

TÉRMINOS Y CONDICIONES DE USO — CONNECTILOGS

Entre **10dencehisphard SLU, cdmon** (en adelante, el **Proveedor**) y la persona física o jurídica que contrata, accede o utiliza ConnectiLogs (en adelante, el **Ciente** o el **Usuario**, según corresponda), se acuerdan los presentes Términos y Condiciones de Uso (en adelante, el **Contrato**).

Este documento regula el acceso, uso, prestación, limitaciones, disponibilidad, responsabilidades, tratamiento de datos y demás aspectos vinculados al servicio ConnectiLogs.

LEY APLICABLE Y JURISDICCIÓN

El presente contrato se rige por la legislación española. Las partes se someten a los Juzgados y Tribunales de Barcelona, renunciando expresamente a cualquier otro fuero que pudiera corresponderles.

OBJETO DEL CONTRATO

El presente Contrato tiene por objeto regular las condiciones bajo las cuales el Proveedor pone a disposición del Cliente el servicio **ConnectiLogs**, una plataforma orientada a la recopilación, ingesta, almacenamiento, normalización, consulta, correlación, análisis y visualización de registros de actividad, eventos técnicos y señales de seguridad asociados a los servicios contratados por el Cliente.

ConnectiLogs permite, entre otras funciones, la visualización de información mediante paneles de control (dashboards) y la generación de consultas de datos históricos y la obtención de indicadores relacionados con actividad, disponibilidad, rendimiento, alertas o amenazas detectadas.

El Servicio tiene naturaleza instrumental y de apoyo. Su finalidad es facilitar al Cliente el acceso ordenado a información técnica y operativa, pero no constituye por sí mismo un sistema de protección absoluta, ni una garantía de ausencia de incidentes, ataques, errores, pérdidas de información o interrupciones.

ACEPTACIÓN DEL CONTRATO

El acceso al Servicio implica la aceptación íntegra del presente Contrato. Si el Cliente no está de acuerdo con cualquiera de sus cláusulas, deberá abstenerse de acceder o utilizar ConnectiLogs.

DEFINICIONES

A efectos de este Contrato, los términos siguientes tendrán el significado que se indica:

Servicio: la plataforma ConnectiLogs, incluyendo sus funcionalidades, interfaces, API, paneles, módulos, desarrollos, integraciones, documentación y actualizaciones.

Ciente: persona física o jurídica que contrata el Servicio o para la que se presta el Servicio.

Usuario: persona que accede al Servicio con credenciales válidas, ya sea en nombre propio o del Cliente.

Datos: toda la información procesada, consultada, almacenada o visualizada a través de ConnectiLogs.

Logs: registros técnicos, de actividad, de eventos o de seguridad generados por sistemas, aplicaciones, cuentas, servicios, infraestructura o acciones de usuario.

Fuente de datos: origen concreto desde el que se obtienen los logs o eventos.

Dashboard: panel o vista de representación gráfica o tabular de datos.

Fase beta: periodo en el que el Servicio se encuentra en pruebas, validación, evolución o preproducción, y en el que ciertas funcionalidades pueden no estar estabilizadas o pueden cambiar sin previo aviso.

Incidencia: cualquier interrupción, error, degradación, inconsistencia, fallo de visualización, pérdida temporal de disponibilidad o comportamiento no esperado del Servicio.

Dato personal: cualquier información relativa a una persona física identificada o identificable.

Tratamiento: cualquier operación realizada sobre datos personales, como recogida, registro, organización, conservación, consulta, extracción, comunicación o supresión.

DESCRIPCIÓN DETALLADA DEL SERVICIO

ConnectiLogs está diseñado para proporcionar al Cliente una vista centralizada de actividad y eventos técnicos procedentes de sus servicios contratados con el Proveedor y, en su caso, de otras fuentes compatibles que se habiliten expresamente.

El Servicio puede incluir, según configuración, plan contratado y estado de desarrollo, las siguientes capacidades:

- ingestión de logs y eventos
- normalización y estructuración de información procedente de distintas fuentes
- indexación y almacenamiento para consulta posterior
- consulta por filtros, rangos temporales, fuentes, servicios, colecciones o criterios equivalentes
- visualización de consultas mediante diferentes tipos de gráficos o tablas

El Cliente reconoce que el Servicio es una herramienta de observabilidad y análisis, no una promesa de resultado. El hecho de que un evento no aparezca en ConnectiLogs no significa necesariamente que no haya ocurrido. Del mismo modo, la presencia de un evento, alerta o indicador no implica automáticamente que exista una amenaza real, ya que pueden producirse falsos positivos, retrasos de ingesta, incidencias en la ingesta o enriquecimiento de datos.

