

## Plan de Copias de Seguridad

1. Evaluación de Requerimientos y Análisis de Riesgos		
Datos Críticos:	Frecuencia de Cambio:	Análisis de Riesgos:
Información de clientes, detalles de eventos, información de pagos, direcciones entre otros.	Variables dependiendo de la actividad del servicio.	Pérdida de datos debido a errores humanos, corrupción de archivos o fallas de hardware podría resultar en pérdida de ingresos, daño a la reputación y violación de regulaciones sanitarias.
2. Establecimiento de Objetivos de Nivel de Servicio (SLA)		
RPO:		RTO:
<ul style="list-style-type: none"> <li>Máximo 24 horas después de la pérdida de datos.</li> </ul>		<ul style="list-style-type: none"> <li>Recuperación en menos de 4 horas.</li> </ul>
3. Selección del Tipo de Copia de Seguridad		
Tipo de Copia:		
<ul style="list-style-type: none"> <li>Copias de seguridad completas lógicas (logs) de la base de datos.</li> <li>Copias de seguridad incrementales lógicas (logs) para cambios recientes en la base de datos.</li> </ul>		
4. Planificación de la Frecuencia y el Horario		
Horario de Copias de Seguridad:		
<ul style="list-style-type: none"> <li>Cada día a las 2:00 AM durante la semana laboral (incrementales).</li> <li>Todos los Domingos a las 3:00 AM al cierre de la semana (completa).</li> </ul>		
5. Estrategia de Almacenamiento		
Ubicación de Almacenamiento:		Medidas de Redundancia:
<ul style="list-style-type: none"> <li>Almacenamiento local en un servidor dedicado para acceso rápido.</li> </ul>		<ul style="list-style-type: none"> <li>Almacenamiento en la nube por medio de GitHub para redundancia y seguridad adicional.</li> </ul>
6. Seguridad y Encriptación		
Medidas de Seguridad:		
<ul style="list-style-type: none"> <li>Encriptación AES-256 de las copias de seguridad almacenadas localmente y en la nube.</li> <li>Se utilizará una contraseña segura para las copias.</li> </ul>		
7. Automatización		
Herramientas Utilizadas:		
<ul style="list-style-type: none"> <li>Uso de herramientas de respaldo basado en Scripts personalizados (.bat) para automatizar el proceso.</li> <li>Monitorización automática para alertar sobre fallos en las copias de seguridad (Programador de tareas).</li> <li>7Zip para la encriptación y comprimido de las copias así como su desencriptación al momento de la restauración.</li> </ul>		

- *Git y github para el control de versiones y almacenamiento en la nube de las copias de seguridad*

### 8. Pruebas y Validación

#### Programa de Pruebas:

- *Pruebas regulares de restauración de datos para garantizar la integridad y la eficacia de las copias de seguridad.*
- *Pruebas mensuales de recuperación para evaluar el tiempo necesario para restaurar los datos.*

### 9. Documentación y Procedimientos de Recuperación

#### Documentación Detallada:

- *Manual de procedimientos de recuperación con instrucciones paso a paso.*

#### Capacitación:

- *Se dará una sesión para el personal sobre los procedimientos de recuperación de datos y en caso de haber cambios en los procedimientos se volverá a capacitar.*

### 10. Revisión y Actualización Regular

#### Programa de Revisión:

- *Revisión trimestral para incorporar cambios en el sistema y en los requisitos del negocio.*
- *Actualización del plan de copias de seguridad según las nuevas tecnologías y mejores prácticas de seguridad.*

## Manual de Procedimiento para Copias de Seguridad en Bases de Datos

### 1. Objetivo




- Garantizar la integridad y disponibilidad de los datos del servicio de buffet para la aplicación web foodster esto mediante la realización regular de copias de seguridad automatizadas de la base de datos **foodster**.

### 2. Preparación

- Revisión de la Base de Datos: Verificar la integridad de la base de datos (que existe) y la disponibilidad de los datos a respaldar (que tiene datos).
- Validar que tenemos instalado 7zip y está configurado en el path del sistema (Variable de entorno) para que la encriptación de copias se realice correctamente.
- Configurar git con su usuario adecuado globalmente.
- Verificar que tenemos acceso al repositorio remoto.
- Comprobamos que el usuario de copias inicie correctamente sesión en mysql.
- Comprobar las variables de los scripts y al repositorio remoto que apuntan.
- Programación de la Copia de Seguridad: Configurar la automatización de las copias de seguridad mediante los scripts bat y programación de tareas.

### 3. Proceso de Copia de Seguridad

- **1. Identificar scripts:** Tenemos dos tipos de copias las incrementales y las completas cada una con su script dedicado

 backup_completo.bat	11/04/2024 11:25 a. m.	Archivo por lotes ...	2 KB
 backup_incremental.bat	11/04/2024 11:24 a. m.	Archivo por lotes ...	2 KB
 backup_completo.bat	11/04/2024 10:21 a. m.	Archivo por lotes ...	1 KB

- **2. Acceso a la Herramienta de Copia de Seguridad:** Los scripts utilizan `mysqldump`, una herramienta de línea de comandos que viene con MySQL, para realizar la copia de seguridad de la base de datos. También utilizan `7z` para cifrar la copia de seguridad y `git` para guardar en un repositorio.

```
C:\Users\prac.des5>mysqldump
Usage: mysqldump [OPTIONS] database [tables]
OR      mysqldump [OPTIONS] --databases [OPTIONS] DB1 [DB2 DB3...]
OR      mysqldump [OPTIONS] --all-databases [OPTIONS]
For more options, use mysqldump --help

C:\Users\prac.des5>7z

7-Zip 24.04 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-04-05

Usage: 7z <command> [<switches>...] <archive_name> [<file_names>...] [@listfile]
<Commands>
```

