

PAQUETE SECTORIAL · BANCA

Proveedores, oficinas y agentes de IA, bajo control demostrable

Control, aprobación y evidencia verificable para las acciones críticas sobre los sistemas del banco: proveedores TIC, operación interna, red de oficinas y agentes de IA — al nivel probatorio que exige DORA.

Un banco moderno lo operan muchas manos que no son del banco: **proveedores TIC interviniendo sobre el core, integradores, mantenimientos, automatización creciente y ya agentes de IA** — mientras DORA exige gobernar y demostrar la resiliencia de todo ello, terceros incluidos. Una credencial válida ya no basta como control. *¿Quién autoriza cada intervención sobre sus sistemas, bajo qué política, y cómo se demuestra ante el supervisor?*

QUÉ APORTA VELANTIA A ESTE SEGMENTO

GATE — decide cada acción crítica sobre core, pagos y sistemas centrales: **permitir, condicionar, derivar a aprobación o bloquear** intervenciones de empleados, proveedores y automatismos, según política y contexto.

SENTINEL — observa la actividad en servicios centrales y red de oficinas, **detecta anomalías** y atribuye cada actuación a su autor: empleado, proveedor TIC, sistema o agente.

EVIDENCE — conserva la **historia probatoria** de cada intervención y cada incidente: lista para auditoría interna, el supervisor y el reporte de incidentes que DORA exige.

AUTONOMY — gobierna la automatización y los agentes de IA del banco — atención, operaciones, riesgo — con **límites explícitos, aprobación humana y revocación**.

QUÉ PUEDE HACER CON ELLO

- ▶ **Gobernar al proveedor TIC — el corazón de DORA:** cada intervención de terceros sobre sus sistemas ocurre bajo permisos definidos, con registro íntegro de lo que hicieron.
- ▶ **Exigir aprobación humana** antes de acciones sensibles sobre core, pagos o parámetros de riesgo — sin frenar la operación diaria.
- ▶ **Extender el control a la red de oficinas** y canales con las mismas políticas que los servicios centrales.
- ▶ **Responder al supervisor con evidencia, no con relatos:** qué pasó, quién lo hizo, qué política se aplicó y quién lo aprobó — ya generado cuando llega el requerimiento.

El banco sigue operando — cada intervención con permiso, contexto y una historia demostrable.

DESPLIEGUE

Para servicios centrales, el appliance **CORE 900**; para la red de oficinas, **EDGE 200**; para claves y firmas, **KEY VAULT 500** con HSM y secure element de socios especializados (todos en pre-reserva), gobernados desde **VELANTIA ONE**. También software, máquina virtual o nube privada. Se integra con su identidad, SIEM y operativa **sin reemplazar el stack existente**.

POR QUÉ AHORA

DORA ya está en vigor y el supervisor ha empezado a pedir cuentas: **resiliencia demostrable, terceros gobernados e incidentes reportados con evidencia** — justo cuando los agentes de IA entran en la operación bancaria. Quien convierta hoy el cumplimiento en control real llegará al próximo requerimiento con la respuesta ya generada.

Próximo paso: una reunión inicial y una demostración.

Flujo completo sobre un caso acotado: intervención → política → aprobación o bloqueo → evidencia. Disponible propuesta de piloto acotada, con métricas y sin compromiso de despliegue.