



@server

iSeries

Planear uma estratégia de cópia de segurança e recuperação

*Versão 5 Edição 3*







@server

iSeries

Planear uma estratégia de cópia de segurança e  
recuperação

*Versão 5 Edição 3*

**Obs.**

Antes de usar estas informações e o produto a que se referem, não deixe de ler as informações em “Avisos”, na página 19.

| **Sexta Edição (Agosto 2005)**

| Esta edição aplica-se à versão 5, edição 3, modificação 0 do IBM Operating System/400 (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.

© Copyright International Business Machines Corporation 1998, 2005. Todos os direitos reservados.

---

# Índice

## **Planear uma estratégia de cópia de segurança e recuperação . . . . . 1**

Calendário de cópia de segurança e recuperação . . . . .	1
Descrição da imagem . . . . .	2
Saber o que guardar e com que frequência . . . . .	2
Determinar o tempo atribuído para salvaguarda . . . . .	3
Estratégia de salvaguarda simples . . . . .	4
Estratégia de salvaguarda média. . . . .	4
Estratégia de salvaguarda complexa . . . . .	6
Escolher as opções de disponibilidade . . . . .	7

Testar a estratégia . . . . .	7
Plano de recuperação de acidentes—modelo . . . . .	8
Plano de Recuperação de Acidentes. . . . .	8

## **Apêndice. Avisos . . . . . 19**

Marcas Registadas . . . . .	20
Termos e condições para descarregar e imprimir publicações . . . . .	20
Informações de renúncia sobre códigos . . . . .	21



---

## 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, 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, **vai** 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 um tempo atribuído para salvaguarda
3. Escolher opções de disponibilidade
4. Testar a estratégia

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 Back up your server. O tópico Roteiro de disponibilidade para o servidor iSeries inclui informações sobre os tipos comuns de falhas que podem ocorrer.

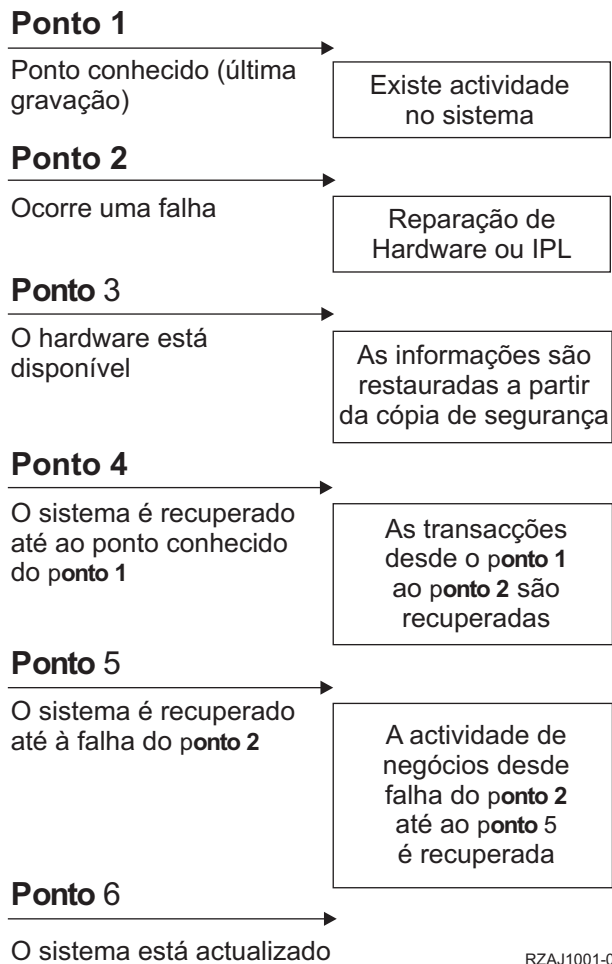
---

## 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 ou não 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 será possível com a estratégia de salvaguarda que planeou?



## 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.

## 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 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

- 2 iSeries: Planear uma estratégia de cópia de segurança e recuperação



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

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

Descrição do Artigo	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 <sup>1</sup>
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 <sup>1</sup>
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

<sup>1</sup> 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; poderá guardá-las semanalmente.

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

Descrição do Artigo	Fornecido pela IBM?	Quando Ocorrem as Alterações
Licensed Internal Code	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 (QHLPYSYS, 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

## Determinar o tempo atribuído para salvaguarda

Em termos reais, 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.

