BIBLIOTECA
ACCCF

12
VOLUMEN

ACCCF / CONOCIMIENTO APLICADO

Manual de análisis de redes de bots, perfiles falsos y daño mediático

Conservación, cronología, indicadores, grafos, hipótesis alternativas e informe técnico

Analizar conducta coordinada sin convertir una coincidencia en prueba de automatización, una relación de cuentas en prueba de titularidad ni una opinión impopular en prueba de delito.

Coordinación editorial · Jocsan Laguna

Consejo Americano de Ciberseguridad y Cómputo Forense · 2026

Guía técnica general. Ejemplos y cifras de demostración son ficticios.

Contenido

Índice navegable. Los títulos enlazan a su ubicación dentro del documento.

Presentación: muchas cuentas no son una sola persona . . . 4

Capítulo 1. Pregunta y criterios . . . 4

1.1 Afirmaciones que necesitan pruebas distintas . . . 4

1.2 Hipótesis y falsación . . . 5

Capítulo 2. Conservación de la escena . . . 5

2.1 Objetos que pueden desaparecer . . . 5

2.2 Relaciones y secuencia . . . 5

2.3 Privacidad y proporcionalidad . . . 6

Capítulo 3. Contenido y cronología . . . 7

3.1 Texto, variantes y origen temprano . . . 7

3.2 Ventanas y frecuencia . . . 7

3.3 Enlaces y parámetros . . . 7

Capítulo 4. Coordinación e hipótesis . . . 8

4.1 Indicadores convergentes . . . 8

4.2 Edad, cambios y comunidad . . . 8

4.3 Evaluación de automatización . . . 8

Capítulo 5. Grafos e infraestructura . . . 9

5.1 El nodo no es la persona . . . 9

5.2 Dominios, IP y servicios compartidos . . . 9

5.3 Escala de atribución . . . 10

Capítulo 6. Daño mediático e informe . . . 10

6.1 Alcance y consecuencias . . . 10

6.2 Informe técnico reproducible . . . 10

6.3 Acciones posteriores . . . 11

Anexo A. Formatos de análisis . . . 11

A.1 Inventario de cuentas y contenido . . . 12

A.2 Matriz de indicadores 12

A.3 Estructura de informe 12

A.4 Registro de simulación si se utiliza 12

Anexo B. Marco jurídico y control final 13

Presentación: muchas cuentas no son una sola persona

Una docena de perfiles que publican el mismo texto puede parecer una operación centralizada. También puede ser una comunidad que comparte una plantilla, una noticia urgente o una causa legítima. El análisis comienza por evitar la conclusión fácil: se describe qué hicieron las cuentas, con qué secuencia, qué relaciones existen y qué otras explicaciones podrían producir el mismo patrón.

“Bot”, “perfil falso”, “cuenta coordinada”, “troll”, “granja” y “operación de influencia” no son sinónimos. Una cuenta puede ser automatizada sin estar coordinada; varias personas pueden coordinarse sin automatización; un perfil puede usar un nombre ficticio sin ser falso en su totalidad; una campaña puede tener contenido verdadero y comportamiento engañoso. El informe define sus categorías y las prueba por separado.

El análisis no necesita inventar un titular para ser útil. Puede demostrar que un conjunto de cuentas comparte texto, ventana, enlaces, secuencia y relaciones de forma anómala respecto a una referencia documentada. La infraestructura común puede aportar indicios, pero una dirección IP o un dominio no convierte a todas las cuentas en una misma persona. La atribución se detiene donde termina la fuente.

> **Regla rectora**
>
> Primero patrón y cobertura; después alternativas; solo al final, el grado de atribución que la evidencia realmente permite.

Capítulo 1. Pregunta y criterios

1.1 Afirmaciones que necesitan pruebas distintas

Se separan cinco preguntas: qué contenido se publicó, qué cuentas participaron, qué comportamiento muestran, qué relaciones existen y quién las controla. Las primeras pueden responderse con publicaciones y registros; la coordinación exige comparación; la titularidad requiere otra clase de fuente. Si no se distingue, un gráfico atractivo termina afirmando más que la investigación.

El alcance incluye plataforma, período, zona, cuentas iniciales, términos, tipo de contenido, fuentes de datos y exclusiones. Se documenta cómo se encontró la muestra: búsqueda, lista previa, API, exportación, referencias o selección manual. La selección por indignación produce una muestra sesgada. Si solo se capturan publicaciones virales, no se compara con el comportamiento ordinario.

