Jornada Informativa

OAP Valencia

10 de Junio de 2026

Optimiza las del Producto Industrial Personalizable:
Configurador Web com 3D e IA

semantic systems

Ponentes

Optimiza las del Producto Industrial Personalizable: Configurador Web con 3D e IA

Día: Miércoles 10
Mes: Junio
Año: 2026

Juan Antonio Gomez |
Consultor preventa repcon configurator

Semantic Systems
comercial@semantic-systems.com

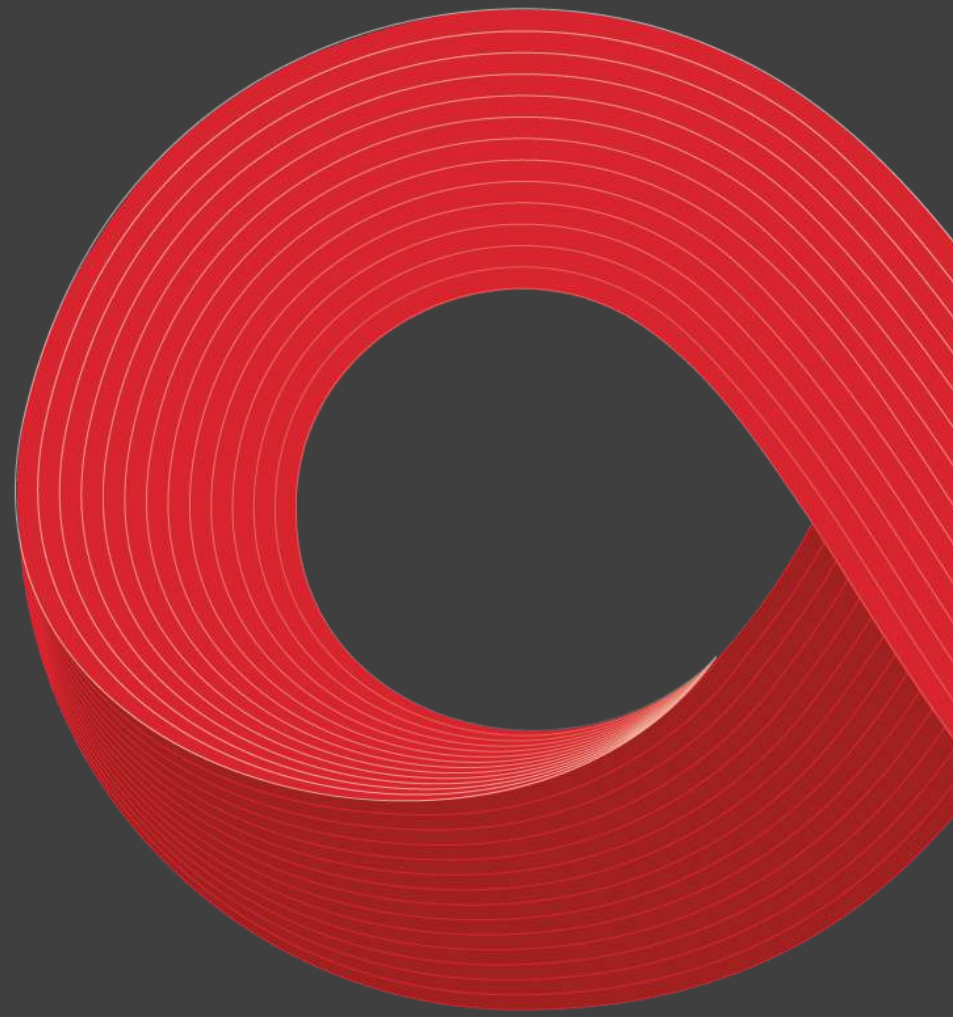
David Montia |
Responsable Desarrollo de Negocio | Marketing

Semantic Systems
dmp@semantic-systems.com

semantic systems

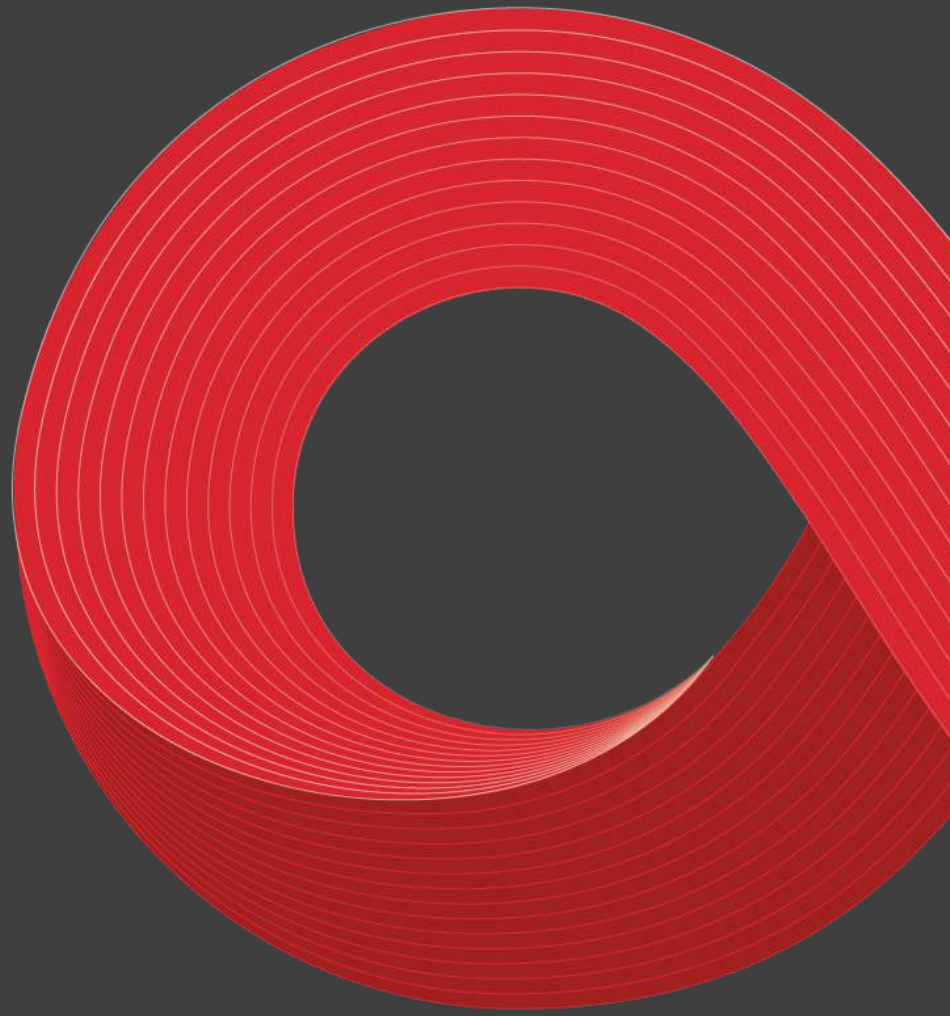
semantic
systems

ÍNDICE



semantic
systems

Semantic Systems



CREAMOS TECNOLOGÍA

Soluciones que Digitalizan Empresas

semantic systems

Semantic Systems

Transformación Digital de la Cadena de Valor

Industria 4.0 | repcon

Digitalizamos los procesos de fabricación y configuración, optimizando las operaciones para mejorar la competitividad de las industrias

Digitalización de Procesos | repcon

Ayudamos a gestionar el conocimiento de la organización y su integración con las plataformas de gestión de los procesos de negocio

Gestión Empresarial | ERP

Mejoramos los procesos de negocio en las empresas asesorando, implementando y optimizando software de gestión empresarial (ERP, CRM, BI, MES ,..)

Outsourcing | Servicios Gestionados

Implementamos y gestionamos las infraestructuras informáticas de nuestros clientes, garantizando la continuidad del negocio

Repcon IA

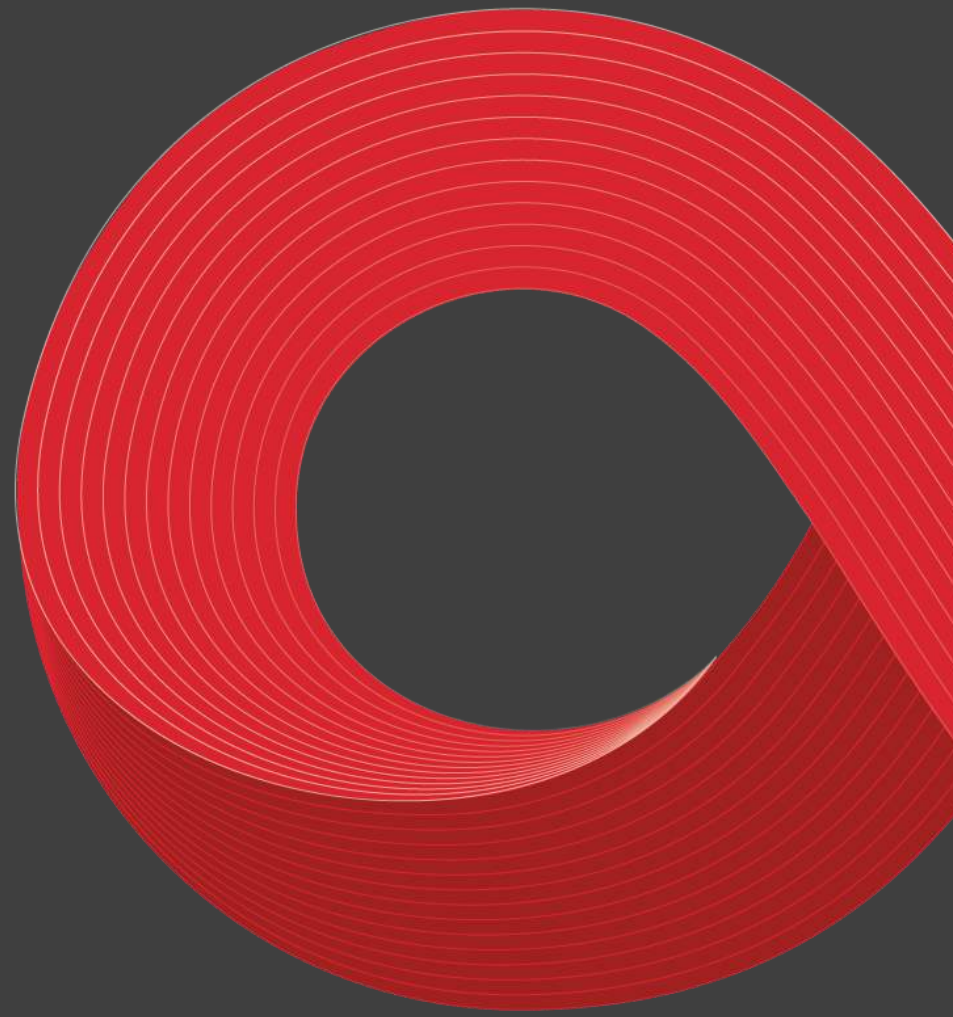
Facilitamos la agilidad y la estrategia de las empresas, anticipando problemas y ajustando procesos a las necesidades del negocio con herramientas de IA generativa y analítica avanzada.

semantic systems

semantic systems

Productos personalizables

El reto de la venta del Producto Industrial



Venta del Producto Industrial

Cómo afrontar la complejidad del mercado

Venta B2B = Entorno complejo

- Procesos de Venta **más largos y complicados**
- Equipos de **ventas desbordados**
- ¿Qué **competencias necesitan** los equipos?
- ¿Qué **herramientas** o **IA** son necesarias?

Necesidad de Producto Personalizable

- Venta de **más valor**
- **Diferenciarse** frente a la competencia,
- Acceso **más mercados** con menos esfuerzo

semantic systems

¿Te reconoces en estas situaciones?

Venta del Producto Personalizable

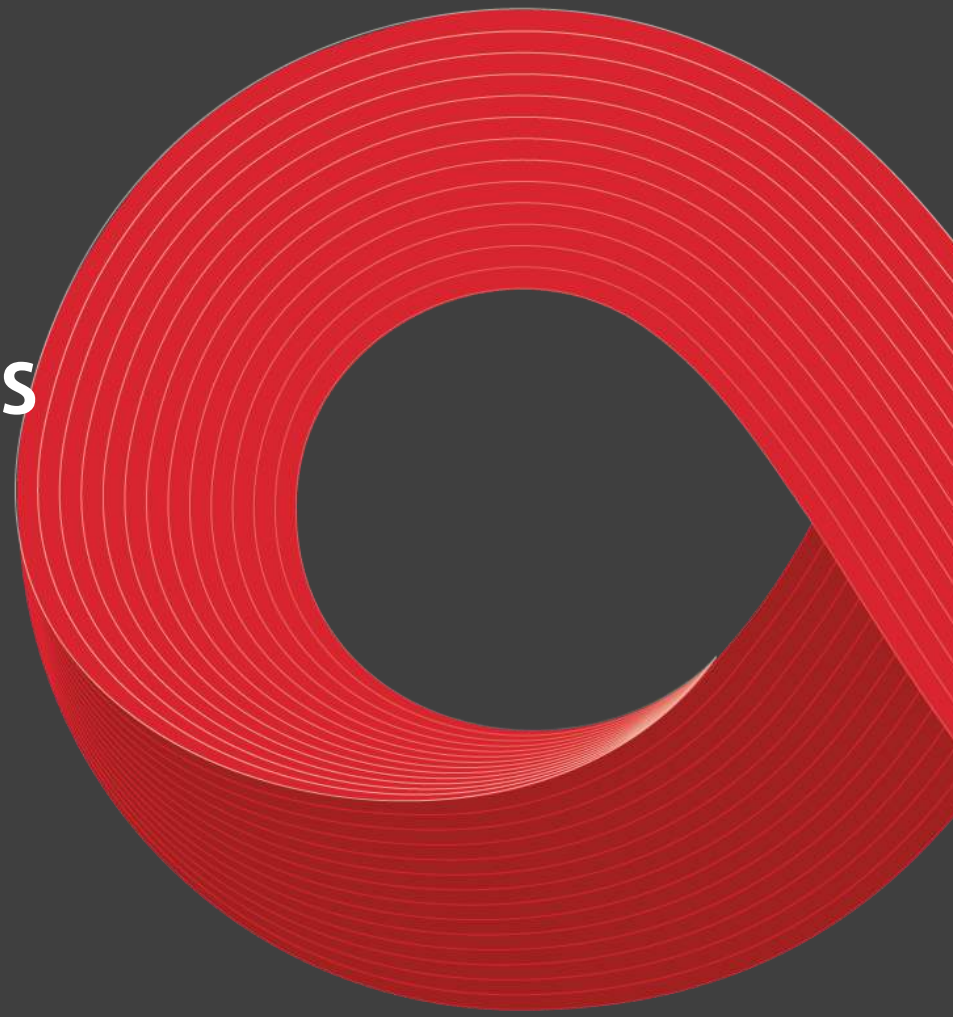
- Demasiado **tiempo comercial** elaborando ofertas
- **Conocimiento disperso** y no actualizado
- Diferentes **herramientas** (excels…) , **sistemas** y **procesos**
- On boarding complejo de **comerciales/distribuidores**
- Adaptación a **zonas, horarios, monedas, dispersión**…
- **Errores no detectados** o detectados tarde
- **Oficina técnica** es un cuello de botella

semantic systems

semantic systems

Configurador de Ofertas y Productos

Crear producto y ofertas personalizadas



¿Cómo funciona?

repcon pricing & quoting | configurator

Conocimiento sobre el producto

Aplicación de **Reglas** de negocio

Cualquier usuario: Incluso sin conocimientos

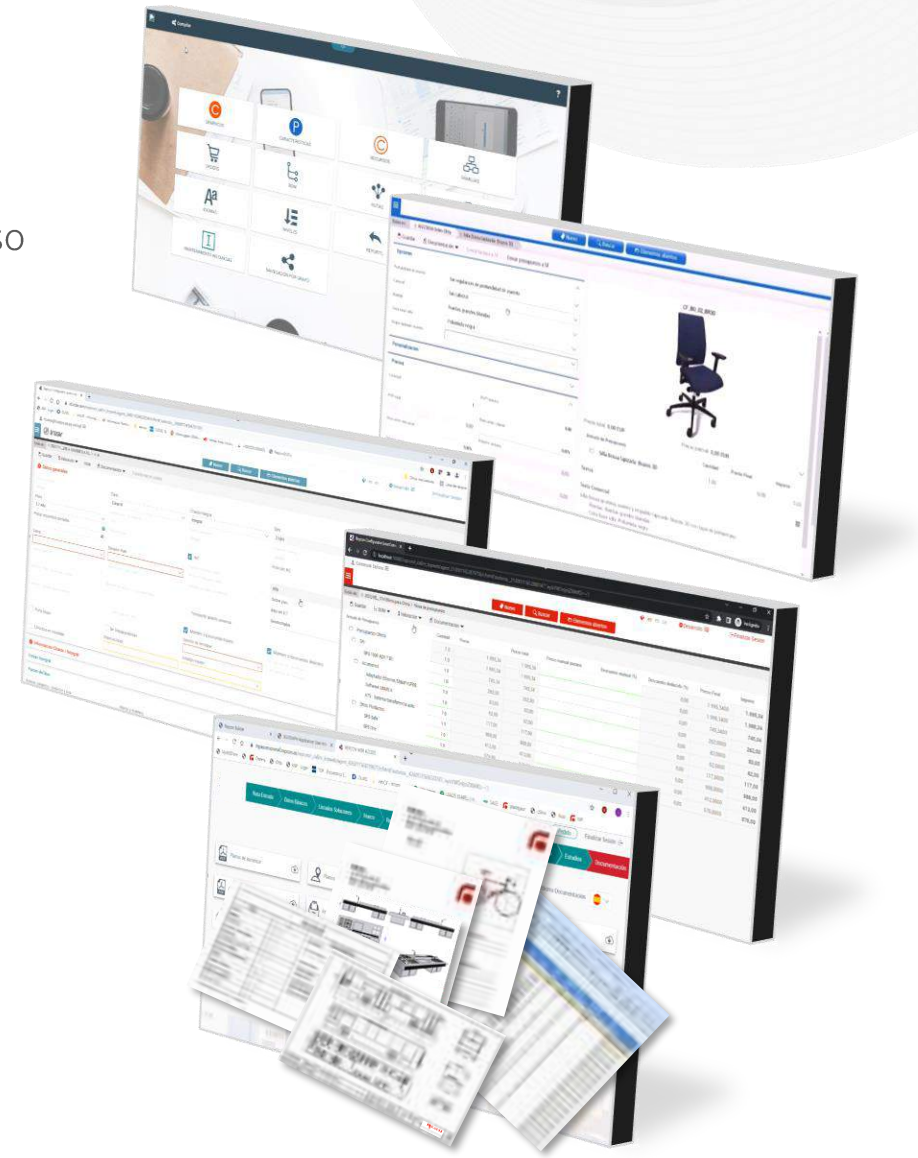
Formularios adaptados en tiempo real que fijan, amplían o limitan opciones

Detalle del **producto personalizado**

Cotización exacta y sin errores

Propuesta: oferta, listas, planos, fichas técnicas…

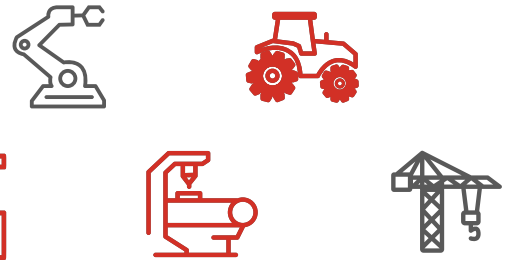
Pedido: BoM, RoU, listas, planos, fichas técnicas…



