

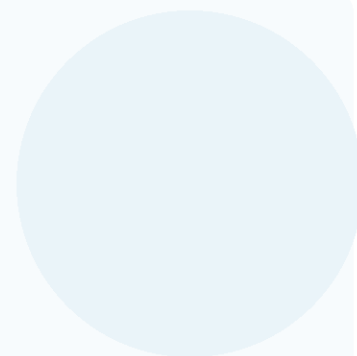
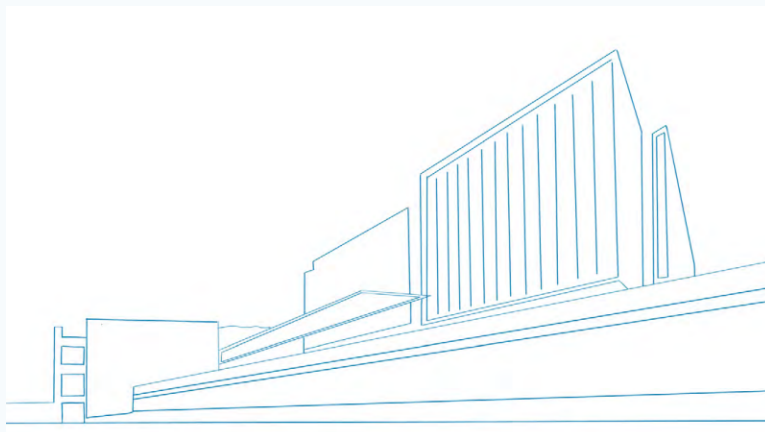
GUÍA PARA INVESTIGADORES UDD

ORIENTACIONES PARA

PRIVACIDAD, CONFIDENCIALIDAD Y DATOS

Orientaciones éticas y metodológicas
para equipos de investigación

Protección durante todo el
estudio



CONTENIDOS

Orientaciones éticas y metodológicas para equipos de investigación

PRIVACIDAD, CONFIDENCIALIDAD Y DATOS

1. Introducción
2. Privacidad y Confidencialidad: Distinción Operativa
3. Información Privada y Expectativa Razonable de Privacidad
4. Riesgos por Método: Observación, Grupos Focales, Muestreo en Red y Comunicaciones
5. Principios de la Ley 21.719 Relevantes para Investigación
6. Consentimiento y otras Bases de Licitud
7. Derechos de las Personas Titulares y su Implicancia en Investigación
8. Seguridad de la Información: Medidas Técnicas y Organizativas
9. Evaluación de Impacto (DPIA) en Protección de Datos
10. Transferencias, Terceros Encargados y Gobernanza
11. Traducción a Documentos del Estudio: Protocolo, Consentimiento y Materiales de Reclutamiento
12. Referencias

Capítulo I

Fundamentos y contexto

1. INTRODUCCIÓN

La protección de la privacidad y el resguardo de la confidencialidad constituyen condiciones básicas de una investigación ética en ciencias sociales y del comportamiento. En muchos estudios, el principal riesgo no proviene de los procedimientos en sí, sino de la posibilidad de que información sensible o identificable sea observada, inferida, reutilizada o divulgada fuera del marco de confianza propio de la relación investigativa. En Chile, la Ley N° 21.719 moderniza el régimen de protección de datos personales y establece principios, derechos y deberes que inciden directamente en el diseño, la ejecución y la gobernanza de datos de investigación (con vigencia diferida al 01-12-2026).



2. PRIVACIDAD Y CONFIDENCIALIDAD: DISTINCIÓN OPERATIVA

Privacidad se relaciona con el control sobre el acceso a la persona y a su información: cuándo, cómo y en qué circunstancias se observa, registra o solicita información. Confidencialidad, en cambio, se refiere a la obligación del equipo investigador y de la institución de proteger apropiadamente la información que las personas han entregado en una relación de confianza, evitando divulgaciones incompatibles con el entendimiento original. La distinción es útil porque permite localizar el riesgo: un estudio puede ser respetuoso de la privacidad (p. ej., consentimiento y en un espacio privado) pero fallar en confidencialidad (p. ej., filtración de bases); o viceversa.

3. INFORMACIÓN PRIVADA Y EXPECTATIVA RAZONABLE DE PRIVACIDAD

En investigación observacional y en investigación digital, la evaluación ética debe considerar la expectativa razonable de privacidad del sujeto, más que una noción rígida de 'espacio público versus privado'. Existen conductas en espacios públicos que pueden ser razonablemente consideradas privadas (por ejemplo, conversaciones en un parque), y el avance tecnológico hace posible registrar a distancia interacciones que las personas asumen no grabadas. Además, estándares culturales y generacionales modifican la expectativa de privacidad, por lo que el diseño debe explicitar supuestos contextualizados.

