

IBM

@server

iSeries

Disponibilidad del servidor iSeries







@server

iSeries

Disponibilidad del servidor iSeries



---

# Contenido

<b>Disponibilidad del servidor iSeries</b> . . . . .	1
Conceptos relacionados con la disponibilidad . . . . .	2
Estimar el valor de la disponibilidad . . . . .	3
Determinar qué nivel de disponibilidad necesita . . . . .	4
Evitar las interrupciones no planificadas . . . . .	6
Evitar las interrupciones no planificadas: Preparación ante las anomalías en el disco . . . . .	6
Evitar las interrupciones no planificadas: Planificación para una pérdida de la alimentación. . . . .	7
Evitar las interrupciones no planificadas: Uso de métodos eficaces de gestión de sistemas. . . . .	8
Evitar las interrupciones no planificadas: Preparación del espacio para el servidor . . . . .	9
Reducción de las interrupciones no planificadas . . . . .	9
Reducir las interrupciones no planificadas: Reducción del tiempo para reiniciar el servidor . . . . .	10
Reducir las interrupciones no planificadas: Recuperación de los cambios recientes tras una interrupción no planificada . . . . .	11
Reducir las interrupciones no planificadas: Recuperación de los datos perdidos tras una interrupción no planificada . . . . .	11
Reducción de las interrupciones planificadas . . . . .	13
Reducir las interrupciones planificadas: Reducción de la duración de las copias de seguridad . . . . .	13
Reducir las interrupciones planificadas: Reducción de la duración del mantenimiento y de las actualizaciones de software . . . . .	17
Reducir las interrupciones planificadas: Reducción de la duración del mantenimiento y de las actualizaciones de hardware . . . . .	17
Disponibilidad para varios servidores: Clústeres . . . . .	18
Programas altamente disponibles . . . . .	19
Información relacionada con la disponibilidad . . . . .	19



---

# Disponibilidad del servidor iSeries

En un entorno basado en Internet de rápido desarrollo como el actual, la disponibilidad de los datos y de las aplicaciones cuando se necesitan es un aspecto vital. Si los clientes no pueden acceder a su sitio web porque el servidor no está activo, puede que acudan a la competencia.

La **disponibilidad** es la medición de la frecuencia con la que los datos y las aplicaciones están preparados para que pueda acceder a ellos cuando los necesite. Cada empresa tiene sus propias necesidades de disponibilidad. Cada servidor dentro de la misma empresa tiene sus propias necesidades de disponibilidad. La finalidad de este tema es mostrarle los distintos niveles de disponibilidad de iSeries y ayudarle a determinar qué herramientas de disponibilidad son las adecuadas para su empresa. Es importante observar que la disponibilidad requiere una planificación detallada; estas herramientas de disponibilidad sólo son útiles si las ha implementado **antes** de que se produzca una interrupción.

Antes de empezar realmente a realizar la planificación de la disponibilidad en el sistema, deberá entender algunos conceptos. Para obtener más información, consulte los temas siguientes:

## **Conceptos relacionados con la disponibilidad**

Este tema contiene las definiciones de los términos relacionados con la disponibilidad que se utilizan en todo este tema.

## **Estimar el valor de la disponibilidad**

Este tema le ayuda a evaluar el coste que puede representar una interrupción para la empresa.

## **Determinar qué nivel de disponibilidad necesita**

Este tema le ayuda a determinar qué nivel de disponibilidad necesita su empresa.

Cuando haya adquirido conocimientos básicos de los conceptos relacionados con la disponibilidad y haya determinado qué nivel de disponibilidad necesita, podrá empezar a realizar la planificación de ese nivel en el servidor. Existen varias formas distintas de enfocar la disponibilidad en función de la configuración y de los tipos de interrupciones que posiblemente puedan producirse, tal como se indica a continuación:

## **Soluciones de disponibilidad para un solo servidor**

El iSeries destaca especialmente por su fiabilidad. No obstante, si tiene necesidades de disponibilidad muy altas para el servidor, existen varias herramientas que puede utilizar para lograr sus objetivos de disponibilidad.

### **Evitar las interrupciones no planificadas**

En este tema se describe cómo evitar que se produzcan interrupciones no planificadas sobre las que tiene algún control y cómo prepararse para hacer frente a las que no puede controlar.

### **Reducir las interrupciones no planificadas**

En este tema se describe qué puede hacer para garantizar que las interrupciones no planificadas sean, en caso de que se produzcan, lo más breves que sea posible.

### **Reducir las interrupciones planificadas**

En este tema se describe cómo puede reducir las interrupciones planificadas que puede controlar.

## **Soluciones de disponibilidad cuando se utilizan varios servidores**

Si necesita un nivel de disponibilidad superior al que puede obtener con un solo servidor, debe considerar la utilización de clústeres. Consulte el tema siguiente para obtener más información acerca de los clústeres:

## Disponibilidad para varios servidores: Clústeres

En este tema se describe cómo pueden ayudarle los clústeres a obtener una disponibilidad cercana al 100 por cien para las aplicaciones y los datos más importantes.

Para obtener información detallada acerca de la disponibilidad y acerca de las herramientas de disponibilidad que se indican en este tema, consulte Información relacionada.

---

## Conceptos relacionados con la disponibilidad

Antes de realizar la planificación de la disponibilidad, es importante entender algunos de los conceptos asociados a este tema.

La disponibilidad se mide en términos de **interrupciones**, que son los períodos de tiempo durante los que el servidor no está disponible para los usuarios. Durante una **interrupción planificada** (también denominada interrupción programada) se hace, deliberadamente, que el sistema no esté disponible para los usuarios. Puede utilizar una interrupción programada para ejecutar un trabajo de proceso por lotes, para realizar la copia de seguridad del servidor o para aplicar arreglos.

Una **interrupción no planificada** (también denominada interrupción no programada) suele deberse a una anomalía. Puede realizar la recuperación de algunas interrupciones no planificadas (por ejemplo, una anomalía en el disco, una anomalía en el sistema, una anomalía en la alimentación, una anomalía en el programa o un error humano) si dispone de una estrategia de realización de copias de seguridad adecuada. Sin embargo, para una interrupción no planificada que dé lugar a una pérdida completa del sistema, como por ejemplo, la que puede producirse a consecuencia de una fuerte tormenta o de un incendio, es necesario disponer de un plan de recuperación detallado para situaciones muy graves con el fin de poder realizar su recuperación.

La **duración de la copia de seguridad** es el período de tiempo durante el cual el servidor no está disponible para los usuarios mientras se realizan operaciones de copia de seguridad. La duración de la copia de seguridad supone una interrupción programada que suele producirse por las noches o los fines de semana, cuando el servidor experimenta menos tráfico.

Existen varios niveles de disponibilidad, que se diferencian por el tipo y la duración de las interrupciones que admiten. Estos niveles son los siguientes:

- **Altamente disponible.** El servidor ofrece un nivel aceptable o acordado de servicio durante su período de funcionamiento programado. El objetivo es que el servidor esté disponible cuando el cliente lo necesite.
- **Alta disponibilidad.** El servidor ofrece un nivel aceptable o acordado de servicio durante su período de funcionamiento programado. El objetivo es que no se produzca ninguna interrupción no planificada; podrían producirse algunas interrupciones planificadas.
- **Operaciones continuadas.** El servidor ofrece un nivel aceptable o acordado de servicio 24 horas al día, 365 días al año. El objetivo es que el servidor funcione sin interrupciones planificadas; podrían producirse algunas interrupciones no planificadas.
- **Disponibilidad continuada.** El servidor ofrece un nivel aceptable o acordado de servicio 24 horas al día, 365 días al año. El objetivo es que no se produzca ninguna interrupción planificada ni no planificada.

