ACCCF / BIBLIOTECA DE CONOCIMIENTO APLICADO

02

VOLUMEN

Privacidad aplicada, seguridad y decisiones documentadas

Edición en español · 2026

Manual de protección de datos personales y evidencia de cumplimiento

Inventario, derechos, proveedores, incidentes, conservación y eliminación verificable

Proteger a las personas mediante decisiones que puedan explicarse y comprobarse, no mediante políticas copiadas ni carpetas de documentos que nadie practica.

Para responsables de privacidad, equipos jurídicos, seguridad, tecnología, recursos humanos, dirección y proveedores que tratan información personal. Incluye una ruta de trabajo para organizaciones pequeñas y otra para operaciones complejas.

Autores: Jocsan Laguna y Jessica Matus · Consejo Americano de Ciberseguridad y Cómputo Forense

Guía técnica general y material educativo abierto. No constituye asesoría legal, dictamen pericial ni instrucción para acceder a sistemas sin autorización. Ejemplos y datos son ficticios; las figuras son reconstrucciones editoriales.

Contenido

La paginación visible corresponde a la edición PDF. Word puede actualizar este índice al abrir el documento; los títulos conservan navegación interna.

Presentación: la privacidad se demuestra en la operación 3
Capítulo 1. Inventario que permite decidir 3
1.1 Describir el tratamiento sin esconderlo detrás de una sigla 3
1.2 Encontrar las copias invisibles 4
Capítulo 2. Finalidad, fundamento y minimización 5
2.1 Separar finalidades que parecen iguales 5
2.2 La prueba del dato que sobra 5
2.3 Información y aviso comprensible 6
Capítulo 3. Derechos de las personas sin obstáculos artificiales 6
3.1 Recepción, identidad y alcance 6
3.2 Acceso sin entregar a otras personas 7
3.3 Cuando una supresión no significa destruirlo todo 7
Capítulo 4. Seguridad que puede comprobarse 7
4.1 Riesgo antes que catálogo de controles 7
4.2 Controles y evidencia de funcionamiento 8
4.3 Seudónimo no significa anónimo 8
Capítulo 5. Proveedores, nube y transferencias 9
5.1 El proveedor no absorbe la responsabilidad 9
5.2 Mapa de flujo y transferencia 9
5.3 Salida controlada y dependencia tecnológica 10
Capítulo 6. Vulneraciones: contener, comprender y notificar 10
6.1 Primeras acciones sin borrar la escena 10
6.2 Decisión de notificar y contenido útil 11
6.3 Daño, alcance y cierre 11
Capítulo 7. Conservación, eliminación y portabilidad 12
7.1 Un calendario con razones, no con caprichos 12
7.2 Portabilidad que sí pueda usarse 12
Capítulo 8. Tres recorridos completos 13
8.1 Recursos humanos: la carpeta compartida 13
8.2 Salud: el mensaje enviado al grupo equivocado 13
8.3 Analítica: el informe que volvía identificables a las personas 13
Anexo A. Equivalencias funcionales de privacidad 14
A.1 La tabla para elegir fundamento, no para traducir números 14
Anexo B. Formatos listos para adaptar 15
B.1 Registro de actividad de tratamiento 15
B.2 Ficha de solicitud de titular 15
B.3 Cronología de vulneración 16
B.4 Evaluación de proveedor 16
B.5 Constancia de eliminación o bloqueo 16
Anexo C. Glosario y control de salida 16

Presentación: la privacidad se demuestra en la operación

Una política de privacidad puede ser correcta y, aun así, la organización puede exponer todos los días información que no necesita. El cumplimiento empieza donde termina la redacción: en el formulario que pide datos de más, en la carpeta compartida con personal externo, en el proveedor que puede descargar una base completa, en la copia de seguridad que nadie sabe restaurar y en la eliminación que solo ocurre en la pantalla. La pregunta útil no es si existe un documento, sino qué sucede con una persona concreta y su información desde que se recoge hasta que deja de ser necesaria.

Este manual utiliza una unidad sencilla de trabajo: dato → finalidad → fundamento → acceso → riesgo → evidencia → destino final. Cada eslabón debe poder responderse sin recurrir a frases generales. Si un registro sirve para demostrar una venta, se identifica qué campos necesita esa finalidad, quién los administra, durante cuánto tiempo se conservan y qué otra información llegó junto con ellos. Si aparece una nueva finalidad, no basta cambiar el nombre de la carpeta: hay que revisar la licitud, la información al titular y el alcance del acceso.

La evidencia de cumplimiento tampoco es acumular capturas para aparentar trabajo. Es conservar la versión de una decisión, la fuente que la justificó, la persona que la autorizó, el control que se aplicó y el resultado de comprobarlo. Las leyes comparadas no se usan para copiar una política de otro país. Sirven para localizar la función que la organización necesita documentar: minimización, seguridad, transparencia, derechos, encargado, incidente o transferencia. El fundamento y los plazos siempre se revisan en el territorio, el sector y la fecha del tratamiento.

> **Primera decisión**
> Antes de comprar una herramienta o redactar otra política, elige un proceso real y recórrelo con datos ficticios. Si no puedes explicar qué información entra, por qué, quién la ve, dónde termina y cómo se ejerce un derecho, ahí tienes el primer trabajo concreto.

Capítulo 1. Inventario que permite decidir

1.1 Describir el tratamiento sin esconderlo detrás de una sigla

Un inventario útil no comienza con “base de datos de clientes”, porque esa etiqueta puede mezclar ventas, soporte, cobranza, mercadotecnia y selección de personal. Comienza con una actividad comprensible: registrar una compra, atender una garantía, evaluar una solicitud de empleo, pagar nómina, responder una consulta o mantener la seguridad de un edificio. Para cada actividad se anota el propósito específico, los campos necesarios, las personas comprendidas, el sistema, el custodio, el canal de entrada y la salida prevista.

