



SOP-09 | Protección de Datos e IDs de Participantes

Procedimiento Operativo Estándar

Documento	SOP-09
Estado	Borrador para aprobación interna
Versión	0.1
Entrada en vigor	A partir de su aprobación
Responsable	Lab Manager de BEER
Ciclo de revisión	Al menos anual
Aplica a	Proyectos y personal comprendidos por este SOP

Behavioral & Experimental Economics Research Lab · Tecnológico de Monterrey

1. Propósito

Proteger la información de participantes y asegurar que identidad, pagos, reclutamiento y datos analíticos se vinculen únicamente cuando sea necesario y bajo acceso controlado.

2. Clases de datos

Clase	Ejemplos	Manejo predeterminado
Identificadores directos	Nombre, email, teléfono, matrícula	Separados, restringidos, encriptados
Archivo de enlace	BEER ID ↔ study ID	Muy restringido, separado
Pago/admin	Referencia bancaria, firma, monto	Separado de datos conductuales
Datos de investigación	Decisiones, outcomes, encuestas	Controles de acceso del proyecto
Datos sensibles	Salud, victimización, biometría, ubicación precisa	Controles reforzados y mínima recolección

3. Arquitectura de identificadores

La arquitectura preferida es ORSEE/contact ID → BEER participant ID → project experimental ID. Los archivos analíticos deberán utilizar el project ID y no contener identificadores directos salvo necesidad científica.

4. Control de acceso

- Otorgar el mínimo acceso necesario por rol.
- No compartir cuentas o credenciales.
- Retirar accesos oportunamente cuando alguien deja el proyecto.
- El PI mantiene lista de accesos a archivos con PII o datos sensibles.

5. Almacenamiento y transferencia

- Utilizar almacenamiento institucionalmente aprobado o expresamente autorizado.
- Encriptar PII y datos sensibles en reposo y tránsito cuando sea factible.
- No transmitir PII por apps personales de mensajería o adjuntos de correo no seguros.
- Los dispositivos de campo deberán utilizar bloqueo de pantalla y encriptación cuando sea compatible.

6. Archivos de enlace

El archivo que conecta identificadores directos con IDs del estudio debe almacenarse por separado y ser accesible solo para personal que necesite reidentificación por razones operativas aprobadas.

7. Minimización y retención

Recolectar únicamente identificadores necesarios para reclutamiento, follow-up, pago o linkage aprobado. Eliminar o desidentificar irreversiblemente PII cuando deje de ser necesaria, sujeto al consentimiento, requisitos éticos, obligaciones legales de retención y necesidades de reproducibilidad.

8. Datos compartidos o públicos

Antes de compartir datos se deberá evaluar riesgo de reidentificación, incluyendo combinaciones de identificadores indirectos. La eliminación de nombres no hace automáticamente seguro un dataset para publicación.

9. Brecha de datos

El acceso no autorizado sospechado, la pérdida de dispositivos con datos o la divulgación accidental se tratarán como incidentes bajo SOP-10. Se conservarán logs y no se eliminará evidencia necesaria para evaluar la brecha.

10. Documentos relacionados

- SOP-02 Participant Pool and ORSEE
- SOP-08 Field Experiments
- SOP-10 Incident Reporting
- SOP-11 Project Closeout