



Sistemas Integrales Ltda.

**Política de Almacenamiento, Respaldo y
Recuperación de Información**

ERP SOLIN — SOLINcloud

	POLÍTICA DE ALMACENAMIENTO, RESPALDO Y RECUPERACIÓN DE INFORMACIÓN	Versión: 1
		Fecha: 18/06/2023
	Sistemas Integrales Ltda. Copia Controlada (X) Copia No Controlada ()	Código: P-A-01
		Página 1 de 5

1. Introducción

Como parte de su compromiso con la seguridad, integridad y disponibilidad de la información de sus clientes, Sistemas Integrales Ltda. (SINTEG) ha definido una política integral de almacenamiento, respaldo y recuperación de datos para las bases de datos transaccionales que soportan la operación del ERP SOLIN bajo el modelo de servicio SOLINcloud.

Esta política establece los procedimientos, frecuencias, herramientas y mecanismos de verificación que garantizan la protección continua de los datos, así como la capacidad de restauración ante eventos de pérdida, corrupción o desastre.

El presente documento es aplicable a todos los clientes del servicio SOLINcloud y se enmarca en las buenas prácticas de gestión de la información conforme a los estándares de calidad CMMI Nivel 5 que rigen los procesos de SINTEG.

2. Alcance

Esta política aplica a todas las bases de datos transaccionales que soportan la operación del ERP SOLIN para los clientes del servicio SOLINcloud, incluyendo:

- Bases de datos financieras y administrativas (Contabilidad, Tesorería, Cartera, Cuentas por Pagar, Inventarios, Compras, Presupuesto, Nómina, Activos Fijos).
- Bases de datos comerciales del sistema de servicios públicos (Suscriptores, Lecturas, Facturación, Recaudos, Cartera, PQRs).
- Bases de datos de configuración, maestros y parámetros del ERP.
- Bases de datos de reportería.

Cada cliente de SOLINcloud cuenta con bases de datos dedicadas e independientes, lo que garantiza el aislamiento lógico de su información.

3. Infraestructura de Almacenamiento

La infraestructura de SOLINcloud opera sobre plataformas de nube empresarial que garantizan alta disponibilidad, escalabilidad y seguridad:

3.1. Servidor de Bases de Datos — Amazon Web Services (AWS)

Componente	Detalle
------------	---------

	POLÍTICA DE ALMACENAMIENTO, RESPALDO Y RECUPERACIÓN DE INFORMACIÓN	Versión: 1
		Fecha: 18/06/2023
	Sistemas Integrales Ltda. Copia Controlada (X) Copia No Controlada ()	Código: P-A-01
		Página 2 de 5

Proveedor de Nube	Amazon Web Services (AWS)
Tipo de Instancia	Amazon EC2 (Elastic Compute Cloud)
Motor de BD	Microsoft SQL Server
Almacenamiento	Amazon EBS (Elastic Block Store) — volúmenes de alto rendimiento
Disponibilidad	7x24 con monitoreo continuo

3.2. Almacenamiento de Respaldos en la Nube

Servicio	Uso
Amazon S3	Almacenamiento primario de respaldos. Buckets segregados por cliente con acceso controlado mediante políticas IAM.
Azure Blob Storage	Almacenamiento de respaldos históricos y de largo plazo. Retención completa desde 2022, organizado por año y mes.

4. Política de Respaldo

El sistema de respaldo opera de forma completamente automatizada mediante SQL Server Agent y Maintenance Plans, sin intervención manual. Los respaldos se ejecutan en ventanas de mantenimiento que no afectan la operación normal del sistema.

4.1. Servidor AWS (Clientes Cloud)

Tipo de Respaldo	Frecuencia	Horario (COT)	Formato
Full (Completo)	Semanal	Lunes 01:00 AM	.bak nativo
Diferencial	2 veces al día	01:00 AM y 01:00 PM	.bak nativo

Descripción de los tipos de respaldo:

- **Full Backup (Copia completa):** Contiene todos los datos de la base de datos a esa fecha. Es el respaldo base sobre el cual se aplican los diferenciales. Se ejecuta los días lunes.
- **Differential Backup (Copia diferencial):** Solo respalda la información que ha cambiado desde el último backup Full. Se ejecuta dos veces al día (madrugada y mediodía), de martes a domingo.

4.2. Proceso Automatizado

Cada job de respaldo consta de dos pasos secuenciales:

	POLÍTICA DE ALMACENAMIENTO, RESPALDO Y RECUPERACIÓN DE INFORMACIÓN	Versión: 1
		Fecha: 18/06/2023
	Sistemas Integrales Ltda. Copia Controlada (X) Copia No Controlada ()	Código: P-A-01
		Página 3 de 5

- **Paso 1 — Ejecución del Maintenance Plan:** SQL Server genera el archivo de respaldo (.bak o .7z) en el almacenamiento local del servidor.
- **Paso 2 — Sincronización a la Nube:** Un script automatizado (PowerShell) transfiere el respaldo al almacenamiento en la nube (Amazon S3 o Azure Blob Storage) inmediatamente después de su generación

5. Almacenamiento en la Nube

5.1. Amazon S3 (Almacenamiento Primario)

- Cada cliente dispone de un bucket S3 independiente y dedicado exclusivamente a sus respaldos.
- El acceso está controlado mediante políticas IAM (Identity and Access Management) de AWS, garantizando que solo usuarios autorizados puedan acceder a los datos.
- Los respaldos disponibles en S3 corresponden a la última semana (Full del lunes + diferenciales diarios).
- Opcionalmente, se puede proporcionar acceso de solo lectura al cliente para la descarga directa de sus respaldos desde la consola de AWS.

