**Objetivo SMART - Prueba de Concepto**

**Sistema de Detección de Fraudes Financieros GlobalBank**

**Definición del Objetivo SMART**

**Objetivo Principal de la PoC**

**"Desarrollar y demostrar un prototipo funcional de detección de fraudes financieros que procese 1,000 transacciones sintéticas en tiempo real, logre una precisión mínima del 80% en la clasificación de fraudes, y genere alertas automáticas para transacciones de alto riesgo, todo implementado en un entorno cloud utilizando el modelo Random Forest desplegado en Hugging Face."**

**Desglose SMART Detallado**

**S - ESPECÍFICO (Specific)**

**¿Qué exactamente vamos a construir y demostrar?**

1. **Prototipo funcional** que incluye:
   * ✅ **API de inferencia**: Endpoint REST para scoring de transacciones
   * ✅ **Pipeline de datos**: Ingesta, procesamiento y feature engineering
   * ✅ **Sistema de alertas**: Clasificación automática por niveles de riesgo
   * ✅ **Dashboard básico**: Visualización en tiempo real de resultados
   * ✅ **Integración ML**: Modelo Random Forest desplegado en Hugging Face
2. **Casos de uso específicos a demostrar**:
   * Procesamiento de transacciones legítimas (scoring bajo riesgo)
   * Detección de patrones fraudulentos (scoring alto riesgo)
   * Generación de alertas automáticas para scores >0.7
   * Análisis de feature importance en tiempo real
3. **Tecnologías específicas**:
   * **Frontend**: Python Streamlit
   * **Backend**: FastAPI para APIs
   * **ML**: Modelo fraud-model-rf en Hugging Face Hub
   * **Datos**: Dataset sintético basado en Kaggle Financial Transactions
   * **Cloud**: AWS Learner Lab (EC2, S3) y Hugging Face

**M - MEDIBLE (Measurable)**

**¿Cómo mediremos el éxito de la PoC?**

**Métricas Técnicas Cuantificables:**

|  |  |  |  |
| --- | --- | --- | --- |
| Métrica | Objetivo Mínimo | Objetivo Ideal | Método de Medición |
| Precisión del Modelo | ≥80% | ≥85% | Confusion matrix en dataset test |
| Recall (Sensibilidad) | ≥75% | ≥80% | Detección de fraudes verdaderos |
| Velocidad de Procesamiento | ≥100 trans/min | ≥200 trans/min | Throughput API medido |
| Latencia de Respuesta | ≤3 segundos | ≤1 segundo | Tiempo respuesta API |
| Transacciones Procesadas | 1,000 mínimo | 2,000+ ideal | Contador en dashboard |
| Uptime durante Demo | 100% | 100% | Monitoreo en vivo |

**Métricas Funcionales:**

* ✅ **Alertas generadas**: Mínimo 5 alertas de alto riesgo durante demo
* ✅ **Casos de prueba**: 3 escenarios (legítimo, sospechoso, fraudulento)
* ✅ **Features analizadas**: Visualización de top 10 características más importantes
* ✅ **False positives**: <10% de transacciones legítimas marcadas como fraude

**A - ALCANZABLE (Achievable)**

**¿Es realista este objetivo con nuestros recursos y tiempo?**

**Recursos Disponibles:**

1. **Equipo y Expertise**:
   * 4 integrantes con conocimientos en ML y Python
   * Experiencia previa en proyectos de ciencia de datos
   * Acceso a herramientas académicas (AWS Learner Lab, Hugging Face)
2. **Tecnología ya desarrollada**:
   * ✅ Modelo Random Forest entrenado y funcionando
   * ✅ Modelo desplegado en Hugging Face Hub
   * ✅ Dataset preparado y validado
   * ✅ Código base en GitHub
3. **Infraestructura disponible**:
   * AWS Learner Lab con $50 créditos
   * Hugging Face gratuito para hosting del modelo
   * Google Colab Pro si se requiere procesamiento adicional

**Análisis de Factibilidad:**

|  |  |  |  |
| --- | --- | --- | --- |
| Componente | Complejidad | Tiempo Estimado | Estado Actual |
| API de Inferencia | Baja | 8 horas | 🟢 Completado |
| Dashboard Web | Media | 12 horas | 🟡 En progreso |
| Pipeline de Datos | Media | 10 horas | 🟡 En progreso |
| Integración HF | Baja | 4 horas | 🟢 Completado |
| Testing & Debug | Media | 8 horas | 🟡 En progreso |
| Documentación Demo | Baja | 6 horas | 🟡 En progreso |
| Total | - | **48 horas** | **71% completado** |