Sectores

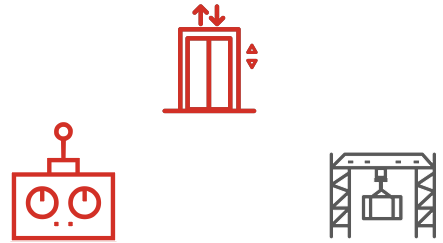
Productos Personalizables

Maquinaria Industrial

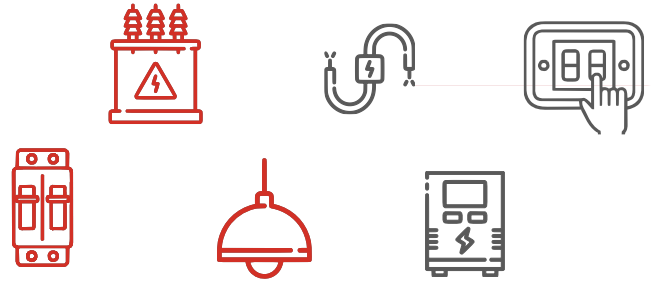


Automoción

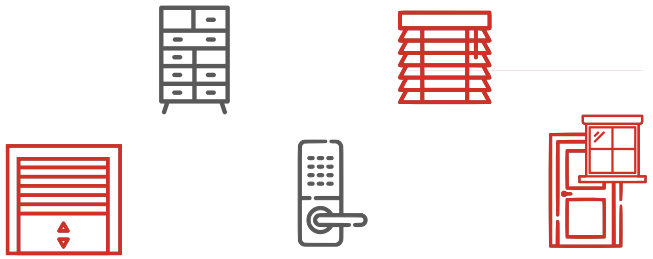
Medios de elevación



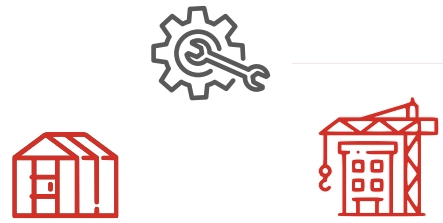
Componentes Eléctricos



Muebles | Cerramientos



Ingenieria | Construcción



Beneficios por Área

repcon pricing & Quoting | Configurator

Comercial | Marketing

Capta la **atención** del **mercado**
Permite nuevos **Canales Venta**
Acorta periodos **on-boarding**
Fija opciones **producto/tarifas**
Menos **tiempo/oferta** = +ofertas
Venta de más valor **sin depender de OT**

Oficina Técnica/Ofertas

Automatiza estructuras/códigos
Elimina **cuello de botella** O.T.
Mejora productividad = **+Valor**
Mejora **plazos** de entrega
Simplifica **mantenimiento** de producto
Reduce **Time-to-Market**

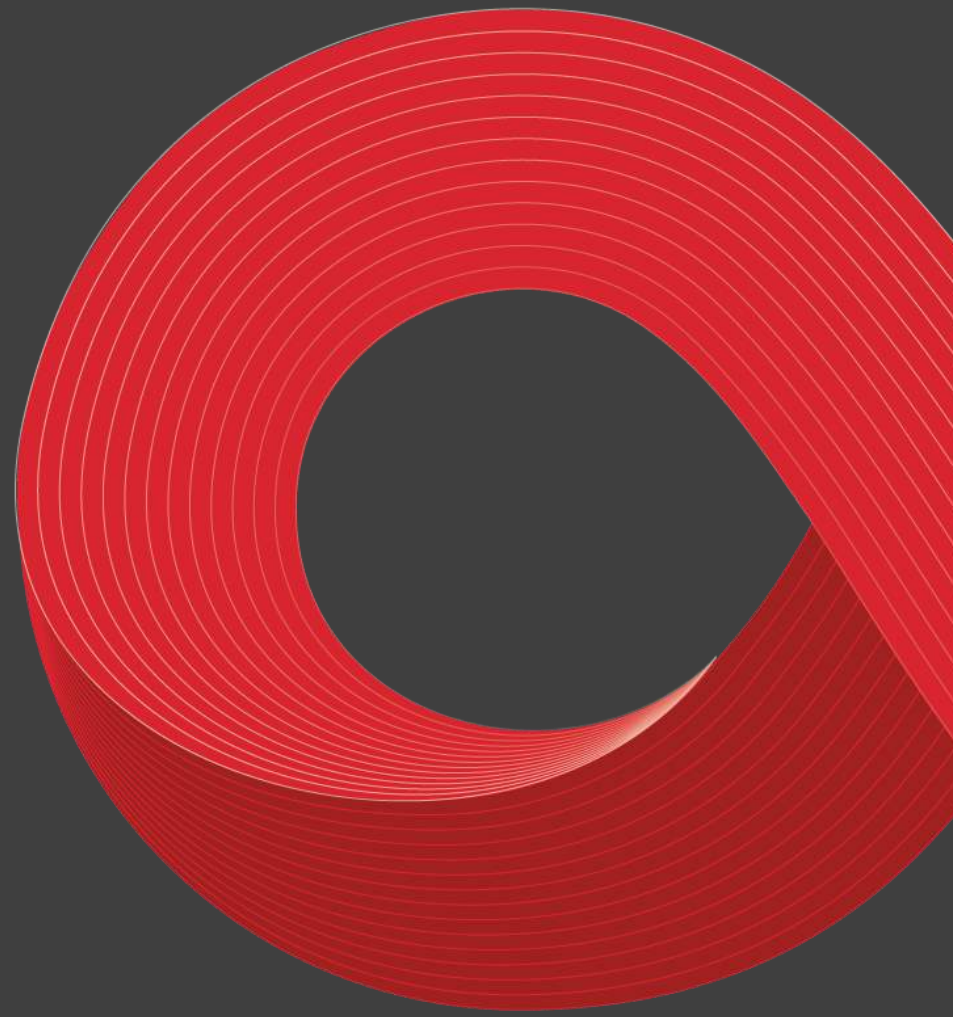
Producción

Automatiza cálculo operaciones y tiempos
Elabora doc. Técnica: normativas o necesidades producción
Menos reprocesos por errores
Reduce costes preparación
Optimiza logística y provisión

semantic systems

Configurador web y 3D

Crear producto y ofertas personalizadas

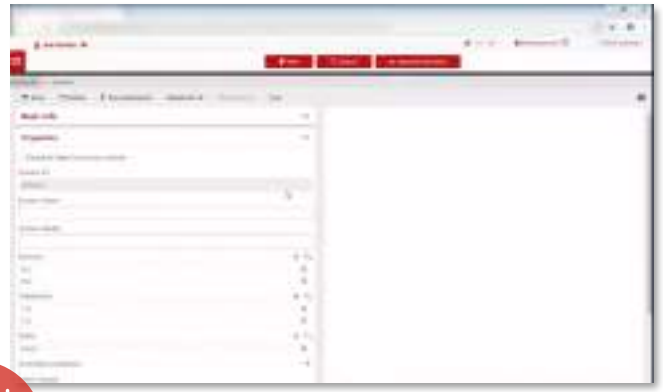


Tipos de Configuración de Producto

Adaptación de la aplicación al producto

Formulario

Basada en características predefinidas y ajustables. Cada característica tiene un conjunto de opciones modificables



Sobre plano 2D

Interactuación con una representación bidimensional del producto. Visualizar cómo se verá el producto final desde una perspectiva plana

Sobre sólido 3D

Interactuación con un modelo tridimensional del producto. Es posible rotar y ver el producto desde diferentes ángulos, y ajustar características y reubicar componentes

Mixto

Combina elementos de las configuraciones por formulario, sobre planos 2D y sobre sólidos 3D. Aprovecha las ventajas de cada una de las modalidades.

semantic systems

Qué es el configurador 3D

Características y beneficios

Modelos geométricos 3D

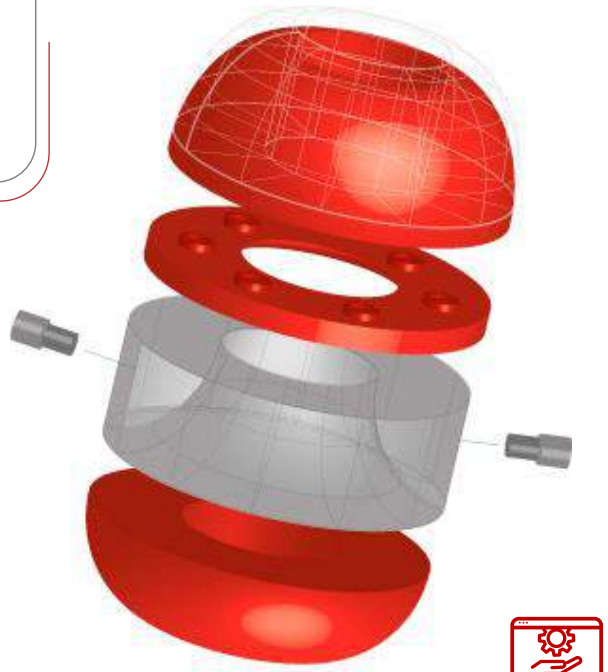
Representación poligonal de la forma y componentes del producto

Materiales y texturas

Definen cómo la luz interactúa con la superficie

Escena 3D con entorno

Define el escenario virtual, iluminación y cámaras



Interactividad realista

Proporcionar una experiencia al usuario interactiva y realista

Accesibilidad Total

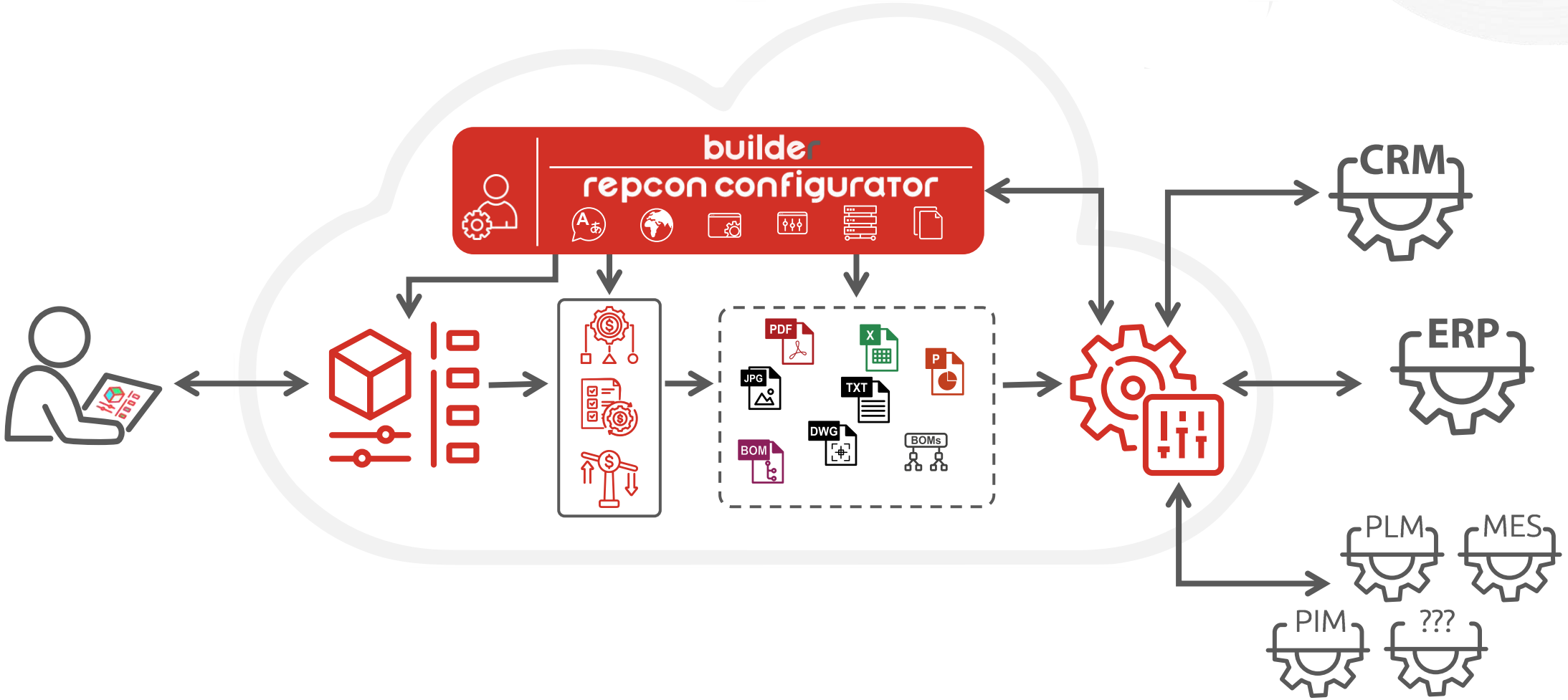
Solo requiere un navegador web sin necesidad de plugins adicionales

Funciones Avanzadas

Movimiento fluido, cambios de vista, asistentes lógicos

Arquitectura | Integración con el Ecosistema IT

repcon pricing & quoting | configurator



Repcon Builder | Modelado de Producto

repcon Configurator

Low-code Real

Asistentes o wizards: experiencia guiada, sin necesidad de programar

Accesible

Cloud: trabajo remoto y colaborativo desde cualquier dispositivo

Escalable

Diseñado para manejar modelos complejos y con gran volumen de datos

Tiempo Real

Permite realizar las pruebas del modelo sin afectar la operación

Trabajo en equipo

Colaboración entre departamentos (comercial, técnico, producción…)

Registro Histórico

Registra los cambios realizados sobre el modelo, lo que mejora la calidad y el control

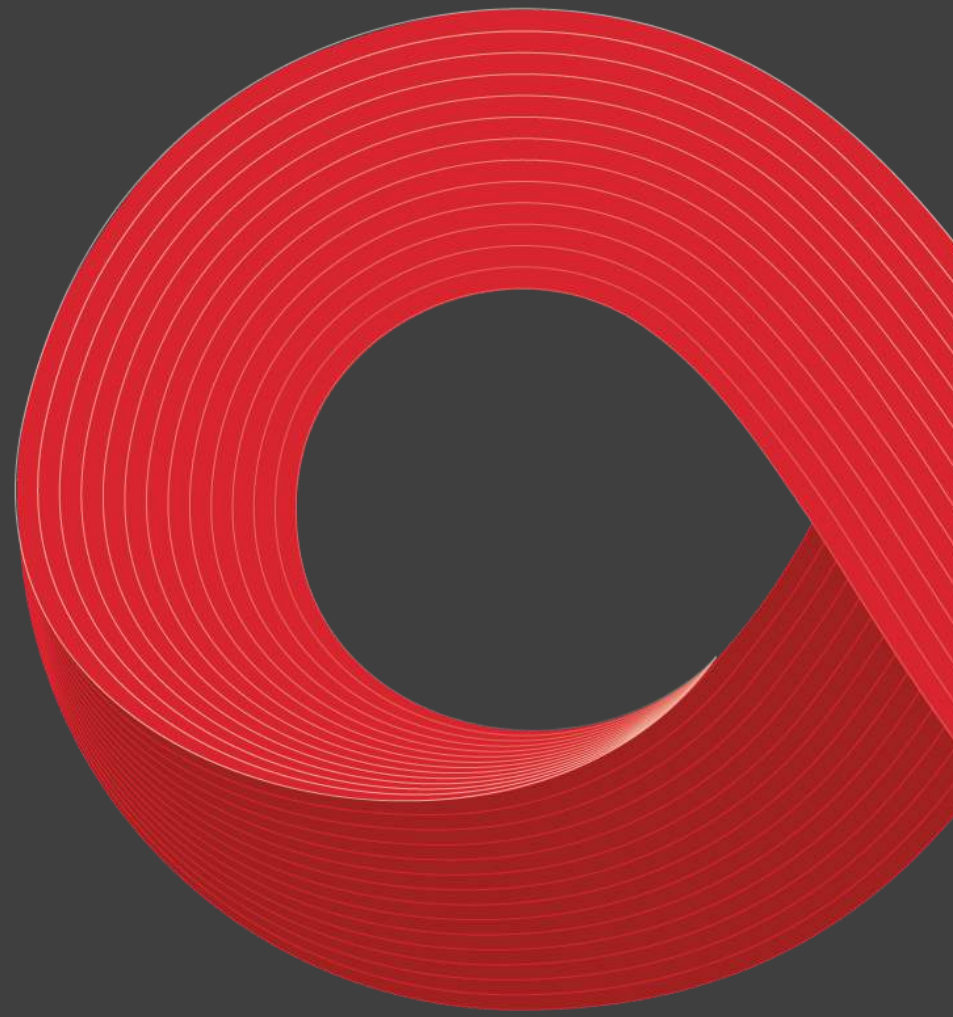
Versionado

Trabajo con diferentes versiones del modelo y gestión de la evolución de los productos

