CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERÍAS

DEPARTAMENTO DE CIENCIAS COMPUTACIONALES

UNIVERSIDAD DE GUADALAJARA

Red Universitaria e Institución Benemérita de Jalisco

Seguridad

Sección D04

Profesor: Vazquez Curiel Armida Griselda

20 - 04 - 2024

Autor: Juan Antonio Perez Juarez

Actividad 2.1 Respaldo

Respaldo

Primero debemos definir lo que es un sistema de respaldo.
La copia de seguridad, también llamada respaldo o backup, se refiere a la copia de archivos físicos o virtuales o bases de datos a un sitio secundario para su preservación en caso de falla del equipo u otra catástrofe. El proceso de copia de seguridad de los datos es fundamental para un plan de recuperación de desastres (DRP) exitoso.

¿Qué son el respaldo y la recuperación?
Las empresas hacen una copia de seguridad (respaldo) de los datos que consideran vulnerables en caso de software defectuoso, corrupción de datos, falla de hardware, piratería maliciosa (hacking), error de usuario u otros eventos imprevistos. Las copias de seguridad capturan y sincronizan una instantánea de un punto en el tiempo que luego se usa para devolver los datos a su estado anterior.

Las pruebas de copia de seguridad y recuperación examinan las prácticas y tecnologías de una organización para la seguridad y la replicación de datos. El objetivo es garantizar una recuperación de datos rápida y confiable en caso de que surja la necesidad. El proceso de recuperación de archivos de datos respaldados se conoce como restauración de archivos.

Los términos copia de seguridad de datos y protección de datos a menudo se usan indistintamente, aunque la protección de datos abarca los objetivos más amplios de continuidad empresarial, seguridad de datos, administración del ciclo de vida de la información y prevención de malware y virus informáticos.
Las copias de seguridad y la recuperación de datos implican el proceso de hacer un respaldo de los datos en caso de pérdida y configurar sistemas seguros con los que sea posible recuperar los datos como resultado. El respaldo de datos requiere copiar y archivar los datos de la computadora para que se pueda acceder a estos si se dañan o se eliminan. Sólo puedes recuperar los datos de un momento anterior si has hecho una copia de seguridad con un dispositivo fiable.

La copia de seguridad de datos es una forma de recuperación después de un desastre, por lo que es una pieza esencial de todo plan de recuperación.

La copia de seguridad de los datos no siempre puede restaurar todos los datos y configuraciones del sistema operativo de su empresa. Por ejemplo, los clústeres de computadoras, los servidores de base de datos o los servidores de Active Directory pueden necesitar tipos adicionales de recuperación después de un desastre, ya que es posible que un respaldo y una recuperación no reconstituyan los datos por completo.

Hoy en día, se puede hacer la copia de seguridad de una gran cantidad de datos mediante el almacenamiento en la nube; por lo tanto, no es necesario archivar los datos en el disco duro de un sistema local o en un almacenamiento externo. Además, es posible configurar los dispositivos móviles mediante tecnologías en la nube para permitir la recuperación automática de datos.

La **copia de seguridad en la nube**, también llamada “en línea”, es una estrategia de respaldo de datos que implica el envío de una copia de los datos primarios a través de una red pública o privada a un servidor externo. Generalmente, el servidor se aloja en un proveedor de servicios externo que cobra una tarifa basada en el ancho de banda, la capacidad o la cantidad de usuarios.

La implementación de la copia de seguridad de datos en la nube puede ayudar a reforzar la estrategia de protección de datos de su organización sin agregar carga de trabajo a su personal de TI.

El proceso de respaldo en la nube copia los datos y luego los almacena en diferentes medios o en un sistema de almacenamiento separado que permite un fácil acceso en caso de una situación de recuperación. Entre otras opciones, se encuentran:

Realizar copias de seguridad de los datos directamente en la nube pública. Esto implica escribir los datos directamente en un proveedor de infraestructura en la nube como Amazon Web Services (AWS), Google Cloud, IBM Cloud y Microsoft Azure.