La clasificación debe reflejar consecuencias, no solo sensibilidad nominal. Un nombre y un teléfono pueden ser de bajo riesgo en un directorio de contacto y de alto riesgo cuando revelan la ubicación de una persona amenazada. El expediente de una investigación puede combinar identidad, salud, situación económica, comunicaciones y terceros no relacionados. La etiqueta “confidencial” no basta: se define quién puede usarlo, con qué controles, para qué decisión y durante cuánto tiempo. El contexto puede convertir una combinación de datos aparentemente comunes en un perfil íntimo.

Campo del inventario	Pregunta operativa	Ejemplo ficticio
Actividad	¿Qué tarea concreta se realiza?	Atención de garantía de equipo comprado en línea.

Campo del inventario	Pregunta operativa	Ejemplo ficticio
Datos mínimos	¿Qué campos permiten cumplirla y cuáles son accesorios?	Pedido, contacto, domicilio de entrega y diagnóstico; no historial laboral.
Personas	¿Titulares, terceros, menores o grupos vulnerables?	Comprador, receptor del paquete y técnico asignado.
Flujo	¿De dónde llega y a quién se comunica?	Tienda → plataforma de soporte → paquetería; sin difusión pública.
Custodia y plazo	¿Quién decide y cuándo deja de ser necesario?	Responsable de posventa; plazo definido por operación y obligaciones comprobables.
Evidencia	¿Cómo se demuestra la decisión y su ejecución?	Versión del aviso, roles, bitácoras, contrato y registro de eliminación.

1.2 Encontrar las copias invisibles

El inventario debe incluir exportaciones, archivos adjuntos, papel escaneado, carpetas personales, registros de aplicaciones, copias de respaldo y servicios de terceros. La base oficial puede estar controlada mientras un archivo de Excel circula por mensajería sin propietario ni fecha de eliminación. Esa copia no deja de ser tratamiento por llamarse “temporal”. Se documenta quién la creó, por qué era necesaria, dónde quedó, quién puede abrirla y cómo se retirará cuando termine su función.

Una buena entrevista de levantamiento no se limita a preguntar qué sistema usa el área. Pide que una persona muestre una jornada completa con información ficticia: cómo llega una solicitud, qué descarga, a quién reenvía, dónde guarda notas, qué ocurre cuando hay un error y qué hace al salir de vacaciones. El mapa real aparece en las excepciones. Las contraseñas no se escriben en el inventario; se registra el mecanismo de control y su responsable.

> **Control de salida**
> Ningún proceso se cierra con “y otros datos que sean necesarios”. Se especifican los campos, la fuente, el destino y el motivo. Lo desconocido se marca para investigar, no se sustituye por una casilla tranquilizadora.



Figura 1. Del dato al destino final. Cada decisión deja una fuente y una comprobación Reconstrucción editorial; no constituye evidencia real.

Capítulo 2. Finalidad, fundamento y minimización

2.1 Separar finalidades que parecen iguales

Vender un producto, enviar publicidad y elaborar un perfil de comportamiento no son una sola finalidad. La primera puede ser necesaria para una relación; las otras necesitan su propio análisis. Cuando una organización mezcla propósitos en una frase como “fines administrativos y comerciales”, impide decidir qué datos son realmente necesarios y qué comunicaciones deben explicarse por separado. El registro debe conservar esa separación para que una persona pueda rechazar un uso sin perder indebidamente el servicio esencial.

El consentimiento es una posible base, no una llave universal. Puede existir obligación legal, ejecución de una relación, ejercicio de funciones públicas, defensa de derechos u otro supuesto previsto en la jurisdicción. Se identifica la regla concreta antes de elegir un formulario. Pedir consentimiento para todo puede trasladar falsamente la responsabilidad a la persona y volver confusa una operación que ya tiene otro fundamento. Si el tratamiento cambia, se revisa la compatibilidad, la información y los controles antes de ejecutarlo.

México contiene principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; Colombia desarrolla legalidad, finalidad, libertad, calidad, transparencia, acceso restringido, seguridad y confidencialidad; Ecuador exige responsabilidad proactiva y demostrada. La semejanza de principios ayuda a construir un método, pero cada supuesto y excepción debe leerse en la norma y el sector aplicables.[1][2][3]

2.2 La prueba del dato que sobra

Toma un campo y elimínalo del ejemplo ficticio. Si la actividad puede cumplirse sin él, necesitas justificar por qué se pide. El criterio no es si puede resultar interesante en el futuro, sino si es adecuado y necesario para la finalidad actual. Un teléfono puede bastar para avisar una entrega; no hace falta una copia de identificación si la identidad puede verificarse por un medio menos intrusivo. Para un análisis estadístico, quizá no sea necesario conservar el nombre junto con el resultado.

Situación	Decisión de minimización	Registro que evita improvisar
Soporte de una compra	Pedido y canal de contacto, no expediente completo del cliente.	Campos aprobados y captura del formulario vigente.
Validación de identidad	Elegir el método menos invasivo que alcance la seguridad requerida.	Alternativas evaluadas, riesgo y aprobación.
Informe agregado	Quitar identificadores y revisar combinaciones reidentificables.	Prueba de grupos pequeños y supresión aplicada.
Consulta de terceros	Separar datos del solicitante de datos de otras personas.	Versión entregada y revisión previa de contenido.
Nueva finalidad	Detener hasta revisar compatibilidad y fundamento.	Solicitud, análisis y autorización fechada.

[1]México. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, texto publicado el 20-03-2025 y reforma del 14-11-2025. Artículos 5–9, 18–20 y 31: principios, seguridad, confidencialidad, vulneraciones y atención de derechos. La autoridad federal actual es la Secretaría Anticorrupción y Buen Gobierno. Fuente oficial en línea

[2]Colombia. Ley Estatutaria 1581 de 2012, artículos 4, 8, 12, 17–18 y 26: principios, derechos, información, deberes de responsables y encargados, y transferencia a terceros países. Fuente oficial en línea

[3]Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artículos 10, 37–44: principios, medidas de seguridad, protección desde el diseño, riesgos y tratamiento ante incidentes. Fuente oficial en línea

2.3 Información y aviso comprensible

El aviso de privacidad debe permitir que la persona reconozca quién decide, para qué usa sus datos, con quién los comparte, cómo ejerce sus derechos y dónde plantea una duda. Un texto extenso no sustituye una explicación oportuna. Se conserva la versión efectivamente presentada y el contexto: página, fecha, flujo, idioma y cambios. Si el sitio cambia, no se borra la versión anterior del registro de cumplimiento.

