ESPECIFICACIÓN DE EVIDENCIA ELECTRÓNICA DE VINTY

ESTÁNDAR TÉCNICO-JURÍDICO DEL MVP

Versión 1.0 | Emisión y entrada en vigor: 21 de julio de 2026 | Documento de plataforma

1. OBJETO

1.1. Esta Especificación establece los controles mínimos para generar, vincular, conservar, consultar, reproducir y verificar la evidencia electrónica de los actos realizados dentro de Vinty.

1.2. Su finalidad es permitir que cada acto relevante pueda relacionarse con:

a) una persona usuaria autenticada;

b) una cuenta y, cuando corresponda, un Negocio u Organización determinados;

c) el documento o configuración exactos que fueron presentados;

d) una acción afirmativa concreta;

e) la fecha y hora registradas en UTC; y

f) un expediente que pueda consultarse posteriormente.

1.3. Esta Especificación regula la evidencia que produce la plataforma. No sustituye los Términos de Uso, el Aviso de Privacidad, el Anexo de Tratamiento de Datos, la Autorización de Agencia ni los contratos celebrados entre usuarios.

2. IDENTIDAD Y FUNCIÓN DE VINTY

2.1. Vinty es una plataforma tecnológica operada por Enrique Salas Marin.

2.2. Vinty proporciona infraestructura, autenticación, cuentas, organizaciones, permisos, expedientes, almacenamiento, auditoría y mecanismos de aceptación electrónica.

2.3. Vinty no es una agencia de publicidad, no presta los servicios profesionales de las agencias que usan la plataforma y no se convierte en parte de sus contratos por conservar evidencia relacionada con ellos.

2.4. Vinty Marketing es una agencia independiente. No es la plataforma ni opera la infraestructura tecnológica de Vinty.

3. ALCANCE

3.1. Esta Especificación aplica a los eventos que Vinty identifique como jurídicamente relevantes, entre ellos:

a) aceptación o reaceptación de Términos de Uso;

b) puesta a disposición del Aviso de Privacidad;

c) aceptación de anexos contractuales;

d) declaración de facultades para actuar por un Negocio;

e) reclamación o activación de una Organización;

f) otorgamiento, modificación, suspensión o revocación de permisos;

g) Autorizaciones de Agencia;

h) aceptación de documentos electrónicos mediante funciones habilitadas de Vinty; y

i) cualquier otro acto para el cual la interfaz solicite una acción afirmativa y genere un acuse.

3.2. El registro de puesta a disposición del Aviso de Privacidad acredita que el documento y su enlace estuvieron disponibles en el flujo correspondiente. No declara que la persona lo abrió o leyó, no convierte el Aviso en contrato, no equivale por sí mismo al consentimiento para finalidades que requieran una manifestación separada y no limita los derechos de las personas titulares.

3.3. Un registro técnico ordinario, como una visita de página, apertura de sesión, desplazamiento, consulta o descarga, no constituye por sí mismo aceptación de un documento.

3.4. Sólo existe un Evento de Aceptación cuando se cumplen los requisitos de esta Especificación y el sistema confirma que el registro fue concluido correctamente.

4. DEFINICIONES

4.1. Acción Afirmativa: conducta consciente mediante la cual una persona selecciona un control no premarcado y activa un botón cuyo texto describe el acto que realizará.

4.2. Acuse: constancia legible que resume el Evento de Evidencia y permite relacionarlo con su expediente.

4.3. Documento Canónico: archivo exacto que la plataforma identifica como versión jurídicamente controlada de un instrumento. Cuando un instrumento indique que su PDF es canónico, el DOCX tendrá carácter editable o de consulta y no sustituirá al PDF.

4.4. Evento de Evidencia: registro electrónico de una acción o cambio relevante realizado dentro de Vinty.

4.5. Evento de Aceptación: Evento de Evidencia que documenta la manifestación afirmativa de aceptar un instrumento o asumir una declaración.