En el diagrama siguiente se muestra cómo se relacionan entre sí estos distintos niveles de disponibilidad y qué tipos de empresas son adecuados para cada nivel.



\*

Para obtener más información acerca de estos conceptos y cómo se relacionan entre sí, consulte Información relacionada.

## Estimar el valor de la disponibilidad

Nadie discute la importancia que tiene la disponibilidad. Sin embargo, cuando a las personas se les plantea que realicen una estimación del coste de hardware adicional necesario para dar soporte a una mejor disponibilidad, muchas de ellas no saben desarrollar un argumento. En los pasos siguientes se describe cómo realizar una estimación del valor de los servicios de información:

1. **Confeccione una lista de los principales servicios que proporciona su servidor.** La finalidad del servidor es que los usuarios finales puedan realizar tareas. Para estimar correctamente el valor que tiene el servidor para la organización, debe identificar para qué utilizan el servidor los usuarios.
2. **Valore cuál es el coste derivado de la no disponibilidad de esos servicios.** Cada aplicación o servicio afecta a las personas que utilizan el servidor. Debe determinar qué usuarios pueden verse afectados y cómo se ven afectados.
3. **Compare los costes directos con los costes indirectos.** Los costes directos son pérdidas que nos conducen directamente al servidor que no está disponible. Los costes indirectos son los contraídos por otro departamento o función como resultado de una interrupción.
4. **Compare los costes tangibles con los costes intangibles.** Los costes tangibles son los que pueden medirse económicamente. Sin embargo, existen otros costes que no se miden en dinero, como por ejemplo, la participación en el mercado, la pérdida de oportunidades y la buena voluntad.
5. **Analice los costes fijos frente a los costes variables.** Los costes fijos son los que resultan de una anomalía y siempre son los mismos, con independencia de la duración de la interrupción. Los costes variables son los que varían en función de la duración de la interrupción.

Para obtener ayuda para calcular qué puede costarle el tiempo de inactividad, puede utilizar la herramienta IT Cost of Downtime Calculator



Otra fuente de consulta que le resultará de utilidad es la publicación *So you want to estimate the value of availability?* (GG22-9318). Puede solicitarla a través del centro de publicaciones de IBM



---

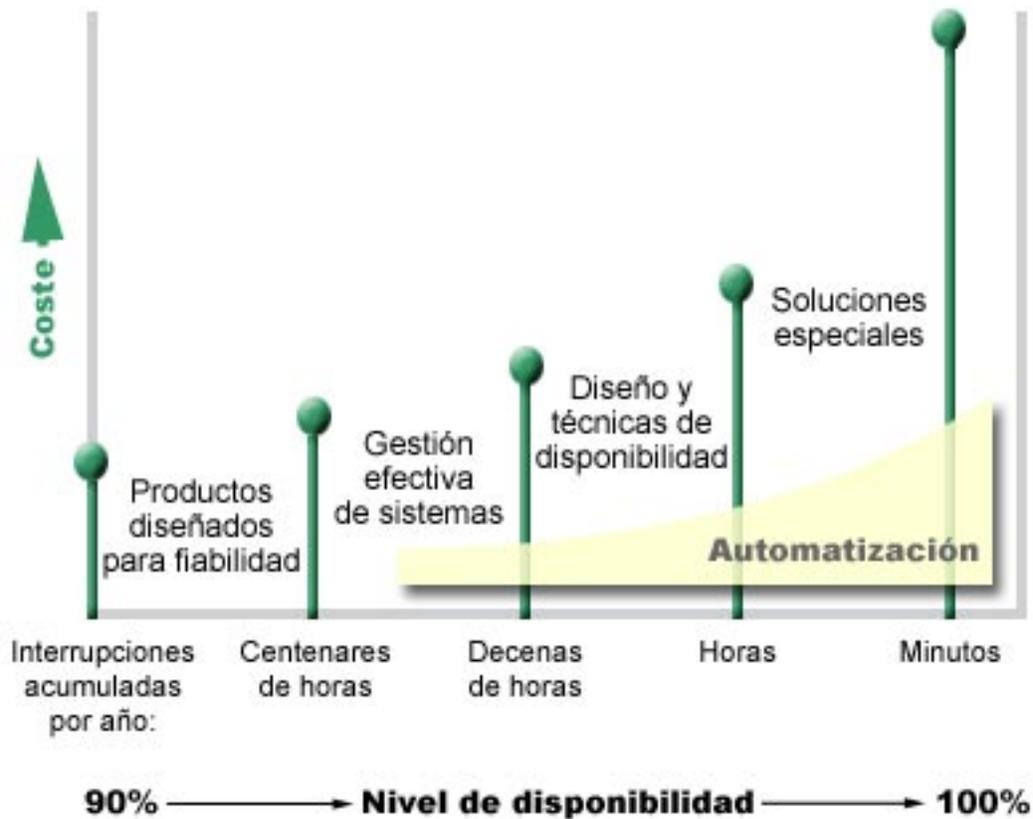
## Determinar qué nivel de disponibilidad necesita

Ahora que ya entiende algunos de los conceptos relacionados con la disponibilidad y tiene una idea de los costes que el tiempo de inactividad conlleva, también debe saber que la disponibilidad tiene un precio. Cuanto más alto sea el nivel de disponibilidad necesario, mayor será el precio. Por lo tanto, es importante haber analizado cuidadosamente las necesidades de la empresa para determinar qué nivel de disponibilidad puede mantener.

Para determinar qué nivel de disponibilidad necesita, considere las preguntas siguientes:

### ¿Tiene alguna aplicación que necesite un 100% de disponibilidad?

En la mayoría de los casos, puede obtenerse un alto nivel de disponibilidad implementando los procesos y los métodos de gestión de sistemas adecuados. Cuanta más disponibilidad continuada necesite, mayor será la inversión que deberá realizar. Antes de realizar una inversión de este tipo, debe estar seguro de que necesita ese nivel de disponibilidad. En la figura siguiente se muestra cómo distintas técnicas pueden mejorar la disponibilidad, aunque también pueden aumentar el precio que deberá pagar por ello.



\*

### ¿Cuánto tiempo de inactividad le parece aceptable?

Puede que le ayude saber la cantidad de tiempo de inactividad que representa cada nivel de disponibilidad. En la tabla siguiente se muestra la cantidad de tiempo de inactividad que debe esperarse en los distintos niveles de disponibilidad.

Nivel de disponibilidad	Tiempo de inactividad por año
90%	36,5 días
95%	18,25 días
99%	3,65 días
99,9%	8,76 horas

Además de saber el tiempo de inactividad que considera aceptable, también debe tener en cuenta cómo puede producirse ese tiempo de inactividad. Por ejemplo, es posible que considere que el 99% de disponibilidad es aceptable si el tiempo de inactividad es una serie de interrupciones breves que tienen lugar a lo largo de todo el año. No obstante, es probable que no piense lo mismo acerca del 99% de disponibilidad si el tiempo de inactividad fuera en realidad una única interrupción que durara 3,65 días.

### ¿Qué nivel de acceso a la empresa necesitan sus clientes?

Anteriormente, los clientes solían acceder a la empresa desde las 9 de la mañana hasta las 5 de la tarde, por lo tanto, cabría suponer que el servidor sólo debía estar disponible durante esas horas. Sin embargo,

Internet ha cambiado esa suposición; los clientes pueden acceder al sitio web de la empresa en cualquier momento del día o de la noche. Cuando determine el nivel de disponibilidad que desea mantener, también deberá determinar qué es lo que los clientes esperan y cuál es la postura más realista respecto a ello.