Quando 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 levar 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 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.

Escolha uma das seguintes estratégias de salvaguarda, com base na extensão de tempo atribuído à salvaguarda que decidiu. A seguir, avalie novamente a sua decisão com base no posicionamento de recuperação que a estratégia de salvaguarda lhe permite.

- **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).
- **Estratégia de salvaguarda média**  
Dispõe de um tempo médio atribuído à salvaguarda média, o que significa que dispõe diariamente de um período de tempo mais reduzido (4 a 6 horas) sem actividade no sistema.
- **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.

## 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 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

## Estratégia de salvaguarda média

Pode 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:

<b>Dia</b>	<b>Volume de Trabalho Batch</b>	<b>Operação de Salvaguarda</b>
Sexta-feira à noite	Parcial	Opção 21 do menu Guardar
Segunda-feira à noite	Completo	Guardar apenas as alterações <sup>1</sup>
Terça-feira à noite	Parcial	Opção 23 do menu Guardar
Quarta-feira à noite	Completo	Guardar apenas as alterações <sup>1</sup>
Quinta-feira à noite	Completo	Guardar apenas as alterações <sup>1</sup>
Sexta-feira à noite	Parcial	Opção 21 do menu Guardar

<sup>1</sup> 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:

<b>Dia</b>	<b>Volume de Trabalho Batch</b>	<b>Operação de Salvaguarda</b>
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.

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

## **Estratégia de salvaguarda complexa**

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, pode 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.

Se estiver na V4R4 ou em edição posterior, 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. O tópico Controlo de consolidações contém informações mais detalhadas sobre controlo de consolidações. O tópico Gestão de diário contém informações mais detalhadas sobre registo em diário.

---

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

Seguem-se as opções de disponibilidade que pode utilizar para complementar 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 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 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 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.

---

## Testar a estratégia

Se a 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, 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 com êxito, poderá perder informações quando tentar restaurar.

Existem várias organizações que prestam serviços de testes de recuperação. A IBM Continuity and Recovery Services  é uma organização que o poderá nos testes de recuperação.

---

## Plano de recuperação de acidentes—modelo

O objectivo de um plano de recuperação de acidentes é garantir uma forma de estar preparado para recuperar de um acidente ou de qualquer outra emergência que afecte os sistemas de informação e, assim, minimizar o impacto no funcionamento da empresa. Este tópico fornece as directrizes para o tipo de informações e procedimentos que são necessários para recuperar de um acidente. 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

### 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

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 (DPSFWRSC) 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

**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**

- iSeries Server
  - 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 acidente de 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**

Para documentar as respostas de emergência apropriadas a incêndios, catástrofes 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 acidente.

### *Lista de verificação de acções em caso de acidente*

1. Início do 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, de acordo com a extensão do acidente (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 acidente***

1. Notificar \_\_\_\_\_, 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 notificado da selecção do plano de recuperação.

- a. Números de contacto em caso de acidente

\_\_\_\_\_ ou \_\_\_\_\_

Estes números de telefone estão em serviço das \_\_\_\_\_ am até às \_\_\_\_\_ pm 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. Indique \_\_\_\_\_ 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. Contacte as companhias da electricidade e dos telefones e programar as ligações de assistência necessárias.
5. Notifique imediatamente \_\_\_\_\_ caso seja necessário alterar algum dos planos relacionados.

**Secção 7. Plano de recuperação–unidade móvel**

1. Notifique \_\_\_\_\_ da natureza do acidente e da necessidade de seleccionar o plano para a unidade móvel.
2. Confirme por escrito o conteúdo da comunicação telefónica com \_\_\_\_\_ num prazo de 48 horas da mesma.
3. Confirme todos os suportes de segurança necessários disponíveis para instalar na máquina de reserva.
4. Prepare uma ordem de compra que contemple a utilização do equipamento de reserva.
5. Notifique \_\_\_\_\_ 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. Consoante as necessidades de comunicação, notifique a companhia dos telefones (\_\_\_\_\_) de possíveis alterações de linhas de emergência.
7. Inicie 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 (\_\_\_\_\_), corte 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 acidente.
8. Quando a caravana chegar, faça as ligações à corrente e efectue as verificações necessárias.
9. Faça as ligações às linhas de comunicações e efectue as verificações necessárias.
10. Inicie o carregamento do sistema a partir das cópias de segurança (consulte a Secção 9. Restaurar Todo o Sistema).
11. Inicie as operações normais assim que for possível:
  - a. Trabalhos diários
  - b. Salvaguardas diárias
  - c. Salvaguardas semanais
12. Estabeleça 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. Proteja a unidade móvel e distribua as chaves necessárias.
14. Mantenha 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 acidente*