En Argentina se informa previamente la finalidad, los destinatarios o clases de destinatarios, el responsable y la posibilidad de ejercer derechos. En Colombia existe deber de información clara y expresa al solicitar autorización, y conservación de prueba de su cumplimiento. Son ejemplos de por qué la evidencia debe unir texto y contexto: una URL actual no demuestra qué vio la persona años atrás.[4][5]

> **Caso ficticio: la promoción que pedía un expediente**
> Un comercio solicita identificación oficial, estado civil y domicilio para entregar un cupón digital. El análisis termina con una versión que pide correo, consentimiento para publicidad separado y ninguna copia de identidad. Se documenta qué datos dejaron de recogerse y qué hace la organización con las copias ya recibidas. Mejorar el formulario no autoriza a olvidar el pasado.

Capítulo 3. Derechos de las personas sin obstáculos artificiales

3.1 Recepción, identidad y alcance

El canal de derechos necesita un registro con fecha, solicitante aparente, tipo de petición, alcance, responsable, plazo aplicable y estado. La identidad se comprueba con proporcionalidad: exigir un expediente excesivo para cualquier solicitud puede convertirse en una barrera y generar otra exposición. Se revisa qué información ya tiene la organización para autenticar la petición, qué riesgo habría al entregar a otra persona y qué alternativas de verificación ofrece el canal.

Después se delimita qué pide realmente la persona: conocer si existe tratamiento, obtener una copia, corregir un dato, oponerse a publicidad, suprimir, bloquear, revocar, portar o expresar una queja. No se transforma toda petición en eliminación total ni se contesta “no procede” sin explicar el motivo y la vía de revisión. Si la respuesta contiene terceros, se prepara una entrega que preserve sus derechos sin inventar una supresión de hechos del expediente original.

Etapa	Qué se documenta	Error que evita
Recepción	Canal, fecha y zona, contenido literal y acuse.	Medir el plazo desde que alguien decidió revisar el correo.
Identidad	Método elegido, riesgo y datos utilizados, sin secretos en la ficha.	Crear una nueva copia de identidad innecesaria.
Localización	Sistemas, respaldos, encargados y criterios de búsqueda.	Responder solo desde la base principal.
Decisión	Fundamento, exclusiones, revisión y datos entregados.	Enviar información de terceros o negar sin razón.

[4] Argentina. Ley 25.326, texto actualizado. Artículos 4–6, 9–10, 14–16 y 25: calidad, información, seguridad, confidencialidad, derechos de titulares y prestación de servicios de tratamiento por cuenta de terceros. Fuente oficial en línea

[5] Colombia. Ley Estatutaria 1581 de 2012, artículos 4, 8, 12, 17–18 y 26: principios, derechos, información, deberes de responsables y encargados, y transferencia a terceros países. Fuente oficial en línea

Etapa	Qué se documenta	Error que evita
Cierre	Fecha, canal, evidencia de entrega y acciones en sistemas.	Marcar como resuelta sin ejecutar el cambio.

3.2 Acceso sin entregar a otras personas

Una exportación puede contener datos de empleados, clientes, familiares o participantes de una conversación. El derecho de acceso no autoriza automáticamente a revelarlos. Se revisan campos, identificadores, contenido, adjuntos y metadatos; se utiliza una versión de entrega separada del original preservado. La revisión no debe modificar el significado ni ocultar información que sí pertenece al solicitante.

En Argentina, la información debe ser clara, amplia y no revelar datos de terceros aunque estén vinculados con el interesado. La rectificación, actualización o supresión tiene reglas y plazos propios, además de excepciones cuando existe obligación de conservar o derechos de terceros. No se copia ese plazo a otro país: se registra el régimen aplicable al caso.[6]

3.3 Cuando una supresión no significa destruirlo todo

Puede coexistir una petición de eliminación con una obligación de conservación o con la defensa de un derecho. La respuesta distingue qué tratamiento cesa, qué registro se bloquea, qué copia se conserva restringida y con qué fundamento. Se ejecutan acciones en los sistemas y con los encargados, no solamente en el texto de respuesta. Si una base se conserva para defensa, se limita su uso a esa finalidad y se controla el acceso posterior.

> **Ejemplo ficticio**
> Una persona pide eliminar toda su información tras cerrar su cuenta. La organización retiene el comprobante fiscal necesario, bloquea su perfil de mercadotecnia, elimina atributos de segmentación y documenta la lista de sistemas donde ejecutó cada medida. La respuesta explica lo eliminado, lo bloqueado y lo conservado, sin afirmar que todo desapareció.

Capítulo 4. Seguridad que puede comprobarse

4.1 Riesgo antes que catálogo de controles

El análisis parte de las personas y del daño posible, no de una lista de productos. Se identifica quién podría acceder, qué error es plausible, qué copia es más expuesta y qué consecuencia tendría la alteración, pérdida, indisponibilidad o divulgación. Luego se seleccionan controles de acceso, cifrado, registro, segregación, respaldo, formación y revisión. Un control costoso puede ser desproporcionado para un directorio público e insuficiente para un archivo clínico.