---

## Evitar las interrupciones no planificadas

Una forma de enfocar la disponibilidad es intentar evitar las interrupciones no planificadas. En este tema se describen distintos métodos que puede utilizar para asegurarse de que el servidor experimente el menor tiempo de inactividad no planificado posible.

Para evitar las interrupciones no planificadas, debe realizar lo siguiente:

### **Preparación ante las anomalías en el disco**

Las anomalías en el disco se producen raras veces, pero es algo para lo que puede estar preparado. En este tema se describe cómo hacerlo.

### **Planificación para una pérdida de la alimentación**

La pérdida de la alimentación es algo que no puede planificarse o evitarse, pero puede estar preparado para cuando se produzca. En este tema se describe cómo hacerlo.

### **Uso de métodos eficaces de gestión de sistemas**

En este tema se describe cómo supervisar el rendimiento del sistema y cómo gestionar las operaciones del sistema que pueden contribuir a obtener una mejor disponibilidad general.

### **Preparación del espacio para el servidor**

El espacio físico en el que reside el servidor debe prepararse cuidadosamente para garantizar que las condiciones favorezcan una disponibilidad óptima. En este tema se describe cómo deben ser las condiciones físicas para el servidor.

Si dispone de un solo servidor y no puede obtener el nivel de disponibilidad que necesita mediante la utilización de estas estrategias, considere la posibilidad de utilizar clústeres. Para obtener más información al respecto, consulte Disponibilidad para varios servidores: Clústeres.

## Evitar las interrupciones no planificadas: Preparación ante las anomalías en el disco

El almacenamiento en disco es el almacenamiento interno del servidor iSeries o un almacenamiento conectado al mismo. El servidor considera que este espacio en disco, junto con la memoria principal del servidor, es un área de almacenamiento de gran tamaño. Cuando guarda un archivo, no lo asigna a una ubicación de almacenamiento; en lugar de ello, el servidor coloca el archivo en la ubicación que garantiza el mejor rendimiento. Es posible que distribuya los datos del archivo entre varias unidades de disco si ello constituye la mejor opción. Cuando se añaden más registros al archivo, el sistema asigna espacio adicional en una o más unidades de disco. Esta forma de direccionar el almacenamiento se denomina **almacenamiento de un solo nivel**.

Puesto que los datos se distribuyen entre los discos, es importante considerar cómo pueden protegerse los datos en caso de que se produzca una anomalía en uno de esos discos. La finalidad de este tema es ofrecer una descripción de los métodos que puede utilizar para proteger los discos. Para obtener información adicional acerca de los métodos que aquí se describen, consulte Protección del disco.

### **Protección de dispositivo por paridad**

La protección de dispositivo por paridad permite que el servidor pueda seguir funcionando cuando un disco presenta una anomalía o se daña. Cuando se utiliza la protección de dispositivo por paridad, el adaptador de entrada/salida (IOA) del disco calcula y guarda un valor de paridad para cada bit de datos. El IOA calcula el valor de paridad de los datos en la misma ubicación de cada una de las demás unidades

de disco del conjunto de paridad de dispositivo. Cuando se produce una anomalía en el disco, los datos pueden reconstruirse utilizando el valor de paridad y los valores de los bits de las mismas ubicaciones de los otros discos. Mientras tiene lugar la reconstrucción de los datos, el servidor sigue en ejecución.

Para obtener información detallada acerca de la protección de dispositivo por paridad, consulte Protección de dispositivo por paridad.

### **Protección por duplicación**

La protección por duplicación es una forma de proteger los datos en caso de que se produzca una anomalía en el disco. Los datos quedan protegidos porque el sistema mantiene dos copias de los datos en dos unidades de disco distintas. Cuando se produce una anomalía en un componente relacionado con un disco, el sistema puede seguir funcionando sin interrupciones utilizando una copia duplicada de los datos hasta que se repara el componente anómalo.

Son posibles distintos niveles de protección por duplicación, en función del hardware que se haya duplicado. Puede duplicar lo siguiente:

- Las unidades de disco
- Los controladores de disco
- La unidad de bus de E/S
- Los procesadores de E/S de disco
- Un bus

Para obtener información detallada acerca de la protección por duplicación, incluidos su funcionamiento y su planificación, consulte Protección por duplicación.

### **Agrupaciones de discos independientes**

Las agrupaciones de discos independientes (también denominadas agrupaciones de almacenamiento auxiliar independientes) permiten evitar que se produzcan interrupciones no planificadas porque los datos de éstas quedan aislados del resto del servidor. Si una agrupación de discos independiente presenta una anomalía, el servidor puede seguir funcionando. Para obtener información detallada acerca de la utilización de las agrupaciones de discos independientes, consulte Agrupaciones de discos independientes.

## **Evitar las interrupciones no planificadas: Planificación para una pérdida de la alimentación**

Para garantizar que el servidor estará disponible cuando se necesite, es necesario asegurarse de que dispone de una fuente de alimentación adecuada y de que está protegido en caso de que se produzca una pérdida de la alimentación.

### **Requisitos de alimentación**

Una parte del proceso de planificación para el servidor consiste en garantizar que se dispone de una fuente de alimentación adecuada. Deberá saber cuáles son los requisitos del servidor y solicitar la ayuda de un electricista cualificado para instalar los cables correctos. Para obtener información detallada acerca de cómo puede garantizarse que el servidor dispondrá de la alimentación adecuada, consulte el tema Determinar los requisitos de alimentación.

### **Baterías de reserva**

Algunos servidores iSeries se entregan con baterías de reserva. La unidad de batería de reserva proporciona 30 segundos de ejecución. Si la alimentación no se restablece transcurridos 30 segundos, el sistema entra inmediatamente en un estado de conclusión controlada.

## Fuentes de alimentación redundante

Algunos servidores iSeries disponen de fuentes de alimentación redundante. Una fuente de alimentación redundante es una característica que evita que se produzca una interrupción no planificada proporcionando alimentación en caso de que una fuente de alimentación deje de suministrarla.

## Fuentes de alimentación ininterrumpida

Aun cuando cuente con una fuente de alimentación adecuada, es posible que se produzca un corte en la alimentación, por ejemplo, durante una tormenta. Para evitar las interrupciones no planificadas que tienen lugar como consecuencia de una pérdida de la alimentación, puede que sea necesario realizar una inversión en hardware específicamente diseñado para mantener el servidor en funcionamiento cuando se pierde la alimentación. Un dispositivo de hardware de este tipo sería una **fuentes de alimentación ininterrumpida (UPS)**. Puede utilizar una UPS para suministrar alimentación auxiliar al procesador, los discos, la consola del sistema y cualquier otro dispositivo que crea que la necesita. Las fuentes de alimentación ininterrumpida proporcionan las ventajas siguientes:

- Permiten continuar con las operaciones cuando se han producido interrupciones en la alimentación de corta duración.
- Protegen el servidor en caso de producirse picos de voltaje.
- Proporcionan una finalización normal de las operaciones, lo que puede reducir el tiempo de recuperación al reiniciar el servidor. Para obtener información acerca de la escritura de un programa que le ayude a controlar la conclusión del servidor ante estas situaciones, consulte Controlar la conclusión del servidor mediante un programa de manejo de la alimentación.

Para obtener información acerca de las fuentes de alimentación ininterrumpida que son compatibles con el servidor iSeries, consulte Sistemas de fuentes de alimentación ininterrumpida.