semantic systems

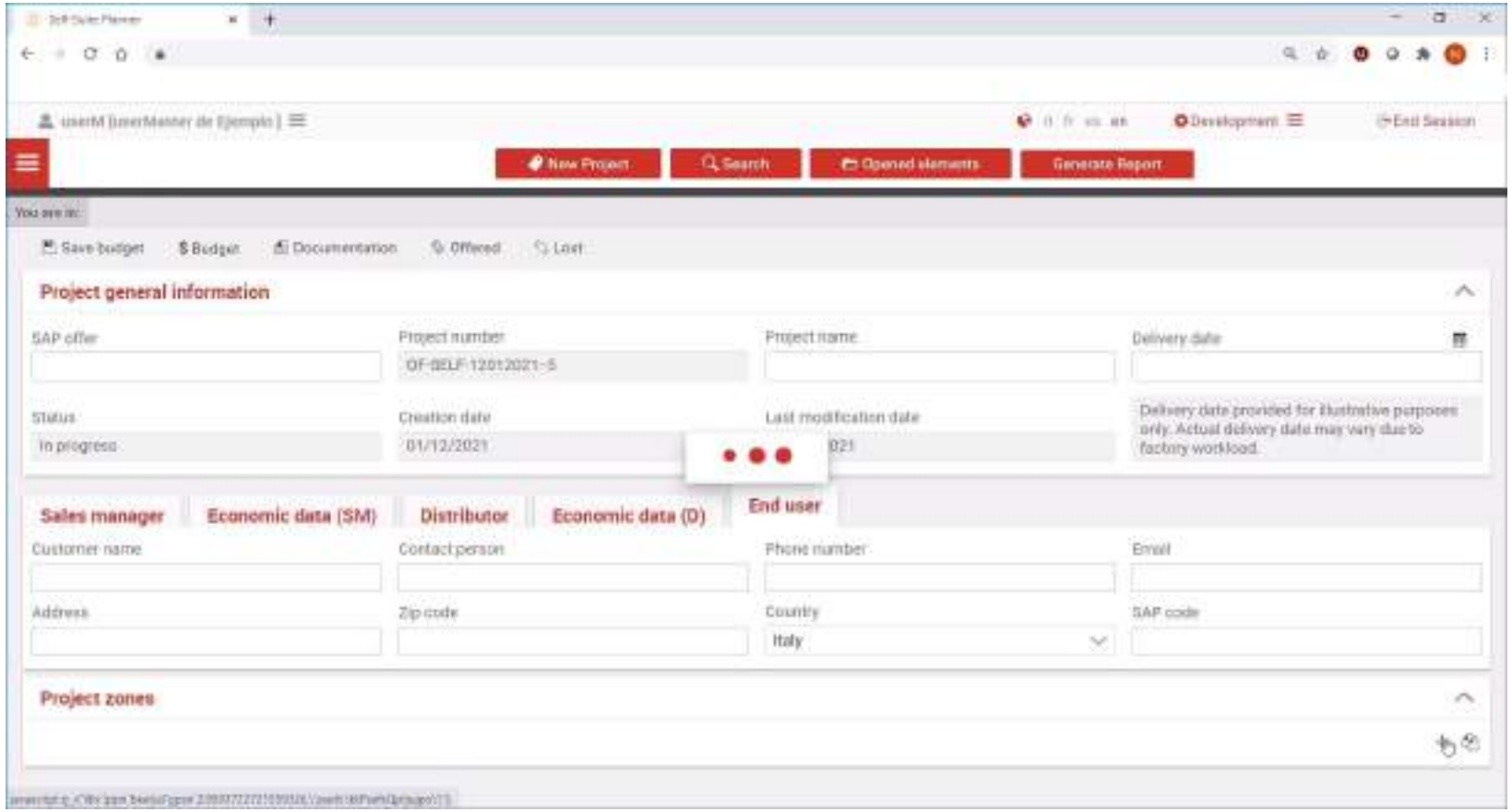
IA, impacto en la Configuración

El valor que aporta la Inteligencia Artificial



Video - Demostración

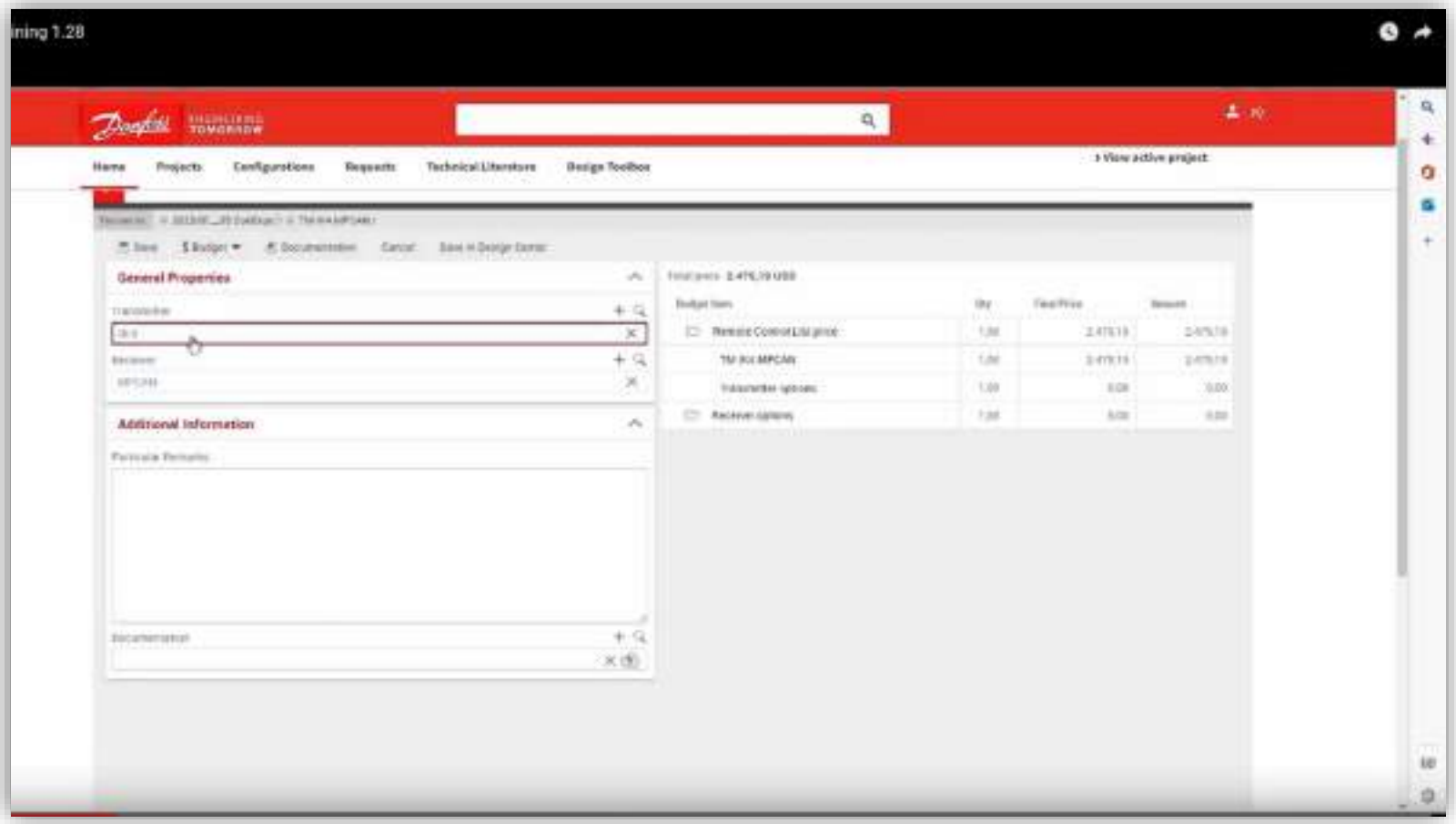
repcon pricing & quoting



semantic systems

Video - Demostración

repcon pricing & quoting

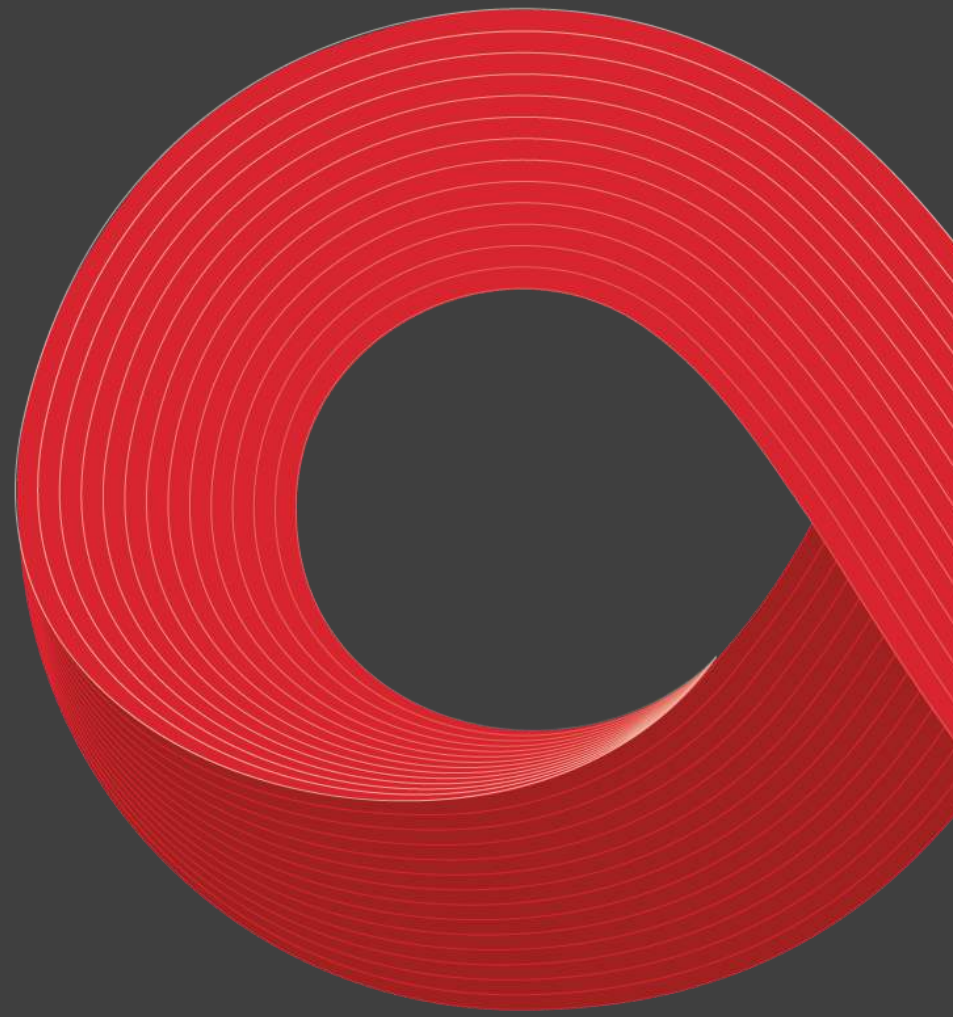


semantic systems

semantic systems

IA, impacto en la Configuración

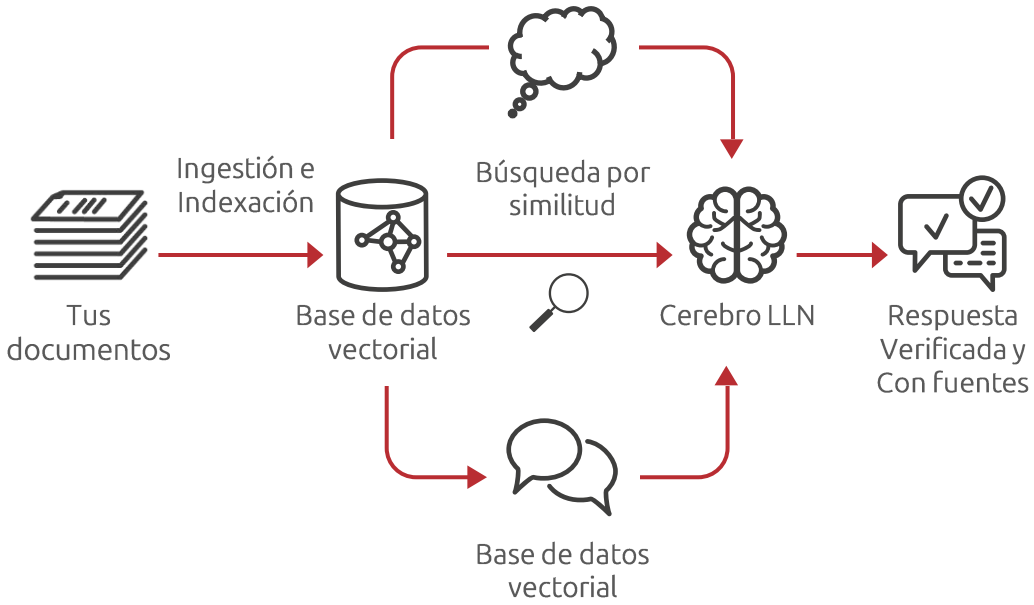
El valor que aporta la Inteligencia Artificial



El motor de la IA generativa: Precisión con RAG y Profundidad con KAG

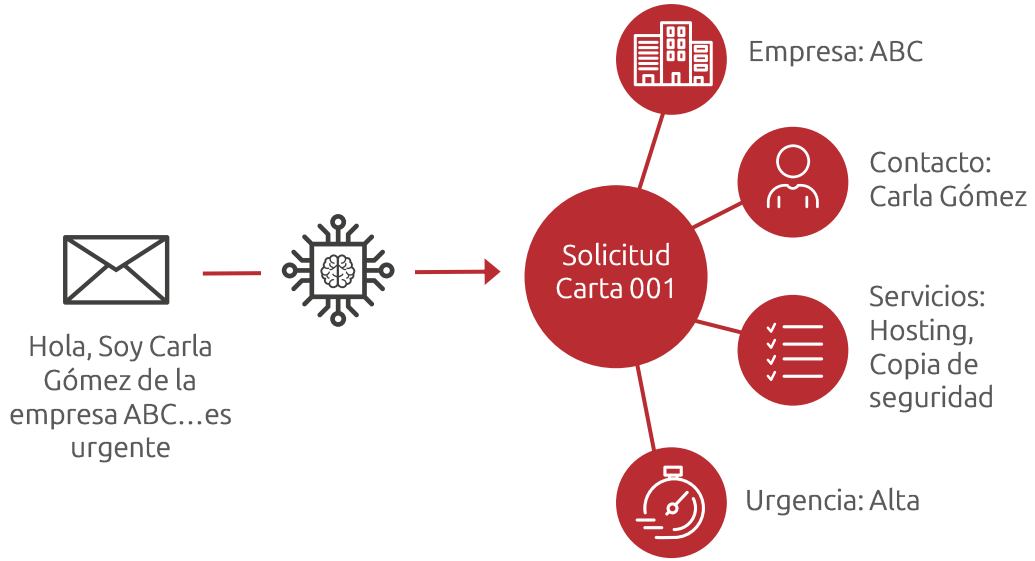
RAG (Retrieval-Augmented Generation)

Combina la recuperación de tu información con la capacidad generativa de los LLMs para eliminar “alucinaciones”



KAG (Knowledge-Augmented Generation)

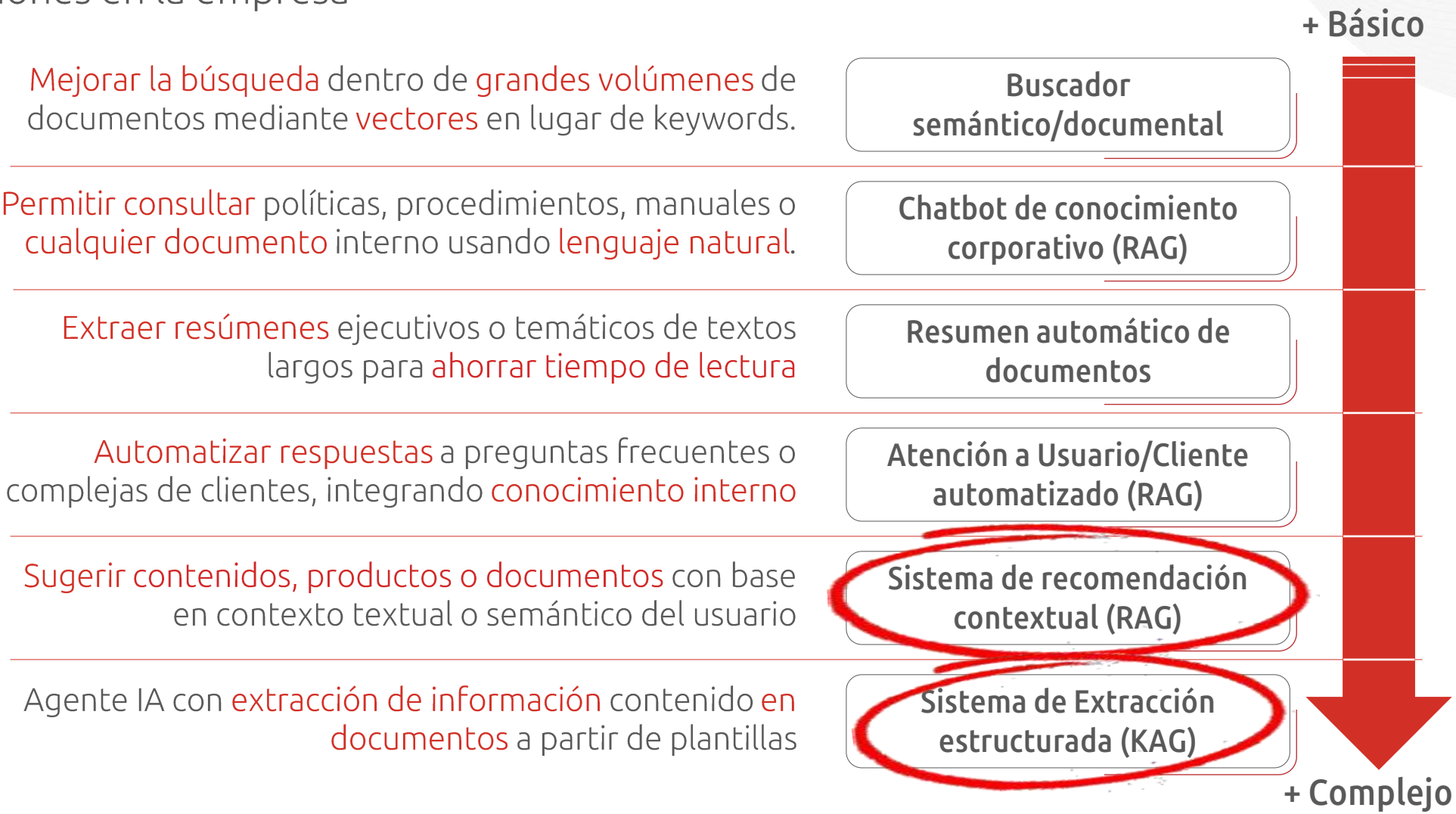
KAG va un paso más allá. No solo encuentra información, sino que la extrae, la estructura y la convierte en conocimiento accionable



semantic
systems

IA Generativa

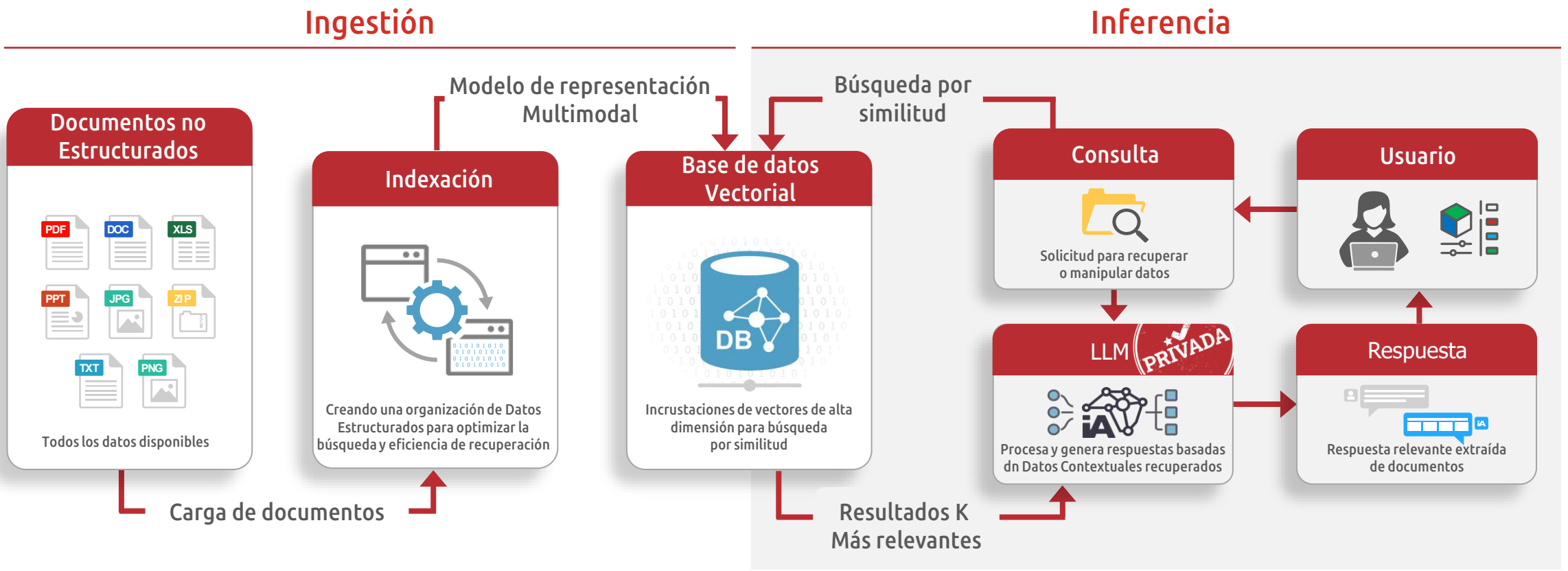
Aplicaciones en la empresa



IA Generativa | Conceptos clave de RAG

RAG (Retrieval-Augmented Generation)

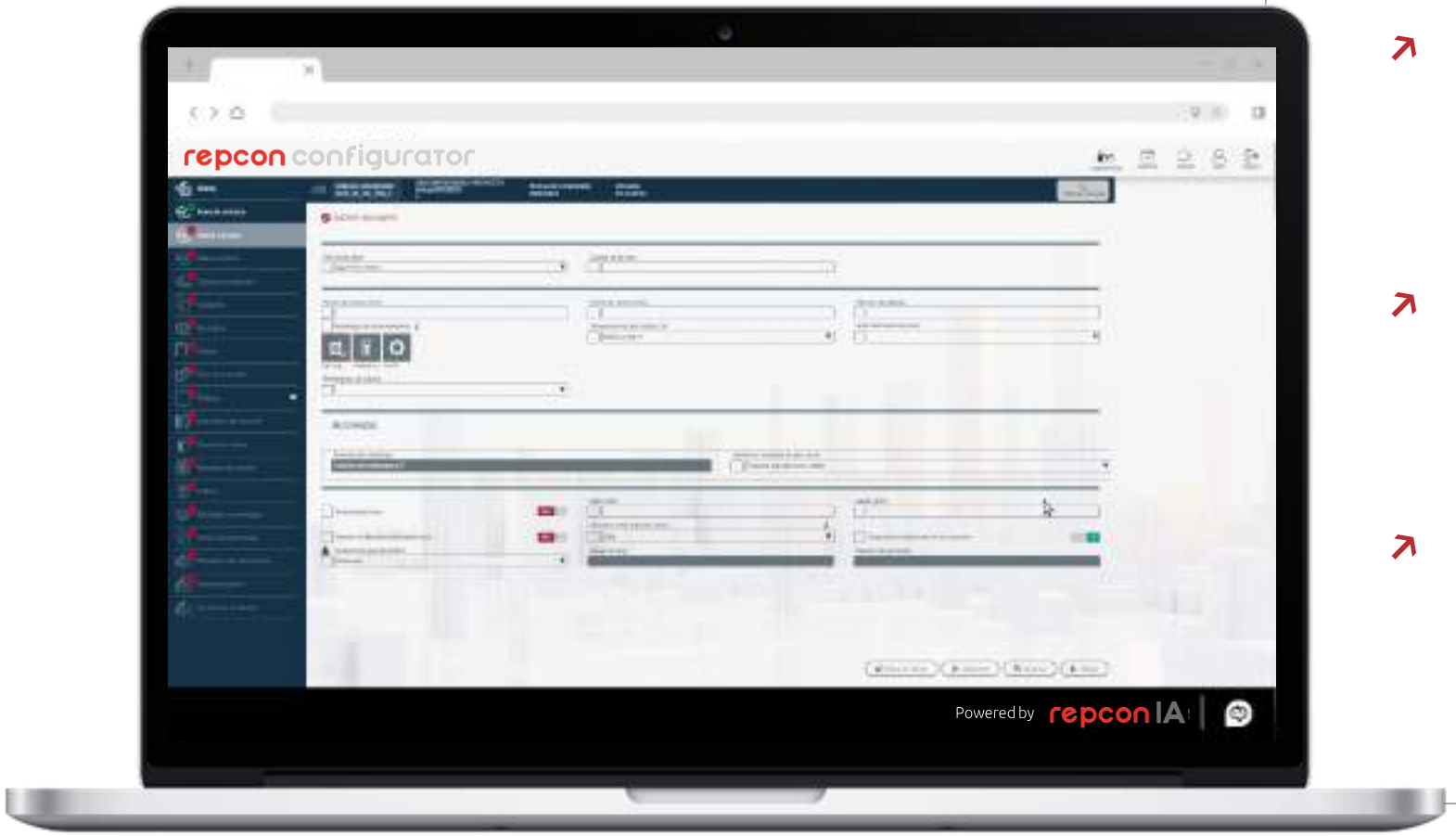
Combinación de la potencia de los modelos de recuperación de información con capacidad generativa de los LLM



semantic systems

IA Generativa

Asistente de Configuración



IA en la Configuración de Producto

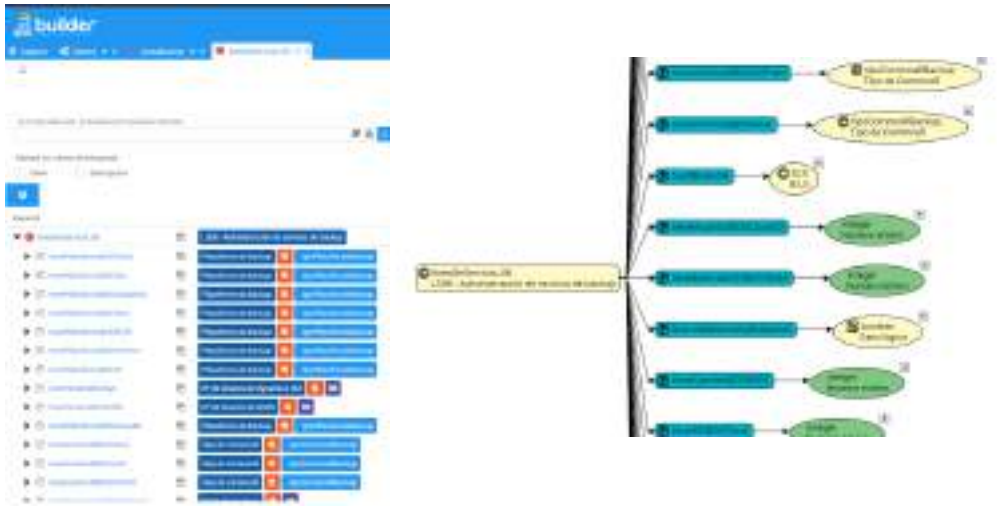
- **Soporte en lenguaje natural**
  - Chat soportado por IA
  - Procesamiento LLM
  - Dialogo con el configurador
- **Guía clara y sencilla para configurar productos**
  - De manera eficiente
  - Mínima experiencia
- **Lo mejor de dos mundos**
  - Determinista, configurador
  - No determinista, de una red neuronal.

