INFORME DE PROCEDIMIENTO PARA LAS COPIAS DE RESPALDO DE LA INFORMACIÓN

1. Introducción

En el presente documento se detalla el procedimiento implementado para la realización de copias de respaldo de la información en el Hospital Mental Rudesindo Soto. Se establecen los objetivos del proceso, la clasificación de los tipos de respaldo, la frecuencia con la que se ejecutan, los medios de almacenamiento utilizados, los responsables del proceso y las políticas de retención y restauración de datos. Este procedimiento es fundamental para garantizar la integridad, disponibilidad y continuidad de la información clínica, administrativa y operativa del hospital, protegiendo así datos sensibles de pacientes y asegurando la prestación ininterrumpida de los servicios de salud mental.

2. Objetivos

Objetivo general:

- Establecer un procedimiento estandarizado para la generación, almacenamiento y recuperación de copias de respaldo que asegure la continuidad operativa de los sistemas informáticos y la protección de la información institucional.

Objetivos específicos:

- Garantizar la existencia de copias actualizadas de la información crítica.
- Establecer políticas de frecuencia, almacenamiento y conservación de los respaldos.
- Facilitar la recuperación eficiente de datos ante pérdidas o incidentes.

- Minimizar los riesgos de pérdida de información por errores humanos, fallos técnicos o ciberataques.

3. Procedimiento para las copias de respaldo

3.1. Alcance:

Aplica a todos los sistemas, servidor, bases de datos y dispositivos que contengan información relevante para la operación del hospital.

3.2. Tipos de respaldo:

- **Completo:** Copia total de toda la información. Se realiza semanalmente.
- **Incremental:** Copia de los datos modificados desde el último respaldo. Se realiza diariamente.
- **Diferencial:** Copia de los datos modificados desde el último respaldo completo. Opcional, según necesidad.

3.3. Frecuencia de respaldo:

- Respaldo completo: cada domingo a las 2:00 a.m.
- Respaldo incremental: de lunes a sábado a las 2:00 a.m.
- Verificación de respaldos: cada lunes a las 9:00 a.m.

3.4. Medio de almacenamiento:

- Almacenamiento en servidores locales cifrados.
- Copia redundante en la nube mediante plataforma segura.
- Copia externa (disco duro en la caja fuerte) una vez por semana.

3.5. Retención y eliminación de respaldos:

- Retención de respaldos diarios: 15 días.

- Retención de respaldos semanales: 2 meses.
- Retención de respaldos mensuales: 1 año.
- Eliminación segura mediante software de borrado seguro.

3.6. Responsables:

- El área de sistemas será la encargada de ejecutar y verificar los respaldos.
- Se debe documentar cada respaldo realizado (fecha, tipo, estado).
- En caso de incidentes, el área deberá coordinar el proceso de recuperación.

3.7. Pruebas de restauración:

- Se realizarán pruebas trimestrales de recuperación de datos para asegurar la efectividad del respaldo.

4. Conclusiones

La implementación de un procedimiento formal para las copias de respaldo es esencial para mitigar los riesgos asociados a la pérdida de información. Este procedimiento garantiza que la organización pueda responder de forma oportuna y efectiva ante cualquier contingencia tecnológica, permitiendo la continuidad del servicio y la preservación de la integridad de los datos.

Es responsabilidad de todas las áreas involucradas seguir este protocolo con disciplina y constancia, asegurando así la seguridad de la información y el cumplimiento de las normativas vigentes en protección de datos.