4.6. Evento de Puesta a Disposición: Evento de Evidencia que documenta la disponibilidad de un aviso informativo en un flujo determinado, sin atribuir una acción que no ocurrió y sin convertirlo en aceptación contractual o consentimiento.

4.7. Expediente de Evidencia: conjunto relacionado de documento, metadatos, eventos, acuses y registros de auditoría necesarios para reconstruir un acto.

4.8. Hash SHA-256: resumen criptográfico de 256 bits calculado sobre los bytes exactos de un archivo o sobre una representación canónica de datos.

4.9. Negocio: persona física que actúa en relación con una actividad empresarial o profesional, o persona moral, identificada dentro de Vinty y vinculada con una Organización. La Organización no constituye por sí misma una persona ni una parte contractual.

4.10. Organización o Workspace: espacio lógico de Vinty asociado con un Negocio y sus usuarios, recursos, permisos y registros.

4.11. OPERADOR: Enrique Salas Marin, en su carácter de operador tecnológico de Vinty.

4.12. Registro Canónico del Evento: representación estructurada e inmutable de los datos que forman un Evento de Evidencia.

4.13. UTC: Tiempo Universal Coordinado utilizado por Vinty como referencia uniforme de fecha y hora.

4.14. Usuario: persona física que accede a Vinty mediante una cuenta individual.

5. PRINCIPIOS DE EVIDENCIA

5.1. El sistema de evidencia se regirá por los siguientes principios:

a) **atribución**, para relacionar el acto con una cuenta autenticada y su contexto;

b) **integridad**, para detectar modificaciones al documento o registro;

c) **accesibilidad**, para permitir consulta y reproducción posterior;

d) **trazabilidad**, para reconstruir la secuencia de eventos relevantes;

e) **claridad**, para que la persona conozca qué acto realiza;

f) **mínimo privilegio**, para limitar el acceso a los expedientes;

g) **minimización**, para no incorporar datos innecesarios; y

h) **continuidad**, para conservar la evidencia aunque una cuenta, permiso o relación comercial termine.

5.2. Ningún elemento aislado se considerará prueba absoluta de identidad, voluntad o representación. La atribución se evaluará con el conjunto del expediente.

6. CONTROL DE DOCUMENTOS

6.1. Antes de presentar un documento para aceptación, Vinty deberá registrar:

a) su nombre exacto;

b) identificador interno único;

c) número de versión;

d) fecha de emisión;

e) estado de publicación;

f) formato canónico;

g) tamaño en bytes;

h) hash SHA-256 del archivo exacto; y

i) fecha y hora UTC de su publicación.

6.2. Cada formato tendrá su propio hash. El hash de un PDF no se reutilizará como hash del DOCX correspondiente.

6.3. El Documento Canónico asociado con una aceptación quedará inmovilizado. Una modificación, aunque sea pequeña, deberá publicarse como una nueva versión o corrección identificable.

6.4. La sustitución de un archivo no deberá sobrescribir el archivo previamente aceptado ni romper la relación entre el Evento de Aceptación y la versión que le correspondía.

6.5. Los cambios materiales requerirán una nueva acción afirmativa cuando así lo establezcan los Términos de Uso o el propio instrumento.

6.6. Las correcciones meramente editoriales podrán documentarse como una nueva versión sin exigir reaceptación únicamente cuando no modifiquen derechos, obligaciones, alcances, finalidades, permisos o consecuencias jurídicas.

7. AUTENTICACIÓN PREVIA

7.1. Todo Evento de Aceptación deberá realizarse dentro de una sesión autenticada.

7.2. La evidencia deberá asociar el evento con un identificador único de usuario y con el estado de verificación de su correo electrónico al momento del acto.

7.3. Cuando Vinty habilite factores adicionales de autenticación, podrá registrar que el factor fue satisfecho, sin conservar secretos, contraseñas, códigos completos ni credenciales reutilizables.

7.4. La autenticación de una cuenta aporta un elemento de atribución, pero no certifica por sí sola la identidad civil, capacidad o representación legal del usuario.

