Análisis de cumplimiento contractual

Plataforma Kynda

1. Incumplimientos verificados

1.1 Titularidad y control de los activos

Este es el incumplimiento de mayor solidez probatoria, dado que no depende de valoración técnica alguna y se ha confirmado con datos obtenidos directamente de la plataforma.

El repositorio no es propiedad de la Sociedad. La Sociedad carece de control sobre él. La cláusula 6.3 exige acceso permanente con permisos suficientes para el control y la continuidad. La cuenta de la Sociedad consta como colaboradora con permiso de escritura, pero sin permisos de administración.
Actualmente el único administrador es el desarrollador.

Existe dependencia crítica de cuentas personales, supuesto que la cláusula 6.4 prohíbe de forma expresa. La declaración de no dependencia resulta materialmente inexacta.

La cláusula 5.2 exige confirmación escrita de que ningún activo permanece bajo cuentas personales, licencias nominativas o entornos controlados por el desarrollador. El inventario entregado afirma que no existen pasos dependientes de la máquina o la memoria de una persona concreta. El repositorio contradice esa afirmación en dos puntos comprobables.

1.2 Tipos de evidencia admitidos

El Anexo I lo exige en dos lugares distintos. El módulo 5 requiere admitir imagen en formatos JPEG, PNG y HEIC, vídeo en formatos MP4 y MOV, y texto. El módulo 2 requiere poder definir el tipo de evidencia exigida para validar cada acción, incluyendo al menos imagen, vídeo o texto.

El vídeo no existe en ninguna capa del sistema. La búsqueda de cualquier referencia a formatos de vídeo en la totalidad del repositorio no devuelve ninguna coincidencia. El selector de ficheros admite exclusivamente imágenes, y la pantalla del validador, ante un fichero de otra naturaleza, muestra el nombre técnico del formato en lugar de un reproductor.

El texto no constituye un tipo de evidencia autónomo. Existen campos de texto, pero el envío queda bloqueado si no se adjunta al menos una fotografía. La columna de la base de datos destinada al texto libre de la evidencia, además, no se escribe ni se lee en ningún punto del código.

No hay control sobre los formatos admitidos. El contrato nombra tres formatos de imagen. El sistema acepta cualquiera, sin lista blanca ni validación en el servidor. El formato HEIC, propio de los dispositivos iPhone, se acepta en la subida pero no se previsualiza en los navegadores de uso mayoritario.

La configuración de tipos de evidencia carece de efecto. El panel de administración permite marcar qué tipos se exigen y almacena esa configuración, pero ningún punto del código la consulta para condicionar el formulario del participante. Desmarcar la fotografía no produce efecto alguno, ya que continúa siendo obligatoria.

1.3 Formalización del cambio de alcance

El desarrollador sostiene que la retirada del vídeo y del texto responde a una decisión de la Sociedad adoptada el 12 de junio de 2026.

La cláusula 8 del Anexo I exige que toda eliminación de funcionalidades acordadas se formalice mediante documento de control de cambios firmado por ambas partes, en el que se identifiquen cinco elementos: la descripción del cambio, su justificación y la parte solicitante, el impacto en alcance y plazos, el impacto económico y la fecha de entrada en vigor. La cláusula concluye estableciendo que el desarrollador no podrá reducir, eliminar ni aplazar unilateralmente el alcance acordado.

Se ha planteado que ese control de cambios lo constituirían las modificaciones registradas en el repositorio. Se examinó el historial completo, con el siguiente resultado. Ninguna de las noventa modificaciones registradas menciona la retirada del vídeo o del texto; la búsqueda por esos términos no devuelve coincidencia alguna relacionada con el alcance. La única modificación registrada el 12 de junio de 2026, fecha de la decisión invocada, versa sobre la documentación de direcciones de entorno.

Con independencia de ese resultado, un registro de modificaciones no satisfaría la cláusula ni aunque documentara el cambio. Se trata de un acto unilateral del desarrollador, carece de firma de la Sociedad y no identifica a la parte solicitante. Acredita qué se modificó y en qué momento, pero no acredita acuerdo entre las partes.