## Generador de alimentación

Si cree que puede experimentar una anomalía general en la alimentación, es importante considerar la posibilidad de comprar un generador. Un generador ofrece más ventajas que una UPS porque permite seguir realizando operaciones normales cuando se producen cortes en la alimentación de mayor duración.

Si necesita ayuda para planificar las necesidades de alimentación del servidor iSeries, consulte Power Protection Services



## Evitar las interrupciones no planificadas: Uso de métodos eficaces de gestión de sistemas

Una de las formas más sencillas de evitar las interrupciones no planificadas es asegurarse de realizar todo lo necesario para garantizar la correcta ejecución del servidor. Esto incluye la realización de tareas básicas de mantenimiento preventivo y de gestión de sistemas que ayuden a maximizar el rendimiento del sistema. La mayoría de estas tareas de gestión de sistemas pueden automatizarse, lo que ayuda a evitar que se produzcan anomalías que pueden ser el resultado de un error humano o de un descuido.

Una forma de garantizar la disponibilidad del servidor es supervisar su rendimiento y reaccionar con prontitud ante cualquier problema que pueda detectarse. Puede utilizar los servicios de recogida y las funciones de supervisión de Management Central para activar y realizar el seguimiento del rendimiento del servidor activamente. Puede hacer que se le envíen notificaciones acerca de cualquier problema que comprometa la disponibilidad del servidor, a tiempo para reaccionar y evitar una interrupción no planificada. Para obtener más información acerca de la planificación y de la gestión del rendimiento del servidor, consulte Rendimiento.

Los arreglos también son un importante componente de la gestión de sistemas que pueden ayudarle a mantener la disponibilidad del sistema. Cuando se detectan problemas en los programas de iSeries, IBM facilita un **arreglo** (también denominado PTF o arreglo temporal del programa) para corregir el problema. Debe estar informado acerca de los arreglos e instalarlos en el servidor para asegurarse de que su funcionamiento esté en su nivel óptimo. Debe crear una estrategia de gestión de arreglos y establecer que el proceso de verificación y aplicación de nuevos arreglos forme parte del mantenimiento habitual del servidor. Para obtener más información acerca de la obtención y aplicación de arreglos, consulte Uso de arreglos de software. Para obtener ayuda acerca de la determinación de una estrategia para realizar un mantenimiento preventivo en función del entorno y de las aplicaciones de iSeries, consulte Fix Maintenance Advisor



## Evitar las interrupciones no planificadas: Preparación del espacio para el servidor

Una forma de evitar que se produzcan interrupciones no planificadas es asegurarse de que el espacio en el que coloca el servidor favorezca la disponibilidad. En el rendimiento del servidor participan numerosos factores físicos y del entorno.

En primer lugar, debe familiarizarse con el servidor. Los distintos modelos de servidor tienen requisitos distintos en relación con las condiciones en las que deben estar, por lo tanto, debe conocer las necesidades del servidor. Para obtener más información acerca de las características físicas de cada modelo, consulte Especificaciones del servidor. Para obtener información acerca de las características físicas del hardware que se conecta con el servidor, consulte Hojas de especificaciones de hardware.

Cuando se haya familiarizado con las características físicas del servidor, tenga presente lo siguiente acerca del espacio en el que debe residir el servidor:

- **Ubicación.** La ubicación física del servidor puede influir en su disponibilidad. Por ejemplo, si la sala no es segura, el servidor podría quedar expuesto a cualquier agresión o, incluso, podría desenchufarse accidentalmente el cable de alimentación. Para obtener información más detallada acerca de las precauciones que deben tomarse respecto a la ubicación del servidor, consulte Consideraciones acerca de la ubicación.
- **Cables.** Con frecuencia, no se da mucha importancia a los cables, pero, sin ellos, no podríamos utilizar el servidor. Debe asegurarse de que los cables están en perfectas condiciones y de que su utilización es la correcta. Para obtener más información acerca de cómo estar seguro de que los cables están utilizándose correctamente, consulte el tema Consideraciones generales acerca del cableado.
- **Entorno.** El entorno en el que se instala el servidor también es muy importante para la disponibilidad. El entorno incluye, por ejemplo, la temperatura, la humedad y otros factores que pueden impedir que el rendimiento del servidor sea correcto. Para obtener información más detallada acerca del entorno en el que ha de instalarse el servidor, consulte Referencia del entorno.

---

## Reducción de las interrupciones no planificadas

Las interrupciones no planificadas, sin duda, se producen, y la clave para contar con la disponibilidad adecuada consiste en asegurarse de que, cuando se produzcan, podrá realizar la recuperación de éstas en el menor tiempo posible. La finalidad de todas las estrategias de recuperación es devolverle al punto en el que se encontraba antes de que se produjera la interrupción.

En los temas siguientes se describen las herramientas de disponibilidad que pueden ayudarle a reiniciar el servidor y a recuperar los datos con la mayor celeridad posible tras producirse una interrupción:

### **Reinicio del servidor**

En este tema se describen las herramientas de disponibilidad que pueden utilizarse para garantizar el servidor se reiniciará tan pronto como sea posible tras una interrupción.

### **Recuperación de los cambios recientes**

En este tema se describen las herramientas de disponibilidad que pueden utilizarse para realizar la recuperación de una interrupción cuando sólo se han perdido los últimos cambios realizados justo antes de la interrupción.

### **Recuperación de los datos perdidos**

En este tema se describen las herramientas de disponibilidad que pueden utilizarse para realizar la recuperación de una interrupción que da lugar a la pérdida de datos. La pérdida puede ser de algunos archivos o de todo el sitio, como sucede cuando se ha producido un desastre natural.

Si dispone de un solo servidor y no puede obtener el nivel de disponibilidad que necesita mediante la utilización de estas estrategias, considere la posibilidad de utilizar clústeres. Para obtener más información al respecto, consulte Disponibilidad para varios servidores: Clústeres.

## **Reducir las interrupciones no planificadas: Reducción del tiempo para reiniciar el servidor**

El servidor, antes de apagarse, realiza ciertas actividades para garantizar que los datos están protegidos y que los trabajos finalizan de forma controlada. Cuando experimenta una interrupción no planificada, el servidor no puede realizar estas actividades. Para obtener información más detallada acerca de qué sucede cuando el servidor finaliza de forma anormal, consulte Iniciar y detener el servidor iSeries.

La finalidad de este tema es ofrecer una descripción de algunas herramientas de disponibilidad que pueden utilizarse para que el servidor se reinicie tan pronto como sea posible.

### **Protección por vía de acceso gestionada por el sistema (SMAPP)**

Una **vía de acceso** es la ruta que una aplicación toma a través de un archivo de base de datos hasta llegar a los registros que necesita. Un archivo puede tener varias vías de acceso si existen distintos programas que necesitan detectar los registros en distintas secuencias. Cuando el servidor finaliza de forma anormal, como en el caso de una interrupción no planificada, el servidor debe volver a crear las vías de acceso la próxima vez que se inicia, actividad que puede tardar bastante tiempo en completarse. Cuando se utiliza la protección por vía de acceso gestionada por el sistema, el servidor protege las vías de acceso para que no tengan que volver a crearse al iniciarse el servidor tras una interrupción no planificada. Esto le ahorrará tiempo al reiniciar el servidor, lo que le permitirá volver a los procesos normales de su empresa con la mayor celeridad posible. Para obtener información detallada acerca de SMAPP, consulte Protección por vía de acceso gestionada por el sistema.

