
WHITE PAPER

MasRisk

Compartición Soberana de Datos de Fraude y Scoring bajo Estándares Europeos

Agosto 2026

«Financiado por la Unión Europea - Next Generation EU. Sin embargo, los puntos de vista y las opiniones expresadas son únicamente los del autor o autores y no reflejan necesariamente los de la Unión Europea o la Comisión Europea. Ni la Unión Europea ni la Comisión Europea pueden ser consideradas responsables de las mismas»

INDICE

1. Introducción y Contexto del Proyecto	3
2. El Desafío del Riesgo y el Fraude en Entornos Digitales	3
3. Arquitectura Tecnológica de la Solución (MVDS)	4
4. Casos de Uso de Negocio e Interoperabilidad.....	5
4.1 Onboarding Digital Seguro y Validación de Identidad	6
4.2 Prevención de Fraude en Apertura de Cuentas y Transacciones Críticas	6
4.3 Evaluación Alternativa de Scoring y Financiación	6
5. Modelado Analítico y Lógicas de Inteligencia Artificial	6
5.1 Enfoque del Modelo y Lógicas de Decisión	6
5.2 Algoritmo y Optimización.....	7
5.3 Calibración del Riesgo	7
5.4 Resultados de Validación y Estabilidad Temporal	7
6. Catálogo de APIs de Fraude e Identidad Digital	8
7. Retos Técnicos y Operativos Afrontados	8
8. Lecciones Aprendidas	9
9. Transferencia de Conocimiento y Contribución al Ecosistema Europeo	9
10. Conclusiones	10

1. INTRODUCCIÓN Y CONTEXTO DEL PROYECTO

En el escenario actual de transformación digital, los datos se han consolidado como un activo estratégico indispensable para mitigar riesgos financieros y prevenir el fraude de identidad. No obstante, las organizaciones que manejan información de carácter sensible se enfrentan al desafío de intercambiar esta información garantizando de manera absoluta la seguridad, el cumplimiento riguroso del Reglamento General de Protección de Datos (RGPD) y, por encima de todo, la soberanía del dato.

El proyecto **MasRisk** (*Modelo de compartición de datos en los ámbitos de fraude y scoring*), (TSI-100130-2024-19) financiado bajo el Plan de Recuperación, Transformación y Resiliencia - Next Generation EU (Programa Espacios de Datos Sectoriales), nace para dar respuesta a este desafío. Liderado por **Orange España SAU** con la colaboración de un socio especializado en información crediticia y analítica de riesgo para las fases de prueba y validación, el proyecto ha diseñado, desarrollado, desplegado y validado un **Espacio de Datos Mínimo Viable (MVDS - Minimum Viable Dataspace)**.

Haciendo uso del conector abierto de referencia **Eclipse Dataspace Components (EDC)** e integrando estándares globales de red como **GSMA Open Gateway** y las directrices de **Gaia-X** e **IDSA**, MasRisk demuestra la viabilidad técnica y operativa de compartir información de valor en un entorno descentralizado, gobernada por políticas y libre de intermediarios centralizados.

Este WhitePaper técnico difunde de manera abierta los resultados del proyecto para transferir el conocimiento adquirido al tejido productivo, tecnológico e institucional interesado en la implantación de espacios de datos seguros en Europa.

2. EL DESAFÍO DEL RIESGO Y EL FRAUDE EN ENTORNOS DIGITALES

La proliferación de transacciones y contrataciones no presenciales ha expuesto a las organizaciones a riesgos financieros y operativos complejos:

- **Limitaciones de los Modelos de Riesgo Tradicionales**

Los modelos de scoring convencionales dependen en gran medida de historiales de crédito presentes en burós tradicionales. Esto penaliza o impide la correcta evaluación de clientes con perfiles de información reducida (*thin files*) o sin historial financiero previo, limitando la conversión de las empresas. Las señales de red y comportamiento de uso del sector de las telecomunicaciones ofrecen una fuente