Realizar respaldos de los datos en un proveedor de servicios. Aquí, debe escribir los datos en un proveedor de servicios de nube (CSP, Cloud Service Provider) que ofrece servicios de respaldo en su centro de datos administrado.

La opción de copia de seguridad de nube a nube es para los datos que se encuentran en la nube en aplicaciones de software como servicio (SaaS). Este método copia los datos en otra nube.

Cuando se comienzan a utilizar los servicios de copia de seguridad en la nube, el respaldo inicial puede tardar días en terminar de cargarse a través de la red debido al volumen de datos. Por lo tanto, se utiliza una técnica llamada “propagación en la nube”, con la que un proveedor de copias de seguridad en la nube puede enviarle un dispositivo de almacenamiento, como un cartucho de cinta o una unidad de disco, para hacer la copia de seguridad de sus datos localmente antes de enviar el dispositivo de regreso al CSP. Una vez completada la propagación inicial, el proveedor solo hace una copia de seguridad de sus datos en la red.

Normalmente, los sistemas de respaldo de datos en línea se basan en aplicaciones de software cliente que se ejecutan en un horario determinado por el nivel de servicio adquirido. Si, por ejemplo, contrató un CSP para realizar respaldos diarios, la aplicación recopilará, comprimirá, cifrará y transferirá sus datos al servidor del CSP cada 24 horas. Para reducir el tiempo necesario para completar las transferencias, así como el ancho de banda utilizado, es posible que el CSP sólo proporcione respaldos incrementales después de su primera respaldo completa.

Muchas suscripciones de nube se contratan de forma anual o mensual. Además, ahora los servicios de copias de seguridad en la nube se utilizan comúnmente tanto en las pequeñas y medianas empresas (PYMES) como en las grandes corporaciones. En las grandes empresas y organizaciones, los servicios de copia de seguridad de datos en la nube se utilizan como opción complementaria.

La **diferencia** principal entre el **respaldo y la recuperación** es que la primera es una copia de los datos originales que se pueden utilizar en caso de un error en la base de datos, mientras que la recuperación hace referencia al proceso de restaurar la base de datos a su estado correcto (original) cuando se produce un error.

Como se indicó anteriormente, el respaldo hace referencia a una copia representativa de los datos e incluye elementos esenciales de una base de datos, como archivos de datos y archivos de control. Como los errores

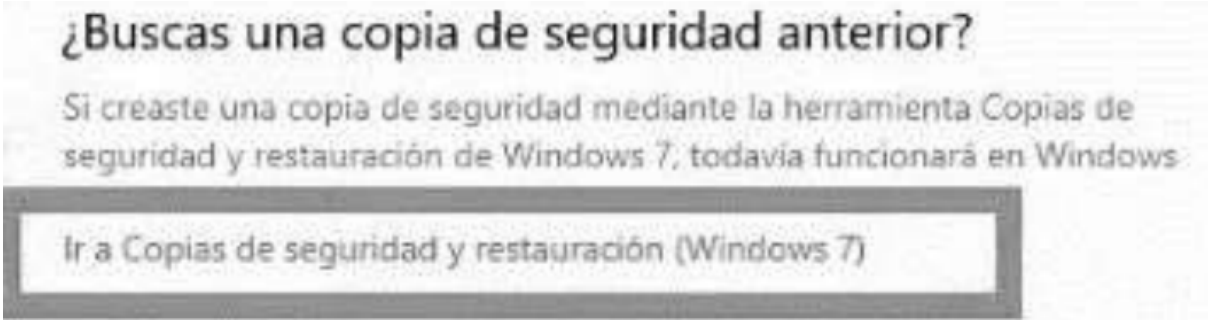
inesperados en la base de datos no se pueden evitar, se requiere un respaldo de toda la base de datos. Existen dos tipos principales de respaldos:

Respaldo físico: Es una copia de los archivos de la base de datos física, como datos, archivos de control, archivos de registro y registros de rehacer archivados. Es una copia de los archivos que almacenan información de la base de datos en otra ubicación y forma la base del mecanismo de recuperación de la base de datos.