Afirmación	Evidencia necesaria	No concluir por defecto
Contenido idéntico	Texto, versión, URL, fecha y origen temprano.	Un único autor o central de publicación.
Simultaneidad	Zona, segundos disponibles y secuencia completa.	Automatización solo por cercanía temporal.
Coordinación	Varios indicadores y comparación de referencia.	Coordinación por una sola coincidencia.
Automatización	Patrones técnicos, actividad y controles disponibles.	Todo comportamiento repetitivo es bot.

Afirmación	Evidencia necesaria	No concluir por defecto
Titularidad	Registros de control y corroboración legal.	Una persona por foto, IP o nombre.
Daño	Contenido, alcance, contexto y consecuencias acreditadas.	Impacto total por impresiones.

1.2 Hipótesis y falsación

Una hipótesis inicial puede ser “las cuentas A–H actúan coordinadamente para amplificar el contenido X”. La alternativa puede ser “usuarios independientes comparten una plantilla por un evento externo”. Otra puede ser “la plataforma muestra un patrón aparente por su orden de recomendación”. Cada una necesita una comprobación capaz de debilitarla: fuente temprana, variación de textos, secuencia previa, comportamiento fuera del evento y comparación con otros grupos.

La referencia se define antes de calcular. Puede ser otra conversación del mismo tema, otro período de las mismas cuentas o un conjunto comparable de usuarios. No se elige un umbral porque produce el resultado deseado. Si no hay referencia adecuada, se declara que la anomalía es descriptiva y no se asigna una probabilidad inventada.

> **Principio de prueba**
>
> Una buena investigación no busca solo más indicios de coordinación. Busca datos que podrían demostrar que la explicación inicial no es necesaria.

Capítulo 2. Conservación de la escena

2.1 Objetos que pueden desaparecer

Se preservan publicaciones, perfiles, biografías, imágenes, respuestas, citas, reenvíos, enlaces, métricas, fechas y cambios visibles. Cada objeto recibe identificador y se relaciona con URL, cuenta, plataforma, fecha y método de adquisición. La captura de una página principal no demuestra todas las publicaciones de una cuenta ni el estado anterior de una red.

Si existe exportación o API autorizada, se registran endpoint o función sin secretos, versión, parámetros, filtros, paginación, límites, zona, formato, fecha y errores. Los datos recibidos se conservan en formato nativo con diccionario cuando exista. Si solo hay captura manual, se anota quién la tomó, qué rol usó y hasta dónde llegó la revisión. No se evaden límites de acceso para completar el conjunto.

2.2 Relaciones y secuencia

Las relaciones se registran como objetos separados: cuenta A responde a B, cita a C, comparte enlace D o sigue a E. Se conserva el contenido que prueba cada arista y la fecha visible. Un grafo creado sin esas referencias puede ser estético y no verificable. La dirección de la relación importa: seguir no equivale a ser seguido, citar no equivale a escribir el texto original.

La cronología conserva fecha literal, zona, precisión y significado: creación, edición, publicación, captura y métrica son eventos distintos. Las plataformas pueden ordenar por relevancia y no por

tiempo. La secuencia se construye con identificadores de publicación y fuentes externas cuando sea posible, sin asumir que el orden en pantalla es el orden real.

Objeto	Registro mínimo	Límite
Publicación	URL, ID, cuenta, texto, multimedia y fecha.	No contexto completo de la cuenta.
Perfil	URL, nombre visible, biografía y cambios.	No titular real ni ubicación automática.
Relación	Origen, tipo, destino y evidencia.	No dirección de control ni intención.
Métrica	Valor, fecha, significado y plataforma.	No lectores únicos ni daño total.
Exportación	Parámetros, cobertura, filtros y diccionario.	No exhaustividad fuera de consulta.
Captura	Operador, rol, fecha y recorrido.	No sustituye formato nativo disponible.

2.3 Privacidad y proporcionalidad

La investigación de perfiles puede exponer personas sin relación con el daño. Se limita recolección a lo necesario y se separa versión de trabajo de versión pública. Los datos personales no se publican para “probar” una hipótesis. Los perfiles privados no se acceden mediante suplantación ni cuentas falsas; se solicita la vía autorizada o se declara la limitación.

Criterio de seguridad

No conviertas una investigación de daño mediático en otro daño. El informe puede demostrar relaciones sin publicar domicilios, teléfonos, menores, fotografías o supuestas identidades no acreditadas.