**Distribución de trabajo**: 12 horas por integrante = factible en 2 semanas

**R - RELEVANTE (Relevant)**

**¿Por qué esta PoC es importante para GlobalBank y el curso?**

**Relevancia para el Negocio:**

1. **Impacto Financiero Demostrable**:
   * Simulación de $50k en transacciones durante demo
   * Identificación de $5k+ en fraudes potenciales
   * ROI visible: costo de falsos positivos vs. fraudes prevenidos
2. **Casos de Uso Reales**:
   * **Transacciones ATM**: Retiros sospechosos por ubicación/horario
   * **Compras online**: Patrones de gasto anómalos
   * **Transferencias**: Montos inusuales o destinos sospechosos
3. **Validación Técnica**:
   * Prueba de concepto de arquitectura cloud
   * Validación de modelo en condiciones semi-reales
   * Demo de integración entre componentes

**Relevancia Académica:**

1. **Cumplimiento de Objetivos del Curso**:
   * ✅ Aplicación práctica de ML en caso real
   * ✅ Integración de múltiples tecnologías IA
   * ✅ Desarrollo de solución end-to-end
   * ✅ Evaluación de performance en producción
2. **Competencias Demostradas**:
   * Diseño de arquitecturas ML escalables
   * Deployment y operación de modelos
   * Análisis de métricas de negocio
   * Presentación de resultados técnicos

**T - TEMPORAL (Time-bound)**

**¿Cuándo se completará cada fase y la demo final?**

**Timeline Detallado:**

CRONOGRAMA PoC - 14 días calendario

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

SEMANA 1 (26-31 Mayo)

├── Día 26-28: API de Inferencia + Integración HuggingFace

├── Día 28-29: Pipeline de datos y feature engineering

├── Día 30: Dashboard básico (frontend)

└── Día 31: Integración componentes + testing inicial

SEMANA 2 (2-6 Junio)

├── Día 2-3: Sistema de alertas + optimización performance

├── Día 3-4: Dashboard avanzado + UX/UI

├── Día 4-5: Testing completo + preparación demo

└── Día 6: Ensayo demo + ajustes finales

DEMO FINAL: 6 Junio 2025 - 15 minutos

**Hitos Críticos:**

|  |  |  |  |
| --- | --- | --- | --- |
| Fecha | Hito | Entregable | Responsable |
| 28 Mayo | ✅ API Funcional | Endpoint REST operativo | Juan S. Giraldo |
| 30 Mayo | ✅ Dashboard MVP | Interfaz básica funcionando | Juan S. Navas |
| 31 Mayo | ✅ Integración Completa | Sistema end-to-end | Daniel Ruiz |
| 5 Junio | ✅ Testing & Validación | Métricas objetivo alcanzadas | Carlos Trujillo |
| 6 Junio | 🎯 **DEMO FINAL** | Presentación 15 minutos | **Todo el equipo** |

**Contingencias Temporales:**

* **Buffer de 2 días**: Para resolución de bugs críticos
* **Plan B**: Demo en Google Colab si falla infraestructura AWS
* **Scope reduction**: Funcionalidades "nice-to-have" eliminables si es necesario

**🎬 Estructura de la Demo (15 minutos)**

**Guión Detallado:**

**Minuto 1-2: Introducción y Contexto**

* 📊 Problema de GlobalBank (estadísticas de fraude)
* 🎯 Objetivo de la PoC y métricas de éxito
* 🏗️ Arquitectura general (diagrama de alto nivel)

**Minuto 3-4: Demostración en Vivo**

* 🔴 **LIVE DEMO**: Procesamiento de transacciones en tiempo real
* 📱 Dashboard mostrando: scores, alertas, métricas
* 🚨 Generación de alertas para transacciones fraudulentas
* 📈 Visualización de feature importance

**Minuto 5-10: Análisis de Resultados**

* 📊 Métricas alcanzadas vs. objetivos SMART
* 💡 Insights del modelo (patrones detectados)
* ⚡ Performance técnico (latencia, throughput)
* 💰 Impacto de negocio simulado

