UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

GUÍA SOBRE LA PROTECCIÓN DE DATOS EN LOS PROYECTOS DE INVESTIGACIÓN

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Guía sobre la protección de datos en los proyectos de investigación

Enfoque ejecutivo, normativo y de ciberseguridad

Documento base	Guía para delegados de protección de datos. Guía sobre la protección de datos en los proyectos de investigación
Entidad	CRUE - Secretarías Generales / Grupo de Trabajo de Delegadas y Delegados de Protección de Datos
Fecha del documento	Febrero de 2024
Marco principal	RGPD (UE) 2016/679 y LOPDyGDD española

Nota de alcance. El documento original ya se encuentra redactado en español. Por ello, este entregable no realiza una traducción literal, sino una síntesis ejecutiva en español técnico y claro, conservando el sentido, la terminología y el marco normativo de la fuente.

1. Síntesis ejecutiva

La Guía constituye un marco práctico para integrar la protección de datos personales en proyectos de investigación universitaria, incluidas tesis doctorales, trabajos fin de titulación y otras actividades académicas. Está dirigida principalmente a delegados de protección de datos (DPD) que ejercen funciones de asesoramiento, supervisión y control. Su planteamiento central es que la privacidad no debe abordarse como una formalidad posterior, sino como un componente del diseño, ejecución, seguridad, publicación, reutilización y cierre de la investigación.

Desde una perspectiva de ciberseguridad, la Guía articula la protección jurídica del dato con controles técnicos y organizativos orientados a preservar confidencialidad, integridad y disponibilidad. El tratamiento debe estar legitimado, limitarse a la finalidad declarada, utilizar únicamente los datos necesarios, restringir accesos, reducir la identificabilidad mediante anonimización o seudonimización cuando proceda, gestionar los riesgos antes del tratamiento y mantener evidencia documental que permita demostrar el cumplimiento.

El mensaje operativo más relevante es la aplicación de un enfoque basado en riesgo y responsabilidad proactiva. La investigación debería priorizar datos anónimos o anonimizados; si ello no permite alcanzar los objetivos científicos, recurrir a datos seudonimizados y, solo cuando resulte necesario, a datos directamente identificables. Paralelamente, deben definirse roles, bases jurídicas, plazos de conservación, destinatarios, transferencias internacionales, encargados, medidas de seguridad y mecanismos para atender los derechos de los participantes.

2. Alcance, conceptos y responsabilidades

La Guía se aplica a tratamientos de datos personales originados en proyectos y actividades de investigación científica. No sustituye el criterio independiente del DPD ni constituye una decisión vinculante; funciona como orientación para estructurar el cumplimiento.

Conceptos esenciales

- Dato personal: cualquier información relativa a una persona física identificada o identificable, incluidos identificadores, localización, imagen, voz, datos académicos, profesionales, familiares o de salud.
- Dato seudonimizado: sigue siendo dato personal. La identidad puede reconstruirse mediante información adicional que debe mantenerse separada y protegida.

- Dato anónimo/anonimizado: la persona no es identificable razonablemente. Si existe una posibilidad razonable de reidentificación, el dato no debe considerarse verdaderamente anónimo.
- Tratamiento: comprende todo el ciclo de vida del dato: recogida, registro, organización, conservación, consulta, uso, comunicación, difusión, modificación, supresión y destrucción.

Roles

El responsable del tratamiento determina los fines y medios. En el contexto descrito, la Universidad u órgano establecido asume esta responsabilidad y el investigador debe observar sus normas y directrices. Existe corresponsabilidad cuando dos o más entidades determinan conjuntamente objetivos y medios. El encargado del tratamiento actúa por cuenta del responsable, como puede ocurrir con proveedores de nube, software, transcripción o destrucción documental, y requiere un acuerdo contractual conforme al RGPD.

3. Licitud y principios de protección de datos

Todo tratamiento necesita al menos una base jurídica válida: consentimiento, ejecución contractual, obligación legal, intereses vitales, misión de interés público o ejercicio de poderes públicos, o interés legítimo cuando resulte aplicable. La Guía advierte que el consentimiento en protección de datos no debe confundirse con el consentimiento informado exigible por razones éticas o por normativa sectorial.