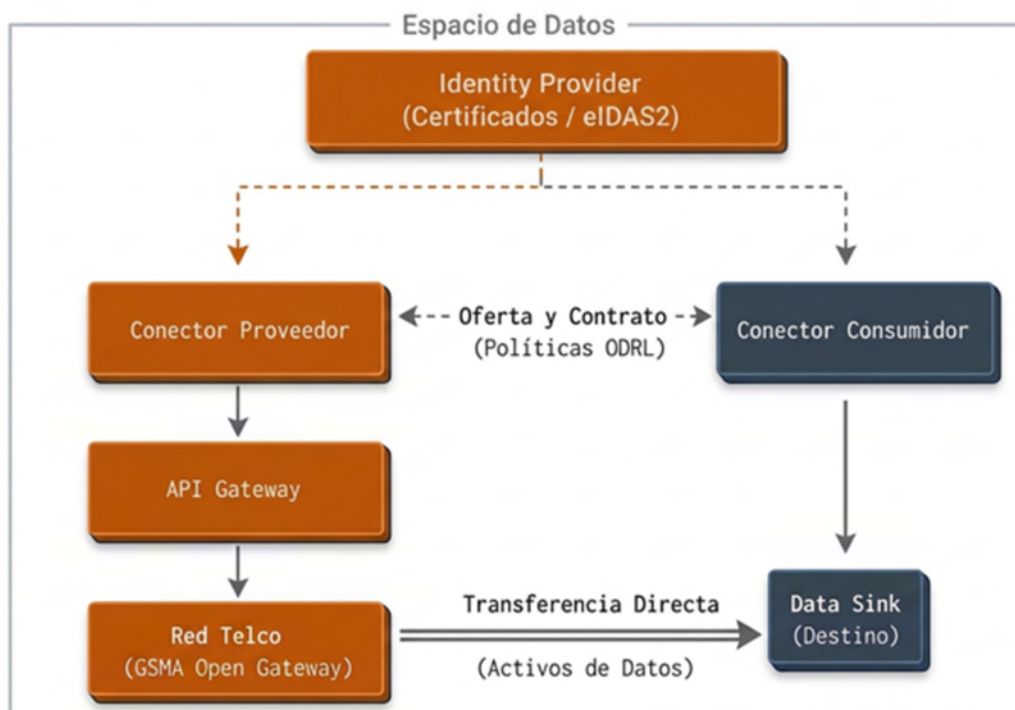
alternativa y de gran valor predictivo para enriquecer estas evaluaciones y contribuir a mitigar la exclusión financiera.

- **Amenazas de Fraude y Suplantación Dinámica**

Procesos críticos como el alta digital de clientes (*onboarding*) o la autorización de transacciones sensibles se enfrentan de manera continua a técnicas como la suplantación de tarjetas SIM (*SIM Swap*) o el robo de cuentas (*Account Takeover*). Los métodos reactivos o de autenticación basados exclusivamente en códigos temporales por SMS (OTP) resultan vulnerables. El mercado demanda indicadores técnicos de red, provistos directamente por el operador en tiempo real, que confirmen la integridad de la línea de forma transparente y sin fricciones para el usuario.

3. ARQUITECTURA TECNOLÓGICA DE LA SOLUCIÓN (MVDS)

La arquitectura de MasRisk se ha implementado mediante un enfoque de **infraestructura cloud-native basada en contenedores y microservicios**. La plataforma adopta el framework **Eclipse Dataspace Components (EDC)** y el protocolo **Dataspace Protocol (DSP)**, asegurando que la compartición de datos se realice bajo los principios de descentralización y soberanía.