IA Generativa | Conceptos KAG

(Knowledge-Augmented Generation)

Ontología base

- Modelado de Entidades y Relaciones



- Constructor de Ontologías

builder

Ejemplo: Lectura de correos

Hola,

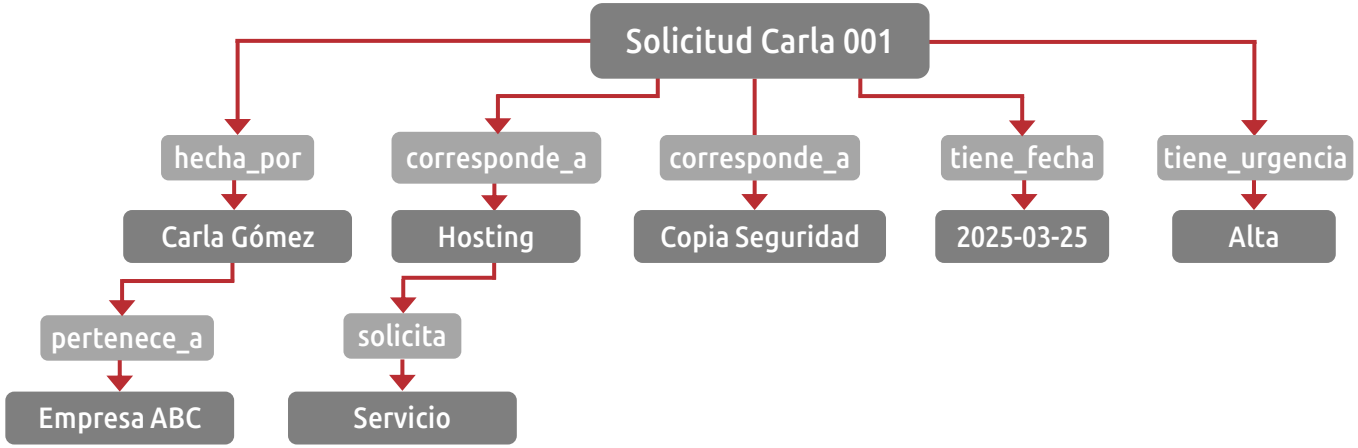
Soy Carla Gomez de la empresa ABC. Estamos interesados en contratar vuestros servicios para albergar una página Web.

Necesitamos oferta de hosting y copia de seguridad para la duración del proyecto de a años, incluyendo gestión de dominio y certificados.

Nos gustaría recibir la oferta esta semana, ya que es urgente

Gracias,
Carla

Extracción del Conocimiento



IA Generativa

repcon IA | Generación de oferta asistida por IA

Hola,

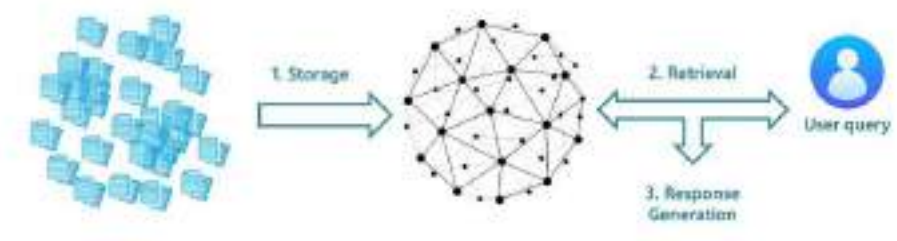
Soy Carla Gomez de la empresa ABC. Estamos interesados en contratar vuestros servicios para albergar una página Web.

Necesitamos oferta de hosting y copia de seguridad para la duración del proyecto de a años, incluyendo gestión de dominio y certificados.

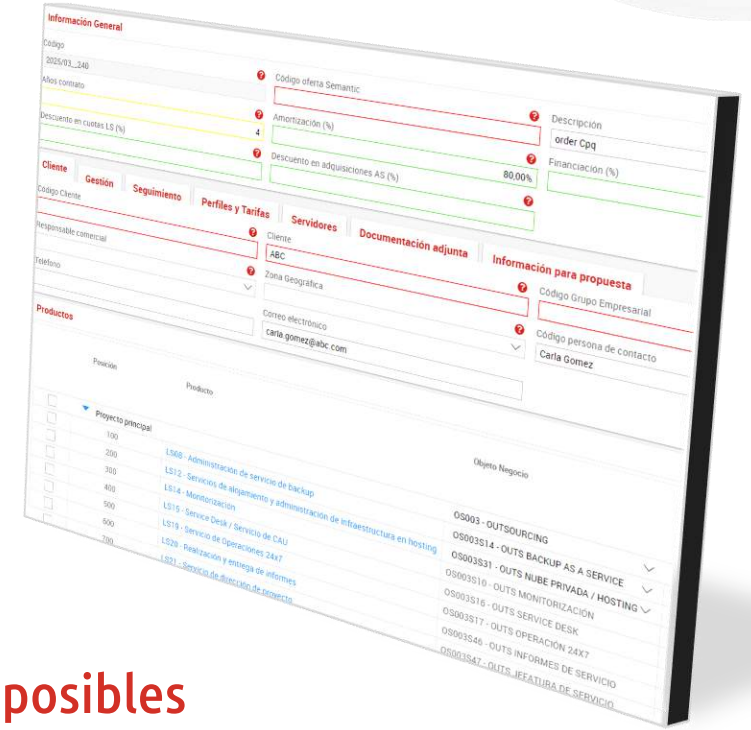
Nos gustaría recibir la oferta esta semana, ya que es urgente

Gracias,
Carla

Extracción del Conocimiento



Salida 1: Generación preconfiguración



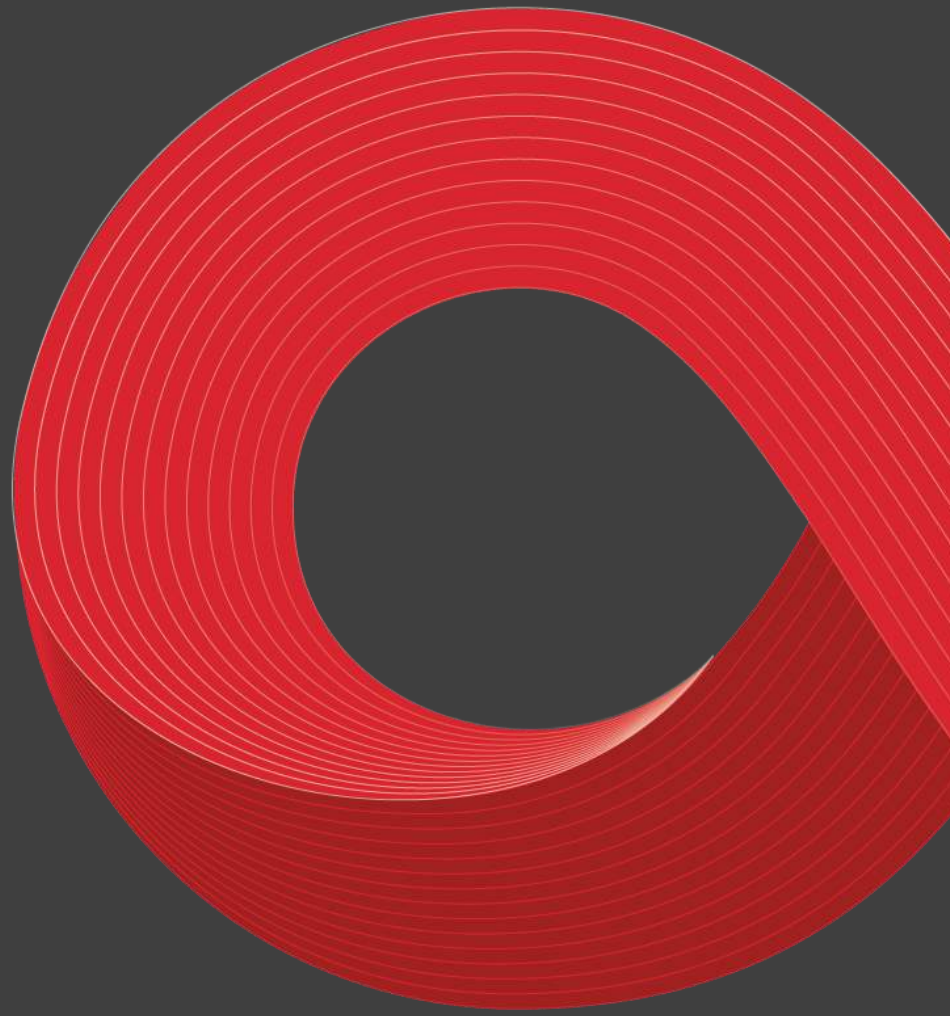
Salida 2: Consultas posibles

- ¿Qué clientes solicitaron un producto determinado?
- ¿Qué opcionales se solicitaron más en marzo?
- ¿Qué grupo(s) de características están más solicitadas?
- ¿Qué nos pidió exactamente el cliente?

semantic
systems

Semantic y repcon

El Valor de la Experiencia



Metodología del Proyecto

repcon pricing & quoting | configurator

Análisis

Identificación y racionalización de la información del producto (opciones características, reglas, precios…)

Modelado

Cargar la información de producto y reglas en Repcon Configurator mediante Builder

Formación

Capacitación del equipo del cliente en uso, mantenimiento y buenas prácticas

Producción

Validación/ despliegue del configurador y monitoreo inicial del rendimiento

semantic systems

Soporte Funcional: La Tecnología como Servicio

Una experiencia diferente para cada usuario

01

Ventaja Competitiva

La tecnología como tu aliado estratégico, respaldada por un soporte funcional experto, que te diferencia dentro de tu ecosistema empresarial

02

Evolución Continua

Servicios de soporte que se adaptan en tiempo real a las necesidades cambiantes del cliente

03

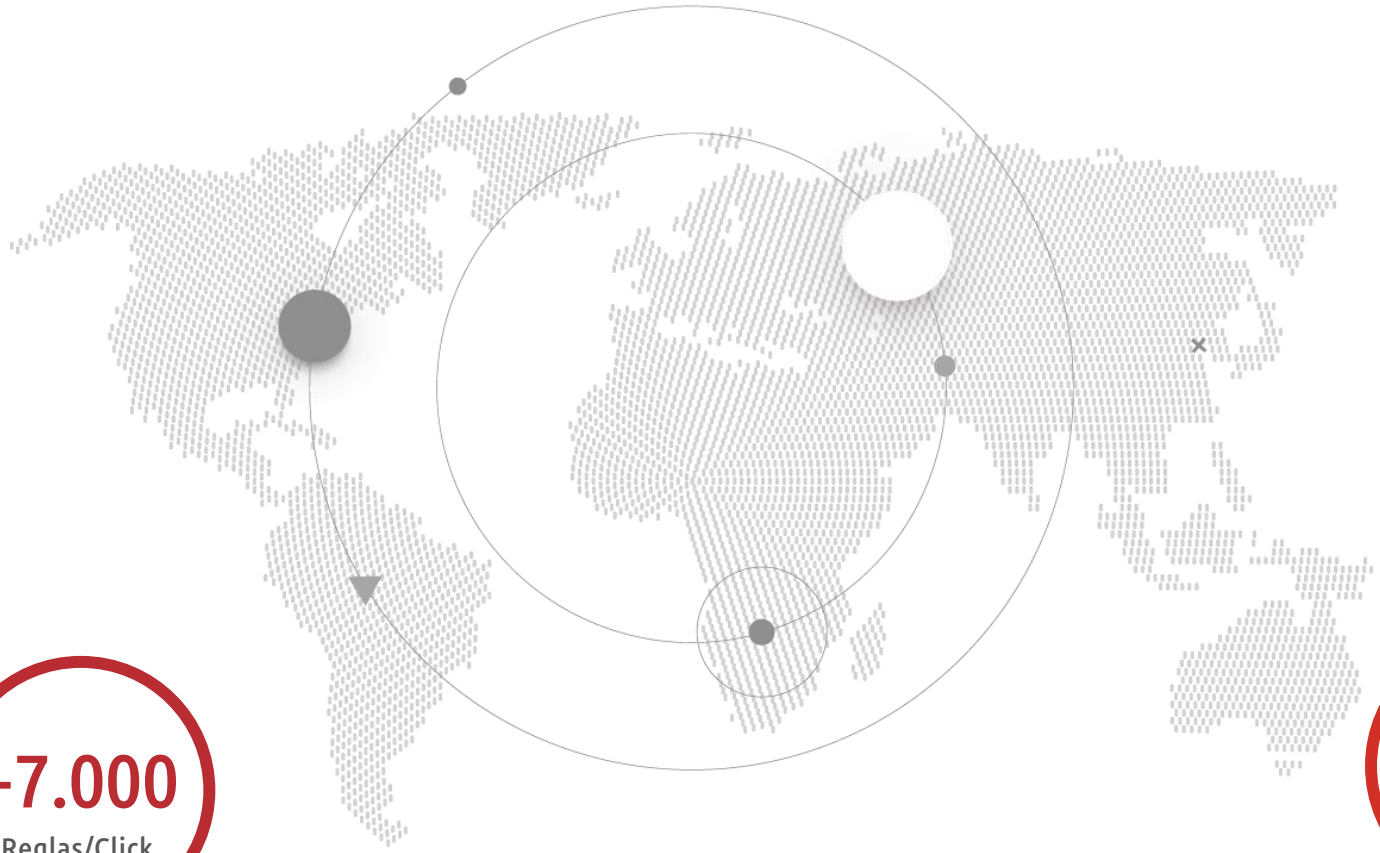
Mantenimiento y Soporte

Gestión continua y proactiva que anticipa y resuelve necesidades funcionales y tecnológicas al ritmo de tu negocio

- Equipo de Soporte dedicado
- Acceso a los conocimientos multidisciplinares del equipo de trabajo.
- Gestión centralizada
- Acceso del cliente a la herramienta de ticketing

semantic systems

repcon Pricing&Quoting | Configurator



+23
Años

Desde 2003

Crecimiento sostenido y consolidación en múltiples sectores

+20
Países

Uso Global

Conexiones desde cualquier punto del planeta confían en repcon configurator

+7.000
Reglas/Click

Alta complejidad

Empresas con grandes volúmenes de información, asegurando disponibilidad a y consistencia

+2.000
Usuarios

Fiabilidad

Miles de usuarios utilizando la herramienta a diario demuestra su fiabilidad y beneficios

semantic systems

¿Por qué Semantic Systems y repcon?

Producto e Innovación

I+D
Evolución continua del producto propio

Integración Fiable
Con ERP y resto del ecosistema IT

Apuesta de Futuro
Inquietud por la Evolución permanente de nuestros servicios y productos.

Fabricante
Mayor influencia y prioridad del cliente en la evolución del producto

Equipo y Experiencia

Equipo Humano
+250 personas con alta experiencia y expertise

Experiencia
+20 años de evolución e integración de nuestras soluciones y servicios

Cercanía
Equipo próximo y flexible, entendemos tus problemas

Configurador de producto

repcon pricing & quoting | configurator

Fotorrealismo: Ascensores

Configuración de una cabina de ascensor con múltiples materiales y luminarias.

- Materiales metálicos, plásticos, cristales, maderas y granitos
- Múltiples espejos
- Capturas de imágenes para ficha comercial

semantic systems

Configurador de producto

repcon configurator

Ensamblado y posicionamiento 3D:
Equipos de control remoto

Configuración de pedidos personalizados de equipos de control remoto definiendo de manera interactiva mecanismos, materiales, electrónica, montaje etc.

- Posicionamiento de mecanismos en faceplates
- Aplicación de restricciones geométricas
- Cálculo de colisiones en tiempo real
- Textos e iconos
- Generación de planos

semantic systems

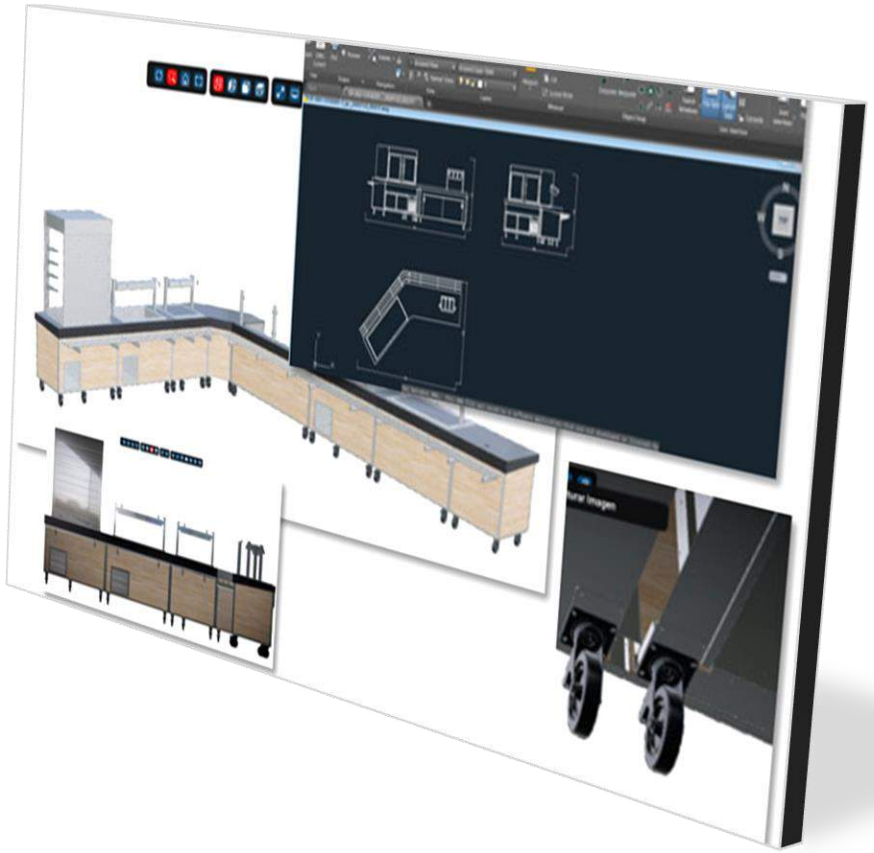
Configurador de producto

repcon configurator

Generación de planos: Líneas self services

Partiendo de modelos 3D en composición de líneas de self service mediante configuración 3D con una gama de productos muy alta aplicando componentes, materiales y texturas variadas.