Ecuador exige analizar riesgos, amenazas y vulnerabilidades considerando el tratamiento, las personas y las categorías y volumen de datos. La Unión Europea pide medidas técnicas y organizativas apropiadas al riesgo, con protección desde el diseño y por defecto. El registro de esa evaluación es más útil que afirmar

[6] Argentina. Ley 25.326, texto actualizado. Artículos 4–6, 9–10, 14–16 y 25: calidad, información, seguridad, confidencialidad, derechos de titulares y prestación de servicios de tratamiento por cuenta de terceros. Fuente oficial en línea

"contamos con los más altos estándares", porque permite explicar por qué se eligió cada medida y qué riesgo residual aceptó la organización.[78]

4.2 Controles y evidencia de funcionamiento

Control	Prueba con información ficticia	Evidencia conservada
Mínimo privilegio	Un usuario de soporte no puede abrir nómina ni descargar toda la base.	Rol, autorización, resultado de intento y revisión de accesos.
Cifrado y llaves	Se cifra una copia y solo un rol autorizado puede recuperarla.	Configuración, responsables, recuperación y ausencia de llaves en el acta.
Registros	Una acción de prueba genera evento con usuario, fecha, zona y objeto.	Exportación nativa, diccionario, retención y revisión.
Respaldo	Se restaura un conjunto ficticio en entorno aislado.	Fecha, duración, incidencias, hash y validación de apertura.
Salida de personal	Se retira acceso y se comprueba que ya no opera.	Fecha de baja, sistemas revisados y responsable.
Anonimización	Se intenta identificar registros por combinaciones y valores extremos.	Método, riesgo residual, prueba y aprobación de difusión.

La evidencia debe demostrar funcionamiento, no solo existencia. Una captura de una consola cifrada no demuestra que todas las copias estén protegidas; una política de contraseñas no prueba que los privilegios se revisen; una carpeta denominada "respaldo" no acredita recuperación. La prueba se diseña con datos ficticios para no crear una vulneración mientras se evalúa otra. Si un acceso inesperado sí funciona, se conserva el evento y se corrige antes de publicar el informe.

4.3 Seudónimo no significa anónimo

Sustituir nombres por folios reduce exposición directa, pero la identidad puede regresar al combinar fecha, domicilio, puesto, aficiones o una operación singular. La seudonimización conserva posibilidad de asociación mediante información adicional; la anonimización exige un análisis de reidentificación en el contexto real de difusión. El expediente debe separar la versión de trabajo de la versión pública y proteger la tabla de correspondencia con controles distintos.

Antes de compartir un conjunto, revisa grupos pequeños, valores únicos, archivos adjuntos, coordenadas, secuencias y metadatos. Un testimonio sin nombre puede seguir identificando a una persona por el pueblo y el cargo. En ese caso se generaliza, se suprime o no se publica. No se anuncia anonimidad perfecta: se documenta método, supuestos, riesgo residual y revisión si el contexto cambia.

> **Regla práctica**
> No demuestres la eficacia de una anonimización con la pregunta "¿veo un nombre?". Pregunta qué otra fuente puede combinar alguien razonablemente y qué persona quedaría identificada por una característica poco común.

[7] Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artículos 10, 37–44: principios, medidas de seguridad, protección desde el diseño, riesgos y tratamiento ante incidentes. Fuente oficial en línea

[8] Unión Europea. Reglamento (UE) 2016/679, artículos 5, 25, 28 y 32–34: principios, protección desde el diseño, encargados, seguridad y notificación/comunicación de violaciones de seguridad. España exige revisar además la legislación nacional y sectorial aplicable. Fuente oficial en línea

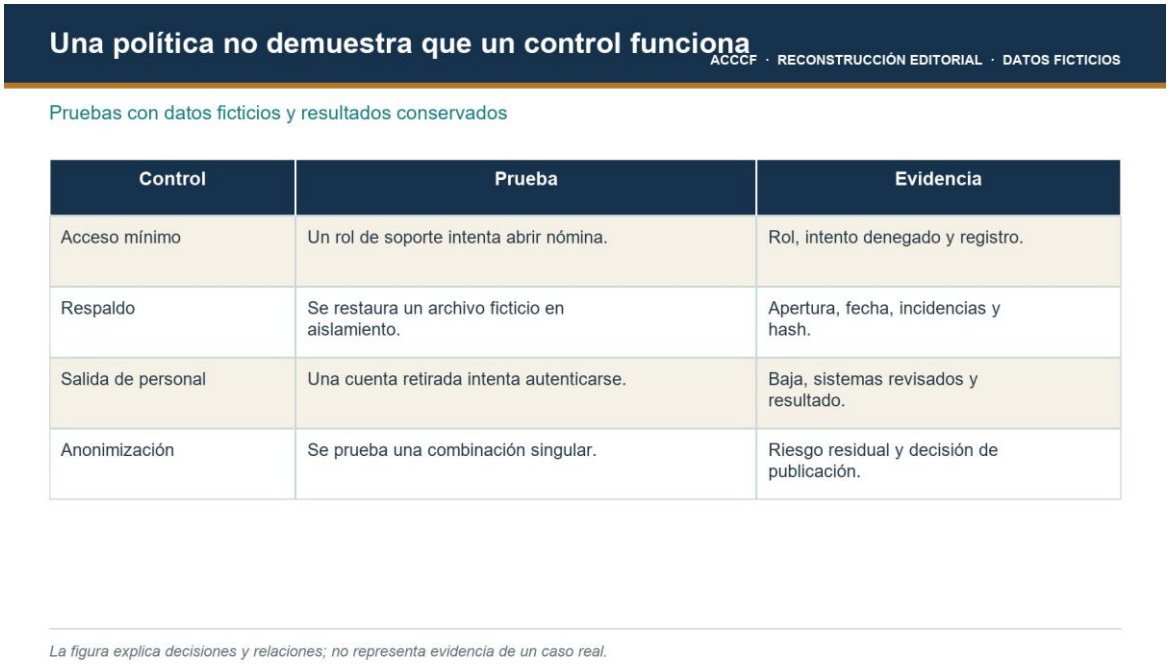


Figura 2. Una política no demuestra que un control funciona. Pruebas con datos ficticios y resultados conservados Reconstrucción editorial; no constituye evidencia real.

Capítulo 5. Proveedores, nube y transferencias

5.1 El proveedor no absorbe la responsabilidad

Cuando un proveedor trata datos por cuenta de la organización, se definen instrucciones, finalidad, personal autorizado, ubicación, subcontratistas, confidencialidad, medidas de seguridad, apoyo ante incidentes, atención de derechos, devolución, eliminación y evidencia disponible para revisión. Firmar un contrato no basta: hay que saber qué botón puede descargar la base, quién puede restaurarla y dónde están los registros de acceso.