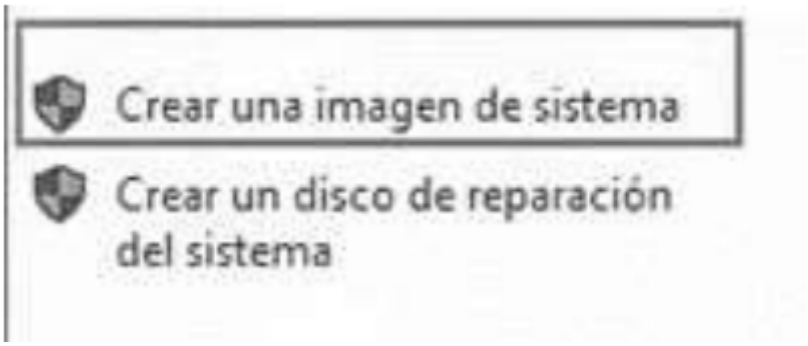
Respaldo lógico: Contiene los datos lógicos que se extraen de una base de datos, y consta de tablas, procedimientos, vistas, funciones, etc. Sin embargo, no se recomienda ni es útil mantener un respaldo lógico por sí solo, ya que solo proporciona información estructural.

La recuperación, por otro lado, ayuda a restaurar la base de datos a su estado correcto en caso de que se produzca un error. Mejora la confiabilidad de la base de datos, ya que permite que la base de datos se recupere a un estado coherente después de un error repentino.

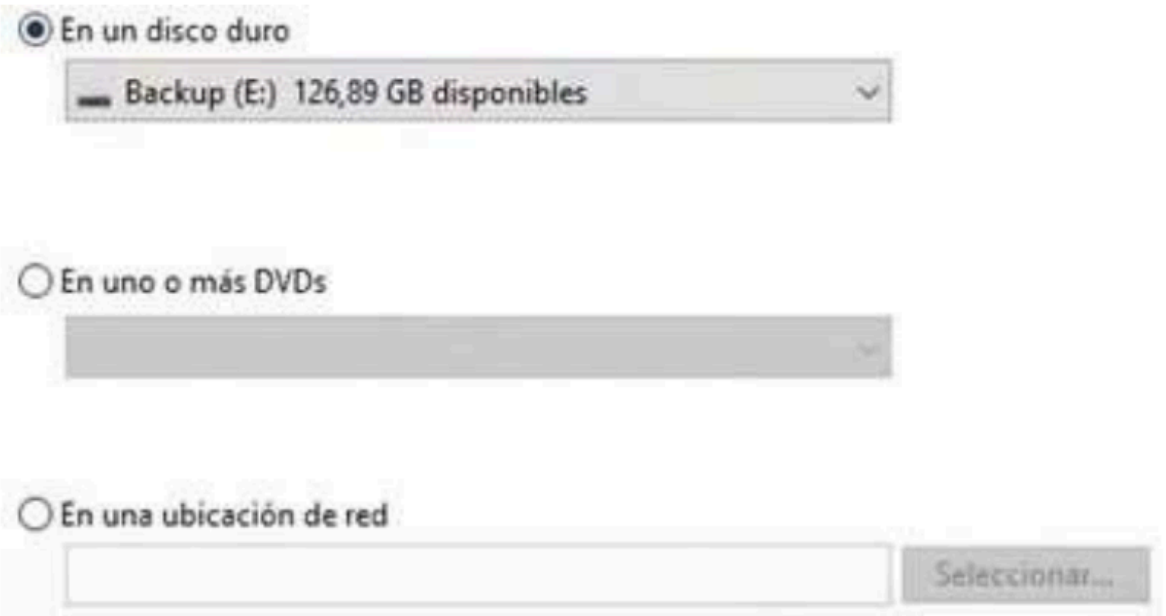
Sistema de respaldo de Windows Windows cuenta con una herramienta de respaldo llamada "Copia de seguridad y restauración" que permite realizar copias de seguridad de los archivos y configuraciones importantes en el sistema. Esta herramienta puede ser accedida desde el Panel de control y se puede programar para realizar copias de seguridad periódicas. Pasos para usar dicha herramienta:
1. Es necesario contar con una unidad con suficiente espacio de almacenamiento para hacer la copia de seguridad, para esto podemos hacer una partición en el mismo disco duro o usar un medio externo.
2. Dirigirse a “Configuración” -> “Actualización y seguridad” -> “Copia de seguridad”
3. Dar click en:



4. Seleccionar la opción:



5.- Elige la opción deseada:



6.- Seleccionar la opción de “Iniciar Copia de Seguridad”

7.- Una vez terminado el proceso, el equipo estaría respaldado.

Pasos para hacer una partición dentro del mismo disco duro donde se encuentra Windows:

1. Presione la tecla Windows + X y seleccione "Administrador de disco" en el menú desplegable.

2. Seleccione el disco duro que desea particionar y haga clic en "Redimensionar volumen".

3. Arrastre la barra del espacio sin asignar hacia la partición que desea reducir.

4. Haga clic en "Nuevo volumen simple" y siga las instrucciones en pantalla para crear una nueva partición.

5. Asigne una letra de unidad y un nombre a la partición.

6. Haga clic en "Finalizar" y espere a que se complete el proceso.

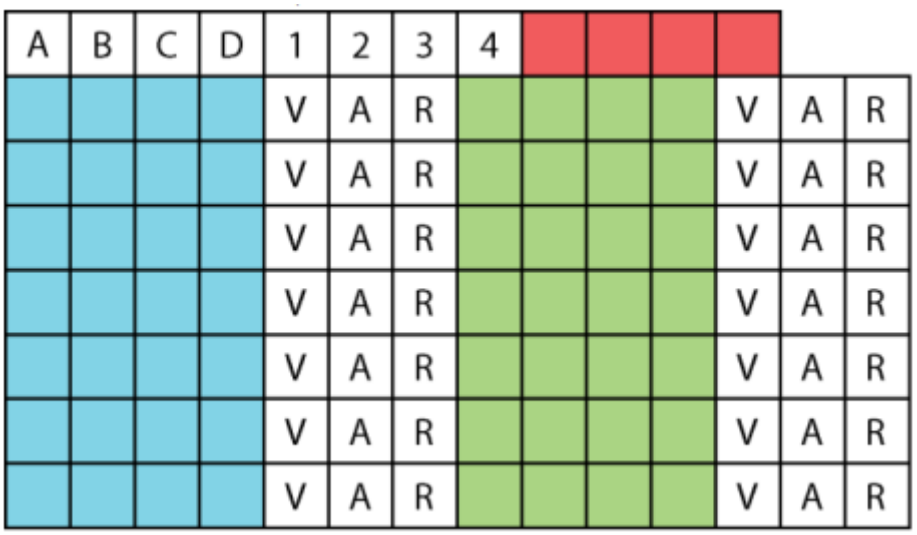
Sistema de respaldo en python (Con encriptación simple)

```python
def backup_folder(src: str, dst: str, password: str):

    # Obtener nombres de carpetas/archivos
    files = get_filenames(src)

    # Archivo de salida
    output = io.BytesIO()

    # Escribir la propia contraseña en el archivo
    output.write(password.encode('utf-8'))

    # Escribir en 4 bytes la cantidad total de archivos
    output.write(struct.pack('I', len(files)))

    for f in files:

        # Nombre del archivo
        # Sin el nombre de la carpeta raiz
        subpath = os.path.relpath(f, src)

        # Escribir en 4 bytes la longitud del nombre del archivo
        output.write(struct.pack('I', len(subpath)))

        # Escribir el nombre del archivo como tal
        output.write(subpath.encode('utf-8'))

        # Escribir la longitud de los datos
        output.write(struct.pack('I', os.path.getsize(f)))

        # Escribir los datos como tal
        input_file = open(f, 'rb')
        output.write(input_file.read())
        input_file.close()

    ### ENCIPTACION ###

    # Crear lista a partir de los bytes escritos
    byte_array = list(output.getvalue())

    # Generar contraseña y encpriptar solo si la proporciona el usuario
    if len(password) != 0:
        # Generar un entero a partir de la contraseña dada
        key = 0
        for c in password:
            key += ord(c)

        # Modificar cada byte, sumandole la llave
        for i in range(len(byte_array)):
            byte_array[i] = (byte_array[i] + key) % 255

    # Escribir el archivo ya encriptado en el disco
    output_file = open(dst, 'wb')
    output_file.write(bytearray(byte_array))
    output_file.close()

    # Mostrar mensaje de exito
    showinfo('Operación exitosa', 'Los archivos han sido respaldados correctamente')
```