Figura 1. La red se conserva antes de que desaparezca. Objeto, relación, momento y cobertura Reconstrucción editorial; no constituye evidencia real.

Capítulo 3. Contenido y cronología

3.1 Texto, variantes y origen temprano

Se compara el texto literal y sus variantes: palabras, hashtags, errores compartidos, espacios, enlaces, emojis, formato y recortes. Una plantilla pública puede explicar coincidencias; un error poco común puede sugerir una fuente común, pero no identifica a su autor. Se busca la versión temprana y se registra si pudo existir otra anterior fuera del alcance.

Las imágenes y videos pueden compartir archivo, marca, recorte o metadatos. El mismo archivo en dos cuentas no prueba coordinación si es una imagen popular o proporcionada por una organización. Se analiza quién lo publicó primero en el conjunto, cómo cambió y si las cuentas utilizaron parámetros de enlace o nombres relacionados. La autenticidad de escena se evalúa por otro método.

3.2 Ventanas y frecuencia

La simultaneidad debe tener unidades y una referencia. ¿Qué significa “al mismo tiempo”: mismo segundo, minuto, hora o día? Una noticia urgente puede producir miles de publicaciones cercanas. Se compara la distribución con períodos previos y otras conversaciones, con zona y precisión. No se elige una ventana después de ver que agrupa exactamente las cuentas sospechosas.

La frecuencia de publicación puede sugerir automatización o un equipo de personas, pero también una campaña programada o una persona muy activa. Las pausas, la regularidad, la variedad de contenido y el horario se analizan con contexto. Una cuenta que publica durante 24 horas no es automáticamente un bot: puede tener administradores en varias zonas.

3.3 Enlaces y parámetros

Los enlaces se analizan por dominio, ruta, redirección, parámetros, campaña, fecha de registro cuando sea pública y relación con otros objetos. Un parámetro idéntico puede indicar copia del mismo enlace, una plantilla o una configuración compartida; no prueba propiedad común. Se conserva la secuencia de redirecciones y el contenido final sin visitar destinos peligrosos en producción.

Indicio	Alternativa legítima	Comprobación
Mismo error de texto	Plantilla o cita compartida.	Origen temprano y variación entre cuentas.
Publicación cercana	Noticia urgente o evento programado.	Distribución de referencia y comportamiento previo.
Mismo enlace	Fuente popular o campaña pública.	Parámetros, primer uso y redirecciones.
Misma imagen	Recurso de comunicación o tendencia.	Archivo, versión, recorte y publicación inicial.
Actividad continua	Turnos, programación o uso intenso.	Tipos de acción, zonas y registros disponibles.

Caso ficticio

Ocho cuentas publican el mismo enlace en dos minutos. La referencia muestra que miles lo comparten por una noticia. Sin embargo, solo esas ocho usan el mismo parámetro poco común y el mismo error de texto, y ya habían actuado juntas antes. La coordinación gana fuerza por convergencia, no por los dos minutos.

Capítulo 4. Coordinación e hipótesis

4.1 Indicadores convergentes

Se construye una matriz con contenido, tiempo, enlaces, historial, relaciones, cambios de perfil, comportamiento previo y posibles fuentes externas. Cada indicador recibe una explicación alternativa y una comprobación. La fuerza no se decide por votación simple de señales: algunas son dependientes entre sí y otras pueden ser comunes en la plataforma.

La referencia permite decir si una frecuencia o relación es atípica. Se puede comparar la distribución de intervalos con períodos anteriores o con permutaciones controladas de los datos, conservando características relevantes. Si se utiliza simulación, se documenta semilla, reglas, supuestos y número de iteraciones. No se presenta una probabilidad estadística si el modelo no representa el proceso real.

4.2 Edad, cambios y comunidad

Muchas cuentas nuevas pueden aparecer por una migración de plataforma o por una campaña de invitación. Las fechas de creación se analizan como grupo y se comparan con la actividad anterior y posterior. Cambios simultáneos de nombre, imagen o descripción pueden indicar plantilla, pero también un evento comunitario. Se preserva el historial visible antes de que desaparezca.

Seguirse entre cuentas puede indicar una red o simplemente una comunidad afín. Se compara densidad de conexiones con otros grupos, reciprocidad, actividad fuera del grupo y relaciones previas. La densidad no demuestra control central. Un grupo pequeño puede estar muy conectado porque sus miembros se conocen; el grafo debe acompañarse de contenido y cronología.