Los principios que deben gobernar la investigación son: licitud; lealtad y transparencia; limitación de la finalidad; minimización; limitación del plazo de conservación; integridad y confidencialidad; y responsabilidad proactiva. La protección de datos desde el diseño y por defecto exige incorporar salvaguardas desde la concepción del proyecto y limitar, por defecto, la cantidad de datos, el alcance del tratamiento, el tiempo de conservación y el número de personas con acceso.

La minimización tiene una consecuencia práctica contundente: ante la falta de una justificación clara sobre la necesidad de un dato personal, ese dato debe excluirse. El acceso debe concederse por necesidad funcional y no por mera pertenencia al equipo de investigación.

4. Derechos de los participantes

Los participantes pueden ejercer los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición, con los requisitos y límites previstos en el RGPD. El acceso permite conocer si existen tratamientos, sus finalidades, legitimación, origen, destinatarios, conservación y, cuando corresponda, decisiones automatizadas. La rectificación permite corregir o

completar información; la supresión opera, entre otros supuestos, cuando los datos dejan de ser necesarios, se retira el consentimiento o el tratamiento es ilícito.

La portabilidad se circunscribe a tratamientos automatizados basados en consentimiento o contrato. La oposición puede operar incluso en investigación científica, histórica o estadística cuando concurran las bases señaladas por el RGPD. La Guía también recuerda que pueden existir excepciones legales en investigación cuando el ejercicio de determinados derechos imposibilite o dificulte gravemente los fines científicos, siempre dentro de las garantías exigidas.

5. Evaluación de Impacto relativa a la Protección de Datos (EIPD)

La EIPD es un proceso preventivo para analizar los riesgos que un tratamiento puede generar para los derechos y libertades de las personas y determinar medidas técnicas y organizativas antes de iniciar el tratamiento. Es obligatoria cuando exista alto riesgo.

Entre los criterios de riesgo destacados figuran la elaboración de perfiles; decisiones automatizadas con efectos significativos; observación sistemática; categorías especiales o datos penales; biometría para identificación; datos genéticos; tratamiento a gran escala; cruce de conjuntos de datos; personas vulnerables; uso innovador de tecnologías; y tratamientos que condicionen el ejercicio de derechos o el acceso a servicios. La concurrencia de dos criterios hace probable la necesidad de una EIPD, aunque la decisión debe atender al contexto y quedar documentada.

La EIPD debe iniciarse lo antes posible durante el diseño y revisarse a lo largo del ciclo de vida del proyecto. No es responsabilidad del DPD ejecutarla: corresponde al responsable del tratamiento. El DPD supervisa y asesora sobre necesidad, metodología, medidas de mitigación y resultados; el responsable de seguridad debe participar en las cuestiones de seguridad de la información.

6. Seguridad técnica y organizativa

El RGPD no impone un catálogo cerrado de controles. Las medidas deben seleccionarse según el riesgo, el estado de la técnica, el contexto, la naturaleza del tratamiento y los costes. Para universidades públicas españolas, la Guía remite además a las medidas aplicables del Esquema Nacional de Seguridad y a las políticas internas de cada institución.

Anonimización y seudonimización

La anonimización busca eliminar o reducir al mínimo el riesgo de reidentificación sin distorsionar la utilidad de los datos. Debe considerar tanto las posibilidades actuales como razonablemente futuras de identificación. La

seudonimización, en cambio, reduce el vínculo directo con la identidad pero no elimina la naturaleza personal del dato.

Para datos seudonimizados se recomienda separar funciones: rol técnico que recoge datos y asigna seudónimos; rol gestor que custodia la tabla de correspondencia; y rol investigador que trabaja con datos seudonimizados. Si una persona acumula roles, la justificación y las salvaguardas deben documentarse.