7.5. Vinty nunca incorporará al expediente contraseñas, llaves privadas, tokens activos de sesión ni respuestas secretas de recuperación.

8. IDENTIFICACIÓN DEL ACTOR Y DEL CONTEXTO

8.1. El Registro Canónico del Evento conservará una fotografía lógica de los datos relevantes existentes al momento del acto, sin depender únicamente de datos que puedan cambiar después.

8.2. La fotografía lógica incluirá, según corresponda:

a) identificador del usuario;

b) nombre mostrado por el usuario;

c) correo electrónico asociado y su estado de verificación;

d) identificador del Negocio u Organización;

e) nombre del Negocio mostrado en la plataforma;

f) rol técnico del usuario;

g) identificador de la Agencia, cuando intervenga una; y

h) declaración específica de facultades, cuando el acto se realice por un Negocio.

8.3. El rol técnico de administrador, colaborador o miembro no constituye por sí mismo poder, mandato ni representación legal.

8.4. Cuando el acto pretenda obligar a un Negocio, la plataforma deberá solicitar una declaración separada de facultades y conservar su texto exacto.

8.5. Vinty registra la declaración de la persona, pero no emite fe pública ni certifica que sus facultades sean suficientes conforme a documentos externos.

9. PRESENTACIÓN DEL DOCUMENTO

9.1. Antes de solicitar la aceptación, la interfaz deberá mostrar de forma clara:

a) el título del documento;

b) su versión;

c) la identidad de la parte o cuenta a la que se aplicará;

d) un enlace funcional para leer y descargar el documento completo; y

e) una explicación breve del efecto de la acción.

9.2. El control de aceptación deberá aparecer inicialmente desmarcado.

9.3. El texto de aceptación deberá ser visible y comprensible, sin quedar oculto dentro de textos generales o controles ambiguos.

9.4. El botón final deberá describir la acción, por ejemplo: “Aceptar y continuar”, “Autorizar acceso”, “Firmar documento” o “Revocar autorización”.

9.5. La inactividad, el silencio, una casilla premarcada, el simple uso de la plataforma o la apertura de un archivo no se registrarán como aceptación.

9.6. Si la persona no puede acceder al Documento Canónico, el sistema deberá impedir la conclusión del Evento de Aceptación.

9.7. Cuando se muestre el Aviso de Privacidad, la interfaz distinguirá claramente entre su puesta a disposición o reconocimiento y cualquier manifestación separada que la ley exija para una finalidad específica.

10. SECUENCIA MÍNIMA DEL EVENTO DE ACEPTACIÓN

10.1. La secuencia mínima será:

a) autenticación del usuario;

b) recuperación de la versión vigente del documento;

c) verificación del hash registrado;

d) presentación de la información exigida por la cláusula 9;

e) selección voluntaria del control de aceptación;

f) declaración de facultades, cuando corresponda;

g) activación del botón final;

h) validación del estado de cuenta, versión, permisos y sesión;

i) creación atómica del Registro Canónico del Evento; y

j) emisión del Acuse.

10.2. Si el documento cambia entre su presentación y la activación del botón, la operación deberá detenerse y la nueva versión deberá mostrarse antes de solicitar otra aceptación.

10.3. Si falla la creación del registro, la interfaz no deberá confirmar que el acto fue completado.

11. CONTENIDO MÍNIMO DEL REGISTRO CANÓNICO DEL EVENTO

11.1. Cada Evento de Aceptación deberá contener, según resulte aplicable:

a) identificador único del evento;

b) tipo de evento;

c) resultado del evento;

d) fecha y hora del servidor en UTC;

e) versión de esta Especificación;

f) identificador del usuario actor;

g) nombre y correo electrónico mostrados al momento del evento;

h) estado de verificación del correo;

i) identificador de sesión o correlación técnica no reutilizable;

j) identificador y nombre del Negocio u Organización;

k) rol técnico del usuario;

l) identificador y nombre de la Agencia, si existe;