### **Registro por diario de las vías de acceso**

Al igual que SMAPP, el registro por diario de las vías de acceso puede ayudarle a garantizar que los archivos y las vías de acceso más importantes estarán disponibles en el menor tiempo posible tras el reinicio del servidor. Sin embargo, cuando se utiliza SMAPP, el *servidor decide* qué vías de acceso deben protegerse. Por lo tanto, si el servidor no protege una vía de acceso que podría considerarse importante, puede que la reanudación de las actividades de la empresa sufra algún retardo. Cuando las vías de acceso se registran por diario, *puede decidir personalmente* qué vías de acceso deben registrarse por diario. Para obtener información más detallada acerca del registro por diario de las vías de acceso, consulte SMAPP y registro por diario de vías de acceso.

## **Reducir las interrupciones no planificadas: Recuperación de los cambios recientes tras una interrupción no planificada**

Tras producirse una interrupción no planificada, el objetivo es volver a establecer el funcionamiento del servidor tan pronto como sea posible. Es importante volver al punto en el que se encontraba antes de que se produjera la interrupción sin tener que volver a entrar transacciones manualmente. Esto puede implicar la reconstrucción de algunos de los datos. Existen varias herramientas de disponibilidad que puede utilizar y que le ayudarán a volver más rápidamente al estado en el que se encontraba antes de que se produjera la interrupción.

### **Registro por diario**

La gestión del registro por diario evita que se pierdan transacciones si el servidor experimenta una finalización anormal. Cuando registra un objeto por diario, el servidor conserva un registro de los cambios que ha realizado en ese objeto. Para obtener información detallada acerca de cómo planificar y utilizar el registro por diario, consulte Gestión del registro por diario.

### **Control de las confirmaciones**

El control de las confirmaciones ayuda a proporcionar integridad de los datos en el servidor. Permite definir y procesar un grupo de los cambios realizados en los recursos, como por ejemplo, los archivos o las tablas de base de datos, como si fuera una única transacción. Así pues, garantiza que o bien se producirá el grupo completo de los cambios individuales o bien no se producirá ningún cambio. Por ejemplo, supongamos que pierde la alimentación justo cuando está realizándose una serie de actualizaciones en la base de datos. Sin el control de las confirmaciones, se corre el riesgo de que los datos no estén completos o que se hayan dañado. Con el control de las confirmaciones, las actualizaciones que no se han completado volverían a la base de datos al reiniciarse el servidor.

Puede utilizar el control de las confirmaciones para diseñar una aplicación que haga que el sistema pueda reiniciar la aplicación si un trabajo, un grupo de activación dentro de un trabajo o el sistema finaliza de forma anormal. Con el control de las confirmaciones puede garantizarse que, cuando vuelva a iniciarse la aplicación, en la base de datos no habrá ninguna actualización parcial debida a la existencia de transacciones incompletas resultantes de una anomalía anterior.

Para obtener información detallada acerca de la planificación y de la utilización del control de las confirmaciones, consulte Control de las confirmaciones.

## **Reducir las interrupciones no planificadas: Recuperación de los datos perdidos tras una interrupción no planificada**

Es posible que pierda datos a consecuencia de una interrupción no planificada, como por ejemplo, una anomalía en el disco. El ejemplo más extremo de una pérdida de datos es la pérdida de todo el sitio, que podría producirse como resultado de una inundación o de una fuerte tormenta. Existen formas de evitar la pérdida de datos ante tales situaciones o, como mínimo, limitar la cantidad de datos perdidos.

### **Copia de seguridad y recuperación**

Es muy importante disponer de una estrategia eficaz para la realización de una copia de seguridad del servidor; el tiempo y el dinero que invierta en la creación de esta estrategia estarán más que amortizados si tiene que realizar la restauración de los datos perdidos o llevar a cabo una recuperación. Cuando haya creado una estrategia, deberá asegurarse de que funciona probándola, lo que implica realizar una copia de seguridad y una recuperación y, a continuación, validar si los datos de los que se ha hecho una copia de seguridad y que se han restaurado son correctos. Si realiza algún cambio en el servidor, deberá determinar si también debe realizar algún cambio en la estrategia de copia de seguridad y recuperación.

Todos los entornos de servidor y empresariales son distintos pero, idealmente, debería intentar realizar una copia de seguridad completa del servidor, como mínimo, una vez a la semana. Si su entorno es muy dinámico, también será necesario realizar una copia de seguridad de los cambios realizados en los objetos del servidor desde la última copia de seguridad. De este modo, si experimenta una interrupción no esperada y tiene que recuperar esos objetos, podrá recuperar la última versión de éstos.

Para obtener información acerca de la creación de una estrategia de copia de seguridad y recuperación, consulte Planificación de una estrategia de copia de seguridad y recuperación. Para obtener instrucciones acerca de la realización de las copias de seguridad del servidor, consulte Copia de seguridad del servidor. Para obtener más información acerca de la restauración del servidor, consulte Recuperación del servidor.

Si desea una solución que le ayude a gestionar la estrategia de copia de seguridad y restauración y los medios de copia de seguridad, puede utilizar el programa BRMS (Backup, Recovery and Media Services). **BRMS** es un programa que le ayuda a implementar un enfoque disciplinado para gestionar las copias de seguridad y que le ofrece un procedimiento metódico para recuperar los datos perdidos o dañados. Mediante la utilización de BRMS, podrá gestionar fácilmente las copias de seguridad más críticas y complejas, incluidas las copias de seguridad en línea de los servidores de Lotus. También podrá recuperar todo el servidor en caso de producirse una situación o una anomalía muy grave.

Además de estas características de copia de seguridad y recuperación, BRMS le permite realizar el seguimiento de los medios de copia de seguridad desde su creación hasta su caducidad. Ya no tendrá que preocuparse de qué información de copia de seguridad se encuentra en qué volumen ni de grabar accidentalmente sobre los datos activos. También puede realizar el seguimiento del traslado de medios hacia y desde ubicaciones externas.

Para obtener información detallada acerca de las tareas que el programa BRMS puede ayudarle a realizar, consulte Servicios de copia de seguridad, recuperación y medios.

Para obtener ayuda para planificar y gestionar la estrategia de copia de seguridad y recuperación, póngase en contacto con IBM Business Continuity and Recovery Services



### Limitación de la cantidad de datos que pueden perderse

Puede agrupar las unidades de disco en subconjuntos lógicos denominados **agrupaciones de discos** (conocidos también como agrupaciones de almacenamiento auxiliar o ASP). Los datos de una agrupación de discos quedan aislados de los datos de las otras agrupaciones de discos. Si se produce una anomalía en una unidad de disco, sólo tendrá que recuperar los datos que se habían almacenado en la agrupación de discos de la que la unidad de disco anómala formaba parte.

Para obtener información detallada acerca de las agrupaciones de discos, los tipos de agrupaciones de discos y ejemplos de utilización de las agrupaciones de discos para distintas finalidades, consulte Agrupaciones de discos. Para obtener información acerca de la configuración de las unidades de discos y de las agrupaciones de discos, consulte Gestión de las agrupaciones de discos.

Las **agrupaciones de discos independientes** son agrupaciones de discos que pueden establecerse en estado en línea y en estado fuera de línea sin depender del resto del almacenamiento de un sistema. Esto es posible porque toda la información del sistema necesaria que se asocia a la agrupación de discos independiente está contenida dentro de la agrupación de discos independiente. Las agrupaciones de discos independientes ofrecen varias ventajas de disponibilidad y rendimiento tanto en los entornos de un único sistema como en los entornos de varios sistemas. Para obtener información detallada al respecto, consulte Agrupaciones de discos independientes.

