



# UF1895: Auditorías y continuidad de negocio

**Certificado de Profesionalidad**

*IFCT0510 - Gestión de sistemas informáticos*



IFCT0510 > MF0485\_3 > UF1895

**ic** editorial

**Joaquín Pintos Fernández**

**Auditorías y continuidad de  
negocio.  
IFCT0510**

Joaquín Pintos Fernández

**ic** editorial

**Auditorías y continuidad de negocio. IFCT0510**  
**Autor: Joaquín Pintos Fernández**

1ª Edición

© IC Editorial, 2014

Editado por: IC Editorial

C.I.F.: B-92.041.839

c/ Cueva de Viera, 2, Local 3 Centro Negocios CADI

29200 ANTEQUERA, Málaga

Teléfono: 952 70 60 04

Fax: 952 84 55 03

Correo electrónico: [iceditorial@iceditorial.com](mailto:iceditorial@iceditorial.com)

Internet: [www.iceditorial.com](http://www.iceditorial.com)

**IC Editorial** ha puesto el máximo empeño en ofrecer una información completa y precisa. Sin embargo, no asume ninguna responsabilidad derivada de su uso, ni tampoco la violación de patentes ni otros derechos de terceras partes que pudieran ocurrir. Mediante esta publicación se pretende proporcionar unos conocimientos precisos y acreditados sobre el tema tratado. Su venta no supone para **IC Editorial** ninguna forma de asistencia legal, administrativa ni de ningún otro tipo.

Reservados todos los derechos de publicación en cualquier idioma.

Según el Código Penal vigente ninguna parte de este o cualquier otro libro puede ser reproducida, grabada en alguno de los sistemas de almacenamiento existentes o transmitida por cualquier procedimiento, ya sea electrónico, mecánico, reprográfico, magnético o cualquier otro, sin autorización previa y por escrito de IC EDITORIAL; su contenido está protegido por la Ley vigente que establece penas de prisión y/o multas a quienes intencionadamente

reprodujeren o plagiaren, en todo o en parte, una obra literaria, artística o científica.

ISBN: 978-84-16629-06-0

Nota de la editorial: IC Editorial pertenece a Innovación y Cualificación S. L.

## Presentación del manual

El **Certificado de Profesionalidad** es el instrumento de acreditación, en el ámbito de la Administración laboral, de las cualificaciones profesionales del Catálogo Nacional de Cualificaciones Profesionales adquiridas a través de procesos formativos o del proceso de reconocimiento de la experiencia laboral y de vías no formales de formación.

El elemento mínimo acreditable es la **Unidad de Competencia**. La suma de las acreditaciones de las unidades de competencia conforma la acreditación de la competencia general.

Una **Unidad de Competencia** se define como una agrupación de tareas productivas específica que realiza el profesional. Las diferentes unidades de competencia de un certificado de profesionalidad conforman la **Competencia General**, definiendo el conjunto de conocimientos y capacidades que permiten el ejercicio de una actividad profesional determinada.

Cada **Unidad de Competencia** lleva asociado un **Módulo Formativo**, donde se describe la formación necesaria para adquirir esa **Unidad de Competencia**, pudiendo dividirse en **Unidades Formativas**.

El presente manual desarrolla la Unidad Formativa **UF1895: Auditorías y continuidad de negocio**,

perteneciente al Módulo Formativo **MF0485\_3: Administración software de un sistema informático**,

asociado a la unidad de competencia **UC0485\_3: Instalar, configurar y administrar el software de base y de**

**aplicación del sistema,**

del Certificado de Profesionalidad **Gestión de sistemas informáticos.**

# Índice

**Portada**

**Título**

**Copyright**

**Presentación del manual**

**Índice**

**Capítulo 1 Copias de respaldo**

1. Introducción
2. Tipificar los datos según sus necesidades de copia
3. Diferenciar los distintos tipos de copias distinguiendo las diferencias entre copias completas, incrementales, y diferenciales, así como las ventajas e inconvenientes de cada una de ellas, y las combinaciones más habituales de las mismas
4. Establecer correctamente los periodos de retención acordes con las normas de seguridad de la empresa, con las necesidades según el tipo de datos, y con la legislación vigente
5. Dimensionar las copias de seguridad
6. Establecer la política de copias de la organización
7. Proponer los dispositivos de copia y soportes más adecuados en base a las necesidades de la organización
8. Realizar las copias de seguridad según los procedimientos y políticas vigentes en la organización
9. Gestionar el ciclo de vida de los soportes
10. Documentación de planes de recuperación