Inclua aqui o plano das comunicações em caso de acidente, 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 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. Notifique \_\_\_\_\_ da natureza do acidente e da necessidade de um centro de emergência.
2. Solicite transporte aéreo dos modems para \_\_\_\_\_ para as comunicações. Consulte \_\_\_\_\_ para comunicações para o centro de emergência.

3. Confirme por escrito o conteúdo da comunicação telefónica com \_\_\_\_\_ num prazo de 48 horas da mesma.
4. Comece a tomar as medidas necessárias para a deslocação da equipa de operações até às instalações.
5. Confirme se todas as bandas necessárias estão disponíveis e empacotadas para serem enviadas para se fazer o restauro no sistema de segurança.
6. Prepare 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 centro de emergência.
8. Certifique-se de que a equipa de recuperação de acidentes que está no local tem as informações necessárias para começar a restaurar as instalações. Consulte a Secção 12. Reconstrução das instalações do acidente.
9. Encarregue-se das despesas de viagem (tenha dinheiro disponível).
10. Depois de chegar ao centro de emergência, contacte a instalação central para estabelecer os procedimentos de comunicação.
11. Reveja se os materiais transportados para o centro de emergência estão completos.
12. Comece a carregar o sistema a partir das bandas de salvaguarda.
13. Inicie as operações normais assim que for possível:
  - a. Trabalhos diários
  - b. Salvaguardas diárias
  - c. Salvaguardas semanais
14. Estabeleça 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*

Inclua 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*, SC10-3123-07.

*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, 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
- Registo do histórico da operação de salvaguarda integral mais recente
- Registo do histórico da operação de salvaguarda semanal mais recente

- Registo do histórico das operações de salvaguarda diárias
- O manual *Instalação, actualização ou eliminação do OS/400 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 preparado em termos de utilização de computadores?

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

### Secção 11. Testar o plano de recuperação de acidentes

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*

Artigo	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 4. Áreas a testar

Artigo	Sim	Não	Aplicável	Não Aplicável	Comentários
Recuperação de sistemas de aplicações individuais utilizando ficheiros e documentação armazenados fora das instalações.					
Novo carregamento de bandas do sistema e realização de um IPL utilizando ficheiros e documentação guardados fora das instalações.					
Capacidade de efectuar o processamento noutra 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 de segurança alternativos 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 dar entrada em sistemas essenciais utilizando instalações alternativas e suportes de entrada de dados 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 dos resultados produzidos nas instalações de recuperação.					
Disponibilidade do stock 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. 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:

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





---

## 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 da IBM 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
- | U.S.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
- | Tokyo 106-0032, Japan

**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 impressas 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) referidos 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 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 49XA
- | 3605 Highway 52 N
- | Rochester, MN 55901
- | U.S.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 sob os termos do IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, ou qualquer acordo existente entre ambos.

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 tais produtos e não pode confirmar a exactidão do desempenho, a compatibilidade ou outras alegações relativas a produtos que lhe são alheios. Quaisquer perguntas sobre as capacidades de produtos alheios à IBM deverão ser endereçadas aos fornecedores desses produtos.

Todas as instruções relativas a projectos e intenções futuras da IBM estão sujeitas a alteração ou eliminação sem aviso prévio e representam meramente metas e objectivos.

Estas informações destinam-se somente a fins de planeamento. As presentes informações estão sujeitas a alterações antes de os produtos aqui mencionados serem disponibilizados.

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.

---

## Marcas Registadas

Os termos que se seguem são marcas registadas da International Business Machines Corporation nos Estados Unidos e/ou noutros países:

AS/400  
e(logo)server  
iSeriesOperating System/400  
OS/400

Outros nomes de empresas, produtos e serviços podem ser marca registada de terceiros.