En Argentina, quien presta servicios informatizados por cuenta de terceros no puede aplicar los datos a un fin distinto del contrato ni cederlos para conservación; al cumplir la prestación se aplica el régimen de destrucción o conservación autorizada previsto por la ley. En Colombia se diferencian responsable y encargado y se atribuyen deberes específicos a ambos. La clasificación contractual debe corresponder a lo que realmente decide cada parte, no al nombre comercial del servicio.[9][10]

5.2 Mapa de flujo y transferencia

Una nube puede tener administración en un país, almacenamiento en otro, soporte en un tercero y respaldos en varios. El mapa registra esas rutas, la entidad que decide, los encargados, los subencargados, la razón de cada acceso y la garantía o mecanismo que la legislación exige. “El servidor está en la nube” no describe ubicación ni riesgo. La transferencia internacional no se reduce a copiar una cláusula: exige verificar ámbito, excepciones, destinatario y controles.

Pregunta al proveedor	Respuesta documentada esperada	Señal de alerta
¿Quién puede acceder?	Roles, ubicación, autenticación, registro y revisión.	“Soporte global” sin personas ni condiciones.

[9] Argentina. Ley 25.326, texto actualizado. Artículos 4–6, 9–10, 14–16 y 25: calidad, información, seguridad, confidencialidad, derechos de titulares y prestación de servicios de tratamiento por cuenta de terceros. Fuente oficial en línea

[10] Colombia. Ley Estatutaria 1581 de 2012, artículos 4, 8, 12, 17–18 y 26: principios, derechos, información, deberes de responsables y encargados, y transferencia a terceros países. Fuente oficial en línea

Pregunta al proveedor	Respuesta documentada esperada	Señal de alerta
¿Qué subencargados intervienen?	Identidad, función, ubicación y mecanismo de cambio.	Lista secreta o cambios sin aviso.
¿Cómo ayuda con derechos?	Consulta, corrección, bloqueo, exportación y plazos.	Solo ofrece PDF sin búsqueda ni filtros.
¿Cómo entrega incidentes?	Canal, contacto, cronología, evidencia y actualizaciones.	Notificación oral sin registro.
¿Cómo termina la relación?	Exportación, legibilidad, eliminación, respaldos y constancia.	Cierre de cuenta sin recuperación de información.

5.3 Salida controlada y dependencia tecnológica

Antes de contratar, se prueba la salida con datos ficticios. Se descarga una exportación, se abre en una herramienta independiente y se revisa si conserva campos, zona, relaciones y diccionario. Si la plataforma solo permite imprimir, el riesgo de dependencia se declara. La salida también comprende eliminación en producción, copias de prueba, respaldos y registros; algunos componentes pueden conservarse por obligación o seguridad, pero deben quedar delimitados.

> **Caso ficticio**
> Una organización cambia de proveedor de encuestas. La exportación contiene respuestas, pero no identificadores de formularios ni zona horaria. Se solicita una nueva entrega con diccionario, se conservan ambas como objetos distintos y se registra la limitación de la primera. Al final se elimina la cuenta y se obtiene constancia del alcance real de esa acción.

Capítulo 6. Vulneraciones: contener, comprender y notificar

6.1 Primeras acciones sin borrar la escena

El primer objetivo es proteger a las personas y limitar el daño sin destruir la información que explica el incidente. Se registra cuándo se detectó, quién lo reportó, qué sistemas parecen afectados, qué datos podrían estar involucrados y qué acciones ya ocurrieron. Las contraseñas se cambian por un canal seguro, pero se preservan antes los eventos de acceso relevantes. La restauración no se utiliza para borrar evidencia ni para afirmar prematuramente que todo terminó.

NIST SP 800-61 Rev. 3 integra respuesta en preparación, detección, respuesta, recuperación y mejora continua. Eso evita una lectura estrecha: no hay incidente solo cuando se “apaga el servidor”; hay que comprender alcance, comunicación, efectos en personas y cambios posteriores. En una vulneración de datos también se conserva qué campos se expusieron, con qué precisión y qué copias pudo obtener un tercero.[11][12]

Momento	Acción documentada	No hacer por reflejo
Detección	Registrar señal, fuente, hora, responsable y primer alcance.	Declarar causa raíz por la primera sospecha.

[11] NIST SP 800-61 Rev. 3 (abril de 2025). Recomendaciones de respuesta a incidentes integradas en CSF 2.0: preparación, detección, respuesta, recuperación y mejora. Sustituye la revisión 2. Fuente oficial en línea

[12] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Guía metodológica, no legislación ni garantía de admisibilidad. Fuente oficial en línea

Momento	Acción documentada	No hacer por reflejo
Contención	Elegir medida proporcional y anotar evidencia previa.	Restablecer equipos o eliminar cuentas sin exportar registros.
Evaluación	Identificar datos, titulares, acceso, uso y consecuencias plausibles.	Confundir número de filas con número de personas.
Notificación	Aplicar sujeto, umbral, destinatario, contenido y plazo local.	Copiar 72 horas o 48 horas en todo país y sector.
Recuperación	Verificar control, monitoreo, apoyo a afectados y cambios.	Cerrar con una carpeta nueva y ninguna lección.

6.2 Decisión de notificar y contenido útil

La notificación depende de la legislación aplicable, el tipo de organización, la naturaleza y gravedad del incidente y las personas afectadas. En México la ley vigente en 2026 exige informar de inmediato las vulneraciones significativas a los afectados para que puedan defender sus derechos. En Perú, el Reglamento aprobado en 2024 introduce reporte oportuno de incidentes a la autoridad y comunicación a afectados según exposición; la fuente oficial señala 48 horas en principio, salvo motivos fundados. En la Unión Europea, los artículos 33 y 34 distinguen notificación a la autoridad y comunicación al interesado según riesgo. No son reglas intercambiables.[13][14][15]

Un aviso útil explica qué ocurrió dentro de lo conocido, qué categorías de datos podrían estar afectadas, qué se está haciendo, qué medidas razonables puede adoptar la persona y dónde obtener información. No se incluyen secretos ni una versión especulativa del atacante. Si los hechos cambian, se actualiza el aviso y se conserva el historial. Ocultar un incidente para proteger la reputación puede multiplicar el daño que se pretendía evitar.