La reducción de alcance queda, por tanto, documentada por una sola de las partes y sin formalizar. El acta de aceptación que el desarrollador invoca como respaldo permanece sin firmar, en estado de plantilla.

1.4 Política de copias de seguridad

El apartado 3.2 del Anexo I exige copias de seguridad automáticas diarias, con retención mínima de treinta días y verificación periódica de la capacidad de restauración. Los tres requisitos incumplen, y el propio desarrollador lo documenta:

Exigencia contractual	Estado documentado por el desarrollador
Retención mínima de 30 días	Siete días. La recuperación a punto en el tiempo consta como acción pendiente de puesta en producción
Cobertura de las evidencias	Las copias no incluyen los ficheros de almacenamiento, esto es, las fotografías
Verificación periódica de restauración	El registro de ensayos contiene una única línea, con la anotación "pendiente"

1.5 Protección de datos: retención indefinida por defecto

El apartado 3.1 exige que la plataforma se diseñe conforme a los principios de privacidad desde el diseño y por defecto, con inclusión expresa de la minimización de datos, la limitación de la finalidad y las políticas de retención.

El mecanismo de purga existe, está correctamente implementado y cuenta con prueba automatizada. El problema reside en el valor predeterminado. La columna que fija el plazo de retención no es obligatoria ni tiene valor por defecto, y la purga actúa únicamente sobre las campañas que lo tengan cumplimentado. El manual de administración lo confirma al advertir que, si el campo se deja vacío, no se produce purga automática.

Una campaña creada sin cumplimentar ese campo conserva de forma indefinida fotografías de personas identificables. Ello contraviene el principio de privacidad por defecto que la cláusula exige y que el artículo 25.2 del Reglamento General de Protección de Datos impone.

A lo anterior se añade que la interfaz de ajustes ofrece al usuario la supresión de sus datos personales, mientras que el código se limita a revocar su pertenencia al portal y a cerrar la sesión. No existe ninguna vía de supresión ni de anonimización, de modo que el registro con su nombre y su dirección de correo permanece. Se trata de una promesa de interfaz carente de respaldo funcional. El consentimiento relativo a los Términos, por su parte, figura bloqueado en la interfaz y no puede retirarse, pese a que el servidor sí lo permitiría.

1.6 Reglas de participación: la elegibilidad no se aplica

El módulo 2 exige poder configurar criterios de elegibilidad. El panel ofrece elegir entre el conjunto de la empresa o un departamento concreto, y almacena la elección.

Ese valor no se comprueba en ningún momento durante la inscripción. Todas las referencias localizadas en el código corresponden a operaciones de escritura, clonado o presentación en pantalla. El modelo de datos, además, no contempla campo alguno de departamento en el usuario, por lo que la regla resulta inaplicable por construcción. Cualquier miembro del portal puede inscribirse en una campaña reservada a otro departamento.

Las fechas de vigencia de campaña presentan idéntico comportamiento: se configuran y se muestran, pero no producen ningún efecto restrictivo. Una campaña activa cuya fecha de finalización haya transcurrido continúa admitiendo inscripciones hasta que un administrador la pause manualmente.

1.7 Aceptación y defectos

El acta de aceptación permanece sin firmar, en estado de plantilla y con la tabla de firmas vacía. La cláusula 2.2 la enumera entre los entregables exigibles.

En cuanto al criterio del apartado 2.3, que condiciona la aceptación a la inexistencia de defectos críticos o mayores que impidan el uso normal, conviene precisar el argumento. El cuerpo del acuerdo define el defecto relevante como aquel que impida o limite de forma significativa el uso del entregable conforme a los requisitos funcionales acordados. Una vulnerabilidad de seguridad no impide el uso, de manera que el encuadre directo resulta débil.

