GUÍA PRÁCTICA 2026

IA y Ciberseguridad para la empresa española.

¿Por dónde empezar? ¿Qué exige NIS2? ¿Cuándo tiene sentido el servidor propio?

Elaborada por el equipo técnico de TOWINIA para directivos y responsables de tecnología. Sin tecnicismos. Con criterios prácticos y casos reales del mercado español.

TOWINIA · TYBSI SL · Zamora, España onpremise@towinia.es · towinia.es

CONTENIDOS

01

Por qué la IA genérica no es suficiente para su empresa.

ChatGPT, Copilot, Gemini — potentes, sí. Pero no saben nada de usted.

EL PROBLEMA DE FONDO

Cuando su empresa usa un servicio de inteligencia artificial en la nube pública, está cediendo algo más que datos: está cediendo el contexto de su negocio. En primer lugar, sus documentos internos, sus contratos y los datos de sus clientes se procesan en servidores ubicados fuera de España — frecuentemente en Estados Unidos o Irlanda — bajo condiciones de uso que el proveedor puede cambiar en cualquier momento. Además, en muchos casos, esa información contribuye al entrenamiento de los modelos públicos de terceros.

Por otro lado, la IA genérica no conoce su empresa. No sabe cómo se llaman sus productos, no aplica sus políticas y puede inventar información que parece correcta pero no lo es. En consecuencia, cada respuesta hay que verificarla manualmente, lo que elimina gran parte del ahorro de tiempo que prometía la herramienta.

LOS TRES PROBLEMAS REALES

Soberanía de datos

Sus datos estratégicos salen de su perímetro y quedan bajo jurisdicción extranjera. Por tanto, cualquier cambio en los términos del servicio puede impactar su operativa sin previo aviso.

Privacidad normativa

El RGPD exige que el tratamiento de datos personales se realice bajo condiciones controladas y documentadas. Sin embargo, la mayoría de servicios cloud americanos no cumplen de forma demostrable con el estándar europeo.

Falta de especialización

Una IA entrenada con internet no conoce su sector ni sus procesos. En consecuencia, produce respuestas genéricas que requieren validación manual y no aportan valor real.

La alternativa soberana

Una IA fine-tuned con los datos reales de su empresa, desplegada en infraestructura española que usted controla, no comparte ninguno de estos problemas. Sus datos no salen de su perímetro, el modelo conoce su empresa en profundidad y el cumplimiento normativo es demostrable ante cualquier auditor.

02

Los 5 errores más comunes al adoptar IA en una PYME española.

Evitarlos puede ahorrarle meses de trabajo y decenas de miles de euros.

ERROR 01

Empezar con el modelo equivocado

Muchas empresas adoptan el modelo más conocido del mercado sin preguntarse si es el adecuado para su caso de uso. En primer lugar, un modelo de propósito general raramente es el más eficiente para una tarea específica. Por ello, antes de elegir herramienta, defina con precisión qué problema quiere resolver.

ERROR 02

No definir dónde viven los datos

Adoptar IA sin preguntarse dónde se almacenan y procesan los datos es el error más costoso. Asimismo, muchas empresas descubren tarde que su información sensible ha estado procesándose en jurisdicciones extranjeras sin que nadie lo autorizara. Exija siempre una respuesta documentada a esta pregunta.

ERROR 03

Infravalorar el fine-tuning

Un modelo genérico sin fine-tuning produce resultados genéricos. Sin embargo, el fine-tuning con los datos reales de su empresa puede convertir una herramienta mediocre en un activo diferencial. Por tanto, contemple esta inversión en el presupuesto inicial del proyecto.

ERROR 04

Ignorar NIS2 hasta el último momento

La Directiva NIS2 ya está en vigor. En consecuencia, las empresas de sectores afectados que no hayan iniciado el proceso de cumplimiento se enfrentan a inspecciones con expediente vacío. Además, prepararse a última hora multiplica el coste y el riesgo del proceso.

ERROR 05

No tener plan de continuidad para la IA

Si la IA se convierte en parte crítica de sus operaciones, una caída del servicio tiene impacto directo en su negocio. Por ello, antes de desplegar, defina qué ocurre si el sistema no está disponible y qué nivel de SLA necesita realmente.