- **3. Selección de Datos para la Copia:** Los scripts realizan una copia de seguridad de la base de datos especificada en la variable `base\_datos`.

```
@echo off
setlocal

REM Variables
set usuario=copias
set password=zWxDCqEX1kPto9B
set host=localhost
set port=33060
set ruta_backup=C:\CopiasBD\Completa
set ruta_git=C:\CopiasBD\
set base_datos=foodster
```

- **4. Configuración de la copia:** Las variables al principio del script establecen los parámetros de la copia de seguridad. `usuario` y `password` son las credenciales para acceder a la base de datos. `host` y `port` especifican dónde se encuentra la base de datos. `ruta backup` es la ubicación donde se guardará la copia de seguridad. `ruta git` es la ubicación del repositorio Git.

```
REM Variables
set usuario=copias
set password=zWxDCqEX1kPto9B
set host=localhost
set port=33060
set ruta_backup=C:\CopiasBD\Completa
set ruta_git=C:\CopiasBD\
set base_datos=foodster
```

- **5. Ejecución de la Copia de Seguridad:** Los scripts crean una carpeta para la copia de seguridad si no existe, obtienen la fecha y hora actuales, y luego ejecutar `mysqldump` para realizar la copia de seguridad de la base de datos. Luego cifra la copia de seguridad con `7z` y la guarda en la carpeta especificada. Después de eso, elimina la copia de seguridad sin cifrar.

```
C:\Users\prac.des5>C:\Users\prac.des5\Downloads\backup_completo.bat
mysqldump: [Warning] Using a password on the command line interface can be insecure.

7-Zip 24.04 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-04-05

Scanning the drive:
1 file, 65748957 bytes (63 MiB)

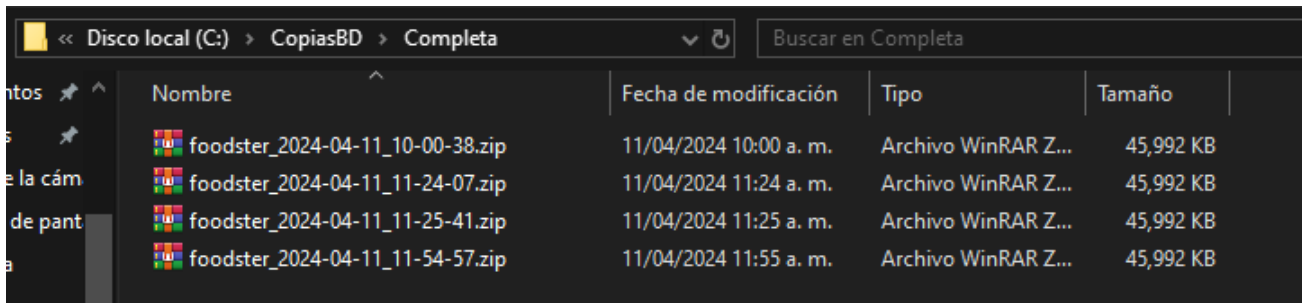
Creating archive: C:\CopiasBD\Completa\foodster_2024-04-11_11-54-57.zip





Add new data to archive: 1 file, 65748957 bytes (63 MiB)

Files read from disk: 1
Archive size: 47095081 bytes (45 MiB)
Everything is Ok
[main 1f3ae89] fecha=2024-04-11
  1 file changed, 0 insertions(+), 0 deletions(-)
  create mode 100644 Completa/foodster_2024-04-11_11-54-57.zip
Enumerating objects: 6, done.
Counting objects: 100% (6/6), done.
Delta compression using up to 16 threads
Compressing objects: 100% (4/4), done.
Writing objects: 100% (4/4), 44.93 MiB | 1.22 MiB/s, done.
Total 4 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), completed with 1 local object.
To https://github.com/CristianRdz/copiasSeguridadFoodster.git
   d0b3d58..1f3ae89  main -> main

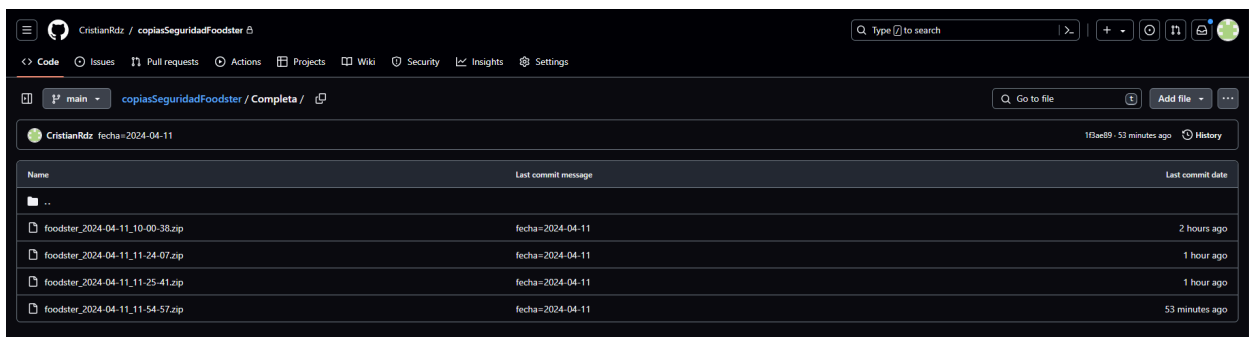
C:\Users\prac.des5>
```

- **6. Verificación:** El script no verifica automáticamente que la copia de seguridad se haya realizado correctamente. Deberías verificar manualmente que el archivo cifrado de la copia de seguridad esté en la ubicación especificada y que puedas descomprimirlo y acceder a los datos.



