instalações centrais.

Configuração do sistema do centro de emergência

Incluir aqui a configuração do sistema do centro de emergência.

Secção 9. Restaurar todo o sistema

Para repor o sistema como estava antes do acidente, utilize os procedimentos de recuperação após perda total do sistema no manual *Cópia de Segurança e Recuperação, SC10-3123-05-07*.

Antes de começar: Localizar 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, precisará 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 de salvaguarda diária mais recente
- Todas as bandas da operação de salvaguarda 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 de salvaguarda integral mais recente
- Lista das bandas da operação de salvaguarda semanal mais recente
- Lista das bandas das operações de salvaguarda diárias
- Histórico da operação de salvaguarda integral mais recente
- Histórico da operação de salvaguarda semanal mais recente
- Histórico das operações de salvaguarda diárias
- O manual *Install, upgrade, or delete i5/OS e software relacionado*
- 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 prevista de todo o equipamento informático necessário?
- Será mais eficaz e eficiente actualizar os sistemas informáticos com equipamento mais recente?
- Qual o tempo considerado necessário para reparações ou construção das instalações dos dados?
- Existe algum local alternativo que possa ser mais facilmente actualizado para fins de utilização de computadores?

Uma vez tomada a decisão de reconstruir o centro de dados, avance para “Secção 12. Reconstrução das instalações do acidente.” na página 19.

Secção 11. Testar o plano de recuperação de acidentes

No planeamento satisfatório de contingências, 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 8. Efectuar um teste de recuperação

Elemento	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 acidentes de acordo com as necessidades.					

Tabela 9. Áreas a testar

Elemento	Sim	Não	Aplicável	Não Aplicável	Comentários
Recuperação de sistemas de aplicações individuais utilizando ficheiros e documentação armazenados fora das instalações.					
Recarregamento 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 administração 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 de segurança alternativos durante o período de recuperação.					

Tabela 9. Áreas a testar (continuação)

Elemento	Sim	Não	Aplicável	Não Aplicável	Comentários
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 dar entrada em sistemas essenciais utilizando instalações alternativas e suportes de entrada de dados diferentes.					
Disponibilidade de equipamento e processamento periférico como, por exemplo, impressoras e scanners.					
Disponibilidade de equipamento de suporte como, por exemplo, aparelhos de ar condicionado e desumidificadores.					
Disponibilidade da assistência: fornecedores, transporte, comunicações.					
Distribuição dos dados produzidos nas instalações de recuperação.					
Disponibilidade das existências de tipos de papel importantes.					
Capacidade de adaptação do plano a acidentes menores.					

Secção 12. Reconstrução das instalações do acidente.

- Planta do centro de dados.
- Determinar as necessidades actuais de hardware e as alternativas possíveis. (Consultar "Secção 4. Perfil do inventário" na página 11.)
- Comprimento em metros quadrados, requisitos eléctricos e requisitos de segurança do centro de dados.
  - _____ metros quadrados
  - Requisitos de alimentação/energia _____
  - Requisitos de segurança: área que é possível isolar, preferencialmente com fechadura com combinação numa porta.
  - Vigas de suporte
  - Detectores de calor, água, fumo, incêndio e movimento
  - Chão falso

Fornecedores

Planta das instalações

Incluir 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:

```
DSPHDWRSC OUTPUT(*PRINT)
```

Informações relacionadas

DSPHDWRSC

Apêndice. Avisos

Estas informações foram desenvolvidas para produtos e serviços disponibilizados nos E.U.A.

A IBM poderá não disponibilizar os produtos, serviços ou funções mencionados neste documento em outros países. Consulte o representante local da IBM para informações sobre produtos e serviços actualmente disponíveis na sua área. As referências a um produto, programa ou serviço da IBM não implicam que só se deva utilizar esse produto, programa ou serviço da IBM. Qualquer produto, programa ou serviço funcionalmente equivalente e que não infrinja os direitos de propriedade intelectual da IBM poderá ser utilizado. Todavia, é da responsabilidade do utilizador avaliar e verificar o funcionamento de qualquer produto, programa ou serviço alheio à IBM.

A IBM poderá ter patentes ou pedidos de patente pendentes relativos a temáticas abordadas neste documento. O facto deste documento ser disponibilizado ao utilizador não implica quaisquer licenças sobre essas patentes. Poderá enviar pedidos de licença, por escrito, para:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
E.U.A.

Para pedidos de licença relativos a informações de duplo byte (DBCS), contacte o IBM Intellectual Property Department do seu país ou envie pedidos por escrito para:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tóquio 106-0032, Japão

O parágrafo seguinte não se aplica ao Reino Unido nem a qualquer outro país onde as respectivas cláusulas sejam incompatíveis com a lei local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FACULTA ESTA PUBLICAÇÃO "TAL COMO ESTÁ", SEM GARANTIAS DE QUALQUER TIPO, EXPRESSAS OU IMPLÍCITAS, INCLUINDO A TÍTULO MERAMENTE EXEMPLIFICATIVO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRACÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A DETERMINADO FIM. Existem estados que não permitem a renúncia de garantias expressas ou implícitas em certas transacções, de modo que estas cláusulas podem não ser aplicáveis ao utilizador.

Estas informações podem conter imprecisões técnicas ou erros tipográficos. Estas informações são alteradas periodicamente; estas alterações serão incluídas em novas edições da publicação. A IBM poderá introduzir melhorias e/ou alterações em produto(s) e/ou programa(s) idos nesta publicação em qualquer altura e sem aviso prévio.

As referências contidas nestas informações relativas a sítios na Web alheios à IBM são facultadas a título de conveniência e não constituem de modo algum aprovação desses sítios na Web. Os materiais mencionados nesses sítios na Web não fazem parte dos materiais da IBM relativos ao presente produto, de modo que a utilização desses sítios na Web é da inteira responsabilidade do utilizador.