m) identificador, título, versión y fecha del documento;

n) nombre del archivo canónico;

o) tamaño en bytes del archivo;

p) hash SHA-256 del Documento Canónico;

q) texto exacto de la declaración aceptada;

r) etiqueta exacta del botón activado;

s) idioma de la interfaz;

t) permisos, recursos y vigencia seleccionados, cuando corresponda;

u) estado anterior y estado posterior, cuando exista una modificación;

v) identificador del evento precedente o relacionado;

w) dirección de red y datos generales del agente de usuario, cuando estén disponibles y su tratamiento se encuentre informado; y

x) identificador del Acuse.

11.2. Los datos técnicos del dispositivo o red serán elementos complementarios. No se usarán como sustituto único de la autenticación ni como prueba concluyente de ubicación física.

11.3. Cuando un campo no resulte aplicable, el registro deberá conservar una indicación técnica inequívoca de no aplicabilidad y no un valor inventado.

12. REPRESENTACIÓN CANÓNICA Y HASH DEL EVENTO

12.1. El Registro Canónico del Evento se representará en datos estructurados codificados en UTF-8.

12.2. Para calcular su hash, la representación excluirá únicamente el campo destinado a almacenar ese mismo hash.

12.3. La canonicalización deberá aplicar de manera uniforme:

a) nombres de campos estables;

b) orden lexicográfico de claves;

c) ausencia de espacios no significativos;

d) conservación del orden semántico de los arreglos;

e) fechas completas en UTC;

f) valores booleanos y nulos inequívocos; y

g) normalización uniforme de texto Unicode.

12.4. El hash se calculará con SHA-256 sobre los bytes exactos resultantes y se expresará mediante 64 caracteres hexadecimales en minúsculas.

12.5. Una vez confirmado el evento, su representación canónica no deberá editarse. Cualquier aclaración, corrección, revocación o evento posterior se conservará como un registro nuevo vinculado al anterior.

12.6. El hash permite detectar diferencias entre representaciones. Por sí solo no prueba identidad, autoridad, tiempo cierto ni contenido lícito.

13. EVIDENCIA DE FACULTADES EMPRESARIALES

13.1. Cuando el usuario actúe por un Negocio, el Evento de Aceptación deberá incorporar una declaración expresa de que cuenta con facultades suficientes para realizar el acto.

13.2. La declaración será independiente de la selección general de los Términos de Uso.

13.3. La evidencia deberá identificar el Negocio al que se refiere mediante sus datos vigentes y su identificador interno.

13.4. Un rol técnico no sustituirá la declaración ni facultará automáticamente al usuario para:

a) aceptar instrumentos por el Negocio;

b) transferir la Organización;

c) cerrar la cuenta;

d) autorizar una Agencia; o

e) realizar otros actos reservados al propietario o representante autorizado.

14. EVIDENCIA DE AUTORIZACIONES DE AGENCIA

14.1. El otorgamiento de acceso a una Agencia requerirá dos eventos separados y relacionados:

a) el Evento de Autorización del Negocio; y

b) el Evento de Aceptación de Acceso de la Agencia.

14.2. El acceso no se activará hasta que ambos eventos hayan sido confirmados correctamente.

14.3. El Evento de Autorización del Negocio deberá conservar:

a) Negocio otorgante;

b) usuario que otorga y su declaración de facultades;

c) Agencia beneficiaria;

d) permisos expresamente seleccionados;

e) recursos o áreas a los que se aplican;

f) fecha de inicio;

g) plazo o condición de terminación;

h) restricciones aplicables; e

i) identificación, versión y hash de la Autorización de Agencia.

14.4. El Evento de Aceptación de Acceso de la Agencia deberá conservar la identidad de la Agencia y de su usuario, su declaración de facultades, el alcance recibido y el texto exacto de su aceptación.