El servidor iSeries también le ofrece la posibilidad de dividir un servidor en varios servidores independientes. Esta tecnología se denomina **particiones lógicas**. La utilización de particiones lógicas es otra forma de aislar los datos, las aplicaciones y otros recursos. Puede utilizar particiones lógicas para mejorar el rendimiento del servidor, por ejemplo, ejecutando procesos por lotes y procesos interactivos en distintas particiones. También puede proteger los datos instalando una aplicación importante en una partición distinta de las demás aplicaciones. De este modo, si otra partición presenta alguna anomalía, ese programa quedará protegido.

Aunque las particiones lógicas tienen muchas ventajas, también tienen algunos inconvenientes que deben tenerse en cuenta. Las particiones lógicas pueden hacer que la recuperación de todo el sistema sea más compleja, lo que aumentará el tiempo durante el cual el servidor no estará disponible.

Para obtener información detallada acerca de las particiones lógicas y acerca de su utilización, consulte Particiones lógicas.

---

## Reducción de las interrupciones planificadas

Las interrupciones planificadas son necesarias y se cuenta con ellas; sin embargo, el hecho de que sean planificadas no significa que no sean disruptivas. Las interrupciones planificadas suelen estar relacionadas con el mantenimiento del sistema. En los temas siguientes se describe cómo podrá reducir las interrupciones que son el resultado de distintos tipos de mantenimiento:

### **Reducción de la duración de las copias de seguridad**

Este tema incluye información acerca de cómo puede reducir el período de tiempo durante el cual el servidor no está disponible mientras se realizan las copias de seguridad.

### **Reducción de la duración del mantenimiento y de las actualizaciones de software**

El tiempo que emplea en la realización del mantenimiento del software y las actualizaciones es tiempo durante el cual el servidor no está disponible para los usuarios. Aprenda cómo puede reducir estos tiempos.

### **Reducción de la duración del mantenimiento y de las actualizaciones de hardware**

El tiempo que emplea en la realización del mantenimiento del hardware y las actualizaciones es tiempo durante el cual el servidor no está disponible para los usuarios. Aprenda cómo puede reducir estos tiempos.

Si dispone de un solo servidor y no puede obtener el nivel de disponibilidad que necesita mediante la utilización de estas estrategias, considere la posibilidad de utilizar clústeres. Para obtener más información al respecto, consulte Disponibilidad para varios servidores: Clústeres.

## Reducir las interrupciones planificadas: Reducción de la duración de las copias de seguridad

Una forma de reducir el período de tiempo durante el cual el servidor no está disponible es reducir la cantidad de tiempo que se necesita para realizar las copias de seguridad. Para reducir la cantidad de tiempo que se emplea en la realización de las copias de seguridad, puede hacer varias cosas, incluidas las siguientes:

### **Mejorar el rendimiento de las cintas**

Si realiza las copias de seguridad en cinta, lógicamente podrá reducir la duración de la copia de seguridad incrementando la velocidad a la que puede realizar las copias de seguridad. En este tema se describen las opciones de que dispone para hacerlo.

### Realizar copias de seguridad en línea

Existen determinados objetos y tipos de datos cuya copia de seguridad puede realizarse mientras éstos están utilizándose, sin interrumpir las operaciones del servidor o bien con una interrupción mínima.

### Realizar la copia de seguridad de menos datos

También puede reducir la duración de la copia de seguridad teniendo que guardar menos datos en el momento de realizar la copia de seguridad. Puede realizar la copia de seguridad de algunos objetos en distintos momentos a lo largo de la semana, con lo que se reduce el número de objetos que deben guardarse al realizar la copia de seguridad.

## Reducir la duración de las copias de seguridad: Mejora del rendimiento de las cintas

En este artículo se describe la forma en que los clientes pueden reducir la duración de las copias de seguridad incrementando la velocidad y la capacidad de los medios y del hardware que utilizan.

### Hardware de alto rendimiento

Una forma de reducir la duración de las copias de seguridad es utilizar hardware de cintas que proporcione un rendimiento muy alto. Lógicamente, cuanto más rápida sea la realización de la copia de seguridad de los datos, menos durará la operación. Como ejemplo de este hardware de alto rendimiento cabe citar el sistema IBM TotalStorage<sup>(TM)</sup> Enterprise Tape System 3590. Para obtener más información acerca de dispositivos de cinta de alta velocidad, consulte IBM TotalStorage Enterprise Tape System 3590



Otra solución de cintas que puede ayudarle a reducir la duración de las copias de seguridad es la tecnología LTO (Linear Tape-Open). Esta tecnología ofrece un rendimiento comparable al del sistema de cintas 3590 a un precio que, con toda seguridad, resultará más asequible a la pequeña empresa. Para obtener información más detallada sobre la tecnología LTO y sobre cómo puede utilizarla con el iSeries, consulte Linear Tape-Open



Para obtener información detallada acerca de las velocidades de los dispositivos de copia de seguridad que reciben soporte en el servidor iSeries y sugerencias para mejorar el rendimiento, consulte Performance Capabilities Reference



### Copias de seguridad simultáneas y paralelas

Otra forma de utilizar el hardware de cintas para mejorar la velocidad de las copias de seguridad es utilizar varios dispositivos de cinta que realicen copias de seguridad simultáneas y paralelas. Estos tipos de copia de seguridad pueden reducir considerablemente la duración de las copias de seguridad y hacer que las operaciones de copia de seguridad sean más eficaces.

Cuando se realiza una **copia de seguridad simultánea**, se envían varios trabajos de guardado a varios dispositivos de cinta para que se procesen al mismo tiempo. Por ejemplo, mediante la utilización de una estrategia de copia de seguridad simultánea, podría enviar una biblioteca o un grupo de bibliotecas a un dispositivo de cintas y otro conjunto de bibliotecas a otro dispositivo de cintas. Todo lo que puede

guardarse de forma simultánea, puede restaurarse también de forma simultánea, con lo que se reduce el tiempo de inactividad tras una anomalía en el sistema, ya que se recuperan varias bibliotecas u objetos al mismo tiempo.

Cuando se realiza una **copia de seguridad paralela**, la copia de seguridad de la información se realiza en dos o más dispositivos al mismo tiempo. Existen dos métodos para realizar copias de seguridad paralelas: el soporte paralelo de las operaciones guardar/restaurar y el soporte paralelo de varias bibliotecas. El soporte paralelo de las operaciones guardar/restaurar distribuye cada objeto entre varios recursos. El soporte de varias bibliotecas distribuye las bibliotecas entre varios recursos, de modo que la copia de seguridad de cada biblioteca se realiza en un único recurso. Puede utilizar estos dos métodos para optimizar el rendimiento de los dispositivos y, al mismo tiempo, mantener el equilibrio entre los recursos.

Para obtener más información acerca de las copias de seguridad simultáneas y paralelas, consulte Guardar en varios dispositivos para reducir la duración de la operación de guardar. También puede utilizar el programa BRMS (Backup, Recovery and Media Services) para realizar estos tipos de copia de seguridad.

### **Automatización**

Sin duda alguna, en la mayoría de las empresas las copias de seguridad se activan por la noche, cuando normalmente no se dispone de personal que realice las operaciones de copia de seguridad. Existen varias formas de automatizar los procesos para reducir la duración de las copias de seguridad y hacer que la intervención humana sea innecesaria. Esta automatización recorta gastos y también ayuda a evitar la posibilidad de que se produzcan errores humanos o retardos.

El programa BRMS (Backup, Recovery and Media Services) permite planificar las operaciones mediante un **planificador de trabajos**, como por ejemplo, el planificador de trabajos Management Central. Así, por ejemplo, puede planificar la realización de una copia de seguridad completa desatendida los sábados por la noche y, a continuación, planificar las tareas de mantenimiento que deben llevarse a cabo inmediatamente después de la copia de seguridad. También puede planificar el traslado de los medios de copia de seguridad a ubicaciones externas y realizar el seguimiento de su ubicación durante el traslado.