11. Resumen  
Ejercicios de repaso y autoevaluación

## **Capítulo 2 Legislación vigente**

1. Introducción
2. Conocer las leyes vigentes relacionadas con el tratamiento de datos
3. Enumerar los puntos principales a tener en cuenta
4. Resumen  
Ejercicios de repaso y autoevaluación

## **Capítulo 3 Alternativas a las copias**

1. Introducción
2. Distinguir entre salvaguarda de datos y disponibilidad del servicio
3. Enumerar las alternativas para garantizar la disponibilidad del servicio
4. Indicar ventajas e inconvenientes de las alternativas para garantizar la disponibilidad del servicio sobre las copias de seguridad
5. Resumen  
Ejercicios de repaso y autoevaluación

## **Capítulo 4 Planes de auditoría**

1. Introducción
2. Describir los objetivos de los planes de auditoría
3. Describir el perfil del auditor
4. Auditar el sistema
5. Resumen  
Ejercicios de repaso y autoevaluación

## **Bibliografía**

# Capítulo 1

## Copias de respaldo

### 1. Introducción

La tecnología no está libre de fallos o errores, y las copias de seguridad, *backups* o copias de respaldo se utilizan como medida preventiva contra la pérdida de datos por desastres que puedan ocurrir. Es muy importante clasificar correctamente la información según su importancia para poder optimizar los recursos disponibles para su protección.

Existen varios tipos de copia y es necesario conocerlos para aprovechar sus ventajas. Dependiendo de la importancia y la cantidad de datos modificados se puede decidir qué método o combinación de ellos utilizar. Para esta tarea existen herramientas *hardware* y *software*, algunas incluidas en los sistemas operativos y otras específicas. Hay que concienciar sobre la necesidad de realizar copias de seguridad y confeccionar un plan de copias si se valora el trabajo o la información almacenada en un ordenador. Al igual que es importante deshacerse de forma segura de los datos que ya no son necesarios.

Realizar las copias no es suficiente. También hay que tener todo el proceso bien documentado, verificar que las copias se han realizado correctamente y realizar simulacros de caída del sistema completo para asegurar realmente que se está preparado contra cualquier desastre.

## 2. Tipificar los datos según sus necesidades de copia

Lo más valioso de cualquier negocio son sus datos. Si se estropea el monitor de un equipo, o falla el lector de DVD, o se rompe el procesador se soluciona simplemente sustituyendo la pieza estropeada por otra. Pero si lo que falla es el disco duro el daño puede ser irreversible si no se puede recuperar la información que contiene. Esta es la razón principal por la que es necesario tener una copia de seguridad de la información importante.

Todos los datos que se crean o se mantienen almacenados deben identificarse y organizarse para que cuando se necesite trabajar con ellos se sepa dónde encontrarlos y que la recuperación se pueda realizar de forma eficiente. Clasificar los datos también permite saber qué datos son los más importantes, cómo tratarlos, si son datos de carácter personal, dónde almacenarlos, la cantidad de datos, si deben ser eliminados o por el contrario no pueden serlo.



### **Sabía que...**

---

El mayor riesgo de pérdida de información son los fallos de los sistemas, errores humanos o robos.

---

Hay que salvaguardar todos los datos importantes para la empresa pero dando prioridad a los archivos que son muy difíciles o imposibles de volver a obtener.

### **2.1. Clasificación de la información**

Una clasificación correcta de la información ayuda a evitar la pérdida de datos. Es muy importante conocer lo críticos que son los datos que se manejan y establecer una correcta clasificación. Se pueden clasificar según su importancia, posibilidades de recuperación o confidencialidad.