Como se menciona en los comentarios del código, el algoritmo toma el nombre de los archivos de manera recursiva y los guarda en una lista.

Posteriormente se crea un objeto de tipo ByteIO, el cual nos permite usarlo como si fuera un archivo.
Escribimos en el archivo al principio la contraseña ingresada por el usuario si es que la proporcionó, posteriormente escribimos en 4 bytes la cantidad total de archivos.

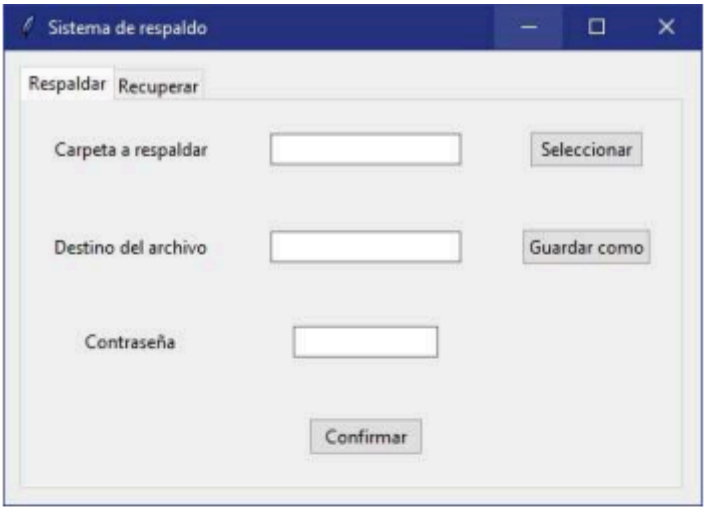
Posteriormente el codigo itera entre cada archivo abriendolo y repitiendo los siguientes pasos para cad uno de ellos:
● A cada directorio se le resta la parte del directorio raiz, por ejemplo: c:/Users/Documents/Prueba/Archivo.png, solo dejamos la parte de: Archivo.png
● Escribimos en 4 bytes, la longitud de la string del nombre del archivo
● Escribimos el nombre del archivo (variable)
● Escribimos en 4 bytes, la longitud de los datos del archivo
● Escribimos los datos del archivo (variable)
En este punto tenemos el archivo de la siguiente manera: (En este ejemplo se está usando como contraseña: ABCD1234)