Componentes clave de la arquitectura de referencia:

1. **Separación Lógica de Planos (Control Plane vs. Data Plane):**
 - o Control Plane (Plano de Control): Se encarga exclusivamente de las fases de gobernanza y control. Gestiona la negociación automática de contratos, la consulta y descubrimiento de activos en el catálogo de datos federado, la validación de identidades y la verificación de las reglas de cumplimiento. Este componente nunca entra en contacto con el flujo de datos de negocio.
 - o Data Plane (Plano de Datos): Es el motor de transferencia. Únicamente tras la firma digital de un acuerdo contractual válido (Contract Agreement) autorizado por el Control Plane, el Data Plane ejecuta la transferencia cifrada de datos de forma directa y segura entre los participantes (proveedor y consumidor), garantizando la no persistencia de información en intermediarios.
2. **Gestión de Identidades Descentralizadas (Identity Hub):** La autenticación de los participantes se articula mediante identificadores descentralizados (**DID**) y credenciales verificables, eliminando la dependencia de un proveedor de identidad centralizado y facilitando el alineamiento de la confianza digital europea (**eIDAS2**) y los futuros monederos digitales (**EU ID Wallet**) utilizando mecanismos avanzados de identidad descentralizada.
3. **Gobernanza mediante Políticas Contractuales (ODRL):** Los activos del catálogo se exponen asociados a contratos de uso expresados en el estándar ODRL (Open Digital Rights Language). El motor de políticas (*Policy Engine*) evalúa automáticamente si el consumidor cumple con las reglas del contrato antes de autorizar el acceso al dato.
4. **Criptografía y Gestión de Secretos:** La seguridad de las claves criptográficas, certificados y tokens necesarios para la confianza del ecosistema está delegada en **un servicio seguro de gestión de secretos criptográficos, asegurando tolerancia a fallos, aislamiento y resiliencia** de la plataforma.
5. **Pasarela de APIs:** Una **solución corporativa de gestión de APIs** actúa como pasarela corporativa gestionando la seguridad perimetral, el control de acceso inicial mediante autenticación segura y el enrutamiento hacia las APIs de red.

4. CASOS DE USO DE NEGOCIO E INTEROPERABILIDAD

La solución tecnológica de MasRisk ha sido diseñada para ser integrada de forma directa en los motores de decisión de las organizaciones participantes, habilitando los escenarios operativos de alto impacto descritos a continuación.

4.1 ONBOARDING DIGITAL SEGURO Y VALIDACIÓN DE IDENTIDAD

En procesos de alta de nuevos clientes en sectores como banca, seguros o comercio electrónico, MasRisk permite validar en tiempo real si los atributos de identidad proporcionados por un solicitante coinciden de forma consistente con los registros contractuales del operador móvil, disminuyendo el fraude de identidad y la creación de perfiles sintéticos de forma no intrusiva.

4.2 PREVENCIÓN DE FRAUDE EN APERTURA DE CUENTAS Y TRANSACCIONES CRÍTICAS

Antes de autorizar operaciones de alto riesgo o la apertura de cuentas de forma completamente digital, las entidades consumidoras pueden interconectar su conector con el de MasOrange para comprobar anomalías recientes en la red móvil. Esto permite activar controles de seguridad adicionales de forma dinámica y automatizada, mitigando intentos de suplantación en tiempo real.

4.3 EVALUACIÓN ALTERNATIVA DE SCORING Y FINANCIACIÓN

Las entidades de financiación al consumo o plataformas de pago aplazado pueden consumir indicadores de score de riesgo alternativo calculados a partir de patrones de comportamiento de telecomunicaciones.

Indicador de Impacto: La combinación de señales telco y de comportamiento con modelos predictivos avanzados permite mejorar de forma sustantiva la capacidad predictiva respecto a los modelos basados únicamente en información financiera tradicional, facilitando la inclusión de perfiles sin historial crediticio previo de manera robusta y disminuyendo los índices de morosidad.