« Disco local (C:) > CopiasBD > Completa		Buscar en Completa		
	Nombre	Fecha de modificación	Tipo	Tamaño
	 foodster_2024-04-11_10-00-38.zip	11/04/2024 10:00 a. m.	Archivo WinRAR Z...	45,992 KB
	 foodster_2024-04-11_11-24-07.zip	11/04/2024 11:24 a. m.	Archivo WinRAR Z...	45,992 KB
	 foodster_2024-04-11_11-25-41.zip	11/04/2024 11:25 a. m.	Archivo WinRAR Z...	45,992 KB
	 foodster_2024-04-11_11-54-57.zip	11/04/2024 11:55 a. m.	Archivo WinRAR Z...	45,992 KB

- **7. Guardado en Git:** Si la carpeta especificada en `ruta git` no contiene un repositorio Git, el script inicializa uno, agrega todos los archivos, realiza un commit con la fecha y hora actuales como mensaje, y luego hacer push al repositorio remoto especificado. Si la ruta ya contiene un repositorio Git, simplemente agrega todos los archivos, realiza un commit y hace push.



#### 4. Almacenamiento de la Copia de Seguridad

- **Localización:** Las copias de seguridad se almacenarán en una ubicación local y se subirán a un repositorio de GitHub.
- **Protección de Datos:** Se implementarán medidas de seguridad para proteger las copias de seguridad, como el cifrado de archivos y la restricción de acceso al repositorio de github.

#### 5. Registro y Documentación

- **Registro de Actividades:** Mantener un registro de las actividades de copia de seguridad, incluyendo fechas, horarios, y resultados.
- **Revisión Periódica:** Revisar periódicamente los registros de actividades para garantizar la integridad de las copias de seguridad y realizar ajustes según sea necesario.

#### 6. Pruebas y Validación

- Realizar pruebas regulares de restauración de datos para validar la efectividad del proceso de copia de seguridad y garantizar la disponibilidad de los datos en caso de necesidad.

## Procedimientos de Restauración de Base de Datos

### 1. Objetivo



- Restaurar la base de datos **foodster** a partir de una copia de seguridad previamente realizada, asegurando la integridad y disponibilidad de los datos.

### 2. Preparación


- Revisión de copia, validar que copia necesitamos basándonos en la hora y fecha que fue generada
- Validar que tenemos instalado 7zip y está configurado en el path del sistema (Variable de entorno) para que la encriptación de copias se realice correctamente.
- Comprobamos que el usuario de copias inicie correctamente sesión en mysql.
- Comprobar las variables de los scripts.

### 3. Proceso de Copia de Seguridad

- Acceso al Sistema:** Iniciar sesión en el sistema de gestión de bases de datos en MySQL.
- Identificar scripts:** Tenemos dos tipos de copias las incrementales y las completas cada una con su script dedicado

 restablecer_incremental.bat	11/04/2024 11:01 a. m.	Archivo por lotes ...	1 KB
 restablecer_completo.bat	11/04/2024 11:00 a. m.	Archivo por lotes ...	1 KB

- Selección de la Copia de Seguridad:** Seleccionar la copia de seguridad adecuada para la restauración colocándola en el script, identificándose por su nomenclatura de fecha y hora.

 foodster_2024-04-11_11-54-57.zip	11/04/2024 11:55 a. m.	Archivo WinRAR Z...	45,992 KB
--	------------------------	---------------------	-----------

```
set fecha_hora=2024-04-11_10-00-38
```

- Configuración de Restauración:** Configurar los parámetros de restauración, en el caso de que el servidor mysql se encuentre en un contenedor de docker colocar el id el contenedor, nombre de la base de datos destino y la ubicación de las copias de seguridad.

```
REM Variables
set usuario=copias
set password=zWxDCqEX1kPto9B
set host=localhost
set port=33060
set ruta_backup=C:\CopiasBD\Completa
set base_datos=foodster
set fecha_hora=2024-04-11_10-00-38
set docker_container_id=e7afc2b203c5
```

- **Inicio del Proceso de Restauración:** Ejecutar el script de restauración para comenzar el proceso de restauración.

```
C:\Users\prac.des5>C:\Users\prac.des5\Downloads\restablecer_completo.bat

7-Zip 24.04 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-04-05

Scanning the drive for archives:
1 file, 47095081 bytes (45 MiB)

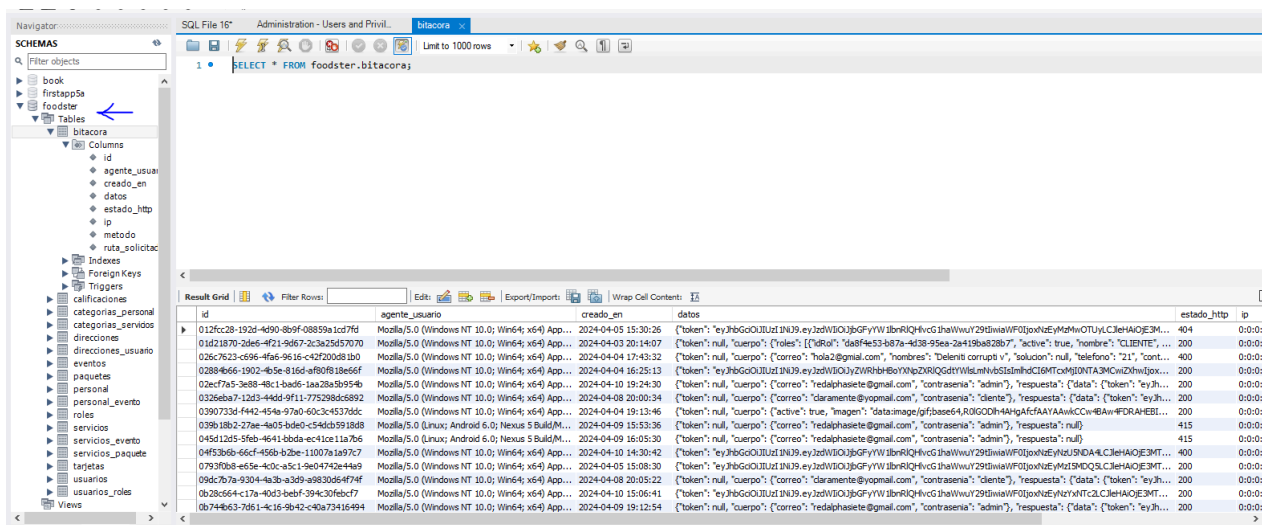
Extracting archive: C:\CopiasBD\Completa\foodster_2024-04-11_10-00-38.zip
--
Path = C:\CopiasBD\Completa\foodster_2024-04-11_10-00-38.zip
Type = zip
Physical Size = 47095081

Everything is Ok

Size:          65748957
Compressed: 47095081
"mysql" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.
mysql: [Warning] Using a password on the command line interface can be insecure.

C:\Users\prac.des5>
```

- **Verificación Post-Restauración:** Verificar que la restauración se haya completado correctamente y que los datos estén disponibles y consistentes.