El encuadre sólido es otro. Ese mismo apartado exige que la plataforma haya sido utilizada en los dos pilotos reales previstos. La verificación de seguridad realizada en agosto acreditó que el administrador de cualquier empresa cliente puede obtener acceso a los datos del resto. Una plataforma en la que un piloto accede a los datos del otro no se encuentra funcionalmente preparada para el uso que el propio Anexo I define como objetivo.

2. Extremos cumplidos

Reclamar aquello que ha sido entregado debilita la posición contractual, razón por la cual conviene dejar constancia.

El módulo 3, relativo a la gestión de cadenas, cumple sus ocho requisitos y presenta una construcción superior a la exigible: las reglas de negocio se imponen mediante restricciones y disparadores en la base de datos, y no únicamente en la capa de aplicación. El módulo 4, relativo a las pulseras con código QR, cumple, si bien con la salvedad de que el código es único por campaña y no por pulsera, lo que obliga a introducir manualmente el código lateral y resta automatismo al escaneo. El módulo 8, relativo al flujo de usuario, cumple sus seis requisitos. El módulo 6, relativo a la validación manual, cumple, incluida la trazabilidad completa de cada decisión sobre un registro de auditoría inmutable. El módulo 9 cuenta con pruebas automatizadas de extremo a extremo.

La documentación mínima exigida por el apartado 5.1 se encuentra prácticamente completa, con documento de arquitectura y diagramas, descripción del modelo de datos, manuales de administración y de usuario, inventarios y procedimientos de copia de seguridad. Los entornos de Validación y Producción están separados en los niveles de base de datos, rama de código y proceso de despliegue.

Merece constancia que la documentación del desarrollador es honesta y declara con precisión sus propios pendientes. Buena parte de los incumplimientos recogidos en este informe se acreditan con sus propios documentos. El problema no radica, por tanto, en la opacidad, sino en que diversos entregables contractuales figuran documentados como planificados en lugar de ejecutados. La única declaración que afirma cumplimiento categórico, la relativa a la ausencia de dependencia personal, es precisamente aquella que el repositorio contradice.

3. Cuadro resumen

Cláusula	Materia	Dictamen
2.2 · 6.1 · 6.3	Titularidad y control de activos	**Incumple**
6.4 · 5.2	Dependencia de cuentas personales	**Incumple**
Anexo I, Mód. 2 y 5	Tipos de evidencia admitidos	**Incumple**
Anexo I, cláusula 8	Formalización del cambio de alcance	**Incumple**
Anexo I, 3.2	Copias de seguridad	**Incumple en sus tres requisitos**
Anexo I, 3.1	Privacidad por defecto y supresión de datos	**Incumple**
Anexo I, Mód. 2	Criterios de elegibilidad	**Incumple**
2.2	Registro de aceptación firmado	**No emitido**
Anexo I, Mód. 3, 4, 6, 8, 9	Funcionalidad principal	**Cumple**
Anexo I, 5.1	Documentación	**Cumple**

4. Orden de prioridad para la reclamación

Tres incumplimientos admiten defensa sin margen de discusión, por resultar verificables con datos objetivos y no depender de criterio técnico.

1. Primero, la titularidad de los activos. El repositorio reside en una cuenta personal, la Sociedad carece de permisos de administración y ningún activo ha sido transferido. La comprobación es inmediata y afecta a la continuidad del negocio, no solo al cumplimiento contractual.

2. Segundo, las copias de seguridad. Siete días de retención frente a los treinta exigidos, las fotografías sin respaldo alguno y ningún ensayo de restauración realizado. Lo documenta el propio desarrollador.

3. Tercero, los tipos de evidencia. El vídeo no existe, el texto no constituye un tipo autónomo y la reducción de alcance no se ha formalizado conforme a la cláusula 8. El historial del repositorio, examinado, tampoco la documenta.

La retención indefinida de datos personales por defecto y la supresión ofrecida pero no implementada requieren tratamiento separado. No constituyen únicamente un incumplimiento contractual: exponen a la Sociedad, en su condición de responsable del tratamiento, frente a la autoridad de protección de datos, con independencia de lo que finalmente se acuerde con el desarrollador.