- Iluminaciones, texturas o logotipos sobre superficies
- Planos dwg, de la solución y de cada uno de los elementos
- Fichas técnicas por cada módulo detalles técnicos completos



semantic systems

Configurador de producto

repcon configurator

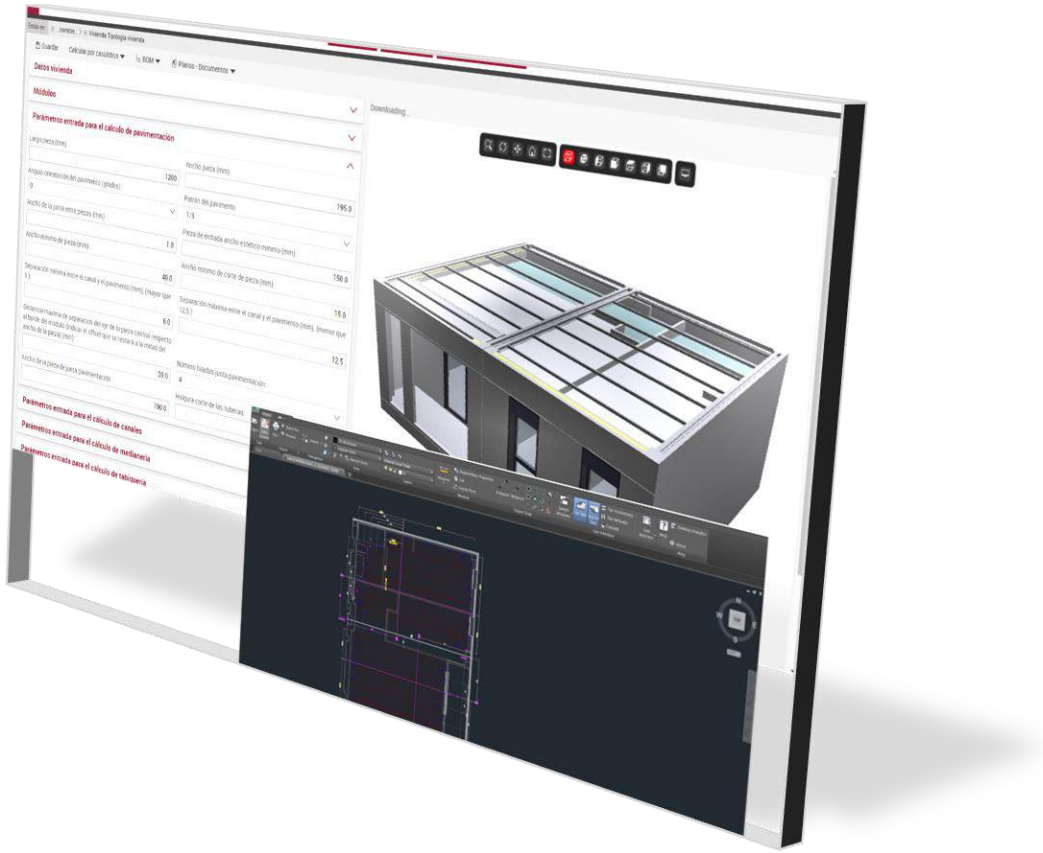
Generación de documentación: Edificios modulares

A partir de un edificio en formato IFC y parametrización por parte del usuario, generación de planos de distinta naturaleza.

Tanto técnica como comercial: presupuesto, oferta, ficha técnica, manuales…

Generación DINAMICA de documentación: Word, Excel, PDF, con imágenes variables: planos .dwg, ficheros BIM, croquis, esquemas, etc.

Basada en plantillas y/o composición de archivos, para un fácil mantenimiento.



semantic systems

Configurador de producto

repcon configurator

Lista de materiales: Invernaderos

Generación de estructura de materiales, o Bill of Materials (BOM), sin límite de niveles. Documento que define todos los elementos indispensables para llevar a cabo un proceso de producción de un producto determinado. Generación de rutas de fabricación (maquinas, tiempos…)

Cálculo de coste estimado:

- Costes de máquina
- Costes de material
- Costes de operación

semantic systems

Configurador de producto

repcon configurator

Libro digital del edificio

Representa un registro de los principales eventos y cambios en el ciclo de vida de un edificio, como cambio de propiedad, tenencia o uso, mantenimiento, renovación, así como otras intervenciones. Las distintas etapas que se pueden cubrir son el alta, ejecución, garantía y mantenimiento.

- Creación automática de elementos estructurales a partir de IFC
- IoT para cumplimentar el libro digital del edificio
- Modificaciones manuales por parte de usuarios
- Integración de alertas
- Analítica de datos

semantic systems

Preguntas y respuestas

comercial@semantic-systems.com
dmp@semantic-systems.com

semantic
systems

GRACIAS

Semantic Systems

David Montia
dmp@semantic-systems.com
607 161 745 | 94 454 55 50

semantic
systems

Radiografía ciber: ¿sobrevivirías a una auditoría hoy?

Una ponencia de **Beatriz Carratalá**, Socia y Directora del Área de Ciberriesgos en **Securizable**

CIBERSEGURIDAD INDUSTRIAL | NIS 2 | CIBERSEGUROS

SECURIZABLE

SECURIZABLE

Antes de empezar

Dos preguntas incómodas

Pregunta 1

Si vuestra empresa sufriera mañana un ciberataque que parara la producción **una semana entera**, ¿podría seguir operando sin un impacto financiero crítico?

Pregunta 2

¿Sabéis con certeza si vuestra empresa cumple hoy los requisitos para que una aseguradora **le pague un siniestro cibernético**?

Si las dos respuestas no son un sí rotundo, esta ponencia es para vosotros. Y para quien piense que esto va de otros, tres datos que sitúan el problema:

3/día

Ciberataques graves en España

En el segundo semestre del último año, con la industria como blanco prioritario.

#1

Manufactura: sector más atacado

Por cuarto año consecutivo, por delante incluso del sector bancario a escala global.

£196M

Impacto Jaguar Land Rover

Seis semanas con producción parada. Solo en el trimestre del ataque. Y sin un ciberseguro cerrado que lo cubriera.

Beatriz Carratalá LLeó es especialista en ciberseguridad y gestión de ciberriesgos con una sólida base jurídica y tecnológica.

En 2022, Beatriz cofundó SECURIZABLE, una consultora de vanguardia en gestión de riesgos tecnológicos, donde dirige la consultoría de ciberriesgos.

Como educadora y mentora dedicada, ha sido coautora de módulos de formación, tutora de cursos y ha impartido charlas sobre ciberseguridad.

Beatriz también forma parte de la Junta Directiva de Women4cyber y apoya activamente el uso ético de la tecnología a través de organizaciones como Incibe.

SECURIZABLE

Agenda de la sesión

Lo que vamos a construir juntos hoy

Esta sesión no es una clase magistral busca conformar una radiografía en tres dimensiones aplicada a vuestra realidad como empresa industrial: dónde está hoy vuestra seguridad, qué os va a exigir NIS 2 y qué condiciones tenéis que cumplir para que un ciberseguro sea una red de verdad —y no un papel inútil— el día que lo necesitéis.

Saber dónde estás

Por qué auditar hoy: ataques, NIS 2 y aseguradoras. Marcos de referencia: ISO 27001, ENS, NIST e IEC 62443 para entorno OT. Áreas clave de una auditoría industrial.

Cumplir lo que te van a exigir

Cumplimiento NIS 2: qué evidencias necesitas y cómo demostrarlas ante el regulador, vuestros clientes y vuestra cadena de suministro.

Tener red de seguridad

Elegibilidad aseguradora: los controles que exige el mercado.

Bloque 1 — La nueva realidad

Por qué la industria se ha convertido en objetivo prioritario

La respuesta no es que seamos un objetivo especialmente atractivo por lo que producimos. **Es algo más estructural**: hemos transformado, en muy pocos años, la forma en que funcionan nuestras fábricas. Y esa transformación ha tenido consecuencias de seguridad que no siempre se miden.

SECURIZABLE

La convergencia IT-OT: la puerta que abrimos sin medir

Durante décadas, la planta y la oficina vivían en mundos separados. El **IT** —ordenadores, correo, ERP— por un lado. El **OT** —autómatas, PLC, SCADA, las máquinas que fabrican— por otro. Ese segundo mundo estaba aislado: sin conexión con el exterior, y esa desconexión era, en sí misma, su seguridad.
La **digitalización industrial** ha unido esos dos mundos. Datos de planta en tiempo real, mantenimiento predictivo, acceso remoto del fabricante, sensores que reportan a la nube. Todo eso aporta eficiencia y competitividad. Pero tiene una consecuencia directa: **cada conexión nueva es una puerta nueva**. La ***superficie de ataque*** —el conjunto de puntos por los que alguien podría entrar— **se ha multiplicado**.

Convergencia IT-OT

Máquinas diseñadas para estar aisladas hoy cuelgan de la misma red que el correo electrónico. Un incidente que empieza en una bandeja de entrada puede acabar en la línea de producción.

Accesos remotos no revisados

Accesos abiertos con prisa para mantenimiento de proveedor o teletrabajo, y que nunca se revisaron ni cerraron. Son vectores activos de entrada con credenciales a menudo sin caducidad.

Equipamiento heredado sin parche

En Europa, el **80% de los fabricantes** opera sistemas OT críticos con vulnerabilidades ya conocidas y documentadas. No ocultas: conocidas. Parcharlos implica parar producción, y ese coste se pospone indefinidamente.

La cadena de suministro extendida

Vuestra superficie de ataque no termina en la valla de la fábrica. Compartís datos, conexiones y sistemas con proveedores, socios y clientes. La unidad real a proteger es la **empresa extendida**.

SECURIZABLE

El Riesgo de Terceras y Cuartas Partes

Vuestra seguridad es tan fuerte como el eslabón más débil de vuestra cadena. Podéis tener la casa en orden y veros comprometidos por la puerta de otro. Las vulnerabilidades de vuestro proveedor son, en la práctica, vuestras vulnerabilidades.

~30%

Brechas con terceros

Según el Verizon DBIR 2024, aproximadamente el 30% de las brechas de seguridad implica a un tercero en la cadena.

60%

Ataques por suministro

Iberdrola estima que hasta el 60% de los ciberataques a empresas comienzan explotando la cadena de suministro.

N+?

Partes invisibles

Más allá del tercero directo, la cadena se prolonga en cuartas, quintas y enésimas partes que rara vez se monitorizan.

¿Qué es un tercero?

Cualquier entidad externa con relación contractual: proveedores de software, plataformas SCADA, asesorías de nóminas, servicios en la nube, mantenedores de maquinaria. Sobre ellos existe ya cierta conciencia del riesgo.

¿Y el nivel siguiente?

Los **terceros subcontratan a su vez**: son las cuartas partes, los proveedores de vuestros proveedores. Y como ellos también subcontratan, hablamos de **enésimas partes**: una cadena que se prolonga mucho más allá de lo que véis. Si un cuarto eslabón con malas prácticas falla, acabáis afectados aunque ni supierais que existía.

La disciplina específica

Para abordar este problema existe la **gestión de riesgo de terceras y cuartas partes**, una práctica que identifica, evalúa y vigila ese riesgo en toda la red de proveedores, no solo en los inmediatamente visibles. Esto ya no es solo buena práctica: **NIS 2 obliga explícitamente a evaluar la cadena de suministro e incorporar estas exigencias a los contratos**.

⚠ El riesgo no termina en quien factura directamente. Termina donde termina la cadena, y esa cadena no tiene un fin visible.

¿Cómo se gestiona sin volverse loco?

1

Conoce tu cadena de suministro

Identifica quiénes son todos tus proveedores directos e indirectos, a qué sistemas y datos tienen acceso, y qué terceros emplean a su vez. Sin visibilidad no hay gestión posible. Un inventario actualizado es el punto de partida imprescindible.

2

Evalúa antes de confiar

Evalúa la madurez de seguridad de un proveedor **antes** de formalizar la relación, no solo su precio o capacidad técnica. Utiliza cuestionarios de seguridad, auditorías o certificaciones reconocidas (ISO 27001, ENS) como criterios de selección objetivos.

3

No los pierdas de vista

La evaluación inicial no es suficiente. El riesgo evoluciona: un proveedor seguro hoy puede no serlo mañana tras un cambio de subcontratista, una fusión o una configuración deficiente. Establece revisiones periódicas y alertas de incidentes de terceros.

4

Cierra el círculo contractualmente

Exige en los contratos que **tus terceros gestionen con el mismo rigor a sus propios proveedores**. Este requisito de flujo descendente es la única manera de extender los controles más allá del perímetro directo. NIS 2 respalda y refuerza esta exigencia.

«Vuestra seguridad es tan fuerte como el eslabón más débil de vuestra cadena. Podéis tener la casa en orden y veros comprometidos por la puerta de otro.»

SECURIZABLE

Los Datos dimensionan la superficie

En 2025, la ciberseguridad ha dejado de ser una preocupación teórica para convertirse en una realidad operativa. Las cifras hablan por sí solas: el volumen, la frecuencia y el impacto de los ataques se disparan año tras año.

122.223

Incidentes gestionados por INCIBE

Un **26% más** que el año anterior

605

Ciberataques de alto impacto

Solo en el segundo semestre, según NTT Data. **3 al día** con capacidad real de paralizar operaciones

19,4%

Sistemas industriales atacados

De los sistemas de control industrial en España detectaron intentos de ataque **en un solo trimestre**, según Kaspersky

36.400

Alertas procesadas por CSIRT-CV

El centro autonómico valenciano registró un **96% más** que el año anterior en 2024

Casos reales en la industria española

Vicky Foods (Dulcesol) y San Benedetto —embotelladora en Requena, Comunitat Valenciana— reconocieron abiertamente haber sufrido incidentes de ciberseguridad en una jornada sectorial sobre la industria agroalimentaria.

Cuando la producción se detiene

En septiembre de 2024, la siderúrgica **Aceros Olarra** tuvo que paralizar por completo su producción de acero durante **una semana entera** a consecuencia directa de un ciberataque. Un coste operativo, reputacional y económico difícil de ignorar.

⊗ El mensaje es claro: ningún sector, ninguna empresa y ninguna región están al margen. La pregunta ya no es *si* se producirá un ataque, sino *cuándo* y si la organización estará preparada para responder.

SECURIZABLE

Las cinco modalidades de ataque que se repiten

Los vectores son diversos, pero en la práctica industrial se repiten cinco patrones. Conocerlos es el primer paso para auditarlos.

Ransomware

El más frecuente. El atacante cifra los sistemas para impedir operar y exige un rescate. La evolución actual es la **doble extorsión**: primero roban una copia de vuestra información y luego cifran. Si no pagáis, amenazan con publicarla o avisar a vuestros clientes. Presión financiera y reputacional simultánea.

Fraude al directivo (CEO fraud)

Ingeniería social pura. Un correo, una llamada o, hoy, una voz o vídeo imitados con inteligencia artificial que suplantan a un responsable y ordenan una transferencia urgente o un cambio de cuenta bancaria. No rompe ningún sistema: explota la **confianza y la prisa**.

Ataque a través de la cadena de suministro

Entrar en una organización bien protegida usando como puente a un proveedor o a un software de confianza. SolarWinds, Kaseya, XZ Utils: los casos paradigmáticos demuestran que no hace falta atacar la fortaleza; basta con atacar a quien tiene las llaves.

Ataque directo a la OT

Busca el proceso industrial: alterar parámetros, detener una línea, manipular un sistema de control. Es el más específico del sector industrial y el que puede tener **consecuencias físicas**, no solo económicas: seguridad de las personas, daño medioambiental, responsabilidad civil.

Robo de propiedad industrial

Planos, fórmulas, parámetros de máquina, configuraciones, secretos industriales. A veces el objetivo no es pararos, sino **llevarse el conocimiento** que os ha costado años y millones de euros desarrollar. Sin cifrado, sin alarma visible: la empresa puede no saberlo durante meses.

SECURIZABLE

El punto de partida honesto: dónde estamos como sector

Conviene ser honestos, sin dramatizar. La fotografía del sector industrial en materia de ciberseguridad muestra un desequilibrio claro entre el ritmo de la digitalización y el de la protección.

IT vs. OT: dos velocidades

Proteger el IT empieza a estar interiorizado en muchas empresas. Proteger el OT —los sistemas que controlan la producción— sigue siendo una asignatura pendiente para la mayoría, incluidas algunas grandes. El 80% de fabricantes europeos opera con vulnerabilidades OT conocidas y sin parchar.

Pymes en el punto de mira

El **70% de los ciberataques afecta a pymes**, con un coste medio de 35.000 € por incidente. El tamaño no protege: una planta parada cuesta lo mismo, en proporción, sea grande o mediana. Y muchas pymes industriales son proveedoras de empresas más grandes que pronto les exigirán.

La presión regulatoria llega

NIS 2 obliga a las empresas grandes a trasladar sus exigencias de ciberseguridad por contrato a sus proveedores. La seguridad va a dejar de ser una recomendación para convertirse en una condición para seguir siendo proveedor.

"La digitalización ha ido por delante de la seguridad. Hemos conectado mucho y protegido menos. Y ahora el entorno regulatorio y el mercado asegurador empiezan a exigir que lo que conectamos también esté protegido."

— Beatriz Carratalá, Securizable

La conclusión práctica: La superficie de ataque se ha ampliado más deprisa que nuestras defensas. El entorno regulatorio empieza a exigir. Los clientes grandes pronto preguntarán. La auditoría deja de ser un trámite técnico para convertirse en la herramienta que **ordena la respuesta**. Es lo que veremos a continuación.

SECURIZABLE

¿Por qué auditar tu ciberseguridad, y por qué precisamente hoy?

Una sesión de trabajo para PYMEs del sector metalmecánico que no pueden permitirse ignorar lo que ya está ocurriendo — ni las consecuencias de no actuar.

BLOQUE 2. · LA RADIOGRAFÍA PRECEPTIVA

SECURIZABLE

Cinco razones que convergen al mismo tiempo

Antes de mostrar lo que falla, hay que responder a la pregunta más legítima de cualquier responsable industrial: **«Bastante tengo con sacar la producción, los plazos, los márgenes y encontrar gente»**. Es una objeción justa. Pero para una PYME industrial del metal, evaluar el punto de partida en ciberseguridad ya no es un ejercicio técnico opcional. Es una necesidad estratégica y de supervivencia.
Las cinco razones que siguen se articulan sobre tres pilares que hoy ya no van por separado: te empujan los tres a la vez.

Operativo	Seguridad	Legal
Tu negocio y su continuidad de producción	La amenaza real que ya te ha elegido	Lo normativo y lo societario, con sanciones directas

01

Diagnóstico de supervivencia

Saber de dónde partes y qué tienes expuesto

02

La amenaza real

El metal está en el punto de mira de los atacantes

03

Continuidad de negocio

Resiliencia operativa y recuperación real

04

NIS 2

La auditoría como obligación legal imperativa

05

Responsabilidad personal

La dirección responde con cargo y patrimonio

SECURIZABLE

RAZÓN 1 · DIAGNÓSTICO PROACTIVO

No puedes proteger lo que no sabes que tienes

La falsa sensación de seguridad

Muchas PYMEs confían ciegamente en que «tienen un buen antivirus» o un soporte informático externo básico, e ignoran su superficie real de exposición: redes industriales OT, APIs de integración con clientes, accesos remotos de mantenimiento. La frase **«nosotros nunca hemos tenido un problema»** nace exactamente de ahí — de no haber mirado.

La digitalización del sector crea nuevas puertas

El sector metalmecánico opera hoy bajo una digitalización profunda: producción conectada, ERP integrado con la cadena de suministro, automatización de planta (OT) y plataformas de diseño compartido con clientes. Cada una de esas conexiones es una puerta de entrada. Conocer el punto de partida permite dos cosas fundamentales:

- **Evitar la falsa sensación de seguridad** que genera no haber medido la exposición real.
- **Optimizar la inversión**: siguiendo metodologías como el marco NIST o MAGERIT (del Centro Criptológico Nacional), la empresa sabe dónde concentrar cada euro.