03

Servidor propio (on premise) vs SaaS. ¿Cuándo tiene sentido cada opción?

No hay una respuesta única. Depende de sus datos, su sector y su volumen.

TABLA COMPARATIVA

Criterio	Towin Box — On Premise	Towinia Cloud — SaaS
Sus datos	Nunca salen de su edificio	En CPD español, aislados por cliente
Inversión inicial	Alta — hardware + instalación	Ninguna
Coste mensual	Solo soporte y mantenimiento	Cuota mensual predecible
Tiempo de arranque	2–3 semanas	3–7 días laborables
Sin internet	Sí — funciona offline	No — requiere conectividad
Escalabilidad	Limitada al hardware instalado	Inmediata, sin planificar
Cumplimiento normativo	Máximo — control físico total	Alto — CPD español certificado
Ideal para	Legal, sanidad, gobierno, industria	Empezar rápido, equipos distribuidos

LA REGLA PRÁCTICA

Elige ON PREMISE si…

— Sus datos no pueden salir de su edificio bajo ningún concepto

— Opera en sanidad, legal, defensa, gobierno o industria regulada

— Necesita que el sistema funcione sin conexión a internet

— Prefiere propiedad permanente sobre suscripción mensual

Elige SAAS si…

— Quiere empezar en días sin inversión en hardware

— Su equipo trabaja desde distintas ubicaciones

— Prefiere coste mensual predecible sin inversión inicial

— Quiere probar antes de comprometerse al hardware propio

04

Qué exige la Directiva NIS2.

Las sanciones alcanzan el 2% de la facturación global. Ya está en vigor.

¿QUÉ ES NIS2?

La Directiva NIS2 (Network and Information Security 2) entró en vigor en octubre de 2024. En concreto, obliga a las empresas de sectores esenciales o importantes a demostrar controles técnicos activos, gestión documentada de riesgos y capacidad de notificación ante incidentes en menos de 24 horas. Además, los directivos pueden incurrir en responsabilidad personal en caso de incumplimiento grave.

SECTORES OBLIGADOS

Sector	Qué actividades cubre
Energía	Electricidad, gas, petróleo, calefacción urbana
Transporte	Aéreo, ferroviario, marítimo, terrestre
Banca y finanzas	Entidades de crédito, infraestructuras de mercado
Sanidad	Hospitales, laboratorios, fabricantes de dispositivos médicos
Agua	Suministro de agua potable y aguas residuales
Infraestructura digital	IXPs, DNS, TLD, CPDs, servicios cloud
Administración pública	Central y regional (excl. defensa)
Fabricación crítica	Vehículos, maquinaria, equipos electrónicos
Alimentación	Producción, transformación y distribución a gran escala
Química	Fabricación y distribución de sustancias peligrosas

Proveedores también afectados

Si su empresa trabaja como proveedor tecnológico de una entidad esencial — software, mantenimiento, consultoría IT — también puede estar en el ámbito de NIS2. Consúltelo con su asesor legal si tiene dudas.

QUÉ EXIGE NIS2 EN LA PRÁCTICA

- Política de seguridad de la información aprobada por dirección
- Análisis de riesgos documentado y actualizado al menos anualmente

- Plan de respuesta a incidentes probado y documentado
- Notificación a la autoridad en menos de 24 horas ante una brecha
- Gestión de la cadena de suministro — control de proveedores tecnológicos
- Autenticación multifactor en sistemas con acceso externo
- Cifrado de datos en tránsito y en reposo
- Continuidad del negocio con plan de recuperación documentado
- Formación en ciberseguridad para el personal relevante

LAS SANCIONES

Categoría	Consecuencias
Entidades esenciales	Hasta 10 M€ o el 2% de la facturación global anual (el mayor)
Entidades importantes	Hasta 7 M€ o el 1,4% de la facturación global anual
Responsabilidad directiva	Los directivos pueden ser declarados responsables personalmente
Plazo de notificación	Alerta en 24 h · Informe completo en 72 h · Informe final en 1 mes

05

Cómo saber si su empresa ha sido comprometida sin saberlo.

La mayoría de las brechas permanecen sin detectar durante semanas.