4.3 Evaluación de automatización

La automatización se apoya en comportamiento técnico: acciones repetitivas con intervalos, uso de interfaces, patrones de contenido, respuesta inmediata y continuidad incompatible con actividad humana razonable. Aun así, hay herramientas de programación legítimas y equipos humanos con rutinas. El informe puede decir “comportamiento compatible con automatización” sin afirmar una herramienta concreta si no hay registros.

Dimensión	Pregunta	Límite de inferencia
Contenido	¿Hay variantes o solo copia literal?	Plantilla no equivale a control central.
Tiempo	¿El patrón es atípico frente a referencia?	Simultaneidad no equivale a bot.
Historial	¿La coordinación precede al evento?	Cuentas nuevas pueden ser migración.
Relaciones	¿La densidad supera una comunidad comparable?	Amistad y afinidad también crean grafos densos.
Interfaz	¿Hay evidencia de automatización?	Programación legítima existe.
Atribución	¿Qué fuente identifica control real?	Una IP o imagen no basta.

Conclusión defendible

“El conjunto presenta coincidencias de contenido, parámetros, secuencia y comportamiento previo compatibles con coordinación. La cobertura no permite atribuir una persona ni una herramienta específica.”

La coordinación se prueba con alternativas ACCCF · RECONSTRUCCIÓN EDITORIAL · DATOS FICTICIOS

Indicadores convergentes, no una sola señal espectacular

Indicio	Explicación alternativa	Comprobación
Mismo texto	Plantilla pública o causa compartida.	Variación, fuente inicial y secuencia.
Publicación simultánea	Zona horaria o noticia urgente.	Ventana, actividad previa y azar de referencia.
Mismos enlaces	Interés legítimo en una fuente.	Dominio, parámetros y primer uso.
Creación reciente	Cambio de plataforma o evento.	Edad conjunta, actividad y vínculos.
Seguirse entre cuentas	Comunidad real o afinidad.	Densidad comparada y comportamiento externo.

La figura explica decisiones y relaciones; no representa evidencia de un caso real.

Figura 2. La coordinación se prueba con alternativas. Indicadores convergentes, no una sola señal espectacular Reconstrucción editorial; no constituye evidencia real.

Capítulo 5. Grafos e infraestructura

5.1 El nodo no es la persona

El nodo representa una cuenta, publicación, enlace o infraestructura, según la leyenda. La arista representa una relación documentada, no una orden. El grafo debe incluir tipo, dirección, período, fuente y cobertura. Si se agrupan nodos por algoritmo, se registra método y parámetros; no se presenta un cluster como una organización real sin validación cualitativa.

Una cuenta central puede ser simplemente una fuente popular. Un puente entre grupos puede ser un medio o una persona que responde a todos. Las métricas de centralidad orientan revisión, no prueban control. El informe conserva la lista de aristas para que otra persona pueda verificar por qué dos nodos están conectados.

5.2 Dominios, IP y servicios compartidos

Una dirección IP puede pertenecer a una plataforma, VPN, empresa, hogar compartido o servicio de asignación dinámica. Un dominio puede tener hospedaje, DNS o certificado compartido con miles de sitios. La infraestructura compartida puede orientar solicitudes y análisis, pero no acredita propiedad común de las cuentas. Se evita geolocalizar personas a partir de ella.

Los registros técnicos se solicitan por canal legal cuando son necesarios. No se realiza escaneo intrusivo ni se consultan bases de credenciales filtradas para vincular cuentas. Si la fuente es pública, se documenta fecha y cobertura. Una filtración no se convierte en autorización para descargar, combinar o publicar datos personales.

5.3 Escala de atribución

Nivel	Qué puede afirmarse	Qué no se deriva
Contenido	Estas publicaciones y versiones existieron.	El hecho narrado ocurrió.
Comportamiento	Estas acciones presentan un patrón.	La cuenta es un bot.
Relación	Las cuentas interactúan de esta forma.	Se controlan entre sí.
Infraestructura	Comparten servicio o parámetros.	Mismo propietario o ubicación.
Coordinación	Indicios convergentes compatibles con coordinación.	Dirección por una persona.
Titularidad	Control acreditado por fuentes legales y contexto.	No inferir de nombre, foto o IP.

Límite profesional

El informe puede ser concluyente sobre coordinación y prudente sobre autoría. No necesita resolver quién está detrás para demostrar cómo se comportó la red.

Capítulo 6. Daño mediático e informe

6.1 Alcance y consecuencias

Se separa contenido, comportamiento, alcance visible y consecuencias acreditadas. Las impresiones no equivalen a lectores únicos, las reacciones no equivalen a apoyo y los comentarios no prueban cambio de opinión. El informe registra métricas con fecha y significado conocido, sin convertirlas en una cifra universal de daño.