Sin un análisis de criticidad formal, se protege igual lo que no importa que lo que es indispensable para fabricar y facturar. Auditar es lo que dice **dónde concentrar cada euro**. Para una PYME, gastar bien el presupuesto de seguridad no es un lujo: es la diferencia entre estar protegido y malgastar.

SECURIZABLE

RAZÓN 2 · LA AMENAZA REAL

SECURIZABLE

El metal está en el punto de mira

Los ciberdelincuentes ya no buscan solo grandes corporaciones. La PYME industrial es un objetivo altamente lucrativo por motivos muy concretos, y la industria manufacturera ya es el **sector más atacado de España**, por encima del sector bancario.

Ransomware: el secuestro de tu planta

Una planta del metal con los servidores cifrados sufre pérdidas inmediatas y devastadoras. El atacante lo sabe: la presión por recuperar la producción empuja a pagar el rescate. **No os atacan a pesar de ser fábrica; os atacan precisamente porque sois una fábrica que no puede permitirse parar.** El tiempo de inactividad se convierte en la palanca de extorsión más efectiva posible.

La PYME como puerta trasera

Si estáis integrados digitalmente con un cliente corporativo grande — y en el metal lo estáis casi siempre — una defensa débil en vuestra casa puede usarse para saltar a la red de ese cliente. **Consecuencia directa: pérdida inmediata del contrato y quiebra reputacional.** Dejáis de ser el proveedor de confianza para convertiros en el agujero por el que entraron.

Para defenderte, lo primero es saber por dónde pueden entrar. **Auditar es levantar ese mapa antes de que lo levante el atacante.**

SECURIZABLE

RAZÓN 3 · CONTINUIDAD DE NEGOCIO

¿Puede tu planta seguir operando si falla el sistema principal?

Esta razón es de pura **resiliencia operativa**. Todo gerente debería poder responder sin dudarlo: *«Si mañana falla el sistema informático principal o un proveedor tecnológico clave, **¿puede mi planta seguir operando bajo mínimos?»***

El factor humano

La concienciación de los empleados es lo que evita los fraudes más comunes: la suplantación en una factura, un correo malicioso de dirección — lo que técnicamente se denomina **fraude del CEO o BEC (Business Email Compromise)**. Sin formación ni protocolos claros, el error humano sigue siendo el vector de entrada más explotado. Una auditoría identifica el nivel real de concienciación de la plantilla y las brechas de procedimiento que nadie ha documentado.

El modo degradado y la recuperación real

La segunda debilidad frecuente es la del **backup y la restauración**. La pregunta no es solo «¿existen las copias de seguridad?» sino **«¿a qué velocidad real se restauran?»**. Una copia que tarda tres semanas en levantar una planta no es una copia: es un problema aplazado. Vuestra ciberseguridad ya no protege «los ordenadores». Protege vuestra capacidad de **seguir produciendo y cobrando**. Y la auditoría responde a la pregunta que debería estar tan presente como vuestro margen: *«¿Cuántos días aguanto parado antes de que esto sea irreversible?»*

22 días

Tiempo medio de inactividad

Duración media de la interrupción operativa tras un ataque de ransomware en empresa industrial

95%

Ataques vía empleado

De los incidentes tienen como vector inicial el factor humano: phishing, BEC o credenciales comprometidas

60%

PYMEs sin plan de continuidad

De las pequeñas y medianas empresas industriales no disponen de un plan de continuidad de negocio documentado y probado

RAZÓN 4 · EL REQUERIMIENTO LEGAL

NIS 2 convierte la auditoría en obligación legal

Para muchas de las empresas presentes, auditarse ya no es una buena práctica voluntaria: es una obligación legal vigente. La ciberseguridad ha dado el salto definitivo al terreno de la regulación imperativa en toda la Unión Europea con la Directiva NIS 2, transpuesta en España a través del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad. Si superáis los **50 empleados** o los **10 millones de euros de facturación**, lo más probable es que estéis dentro de su perímetro.

Artículo 21 · Obligación de evaluar

Obliga a **evaluar la eficacia de vuestras medidas de seguridad**. No basta con tenerlas: hay que comprobar que funcionan. Es decir, auditarlas. Esta obligación aplica también a la cadena de suministro: las empresas grandes deben auditar la ciberseguridad de sus proveedores — eso sois vosotros.

Artículo 32 · Auditorías por la autoridad competente

Faculta a la autoridad a someter a las entidades a **auditorías periódicas** si son esenciales, y a **auditorías específicas y ad hoc tras un incidente** si son importantes. La pregunta ya no es *si* habrá auditoría. Es **quién la dirige**: tú, de forma ordenada y a tu ritmo, o el regulador, justo después del peor momento posible.

Sanciones directas y millonarias

Las sanciones son claras: **hasta 10 millones de euros o el 2% de la facturación global** para entidades esenciales; hasta **7 millones o el 1,4%** para las importantes. Se aplica la que resulte mayor. Y aunque NIS 2 no os aplique directamente, el artículo 21 obliga a vuestros clientes grandes a auditaros a vosotros: os mandarán cuestionarios y sin evidencias dejaréis de ser proveedor homologado.

⚠ Como ocurrió en su día con la ISO 9001: lo que era una ventaja competitiva se convierte en requisito mínimo para entrar en el concurso.

SECURIZABLE

RAZÓN 5 · EL REQUERIMIENTO SOCIETARIO

La responsabilidad sube al despacho de dirección

Esta es la razón más importante y el **cambio de paradigma más drástico**. La ciberseguridad ha dejado de ser un asunto delegable en el departamento de informática. Hoy pertenece al **consejo de administración y a la gerencia**. Tres consecuencias legales concretas que todo directivo debe conocer:

1

El deber de diligencia

El **artículo 225 de la Ley de Sociedades de Capital** obliga a todo administrador a gestionar con la diligencia de un «ordenado empresario», incluyendo el deber de informarse activamente de los riesgos materiales que amenazan la continuidad de la sociedad. Ignorar el estado de las defensas tecnológicas empieza a interpretarse como una dejación de ese deber. **No saber ya no es una excusa: es parte de la negligencia.**

2

Responsabilidad solidaria personal

El marco que deriva de la transposición de NIS 2 introduce de forma explícita que los miembros del órgano de dirección pueden responder **solidariamente** por las infracciones de la entidad. Un administrador puede llegar a responder con su **patrimonio personal** o enfrentarse a la **inhabilitación temporal** para ejercer cargos directivos. La multa ya no es solo de la empresa.

3

La jurisprudencia ya está aquí

El **Tribunal Supremo, sentencia 136/2025 de 19 de febrero**, resolvió un caso de un concesionario de automoción: una brecha en el correo permitió suplantar a un empleado y un socio transfirió dinero a una cuenta fraudulenta. La empresa víctima detectó el incidente y no avisó a sus socios. El Supremo confirmó su **responsabilidad civil subsidiaria** por los daños a terceros. *Ser víctima ya no exime si la dirección actuó con pasividad.*

«¿Y qué hicisteis vosotros para evitarlo, y para limitar el daño a terceros?» — La pregunta que hoy hacen los tribunales.

SECURIZABLE

Cinco frentes, una sola palanca

Cinco razones distintas que hoy convergen en una misma pregunta de fondo: **«¿De verdad sabes cómo está tu seguridad por dentro?»**. Y solo hay una forma honesta de responderla: mirándote.

SECURIZABLE

Una auditoría útil y proporcional al tamaño de vuestra fábrica resuelve los cinco frentes a la vez. No es un gasto que os imponen los informáticos: es una decisión de gobierno, igual que una inversión en maquinaria o la apertura de un mercado. Es la radiografía que os hacéis vosotros, en frío, antes de que os la haga el médico de urgencias, en caliente y con peor pronóstico.

BLOQUE 3 · LA CADENA DE SUMINISTRO

Tu eslabón más débil no está en tu fábrica

Aunque lo hagas todo bien puertas adentro, el atacante entrará por el más débil de tus proveedores. Y, a la vez, tú eres el proveedor de alguien que ya te está mirando.
La seguridad dejó de terminar en nuestra propia empresa.

SECURIZABLE

SECURIZABLE

El perímetro ya no existe

Nuestros negocios exceden hoy de los límites físicos. No terminan en nuestra puerta, ni en nuestra valla. Viven en una red de relaciones digitales cuya extensión pocas empresas han cartografiado del todo:

El mantenedor y el integrador

El proveedor que mantiene el ERP en remoto o actualiza la línea de producción tiene acceso privilegiado a vuestros sistemas más críticos. Si su seguridad falla, la vuestra también.

Logística y datos compartidos

La empresa de logística con la que intercambiáis datos de pedidos y expediciones forma parte de vuestro ecosistema digital, aunque no aparezca en el organigrama de seguridad.

El fabricante de autómatas

Los fabricantes de maquinaria y autómatas que se conectan para diagnóstico remoto abren canales hacia vuestras redes OT que raramente están bajo supervisión de seguridad.

El cliente con el que intercambiáis planos

Las plataformas de diseño compartido con clientes crean vínculos digitales bidireccionales. Vuestra debilidad puede ser la entrada a ellos, y la suya, una puerta hacia vosotros.

El atacante lo ha entendido perfectamente: ¿para qué invertir esfuerzo en atacar de frente si puede entrar por la conexión de un proveedor con la guardia más baja? Ya no basta con preguntarse *«¿estoy yo protegido?»*. Hay que preguntarse **«¿de quién depende que yo esté protegido?»**

DATOS 2025-2026 · CIPHER / PROSEGUR

SECURIZABLE

Las cifras que cambian las prioridades

No es una hipótesis. Son cifras del informe de Cipher, la división de ciberseguridad de Prosegur, publicado a principios de 2026. Los datos son demoledores:

×2

Ataques a la cadena de suministro

Los ataques vía terceros se **duplicaron en 2025** respecto al año anterior. El crecimiento más acelerado de todos los vectores de ataque registrados.

4,33M€

Coste medio por brecha de tercero

El coste medio de una brecha originada en un proveedor o tercero, incluyendo respuesta, recuperación, sanciones y pérdida de negocio.

22,5%

Brechas con origen en proveedor

Del total de brechas de seguridad registradas en 2025 involucraron a un proveedor o tercero. **Una de cada cuatro.** El doble que el año anterior.

254 días

Para detectar y contener la brecha

Cuando la brecha entra por la cadena de suministro, las empresas tardan de media **más de ocho meses** en detectarla y contenerla. Ocho meses con alguien dentro, moviéndose, mirando, esperando.

⊗ Doscientos cincuenta y cuatro días. Entró por una puerta que no vigilabais, porque no era «vuestra» puerta: era la de un proveedor en el que confiabais.

La doble cara: víctima y puerta trasera a la vez

En el sector metalmecánico la posición es única: el riesgo de cadena de suministro os afecta por partida doble.

Sois víctimas potenciales

A través de vuestros propios proveedores — el mantenedor, el integrador, el software de gestión — sois vulnerables. Si uno de ellos cae, podéis caer con él. La brecha no entra por vuestra puerta principal, sino por una conexión de mantenimiento que nadie supervisa, un acceso remoto que nadie ha revisado desde que se instaló, o una actualización de software que viene comprometida de origen.

Sois la cadena de suministro de otro

Sois el proveedor de una automovilística, de una gran ingeniería, de una multinacional. Para esa empresa grande, **vosotros sois el eslabón débil que un atacante podría usar para llegar hasta ella**. Si os comprometen y a través de vuestra conexión saltan a vuestro cliente principal, no solo tenéis un incidente: tenéis una **pérdida de contrato y una quiebra reputacional** de la que es muy difícil recuperarse. Dejáis de ser el proveedor de confianza para ser el agujero por el que entraron.

⚠ Y ese cliente grande, precisamente para evitar que seáis la puerta de entrada, **os va a auditar a vosotros**. No como favor: como requisito contractual.

NIS 2 · ARTÍCULO 21 · CADENA DE SUMINISTRO

Lo que NIS 2 convierte en obligación para toda la cadena

La gestión de la cadena de suministro no es solo una buena práctica recomendable: es una de las **novedades estrella de NIS 2** y una obligación legal directa. El artículo 21 de la directiva exige a las **entidades obligadas que gestionen activamente el riesgo de sus proveedores**, directos e indirectos. Y la palabra clave es *activamente*: esa responsabilidad de supervisión es **indelegable**.

Identificar y clasificar proveedores críticos

Saber cuáles, si caen, os arrastran. No todos los proveedores son iguales: los que tienen acceso a vuestros sistemas de producción o datos de clientes exigen un nivel de supervisión muy superior.

Evaluar su seguridad periódicamente

No una vez al firmar y olvidarse: de forma continua. La evaluación inicial no es suficiente; la situación de un proveedor puede deteriorarse en cualquier momento.

Cláusulas contractuales mínimas

Requisitos de seguridad exigibles, obligación del proveedor de notificar sus propios incidentes y derecho a auditarles. Sin estas cláusulas, el contrato os deja sin herramientas de respuesta.

Verificación, no solo declaración

NIS 2 exige **verificación, no solo declaración firmada**. No basta con que el proveedor firme un papel diciendo que es seguro. Tenéis que poder demostrar que lo habéis comprobado con evidencias.

El mismo control que vuestro cliente grande os va a exigir a vosotros... es el que vosotros tenéis que exigir a vuestros proveedores. La auditoría sirve en las dos direcciones: para demostrar hacia arriba y para verificar hacia abajo.

SECURIZABLE

La buena noticia: no tenéis que inventar nada

Hemos recorrido tres realidades que ya no admiten dilación:

El sector industrial es hoy el objetivo número uno

La industria manufacturera lidera el ranking de sectores más atacados en España. No es una estadística futura: es la realidad operativa de 2025 y 2026.

Las defensas básicas están sin terminar y sin documentar

Las medidas que de verdad detienen los ataques más comunes — segmentación de red, gestión de credenciales, backups verificados, concienciación — suelen estar incompletas o sin evidencia de funcionamiento en la PYME industrial media.

El riesgo se extiende a toda la cadena

Hacia arriba — el cliente que os auditará — y hacia abajo — el proveedor por el que podéis caer. La seguridad ya no es un asunto puertas adentro, y el marco legal ya lo recoge expresamente.

La pregunta lógica llegados a este punto es: *«¿Por dónde empiezo?»*. Y esa es exactamente la buena noticia: **no tenéis que inventar nada**. Hay marcos de referencia probados y reconocidos — NIST, ENS, MAGERIT, ISO 27001 — que dicen exactamente qué mirar y cómo. En el siguiente bloque los veremos en detalle, aplicados al tamaño real de vuestra fábrica.

La auditoría no es el problema. Es la herramienta que os da el mapa antes de que lo necesitéis con urgencia.

Marcos de Referencia y Controles Mínimos en Auditoría Industrial

Sobre qué se construye una auditoría y qué controles no pueden faltar en un entorno industrial

BLOQUE 4

AUDITORÍA · CUMPLIMIENTO · OT/IT

SECURIZABLE

Qué hace, exactamente, un marco de referencia

Una auditoría no consiste en que alguien entre a una empresa y opine. Consiste en **contrastar la realidad de la organización contra un patrón objetivo y reconocido**. Ese patrón es el marco de referencia. Y conviene entender qué hace por dentro, porque ahí está la diferencia entre una auditoría seria y una checklist superficial.

1 · Define dimensiones

Establece **qué aspectos de la seguridad** se van a proteger. No es lo mismo proteger la confidencialidad de un plano técnico que garantizar la disponibilidad de una línea de producción: son objetivos distintos que se miden y se protegen de forma diferente.

2 · Catálogo de controles

Establece un **catálogo de medidas o controles agrupados por familias** para no dejar ningún frente descubierto. Cada familia responde a un área de riesgo específica y garantiza cobertura sistemática.

3 · Gradúa la exigencia

No pide lo mismo a un sistema cuya caída es una molestia que a uno cuya caída paraliza la facturación de toda la empresa. **La intensidad de las medidas es proporcional a la criticidad del sistema**.

Una auditoría bien hecha no es homogénea ni desproporcionada. Es **proporcional al riesgo**. El marco es lo que hace posible esa proporcionalidad.

El punto de partida operativo: análisis de riesgos y gap analysis

No se arranca por la tecnología. Se arranca por dos procedimientos que son la **columna vertebral de cualquier auditoría seria**. La primera pregunta que hace un buen auditor no es técnica, es de negocio: *«¿ante quién necesitáis demostrar qué?»*

Análisis de Riesgos

Antes de proteger nada, hay que saber qué se tiene: el **inventario de activos**, qué amenazas pesan sobre cada uno y qué impacto tendría sobre el negocio su fallo.
En España la metodología de referencia es **MAGERIT**, desarrollada por el Centro Criptológico Nacional y apoyada en la herramienta **PILAR**. Obliga a pensar en activos, amenazas y salvaguardas, y a poner un valor numérico al riesgo, no una intuición. Convierte «esto es importante» en «la indisponibilidad de este sistema me cuesta X con esta probabilidad».

Gap Analysis · Análisis Diferencial

Consiste en poner una al lado de la otra **dos fotografías**: dónde se está hoy, y dónde exige estar el marco aplicable. La distancia entre ambas —la brecha— es el plan de trabajo. Ni más ni menos.
El gap analysis transforma una norma abstracta en una lista concreta y priorizada: *«esto lo tengo, esto me falta, esto lo tengo a medias»*. Es la **radiografía objetiva** del estado real frente al estándar.
El alcance varía según el objetivo: no es lo mismo prepararse para vender a una administración pública (ENS) que responder al cuestionario de una aseguradora o demostrar cumplimiento de NIS 2 a un cliente de automoción.

SECURIZABLE

El ENS como eje: anatomía de un marco por dentro

El **Esquema Nacional de Seguridad (ENS)**, regulado por el Real Decreto 311/2022, es el marco de referencia español. El Centro Criptológico Nacional ha anticipado que el ENS y sus perfiles de cumplimiento serán la **vía principal para acreditar NIS 2 en España**. Entender el ENS es, en buena medida, entender lo que se va a exigir.

SECURIZABLE

Los tres pasos del ENS

1 2 3

Paso 1 · Las cinco dimensiones DICAT

El ENS descompone la seguridad en cinco dimensiones valoradas por separado: **D**isponibilidad, **I**ntegridad, **C**onfidencialidad, **A**utenticidad y **T**razabilidad. En entornos fabriles, la dimensión reina suele ser la disponibilidad: lo que no puede permitirse es que la línea pare.

Paso 2 · Categorización del sistema

Cada sistema se valora en esas cinco dimensiones y, según el impacto de su fallo, se clasifica en una de tres categorías: **básica, media o alta**. Esto gradúa la exigencia: a mayor categoría, mayor número de medidas y mayor intensidad. Se evita tanto la desprotección como el sobrecoste.

Paso 3 · Las 73 medidas del Anexo II

El Anexo II del Real Decreto contiene **73 medidas** organizadas en tres marcos: el **organizativo** (4 medidas de gobierno), el **operacional** (~32 medidas de operación segura) y las **medidas de protección** (~37 medidas centradas en activos concretos).

Marco Organizativo

Cuatro medidas de gobierno: política de seguridad, normativa, procedimientos y autorización de recursos. El **«quién manda y con qué reglas»**.

Marco Operacional

~32 medidas que protegen la operación: planificación, control de accesos, explotación, servicios externalizados, continuidad y monitorización. El **«cómo se opera con seguridad en el día a día»**.

Medidas de Protección

~37 medidas centradas en activos concretos: instalaciones, personal, equipos, comunicaciones, soportes, aplicaciones, datos y servicios. El **«cómo se blinda cada pieza»**.

Organizativo, operacional, protección. Gobierno, operación, activos. **Si se entienden esos tres bloques, se entiende la lógica con la que se va a auditar cualquier empresa**, ya sea con ENS, ISO 27001 o NIS 2: todos comparten esa misma estructura de fondo.

SECURIZABLE

Los Cuatro Marcos de Ciberseguridad: Una Visión Comparada

El ENS no existe en el vacío. A su alrededor orbitan tres marcos internacionales que **comparten su filosofía de fondo pero cambian el enfoque**, el alcance y el público objetivo. Entender sus diferencias —y sus enormes solapamientos— es la clave para trabajar de forma eficiente sin multiplicar el esfuerzo auditor.

ENS — Real Decreto 311/2022

El marco de referencia obligatorio para la Administración Pública española y punto de entrada natural hacia NIS 2. Organiza las medidas en marcos aplicables según la categoría del sistema.

ISO 27001:2022 — Certificación Internacional

El equivalente certificable a escala global. Introduce el concepto de Sistema de Gestión de Seguridad de la Información (SGSI) con 93 controles y un ciclo de mejora continua: Planificar → Hacer → Verificar → Actuar.

