PEDRA

Anti-Money Laundering

A comprehensive platform for the prevention of money laundering and terrorist financing. From know-your-customer procedures to regulatory reporting, all within a single system.

izertis

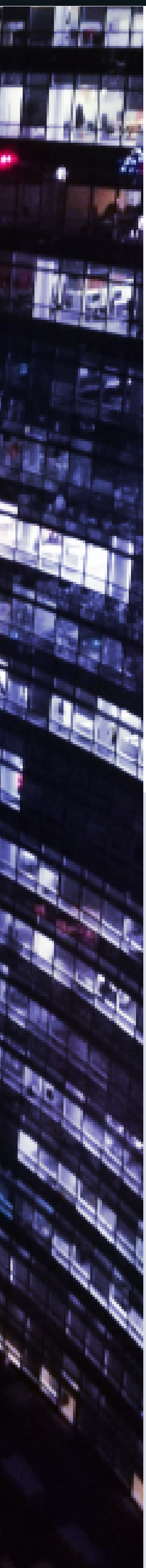
IZERTIS

2026

WHAT IS PEDRA

A single system for the entire regulatory compliance cycle

PEDRA® is a platform for the management, documentation, monitoring and control of activities relating to the prevention of money laundering and terrorist financing. It covers the entire cycle: know-your-customer procedures, cross-checking against lists, monitoring of operations, case management and reporting to SEPBLAC.



The challenge it addresses:
Compliance departments face increasing regulatory pressure, frequently changing sanctions lists and transaction volumes that cannot be reviewed manually. PEDRA® addresses four specific needs:

Autonomy in detection:
Implement new detection scenarios quickly, without relying on the software owner.

Integrated monitoring and analysis:
Traceability of each alert and overall categorisation of the client portfolio.

More accurate alerts:
Weighted, customisable indicators that reduce the number of false positives.

Priority risks addressed:
Know Your Customer (KYC/KYB) and sanctions programmes dealt with at source.

Configurable base module:
Data structure, business rules and parameterisation that each organisation adapts to its local regulations and internal control criteria, without having to rely on the supplier to create new scenarios.

Proven track record:
Over ten years in production at banking, investment and insurance organisations. An Izertis in-house product, with development and support provided by a local team in Spain.

PEDRA IN NUMBERS

Findings that support the proposal

Adoption and operational indicators compiled by organisations already using PEDRA.

99%	+800	+180
ACCURACY	**CUSTOMERS**	**COUNTRIES**
in detection and matching, with a low rate of false positives.	organisations and professional users operating on the platform.	coverage of jurisdictions in screening and reporting.

What an average organisation manages with PEDRA:
sustained volume of activity on a standard deployment.

+1M	+600k	+180
Target Customers	**Transactions/month**	**Daily contrasts**
Risk profiling and ongoing monitoring of the entire portfolio.	Operations monitored on a monthly basis against defined indicators.	Check against lists as part of the daily onboarding process for new customers.

Key figures relating to all PEDRA® installations. The actual volume depends on the size and activity of each organisation.

COMPREHENSIVE PLATFORM

Four capabilities, one platform

A suite that manages risk and ensures compliance with current regulations, with seamless transitions between stages. All information is entered once and feeds into the entire cycle.

KYC / KYB
Automated identity and ultimate beneficial owner verification using advanced OCR. Categorisation of the portfolio by risk profile and associated due diligence.

Global Screening
Real-time searches of sanctions lists, PEPs and adverse media. Compatible with FACTIVA DJ and WorldCheck, as well as the organisation's internal or manual lists.

Transactions
Continuous monitoring of suspicious activity based on rules and configurable indicators. Periodic batch analysis and real-time online response.

Reporting
Automatic generation of regulatory files ready for submission to SEPBLAC (DMO, F19/CTL) and standardised FATCA/CRS files by jurisdiction.

Comprehensive data, covering the entire cycle.
Every customer, contract and transaction is entered into PEDRA® just once and is then available for profiling, screening, alerts, case files and reporting. This eliminates duplicate data sources and reduces the risk of inconsistencies **between stages.**

HOW IT WORKS

From data to the decision to report

PEDRA® organises the work of the Prevention Unit into six interlinked stages. The organisation defines the criteria; the platform systematises the implementation and ensures traceability.