Navigation: Administration - Users and Privileges - bitacora

SELECT \* FROM foodster.bitacora;

id	agente_usuario	creado_en	datos	estado_http	ip
012f2c28-192d-4d90-8b9f-08899a1cd7fd	Mozilla/5.0 (Windows NT 10.0; Win64; x64; App...	2024-04-05 15:30:26	("token": "eyJ3bG90LWludlIN39.eyJzdWI0OjBpGfYyW1bRlRlQHVhVGVzWVwV29lbnVlWF0jbnVlZyM2MmVOTUyLClleHAQGE3M...	404	0:0:0
01d21870-2d6e-4f21-9d67-2c3a25d57070	Mozilla/5.0 (Windows NT 10.0; Win64; x64; App...	2024-04-03 20:14:07	("token": null, "cuerpo": {"roles": [{"rol": "da8f4e53-b87a-4d38-95ea-2a419ba828b7", "active": true, "nombre": "CLIENTE", ...	200	0:0:0
026c7623-c696-4fa6-9616-c42f200d81b0	Mozilla/5.0 (Windows NT 10.0; Win64; x64; App...	2024-04-04 17:43:32	("token": null, "cuerpo": {"correo": "hola2@gmail.com", "nombres": "Delente corrupta v", "solucion": null, "telefono": "21", "cont...	400	0:0:0
02884b66-1902-4b5e-816d-af80f818e6df	Mozilla/5.0 (Windows NT 10.0; Win64; x64; App...	2024-04-04 16:25:13	("token": "eyJ3bG90LWludlIN39.eyJzdWI0OjBpGfYyW1bRlRlQHVhVGVzWVwV29lbnVlWF0jbnVlZyM2MmVOTUyLClleHAQGE3M...	200	0:0:0
02e7f745-9d88-4b0c-b0d6-aa2ba9b9f94b	Mozilla/5.0 (Windows NT 10.0; Win64; x64; App...	2024-04-10 19:24:30	("token": null, "cuerpo": {"correo": "redaphasiete@gmail.com", "contrasena": "admin", "respuesta": {"data": {"token": "eyJ3h...	200	0:0:0
0326ba7f-12d3-44d4-9f11-775298dc6892	Mozilla/5.0 (Windows NT 10.0; Win64; x64; App...	2024-04-08 20:00:34	("token": null, "cuerpo": {"correo": "daranente@gmail.com", "contrasena": "cliente", "respuesta": {"data": {"token": "eyJ3h...	200	0:0:0
0390733d-4442-454a-97a0-60c3c4537d6c	Mozilla/5.0 (Windows NT 10.0; Win64; x64; App...	2024-04-04 19:13:46	("token": null, "cuerpo": {"active": true, "imagen": "data:image/png;base64,R0lGODdhAHgAfAAYAAwKCCwBAAwFDRABEEL...	200	0:0:0
039b18b2-27ae-4a0c-bde0-c546db5918d8	Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/M...	2024-04-09 15:53:36	("token": null, "cuerpo": {"correo": "redaphasiete@gmail.com", "contrasena": "admin", "respuesta": null})	415	0:0:0
045d12d5-5feb-4641-bbda-ec41ce11a7b6	Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/M...	2024-04-09 16:05:30	("token": null, "cuerpo": {"correo": "redaphasiete@gmail.com", "contrasena": "admin", "respuesta": null})	415	0:0:0
04f53b6b-66cf-456b-b2be-11007a1a9c7c	Mozilla/5.0 (Windows NT 10.0; Win64; x64; App...	2024-04-10 14:30:42	("token": "eyJ3bG90LWludlIN39.eyJzdWI0OjBpGfYyW1bRlRlQHVhVGVzWVwV29lbnVlWF0jbnVlZyM2MmVOTUyLClleHAQGE3M...	400	0:0:0
0793f0b8-e65e-40c0-85c1-9e04742e4469	Mozilla/5.0 (Windows NT 10.0; Win64; x64; App...	2024-04-05 15:08:30	("token": "eyJ3bG90LWludlIN39.eyJzdWI0OjBpGfYyW1bRlRlQHVhVGVzWVwV29lbnVlWF0jbnVlZyM2MmVOTUyLClleHAQGE3M...	200	0:0:0
09d07b79-0204-4a3b-a3b9-a98306e47f4f	Mozilla/5.0 (Windows NT 10.0; Win64; x64; App...	2024-04-08 20:05:22	("token": null, "cuerpo": {"correo": "daranente@gmail.com", "contrasena": "cliente", "respuesta": {"data": {"token": "eyJ3h...	200	0:0:0
0b28c664-c17a-40d3-bedf-394c30fbc77	Mozilla/5.0 (Windows NT 10.0; Win64; x64; App...	2024-04-10 15:06:41	("token": "eyJ3bG90LWludlIN39.eyJzdWI0OjBpGfYyW1bRlRlQHVhVGVzWVwV29lbnVlWF0jbnVlZyM2MmVOTUyLClleHAQGE3M...	200	0:0:0
0b74d663-7d51-4c16-9b42-c40a73416494	Mozilla/5.0 (Windows NT 10.0; Win64; x64; App...	2024-04-09 19:12:54	("token": null, "cuerpo": {"correo": "redaphasiete@gmail.com", "contrasena": "admin", "respuesta": {"data": {"token": "eyJ3h...	200	0:0:0



