## ***Tipo de copia***

1. ***Copias de Seguridad Completa***

Descripción: Este tipo de copia de seguridad realiza una copia completa de todos los datos del sistema en su estado actual.

1. ***Copias de Seguridad Incrementales:***

Descripción: Las copias de seguridad incrementales respaldan solo los datos que han cambiado desde la última copia de seguridad completa o incremental.

## ***Horarios de implementación***

## ***Copias de Seguridad Diarias:***

* + Realiza copias de seguridad diarias durante las horas de menor actividad, por ejemplo, temprano en la mañana o tarde en la noche.
  + Horario sugerido: 02:00 AM - 04:00 AM o 10:00 PM - 12:00 AM.

***Copias de Seguridad Semanales (Completa):***

* + Realiza copias de seguridad completas los fines de semana, ya que es probable que haya menos actividad durante estos días.
  + Horario sugerido: Sábado o domingo, entre las 12:00 AM y las 06:00 AM.

***Copias de Seguridad Incrementales o Diferenciales:***

* + Si es posible, implementa copias de seguridad incrementales o diferenciales entre las copias diarias.
  + Programa estas copias durante las horas de menor actividad, como al final de la jornada laboral.
  + **Horario sugerido: 06:00 PM - 08:00 PM.**

## **Restauración de Datos**

Los procesos de restauración de datos deben llevarse a cabo en los siguientes casos:

**Pérdida de Datos Accidental:** Si se produce una eliminación accidental de datos por parte de los usuarios o debido a un error en el sistema, se debe realizar una restauración de los datos afectados a partir de la copia de seguridad más reciente disponible.

**Corrupción de Datos:** En caso de que se detecte corrupción en los datos almacenados, ya sea debido a errores de hardware o software, se debe restaurar una copia de seguridad válida que contenga los datos no corruptos.

**Ataques de Malware o Ransomware:** Si se produce un ataque de malware o ransomware que afecta los datos almacenados, se debe restaurar una copia de seguridad limpia y no infectada para recuperar los datos afectados.

**Fallos de Hardware o Software:** Ante fallos de hardware o software que impidan el acceso a los datos o causen pérdida de los mismos, se debe realizar una restauración de datos a partir de la copia de seguridad más reciente disponible

## prevención de pérdida de datos

***Encriptación de Datos:***

* Utiliza encriptación para proteger datos sensibles, tanto en tránsito como en reposo.
* Implementa HTTPS para la comunicación segura a través de la web.

***Actualización y Mantenimiento del Software:***

* Mantén actualizados todos los sistemas operativos, aplicaciones y herramientas relacionadas.
* Aplica parches de seguridad de manera regular para cerrar posibles vulnerabilidades.