01

Definition of indicators:
The organisation defines the appropriate indicators to comply with regulations and its own control standards.

02

Configuration (Client / KYC)
The variables that make up each indicator and the risk profiling criteria are configured via the front-end.

03

Operational data entry and analysis
Customer accounts, products and transactions are imported from the organisation's transactional systems.

04

Alert generation:
The system automatically generates alerts for defined clients and operational processes. The alerts filter the information that is recorded in the case file.

05

Case Management:
Each case is processed with additional documentation and follow-up until a decision is made as to whether or not to report it, either as a DMO or an F19/CTL.

06

Reporting and traceability:
Files are archived with full traceability of all actions carried out on them.

SPECIALISED MODULES

Tools for each compliance role

The functionality is organised into modules with specific objectives, all accessible from a single interface.
These are the four most commonly used by prevention units.

360 Vision **Executive Dashboard**

An at-a-glance overview of the overall status of AML activities. It consolidates key risk indicators, active alerts and ongoing cases to prioritise urgent matters without losing sight of the strategic picture.

- Summary of total alerts and those pending action
- Clients categorised by risk level
- Direct export to PDF for executive reports
- Updates in line with the organisation's parameters

Operations Management **Alert Manager**

Centralises clients requiring investigation or reporting in accordance with the organisation's criteria. Prioritises, filters and assigns alerts so that the team can focus its efforts where it matters

- Alerts generated by configurable indicators
- Classification by type, urgency and status
- Full traceability from opening to resolution
- Direct integration with customer records

Research **Network analysis**

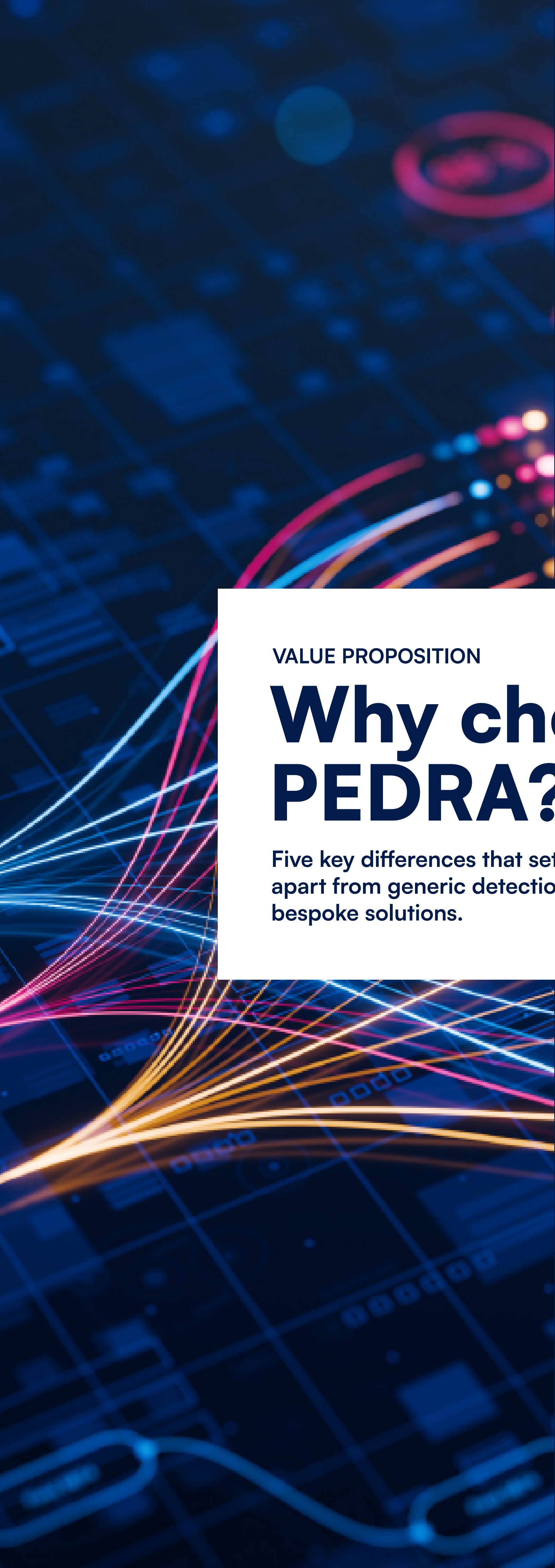
It identifies relationships between individuals, accounts and transactions that would go unnoticed in an individual analysis. Designed to detect complex risk structures.