#### 4. Procedimientos de Emergencia

- **Errores durante la Restauración:** En caso de errores durante el proceso de restauración, detener el proceso y analizar el registro de errores para identificar y solucionar el problema.
- **Escalación de Problemas:** Si se presentan problemas graves que no pueden ser resueltos internamente, contactar al soporte técnico o a un especialista en bases de datos para asistencia.
- **Error de Creación:** En caso de que describa un error de que la base de datos no existe, crearla ya se mediante línea de comandos o MySQL Workbench

Error:

```
mysql: [Warning] Using a password on the command line interf  
ERROR 1049 (42000): Unknown database 'foodster'
```

Solución:



#### 5. Registro y Documentación

- **Documentar el Proceso:** Registrar todos los pasos realizados durante el proceso de restauración, incluyendo fechas, horarios, y acciones tomadas.
- **Revisión de Datos Restaurados:** Realizar una revisión de los datos restaurados para asegurar su integridad y precisión.

#### 6. Pruebas Finales

- **Pruebas de Funcionamiento:** Realizar pruebas de funcionamiento en la base de datos restaurada para verificar que todas las funcionalidades estén operativas.
- **Validación de Datos:** Verificar la consistencia y exactitud de los datos restaurados mediante pruebas y comparaciones con los datos originales.

## Manual de Procedimientos para Pruebas y Validación de Copias de Seguridad en Bases de Datos

### 1. Objetivo

- Validar la efectividad y confiabilidad de las copias de seguridad de la base de datos **foodster** mediante pruebas y procedimientos de validación.

### 2. Procedimiento de Pruebas

- **Restauración de la Copia de Seguridad:** Restaurar la copia de seguridad en un entorno de pruebas utilizando los scripts correspondientes.
- **Verificación de Integridad de Datos:** Se deben verificar que los datos restaurados sean idénticos a los datos originales de la copia completa más próxima posible, es decir cumplen con la estructura planeada en las fases de diseño del modelado de datos y son coherentes, asegurando la integridad y consistencia de la información.
- **Pruebas de Funcionalidad:** Realizar pruebas funcionales en la base de datos restaurada mediante la ejecución de consultas, procesos dentro de la aplicación y demás actividades que requieran el uso de base de datos, esto con el objetivo de validar que no se hayan perdido datos o funcionalidades.

### 3. Validación

1. **Revisión de Registros:** Revisar los registros de pruebas y restauración para verificar que se hayan seguido todos los procedimientos correctamente y que no haya errores.
2. **Comparación de Rendimiento:** Comparar el rendimiento de la base de datos restaurada con el rendimiento de la base de datos original para detectar posibles discrepancias o problemas de rendimiento.

### 4. Documentación

- **Registro de pruebas:** Documentar todos los resultados de las pruebas realizadas, incluyendo cualquier problema encontrado y las acciones tomadas para resolverlo.
- **Evaluación de Proceso:** Evaluar el proceso de pruebas y validación para identificar áreas de mejora y optimización en el proceso de copias de seguridad.

### 5. Procedimientos de Emergencia

- **Escalación de Problemas:** En caso de problemas graves durante las pruebas o la restauración, contactar al equipo de soporte técnico o a un especialista en bases de datos para asistencia inmediata.

### 6. Revisión y Actualización del Plan de Copias de Seguridad

- **Ajustes Basados en Pruebas:** Realizar ajustes en el plan de copias de seguridad basados en los resultados de las pruebas y validación.
- **Evaluación Periódica:** Realizar evaluaciones periódicas del plan de copias de seguridad y del proceso de pruebas para garantizar su eficacia y relevancia continua.

## Política de Copias de Seguridad

### 1. Objetivo

- El objetivo de esta política es garantizar la disponibilidad, integridad y confidencialidad de la información almacenada en la base de datos **foodster** mediante la implementación de procedimientos adecuados de copias de seguridad y restauración.

### 2. Alcance

- **Administradores de bases de datos:** responsables de notificar cualquier error o inconsistencia detectada en los datos respaldados.
- **Equipo de auditoría interna:** encargado de realizar auditorías periódicas para verificar el cumplimiento de las políticas de copias de seguridad.
- **Equipo de recuperación de desastres:** encargado de desarrollar y mantener planes de recuperación de desastres para la base de datos.
- **Control de cambios:** responsable de gestionar y controlar todos los cambios en los procesos, políticas y procedimientos relacionados con las copias de seguridad.

### 3. Procedimientos

- **Frecuencia de Copias de Seguridad:** Se realizarán copias incrementales diariamente a las 2:00 a.m., y copias completas los días domingo a las 3:00 a.m.
- **Tipo de copias de seguridad:** Se implementará una combinación de copias completas e incrementales.
- **Ubicación:** Las copias de seguridad se almacenarán de forma local y en github para garantizar la disponibilidad y seguridad de los datos.
- **Capacidad de Recuperación:** Se establecerán procedimientos claros para la restauración de datos, priorizando las copias locales en caso de pérdida o corrupción de datos no afecte al servidor, y las copias en la nube en caso de desastres que impacten al servidor.

### 4. Recuperación y Restauración

- **Procedimientos:** Se establecerán procedimientos detallados para la recuperación y restauración de datos en caso de pérdida o corrupción, garantizando tiempos de recuperación mínimos (RTO) y pérdida mínima de datos (RPO).
- **Descarga de las Últimas Actualizaciones del Repositorio de GitHub:** Acceder al repositorio de GitHub y utilizar el comando `git pull` para obtener las últimas actualizaciones.
- **Preparación de la Base de Datos para la Restauración:** Verificar la disponibilidad de una copia de seguridad completa antes de proceder con la restauración.
- **Restauración de la Base de Datos:** Utilizar las herramientas adecuadas para restaurar la base de datos desde la copia de seguridad.

- **Verificación de la Restauración:** Verificar la integridad y correcta recuperación de tablas, registros y relaciones.