NIST CSF 2.0 — Lenguaje de Dirección

No es certificable, pero es el mejor organizador estratégico disponible. Estructura la ciberseguridad en seis funciones — Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar— y eleva la seguridad al órgano de dirección.

IEC 62443 — Entornos OT e Industriales

El único estándar diseñado específicamente para sistemas de control industrial, SCADA y autómatas. Donde los otros tres piensan en la IT, éste piensa en OT: la disponibilidad y la seguridad del proceso físico mandan por encima de la confidencialidad.

Tres Marcos en Detalle: ISO 27001, NIST CSF 2.0 e IEC 62443

ISO 27001:2022 — El Certificado que Abre Puertas

La ISO 27001 no es un catálogo de requisitos que se cumple y se archiva. Es un **ciclo vivo de mejora continua** que una entidad acreditada certifica y revisa periódicamente. Sus 93 controles se agrupan en cuatro temas: organizativos, de personas, físicos y tecnológicos.

Para una empresa que exporta, licita con grandes corporaciones o opera en mercados europeos, el certificado ISO 27001 es una **tarjeta de presentación reconocida internacionalmente** que elimina barreras comerciales y genera confianza inmediata.

El solapamiento con NIS 2 es sustancial: según las consultoras especializadas, una entidad con ISO 27001 bien implantada ya ha completado entre el **65 y el 75 % del camino hacia NIS 2**. La inversión no se duplica; se aprovecha y se amplía.

NIST CSF 2.0 — El Lenguaje del Consejo de Administración

La versión 2.0 de 2024 incorporó una sexta función: **Gobernar**. No es un añadido cosmético. Refleja exactamente el mismo desplazamiento que impone NIS 2: llevar la responsabilidad de la seguridad al órgano de dirección, con rendición de cuentas explícita.

Las seis funciones —**Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar**— ofrecen un vocabulario ejecutivo de alto impacto. En seis verbos se puede describir dónde está la empresa hoy y hacia dónde debe ir, sin tecnicismos que alejan a los interlocutores de negocio.

Su principal fortaleza es la **fotografía inicial**: sirve para mapear el estado de madurez de la organización, priorizar inversiones y comunicar el plan de acción al consejo con claridad meridiana.

IEC 62443 — La Capa que Protege la Planta

Los tres marcos anteriores nacieron pensando en sistemas de información de oficina. La IEC 62443 está diseñada para el mundo OT. Introduce dos conceptos metodológicos de alto valor:

- **Zonas y conductos**: en lugar de una red plana donde todo se comunica con todo, la planta se divide en zonas según su criticidad y se controlan rigurosamente los conductos de comunicación entre ellas.
- **Niveles de seguridad (SL-1 a SL-4)**: define la capacidad de resistencia requerida en cada zona según la amenaza que debe soportar. No se protege igual la zona que controla un horno crítico que la red de sensores ambientales.

Este enfoque permite segmentar y dimensionar la inversión con **criterio técnico y proporcional**, no por intuición.

ISO 27001

Certificación internacional + 65-75% de solapamiento con NIS 2

IEC 62443

Zonas, conductos y niveles SL para entornos industriales OT

NIST CSF 2.0

Lenguaje ejecutivo en 6 funciones para dirección y consejo

ENS

Puente hacia lo público y marco de entrada para NIS 2 en España

SECURIZABLE

La Auditoría como Obligación Jurídica: Doctrina Judicial y Tipos de Verificación

La seguridad no se agota en adoptar medidas: los tribunales españoles exigen demostrar que funcionan. Esto convierte a la auditoría en un instrumento jurídico, no en una opción de gestión.

Lo que dicen los tribunales

La **Audiencia Nacional** estableció que el deber de seguridad obliga a verificar la eficacia de las medidas adoptadas, mencionando expresamente las auditorías y las pruebas técnicas como el medio idóneo para hacerlo.
El **Tribunal Supremo** (2022) lo ordenó con precisión: la seguridad es una obligación de medios en **dos niveles**:

1. **Primer nivel:** adoptar medidas adecuadas.
2. **Segundo nivel:** implantarlas, mantenerlas activas y comprobar con diligencia razonable que funcionan.

Quien cumple solo el primer nivel e ignora el segundo, **incumple**. El instrumento que acredita ese segundo nivel es, según el propio criterio judicial, la auditoría.

La AEPD ha advertido expresamente: las evidencias deben ser **previas al incidente**. Un informe improvisado tras el fallo no subsana el incumplimiento.

Cinco tipos de auditoría: cuál responde a cada pregunta

Auditoría de Cumplimiento

Verifica la conformidad con un marco normativo concreto: ENS, ISO 27001, NIS 2. Responde a la pregunta *¿cumplimos lo que nos exige la norma o el cliente?*

Auditoría Técnica de Seguridad

Revisa el estado real de la infraestructura: configuraciones, gestión de accesos, segmentación de redes. Va más allá del papel y examina la realidad operativa.

Test de Intrusión (Pentest)

Simula un ataque real controlado para medir hasta dónde podría penetrar un adversario. Es la **prueba de eficacia** a la que se refieren expresamente los tribunales al exigir verificación.

Auditoría Específica de OT / SCADA

Centrada en sistemas industriales, autómatas y entornos SCADA. No se audita con las mismas metodologías ni criterios que un entorno de oficina; requiere especialización en tecnología operacional.

Análisis Diferencial (Gap Analysis)

El punto de partida habitual: mide la distancia entre el estado actual y los requisitos exigidos por la norma o el cliente. La fotografía que determina por dónde empezar.

La elección del tipo de auditoría debe responder a la pregunta que la organización tiene delante: **¿demostrar cumplimiento?** → auditoría de cumplimiento. **¿Resistiría un ataque?** → pentest. **¿Proteger la planta industrial?** → auditoría OT. **¿Saber por dónde empezar?** → gap analysis. No se necesitan todas a la vez: se necesita la adecuada. Esa es la conversación que debe tenerse antes de auditar nada.

SECURIZABLE

Los Controles Mínimos que Ninguna Auditoría Industrial Puede Ignorar

De las 73 medidas del ENS o las 93 de la ISO, existe un núcleo que coincide en todos los marcos, que exige NIS 2 y que pregunta el asegurador. Ese núcleo es lo innegociable. Y se ordena siempre igual: primero el gobierno, después la operación, por último la protección de cada activo. Lo organizativo es lo primero que se mira en una auditoría... y lo último que la mayoría de empresas tiene en orden.

BLOQUE 5 · CONTROLES MÍNIMOS

SECURIZABLE

Una Advertencia

Cuando una empresa piensa en ciberseguridad, casi siempre piensa en **tecnología**: cortafuegos, antivirus, copias de seguridad. Es la respuesta instintiva, y es la respuesta equivocada como punto de partida.
Cuando un auditor entra, lo primero que pide **no es tecnología**. Es **gobierno**:

- ¿Quién manda en esto?
- ¿Qué política habéis aprobado?
- ¿Dónde está el análisis de riesgos firmado?

Recordad la estructura del ENS: **organizativo → operacional → protección**. Ese orden no es casual. Una empresa puede tener controles técnicos aceptables y, aun así, **suspender la auditoría en gobernanza**. Porque sin gobierno, los controles técnicos son medidas sueltas sin nadie que responda de ellas, sin nadie que las revise, sin nadie que las actualice.

El error más costoso

Invertir en tecnología antes de tener el gobierno en orden es construir sobre arena. El auditor, el asegurador y el regulador de NIS 2 buscan primero la evidencia de que **alguien responde** de la seguridad. Sin esa evidencia, ningún firewall salva la auditoría.
Vamos a recorrer los 15 controles mínimos en ese mismo orden: primero **quién manda**, luego **cómo se opera**, y por último **cómo se blinda cada pieza**.

SECURIZABLE

BLOQUE 1 DE 3 · MARCO ORGANIZATIVO

El Gobierno de la Seguridad: Lo Primero que se Mira

El bloque organizativo es el que más se descuida y más peso tiene en una auditoría. Ninguno de estos cuatro controles cuesta dinero en tecnología. Cuestan **decisión y documentación**. Y son, sistemáticamente, los que más empresas suspenden.

1

Política de seguridad aprobada por la dirección

No un documento que redactó el informático y guardó en una carpeta. Un documento **aprobado y firmado por el órgano de dirección** que fija el compromiso, el alcance y las responsabilidades. NIS 2 hace responsable personalmente al consejo: esta política firmada es la primera evidencia de diligencia debida. Sin ella, ante un incidente, la dirección no puede demostrar que gobernaba el riesgo.

2

Análisis de riesgos vivo

No hecho una vez en 2021 y olvidado. Un análisis —con MAGERIT o metodología equivalente— que identifique activos críticos, amenazas e impacto sobre el negocio, y que se **revise periódicamente**. Sin análisis de riesgos, el resto de medidas es una colección desordenada sin criterio de prioridad.

3

Roles y responsabilidades definidos

Quién es el responsable de la seguridad de la información, quién responde de cada sistema, quién decide en un incidente. NIS 2 y el ENS exigen designar formalmente un responsable de seguridad. En una pyme no hace falta un departamento: hace falta que esté **claro y por escrito** quién responde de qué.

4

Normativa y procedimientos escritos

Las reglas del día a día puestas por escrito: política de contraseñas, uso de dispositivos, gestión de accesos, qué se hace ante un correo sospechoso. Una norma que solo está en la cabeza de una persona no es una norma: es una costumbre que se rompe el día que esa persona está de vacaciones.

⚠ Fijaos en una cosa: ninguno de estos cuatro controles cuesta dinero en tecnología. Cuestan **decisión y documentación**. Y son, sistemáticamente, los que más empresas suspenden en auditoría.

SECURIZABLE

BLOQUE 2 DE 3 · MARCO OPERACIONAL

Cómo se Opera con Seguridad en el Día a Día

El bloque operacional contiene los controles que más suenan —y no por casualidad: son exactamente los que os va a preguntar una aseguradora en su cuestionario y los que exige NIS 2 en su artículo 21.

5 · Control de accesos y mínimo privilegio

Cada persona accede solo a lo que necesita. Sin cuentas compartidas, sin un usuario 'administrador' para cinco personas. Cuando alguien se va, su acceso se revoca **el mismo día**. Uno de los hallazgos más frecuentes: credenciales activas de personas que se fueron hace años.

6 · Autenticación multifactor (MFA)

El control con mejor relación entre lo poco que cuesta y lo mucho que evita. Obligatorio en correo, VPN, accesos de administrador y especialmente en el **acceso remoto a la planta**. El cuestionario del asegurador lo pregunta literalmente. Una contraseña robada sin segundo factor es una puerta abierta.

7 · Gestión de vulnerabilidades y parches

Política clara: vulnerabilidad crítica con exploit conocido → parche en máximo **30 días**. En OT, si no se puede parchear, se aplica el **control compensatorio**: aislar el activo y controlar el tráfico. El auditor no espera lo imposible; espera que el riesgo no eliminable esté **identificado y compensado**.

8 · Monitorización y registro de actividad

Sin registros, no se detecta el ataque mientras ocurre ni se reconstruye qué pasó. Una brecha en la cadena de suministro tarda de media **254 días en detectarse**. La diferencia está en si hay monitorización. Para una pyme existen servicios gestionados MDR que dan vigilancia 24/7 sin construirlo en casa.

9 · Continuidad y copias probadas

Regla **3-2-1**: tres copias, dos soportes, una aislada y protegida contra cifrado. Pero sobre todo: **probar la restauración periódicamente**. Una copia que nunca se ha probado no es una copia, es una suposición. El asegurador pregunta en cuánto tiempo recuperaríais la red tras un ataque.

10 · Plan de respuesta a incidentes ensayado

Quién hace qué, a quién se llama, qué se desconecta, cómo se comunica. Plazos NIS 2: **alerta a las 24 h, informe a las 72 h, informe final en un mes**. Un plan que nunca se ha ensayado con un simulacro no es un plan: es una intención escrita. El día del incidente no hay tiempo de improvisar.

SECURIZABLE

BLOQUE 3 DE 3 · MEDIDAS DE PROTECCIÓN

Blindar Cada Activo: Donde la Realidad Industrial se Separa

El tercer bloque son las medidas de protección: blindar cada activo concreto según lo crítico que sea. Aquí es donde la realidad industrial se separa radicalmente de la de una oficina.

11 · Segmentación IT/OT — El control rey

La red de oficinas y la red de producción **no pueden ser la misma red**. Si un phishing en administración puede alcanzar el autómata de la línea, un solo fallo separa al negocio del desastre. El asegurador lo pregunta directamente. Aplicad IEC 62443: **zonas por criticidad y conductos controlados** entre ellas. La segmentación convierte un incidente en una molestia localizada en lugar de en una parada total de planta.

12 · Protección de equipos: EDR/XDR

No el antivirus tradicional, que solo reconoce amenazas conocidas. Soluciones que detectan **comportamientos anómalos** y permiten responder. El asegurador pregunta si está en todos los dispositivos, en algunos o en ninguno. La respuesta "en algunos" es señal de alarma. Incluye los portátiles de la dirección: objetivo preferente del fraude del CEO.

13 · Cifrado de información sensible

Planos, fórmulas, datos de clientes: cifrados tanto en reposo como en tránsito. Si os roban un portátil o interceptan una comunicación, el cifrado convierte una fuga grave en un susto controlable. Es además lo que el RGPD valora como medida de diligencia cuando hay datos personales implicados.

14 · Seguridad de la cadena de suministro

Identificar a los proveedores críticos, evaluar su seguridad, exigir **cláusulas contractuales** y verificar —no solo confiar en su palabra—. Es una de las grandes novedades del artículo 21 de NIS 2 y uno de los controles que más rápido se está incorporando a las auditorías industriales. La confianza implícita ya no es una postura válida.

15 · Protección física y factor humano

Los dos extremos que con más frecuencia se olvidan. El **físico**: quién entra a la nave, quién accede al armario de servidores, quién conecta un USB a un equipo de planta. El **humano**: formación periódica con simulacros de phishing, porque el engaño a una persona sigue siendo el vector de entrada más rentable. NIS 2 exige formación e incluye expresamente a la dirección.

La IEC 62443 divide la planta en **zonas según criticidad** y controla los conductos entre ellas. Aplicar este modelo es lo que convierte un incidente en una molestia contenida, no en una parada de planta.

SECURIZABLE

El Mínimo Común Denominador: 15 Controles, 3 Bloques, 1 objetivo

Primera idea clave: todos miran lo mismo

Estos 15 controles **son los mismos** mire quien mire. El auditor de NIS 2 los busca. El cuestionario del asegurador los pregunta. El ENS los recoge en sus tres marcos. La ISO en sus cuatro temas. No es casualidad: todos beben del mismo consenso sobre qué funciona.
Por eso **una sola auditoría bien hecha os vale para los tres frentes**: es el mínimo común denominador de estar seguro, ser *compliant* y ser asegurable. No son tres mundos distintos; son tres perspectivas del mismo núcleo.

NIS 2

Art. 21 · Notificación · Responsabilidad directiva

ENS

Organizativo · Operacional · Protección

Asegurador

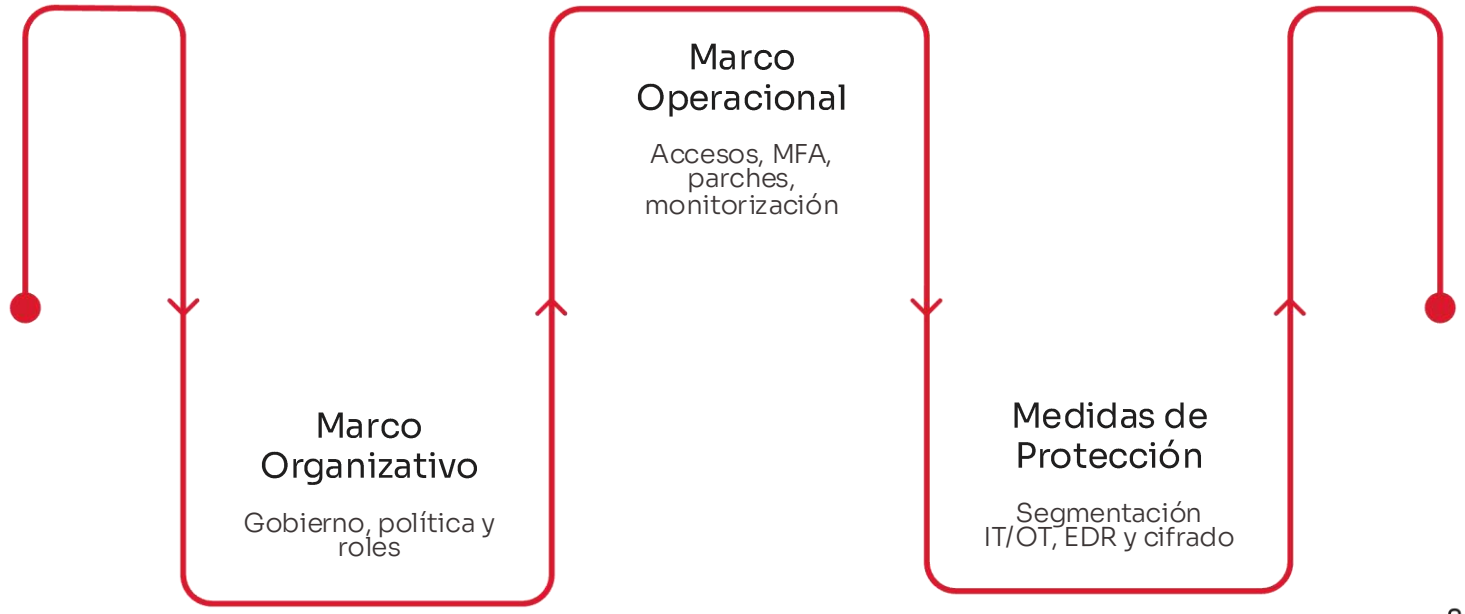
Cuestionario de riesgo · MFA · Parches · Backups

Segunda idea clave: implantado, documentado y verificado

Cada uno de estos 15 controles tiene que estar **implantado Y documentado**. Volvemos al principio de la jornada: la responsabilidad proactiva.

- No basta con tener MFA → hay que poder enseñar el registro
- No basta con tener copias → hay que enseñar la última prueba de restauración
- No basta con segmentar → hay que poder mostrar el esquema de red

Porque ante un auditor, un cliente o una aseguradora, **el control que no se puede demostrar es como si no existiera**.
Este es el mensaje que se lleva toda la ponencia: la ciberseguridad industrial no es solo hacer las cosas bien. Es poder demostrar que se hacen bien, de forma continua y trazable.



Los 15 controles no son una lista arbitraria: son la arquitectura de una seguridad industrial demostrable. El orden importa tanto como el contenido.

SECURIZABLE

El Ciberseguro: La Última Línea de Defensa

El ciberseguro no sustituye la seguridad: la presupone.

SEGURIDAD · CUMPLIMIENTO · COBERTURA

SECURIZABLE

Por qué el ciberseguro ya no es opcional

Volvamos por última vez a Jaguar Land Rover. **300 millones de libras de pérdidas. Seis semanas de fábricas paradas. Cientos de proveedores al borde de la quiebra.** Y un detalle que ahora cobra todo el sentido: no tenían ciberseguro. Toda la factura, íntegra, a su cuenta de resultados.
¿Qué habría cambiado con una póliza adecuada? Gastos forenses cubiertos, defensa jurídica pagada, gestión de crisis por especialistas, y —según el tipo de cobertura— buena parte de la pérdida de beneficios por la parada compensada. La diferencia entre arrastrar a media docena de proveedores a la quiebra y resistir el golpe.

Por eso el ciberseguro no es un lujo ni un papel más. Es la **última línea de defensa**: lo que actúa cuando todo lo anterior ha fallado. Porque el riesgo cero no existe.

¿Qué cubre una póliza adecuada?

- Gastos forenses e investigación del incidente
- Defensa jurídica y gestión de reclamaciones
- Gestión de crisis por especialistas externos
- Pérdida de beneficios por parada operativa
- Notificación a afectados y reguladores
- Daños a terceros derivados de la brecha
- Restauración de Datos y sistemas

⚠ El ciberseguro de 2026 no se parece en nada al de hace cinco años. Conviene entender por qué, para no llevarse una sorpresa el peor día.

SECURIZABLE

El dato incómodo: solo el 17% de las pymes españolas tiene ciberseguro

En julio de 2025, **ESET** publicó una cifra que debería hacernos reflexionar: **casi la mitad de las pymes españolas con menos de 10 millones de facturación sufrió algún incidente de ciberseguridad en 2024**. El riesgo golpeó a una de cada dos empresas. Y, sin embargo, solo una de cada seis cuenta con un ciberseguro. Un desajuste difícil de ignorar.