5. MODELADO ANALÍTICO Y LÓGICAS DE INTELIGENCIA ARTIFICIAL

Para proveer los indicadores de scoring dentro del espacio de datos, se han entrenado y validado modelos predictivos avanzados integrados con los sistemas corporativos existentes.

5.1 ENFOQUE DEL MODELO Y LÓGICAS DE DECISIÓN

El modelo se ha entrenado sobre un volumen masivo de datos históricos agregados y debidamente anonimizados, utilizando una clasificación binaria de perfiles solventes frente a perfiles con presencia de incidencias de pago en un horizonte temporal de rango medio. Las variables predictoras seleccionadas cubren tres dimensiones analíticas:

- Variables Conductuales: Historial de pagos de servicios de red, regularidad en la facturación y presencia de incidencias operativas previas.
- Variables Sociodemográficas: Variables sociodemográficas agregadas y debidamente tratadas para minimizar sesgos.
- Variables Sectoriales: Densidad y volumen de servicios contratados e importes medios.

5.2 ALGORITMO Y OPTIMIZACIÓN

Para capturar de forma óptima las relaciones no lineales y las interacciones complejas de las variables, se implementó un algoritmo de aprendizaje supervisado de gradiente boosting. Los parámetros del modelo fueron optimizados mediante técnicas avanzadas de búsqueda y optimización matemática, asegurando la máxima capacidad de generalización del algoritmo y previniendo el sobreajuste.

5.3 CALIBRACIÓN DEL RIESGO

Para ofrecer un producto de scoring de alta aplicabilidad comercial y evitar la polarización de las probabilidades en los extremos, **se incorporaron mecanismos de calibración e interpretación del riesgo orientados a facilitar el uso operativo de los resultados**. Esta transformación convierte las probabilidades en una escala de distribución homogénea donde cada decil o intervalo de riesgo mantiene una densidad constante de incidencias, lo que permite a los analistas de negocio diseñar políticas de admisión progresivas, estables y equilibradas.

5.4 RESULTADOS DE VALIDACIÓN Y ESTABILIDAD TEMPORAL

La robustez técnica del modelo ha sido evaluada mediante estrictos criterios de calidad y estabilidad temporal que garantizan la fiabilidad de las señales:

- **Poder de Discriminación:** El modelo final alcanza un índice Gini altamente competitivo y una excelente área bajo la curva ROC-AUC sobre conjuntos de prueba con desfase temporal, demostrando una capacidad predictiva muy superior y estable respecto a modelos de referencia lineales tradicionales. Los resultados obtenidos muestran niveles de discriminación y estabilidad temporal comparables a los observados en modelos avanzados utilizados en entornos productivos de gestión del riesgo.
- **Estabilidad de las Variables:** La consistencia de las distribuciones de los predictores en el tiempo se ha verificado mediante el cálculo del Índice de Estabilidad Poblacional (PSI), confirmando que las variables no sufren desviaciones ni degradación por estacionalidad.
- **Capacidad Discriminante Temporal:** Las pruebas estadísticas ratifican con elevada significación la capacidad del modelo para separar y ordenar de forma consistente a las poblaciones de bajo y alto riesgo a lo largo del tiempo.

6. CATÁLOGO DE APIs DE FRAUDE E IDENTIDAD DIGITAL

A través de la infraestructura del espacio de datos, se exponen de forma soberana APIs estandarizadas compatibles con la iniciativa global **GSMA Open Gateway (CAMARA)**:

- **SIM Swap Check:** Comprueba si se ha realizado un cambio reciente de tarjeta SIM en la línea del usuario para alertar sobre posibles secuestros de cuentas bancarias.
- **Device Swap:** Detecta si la SIM se ha introducido en un nuevo terminal móvil, aportando una señal de alerta de riesgo de suplantación.
- **Number Verification:** Valida automáticamente que el número de teléfono con el que interactúa una app web o móvil coincide exactamente con la línea de datos del operador, eliminando la necesidad de contraseñas SMS temporales y reduciendo la fricción.