SEÑALES DE ALERTA — COMPRUEBE AHORA

ALTA	**Equipos más lentos de lo normal sin motivo aparente**	Puede indicar un proceso malicioso consumiendo recursos en segundo plano.
ALTA	**Inicios de sesión a horas inusuales o desde ubicaciones desconocidas**	Los atacantes suelen operar fuera del horario laboral para pasar desapercibidos.
ALTA	**Usuarios que reciben emails de verificación que no solicitaron**	Señal de phishing dirigido o de credenciales ya comprometidas.
MEDIA	**Tráfico de red elevado hacia el exterior, especialmente nocturno**	Puede indicar exfiltración de datos en curso.
MEDIA	**Archivos modificados o desaparecidos sin explicación**	Especialmente relevante en carpetas con documentos estratégicos o financieros.
MEDIA	**Antivirus o sistemas de seguridad que se desactivan solos**	Los atacantes avanzados frecuentemente deshabilitan las defensas antes de actuar.
BAJA	**Llamadas de "soporte técnico" que nadie solicitó**	Ingeniería social — intento de obtener credenciales o acceso remoto.
BAJA	**Correos enviados desde cuentas corporativas que nadie reconoce**	Posible compromiso de la cuenta de email. Cambiar contraseñas inmediatamente.

! ATENCIÓN — Si detecta alguna de estas señales, no apague los equipos afectados ni borre logs. En primer lugar, documente lo que ve. Asimismo, contacte con su equipo de seguridad. Apagar el equipo puede destruir evidencias forenses necesarias para identificar el alcance del ataque.

06

Qué preguntar a cualquier proveedor de IA antes de firmar.

Si no puede responder estas preguntas, no es el proveedor adecuado.

P 01

¿Dónde se almacenan y procesan mis datos?

La respuesta correcta es: en territorio de la UE, con identificación exacta del país y del centro de datos. Si la respuesta es vaga o menciona "múltiples regiones", exija precisión por escrito antes de firmar nada.

P 02

¿Se usan mis datos para entrenar modelos de terceros?

La respuesta correcta es: no, nunca, y así está documentado en el contrato con cláusula específica. Si incluye "solo datos anonimizados", pida la definición exacta de anonimización que aplican.

P 03

¿Qué nivel de SLA ofrecen y qué ocurre si no lo cumplen?

Exija porcentaje de uptime documentado y compensación automática en caso de incumplimiento. Un SLA sin consecuencias no es un SLA — es marketing.

P 04

¿Tienen certificaciones de seguridad auditables (ISO 27001, ENS, SOC 2)?

Las certificaciones deben estar vigentes. Pida el número de certificado y la fecha de última auditoría. "En proceso de certificación" no cuenta.

P 05

¿Cómo gestionan el fine-tuning? ¿El modelo resultante es mío?

El modelo entrenado con sus datos debería ser propiedad suya. Exija claridad sobre la propiedad intelectual del modelo resultante.

P 06

¿Qué ocurre con mis datos si termino el contrato?

Exija plazo exacto de eliminación, confirmación por escrito y procedimiento de exportación en formato estándar. Si no hay respuesta clara, asuma que sus datos no se eliminan.

P 07

¿Cuentan con equipo técnico en España?

Para soporte, incidentes y auditorías, tener interlocutor directo en español con conocimiento del marco normativo español marca una diferencia real.

07

Checklist de cumplimiento RGPD y NIS2 para empresas españolas — 2026.

Imprima esta página. Marque lo que tiene. Lo que quede vacío es su plan de acción.

A. FUNDAMENTOS RGPD

- ☐ Registro de Actividades de Tratamiento (RAT) actualizado
- ☐ Base legal documentada para cada tratamiento de datos personales
- ☐ Cláusulas de privacidad en todos los formularios de recogida de datos
- ☐ Contrato de encargado de tratamiento firmado con todos los proveedores cloud
- ☐ Procedimiento documentado para ejercicio de derechos de los interesados
- ☐ Política de retención y eliminación de datos definida y aplicada
- ☐ Registro de brechas de seguridad con plazo de notificación a AEPD (72h)