El daño se documenta con comunicaciones, decisiones laborales, contratos, testimonios, reportes, atención a afectados y otras fuentes. No se atribuye todo lo ocurrido después de la campaña a esa campaña sin analizar otras causas. La preservación demuestra que existió un patrón; la causalidad necesita una secuencia y evidencia adicionales.

6.2 Informe técnico reproducible

El informe contiene encargo, alcance, fuentes, método, diccionario, cronología, indicadores, referencia, grafo, alternativas, hallazgos, limitaciones y anexos. Se publican identificadores de objetos y consultas para repetir el análisis. Las afirmaciones sobre conducta se vinculan con publicaciones y las de impacto con documentos concretos.

La versión pública puede omitir cuentas o datos que no sean necesarios para comprender el método, sin ocultar el razonamiento. Si una afirmación cambia al quitar una publicación, se revisa su solidez. Si no hay acceso a contenido privado o registros de plataforma, se declara la cobertura. No se completa con especulación.

6.3 Acciones posteriores

El reporte a plataforma identifica contenido, cuentas, patrón y evidencia; no presenta una acusación pública como sustituto. La solicitud de retirada o preservación se registra con fecha y folio. La comunicación a afectados evita repetir el contenido dañino y explica qué se está haciendo. Si hay amenaza o riesgo físico, se prioriza el canal de emergencia local.

El Reglamento de Servicios Digitales regula servicios intermediarios y riesgos sistémicos para determinadas plataformas de muy gran tamaño. El Reglamento (UE) 2024/900 aborda transparencia y segmentación de servicios de publicidad política, con límites sobre el contenido espontáneo. No se aplican automáticamente a toda cuenta o país ni convierten desinformación en una categoría universal de ilicitud.[12]

Cierre

El objetivo del informe es hacer comprensible una conducta y sus límites, no crear una nueva acusación sin prueba. La evidencia se entrega por el canal adecuado, no por escarmiento público.



Figura 3. El informe separa patrón, infraestructura y persona. La conclusión no supera la fuerza de la fuente Reconstrucción editorial; no constituye evidencia real.

Anexo A. Formatos de análisis

A.1 Inventario de cuentas y contenido

Campo	Registro requerido	Control
Cuenta / URL	Identificador, plataforma, perfil y fecha de observación.	No nombre de persona supuesto.
Publicación	ID, texto, versión, multimedia y fecha literal.	Objeto preservado.
Relación	Origen, tipo, destino y evidencia.	No inferir control.
Tiempo	Zona, precisión y significado.	No mezclar creación y captura.
Métrica	Valor, fecha y significado de plataforma.	No lectores únicos.
Cobertura	Consulta, filtros, acceso y ausencias.	No afirmar exhaustividad.
Privacidad	Datos sensibles, restricciones y versión pública.	Minimización real.

A.2 Matriz de indicadores

Indicio	Alternativa	Comprobación	Resultado limitado
Texto / error común	Plantilla o cita.	Origen temprano y variantes.	[ ]
Ventana cercana	Noticia o evento.	Referencia y distribución previa.	[ ]
Parámetro de enlace	Copia o campaña pública.	Primer uso y redirecciones.	[ ]
Edad conjunta	Migración o evento.	Actividad previa y contexto.	[ ]
Grafo denso	Comunidad afín.	Referencia y comportamiento externo.	[ ]
Infraestructura común	Proveedor compartido.	Registro y otras cuentas.	[ ]

A.3 Estructura de informe

Índice operativo

```
1. Encargo, preguntas, alcance y exclusiones
2. Fuentes, cobertura, diccionario y limitaciones
3. Preservación y manifiesto de objetos
4. Cronología y variantes de contenido
5. Indicadores de coordinación y referencia
6. Relaciones y grafo con aristas verificables
7. Hipótesis alternativas y resultados negativos
8. Alcance visible y consecuencias acreditadas
9. Conclusiones por nivel de atribución
10. Privacidad, entrega, anexos y versión
11. Fuentes jurídicas y técnicas consultadas
```

A.4 Registro de simulación si se utiliza

Documentación mínima

```
Pregunta y métrica: [qué se compara]
Datos incluidos y cobertura: [fuente y filtros]
Referencia elegida y razón: [período o grupo]
Reglas de permutación: [qué se conserva y qué cambia]
Semilla y versión de herramienta: [para repetición]
Iteraciones: [cantidad y justificación]
Resultado: [distribución y observación]
Supuestos que no representa: [limitaciones]
Conclusión permitida: [sin probabilidad ficticia]
```