6.3 Daño, alcance y cierre

La evaluación considera posibilidad de uso, confidencialidad de las credenciales, facilidad de contacto, vulnerabilidad de las personas, publicidad del acceso y efectos físicos, económicos o discriminatorios. “Solo fueron nombres” puede ser grave si se vinculan con un centro de atención sensible. La evidencia se recoge sin volver a descargar la filtración desde un enlace público ni distribuirla al equipo entero.

> **Cierre real**
> El incidente no termina cuando se restablece el sistema. Termina con personas informadas según corresponda, controles comprobados, accesos revisados, evidencia preservada y una modificación del proceso que evite la misma secuencia. Si algo sigue desconocido, el informe lo conserva como límite.

[13] México. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, texto publicado el 20-03-2025 y reforma del 14-11-2025. Artículos 5–9, 18–20 y 31: principios, seguridad, confidencialidad, vulneraciones y atención de derechos. La autoridad federal actual es la Secretaría Anticorrupción y Buen Gobierno. Fuente oficial en línea

[14] Perú. Ley 29733 y su Reglamento aprobado por DS 016-2024-JUS. Principios de finalidad, proporcionalidad, seguridad y confidencialidad; el nuevo Reglamento desarrolla incidentes, evaluación preventiva y funciones progresivas del oficial de datos. Fuente oficial en línea

[15] Unión Europea. Reglamento (UE) 2016/679, artículos 5, 25, 28 y 32–34: principios, protección desde el diseño, encargados, seguridad y notificación/comunicación de violaciones de seguridad. España exige revisar además la legislación nacional y sectorial aplicable. Fuente oficial en línea



Figura 3. Vulneración: contener sin borrar la explicación. La cronología guía la respuesta y la notificación Reconstrucción editorial; no constituye evidencia real.

Capítulo 7. Conservación, eliminación y portabilidad

7.1 Un calendario con razones, no con caprichos

La retención se define por finalidad, obligación jurídica, contrato, defensa de derechos y necesidad operativa. No hay una cifra universal para “datos personales”. Se distingue el plazo de uso ordinario del bloqueo restringido y de la conservación probatoria. Cuando cambia el propósito, se revisa el calendario. Guardar todo por si acaso multiplica exposición y hace más difícil responder con precisión a una solicitud.

La eliminación debe abarcar sistemas, exportaciones, usuarios, proveedores y copias disponibles. Los respaldos pueden tener un ciclo técnico distinto: se documenta si se eliminan, sobrescriben o mantienen inaccesibles hasta expirar. Si una restauración puede reintroducir datos eliminados, el procedimiento incluye cómo volver a suprimirlos. No se crea una constancia que diga más de lo que técnicamente ocurrió.

7.2 Portabilidad que sí pueda usarse

Entregar datos no equivale a imprimirlos. Cuando existe derecho de portabilidad o una necesidad de migración, se revisa alcance, formato estructurado, lectura mecánica, interoperabilidad, campos, fechas y vínculos entre tablas. La exportación se prueba con un receptor ficticio, sin exponer información de terceros ni secretos. El EML puede preservar el contexto de entrega y los hashes permiten comparar el archivo transmitido con el recibido; ninguno certifica que el contenido sea completo por sí solo.[16][17]

Acción	Evidencia útil	Límite declarado
Eliminar perfil	Identificador, sistema, fecha, operador y comprobación de ausencia.	Copias técnicas pendientes y fecha de expiración.

[16]RFC Editor. RFC 5322, Internet Message Format: estructura del mensaje, encabezados y cuerpo. Es una referencia técnica para preservar y comprender correo electrónico, no una prueba automática de identidad humana. Fuente oficial en línea

[17]Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artículos 10, 37–44: principios, medidas de seguridad, protección desde el diseño, riesgos y tratamiento ante incidentes. Fuente oficial en línea

Acción	Evidencia útil	Límite declarado
Bloquear por conservación	Motivo, acceso restringido y propósito residual.	No usar para publicidad o analítica ordinaria.
Exportar	Formato nativo, diccionario, filtros, filas, zona y hash.	Cobertura de la consulta y datos excluidos.
Devolver a encargado	Inventario, canal, receptor y verificación de descarga.	Copias restantes bajo control del encargado.
Restaurar respaldo	Prueba en entorno aislado y lista de reaplicación de supresiones.	No afirmar eliminación si el ciclo aún no termina.

La constancia correcta

"Se eliminó el perfil del sistema de mercadotecnia y se comprobó su ausencia el 10 de noviembre de 2026. El respaldo cifrado conserva el ciclo documentado hasta su expiración; si se restaura, se reaplica la supresión." Eso es más riguroso que "toda la información fue destruida".

Capítulo 8. Tres recorridos completos

8.1 Recursos humanos: la carpeta compartida

Una empresa ficticia conserva currículos en una carpeta de acceso general. El recorrido detecta datos de familiares, referencias, documentos y evaluaciones sin plazo. Se decide separar expedientes activos, rechazados y conservación justificada; restringir roles; retirar enlaces públicos; registrar accesos y ejecutar eliminación en exportaciones. Una persona solicita acceso y recibe sus datos sin información de los evaluadores que no corresponde entregar. El cambio se prueba con una cuenta de prueba, no con la curiosidad sobre un expediente real.

8.2 Salud: el mensaje enviado al grupo equivocado

Una clínica ficticia envía una tabla con nombres y diagnósticos a un grupo externo. Se pide dejar de difundirla y eliminarla sin reenviarla al equipo completo; se registran destinatarios, contenido y posibilidad de copia. Se revisan accesos, contactos y el procedimiento de selección de destinatarios. La evaluación de notificación considera sensibilidad y consecuencias, no únicamente cantidad de filas. El cambio final incluye revisión de destinatario, controles de exportación y un ejercicio práctico.