5.2. Azure Blob Storage (Retención Histórica)

- Los respaldos históricos se almacenan en Azure Blob Storage con retención completa.
- Organización por carpetas: Año/Mes/ (ej: 2026/Abril/).
- Se conservan respaldos históricos desde 2018, lo que permite la recuperación de datos de cualquier período anterior bajo solicitud.

6. Procedimiento de Restauración

En caso de requerirse la restauración de una base de datos, el procedimiento es el siguiente:

6.1. Obtención de los Archivos de Respaldo

Los archivos .bak se obtienen desde Amazon S3 (respaldos recientes) o se solicitan a SINTEG para respaldos históricos almacenados en Azure Blob Storage.

	POLÍTICA DE ALMACENAMIENTO, RESPALDO Y RECUPERACIÓN DE INFORMACIÓN	Versión: 1
		Fecha: 18/06/2023
	Sistemas Integrales Ltda.	Código: P-A-01
	Copia Controlada (X) Copia No Controlada ()	Página 4 de 5

6.2. Restauración en SQL Server Management Studio (SSMS)

Paso 1. Abrir SQL Server Management Studio (SSMS) e iniciar sesión en el servidor de destino.

Paso 2. Clic derecho sobre la carpeta Databases y seleccionar Restore Database.

Paso 3. Seleccionar la opción Device, dar clic en los tres puntos y luego en el botón Add para seleccionar el archivo de backup Full (.bak). Este debería ser el más pesado y con fecha de un día lunes.

Paso 4. En la pestaña Options, cambiar el Recovery State a RESTORE WITH NORECOVERY. Esto permite aplicar un backup diferencial adicional. Pulsar OK y esperar la confirmación.

Paso 5. Verificar que la base de datos aparezca en estado "Restoring...", lo que indica que está esperando la restauración del siguiente backup.

Paso 6. Clic derecho sobre la base de datos en estado Restoring y seleccionar Tasks > Restore > Database. Repetir el proceso de selección pero eligiendo el archivo de backup diferencial correspondiente.

Paso 7. Verificar que en la pestaña Options el estado sea RESTORE WITH RECOVERY. Pulsar OK y esperar el mensaje de operación exitosa.

Nota: Si solo se requiere restaurar datos hasta el último backup completo (Full), no es necesario aplicar el diferencial. En ese caso, en el Paso 4 se debe seleccionar RESTORE WITH RECOVERY en lugar de NORECOVERY.

7. Monitoreo y Verificación

SINTEG realiza monitoreo continuo del proceso de respaldo para garantizar su correcta ejecución:

- **Historial de SQL Server Agent:** Cada ejecución de los jobs de respaldo queda registrada con su estado (exitoso/fallido), hora de inicio y finalización.
- **Verificación de archivos en la nube:** Se valida periódicamente que los archivos de respaldo se encuentren en los buckets S3 y en Azure Blob Storage con los tamaños y fechas esperados.
- **Alertas de fallo:** En caso de fallo en la ejecución de un job de respaldo, se generan alertas que son atendidas por el equipo de infraestructura.

	POLÍTICA DE ALMACENAMIENTO, RESPALDO Y RECUPERACIÓN DE INFORMACIÓN	Versión: 1
		Fecha: 18/06/2023
	Sistemas Integrales Ltda.	Código: P-A-01
	Copia Controlada (X) Copia No Controlada ()	Página 5 de 5

8. Política de Retención

Destino	Retención	Tipo de Respaldo
Amazon S3	Última semana (Full + diferenciales)	Operativo (restauración rápida)
Azure Blob Storage	Completa (desde 2018)	Histórico (largo plazo)

Si se requiere un respaldo más antiguo que la última semana disponible en S3, puede ser solicitado al equipo de SINTEG, quien lo recuperará del almacenamiento histórico.

9. Responsables

Rol	Responsabilidad
Área de Infraestructura / DevOps	Configuración, monitoreo y mantenimiento de los procesos de respaldo. Atención de alertas y ejecución de restauraciones.
Gerencia de Tecnología	Supervisión de la política de respaldo, aprobación de cambios en la política y gestión de solicitudes de restauración.
Cliente	Solicitud de restauraciones cuando se requieran. Descarga de respaldos si se le ha proporcionado acceso a S3.

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	Junio 2023	Creación de la Política