14.5. Una modificación deberá mostrar el estado anterior y el nuevo estado.

14.6. La ampliación de permisos requerirá una nueva acción afirmativa del Negocio. También requerirá una nueva aceptación de la Agencia cuando la ampliación modifique el alcance de su acceso, sus responsabilidades o sus obligaciones.

14.7. La reducción o revocación podrá aplicarse inmediatamente mediante un evento separado vinculado con la autorización afectada y no requerirá aceptación ni consentimiento de la Agencia.

14.8. La revocación tendrá efectos técnicos desde la fecha y hora UTC en que el sistema confirme el evento, sin borrar la evidencia de actividades anteriores.

15. CONTRATOS Y OTROS DOCUMENTOS ELECTRÓNICOS

15.1. Cuando una función habilitada permita aceptar o firmar electrónicamente un contrato, el expediente deberá identificar:

a) el archivo exacto;

b) las partes y firmantes declarados;

c) la secuencia de presentación y aceptación;

d) el texto de la manifestación;

e) el hash del documento antes y después de concluir el acto, cuando el proceso genere una versión final; y

f) el Acuse correspondiente.

15.2. El sistema deberá impedir que una Agencia use una autorización técnica para firmar por un Negocio cuando esa facultad se encuentre expresamente excluida.

15.3. La preparación, carga, visualización o envío de un borrador no equivaldrá a su aceptación o firma.

16. ACUSE

16.1. Después de completar un Evento de Aceptación, Vinty pondrá a disposición del usuario un Acuse descargable o consultable dentro de su cuenta.

16.2. El Acuse deberá incluir, como mínimo:

a) identificador del evento;

b) título y versión del documento;

c) identidad mostrada del actor;

d) Negocio u Organización correspondiente;

e) fecha y hora UTC;

f) declaración aceptada;

g) hash del Documento Canónico; y

h) resultado del evento.

16.3. Cuando intervenga una Agencia, el Negocio podrá consultar los permisos vigentes, su historial de cambios y las revocaciones correspondientes.

16.4. El envío de una copia por correo electrónico será complementario. Su falla no invalidará un evento correctamente registrado y accesible en la cuenta.

17. EVENTOS INCOMPLETOS, RECHAZADOS O FALLIDOS

17.1. No existirá aceptación cuando:

a) el usuario abandone el flujo antes de concluirlo;

b) no seleccione el control afirmativo;

c) la sesión haya expirado;

d) la versión presentada ya no sea vigente;

e) el servidor no confirme la escritura íntegra del registro; o

f) el sistema muestre un error antes de emitir el Acuse.

17.2. Vinty podrá conservar registros técnicos de intentos fallidos para seguridad y diagnóstico, pero éstos deberán diferenciarse claramente de un Evento de Aceptación concluido.

17.3. La repetición de un intento fallido no deberá reutilizar el identificador de un evento anterior.

18. INMUTABILIDAD Y CORRECCIONES

18.1. Los eventos confirmados se conservarán bajo un modelo de adición sucesiva.

18.2. No se corregirá un evento confirmado mediante edición silenciosa.

18.3. Una corrección deberá:

a) generar un nuevo evento;

b) identificar el registro anterior;

c) describir el motivo;

d) conservar ambos estados; y

e) ser realizada por una persona o proceso con permisos suficientes.

18.4. La revocación, terminación o sustitución de una autorización no elimina la evidencia del otorgamiento original.

19. ACCESO Y SEPARACIÓN DE FUNCIONES

19.1. El acceso administrativo a expedientes de evidencia se limitará a personal o procesos que lo necesiten para soporte, seguridad, cumplimiento o defensa jurídica.

19.2. Las consultas, exportaciones y acciones administrativas relevantes deberán quedar registradas.

19.3. Una Agencia sólo podrá ver la evidencia necesaria para sus permisos y para comprobar actos en los que haya intervenido.

19.4. La Agencia no podrá acceder a credenciales, controles de recuperación, declaraciones reservadas al propietario ni expedientes ajenos a su autorización.

19.5. El acceso técnico del OPERADOR no convierte a Vinty en representante, mandatario, parte contractual o responsable de las decisiones comerciales de los usuarios.