### 5. Revisiones y Auditorías

- **Evaluación del Plan de Copias de Seguridad:** Revisar periódicamente el plan para asegurar su vigencia y eficacia.
- **Análisis de Procedimientos Actuales:** Identificar áreas de mejora en los procedimientos de copias de seguridad.
- **Actualización de documentación:** Mantener actualizada la documentación relacionada con el plan y los procedimientos.
- **Pruebas de Restauración:** Realizar pruebas regulares de restauración para verificar la efectividad de los procedimientos.

### 6. Capacitación y Concienciación

- **Planificación de la Formación:** Establecer fechas y horarios convenientes para la capacitación del personal.
- **Contenido de la Formación:** Cubrir los fundamentos de la gestión de copias de seguridad, incluyendo procedimientos de respaldo y restauración.
- **Demostraciones Prácticas:** Realizar demostraciones prácticas para reforzar el aprendizaje.
- **Actualización de Conocimientos:** Informar sobre las últimas tendencias y tecnologías en gestión de copias de seguridad.

### 7. Incumplimiento y Sanciones

- El incumplimiento de esta política será sujeto a medidas disciplinarias, que pueden incluir desde advertencias hasta acciones legales dependiendo de la gravedad del incumplimiento y las consecuencias para la organización.
- En caso de incumplimiento, se requerirá que la persona reciba capacitación adicional sobre políticas de seguridad de datos y procedimientos de copias de seguridad, si el incumplimiento se debe a falta de conocimiento o habilidades.

## Registro de Cambios

Fecha	Autor	Descripción del Cambio	Razón del Cambio	Efecto en el plan
2024-03-27	Luis Eduardo Bahena Castillo	Actualización de la frecuencia de las copias completas e incrementales	Aumento de volumen de datos	Incremento en copias diarias para incrementales y completas los domingos
2024-04-01	Luis Eduardo Bahena Castillo	Primer Incidencia Registrada	Registro de la primera incidencia en la base de datos	Reescribir los archivos bat para la automatización de las copias de seguridad
2024-04-04	Luis Eduardo Bahena Castillo y Oscar Miguel Barrios Tecorral	Actualización de la política de copias de seguridad	Garantía de los datos para realizar pruebas periódicas	Realizar pruebas periódicas en la base de datos
2024-04-05	Luis Eduardo Bahena Castillo	Actualización de la política de copias de seguridad	Cambio de horarios	Provee mejor capacidad de disponibilidad
2024-04-11	Cristian Rodriguez Rodriguez	Se añadieron los manuales con imágenes y más detalles	Estaba mal detallado lo anterior	Reescribir parte de los archivos bat para la automatización de las copias de seguridad para que se puedan subir copias a github y asegurarse que se encriptan correctamente
2024-04-11	Luis Eduardo Bahena Castillo	Actualización de los Anexos desde Revisiones y Auditorías	Faltaba definir la revisión de la auditoría	Definir lo que fue la auditoría y planes de mejora

## Reportes de Incidentes

<b>1. Información General</b>
<ul style="list-style-type: none"><li>○ <b>Fecha del Incidente:</b> Lunes 01 de Abril del 2024</li><li>○ <b>Hora del Incidente:</b> 18:45 hrs</li><li>○ <b>Reportado por:</b> Luis Eduardo Bahena Castillo</li></ul>
<b>2. Descripción del Incidente</b>
<ul style="list-style-type: none"><li>○ <b>Tipo de Incidente:</b> Falla de Software</li><li>○ <b>Detalle del Incidente:</b> Hubo un error en el archivo automatizado donde no dejaba crear copias de seguridad</li></ul>
<b>3. Impacto</b>
<ul style="list-style-type: none"><li>● <b>Sistemas Afectados:</b> Archivo .bat automatizado</li><li>● <b>Severidad del Incidente:</b> Baja</li><li>● <b>Datos Comprometidos:</b> Ninguna pérdida de datos</li></ul>
<b>4. Respuesta Inicial</b>
<ul style="list-style-type: none"><li>● <b>Acciones Tomadas:</b> Se optó por modificar el archivo con los cambios correspondientes</li><li>● <b>Persona(s) Responsable(s) de la Respuesta:</b> Luis Eduardo Bahena Castillo</li></ul>
<b>5. Análisis y Resolución</b>
<ul style="list-style-type: none"><li>○ <b>Causa Raíz del Incidente:</b> Error al generar copias de seguridad completa e incremental</li><li>○ <b>Resolución:</b> Se modificó los archivos bat con las variables correspondientes</li><li>○ <b>Tiempo de Resolución:</b> 1 día</li></ul>
<b>6. Lecciones Aprendidas y Medidas Correctivas</b>
<ul style="list-style-type: none"><li>○ <b>Lecciones Aprendidas:</b> Al momento de crear un archivo bat, asegurar que las variables estén correctamente para generar las copias de seguridad (credenciales, ubicación del archivo, etc.)</li><li>○ <b>Acciones Correctivas Propuestas:</b> Guardar en la nube los archivos bat por si se llegan a eliminar las tareas automatizadas</li></ul>
<b>7. Aprobación y Cierre</b>
<ul style="list-style-type: none"><li>○ <b>Aprobado por:</b> Cristian Rodríguez Rodríguez</li><li>○ <b>Fecha de Cierre:</b> Jueves 04 de Abril del 2024</li></ul>

## Revisiones y Auditorías

### 1. Información de la Revisión/Auditoría

- **Fecha de la Revisión/Auditoría:** Viernes 5 de Abril del 2024
- **Realizado por:** Maximiliano Carsi Castrejón

### 2. Alcance de la Revisión/Auditoría

- **Aspectos Revisados:** Procedimientos de Copias de Seguridad, Planificación de Frecuencia y Horario, Estrategia de Almacenamiento, Seguridad y Encriptación.
- **Objetivo de la Revisión/Auditoría:** Evaluar la efectividad y cumplimiento de los procedimientos de copias de seguridad para garantizar la disponibilidad y seguridad de los datos críticos.