- Graphical representation of links between entities
- Identification of corporate or family structures
- Cross-referencing internal and external data
- Documentary evidence supporting the relationship

Risk Model **Risk Matrix**

It enables the organisation to define and apply its own scoring model according to customer profile, product type, source of funds or geographical area. A risk-based approach aligned with SEPBLAC.

- Summary of total alerts and those pending action
- Customers classified by risk level
- Direct export to PDF for executive reports
- Update in accordance with the organisation's guidelines



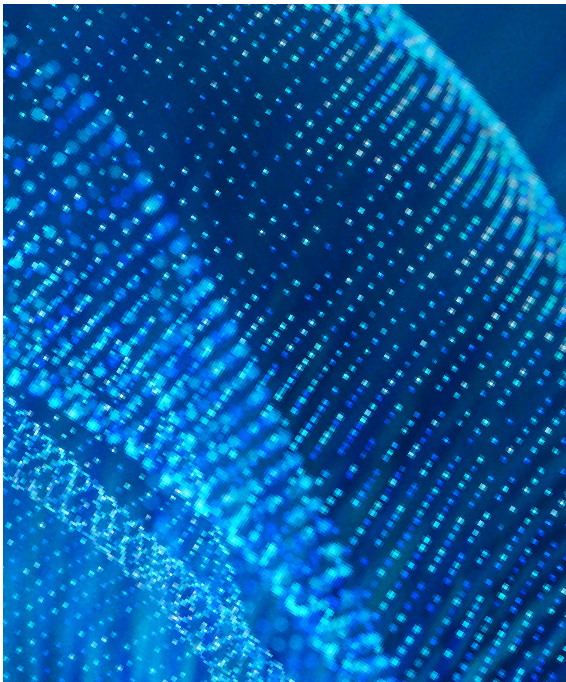
VALUE PROPOSITION

Why choose PEDRA?

Five key differences that set PEDRA® apart from generic detection tools and bespoke solutions.

Smart automation

It reduces manual work by up to 70% by automating data collection and initial screening. The team can focus its time on analysis, rather than data collection.



API-First Integration

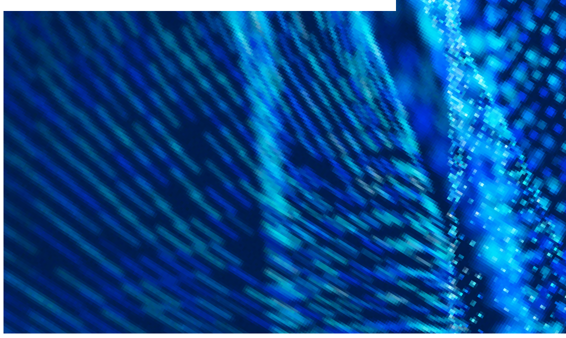
Connection to CRM, ERP or core banking systems via APIs. Integration takes a matter of weeks, not months-long projects, within the organisation's own environments.

Global Compliance

Compliant with regulations in the EU, the UK, the US and Latin America, with screening coverage in over 180 countries.

Auditability: Total

Every action, click and decision is recorded in an immutable log. Traceability is available from the source for regulatory inspections.



Specialist support

Direct access to AML experts, not just technical support. Implementation and ongoing development handled by a local team in Spain.

VALUE FOR BUSINESS AND TECHNOLOGY

What it brings to each area of the organisation

PEDRA® is assessed from two perspectives: its impact on the compliance department and the burden it places on the IT department.