¿Por qué ese desajuste?

No es una cuestión de precio. Es una cuestión de **percepción**. El ciberriesgo no se ve, no ocupa espacio en la nave. Lo que no se ve no se siente como amenaza. Aseguramos el incendio, el robo, el vehículo —riesgos que imaginamos— pero el ciberataque se percibe como algo lejano, que les pasa a otros. **Ahí está el error.**

La realidad cuando el riesgo se materializa

Cuando ese riesgo invisible se vuelve real, el impacto es de los más costosos que existen: paralización operativa, pérdida de datos, sanciones regulatorias y daño reputacional. No contratar un ciberseguro no elimina el riesgo. **Solo significa que, el día que ocurra, lo asumiréis íntegramente vosotros.**

17%

Con ciberseguro

Pymes españolas que han transferido el riesgo a una aseguradora.

~50%

Sufrieron un incidente

De las pymes con menos de 10M€ en 2024, una de cada dos fue afectada.

1 de 6

Se protegen

Por cada seis empresas expuestas, solo una ha tomado medidas contractuales.

Un ciberseguro es, simplemente, **un instrumento para transferir riesgo**: trasladar a la aseguradora una parte del golpe que vuestra empresa no podría absorber sola. No contratarlo no elimina el riesgo; solo significa que, si ocurre, lo asumís vosotros íntegramente.

SECURIZABLE

La fábrica no entra en el producto estándar

Este es el argumento que muy pocos conocen —y que está escrito en la letra pequeña de los cuestionarios de suscripción de las grandes aseguradoras.

El producto estándar te excluye

El seguro de cotización rápida —el que rellenas online y te dan precio en minutos— **excluye expresamente a la fabricación y a las empresas que usan sistemas de automatización industrial: ICS, DCS, SCADA**. Está escrito con todas las letras. Una fábrica del metal con OT no cabe en el seguro "de catálogo".

Cotización manual y estudio individual

Las empresas industriales deben ir a cotización manual, a un estudio individual del riesgo, y rellenar un **cuestionario adicional específico para tecnología operativa**. No es un formulario más: es un examen técnico exhaustivo que evalúa específicamente vuestra OT.

Lo que esto nos dice

Las propias aseguradoras consideran que **una fábrica con OT es un riesgo distinto y superior** al de una oficina. No os meten en la misma categoría que a una asesoría o una tienda online. Una parada de planta es un siniestro de otra magnitud. Por eso el ciberseguro para vosotros no es "rellenar un formulario"; es someteros a un examen técnico de fondo.

SECURIZABLE

Lo que el cuestionario pregunta de verdad

SECURIZABLE

A continuación, lo que ese examen pregunta palabra por palabra —para que veáis hasta qué punto coincide con una auditoría técnica completa.

1

Acceso remoto a la OT

¿Se usa siempre VPN segura? ¿Se exige doble factor para **todos** los accesos remotos? ¿El acceso es controlado y temporal? Cada "no" o "parcialmente" es un punto de exposición que la aseguradora valorará negativamente.

2

Parcheo y soporte

¿Todos sus sistemas tienen soporte del fabricante y se actualizan en un plazo máximo de **30 días**? Y si no: ¿los sistemas sin soporte están aislados de la red, tienen parcheo virtual o soporte extendido? El control compensatorio es exactamente el que os describíamos antes.

3

Copias de seguridad

¿Copias al menos cada 15 días en soportes desconectados o en nube con doble factor? Y aún más: ¿esas copias son **inmutables** —no se pueden alterar ni borrar desde los sistemas originales? Aquí está la diferencia entre recuperarse de un ransomware o rendirse.

4

Endpoints y segmentación

¿Qué solución de seguridad tienen desplegada en sus dispositivos OT: en **todos, en algunos, o en ninguno**? ¿Existe separación efectiva entre red IT y red OT, y cómo se consigue? Dos de las preguntas con mayor peso en la valoración del riesgo.

5

Para empresas más grandes

El cuestionario sube el nivel: pide **pruebas de penetración de la red OT**, certificación **ISO 27001**, y un análisis de impacto en el negocio con tiempos de recuperación concretos: ¿menos de 8 horas? ¿Menos de 24? ¿Menos de una semana?

¿Os dais cuenta? Son exactamente las mismas preguntas que haría una auditoría técnica. MFA, parcheo a 30 días, copias inmutables, EDR, segmentación IT/OT, tiempos de recuperación. El cuestionario del asegurador es, en la práctica, **una auditoría que tenéis que rellenar y firmar vosotros mismos**.

El ciberseguro: la última línea, pero solo si eres elegible

El ciberseguro no sustituye a la seguridad: **la presupone**. No basta con contratar una póliza y pagar la prima. Las aseguradoras no solo te examinan al entrar mediante un cuestionario inicial sino que algunas pólizas condicionan la cobertura a que cumplas la normativa y las buenas prácticas del sector **durante toda la vida del contrato**. Ser compliant deja de ser una opción estratégica: se convierte en la condición para cobrar cuando más lo necesitas.

Clave 1

Lo que respondiste al entrar tiene que ser verdad. La inexactitud en el cuestionario puede anular la cobertura el día del siniestro.

Clave 2

El condicionado de la póliza puede exigir que mantengas medidas de seguridad y cumplimiento normativo de forma continua.

Clave 3

Una auditoría bien hecha resuelve los tres frentes a la vez: protección real, cumplimiento normativo y elegibilidad para cobrar.

SECURIZABLE

CLAVE 1

Lo que firmaste al entrar: la veracidad del cuestionario

La declaración que casi nadie lee

En los cuestionarios de contratación, al final, en la declaración que hay que firmar, se recoge una cláusula que cambia todo. Dice, textualmente: la información debe ser veraz, y **"la falsedad o inexactitud en el cuestionario puede desencadenar en una falta de cobertura"**.
Parece razonable. Nadie debería mentir a su aseguradora. Pero el problema no es la mentira deliberada: es la inexactitud no intencionada, el control que creías implantado y que, bajo presión o por un descuido, no lo estaba de forma completa.

El peor escenario posible

Imaginad que en el cuestionario respondisteis que teníais doble factor de autenticación en todos los accesos remotos a la planta. Llega el ataque, y la investigación forense —que paga la propia aseguradora— descubre que el atacante entró precisamente por un acceso remoto que **no tenía ese doble factor**.
¿Qué ocurre? Que la aseguradora invoca la inexactitud del cuestionario y **no paga**. Pagasteis la prima durante años, sufristeis el ataque, y no cobráis. Sin fraude, sin mala fe, pero sin cobertura.

La conclusión práctica

Lo que respondisteis al entrar tiene que ser verdad en el momento del siniestro, no solo en el momento de firmarlo. Cada control declarado debe poder acreditarse. Pero hay un segundo nivel, todavía más exigente.

SECURIZABLE

CLAVE 2

Lo que tienes que mantener: el condicionado que casi nadie se lee

Una cosa es el cuestionario inicial, y otra distinta es el **condicionado de la póliza**: la letra pequeña que manda el día del siniestro. En pólizas reales del mercado español existen dos cláusulas que cambian radicalmente las reglas del juego.

Cláusula 1: La cobertura no llega a activarse

La primera dice, en esencia, que **las coberturas de la póliza no entran en vigor si no se han implantado las medidas de seguridad indicadas**. No es una penalización por mentir. Es que la cobertura, sencillamente, no se activa si esas medidas no están puestas. Aunque hayas pagado la prima religiosamente durante años.

Cláusula 2: Tres fuentes de obligación simultánea

La segunda establece que la póliza **no otorgará cobertura alguna** cuando el asegurado no haya adoptado y mantenido de manera adecuada las medidas requeridas por tres fuentes: la propia **póliza**, la **normativa aplicable**, y las **prácticas reconocidas del sector**.

Implicación directa para empresas sujetas a NIS 2: La expresión "normativa aplicable" significa que si no sois compliant con NIS 2, podríais quedaros sin cobertura. No por haber mentido en el cuestionario, sino porque la propia póliza exige, como condición para pagar, que cumpláis la normativa que os aplica. El incumplimiento normativo se convierte directamente en una **causa de exclusión** del seguro.

Con el rigor que esta audiencia merece: esta redacción tan exigente se ha encontrado, por ahora, en una póliza concreta, no en todas. No es el estándar universal del mercado hoy. Pero ya existe. Y cuando una compañía introduce una cláusula que le funciona para acotar su riesgo, el resto del mercado tiende a seguirla. **Hoy es una póliza; mañana puede ser la norma.**

SECURIZABLE

CLAVE 3

La auditoría: la herramienta que resuelve los tres frentes

Aquí converge todo. Fijémonos en la cadena lógica que se ha cerrado: para ser asegurables, hay que demostrar controles. Para que la póliza pague, esos controles tienen que estar **realmente implantados y mantenidos**. Y, según hacia dónde va el mercado, hay que además **cumplir la normativa** —NIS 2— y las buenas prácticas del sector. La seguridad, el cumplimiento y el seguro han dejado de ser tres cosas separadas. Son **la misma cosa, mirada desde tres ángulos**.

Os convence a vosotros mismos

Una auditoría bien hecha os dice, con honestidad, si estáis razonablemente protegidos. No para el cuestionario, sino para la realidad operativa de vuestra empresa. Es la única forma de saber si los controles que declaráis realmente funcionan.

Os permite demostrar cumplimiento

Ante clientes, ante reguladores y ante la propia aseguradora, la auditoría genera la evidencia documentada de que cumplís con NIS 2 y con las prácticas del sector. Es el argumento frente a cualquier cuestionamiento.

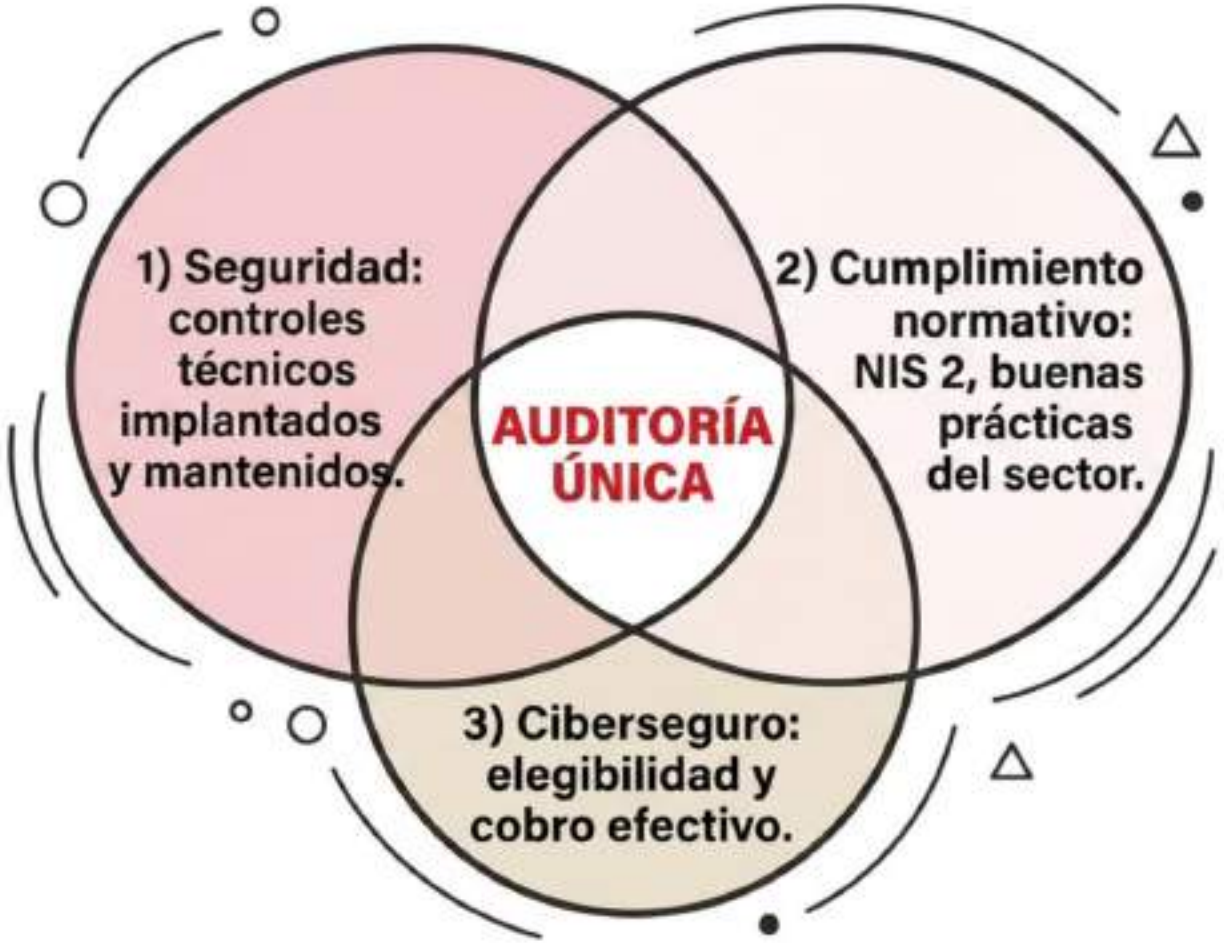
Os permite cobrar el seguro

No como requisito formal para obtener la póliza —ninguna aseguradora exige presentar un informe de auditoría para contratarla— sino como vuestra única forma de saber, **antes de necesitarlo**, que cumpliríais las condiciones del condicionado el día del siniestro.

El cuestionario de contratación pregunta exactamente lo mismo que una auditoría, y el condicionado os exige cumplir de forma continua y demostrable. La auditoría no es un requisito formal del seguro: es **vuestra única forma de saber si estáis en condiciones de cobrar antes de necesitarlo**.

SECURIZABLE

El cierre de la cadena: seguridad, cumplimiento y seguro son lo mismo



"La seguridad, el cumplimiento y el seguro han dejado de ser tres cosas separadas. Son la misma cosa, mirada desde tres ángulos. Y la auditoría es la herramienta que os permite gestionarlas con una sola acción."

SECURIZABLE

BLOQUE 7

Cuando ser víctima no te exime: la responsabilidad que no se puede transferir

Un tribunal español ya ha condenado a una empresa que sufrió un ciberataque —no por sufrirlo, sino por no reaccionar con diligencia. La sentencia cambia las reglas del juego para cualquier administrador.

El caso: Gamboa Automoción · Tribunal Supremo, Sentencia 136/2025

Unos delincuentes suplantaron por correo electrónico a un empleado del departamento comercial de un concesionario de automóviles. Haciéndose pasar por él, indicaron a una empresa asociada una cuenta bancaria fraudulenta para un pago. El segundo concesionario, confiado, transfirió **más de 32.000 euros** a los delincuentes. Hasta aquí, una estafa como tantas. Pero lo que ocurrió después lo cambia todo.

El detalle que lo cambió todo

Gamboa, la empresa cuyo correo fue suplantado, **se había enterado la mañana anterior** de que estaba ocurriendo exactamente lo mismo con otro concesionario. Sabía que había una brecha activa. Y, a pesar de ello, **no avisó** a los demás con los que tenía operaciones abiertas. No levantó el teléfono para decir: "Cuidado, verificad las cuentas antes de pagar."

La resolución del Supremo

El Tribunal Supremo confirmó la condena a Gamboa como **responsable civil subsidiaria** del dinero defraudado. La empresa que fue suplantada acabó respondiendo del perjuicio que sufrió un tercero. No por sufrir el ataque: por la **omisión posterior**, por no actuar con diligencia debida una vez que conocía el incidente.

SECURIZABLE

La doctrina que todo administrador debe conocer

Dos afirmaciones del Supremo que conviene retener

La sentencia contiene dos razonamientos de fondo que van mucho más allá del caso concreto:

1 El sistema informático es parte del "establecimiento"

Vuestros servidores, vuestro correo, vuestros sistemas OT —a efectos de responsabilidad legal— son tan parte de vuestra empresa como vuestra nave industrial. Lo que ocurre en ellos os pertenece.

2 La "infracción" no exige incumplir un reglamento numerado

Basta con no haber actuado con el cuidado que era exigible. Cualquier violación del deber objetivo de cuidado que cause daños a terceros puede generar responsabilidad, aunque no exista una norma técnica específica que se haya infringido.

Lo que esto significa para vuestra fábrica

La doctrina que sienta el Supremo es demoledora en su sencillez: **ser víctima de un ciberataque ya no os exime de responsabilidad** si se demuestra que actuasteis con pasividad, sin los controles preventivos mínimos, o sin reaccionar con diligencia cuando supisteis lo que pasaba.
Fijaos cómo encaja con todo lo visto durante la jornada:

- Si tenéis un análisis de riesgos, controles documentados, un plan de respuesta ensayado y avisáis a tiempo → **estáis demostrando diligencia**
- Si no tenéis nada de eso y, además, cuando llega el incidente no reaccionáis → **estáis en la posición de Gamboa**

⊗ La diferencia entre una cosa y otra no es la suerte. Es la **diligencia demostrable**. No basta con ser diligente: hay que poder probarlo.

SECURIZABLE

Dos pólizas distintas para dos riesgos distintos

Si la seguridad y el cumplimiento no se pueden externalizar —porque la responsabilidad es vuestra e indelegable—, lo que sí podéis hacer es **contener las consecuencias económicas** cuando, pese a todo, algo sale mal. Para ello existen dos pólizas complementarias que muchas empresas confunden.

Ciberseguro · Protege a la empresa

Cubre el daño a la **sociedad**: recuperación de sistemas, investigación forense, pérdida de beneficios por parada operativa, gestión de crisis, notificación a afectados, reclamaciones de terceros por la brecha de datos.

Límite importante: no protege el patrimonio personal del administrador frente a reclamaciones por su gestión. La póliza sostiene a la empresa, no a quien la dirige.

D&O · Protege al directivo

El seguro de Directors & Officers cubre al **directivo como persona**: gastos de defensa jurídica si le reclaman por su gestión, responsabilidades civiles derivadas de sus decisiones, costes de procedimientos. NIS 2 introduce responsabilidad para el órgano de dirección —sanciones, posible inhabilitación temporal—. Para ese riesgo personal existe el D&O.

Son complementarias: el ciberseguro contiene el golpe a la sociedad; el D&O contiene el golpe personal al administrador.

Ambas pólizas **valoran vuestra diligencia**. El D&O también pregunta cómo gobernáis el riesgo. La mejor defensa de un administrador ante una reclamación es demostrar que actuó como un "ordenado empresario": que se informó, aprobó medidas, supervisó y tenía la radiografía hecha. Las pólizas amortiguan el golpe económico, pero **la diligencia demostrable es lo que evita que el golpe llegue siquiera**.

Las tres capas de protección: ninguna sustituye a la anterior

Este es el mensaje que une todo lo trabajado durante la jornada. Tres capas de protección interdependientes, que funcionan en cascada y que todas arrancan del mismo punto de partida.

Capa 1 · Seguridad técnica

Reduce la **probabilidad** de que el incidente ocurra. Controles preventivos, segmentación IT/OT, MFA, parcheo, copias inmutables, EDR en OT. Es la primera y más importante línea. Sin ella, las otras dos no son suficientes.

Capa 2 · Cumplimiento y diligencia documentada

Reduce vuestra **responsabilidad** si el incidente ocurre. NIS 2, análisis de riesgos, planes de respuesta ensayados, evidencias documentadas. No basta con ser diligentes: hay que poder demostrarlo ante reguladores, tribunales y aseguradoras.

Capa 3 · Pólizas: ciberseguro y D&O

Contienen las **consecuencias económicas** cuando todo lo demás ha fallado. Para la empresa: el ciberseguro. Para el administrador personalmente: el D&O. Ambas exigen diligencia demostrable para que la cobertura sea efectiva.

Todo empieza en el mismo sitio: saber dónde estáis. La radiografía. Una auditoría bien hecha es la llave que abre las tres capas simultáneamente: os da la certeza técnica, sostiene el cumplimiento normativo y permite firmar el cuestionario del seguro con la verdad. Una sola inversión. Tres frentes resueltos.

SECURIZABLE

Gracias por su Atención

Contacto y Seguimiento

Para consultas sobre auditorías de seguridad , PDS o asesoramiento en pólizas ciber adaptadas a su sector.

Próximos Pasos

Evalúe su nivel actual de preparación, identifique gaps críticos y priorice las medidas de protección más urgentes para su organización.

Securizable : beatrizcarratala@securizable.es / juanremoli@securizable.es

+34 96 141 07 97

www.securizable.es