Asimismo, puede utilizar **bibliotecas de medios** para mejorar el proceso de realización de copias de seguridad. Estos dispositivos disponen de un gran número de volúmenes y hacen que la realización de las copias de seguridad automatizadas sea mucho más sencilla, ya que cambian las cintas de la unidad automáticamente. No se pierde tiempo en la extracción e inserción de volúmenes a medida que se realiza la copia de seguridad. Para obtener más información acerca de la utilización de las bibliotecas de cintas para mejorar el proceso de la realización de las copias de seguridad, consulte Gestión de las bibliotecas de cintas.

### **Reducir la duración de las copias de seguridad: Copias de seguridad en línea**

Puede reducir la duración de las interrupciones planificadas guardando algunos objetos mientras éstos están activos.

Este método de realización de la copia de seguridad de los objetos se denomina soporte **salvar mientras activo**. La operación de salvar mientras activo permite realizar operaciones de guardado con una interrupción limitada en los trabajos y en los subsistemas. Cuando se utiliza la operación de salvar mientras activo, los objetos dejan de estar disponibles durante un período de tiempo breve al inicio del proceso de copia de seguridad, hasta que alcanzan un punto determinado, el denominado punto de control. Cuando la copia de seguridad ha alcanzado ese punto de control, los usuarios pueden volver a trabajar con esos objetos. La operación de salvar mientras activo es muy útil si se desea reducir el tiempo de una interrupción planificada. Sin embargo, su planificación debe realizarse cuidadosamente, teniendo en cuenta si existe alguna restricción que pudiera afectar al proceso de copia de seguridad. Para obtener información detallada acerca de la operación de salvar mientras activo, consulte Guardar el servidor mientras está activo.

Existe otro método para realizar la copia de seguridad de los objetos mientras éstos están utilizándose que se denomina **copia de seguridad en línea**. Las copias de seguridad en línea son similares a las copias de seguridad realizadas mediante la operación de salvar mientras activo, salvo que en aquellas no existe ningún punto de control. Esto significa que los usuarios pueden utilizar los objetos todo el tiempo mientras se realiza la copia de seguridad. El programa BRMS (Backup, Recovery and Media services) da soporte a la copia de seguridad en línea de los servidores Lotus, como Domino y QuickPlace. Puede direccionar estas copias de seguridad en línea a un dispositivo de cintas, a una biblioteca de medios, a archivos de salvar o a un servidor TSM (Tivoli Storage Manager). Para obtener información detallada acerca de las copias de seguridad en línea de Lotus, consulte Servicios de copia de seguridad, recuperación y medios.

**Nota:** es muy importante seguir realizando la copia de seguridad de la información del sistema además de realizar las copias de seguridad de tipo salvar mientras activo o en línea. Existe información del sistema muy importante de la que no puede realizarse una copia de seguridad mediante estos tipos de copia de seguridad.

### **Reducir la duración de las copias de seguridad: Copia de seguridad de menos datos**

En este tema se describe cómo puede reducir las interrupciones planificadas realizando la copia de seguridad de cantidades de datos más pequeñas en distintos momentos. Para realizar este tipo de operación, existen varias formas de aislar los datos del servidor. Puede utilizar el programa BRMS (Backup, Recovery and Media Services) para realizar todos estos tipos de copia de seguridad.

### **Copias de seguridad incrementales**

Las copias de seguridad incrementales permiten guardar los cambios que se han realizado en los objetos desde la última vez que se realizara la copia de seguridad de éstos. Existen dos tipos de copia de seguridad incremental: acumulativa y solo de cambios. Las copias de seguridad **acumulativas** guardan los cambios que se han realizado en un objeto desde que se realizara la última copia de seguridad completa del mismo. Es útil para los objetos que no cambian con excesiva frecuencia o que no cambian demasiado de una copia de seguridad a otra. Las copias de seguridad **solo de cambios** guardan los cambios que se han realizado en un objeto desde la última vez que se realizara la copia de seguridad de ese objeto, con independencia de si la copia de seguridad era una copia de seguridad completa o una copia de seguridad incremental. Las copias de seguridad incrementales son especialmente útiles para los datos que cambian con frecuencia. Por ejemplo, supongamos que realiza una copia de seguridad completa todos los sábados por la noche. Tiene algunas bibliotecas que se utilizan con mucha frecuencia y, por lo tanto, es necesario realizar la copia de seguridad de éstas con más frecuencia, más de una vez por semana. Puede utilizar copias de seguridad incrementales las otras noches de la semana en lugar de realizar una copia de seguridad completa para capturarlas. Con ello reducirá la duración de las copias de seguridad y, al mismo tiempo, garantizará que se dispone de una copia de seguridad de la última versión de esas bibliotecas.

### **Datos de seguridad y datos de configuración**

También puede reducir las interrupciones planificadas aislando determinados tipos de datos y realizando a continuación la copia de seguridad de éstos por separado. Los datos de seguridad incluyen los perfiles de usuario, las listas de autorización y los propietarios de las autorizaciones. Los datos de configuración incluyen información acerca de la configuración del servidor, como por ejemplo, descripciones de líneas, descripciones de los dispositivos y listas de configuración. Estos tipos de datos se guardan cuando se realiza una copia de seguridad completa del sistema, pero también puede guardarlos por separado sin tener que concluir el servidor. Para obtener información detallada acerca de la realización de la copia de seguridad de estos tipos de datos, consulte Guardar manualmente partes del servidor.

### **Omisión de determinados elementos**

También puede reducir la duración de las copias de seguridad reduciendo el número de objetos que deben guardarse o evitando que los objetos se guarden más de una vez. Para ello, puede optar por omitir determinados objetos de una copia de seguridad. Por ejemplo, supongamos que desea guardar todas las bibliotecas de usuario a excepción de las bibliotecas temporales. Puede optar por omitir todas las bibliotecas temporales de la copia de seguridad, lo que reducirá la duración del proceso de copia de seguridad. La mayoría de los mandatos que puede utilizar para guardar el servidor ofrecen la opción de omitir determinada información de la copia de seguridad. Para obtener información detallada acerca de estos mandatos, consulte Mandatos para guardar partes del servidor y Mandatos para guardar tipos de objetos específicos. Para omitir información de una copia de seguridad, también puede utilizar el programa BRMS (Backup, Recovery and Media Services).

## **Reducir las interrupciones planificadas: Reducción de la duración del mantenimiento y de las actualizaciones de software**

Una forma de garantizar la continua disponibilidad del servidor consiste en mantener el software actualizado. Para este proceso se necesita tiempo y una planificación. La finalidad de este tema es ofrecer una descripción de los métodos que pueden utilizarse para mantener la disponibilidad del servidor mediante la gestión de los arreglos y la instalación de nuevos releases.

### **Gestión de los arreglos**

Para reducir el tiempo durante el cual el servidor no está disponible, debe asegurarse de contar con una buena estrategia de gestión de arreglos. Si está informado acerca de los arreglos disponibles y los instala de forma habitual, tendrá menos problemas. Asegúrese de aplicar arreglos con la frecuencia que haya determinado que es la más adecuada para las necesidades de su empresa. Para obtener información acerca de las recomendaciones para la creación de una estrategia de gestión de arreglos, consulte Planificación de la estrategia de gestión de arreglos.