NATURALEZA DEL SERVICIO Y AUSENCIA DE GARANTÍA ABSOLUTA

El Cliente acepta expresamente que ConnectiLogs:

- no garantiza la detección de la totalidad de amenazas, errores, accesos indebidos, fraudes, fallos de configuración o incidentes de seguridad

- no sustituye la supervisión humana, la configuración segura de sistemas, la administración técnica ni la adopción de medidas preventivas por parte del Cliente
- no reemplaza herramientas de backup, monitorización, firewall, antivirus, EDR, SIEM, IDS/IPS u otras soluciones de seguridad o de continuidad de negocio
- no asegura exactitud perfecta, integridad perfecta o disponibilidad permanente de toda la información
- no debe considerarse una fuente única o exclusiva de verdad para decisiones críticas, teniendo los propios logs del servicio siempre disponibles

El Cliente asume que la interpretación de los datos requiere criterio técnico. Cualquier decisión basada en la información de ConnectiLogs deberá valorarse junto con otras evidencias, procedimientos y controles propios del Cliente.

FASE BETA

Condición beta

Cuando el Servicio, una funcionalidad concreta, una integración, una API, un panel o un módulo se encuentren en fase beta, el Cliente lo acepta expresamente como una versión en evolución, no plenamente estabilizada, destinada a validación real, recopilación de feedback y corrección progresiva.

Consecuencias de la fase beta

Durante la fase beta, el Cliente acepta que:

- pueden existir errores, comportamientos inesperados, fallos parciales o degradaciones
- algunas funciones pueden cambiar, desaparecer, renombrarse o reubicarse sin aviso previo
- la documentación puede estar incompleta o desactualizada en ciertos puntos
- la experiencia de uso puede variar respecto de futuras versiones estables
- la disponibilidad puede ser inferior a la de un servicio en producción
- los datos pueden requerir modificaciones o reconstrucciones técnicas
- ciertas funcionalidades pueden activarse solo para determinados clientes, planes o grupos de prueba

Sin SLA estricto en beta

Salvo pacto expreso en contrario, la fase beta no estará sujeta a un SLA garantizado ni a compromisos de nivel de servicio equivalentes a los de una versión en producción. El Proveedor podrá priorizar estabilidad, corrección y validación funcional frente a disponibilidad continua o rapidez.

Sin garantía de continuidad funcional

Durante beta, el Cliente acepta que una funcionalidad puede:

- modificarse por razones técnicas
- quedar temporalmente deshabilitada
- convertirse en funcionalidad de pago
- ser sustituida por otra solución
- no llegar a producción si el Proveedor decide descartarla

Participación y Feedback

Al participar en el beta, el Cliente acepta colaborar activamente mediante:

- Reporte de errores, incidencias o comportamientos inesperados
- Feedback sobre funcionalidades y experiencia de uso
- Participación en encuestas o entrevistas si así se solicita

El Proveedor podrá utilizar el feedback proporcionado para mejorar el Servicio sin obligación de compensación. Las contribuciones del Cliente no se considerarán confidenciales, salvo acuerdo expreso contrario.

Paso de beta a producción

La transición desde beta a producción, si se produce, podrá implicar:

- cambios de interfaz
- cambios en límites o cuotas incluso llegando a eliminar características
- cambios en retención
- cambios en el modelo comercial
- cambios en disponibilidad de módulos
- migración de datos o modificación

El Proveedor intentará minimizar el impacto, pero no garantiza que la transición sea totalmente transparente.

Duración de la beta

La duración de la fase beta será determinada unilateralmente por el Proveedor, en función de la madurez técnica, la estabilidad operativa, el volumen de incidencias y la calidad de uso observada.

USOS PERMITIDOS Y USOS PROHIBIDOS

Uso permitido

El Cliente podrá utilizar ConnectiLogs únicamente para finalidades legítimas y relacionadas con la gestión, observación, análisis o auditoría de sus propios servicios o de aquellos para los que disponga de autorización válida.