Anexo B. Marco jurídico y control final

La evidencia de publicaciones y registros se conecta con reconocimiento, conservación y valoración del documento electrónico. México usa CCom 89–94 y 1205 y CFPC/CNPCF según transición; Perú separa firma y proceso; Chile diferencia firmas y fecha; Argentina pondera confiabilidad; Colombia y Ecuador exigen conservación con origen y fecha; España combina eIDAS, LEC y servicios digitales. El contenido espontáneo no se equipara a publicidad sin revisar el régimen.[3456789101112 1314]

La investigación de redes también trata datos personales. Se aplican finalidad, proporcionalidad, seguridad y minimización; no se combinan fuentes para identificar a una persona sin fundamento. La libertad de expresión y el análisis de contenido se separan de la evaluación de comportamiento coordinado. La acusación de “bot” puede ser falsa y dañina incluso si la cuenta usa seudónimo.[15161718]

Control final	Pregunta de aceptación
Cobertura	¿Consulta, filtros, período y ausencias están escritos?
Objetos	¿Cada publicación, relación y métrica tiene fuente?
Coordinación	¿Hay convergencia y comparación, no solo coincidencia?
Alternativas	¿Se evaluaron plantilla, evento, comunidad y plataforma?
Grafo	¿Nodo no equivale a persona ni arista a control?
Atribución	¿La conclusión no inventa titulares ni herramientas?
Daño	¿Alcance y consecuencias están separados y acreditados?
Privacidad	¿La investigación evita exposición innecesaria?

Cierre

La red se demuestra con objetos, secuencia y relaciones. La persona no se inventa para completar el gráfico.

Referencias citadas

Cada número remite a la fuente consultada en el cuerpo. La fecha general de revisión documental es el 10 de noviembre de 2026; el uso en un expediente exige comprobar la versión aplicable al hecho, materia, sujeto y jurisdicción.

[1] Reglamento (UE) 2022/2065 de Servicios Digitales. Régimen de servicios intermediarios, gestión de riesgos sistémicos para determinadas plataformas y buscadores de muy gran tamaño y reglas de contenido. No convierte todo patrón en prueba de coordinación ni toda opinión en contenido ilícito. Fuente oficial en línea

[2] Reglamento (UE) 2024/900 sobre transparencia y segmentación de la publicidad política. Reglas específicas para servicios de publicidad política y riesgos asociados; no se aplica indiscriminadamente a todo contenido espontáneo de usuarios. Fuente oficial en línea

[3] 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

[4] Código Nacional de Procedimientos Civiles y Familiares, artículos 348–350. Compilación con reforma del 15-01-2026. La aplicación es gradual y depende de declaratorias. Fuente oficial en línea

[5] 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

[6] Perú. Código Procesal Civil, artículos 188–197 y 245.5: finalidad, legalidad, medios, carga, valoración y fecha por medios técnicos. Fuente oficial en línea

[7] 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

[8] Argentina. Código Civil y Comercial, artículos 318–319: correspondencia por cualquier medio y ponderación de confiabilidad de soportes y procedimientos técnicos. Fuente oficial en línea

[9] 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

[10] 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

[11] 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

[12] España. Ley de Enjuiciamiento Civil, artículos 326 y 384: documentos privados, impugnación, instrumentos para archivar, conocer o reproducir datos, examen, custodia y sana crítica. Fuente oficial en línea

[13] Reglamento (UE) 2022/2065 de Servicios Digitales. Régimen de servicios intermediarios, gestión de riesgos sistémicos para determinadas plataformas y buscadores de muy gran tamaño y reglas de contenido. No convierte todo patrón en prueba de coordinación ni toda opinión en contenido ilícito. Fuente oficial en línea

[14] Reglamento (UE) 2024/900 sobre transparencia y segmentación de la publicidad política. Reglas específicas para servicios de publicidad política y riesgos asociados; no se aplica indiscriminadamente a todo contenido espontáneo de usuarios. Fuente oficial en línea

[15] 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

[16] 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

[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

[18] 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

Aviso editorial: guía técnica general y material educativo. No constituye asesoría legal, dictamen pericial ni autorización para acceder a sistemas o información. Los ejemplos y cifras de demostración son ficticios; las figuras son reconstrucciones editoriales.