7. RETOS TÉCNICOS Y OPERATIVOS AFRONTADOS

La implementación práctica de MasRisk ha supuesto superar desafíos significativos en el plano de la integración de sistemas y la ingeniería de datos:

- **Equilibrio entre simplicidad inicial y escalabilidad futura:** Lograr un diseño e implementación inicial sencillos que permitieran validar la tecnología en fases tempranas, pero manteniendo la estructura totalmente preparada para escalar hacia un ecosistema multi-actor y federado más complejo en etapas posteriores.
- **Adopción de EDC como núcleo tecnológico en un entorno productivo real:** La puesta en marcha de un conector EDC plenamente integrado en el flujo de producción real de un operador móvil como MasOrange requirió la resolución de retos de configuración, ajuste y estabilización del software.
- **Gestión de identidad y seguridad por diseño en la infraestructura:** Diseñar e implementar un modelo de seguridad robusto basado en identidades autosoberanas, aplicando políticas de mínimo privilegio y garantizando la protección absoluta del dato en un entorno cloud-native regulado.
- **Exigencia de integración de sistemas heterogéneos:** Coordinar de forma eficiente múltiples tecnologías y componentes heredados (APIs internas, pasarelas de red, bases de datos), asegurando la trazabilidad de los accesos y el control del dato sin introducir latencia.

8. LECCIONES APRENDIDAS

La ejecución de las actividades del proyecto nos deja un conjunto de aprendizajes clave de cara al despliegue futuro de espacios de datos:

- **Definir desde el inicio un modelo de datos claro y compartido:** La adopción de vocabularios semánticos y ontologías normalizadas desde las fases tempranas es indispensable para garantizar la correcta interoperabilidad y el descubrimiento automático de activos entre sectores.
- **Alinear expectativas de negocio con la evolución técnica del espacio de datos:** Es vital acoplar los hitos tecnológicos de la plataforma con la generación de valor de negocio real, evitando desarrollar infraestructuras complejas que carezcan de un caso de uso prioritario.
- **Definir el modelo de negocio de cada caso de uso:** El éxito comercial de un espacio de datos depende de un análisis previo de su propuesta de valor, el perfil del público objetivo, un esquema claro de consumo y un modelo de monetización definido para cada servicio.

9. TRANSFERENCIA DE CONOCIMIENTO Y CONTRIBUCIÓN AL ECOSISTEMA EUROPEO

Los resultados obtenidos en el proyecto MasRisk se han concebido con vocación de reutilización y transferencia al ecosistema europeo de espacios de datos. El proyecto ha promovido la adopción de estándares abiertos e interoperables como Eclipse Dataspace Components (EDC), Dataspace Protocol (DSP), ODRL, DID y GSMA Open Gateway, favoreciendo la creación de entornos de compartición de datos seguros, escalables y alineados con las iniciativas europeas de soberanía digital.

La publicación de este White Paper forma parte de la estrategia de difusión de resultados del proyecto, cuyo objetivo es compartir las lecciones aprendidas, retos tecnológicos y oportunidades de negocio identificadas durante la ejecución, contribuyendo al avance del estado del arte en materia de prevención del fraude, scoring alternativo y compartición soberana de datos.

10. CONCLUSIONES

El proyecto MasRisk ha demostrado con éxito la viabilidad de compartir información de fraude y scoring de riesgo respetando de forma estricta los principios de soberanía del dato, privacidad y seguridad exigidos por las directrices de la Unión Europea.

A nivel estratégico, el proyecto nos deja tres grandes conclusiones de cara al futuro de la economía del dato:

- "Los espacios de datos permiten compartir valor sin compartir control."
- "La combinación de Data Spaces y Open Gateway abre nuevos modelos de colaboración intersectorial."
- "Los operadores de telecomunicaciones pueden convertirse en proveedores de señales de confianza para la economía digital."