Clasificar la información aporta una serie de beneficios, los más importantes son:

- Demuestra un compromiso para proteger la información.
- Permite identificar la información que es más sensible y la que es más importante.
- Permite garantizar la confidencialidad, integridad y disponibilidad de la información que se utiliza, se genera o almacena.



### **Sabía que...**

---

No existe una única forma de clasificar los datos: se puede utilizar un criterio determinado o varios simultáneamente.

---

Existen muchos criterios de clasificación, pero atendiendo a criterios de confidencialidad la información se pueden clasificar como:

- No clasificada. A esta información puede acceder todo el mundo.
- Sensible, pero no clasificada. Es información secreta pero de poca importancia.
- Confidencial. Es una información de uso exclusivo para el fin proporcionado.

- **Secreta.** Información que es de uso exclusivo de la empresa.



### Recuerde

---

Ante la duda de si un archivo es importante o no, mejor incluirlo en la copia de seguridad.

---

Entre los criterios de clasificación, algunos de los más utilizados son:

- **Valor.** Consiste en asignarle un valor a cada tipo de información relacionado con la importancia de esos datos para la empresa.
- **Temporalidad.** En casos en que la información va perdiendo valor con el paso del tiempo.
- **Vida útil.** En casos donde la información antigua queda obsoleta al ser reemplazada por la nueva información.
- **De carácter personal.** Por ley, toda la información personal debe ser clasificada.



### Recuerde

---

La decisión final sobre qué datos incluir en una copia de seguridad se toma en función de lo críticos que son y su valor para la empresa.

---

## 2.2. Clasificación de roles

Todas las personas que trabajan con información deben asumir su responsabilidad al manejar y tener acceso a los datos. Se puede establecer una clasificación de los roles de las personas que trabajan con información y asignarles una serie de responsabilidades.

Las responsabilidades que debe asumir el dueño de la información son:

- Es el primero que tiene que determinar el nivel de clasificación de los datos.
- De forma periódica debe revisar la clasificación asignada y modificarla en caso de que sea necesario.
- Delegar la responsabilidad de protección a la persona que custodia la información.

Entre las responsabilidades de las personas que custodian la información se pueden destacar:

- Ejecución de procedimientos de respaldo de la información y verificación.
- Ejecución de procesos de recuperación de la información en caso de ser necesario.
- Mantenimiento de registros conformes a la clasificación de la información.
- Impedir que personas no autorizadas accedan a la información.



### **Importante**

---

Desde el primero que crea los datos hasta el último que accede a ellos todos tienen su parte de responsabilidad sobre la información que manejan.

---

Los usuarios de los datos también tienen responsabilidades a la hora de trabajar con los datos. Las responsabilidades de los usuarios son:

- Deben seguir los procesos de operación definidos por la empresa.
- Deben preservar la seguridad de la información durante la realización de su trabajo.
- Deben utilizar los recursos de la empresa exclusivamente para los propósitos de la misma.



### **Recuerde**

---

Los datos deben estar a salvo, es una necesidad.

---



### **Actividades**

---

1. Piense en la información que guarda en su ordenador y qué pasaría si desapareciera mañana. ¿Cuál sería la información más valiosa para usted? ¿Por qué?
  2. Reflexione sobre si la información que contiene su ordenador es igual de importante para usted que para cualquier otra persona. Razone su respuesta.
  3. Realice una clasificación de la información contenida en su ordenador.
- 



### **Aplicación práctica**

---

**Usted ha sido contratado en una nueva empresa y se le asigna un ordenador para que trabaje. El equipo ya había sido usado por un empleado anterior y le piden que antes de empezar a trabajar recopile y clasifique la información que encuentre en el equipo que sea de interés para la empresa.**

**Los datos encontrados son:**

- **Correos personales y correos de clientes.**
- **Fotos personales del antiguo empleado.**
- **Archivos de música y videos no relacionados con la empresa.**
- **Archivo con nombres de usuario y claves para acceder a servicios de la empresa.**
- **Documentos sobre la forma de trabajar elaborados por el trabajador anterior.**
- **Registros de copias de seguridad realizadas.**
- **Documento con tareas pendientes del empleado anterior.**

## **SOLUCIÓN**

Los correos personales no son relevantes pero sí lo son los correos de clientes para contestar a sus preguntas y darles el soporte merecido. Las fotos personales se pueden borrar, al igual que la música y las películas, que suponen un gasto de espacio innecesario. El archivo con claves es muy importante, ya que perderlo puede suponer perder el acceso a otros servicios. Los documentos sobre la metodología utilizada por el antiguo empleado pueden ser muy útiles. Los registros de las copias de seguridad realizadas hay que guardarlo y continuarlos. El documento con tareas pendientes

también es importante para terminar tareas iniciadas sin completar.