B. CONTROLES TÉCNICOS NIS2

- ☐ Política de seguridad aprobada por dirección
- ☐ Análisis de riesgos documentado y actualizado
- ☐ Inventario de activos críticos (sistemas, datos, infraestructura)
- ☐ Segmentación de red — sistemas críticos aislados
- ☐ Autenticación multifactor en todos los sistemas con acceso a internet
- ☐ Gestión de parches y actualizaciones con trazabilidad
- ☐ Backups verificados con prueba de restauración documentada
- ☐ Plan de respuesta a incidentes probado en simulacro
- ☐ Formación en ciberseguridad completada por todo el personal
- ☐ Monitorización activa de sistemas críticos (SIEM o equivalente)

C. GESTIÓN DE PROVEEDORES

- ☐ Inventario de todos los proveedores con acceso a sistemas o datos
- ☐ Cuestionario de seguridad enviado a proveedores críticos
- ☐ Cláusulas de seguridad incluidas en contratos con proveedores tecnológicos
- ☐ Revisión anual del nivel de seguridad de los proveedores críticos

D. CONTINUIDAD DEL NEGOCIO

- ☐ Plan de Continuidad del Negocio (BCP) documentado

- Plan de Recuperación ante Desastres (DRP) con RTOs y RPOs definidos
- Prueba de continuidad realizada en los últimos 12 meses

Resultado del checklist

Si tiene menos del 60% marcado, su empresa tiene vulnerabilidades de cumplimiento que pueden derivar en sanciones ante una inspección. Por ello, le recomendamos solicitar una evaluación gratuita — en 48 horas le decimos qué es prioritario y cuál es el plan de acción más eficiente.

+

Glosario rápido.

Los términos que aparecen en el sector, sin tecnicismos.

Término	Qué significa en la práctica
Fine-tuning	Reentrenamiento de un modelo de IA con datos de su empresa. El resultado es un modelo que habla el idioma de su negocio y no improvisa.
On premise	El servidor y el modelo están físicamente en su oficina. Sus datos no salen de ese perímetro bajo ningún concepto.
SaaS	Modelo de servicio por suscripción mensual. No requiere hardware propio, pero sus datos viajan a la infraestructura de un tercero.
Inferencia	El momento en que la IA piensa y genera una respuesta. La velocidad de inferencia determina qué tan rápido responde el agente.
SIEM	Sistema que recopila y analiza eventos de seguridad en tiempo real. Sin SIEM, un ataque puede pasar semanas sin detectarse.
NIS2	Directiva europea de ciberseguridad. Obliga a sectores esenciales a demostrar controles técnicos bajo pena de multas de hasta el 2% de facturación.
RGPD	Reglamento europeo de protección de datos. Aplica a cualquier empresa que trate datos de ciudadanos europeos.
ENS	Esquema Nacional de Seguridad. Marco obligatorio para administraciones públicas españolas y sus proveedores tecnológicos.
Pentest	Prueba de penetración autorizada. Un equipo ataca sus sistemas de forma controlada para identificar vulnerabilidades antes de que lo haga un atacante real.
RAG	Técnica que permite al modelo consultar documentos actualizados antes de responder. Evita que la IA improvise usando sus documentos corporativos reales.
CPD	Centro de Procesamiento de Datos. El edificio físico donde residen los servidores. Un CPD en España garantiza jurisdicción española.
Threat Intelligence	Información sobre actores maliciosos y sus tácticas. Permite detectar ataques dirigidos antes de que se produzcan.

¿SU EMPRESA NECESITA DAR EL SIGUIENTE PASO?

En definitiva, si después de leer esta guía tiene preguntas concretas sobre su empresa, le ofrecemos una primera consulta técnica sin coste ni compromiso.

Evaluación gratuita de ciberseguridad

En 48 horas identificamos qué está expuesto, si su empresa está en el ámbito NIS2 y cuáles son los pasos urgentes.

Análisis de viabilidad de IA soberana

Le explicamos qué agentes tienen sentido para su caso de uso y cuál es el coste real del proyecto.

Demo de Towin Box o Towinia Cloud

Acceso a una instancia real con datos de ejemplo de su sector antes de comprometerse a nada.

Contacto onpremise@towinia.es
towinia.es

Ubicación Zamora, España
Infraestructura 100% nacional