**Minuto 10-15: Conclusiones y Próximos Pasos**

* ✅ Cumplimiento de objetivos SMART
* 🚀 Roadmap para producción
* ❓ Q&A rápido

**Escenarios de Demo Preparados:**

1. **Escenario Legítimo**:
   * Cliente habitual comprando en su ciudad
   * Score: 0.1-0.3 (bajo riesgo)
   * Sin alertas generadas
2. **Escenario Sospechoso**:
   * Transacción de monto alto fuera del horario habitual
   * Score: 0.5-0.7 (riesgo medio)
   * Alerta de revisión manual
3. **Escenario Fraudulento**:
   * Múltiples transacciones en ubicaciones imposibles
   * Score: 0.8-0.95 (alto riesgo)
   * Alerta crítica + bloqueo automático

**📊 Criterios de Éxito Detallados**

**Éxito Mínimo (Aprobación):**

* ✅ Demo ejecutada sin errores críticos
* ✅ Precisión del modelo ≥80%
* ✅ Procesamiento de 1,000+ transacciones
* ✅ Sistema de alertas funcionando
* ✅ Presentación dentro de 7 minutos

**🔧 Implementación Técnica de la PoC**

**Stack Tecnológico Confirmado:**

# Arquitectura de la PoC

Frontend: HTML/CSS/JavaScript (Bootstrap)

├── Dashboard: Plotly.js para visualizaciones

├── API Client: Fetch API para comunicación

└── Responsive: Mobile-first design

Backend: Python Flask

├── API Routes: /predict, /batch-process, /metrics

├── Integration: Hugging Face Hub API

├── Data Processing: Pandas, NumPy

└── Monitoring: Custom metrics collector

ML Pipeline:

├── Model: fraud-model-rf (Hugging Face)

├── Features: 47 características engineered

├── Preprocessing: StandardScaler, encoding

└── Postprocessing: Risk scoring y alertas

Infrastructure:

├── Hosting: AWS EC2 t2.micro (Learner Lab)

├── Storage: S3 para datasets y logs

├── Database: SQLite para demo (PostgreSQL en prod)

└── Monitoring: CloudWatch básico

**Dataset de Demo:**

* **Fuente**: Sintético basado en Kaggle Financial Transactions
* **Tamaño**: 2,000 transacciones (80% legítimas, 20% fraudes)
* **Features**: 47 características incluyendo geolocalización temporal
* **Formato**: JSON streaming para simular tiempo real

**📝 Documentación Entregable**

**Artefactos a Generar:**

1. **📄 README.md Técnico**:
   * Instrucciones de setup y ejecución
   * Arquitectura detallada de la PoC
   * APIs y endpoints documentados
2. **🎥 Video Demo (3-5 minutos)**:
   * Grabación de pantalla completa
   * Narración explicando cada paso
   * Métricas y resultados en tiempo real
3. **📊 Reporte de Resultados**:
   * Métricas alcanzadas vs. objetivos SMART
   * Análisis de performance técnico
   * Lessons learned y mejoras identificadas
4. **🔧 Código Fuente**:
   * Repositorio GitHub actualizado
   * Código comentado y documentado
   * Requirements.txt y instrucciones deployment

**🎯 Resumen Ejecutivo del Objetivo SMART**

|  |  |
| --- | --- |
| Criterio SMART | Definición Específica |
| S - Específico | Prototipo funcional de detección de fraudes con API, dashboard, alertas e integración Hugging Face |
| M - Medible | Precisión ≥80%, procesamiento 1,000+ transacciones, latencia ≤3s, uptime 100% durante demo |
| A - Alcanzable | 48 horas de desarrollo, recursos disponibles, tecnología validada, equipo capacitado |
| R - Relevante | Soluciona problema real de GlobalBank, cumple objetivos académicos, demuestra competencias ML |
| T - Temporal | 14 días de desarrollo, demo 15 minutos el 6 de junio 2025, hitos semanales definidos |

*Objetivo SMART definido por: Juan Sebastián Giraldo, Juan Sebastián Navas, Daniel Alejandro Ruiz, Carlos Alberto Trujillo*  
*Fecha: 2 de Junio 2025 | Versión: 1.0 | Aprobación: Pendiente*  
*Próxima revisión: 7 de Junio 2025 (Checkpoint Semana 2)*