---

### **3. Diferenciar los distintos tipos de copias distinguiendo las diferencias entre copias completas, incrementales, y diferenciales, así como las ventajas e inconvenientes de cada una de ellas, y las combinaciones más habituales de las mismas**

La tecnología no está libre de errores, y las copias de seguridad son la solución empleada en caso de que se produzcan fallos.

La compra de dispositivos para tener redundancia de datos o sustituir los dispositivos averiados no es caro si se tiene en cuenta que protegen la información que podría ser muy difícil y cara de recuperar o incluso irrecoverable de otro modo. Además, en caso de fallo se podría recuperar la información inmediatamente sin tener que recurrir a ayuda técnica especializada que supone un gasto económico importante, además de que el servicio suele tardar bastante.

La pérdida de los datos de la empresa puede causar importantes daños e incluso suponer el cierre de esta. Algunos efectos negativos para la empresa cuando se produce una pérdida de datos son:

- Imposibilidad de realizar el trabajo por no poder acceder a los datos necesarios para el funcionamiento de la empresa.
- Pérdidas económicas por la pérdida de los datos que pueden ser de clientes o de trabajos ya realizados.
- Pérdida de tiempo por trabajos ya completados que hay que volver a empezar.
- Pérdidas económicas por el tiempo de inactividad hasta que se recupere el sistema.
- Quejas y pérdida de confianza de los clientes.

La realización de copias de seguridad es un elemento de seguridad pasivo. Es una medida que se realiza para, una vez que se ha producido un desastre, minimizar los problemas y restablecer los sistemas lo antes posible.

Se pueden distinguir varios tipos de copias de seguridad o *backups*. Los más comunes son:

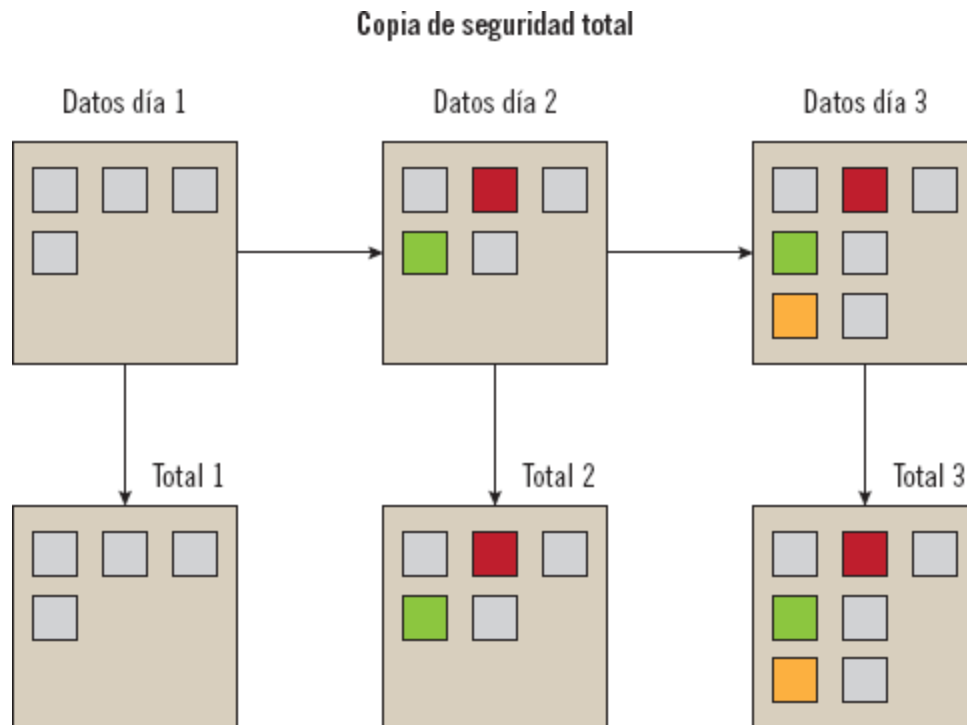
- Copia total o completa.
- Copia incremental.
- Copia diferencial.