Controles prioritarios

- Autenticación y control de acceso según roles y necesidad de conocer.
- Contraseñas robustas, no compartidas ni reutilizadas, preferentemente administradas mediante gestor de contraseñas.
- Doble factor de autenticación cuando sea posible.
- Bloqueo automático de sesión en un periodo razonable, indicado por la Guía como no superior a cinco minutos.
- Cifrado de información, especialmente en dispositivos portátiles.
- Preferencia por infraestructuras y aplicaciones institucionales.
- Evitar, como regla general, almacenamiento local de datos personales en discos de equipos o memorias USB.
- Uso de VPN para acceso seguro desde redes públicas a recursos internos.
- Registro de accesos y custodia separada de información que permita reidentificar.

En soporte papel, la recomendación es reducir su uso al mínimo necesario. Cuando sea inevitable, debe mantenerse bajo llave, impedirse el acceso a impresiones por terceros y evitarse reutilizar hojas que contengan datos personales.

7. Gestión de brechas de seguridad

La Guía define una brecha de datos personales como una violación que produzca destrucción, pérdida, alteración, comunicación o acceso no autorizado. Distingue brechas de confidencialidad, integridad y disponibilidad. La detección o sospecha debe comunicarse con la mayor rapidez posible siguiendo el procedimiento institucional.

Los escenarios frecuentes incluyen accesos no autorizados, errores de destinatario en correo electrónico, divulgación de imágenes, correos masivos con destinatarios visibles, transferencias internacionales sin garantías, alteración o falsificación, fallos de recuperación de copias, pérdida o robo de dispositivos y destrucción inadecuada de soportes. En términos de ciberseguridad, estos ejemplos evidencian que la gestión de incidentes debe

cubrir tanto amenazas tecnológicas como errores humanos y fallas de procedimiento.

8. Transparencia e información al participante

Cuando los datos se obtienen directamente, el participante debe recibir información sobre identidad y contacto del responsable y del DPD, finalidades, base jurídica, destinatarios, transferencias internacionales, conservación, derechos, retirada del consentimiento cuando corresponda, reclamación ante la autoridad de control, obligatoriedad de facilitar datos y decisiones automatizadas. Si los datos no se obtienen directamente, debe informarse además sobre su origen y categorías.

La Guía contempla el sistema de información por capas: una primera capa con información básica y un acceso sencillo a la información ampliada. Este enfoque mejora la transparencia sin sobrecargar al participante, siempre que la información sea clara, accesible y completa.

9. Proveedores, registro y corresponsabilidad

La contratación de servicios que impliquen acceso a datos personales debe incorporar la protección de datos desde el diseño y formalizar el correspondiente acuerdo de encargo. Esto alcanza, entre otros, servicios de software, mantenimiento, análisis, almacenamiento, transcripción y destrucción documental.

Antes del tratamiento debe identificarse la actividad de investigación y documentarse: finalidad, legitimación, objeto, categorías de datos, procedencia, interesados, conservación, cesiones o transferencias internacionales, medidas de seguridad y encargados. La Guía recomienda coordinar con el DPD la inclusión de la actividad en el Registro de Actividades de Tratamiento.

Cuando varias instituciones determinen conjuntamente fines y medios, el acuerdo de corresponsabilidad debe distribuir obligaciones y responsabilidades: recogida de datos, deber de información, punto de contacto, ejercicio de derechos, seguridad, gestión de brechas, contratación de encargados, transferencias internacionales y EIPD.

10. Tratamientos especiales: menores, voz e imagen

En el marco español de la Guía, la LOPDyGDD fija con carácter general los 14 años como edad mínima para que un menor pueda consentir el tratamiento de sus datos, salvo que una norma específica exija intervención de quienes ejercen patria potestad o tutela. La investigación en salud y el uso de muestras biológicas pueden estar sujetos a reglas adicionales y más exigentes.

La voz, fotografías y grabaciones audiovisuales son datos personales y deben someterse a las mismas garantías. Debe informarse al participante y, cuando el consentimiento sea la base jurídica, conservar evidencia de su otorgamiento. Las finalidades deben distinguirse: utilizar una grabación para extraer información dentro del proyecto no equivale a publicarla en congresos, redes sociales o entregables. El acceso a audio y vídeo debe restringirse al mínimo y, si una transcripción satisface la finalidad, puede resultar apropiado destruir la grabación original.