Usos prohibidos

Queda prohibido, de forma enunciativa y no limitativa:

- utilizar el Servicio con fines ilícitos, fraudulentos o contrarios a la buena fe
- acceder a datos de terceros sin autorización
- intentar vulnerar la autenticación, permisos o controles técnicos
- explotar vulnerabilidades o realizar pruebas de intrusión sin permiso
- introducir código malicioso, scripts dañinos o cargas que comprometan la plataforma
- realizar consultas masivas o automatizadas que degraden el Servicio
- revender, sublicenciar o explotar el Servicio sin autorización
- copiar, descompilar, modificar o realizar ingeniería inversa sobre el software, salvo en los casos expresamente permitidos por la ley

El Proveedor podrá adoptar medidas técnicas y contractuales para impedir estos usos.

OBLIGACIONES DEL CLIENTE

El Cliente se compromete a:

- conservar y proteger sus credenciales para evitar accesos no legítimos
- limitar el acceso a personal autorizado
- comunicar incidencias de seguridad o accesos no autorizados
- usar el Servicio conforme a la ley, la normativa aplicable y este Contrato
- no confiar exclusivamente en ConnectiLogs para decisiones críticas sin validación adicional
- realizar sus propias copias de respaldo cuando proceda
- cumplir sus obligaciones de información, consentimiento, transparencia o legitimación cuando los datos tratados incluyan datos personales o datos de terceros.

El Cliente será el único responsable de las consecuencias derivadas de una mala configuración, de la falta de supervisión o de un uso incorrecto de la información obtenida.

OBLIGACIONES DEL PROVEEDOR

El Proveedor se compromete a:

- Prestar el Servicio con diligencia profesional.

- Mantener la plataforma operativa dentro de las posibilidades técnicas de un entorno en fase beta.
- Comunicar interrupciones planificadas cuando sea razonablemente posible

El Proveedor no garantiza:

- Disponibilidad continua o libre de errores
- Que el Servicio cumpla requisitos específicos del Cliente
- Exactitud, integridad o puntualidad de los datos mostrados

El Proveedor podrá:

- introducir mejoras o actualizaciones
- corregir errores
- modificar el rendimiento o la arquitectura
- limitar el acceso por motivos de seguridad
- suspender temporalmente el Servicio por mantenimiento, migración o incidencia

El Proveedor no asume una obligación de resultado, salvo que se establezca expresamente por escrito.

CUENTA Y CREDENCIALES

El acceso al Servicio no requiere nuevas credenciales ni usuarios aparte de el del Panel de Control, es un servicio más como cliente de **cdmon**. El Cliente es responsable de:

- Mantener la confidencialidad de sus credenciales del panel de control.
- Notificar inmediatamente cualquier acceso no autorizado
- Asegurarse de que solo usuarios autorizados tengan acceso
- Proporcionar información veraz y actualizada

El Proveedor podrá suspender o cancelar cuentas con información falsa o que infrinjan estos términos.

DISPONIBILIDAD, MANTENIMIENTO Y CONTINUIDAD

Disponibilidad: Salvo que se pacte un SLA específico, el Servicio se prestará sobre la base de mejores esfuerzos, pudiendo experimentar interrupciones, ralentizaciones, ventanas de mantenimiento o indisponibilidades temporales.

Mantenimiento programado: El Proveedor podrá realizar tareas de mantenimiento correctivo, preventivo, evolutivo o de seguridad, incluso sin aviso previo cuando la urgencia técnica así lo requiera.

Mantenimiento no programado: En caso de incidencia grave, el Proveedor podrá intervenir sin preaviso para restablecer el Servicio, proteger la integridad de los datos o contener riesgos de seguridad.

Contingencias: El Cliente acepta que pueden existir retrasos en la ingesta, reprocesado de datos, colas de eventos, duplicidades temporales, diferencias horarias, huecos parciales o latencias entre la generación de un evento y su visualización.

LIMITACIONES TÉCNICAS DEL SERVICIO

El Cliente reconoce y acepta que el Servicio puede estar sujeto a limitaciones inherentes, entre otras:

- límites de volumen de datos
- límites de retención
- límites de tamaño por evento o archivo
- límites de frecuencia de consultas
- límites de concurrencia
- límites de exportación
- límites por plan o licencia
- dependencia de fuentes externas o integraciones de terceros
- variabilidad en tiempos de respuesta según carga y complejidad de consulta

El Proveedor podrá ajustar dichas limitaciones para preservar la estabilidad global del sistema, evitar abusos o adaptar el Servicio a nuevos requisitos técnicos.