8.3 Analítica: el informe que volvía identificables a las personas

Un equipo publica un conjunto seudonimizado con zona, fecha y una compra excepcional. Un lector puede enlazarla con una publicación previa y reconocer al cliente. Se retira la difusión, se revisan grupos pequeños y se suprimen valores singulares. La nueva versión conserva utilidad estadística sin identificadores directos y declara sus límites. El caso recuerda que una anonimización defectuosa puede ser una nueva vulneración creada por el propio intento de informar.

Método compartido

Los tres casos se resuelven con la misma secuencia: ubicar datos y copias, limitar acceso y difusión, entender consecuencias, decidir comunicación, ejecutar controles y conservar evidencia. Cambian las personas y la tecnología, no la disciplina.

Anexo A. Equivalencias funcionales de privacidad

Revisión documental al 10 de noviembre de 2026. Las funciones comparadas no implican idéntico alcance, fundamento, plazo ni efecto. Los artículos se citan para localizar el régimen, no para resolver automáticamente un expediente. En Chile se señala expresamente la vigencia diferida del nuevo régimen para no presentarlo como aplicable antes de tiempo.

Jurisdicción	Funciones localizadas	Precaución operativa
México	LFPDPPP: principios, seguridad, confidencialidad, derechos y aviso de vulneraciones significativas.	Ley nueva de 2025 y autoridad federal actual; revisar sector y reforma.
Perú	Ley 29733 y Reglamento DS 016-2024-JUS: principios, seguridad, incidentes, prevención y roles progresivos.	El Reglamento tiene transición y detalles propios; no copiar plazos europeos.
Chile	Ley 21.719 modifica la Ley 19.628: principios, derechos, seguridad, responsabilidad y Agencia.	Nuevo régimen con inicio diferido al 01-12-2026; revisar norma aplicable a la fecha.
Argentina	Ley 25.326: calidad, consentimiento, información, seguridad, derechos y servicios por cuenta de terceros.	No reducir derechos a un formulario genérico ni revelar datos de terceros.
Colombia	Ley 1581: principios, categorías, derechos, información, responsables, encargados y transferencias.	Revisar exclusiones, reglas especiales y deberes concretos de cada rol.
Ecuador	LOPDP: principios, seguridad, riesgo, diseño y defecto, incidentes y derechos.	El acceso para respuesta no autoriza tratamiento ilimitado ni conservación eterna.
España / UE	RGPD: principios, diseño, encargados, seguridad y violaciones; complemento nacional y sectorial.	Distinguir riesgo para autoridad y alto riesgo para interesado; revisar LOPDGDD y sector.

Fuentes de la tabla: [18][19][20][21][22][23][24]

A.1 La tabla para elegir fundamento, no para traducir números

Para un caso se escribe primero la función necesaria: recoger un dato, cambiar finalidad, contratar un encargado, transferir fuera del territorio, responder un derecho, notificar un incidente o suprimir. Después se consulta el instrumento aplicable con artículo, materia, sujeto, fecha y excepciones. Si una regla cubre solo sector público, financiero o sanitario, no se convierte en norma universal. Si no se comprobó una excepción, no se inventa una respuesta.

[18] México. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, texto publicado el 20-03-2025 y reforma del 14-11-2025. Artículos 5–9, 18–20 y 31: principios, seguridad, confidencialidad, vulneraciones y atención de derechos. La autoridad federal actual es la Secretaría Anticorrupción y Buen Gobierno. Fuente oficial en línea

[19] Perú. Ley 29733 y su Reglamento aprobado por DS 016-2024-JUS. Principios de finalidad, proporcionalidad, seguridad y confidencialidad; el nuevo Reglamento desarrolla incidentes, evaluación preventiva y funciones progresivas del oficial de datos. Fuente oficial en línea

[20] Chile. Ley 21.719, que modifica la Ley 19.628 sobre protección de datos personales. La versión con el nuevo régimen tiene inicio de vigencia diferido al 01-12-2026; antes de esa fecha debe revisarse la norma entonces aplicable y no anticipar obligaciones futuras como vigentes. Fuente oficial en línea

[21] Argentina. Ley 25.326, texto actualizado. Artículos 4–6, 9–10, 14–16 y 25: calidad, información, seguridad, confidencialidad, derechos de titulares y prestación de servicios de tratamiento por cuenta de terceros. Fuente oficial en línea

[22] Colombia. Ley Estatutaria 1581 de 2012, artículos 4, 8, 12, 17–18 y 26: principios, derechos, información, deberes de responsables y encargados, y transferencia a terceros países. Fuente oficial en línea

[23] Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artículos 10, 37–44: principios, medidas de seguridad, protección desde el diseño, riesgos y tratamiento ante incidentes. Fuente oficial en línea

[24] Unión Europea. Reglamento (UE) 2016/679, artículos 5, 25, 28 y 32–34: principios, protección desde el diseño, encargados, seguridad y notificación/comunicación de violaciones de seguridad. España exige revisar además la legislación nacional y sectorial aplicable. Fuente oficial en línea

Las reglas de documento electrónico de los siete sistemas ayudan a conservar evidencia de decisiones: reconocimiento, atribución, integridad, original, accesibilidad y conservación. Pero una firma, sello o hash no legaliza un tratamiento ilícito ni prueba que la persona comprendió un aviso. Se evalúan por separado privacidad, integridad del registro y veracidad del contenido.[25][26][27][28][29][30][31]

Anexo B. Formatos listos para adaptar

B.1 Registro de actividad de tratamiento

Campo	Contenido mínimo	Control de aceptación
Actividad y responsable	Tarea concreta, dueño del proceso y suplencia.	Otra persona puede ubicar quién decide.
Finalidad y fundamento	Propósito específico, base y excepción si existe.	No usa “gestión” como respuesta completa.
Datos y personas	Campos, sensibilidad, terceros y grupos de atención prioritaria.	Cada campo tiene necesidad explicada.
Flujo y encargados	Entrada, sistemas, accesos, transferencias y destino.	Incluye exportaciones y respaldo.
Retención y derechos	Plazo, bloqueo, eliminación y canal de atención.	No hay “indefinido” sin razón.
Riesgo y controles	Daño plausible, medidas, prueba y riesgo residual.	Existe evidencia de funcionamiento.