Estos tipos de copia se pueden utilizar de forma combinada para obtener los mejores resultados en cuanto a capacidad de almacenamiento y rapidez. Dependiendo del caso la mejor solución será uno u otro método.

### **3.1. Copia de seguridad total o completa**

Consiste en hacer una copia de todos los archivos seleccionados. Es una copia normal de los archivos que se quieren incluir en el *backup*. Cuando se realiza una copia total se pone a 0 el bit de modificación de todos los archivos copiados para indicar que el archivo no se ha modificado

desde la última copia de seguridad. Cuando un archivo se modifica, el bit de modificación de ese archivo se pone a 1. Este bit de modificación es importante cuando se realiza una copia de seguridad incremental o diferencial.



La ventaja de este tipo de copia es que es el más fácil de restaurar. Para restaurarla solo es necesario disponer de la última copia de seguridad realizada.

El principal inconveniente de este tipo de copia es que ocupa mayor espacio, ya que en cada copia se realiza una copia completa de todos los archivos.



### **Sabía que...**

A veces se habla de copia de seguridad parcial. Una copia de seguridad parcial es como una copia total donde solo se incluye una parte de los datos.



## Aplicación práctica

---

**Una pequeña empresa cuenta con un ordenador para almacenar toda la información sobre su negocio, incluidos datos de los clientes, trabajos realizados y contabilidad de la empresa. Un día el único disco duro del equipo se rompe y deja de funcionar.**

**Analice el daño y el impacto que sufre la empresa por esta pérdida.**

### **SOLUCIÓN**

No se puede confiar la parte más importante de una empresa al sistema de almacenamiento de un ordenador al que no se le ha prestado la suficiente atención en cuanto a su *hardware* y *software*.

En este caso los daños *hardware* no son muy grandes económicamente: un disco duro puede ser sustituido por otro rápidamente, pero no así el sistema operativo y todos los programas instalados. Pero lo más importante y en este caso irremplazable si no hay copia de seguridad son los datos guardados en el disco. Incluso aunque la información pudiera ser recuperada, el proceso es caro y no es inmediato, sino que en el mejor de los casos habría que esperar días.

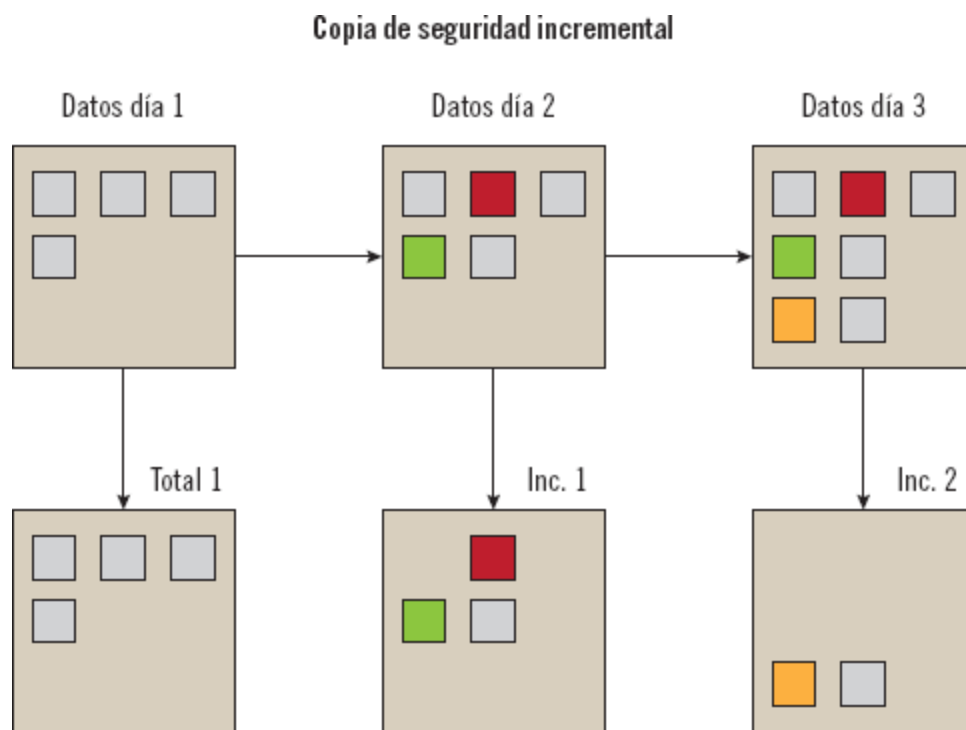
La pérdida de información provoca graves daños a la empresa:

- Pérdida de cartera de clientes.
- Pérdida de oportunidades de negocio.

- Clientes insatisfechos.
- Pérdida de reputación.
- Pérdida de tiempo y dinero.

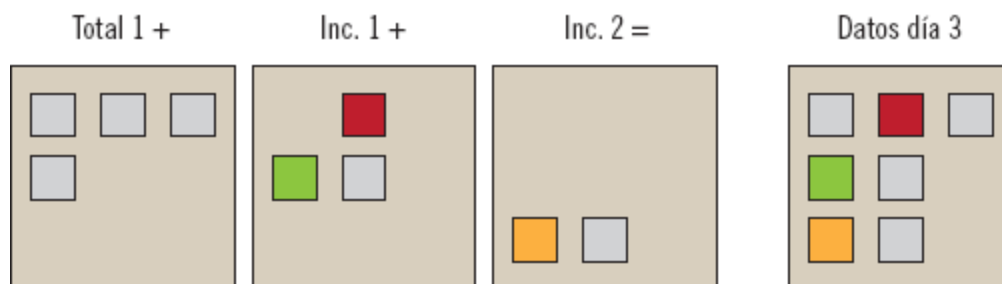
## 3.2. Copia de seguridad incremental

Se hace una copia solo de los archivos que han sido modificados desde la última copia de seguridad incremental o completa. Los archivos que han variado tienen el bit de modificación activado a 1. Cuando se realiza la copia los bits de modificación de los archivos se vuelven a poner a 0.



Para realizar una restauración se necesita la última copia completa y todas las copias incrementales posteriores.

### Restauración de copia de seguridad incremental



La ventaja de este tipo de copia es que necesita menos capacidad de almacenamiento y es el más rápido en realizarse. Solo guarda la información que ha sido modificada desde la última copia de seguridad, ya sea completa o incremental.

Su mayor inconveniente es que para realizar una restauración se necesita la última copia completa y todas las copias incrementales realizadas hasta la fecha. Si alguna de las copias incrementales no está o está dañada no se podrán restaurar los datos.



### Aplicación práctica

**Una empresa realiza periódicamente copias de seguridad. Todos los domingos realiza una copia total y los demás días una copia incremental. Le han contratado y el viernes le encargan como tarea restaurar los datos al estado en el que estaban el jueves.**

**Identifique las copias que necesita y los pasos necesarios para completar la tarea.**

**SOLUCIÓN**

Para restaurar los datos se necesitará la copia total inmediatamente anterior, que será la del domingo. Además se necesitarán todas las copias incrementales posteriores, desde el lunes al jueves.

Los pasos necesarios para restaurar los datos son:

- Restablecer la copia total del domingo anterior.
- Restaurar las copias incrementales desde la más antigua a la más actual. Se restauran las copias del lunes, del martes, del miércoles y la del jueves, en ese orden.