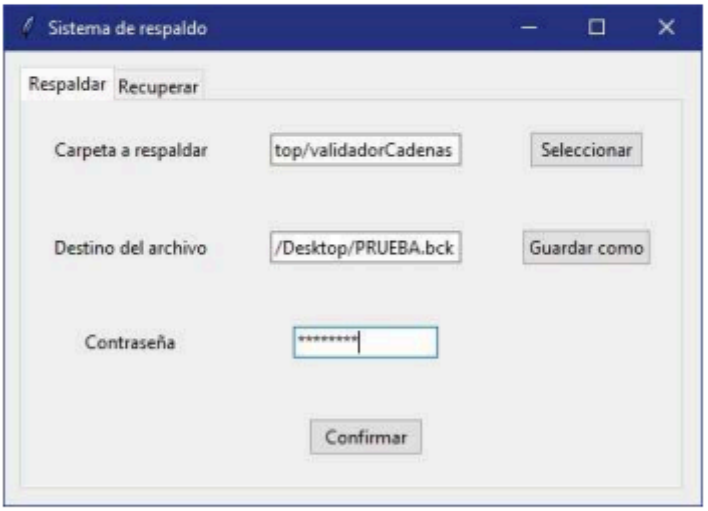


Donde var es tamaño variable y depende de lo que indiquen los enteros.

Encriptación
Para encriptar los archivos básicamente se suma cada valor ascii de la contraseña proporcionada y se guarda en un número, digamos que se genera el número 540, este número se le sumará a cada byte de archivo, modificandolo completamente, sin embargo, esto es reversible restando el mismo valor en el algoritmo de recuperación. Finalmente se escribe el archivo en el disco

Demostración de uso:





Conclusiones:

Tener un sistema de respaldo de información es fundamental en el mundo digital actual. Es como un salvavidas que puede rescatar nuestros datos en situaciones críticas. Si bien es cierto que los fallos técnicos y los errores humanos son inevitables, el impacto que pueden tener en nuestros datos puede ser catastrófico si no contamos con un respaldo adecuado.

La conclusión es clara: la pérdida de datos puede ocasionar consecuencias graves, como la interrupción de operaciones comerciales, la pérdida de la confianza del cliente, la violación de la privacidad y, en casos extremos, el

cierre de empresas. Por lo tanto, tener un sistema de respaldo de información efectivo no solo es importante, sino que es esencial para garantizar la continuidad del negocio y proteger la integridad de los datos. Es una inversión en la seguridad y estabilidad de cualquier organización o individuo en el mundo digital.
Una de las historias más trágicas que ejemplifica la importancia de tener un sistema de respaldo de información ocurrió en el año 2008, cuando la empresa de alojamiento web "ThePlanet" experimentó un incendio en su centro de datos en Houston, Texas. Este incendio causó una interrupción masiva en los servicios de alojamiento, afectando a miles de sitios web y empresas que dependían de ellos.

En este caso, muchos de los servidores y sistemas de almacenamiento de datos fueron destruidos por el fuego, lo que resultó en la pérdida total de la información almacenada en ellos. Muchas empresas que alojaban sus sitios web y bases de datos en ThePlanet no tenían un sistema de respaldo adecuado o no lo mantenían actualizado, lo que significaba que perdieron datos críticos de sus operaciones comerciales.

Las consecuencias de este incidente fueron devastadoras para muchas empresas. Muchas de ellas sufrieron pérdidas financieras significativas debido a la interrupción en sus servicios, la pérdida de datos importantes y la necesidad de reconstruir sus sistemas desde cero. Algunas empresas incluso se vieron obligadas a cerrar debido a la imposibilidad de recuperarse de esta pérdida.

Este caso sirve como un recordatorio sombrío de la importancia de tener un sistema de respaldo de información sólido y actualizado. La pérdida de datos puede ocurrir en cualquier momento debido a una variedad de razones, y estar preparado con copias de seguridad puede marcar la diferencia entre la supervivencia y el fracaso en el mundo digital.

Referencias:
Rouse, M. (2018, 28 septiembre). Copia de seguridad o respaldo. ComputerWeekly.es. https://www.computerweekly.com/es/definicion/Copia-de-seguridad-o-respaldo#:~:text=La%20copia%20de%20seguridad%2C%20tambi%C3%A9n,del%20equipo%20u%20otra%20cat%C3%A1strofe.

Technologies, V. (s. f.). Backup and Recovery of Data: The Essential Guide. https://www.veritas.com/es/mx/information-center/data-backup-and-recovery