

Cumplimiento y seguridad en el desarrollo de aplicaciones financieras: una visión práctica

Lidia Bergua Sarroca
Legal & Compliance Manager en IriusRisk

Encuentro Walqa empresa-universidad

19 de septiembre de 2025



Seguridad y cumplimiento en banca y pagos digitales



Entidades financieras = sectores más regulados

- **UE/ES:** PSD2 · DORA · NIS2 · MiFID II · RGPD
- **EEUU:** GLBA · SOX
- **Estándares:** PCI DSS · ISO 27001



Aplicaciones de banca

- **Datos:** Grandes volúmenes y muy sensibles
- **Internas y externas** (clientes)



El reto

- De la norma/estándar → a realidad operativa: políticas, controles y configuraciones
- Seguridad & Cumplimiento necesitamos un lenguaje común con desarrolladores y resto de áreas.

Seguridad desde el diseño

Problema: Seguridad y Cumplimiento Llegan en etapas tardías → bloqueos, costes



Solución:

Security by
Design

IriusRisk - **Threat Modeling** (Modelado de amenazas)

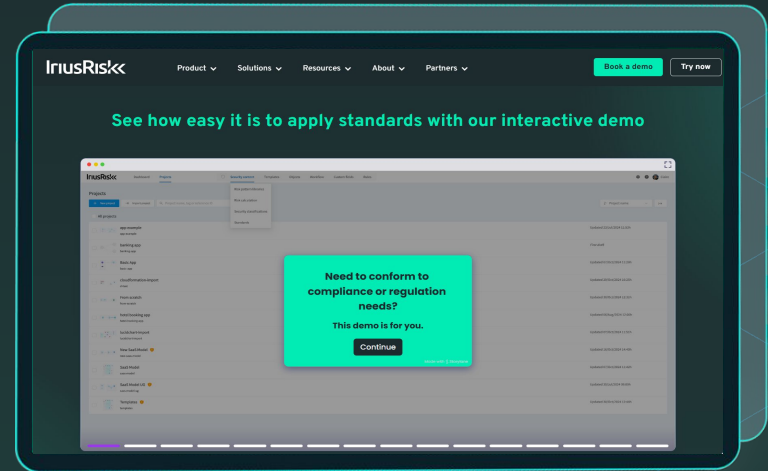
Modelo visual de la arquitectura de la app
Identificación de riesgos y amenazas
Controles y contramedidas desde el diseño

Sinergias internas



Mini demo

IriusRisk Security content libraries demo



Impacto global y beneficios

Bancos → aplicaciones
seguras y confiables

Reguladores → cumplimiento
trazable y transparente

Ecosistema financiero y
clientes → confianza y
estabilidad

Organizaciones → menos
fricciones internas



¡Muchas gracias!



<https://www.linkedin.com/in/lidiaberguasarroca/>

lbergua@iriusrisk.com