---

## Termos e condições para descarregar e imprimir publicações

As permissões para uso das publicações seleccionadas para descarregamento são concedidas sujeitas aos seguintes termos e condições e à indicação de aceitação dos mesmos por parte do utilizador.

**Uso Pessoal:** poderá reproduzir estas Publicações para uso pessoal e não comercial desde que todos os avisos de propriedade sejam preservados. Não é permitida a distribuição, apresentação ou elaboração de trabalhos derivados destas Publicações, ou de qualquer parte das mesmas, sem o consentimento expresso por parte da IBM.

**Uso Comercial:** poderá reproduzir, distribuir e exibir estas Publicações somente na empresa a que pertencer e desde que todos os avisos de propriedade sejam preservados. Não é possível efectuar trabalhos derivados destas Publicações, ou reproduzir, distribuir ou apresentar estas Publicações ou qualquer parte das mesmas, fora da empresa, sem o consentimento expresso da IBM.

Salvo no expressamente concedido nesta permissão, não se concedem outras permissões, licenças ou direitos, expressas ou implícitas, relativamente às Publicações ou a informações, dados, software ou demais propriedade intelectual nela contida.

A IBM reserva-se o direito de retirar as permissões concedidas neste documento sempre que, no seu entender, o uso das Publicações seja prejudicial aos seus interesses ou, conforme determinação da IBM, as instruções acima mencionadas não sejam devidamente respeitadas.

Não tem autorização para descarregar, exportar ou reexportar estas informações salvo em conformidade com leis e regulamentos aplicáveis, incluindo leis e regulamentos sobre exportação dos Estados Unidos. A IBM NÃO GARANTE O CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO DISPONIBILIZADAS "TAL COMO ESTÃO" E SEM GARANTIAS DE QUALQUER TIPO, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, A TÍTULO MERAMENTE EXEMPLIFICATIVO, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO FIM.

Todos os materiais estão vinculados pelos direitos de autor da IBM Corporation.

O descarregamento ou a impressão destas publicações constitui aceitação destes termos e condições por parte do utilizador.

---

## **Informações de renúncia sobre códigos**

A IBM concede ao utilizador uma licença de direitos de autor não exclusiva para utilizar todos os exemplos de códigos de programação, dos quais este pode criar funções semelhantes e personalizadas de acordo com as suas necessidades específicas.

- | SUJEITOS A QUAISQUER GARANTIAS ESTATUTÁRIAS QUE NÃO POSSAM SER EXCLUÍDAS, IBM,
- | OS SEUS PROGRAMADORES E FORNECEDORES NÃO FAZEM GARANTIAS OU CONDIÇÕES QUER
- | EXPRESSAS OU IMPLÍCITAS, INCLUINDO MAS NÃO LIMITANDO A, AS GARANTIAS IMPLÍCITAS
- | OU CONDIÇÕES COMÉRCIO, ADAPTAÇÃO PARA UM DETERMINADO FIM, E NÃO INFRACÇÃO,
- | RELATIVAMENTE AO SUPORTE AO PROGRAMA OU TÉCNICO, SE EXISTIR.
  
- | EM QUAISQUER CIRCUNSTÂNCIAS A IBM, OS SEUS DESENVOLVEDORES OU FORNECEDORES DE
- | PROGRAMAS SERÃO TIDOS COMO RESPONSÁVEIS POR QUALQUER DAS SEGUINTEZ RAZÕES,
- | MESMO QUE INFORMADOS DA SUA POSSIBILIDADE:
- | 1. PERDA DE, OU DANOS EM, DADOS;
- | 2. DANOS ESPECIAIS, INCIDENTAIS OU INDIRECTOS, OU POR QUAISQUER DANOS
- | ECONÓMICOS CONSEQUENCIAIS; OU
- | 3. PERDA DE LUCROS, NEGÓCIOS, PROVEITOS, BOA VONTADE, OU POUPANÇAS ANTECIPADAS.
  
- | ALGUMAS JURISDIÇÕES NÃO PERMITEM A EXCLUSÃO OU LIMITAÇÃO DE DANOS INCIDENTAIS
- | OU CONSEQUENCIAIS, PARTE OU TODAS AS LIMITAÇÕES OU EXCLUSÕES ACIMA PODEM NÃO
- | SE APLICAR A SI.







Impresso em Portugal