Los arreglos individuales pueden **postergarse** o **realizarse inmediatamente**. Los arreglos que se postergan pueden cargarse y aplicarse en dos pasos distintos. Pueden cargarse mientras el servidor está en ejecución y aplicarse la próxima vez que se reinicia el servidor. Con los arreglos inmediatos no es necesario reiniciar el servidor para que éstos entren en vigor, con lo que se evita el tiempo de inactividad. Los arreglos inmediatos pueden tener pasos de activación adicionales que se describen en la información que acompaña al arreglo. Para obtener más información acerca de la aplicación de los arreglos, consulte Instalación de arreglos.

### **Instalación de nuevos releases**

Cuando se instala una nueva versión de OS/400, debe apagarse el servidor. Para minimizar la cantidad de tiempo que se necesita para realizar una actualización del software, es importante planificar la instalación cuidadosamente. Para obtener más información acerca del proceso de planificación, consulte Planificación de la instalación del release de OS/400. Para obtener una lista de comprobación de los pasos de la planificación, consulte Planificación del servidor: Software.

## **Reducir las interrupciones planificadas: Reducción de la duración del mantenimiento y de las actualizaciones de hardware**

A veces, es necesario realizar tareas de mantenimiento rutinarias en el hardware o bien incrementar la capacidad de éste. Estas operaciones pueden interrumpir la ejecución de las tareas habituales de la empresa. No obstante, con una planificación, podrá reducir en gran medida, o incluso eliminar, algunas de estas interrupciones.

Si está realizando una actualización del sistema, asegúrese de realizar una planificación detallada antes de empezar. Cuanto más detallada sea la planificación para el nuevo servidor, más rápida será la actualización. Para obtener información más detallada acerca del proceso de planificación, consulte Actualizaciones.

## Mantenimiento simultáneo

El **mantenimiento simultáneo** es una característica del servidor iSeries que permite que un representante del servicio técnico pueda reparar o sustituir determinados componentes de hardware mientras el servidor realiza sus operaciones normales. Si debe sustituir o actualizar un posible componente, podrá hacerlo sin interrumpir sus tareas habituales.

## Actualización de la capacidad según demanda

Con el método de actualización de la capacidad según demanda, puede activar procesadores adicionales y pagar sólo la nueva capacidad de proceso a medida que crezcan sus necesidades. Puede incrementar su capacidad de proceso sin interrumpir ninguna de las operaciones actuales.

El método de actualización de la capacidad según demanda para iSeries es una característica que ofrece la posibilidad de activar, sin realizar interrupciones, uno o más procesadores centrales del servidor. Este método agrega capacidad de un procesador en incrementos, hasta alcanzarse el número máximo de procesadores. En espera que el modelo pueda incorporar. El método de actualización de la capacidad según demanda aporta un importante valor a las instalaciones en las que se desea realizar actualizaciones sin interrupciones.

Para obtener más información acerca del método de actualización de la capacidad según demanda, consulte Capacity Upgrade on Demand



---

## Disponibilidad para varios servidores: Clústeres

La principal estrategia de disponibilidad para un entorno de varios sistemas es la utilización de clústeres. Un **clúster** es una colección o un grupo de varios servidores iSeries que funcionan conjuntamente como si se tratara de un único servidor. Si su empresa necesita alta disponibilidad o una disponibilidad continuada, debe considerar la posibilidad de utilizar clústeres.

Los servidores de un clúster funcionan en colaboración para proporcionar una única solución de sistemas. En un clúster puede tener hasta 128 servidores. Esto le ofrece la posibilidad de agrupar con eficacia los servidores iSeries con el fin de establecer un entorno que le proporcionará una disponibilidad cercana al 100 por ciento para las operaciones y los datos más importantes. Ello le ayudará a garantizar que los servidores y las aplicaciones más importantes estarán siempre disponibles. Los clústeres también le ofrecen una gestión de sistemas simplificada y mayor escalabilidad para poder incorporar nuevos componentes progresivamente a medida que crece la empresa.

Aunque las ventajas de los clústeres son numerosas, su coste es significativo. Debe comparar el coste de esta solución con el coste del tiempo de inactividad del servidor para determinar si debe implementar o no la utilización de clústeres en su empresa. Para obtener información acerca de cómo determinar el coste del tiempo de inactividad en la empresa, consulte Estimar el valor de la disponibilidad.

Si opta por utilizar clústeres en su entorno, es importante considerar los tipos de aplicaciones que utiliza. Existen algunas aplicaciones que se han diseñado para hacer frente a algunos de los efectos de una anomalía. Para obtener más información acerca de estas aplicaciones, consulte "Programas altamente disponibles" en la página 19.

Para obtener más información acerca de los clústeres, incluido su funcionamiento y su implementación en la empresa, consulte Clústeres. Para obtener más información acerca de los clústeres en el contexto de

otras soluciones de alta disponibilidad, consulte High Availability and Clusters



## Programas altamente disponibles

Las aplicaciones y los datos son muy importantes para su empresa. Si utiliza clústeres, puede utilizar programas que ofrezcan posibilidad de recuperación ante una interrupción en el sistema. Puede diseñar personalmente estas aplicaciones, pero también puede adquirir aplicaciones que satisfagan los criterios necesarios. Si desea diseñar los programas personalmente, deberá entender qué es un programa con posibilidad de recuperación y cuáles son los niveles de disponibilidad de la aplicación. Para obtener más información acerca de estos temas, consulte Aplicaciones para clústeres.

Si adquiere las aplicaciones, también puede estar seguro de que son altamente disponibles. ClusterProven<sup>(R)</sup> es una marca de IBM que identifica estos tipos de aplicación. Una aplicación que sea ClusterProven para iSeries sigue ofreciendo disponibilidad en caso de producirse una interrupción (planificada o no planificada). Para obtener más información acerca de los criterios que deben satisfacer estos programas y una lista de los programas que son ClusterProven, consulte High Availability and Clusters



---

## Información relacionada con la disponibilidad

En la lista siguiente se indican los manuales de iSeries, los IBM Redbooks<sup>(TM)</sup> (en formato PDF) y los sitios web relacionados con la disponibilidad. Puede ver o imprimir cualquiera de los documentos en formato PDF.

### Temas del Information Center

- Copia de seguridad y recuperación
- Clústeres
- Control de las confirmaciones
- Gestión de discos
- Gestión del registro por diario
- Particiones lógicas
- Soluciones de almacenamiento

### Manuales

- Copia de seguridad y recuperación



- Servicios de copia de seguridad, recuperación y medios para iSeries



### Redbooks

- Roadmap to Availability on the iSeries 400



- High Availability on the AS/400 System: A System Manager's Guide



- The System Administrator's Companion to AS/400 Availability and Recovery



- Clustering and IASPs for Higher Availability



- Striving for Optimal Journal Performance on DB2 Universal Database for iSeries



- AS/400 Remote Journal Function for High Availability and Data Replication



### Sitios web

- High Availability and Clusters



- Backup, Recovery and Media Services



- IBM Business Continuity and Recovery Services



- IT Cost of Downtime Calculator



- Logical Partitioning



- Performance Capabilities Reference



- Tape and Optical Storage



Para guardar un archivo PDF en la estación de trabajo para su visualización o impresión:

1. En el navegador, abra el PDF (pulse el enlace anterior).
2. En el menú del navegador, pulse **Archivo**.
3. Pulse **Guardar como...**
4. Localice el directorio en el que desea guardar el PDF.
5. Pulse **Guardar**.

Si necesita el programa Adobe Acrobat Reader para ver o imprimir estos archivos PDF, puede bajar una copia desde el sitio web de Adobe ([www.adobe.com/prodindex/acrobat/readstep.html](http://www.adobe.com/prodindex/acrobat/readstep.html))









Impreso en España