VELANTIA

TRUST INFRASTRUCTURE
FOR CRITICAL ACTIONS

PAQUETE SECTORIAL · INFRAESTRUCTURAS CRÍTICAS

Decisiones con impacto físico, controladas y demostrables

Control con contexto operativo, continuidad y evidencia verificable para energía, agua, transporte, telecomunicaciones, sanidad, puertos y aeropuertos.

En un operador esencial, un fallo no es una fuga de datos: **es un suministro que se corta o un servicio que se detiene**. Operadores, proveedores, sistemas y automatizaciones actúan sobre activos que no pueden fallar. *¿Quién autoriza cada acción sobre el activo esencial, con qué contexto, y qué evidencia queda para el regulador y para la investigación?*

QUÉ APORTA VELANTIA A ESTE SEGMENTO

GATE — autoriza con **contexto operativo** antes de actuar sobre el activo esencial: estado, riesgo, franja, responsable — y bloquea lo que pondría el servicio en peligro.

SENTINEL — observa la actividad sobre la infraestructura, **detecta anomalías** y atribuye cada actuación a su origen: persona, proveedor, sistema o agente.

EVIDENCE — conserva el **rastro verificable** que el regulador y la investigación de incidentes exigirán: decisión, aprobación, ejecución y resultado.

AUTONOMY — gobierna la automatización que llega a los activos físicos, con **límites explícitos, aprobación humana y revocación**.

QUÉ PUEDE HACER CON ELLO

- **Autorización con contexto antes de ejecutar** sobre activos esenciales — no solo una credencial válida.
- **Continuidad local ante pérdida de conexión:** las funciones esenciales siguen operando bajo políticas definidas.
- **Acotar el daño de credenciales o agentes comprometidos:** solo lo que el permiso autoriza, con registro de todo.
- **Responder ante el regulador con evidencia,** no con reconstrucciones: cada incidente con su historia coherente.

Ninguna orden — por muy autenticada que esté — debería poder forzar un estado peligroso del servicio.

DESPLIEGUE

Según el entorno: **SOVEREIGN 700** para operación soberana y **INDUSTRIAL 500R** para planta y OT (ambos en pre-reserva), gobernados desde **VELANTIA ONE**. También software, máquina virtual o nube privada del operador. Se integra con los sistemas existentes **sin reemplazarlos**.

POR QUÉ AHORA

Las **obligaciones de ciberseguridad para operadores esenciales se endurecen** año a año, las amenazas contra infraestructura crecen y la automatización llega a activos con impacto físico. La capacidad de demostrar el control aplicado deja de ser deseable: **es exigible**.

Próximo paso: una reunión inicial y una demostración.

Flujo completo en entorno controlado o simulado, sin actuar sobre infraestructura real. Disponible propuesta de piloto de soberanía e infraestructura crítica, acotada y con métricas.

Agustín López Mayor — Inventor · Co-fundador · **Stephan Hoof** — Co-fundador · Expansión internacional
contact@velantia.io · velantia.io · Villajoyosa (Alicante, España) · Weikersheim (Alemania) · Ruse (Bulgaria)

Nueve solicitudes de patente presentadas ante la OEPM · en tramitación · Documento de presentación estratégica