B.2 Ficha de solicitud de titular

Formato ficticio para registro interno

```
ID: PRIV-DEMO-2026-001
Recepción: [fecha, hora, zona, canal]
Solicitud literal: [acceso, rectificación, supresión, oposición, otra]
Identidad: [método proporcional; no incluir documentos en esta ficha]
Ámbito: [período, sistemas, personas y exclusiones]
Plazo aplicable: [norma, artículo, inicio y vencimiento]
Búsqueda: [sistemas, filtros, encargados y respaldos]
Decisión: [fundamento, revisión, datos de terceros]
Acciones ejecutadas: [sistema, fecha, operador, comprobación]
Entrega: [formato, canal, receptor, fecha y verificación]
Pendientes y límites: [qué no se resolvió y por qué]
```

[25] Código de Comercio de México, artículos 89–94 y 1205: neutralidad, atribución, escrito, original, integridad, accesibilidad y admisión de mensajes de datos. Compilación oficial. Fuente oficial en línea

[26] Colombia. Ley 527 de 1999, artículos 5–13, 16–25 y 28: mensajes de datos, escrito, original, integridad, admisibilidad, conservación, envío, recepción y firma digital. Fuente oficial en línea

[27] Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, artículos 2, 6–8, 10–16: equivalencia, escrito, original, conservación, procedencia, envío, recepción y firma electrónica. Fuente oficial en línea

[28] Reglamento (UE) 910/2014 eIDAS, artículos 25–26 y 46: no discriminación de firmas electrónicas y documentos por su formato, firma avanzada y efectos de firma cualificada. Fuente oficial en línea

[29] Argentina. Ley 25.506 de Firma Digital, artículos 1 y 5–9: documento digital, carga al invocar firma electrónica desconocida y presunciones delimitadas. Fuente oficial en línea

[30] Chile. Ley 19.799 sobre documentos electrónicos y firma electrónica, artículos 1–5: equivalencia, escrito, firma simple/avanzada, fecha y valor probatorio. Fuente oficial en línea

[31] Perú. Reglamento de la IOFE, DS 052-2008-PCM, artículos 3 y 4: exigencia y admisión de documentos electrónicos firmados digitalmente. Fuente oficial en línea

B.3 Cronología de vulneración

Evento	Registro obligatorio	Decisión asociada
Señal inicial	Fuente, valor literal, zona, responsable y evidencia.	Abrir expediente y preservar.
Contención	Medida, autoridad, alcance, efecto y evidencia previa.	Limitar daño sin borrar contexto.
Alcance	Datos, personas, acceso, copias, uso y dudas.	Clasificar riesgo con hechos.
Comunicaciones	Destinatario, contenido, canal, hora y versión.	Cumplir régimen local sin revelar más.
Recuperación	Restauración, accesos, monitoreo y pruebas.	Comprobar que el control funciona.
Mejora	Causa, cambio de proceso, responsable y validación.	Evitar repetición, no solo cerrar.

B.4 Evaluación de proveedor

Lista de verificación antes de activar datos reales

```
1. Rol de cada parte y finalidad contractual.
2. Datos mínimos, ubicación, personas autorizadas y subencargados.
3. Autenticación, mínimo privilegio, registros, cifrado y llaves.
4. Evidencia de seguridad verificable, no solo declaración comercial.
5. Canal de incidentes, contenido y prueba de comunicación.
6. Apoyo a derechos, búsquedas y exportaciones nativas.
7. Transferencias, garantías y cambios de ubicación.
8. Salida: formato, diccionario, accesibilidad y prueba de apertura.
9. Eliminación, respaldos y constancia con límites.
10. Revisión periódica y responsable interno.
```

B.5 Constancia de eliminación o bloqueo

Ejemplo ficticio

```
Objeto: EXP-DEMO-2026-001
Alcance: perfil de mercadotecnia y exportación de campaña
Acción: supresión del perfil activo y bloqueo del comprobante exigido
Sistemas: [nombre, versión, ubicación y responsable]
Ejecución: [fecha, zona, operador y método]
Comprobación: [consulta, ausencia, acceso y resultado]
Respaldo: [ciclo, acceso y reaplicación si se restaura]
Encargados: [notificación y respuesta]
Conservación residual: [fundamento, finalidad y plazo]
Límite: [qué no puede afirmarse]
Revisión: [persona, fecha y evidencia enlazada]
```

Anexo C. Glosario y control de salida

Término	Uso práctico en este manual
Responsable	Quién decide sobre la base y el tratamiento dentro del régimen aplicable.
Encargado	Quién trata por cuenta del responsable, con instrucciones y deberes propios.
Seudonimización	Asociación posible con información adicional; requiere separación y control.
Anonimización	Imposibilidad razonable de asociar en el contexto; necesita prueba y revisión.
Bloqueo	Restricción del tratamiento sin borrar el objeto por una razón justificada.

Término	Uso práctico en este manual
Portabilidad	Entrega estructurada e interoperable dentro del alcance permitido.
Vulneración	Incidente que afecta seguridad de datos personales; su gravedad se evalúa.
Evidencia de cumplimiento	Registro que permite revisar decisión, ejecución y resultado, no solo intención.

Antes de cerrar un proceso	Respuesta exigida
¿Qué datos y copias existen?	Inventario incluidos archivos, respaldos y proveedores.
¿Por qué cada campo es necesario?	Finalidad, fundamento y minimización documentados.
¿Quién puede acceder y con qué prueba?	Roles, registros y prueba con datos ficticios.
¿Cómo ejerce derechos una persona?	Canal, búsqueda, decisión, entrega y ejecución.
¿Qué pasa en incidente o salida?	Cronología, comunicación, exportación y eliminación verificadas.
¿Qué sigue sin saberse?	Límite expreso, responsable y siguiente comprobación.

Cierre

Proteger datos es reducir la posibilidad de que una decisión organizacional se convierta en daño para una persona. La evidencia existe para revisar ese cuidado y corregirlo, no para convertirlo en apariencia administrativa.