Capítulo II

Diseño y criterios éticos

4. RIESGOS POR MÉTODO: OBSERVACIÓN, GRUPOS FOCALES, MUESTREO EN RED Y COMUNICACIONES

RECOMENDACIÓN CEII

No prometer confidencialidad absoluta en grupos focales y usar comunicaciones neutras cuando la temática sea sensible.

La observación encubierta y la recolección de información identificable sin conocimiento/consentimiento pueden constituir invasión directa de privacidad y requieren justificación metodológica robusta y salvaguardas adicionales. En estudios que utilizan grabación de video o audio sin aviso, una buena práctica es prever, cuando corresponda, mecanismos de debriefing y la posibilidad de solicitar destrucción de material, si ello es compatible con el diseño y no genera daños adicionales.



Los grupos focales son metodológicamente valiosos, pero presentan un límite estructural: el equipo no puede prometer confidencialidad respecto de lo que otros participantes puedan repetir fuera del grupo. Esto exige advertencias claras en el consentimiento y, cuando el tema sea sensible, la recomendación de prudencia: se debe invitar a participantes a evaluar qué están dispuestos/as a compartir en un contexto donde no controlan completamente la circulación posterior de lo dicho.

El muestreo en bola de nieve puede vulnerar privacidad cuando participantes entregan nombres de terceros para reclutarlos. En temas sensibles, una alternativa preferible es que quienes ya participan entreguen información del estudio a potenciales interesados, sin transferir datos personales al equipo hasta que la persona contacte voluntariamente.

Las comunicaciones (correo, llamadas, mensajería) son un punto crítico de privacidad. Si el estudio trata condiciones estigmatizantes, ilegalidad o experiencias que las personas no desean que terceros conozcan, la comunicación debe ser neutra y no revelar participación. Esto incluye título del estudio, asuntos de correo, mensajes de recordatorio y lugares de cita, adaptando canales a preferencias de seguridad del participante.

5. PRINCIPIOS DE LA LEY 21.719 RELEVANTES PARA INVESTIGACIÓN

RECOMENDACIÓN CEII

Aplicar minimización: recolectar solo datos necesarios, por finalidades claras y con plazos definidos de conservación.

La Ley 21.719 define dato personal como toda información vinculada o referida a una persona identificada o identificable, y reconoce categorías de datos personales sensibles, incluyendo salud, situación socioeconómica, vida sexual, orientación sexual e identidad de género. La ley incorpora definiciones útiles para investigación, como anonimización (irreversible, tras la cual el dato deja de ser personal) y seudonimización (separación de información adicional que permite atribución).

El tratamiento de datos se rige por principios de licitud y lealtad, finalidad, proporcionalidad (minimización), calidad, responsabilidad, seguridad, transparencia/información y confidencialidad. En términos prácticos, esto obliga a que el protocolo explicita fines, recolecte solo lo necesario, mantenga datos por el tiempo indispensable y adopte controles de acceso y medidas de seguridad acordes al riesgo. El deber de secreto/confidencialidad subsiste aun después de terminada la relación con el titular.

6. CONSENTIMIENTO Y OTRAS BASES DE LICITUD

RECOMENDACIÓN CEII

Describir finalidades específicas y prever operativamente cómo se gestionará retiro o revocación del consentimiento.

La ley establece como regla general la licitud por consentimiento, entendido como manifestación libre, informada y específica respecto de finalidades, otorgada de forma previa e inequívoca; además, reconoce que el titular puede revocar el consentimiento en cualquier momento sin expresión de causa, usando medios equivalentes. Para investigación, esto implica: describir claramente finalidades, evitar consentimientos vagos, y prever operativamente cómo se tramitará un retiro o revocación (por ejemplo, qué sucede con datos ya recolectados).

La ley contempla otras bases de licitud (obligación legal, ejecución contractual, interés legítimo, entre otras). En investigación académica, la base típica suele ser el consentimiento. Si se considera otra base, se recomienda justificarla explícitamente y describir salvaguardas adicionales, dado que el estándar ético exige transparencia con participantes y proporcionalidad en el tratamiento.