20. CONSERVACIÓN

20.1. Los Documentos Canónicos, Registros Canónicos de Evento y Acuses que consignen derechos, obligaciones, autorizaciones o compromisos se conservarán durante un plazo mínimo de diez años contado desde la fecha del evento correspondiente.

20.2. El plazo podrá extenderse cuando resulte necesario para:

a) cumplir una obligación legal;

b) atender una investigación o requerimiento de autoridad;

c) conservar una defensa o reclamación vigente;

d) ejecutar una suspensión de eliminación; o

e) resolver una controversia.

20.3. El cierre de una cuenta, la salida de una Agencia o la terminación de la Beta no producirán la eliminación anticipada de la evidencia sujeta a conservación.

20.4. Al concluir los plazos aplicables, los datos deberán eliminarse, anonimizarse o mantenerse bloqueados cuando exista otra base jurídica de conservación.

20.5. Los derechos de cancelación u oposición se atenderán conforme a la legislación y al Aviso de Privacidad, sin eliminar información que deba conservarse para cumplir obligaciones o ejercer derechos.

21. RESPALDO, RECUPERACIÓN Y VERIFICACIÓN PERIÓDICA

21.1. Vinty deberá mantener medidas razonables de respaldo y recuperación para evitar que una falla ordinaria destruya el único ejemplar de un expediente.

21.2. La restauración de un respaldo no deberá convertir registros incompletos en eventos confirmados ni alterar identificadores, fechas o hashes.

21.3. Deberán realizarse verificaciones periódicas de legibilidad e integridad sobre muestras o conjuntos definidos de expedientes.

21.4. Una inconsistencia deberá documentarse y atenderse conforme a la cláusula 24.

22. EXPORTACIÓN Y REPRODUCCIÓN

22.1. Un expediente exportable podrá incluir:

a) Documento Canónico;

b) Registro Canónico del Evento;

c) Acuse legible;

d) historial relacionado; y

e) manifiesto de hashes.

22.2. La reproducción deberá permitir verificar el hash del archivo frente al valor conservado.

22.3. Una copia podrá mostrar la fecha de exportación o verificación, sin sustituir la fecha original del evento.

22.4. El resultado de una verificación deberá indicar de forma clara si:

a) el hash coincide;

b) el hash no coincide; o

c) no existe información suficiente para verificarlo.

22.5. Una reproducción no deberá presentarse como certificada por una autoridad o tercero independiente cuando no lo esté.

23. PRIVACIDAD Y MINIMIZACIÓN

23.1. Los datos de evidencia se tratarán conforme al Aviso de Privacidad Integral de Vinty y, cuando corresponda, al Anexo de Tratamiento de Datos.

23.2. El Aviso de Privacidad se pone a disposición y puede generar un Evento de Puesta a Disposición. Dicho evento no constituye aceptación contractual ni consentimiento general para el tratamiento.

23.3. Sólo se recopilarán los datos razonablemente necesarios para atribución, seguridad, cumplimiento, soporte y defensa.

23.4. El expediente no deberá contener contraseñas, datos completos de autenticación, contenido ajeno al acto ni datos sensibles que no sean indispensables.

23.5. La dirección de red, agente de usuario y demás datos técnicos se tratarán como elementos de seguridad y evidencia, sujetos a controles de acceso y conservación.

23.6. Vinty distinguirá los datos que trata como responsable para finalidades propias de aquellos que procesa por instrucciones de un Negocio.

24. ANOMALÍAS E INCIDENTES DE INTEGRIDAD

24.1. Si Vinty detecta una posible alteración, pérdida, acceso indebido o inconsistencia, deberá:

a) preservar los registros disponibles;

b) evitar sobrescribir la evidencia afectada;

c) limitar accesos cuando sea necesario;

d) documentar la detección y las acciones tomadas;

e) evaluar el alcance; y

f) realizar las comunicaciones exigidas por la ley o los instrumentos aplicables.