### 3. Metodología

- **Herramientas y Técnicas Utilizadas:** Análisis de Documentación, Entrevistas con el Equipo de Administración de Bases de Datos, Revisión de Registros de Actividades.

### 4. Hallazgos

- **Cumplimiento de Políticas:** Se observó un alto grado de cumplimiento con las políticas establecidas, sin embargo, se identificaron algunas áreas de mejora.
- **Eficiencia del Proceso:** El proceso de copias de seguridad demostró ser eficiente en la mayoría de los casos, pero se detectaron algunos cuellos de botella en la planificación y ejecución.
- **Problemas Identificados:** Falta de documentación detallada sobre la estrategia de almacenamiento y redundancia, así como algunas debilidades en las medidas de seguridad y encriptación.

### 5. Recomendaciones

- **Mejoras Sugieras:** Mejorar la documentación de la estrategia de almacenamiento, reforzar las medidas de seguridad y encriptación, y optimizar la planificación de la frecuencia y el horario de las copias de seguridad.
- **Plan de Acción:** Desarrollar procedimientos actualizados para la estrategia de almacenamiento, implementar controles adicionales de seguridad y realizar ajustes en la planificación de las copias de seguridad.

### 6. Seguimiento

- **Acciones de Seguimiento:** Programar sesiones de capacitación adicionales para el personal relevante, revisar y actualizar los procedimientos de copias de seguridad de acuerdo con las recomendaciones.
- **Fecha de Seguimiento Programada:** Viernes 12 de Febrero del 2024

### 7. Aprobación y Documentación

- **Aprobado por:** Cristian Rodríguez Rodríguez
- **Documentación Adjunta:** Informe completo de la Revisión/Auditoría, registros de actividades, y cualquier evidencia recopilada durante el proceso de revisión.

## Formación y Concienciación

### 1. Objetivo de la Capacitación

- **Propósito:** El objetivo de la capacitación y concienciación es garantizar que todos los empleados comprendan la importancia de las copias de seguridad y estén familiarizados con los procedimientos adecuados para su realización y recuperación en caso de necesidad.

### 2. Programa de Formación

- **Temas a Cubrir:**
  - Procedimientos de copia de seguridad.
  - Seguridad de datos y encriptación.
  - Restauración de datos.
- **Metodología de Enseñanza:** Sesiones interactivas, presentaciones multimedia, demostraciones prácticas y estudios de caso.

### 3. Audiencia Objetivo

- **Grupos de Empleados:**
  - *Administradores de bases de datos.*
  - *Personal de TI responsable de la gestión de datos.*
  - *Departamento de Seguridad de la Información.*

### 4. Calendario de Formación

- **Fechas y Horarios:**
  - *Sesiones de capacitación planificadas durante todo el mes de mayo de 2024.*
  - *Horarios flexibles para permitir la participación de todos los empleados relevantes.*

### 5. Material de Apoyo

- **Recursos:**
  - *Guías detalladas sobre procedimientos de copia de seguridad.*
  - *Manuales de seguridad de datos y encriptación.*
  - *Videos tutoriales sobre restauración de datos.*

### 6. Evaluación y Retroalimentación

- **Evaluación de Competencias:**
  - *Pruebas de conocimientos al final de cada sesión de formación.*
  - *Evaluaciones prácticas para demostrar la competencia en los procedimientos de copia de seguridad. Métodos para evaluar la comprensión y competencia de los empleados.*
- **Retroalimentación:** Encuestas de satisfacción al final de cada sesión para recopilar opiniones y sugerencias para mejorar la calidad de la formación.



## 7. Seguimiento y Actualización

- **Programa de Reciclaje:**
  - *Sesiones de actualización programadas cada seis meses para mantener a los empleados informados sobre cambios en los procedimientos y mejores prácticas.*
  - *Actualizaciones periódicas del material de formación para reflejar las últimas tendencias y tecnologías en copias de seguridad y seguridad de datos.*

## 8. Registro y Documentación

- **Asistencia y Participación:**
  - *Mantenimiento de un registro de asistencia y participación para cada sesión de formación.*
  - *Documentación detallada de los resultados de las evaluaciones de competencias y retroalimentación de los empleados para referencia futura y seguimiento del progreso.*

## Planes de Mejora

### 1. Identificación de Áreas de Mejora

- **Aspectos a Mejorar:**
  - Velocidad de copia de seguridad.
  - Automatización de procesos de copia y restauración.
  - Mejoras en la seguridad de datos.
  - Eficiencia en la gestión del almacenamiento de copias de seguridad.

### 2. Análisis de Causa Raíz

- **Investigación:** Se llevará a cabo un análisis detallado de cada área identificada para determinar las causas fundamentales de los problemas, como la infraestructura subyacente, los procesos actuales y las limitaciones de recursos.

### 3. Propuestas de Mejora

- **Soluciones Sugeridas:**
  - *Implementación de un sistema de almacenamiento de alto rendimiento para acelerar las operaciones de copia de seguridad.*
  - *Desarrollo y despliegue de scripts de automatización más avanzados para simplificar y agilizar los procesos de copia y restauración.*
  - *Mejora de las políticas de seguridad de datos, incluyendo la encriptación mejorada y la gestión de accesos.*
  - *Evaluación y optimización de la estrategia de almacenamiento para reducir la duplicación de datos y mejorar la eficiencia del espacio.*
- **Beneficios Esperados:**
  - *Reducción significativa en el tiempo necesario para completar las copias de seguridad.*
  - *Mayor confiabilidad y consistencia en los procesos de copia y restauración.*
  - *Mejora en la protección de datos sensibles mediante medidas de seguridad reforzadas.*
  - *Optimización del uso del espacio de almacenamiento y reducción de costos asociados.*
  - *Enumerar los beneficios anticipados de implementar las mejoras.*

### 4. Planificación de Implementación

- **Cronograma:** Se establecerá un cronograma detallado que incluya las fechas de inicio y finalización de cada fase de implementación.
- **Recursos Necesarios:** Se asignan recursos humanos y tecnológicos adecuados para llevar a cabo las mejoras planificadas, incluyendo personal de TI, herramientas de software y equipos de seguridad.