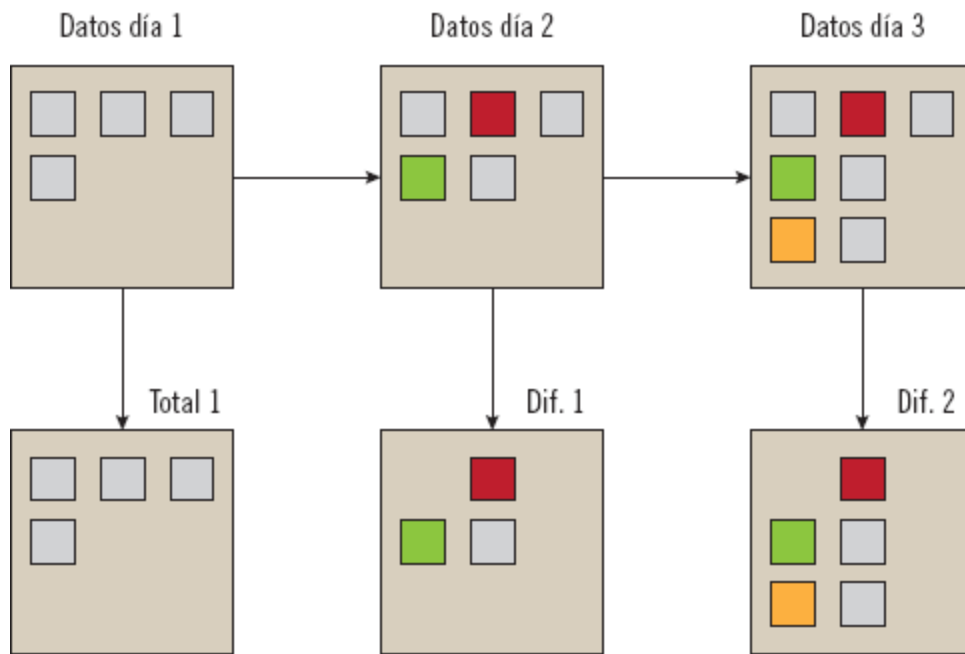
De esta forma ya se tendrán los datos como estaban el jueves.

---

### **3.3. Copia de seguridad diferencial**

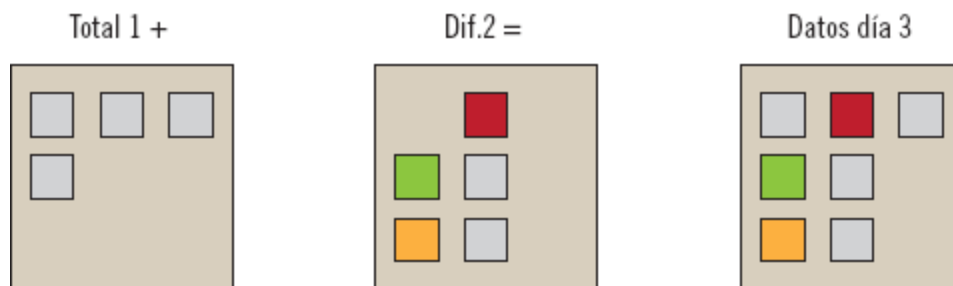
Es igual que la incremental, pero al hacer la copia no se desactivan los bits de modificación a 0, sino que se mantienen activados a 1. Estos bits de modificación solo se desactivarán al realizar una copia de seguridad incremental o completa.

### Copia de seguridad diferencial



Para realizar una restauración se necesita la última copia completa y únicamente la última copia diferencial.

### Restauración de copia de seguridad diferencial



La ventaja de este tipo de copias es que no necesita tanto espacio de almacenamiento como las copias totales y la restauración es más sencilla que la incremental.



**Sabía que...**

Las empresas son las que más recurren a mantener copias de seguridad, pero es una buena práctica también en usuarios particulares.

---

Su desventaja sobre otro tipo de copias es que si los datos cambian mucho las copias diferenciales son cada vez más grandes.

### **3.4. Copias de seguridad combinadas**

Las copias de seguridad incrementales incluirán los archivos modificados desde la última copia total o incremental.

Las copias de seguridad diferenciales incluirán los archivos modificados desde la última copia total o incremental. Los archivos modificados tras las copias diferenciales inmediatamente anteriores son copiados de nuevo en la nueva copia diferencial porque no se desactivan los bits de modificación.