

Qué recibe tu empresa al contratar un diagnóstico Abordo

Una muestra de 6 páginas de los artefactos y las decisiones que produce el diagnóstico: inventario, matriz de riesgos, priorización, roadmap y políticas de uso.

Ejemplo ilustrativo con datos ficticios — no es un caso de cliente

Contexto ficticio de la muestra

Empresa: Servicios Andina S.A. (nombre ficticio) · 120 empleados

Situación: 4 herramientas de IA en uso · 2 pilotos detenidos antes de producción

Motivo del contacto: preocupación por datos de clientes compartidos sin criterio común y por la inversión ya realizada en los pilotos.

Contenido de la muestra

- Resumen ejecutivo con tres decisiones recomendadas
- Matriz de un caso: datos, riesgo, acceso, responsable y control
- Priorización de cinco casos de uso con criterios visibles
- Roadmap de 90 días con dependencias y responsables
- Extracto de política de uso con revisión humana

El documento muestra el nivel de detalle del trabajo. Los datos y la empresa son ficticios.

Situación y tres decisiones recomendadas

El relevamiento identificó 4 herramientas de IA en uso, con suscripciones parcialmente solapadas y sin inventario aprobado. Dos pilotos con inversión realizada están detenidos: nadie definió qué datos pueden procesar, quién aprueba las salidas ni qué acciones pueden ejecutar las herramientas.

Decisión 1 — Frenar el uso no aprobado antes de ampliar nada

Completar inventario y política de uso inicial. Mientras tanto, los datos de clientes solo se procesan en las dos herramientas ya homologadas, con acceso por rol.

Decisión 2 — Priorizar dos casos de uso para implementación controlada

Cotizaciones asistidas y reporte semanal de operaciones: alto impacto, viabilidad alta y riesgo controlable con revisión humana. El agente de acciones en cloud se evalúa después de definir controles de mínimo privilegio.

Decisión 3 — Nombrar responsables y adoptar el roadmap de 90 días

Seguridad define qué datos puede procesar cada herramienta; IT administra identidades y cuentas de servicio; los líderes de cada caso de uso responden por la revisión humana de las salidas.

Qué contiene el diagnóstico completo

Inventario de adopción · Matriz de datos, riesgos y responsabilidades · Priorización de casos de uso · Catálogo inicial y criterios de selección · Políticas y controles recomendados · Roadmap de 90 días · Sesión ejecutiva de cierre.

Ejemplo ilustrativo con datos ficticios



Caso: cotizaciones asistidas por IA

La IA redacta borradores de cotización a partir de condiciones comerciales históricas. Una persona revisa cada borrador antes de enviarlo.

DIMENSIÓN	DEFINICIÓN
Datos utilizados	Nombres y condiciones comerciales de clientes activos. Se excluyen datos personales de contactos y documentación contractual completa.
Riesgo principal	Fuga de información comercial a herramientas externas no aprobadas, y envío de condiciones incorrectas a un cliente.
Acceso requerido	Solo lectura sobre un dataset acotado y anonimizado. Cuenta de servicio con mínimo privilegio, sin credenciales personales ni permisos de escritura.
Responsables	Líder de seguridad: qué datos puede procesar la herramienta. Líder comercial: revisión de cada cotización antes de enviarla. IT: identidades y registros.
Controles	Revisión humana obligatoria de cada salida. Registro de prompts y respuestas. Prohibido ingresar datos de clientes en herramientas no aprobadas. Revisión mensual del dataset permitido.
Criterio para escalar	Dos semanas de uso controlado sin incidentes y con aceptación de las revisiones por parte del equipo comercial.

La matriz no describe una promesa de seguridad absoluta: define quién decide, con qué información y bajo qué revisión. Los controles dependen de las capacidades de los sistemas involucrados.

Ejemplo ilustrativo con datos ficticios

Cinco casos, criterios visibles

Cada caso se evalúa por impacto, viabilidad, riesgo y esfuerzo. La prioridad no depende del entusiasmo por la tecnología sino de la decisión que se puede sostener.

CASO DE USO	IMPACTO	VIABILIDAD	RIESGO	ESFUERZO	DECISIÓN
Cotizaciones asistidas	Alto	Alta	Medio	Bajo	Priorizar
Reporte semanal de operaciones	Medio-alto	Alta	Bajo	Bajo	Priorizar
Agente de acciones en cloud	Alto	Media	Alto	Medio	Evaluar tras controles de mínimo privilegio
Chat con base completa de clientes	Alto	Media	Alto	Alto	Frenar hasta política de datos
Traducción de documentos públicos	Bajo	Alta	Bajo	Bajo	Catálogo abierto

Lectura de la tabla

- Dos casos se priorizan por combinar impacto real y control sencillo.
- Un caso se frena por riesgo de datos, no por falta de interés.
- El agente de cloud queda condicionado a controles técnicos previos, no a una decisión de negocio.

Ejemplo ilustrativo con datos ficticios

Fases, dependencias y responsables

Días 1–30 — Fundamentos

Trabajo: Inventario aprobado, clasificación de datos, política de uso inicial, catálogo de herramientas homologado.

Dependencias: Acceso a registros de suscripciones y a los responsables de cada área.

Responsables: IT (inventario e identidades), seguridad (clasificación), líderes de área (validación).

Días 31–60 — Pilotos controlados

Trabajo: Cotizaciones asistidas y reporte semanal en uso real, con revisión humana y registro de salidas.

Dependencias: Dataset anonimizado aprobado en la fase anterior y cuentas de servicio con mínimo privilegio.

Responsables: Líder comercial y operaciones (revisión), IT (registro y accesos).

Días 61–90 — Escala y transferencia

Trabajo: Evaluación de los pilotos, decisión sobre el agente de cloud, capacitación de equipos y revisión de controles.

Dependencias: Criterios de aceptación medidos en los pilotos y sesión ejecutiva de cierre.

Responsables: Sponsor ejecutivo (decisión de escalar), seguridad (controles), equipo interno (operación continua).

El roadmap se entrega con iniciativas priorizadas y responsables sugeridos: el equipo interno puede ejecutarlo sin dependencia del consultor.

Ejemplo ilustrativo con datos ficticios



Uso aprobado de herramientas de IA

Datos de clientes

Solo se procesan en herramientas homologadas por la empresa, con el dataset aprobado por seguridad. Está prohibido ingresarlos en herramientas no aprobadas.

Revisión humana

Toda salida destinada a un cliente externo requiere revisión de una persona responsable antes de su envío.

Acciones sobre el cloud

Requieren aprobación humana previa y una cuenta de servicio con mínimo privilegio. No se ejecutan acciones con credenciales personales.

Herramientas nuevas

Entran al catálogo solo después de una evaluación de riesgo y con un responsable asignado.

Registro

Se conservan los prompts y las salidas de los casos priorizados para revisión y mejora.

Ejemplo de flujo de revisión humana

Borrador generado por IA → revisión del responsable comercial → corrección si hace falta → envío al cliente → registro de la salida aprobada.

Gobernanza del documento

Responsable: Líder de seguridad. Revisión: mensual o ante un incidente. El documento se versiona en la wiki de la empresa, con historial de cambios.

Esta política es un extracto ilustrativo: la versión real se adapta al contexto, a los sistemas y a los proveedores de cada organización.