EXACTITUD, INTEGRIDAD E INTERPRETACIÓN DE LOS DATOS

El Cliente acepta que los datos mostrados por ConnectiLogs pueden verse afectados por:

- retrasos de ingestión
- pérdidas de conectividad en la fuente
- errores de configuración
- formatos incompatibles
- eventos mal etiquetados
- agregaciones y filtros que simplifican la información
- políticas de retención y purga
- sincronizaciones incompletas
- alteraciones ajenas al control del Proveedor

Por tanto, el Cliente no podrá exigir responsabilidad al Proveedor por conclusiones basadas exclusivamente en una visualización parcial, agregada o retrasada de la información.

SEGURIDAD DE LA PLATAFORMA

Sin perjuicio de ello, el Cliente entiende que ningún sistema conectado a redes públicas puede considerarse infalible. En consecuencia:

- no existe garantía de invulnerabilidad
- pueden producirse incidentes de seguridad pese a la adopción de medidas razonables
- el Cliente debe mantener sus propias prácticas de seguridad, endurecimiento y supervisión

En caso de sospecha de abuso o de evento de seguridad, el Proveedor podrá bloquear accesos, limitar funciones, revocar tokens, reiniciar procesos o tomar otras medidas proporcionadas para contener el riesgo.

El Proveedor implementa medidas técnicas y organizativas diseñadas para proteger el Servicio y los datos procesados, incluyendo, pero no limitándose a:

- Cifrado en tránsito (TLS) y en reposo cuando aplique
- Controles de acceso basados en principios de mínimo privilegio
- Monitorización de seguridad y detección de anomalías
- Parcheo y actualización periódica de componentes
- Segmentación de redes y entornos

TRATAMIENTO DE DATOS PERSONALES Y PRIVACIDAD

El Cliente declara que dispone de base jurídica suficiente para comunicar o hacer tratar los datos que incorpore al Servicio. En particular, deberá asegurarse de que el tratamiento de logs, eventos o metadatos relativos a personas físicas cuenta con una legitimación adecuada, de que se cumple el deber de información cuando proceda y de que no se tratan datos prohibidos o innecesarios.

El Proveedor podrá actuar, según el caso, como encargado del tratamiento o como responsable del tratamiento respecto de determinados datos, siendo amparado por el contrato de encargado de tratamiento que se ha firmado para la prestación de servicios de hospedaje.

El Cliente reconoce que los logs pueden contener datos como IP, identificadores de sesión, marcas temporales, rutas de acceso, actividad de usuario, identificadores técnicos, metadatos de seguridad o elementos equivalentes que, directa o indirectamente, puedan relacionarse con una persona física.

El Cliente será responsable de:

- decidir qué datos introduce o habilita para su tratamiento
- informar a sus usuarios o terceros cuando sea obligatorio

- responder a derechos, reclamaciones o solicitudes que deriven de su relación con
- dichos datos cumplir sus propios deberes de conservación, minimización y limitación de finalidad.

CONSERVACIÓN Y RETENCIÓN DE DATOS

El Servicio podrá conservar datos durante el plazo asociado al plan contratado, a los límites operativos definidos por el Proveedor o a las obligaciones legales aplicables.

Finalizado dicho plazo o alcanzado el límite de almacenamiento, el Proveedor podrá:

- eliminar de forma automática datos antiguos
- bloquear nuevas cargas
- sustituir datos detallados por agregados
- requerir ampliación de plan o capacidad

El Cliente acepta que la retención no es indefinida y que, una vez vencido el periodo correspondiente, ciertos datos podrían no ser recuperables.

PROPIEDAD INTELECTUAL E INDUSTRIAL

Todos los derechos sobre ConnectiLogs, su código, diseño, arquitectura, marca, documentación, pantallas, modelos de datos, componentes, workflows, algoritmos, mejoras y evoluciones pertenecen al Proveedor.

Salvo autorización expresa por escrito, el Cliente no podrá:

- copiar, reproducir o distribuir el Servicio
- modificarlo o crear obras derivadas
- descompilarlo, desensamblarlo o aplicar ingeniería inversa
- extraer de forma sistemática datos o documentación con fines de reproducción del producto
- utilizar marcas, logotipos o signos distintivos del Proveedor fuera de lo permitido

Nada de lo previsto en este Contrato otorga al Cliente derechos de propiedad sobre el software o la plataforma, sino únicamente un derecho de uso limitado, revocable y no exclusivo según las condiciones pactadas.

SOPORTE Y ATENCIÓN AL CLIENTE

El alcance del soporte dependerá del plan contratado, de la naturaleza de la incidencia y de la fase del Servicio.