### 5. Evaluación de Impacto

- **Métricas de Éxito:** Se establecerán métricas específicas para medir el impacto de las mejoras, como el tiempo de copia y restauración, la tasa de éxito de las operaciones y la satisfacción del usuario.
- **Revisión y Ajustes:**
  - **Evaluación Continua:** Se realizarán revisiones periódicas del plan de mejora para evaluar su efectividad y realizar ajustes según sea necesario.
  - **Ajustes:** Se establecerá un proceso para hacer ajustes basados en los resultados de la evaluación y el feedback recibido.

### 6. Documentación y Comunicación

- **Registro de Cambios:** Se mantendrá un registro detallado de todas las modificaciones realizadas durante el proceso de implementación para futuras referencias y auditorías.
- **Comunicación Interna:** Se llevará a cabo una comunicación efectiva con todos los interesados, incluyendo el equipo de TI, los administradores de bases de datos y el personal afectado, para informar sobre los cambios planificados y proporcionar orientación durante la transición.

### Listas de Verificación

#### 1. Antes de la Copia de Seguridad

- Revisar la disponibilidad de recursos necesarios para la copia de seguridad (espacio de almacenamiento, tiempo de procesamiento).
- Verificar la integridad y consistencia de los datos a respaldar.
- Asegurarse de que los sistemas y servicios relevantes estén en un estado operativo adecuado.
- Comprobar que se han realizado las actualizaciones de software y parches de seguridad necesarios.
- Validar que se haya realizado una copia de seguridad completa y exitosa recientemente.

#### 2. Durante la Copia de Seguridad

- Supervisar el progreso de la copia de seguridad para detectar posibles problemas o errores.
- Verificar que se estén aplicando los procedimientos de seguridad adecuados durante la transferencia y almacenamiento de datos.
- Registrar cualquier anomalía o incidencia durante el proceso de copia de seguridad.

#### 3. Después de la Copia de Seguridad

- Verificar la integridad de los datos respaldados mediante pruebas de restauración parciales.
- Confirmar que se haya generado un registro detallado de la copia de seguridad, incluyendo la fecha, hora y resultados.
- Validar que se hayan aplicado correctamente las medidas de seguridad y encriptación a los datos respaldados.
- Comprobar que las copias de seguridad se hayan almacenado en la ubicación designada de manera correcta y segura.

#### 4. Consideraciones Generales

- *Realizar pruebas periódicas de restauración para garantizar la efectividad del proceso de copia de seguridad.*
- *Mantener actualizada la documentación relacionada con las copias de seguridad, incluyendo políticas, procedimientos y registros de auditoría.*
- *Capacitar regularmente al personal responsable de las copias de seguridad en los procedimientos y mejores prácticas.*
- *Revisar y actualizar continuamente las políticas y procedimientos de copias de seguridad en función de las nuevas tecnologías y mejores prácticas de la industria.*

### Acuerdos de Nivel de Servicio (SLAs)

<b>1. Objetivo del SLA</b>	
○	<b>Propósito:</b> El objetivo del SLA es establecer estándares claros y expectativas definidas para el servicio de copias de seguridad, asegurando la disponibilidad, integridad y confidencialidad de los datos respaldados.
<b>2. Alcance del Servicio</b>	
○	<b>Servicios Incluidos:</b> El servicio de copias de seguridad cubre la realización regular de copias de seguridad de los datos críticos de la organización, su almacenamiento seguro, y la capacidad de restauración en caso de pérdida o corrupción de datos.
<b>3. Compromisos de Nivel de Servicio</b>	
●	<b>RTO (Tiempo de Recuperación Objetivo):</b> Se establece un RTO de 4 horas, lo que significa que el proveedor se compromete a restaurar la operatividad del sistema dentro de las 4 horas posteriores a un incidente.
●	<b>RPO (Punto de Recuperación Objetivo):</b> El RPO se fija en 24 horas, lo que implica que el proveedor garantiza que no se perderán más de 24 horas de datos en caso de fallo.
●	<b>Frecuencia de Copias de Seguridad:</b> Se realizarán copias de seguridad incrementales diarias y copias de seguridad completas semanales.
●	<b>Disponibilidad del Servicio:</b> El servicio de copias de seguridad estará disponible el 85% del tiempo planificado, excluyendo periodos de mantenimiento programado.
<b>4. Responsabilidades del Proveedor</b>	
●	<b>Soporte y Mantenimiento:</b> El proveedor se compromete a proporcionar soporte técnico en un lapso de 12 horas al día, los 6 días de semana, y a realizar mantenimientos preventivos para garantizar el buen funcionamiento del sistema de copias de seguridad.
●	<b>Reporte y Comunicación:</b> El proveedor informará al cliente sobre cualquier problema que afecte la disponibilidad o integridad del servicio de copias de seguridad, mediante reportes regulares y comunicación proactiva.
<b>5. Obligaciones del Cliente</b>	
○	<b>Cooperación:</b> El cliente colaborará con el proveedor proporcionando acceso a los sistemas relevantes y cooperando en la realización de pruebas de recuperación.
○	<b>Notificación de Cambios:</b> El cliente notificará al proveedor cualquier cambio en la infraestructura o configuración que pueda afectar la realización de las copias de seguridad.
<b>6. Revisiones y Ajustes del SLA</b>	
○	<b>Frecuencia de Revisión:</b> El SLA será revisado trimestralmente para asegurar que siga siendo relevante y efectivo.
○	<b>Proceso de Modificación:</b> Los cambios al SLA requerirán el consentimiento mutuo por escrito de ambas partes y se documentarán formalmente.
<b>7. Firma y Acuerdo</b>	
○	<b>Firmas de las Partes Involucradas:</b>
	○ Cliente:
	○ Proveedor:

- **Fecha:** Viernes 12 de Abril del 2024