24.2. Un archivo con hash diferente no deberá reemplazar silenciosamente al original.

24.3. Si el documento original no puede recuperarse, el expediente deberá identificar la anomalía y no presentar una reconstrucción como si fuera el original intacto.

24.4. Las acciones de investigación formarán un registro separado y no modificarán el Evento de Aceptación.

25. LIMITACIONES DEL SISTEMA

25.1. El sistema descrito documenta una aceptación electrónica ordinaria basada en autenticación, acción afirmativa, vinculación documental, sello de tiempo del servidor, hash y conservación.

25.2. El MVP no ofrece firma electrónica avanzada, fe pública, verificación oficial de identidad ni certificación externa de conservación.

25.3. Vinty no garantiza que una autoridad atribuya a una evidencia un valor específico. Su admisión y fuerza probatoria dependerán del expediente completo, la legislación aplicable y la valoración de la autoridad competente.

25.4. El hash SHA-256 permite comprobar identidad de bytes, pero no acredita por sí solo quién creó el archivo, cuándo lo hizo o si su contenido es válido.

25.5. Esta Especificación no convierte un acto inválido, ilícito o realizado sin facultades en un acto válido.

26. RESPONSABILIDADES

26.1. Corresponde al OPERADOR implementar y conservar los controles técnicos definidos en esta Especificación.

26.2. Corresponde al Usuario:

a) proteger su cuenta;

b) revisar el documento antes de aceptar;

c) proporcionar datos correctos;

d) no permitir que otra persona use sus credenciales; y

e) declarar sus facultades con veracidad.

26.3. Corresponde al Negocio:

a) mantener actualizado al propietario de su Organización;

b) controlar sus administradores y colaboradores;

c) revisar permisos vigentes;

d) revocar accesos cuando dejen de ser necesarios; y

e) conservar los documentos que le correspondan.

26.4. Corresponde a la Agencia usar el acceso únicamente dentro de la autorización otorgada y conservar sus propios contratos y evidencias.

26.5. Vinty no resuelve por sí misma disputas sobre propiedad de un Negocio, representación, titularidad de contenidos o cumplimiento de servicios profesionales. Podrá preservar evidencia y ejecutar órdenes válidas o medidas de seguridad.

27. RELACIÓN CON OTROS INSTRUMENTOS

27.1. Los Términos de Uso regulan el acceso general a Vinty.

27.2. El Aviso de Privacidad regula las finalidades propias del OPERADOR y los derechos de las personas.

27.3. El Anexo de Tratamiento de Datos regula el procesamiento que Vinty realiza por instrucciones de un Negocio.

27.4. La Autorización de Agencia regula el alcance técnico del acceso otorgado a una Agencia.

27.5. Esta Especificación regula cómo se documentan esos actos, pero no amplía sus alcances sustantivos.

27.6. En caso de contradicción, el instrumento sustantivo correspondiente determinará los derechos y obligaciones, mientras esta Especificación determinará los requisitos técnicos de evidencia.

28. CONTROL DE VERSIÓN

28.1. Esta es la versión 1.0, emitida el 21 de julio de 2026.

28.2. Las modificaciones que reduzcan la integridad, atribución, accesibilidad o plazo mínimo de conservación no podrán aplicarse retroactivamente a eventos ya concluidos.

28.3. Una nueva versión deberá identificarse y conservarse sin reemplazar esta versión en expedientes históricos.

28.4. Los eventos conservarán la versión de esta Especificación que estaba vigente al momento de su generación.

29. VIGENCIA Y CONTACTO

29.1. Esta Especificación entra en vigor el 21 de julio de 2026.

29.2. Su publicación documenta el estándar operativo adoptado por Vinty y no requiere una aceptación separada del usuario.

29.3. Las personas usuarias sí deberán realizar las acciones afirmativas exigidas por cada instrumento o evento particular.

29.4. Las consultas relativas a expedientes de evidencia podrán enviarse a ceo@vinty.network.