Salvo pacto específico, el soporte podrá limitarse a:

- incidencias operativas razonables

- consultas funcionales generales solamente para planes de pago. La vía normal serán los documentos de ayudas publicados.
- verificación de errores reproducibles
- ayuda sobre uso estándar del Servicio solamente para planes de pago. La vía normal serán los documentos de ayudas publicados.

Queda fuera del soporte ordinario, salvo acuerdo expreso:

- consultoría avanzada personalizada
- desarrollos a medida
- análisis forense complejo
- recuperación de datos fuera del periodo de retención
- integración con sistemas de terceros no homologados

El Proveedor podrá priorizar tickets en función de severidad, impacto, plan contratado y disponibilidad de recursos.

MODIFICACIONES DEL SERVICIO Y DEL CONTRATO

El Proveedor se reserva el derecho a modificar, actualizar, sustituir o eliminar funcionalidades del Servicio, así como a adaptar este Contrato cuando sea necesario por razones legales, técnicas, de seguridad, comerciales o de evolución del producto.

Cuando los cambios sean sustanciales, el Proveedor procurará comunicarlo por los medios disponibles. El uso continuado del Servicio tras la entrada en vigor de las modificaciones implicará la aceptación de las mismas.

Si el Cliente no aceptara los cambios, podrá solicitar la baja del Servicio, sin perjuicio de lo previsto en materia de facturación, retención de datos o exportación.

TERMINACIÓN, SUSPENSIÓN Y BAJA

El Proveedor podrá suspender o terminar el acceso al Servicio, total o parcialmente, en los siguientes supuestos:

- incumplimiento del presente Contrato
- impago
- uso fraudulento o abusivo
- riesgo grave para la seguridad o disponibilidad
- requerimiento legal o de autoridad competente
- finalización del periodo de beta sin continuidad del servicio
- cese del producto o de alguna de sus líneas funcionales

La terminación podrá implicar la pérdida de acceso a paneles, API, reportes, históricos o configuraciones asociadas.

El Cliente será responsable de extraer o exportar los datos que desee conservar dentro del plazo que el Proveedor, razonablemente y según capacidad técnica, habilite al efecto.

LIMITACIÓN DE RESPONSABILIDAD

En la máxima medida permitida por la ley, el Proveedor no responderá por:

- daños indirectos, incidentales, especiales o consecuenciales
- pérdida de beneficios, ingresos, contratos o reputación
- pérdida de negocio, oportunidad o clientela
- decisiones adoptadas por el Cliente sobre la base de los datos del Servicio
- daños derivados de errores de configuración del Cliente
- indisponibilidades causadas por terceros, redes, proveedores externos, fuerza mayor o mantenimiento
- pérdida o alteración de datos cuando derive de acciones u omisiones del Cliente o de terceros no controlados por el Proveedor
- falta de detección de una amenaza, alerta o evento de seguridad
- El Proveedor no será responsable por fallos o retrasos causados por circunstancias ajenas a su control razonable, incluyendo, pero no limitado a: desastres naturales, incendios, inundaciones, terremotos, epidemias, actos de terrorismo, guerras, disturbios civiles, fallos en telecomunicaciones, cortes de electricidad, acciones de autoridades gubernamentales, sabotajes, ataques cibernéticos masivos o cualquier otra causa fuera del control razonable del Proveedor.

Cuando la legislación aplicable permita limitar la responsabilidad, esta quedará, en su caso, limitada al importe efectivamente satisfecho por el Cliente por el Servicio durante el periodo inmediatamente anterior al hecho que origine la reclamación, salvo que se establezca un límite distinto en una condición particular o en la normativa imperativa aplicable.

Nada de lo dispuesto en esta cláusula excluirá la responsabilidad que legalmente no pueda ser limitada.

INDEMNIDAD

El Cliente mantendrá indemne al Proveedor frente a reclamaciones, sanciones, pérdidas, costes, daños o gastos derivados de:

- uso ilícito o no autorizado del Servicio por parte del Cliente o de sus usuarios
- incumplimiento normativo en el tratamiento de datos por parte del Cliente
- introducción de contenidos ilegales o derechos de terceros

- incumplimiento de este Contrato
- mala configuración, negligencia o falta de diligencia en la supervisión del Servicio

Esta obligación incluirá, cuando proceda, costas razonables de defensa, asesoramiento y gestión de la incidencia.