Capítulo III

Participación y salvaguardas

7. DERECHOS DE LAS PERSONAS TITULARES Y SU IMPLICANCIA EN INVESTIGACIÓN

La Ley 21.719 reconoce derechos de acceso, rectificación, supresión, oposición, portabilidad y bloqueo temporal del tratamiento. Aunque la aplicación concreta de ciertos derechos puede tener particularidades en contextos de investigación (por ejemplo, cuando el tratamiento es necesario para fines científicos de interés público y se han adoptado garantías), los protocolos deben planificar: canales de contacto, plazos razonables de respuesta, y cómo se gestionarán solicitudes sin comprometer integridad científica ni confidencialidad de terceros.



8. SEGURIDAD DE LA INFORMACIÓN: MEDIDAS TÉCNICAS Y ORGANIZATIVAS

RECOMENDACIÓN CEII

Separar identificadores, limitar accesos por rol, cifrar almacenamiento y definir manejo de audio, video y transcripciones.

La protección efectiva depende de medidas desde el diseño y por defecto. Entre las medidas recomendables se incluyen: recolectar la mínima cantidad de identificadores; sustituir identificadores por códigos; mantener claves de reidentificación separadas y con acceso restringido; cifrar almacenamiento y transmisión; limitar accesos por roles; y reportar resultados de modo agregado, evitando combinaciones de atributos que permitan reidentificación. En investigación cualitativa, debe existir una política de transcripción que elimine identificadores y un plan de manejo de audio/video.

La ley incorpora el deber de adoptar medidas de seguridad apropiadas al riesgo, incluyendo seudonimización y cifrado cuando corresponda. Además, introduce el deber de reportar vulneraciones a las medidas de seguridad a la Agencia cuando exista riesgo razonable para derechos y libertades, y, tratándose de datos sensibles o datos de niños/as menores de 14 años, deber de comunicar a titulares a través de sus representantes, usando lenguaje claro y sencillo.

9. EVALUACIÓN DE IMPACTO (DPIA) EN PROTECCIÓN DE DATOS

La ley establece la evaluación de impacto en protección de datos cuando sea probable un alto riesgo por naturaleza, alcance, contexto, tecnología o fines del tratamiento, y la exige siempre en casos como: observación o monitoreo sistemático de una zona de acceso público; tratamiento masivo; decisiones automatizadas/perfilamiento con efectos significativos; y tratamiento de datos sensibles en ciertas hipótesis. En investigación, esto es relevante para estudios con vigilancia en espacios públicos (p. ej., cámaras), proyectos con grandes volúmenes de datos, o analítica predictiva/perfilamiento.

Capítulo IV

Datos, gestión y comunicación

10. TRANSFERENCIAS, TERCEROS ENCARGADOS Y GOBERNANZA

RECOMENDACIÓN CEII

Formalizar obligaciones de confidencialidad y seguridad con transcriptoras, plataformas o servicios externos.

Cuando se involucra a terceros (por ejemplo, servicios de transcripción, plataformas, almacenamiento en nube), debe existir claridad contractual y organizativa sobre el encargo: finalidad, duración, tipo de datos, obligaciones de seguridad y prohibición de uso para fines distintos. La ley regula el tratamiento por encargados y exige que, terminado el servicio, los datos sean suprimidos o devueltos al responsable, según corresponda. En la práctica, esto obliga a que el equipo justifique la elección de plataformas, preferentemente institucionales, y documente acuerdos de confidencialidad.



11. TRADUCCIÓN A DOCUMENTOS DEL ESTUDIO: PROTOCOLO, CONSENTIMIENTO Y MATERIALES DE RECLUTAMIENTO

RECOMENDACIÓN CEII

El protocolo y el consentimiento deben describir el ciclo de vida del dato desde recolección hasta destrucción o anonimización.

Un protocolo bien diseñado debe describir el ciclo de vida del dato: recolección, codificación/seudonimización, almacenamiento, acceso, análisis, publicación, conservación y destrucción/anonimización. El consentimiento debe reflejar esa arquitectura de forma comprensible para la persona: qué se recopila, quién accede, por cuánto tiempo, si habrá reutilización, y cuáles son los límites de confidencialidad según método (por ejemplo, grupos focales) y según obligaciones legales de reporte cuando sean pertinentes.

Los materiales de reclutamiento deben ser consistentes con la protección de privacidad: títulos neutros cuando el tema es sensible, canales que no expongan participación y guiones de contacto que no revelen información a terceros. En estudios en línea, se recomienda incluir indicaciones prácticas para reducir exposición en el hogar (por ejemplo, cerrar el navegador o usar modo privado cuando la temática es sensible).

12. REFERENCIAS

CITI Program. Privacy and Confidentiality – SBE.

Ley N° 21.719. Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (vigencia diferida desde 01-12-2026).