11. Publicación, reutilización, conservación y supresión

La publicación derivada de obligaciones de transparencia debe realizarse, con carácter general, previa disociación de datos personales, salvo previsión legal específica. La información debe ser clara, estructurada, accesible y preferentemente reutilizable.

La reutilización de datos de investigación financiada públicamente debe favorecer apertura, interoperabilidad y reutilización, pero respetando propiedad intelectual e industrial, confidencialidad, seguridad y protección de datos. Para la difusión, la Guía insiste en una anonimización adecuada o, cuando no sea posible, en la seudonimización acompañada de las garantías correspondientes.

Al finalizar el plazo de conservación, los datos deben destruirse o anonimizarse. El papel debe eliminarse mediante servicios institucionales o destructoras; CD/DVD mediante destrucción física; y soportes digitales mediante borrado seguro siguiendo las indicaciones del área TIC.

Si el tratamiento cambia sustancialmente, las personas afectadas deben ser informadas. Como prevención, la Guía recomienda describir desde el inicio las finalidades con precisión pero con amplitud suficiente dentro del área científica, prever mecanismos de contacto posterior y reforzar las garantías de seguridad.

12. Conclusiones ejecutivas y prioridades de implementación

La Guía propone un modelo de gobernanza donde cumplimiento normativo, ética de investigación y ciberseguridad convergen. Para una universidad o centro de investigación, la eficacia no depende únicamente de formularios de consentimiento, sino de demostrar que los riesgos se han identificado y que las salvaguardas se aplican durante todo el ciclo de vida del dato.

Prioridad	Acción ejecutiva	Resultado esperado
1	Clasificar datos, finalidades, base jurídica y roles antes de recolectar información.	Tratamiento legítimo y trazable.
2	Aplicar minimización y	Reducción de superficie

	priorizar anonimización; usar seudonimización cuando sea necesario.	de exposición y riesgo de reidentificación.
3	Determinar tempranamente si procede una EIPD y mantenerla actualizada.	Riesgos altos identificados y mitigados antes de materializarse.
4	Implantar controles de acceso, MFA, cifrado, bloqueo, VPN y herramientas institucionales.	Protección de confidencialidad, integridad y disponibilidad.
5	Formalizar encargos y corresponsabilidades, incluidas transferencias internacionales.	Cadena de responsabilidades claramente definida.
6	Mantener un procedimiento de brechas conocido por investigadores y proveedores.	Respuesta rápida y reducción del impacto de incidentes.
7	Registrar la actividad y conservar evidencia de decisiones, controles e intervención del DPD.	Responsabilidad proactiva demostrable.
8	Definir conservación, borrado seguro, publicación y reutilización desde el diseño.	Cierre controlado del ciclo de vida del dato.

Valor para la gestión de ciberseguridad

El principal aporte de la Guía es convertir la privacidad en requisitos operativos verificables: limitar accesos, separar funciones, reducir identificadores, cifrar, autenticar, registrar, evaluar riesgos, controlar terceros y destruir información de forma segura. Estas prácticas disminuyen tanto el riesgo regulatorio como la probabilidad y el impacto de incidentes de seguridad.

En consecuencia, la protección de datos en investigación debe gestionarse como un proceso continuo. El DPD asesora y supervisa, el responsable del tratamiento toma y documenta las decisiones, el responsable de seguridad aporta el criterio técnico y el equipo investigador aplica los controles en la

práctica. La evidencia de cumplimiento es tan relevante como el cumplimiento mismo.

13. Referencia del documento base

CRUE - Secretarías Generales, Comisión Delegada del Grupo de Trabajo de Delegadas y Delegados de Protección de Datos. Guía sobre la protección de datos en los proyectos de investigación. Febrero de 2024.

Este resumen ejecutivo se ha elaborado exclusivamente a partir del documento adjunto y conserva su enfoque normativo europeo y español. No incorpora modificaciones derivadas de legislación de otros países.