A IBM poderá utilizar ou distribuir informações facultadas pelo utilizador, no todo ou em parte, da forma que entender apropriada sem incorrer em qualquer obrigação para com o utilizador.

Os titulares de licenças deste programa que pretendam obter informações acerca do mesmo no intuito de fomentar: (i) intercâmbio de informação entre programas criados independentemente e outros programas (incluindo o presente) e (ii) a utilização mútua da informação trocada, devem contactar:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
E.U.A.

As ditas informações poderão ser disponibilizadas, sujeitas a termos e condições, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nestas informações e todo o material licenciado disponível para estas são fornecidos pela IBM nos termos do IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, ou qualquer acordo equivalente entre as partes.

Quaisquer dados de rendimento aqui contidos foram obtidos num ambiente controlado. Assim sendo, os resultados obtidos noutros ambientes operativos podem variar significativamente. Algumas medições podem ter sido efectuadas em sistemas ao nível do desenvolvimento, pelo que não existem garantias de que estas medições sejam iguais nos sistemas normalmente disponíveis. Para além disso, algumas medições podem ter sido calculadas por extrapolação. Os resultados reais podem variar. Os utilizadores deste documento devem verificar os dados aplicáveis ao seu ambiente específico.

As informações relativas a produtos alheios à IBM foram obtidas junto dos fornecedores desses produtos, dos anúncios de publicidade dos mesmos ou de outras fontes disponíveis publicamente. A IBM não testou esses produtos e não pode confirmar a exactidão do rendimento, da compatibilidade ou de quaisquer outras afirmações relacionadas com produtos não produzidos pela IBM. Quaisquer perguntas sobre as capacidades de produtos alheios à IBM deverão ser endereçadas aos fornecedores desses produtos.

Estas informações contêm exemplos de dados e relatórios utilizados em operações empresariais diárias. No intuito de as ilustrar o mais integralmente possível, os exemplos incluem nomes de pessoas, empresas, marcas e produtos. Todos estes nomes são fictícios, de modo que qualquer semelhança com nomes e moradas de empresas reais será mera coincidência.

LICENÇA DE COPYRIGHT:

Esta publicação contém programas de aplicações exemplo em linguagem de origem, os quais pretendem ilustrar técnicas de programação em diversas plataformas operativas. Poderá copiar, modificar e distribuir estes programas exemplo sem qualquer encargo para com a IBM, no intuito de desenvolver, utilizar, comercializar ou distribuir programas de aplicação conformes à interface de programação de aplicações relativa à plataforma operativa para a qual tais programas exemplo foram escritos. Estes exemplos não foram testados exaustivamente nem em todas as condições. Por conseguinte, a IBM não pode garantir a fiabilidade ou o financiamento destes programas.

Cada cópia ou qualquer parte destes programas exemplo ou qualquer trabalho derivado dos mesmos tem de incluir um aviso de direitos de autor, do seguinte modo:

© (o nome da sua empresa) (ano). Algumas partes deste código são derivadas de Programas Exemplo da IBM Corp. © Copyright IBM Corp. _introduza o(s) ano(s). Todos os direitos reservados.

Se estiver a consultar a versão electrónica desta publicação, é possível que as fotografias e as ilustrações a cores não estejam visíveis.

Marcas comerciais

Os termos seguintes são marcas comerciais da International Business Machines Corporation nos Estados Unidos e/ou noutros países:

| eServer
| IBM
| IBM(logótipo)
| iSeries
| i5/OS

Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou marcas de serviço de terceiros.

Termos e condições

As permissões de utilização das informações seleccionadas para descarregamento são concedidas sujeitas aos seguintes termos e condições.

Utilização pessoal: Pode reproduzir estas informações para uso pessoal e não comercial, desde que mantenha todas as informações de propriedade. Não pode executar qualquer trabalho derivado destas informações, nem reproduzir, distribuir ou apresentar estas informações ou qualquer parte das mesmas fora das instalações da sua empresa, sem o expresso consentimento do fabricante.

Utilização comercial: Pode reproduzir, distribuir e apresentar estas informações exclusivamente no âmbito da sua empresa, desde que preserve todas as informações de propriedade. Não pode executar qualquer trabalho derivado destas informações, nem reproduzir, distribuir ou apresentar estas informações ou qualquer parte das mesmas fora das instalações da empresa, sem o expresso consentimento do fabricante.

À excepção das concessões expressas nesta permissão, não são concedidos outros direitos, permissões ou licenças, quer explícitos, quer implícitos, relativos às informações ou quaisquer dados, software ou outra propriedade intelectual contidos nesta publicação.

O fabricante reserva-se o direito de retirar as permissões concedidas nesta publicação sempre que considerar que a utilização das informações pode ser prejudicial aos seus interesses ou, tal como determinado pelo fabricante, sempre que as instruções acima referidas não estejam a ser devidamente cumpridas.

Não pode descarregar, exportar ou reexportar estas informações, excepto quando em total conformidade com todas as leis e regulamentos aplicáveis, incluindo todas as leis e regulamentos de exportação em vigor nos Estados Unidos.

O FABRICANTE NÃO GARANTE O CONTEÚDO DESTAS INFORMAÇÕES. O FABRICANTE NÃO GARANTE O CONTEÚDO DESTAS INFORMAÇÕES. AS INFORMAÇÕES SÃO FORNECIDAS ⌂TAL COMO ESTÃO⌂ E SEM GARANTIAS DE QUALQUER ESPÉCIE, QUER EXPLÍCITAS, QUER IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, NÃO INFRACÇÃO E ADEQUAÇÃO A UM DETERMINADO FIM.