For the business area

Integration
Management, documentation and monitoring of PBC/FT in a single solution.

Adaptability
Alignment with the specific criteria of each compliance department.

Scalability
Simple and gradual integration of regulatory and operational features.

Agility
Improved turnaround times thanks to the systematic processing of information.

Competitiveness
Value for money compared with the implementation and maintenance of alternatives available on the market.

Compatibility
Integration with external AML providers: partnership with FACTIVA DJ and WorldCheck support.

For the technology department

Microsoft Technology
Developed using the Microsoft stack, in line with the organisations' technical and security requirements.

Independence
Low impact on IT resources; the development does not interfere with the technology plan.

Automation
PEDRA®'s BAU is automated: there is virtually no need for IT support.

Local support
Implementation and ongoing development carried out by a local team in Spain.

Expert team
Professionals with in-depth knowledge of the tool and its technology.

In-house product
Izertis develops product enhancements without relying on third parties.

ARCHITECTURE AND SECURITY

Technology designed for the regulated environment

PEDRA® can be deployed across the organisation's environments — on-premises, in the cloud, in a hybrid environment or in a virtualised environment — and integrates with transactional systems in two ways: periodic batch uploads and real-time online services.

BATCH upload
at the frequency agreed with the organisation (daily, weekly, monthly). A central point collects the transaction data to feed into the POST analysis.

Online Services: APIs for customer onboarding verification and real-time transaction processing, integrated into the bank's workflows.

Technology stack

Component	Tech
Web - Front	ASP.NET on .NET Framework 4.7
Web - Back	C# on .NET Framework 4.7
Database	Microsoft SQL Server (recommended) • compatible with Oracle
APIs On Line	C# on ASP.NET Core 7

Safety mechanisms

01

Windows Authentication
Named users in the organisation's domain (Active Directory). PEDRA® delegates authentication to the domain server.

02

Communications encryption
SSL/TLS client-server encryption on Microsoft IIS and HTTPS protocol configuration.

03

Permission Service:
A custom class that validates the user, profile, navigation, permitted URLs and inactivity time.

04

Input validation
Checking files, URLs, cookies and GET/POST fields for potentially dangerous input.

ORGANISATIONS THAT PUT THEIR TRUST IN PEDRA

Working in banking, investment and insurance

PEDRA® is in use at leading organisations in the financial and insurance sectors, with the KYC-TM, DMO-F19, Screening, Online and FATCA-CRS modules, depending on the scope of each project.

Banking and investment

ebn banco · mapfre · santalucía · caser · bankinter · Sabadell · ZURICH · Aganea

Insurance

mapfre España · mapfre Portugal · ZURICH · santalucía · caser · Allianz · MEDVIDA PARTNERS · MUTUALIDAD ABOGACÍA · AVANZA PREVISIÓN · CNP Seguros

+10 years

in production at high-level organisations

Banking Investment

cobertura de los dos grandes sectores regulados

5 módulos

KYC-TM • DMO-F19 • Screening • Online • FATCA-CRS

IMPLEMENTATION MODEL

From signing to production in six months

A standard six-month plan for implementation and go-live with the agreed functionalities.
The scope may be extended depending on the organisation's requirements.

Kick-off — Start
A bespoke class that validates the user, profile, navigability, permitted URLs and idle time.

Design - 2 months
Environments, data models, source data, data quality, scenarios and customer scoring.

Development - 3,5 months
Loading interfaces, automation, scenarios, module customisation, validation and testing.

Implementation — 2 months
Deployment to the UAT environment, load and scenario testing, final adjustments prior to going live.

Commissioning
Production roll-out, final testing, training and documentation.

Monitoring
Post-implementation project for the maintenance and further development of PEDRA®.

Environment requirement
Windows Server 2019 servers (web and database), SQL Server 2019, IIS 10. User workstations with a standard browser (Edge, Chrome, Firefox). Licences and basic hardware are provided by the organisation.

Ready to modernise your AML?

A guided demonstration of reference data, led by a PEDRA® specialist, to view the full compliance cycle on the platform.

Book a Demo

izertis