

L U M B R E



Riesgo de la IA en la empresa: minimización de datos, contrato con el proveedor, sesgo en decisiones y fraude por voz clonada

Materia: Administración y dirección

07/10/2026

Antes de empezar

Tema 6 de 8, cierre de la etapa Personas, datos y riesgo. La base de clientes como préstamo y no como propiedad, el criterio de minimización que resuelve la mitad del riesgo, las cuatro preguntas por escrito al proveedor, qué exige la regulación que ya aplica y qué viene, el sesgo que se esconde en la lista de prospectos y de candidatos, el fraude con voz clonada y la regla de segundo canal. Cuatro videos y cuatro diagramas propios.

QUÉ APRENDERÁS

- Distinguir el dato como activo bajo custodia, aplicar minimización y las cuatro preguntas contractuales al proveedor, reconocer el sesgo que hereda el histórico en priorización y contratación, instaurar la auditoría de descartes y el segundo canal contra fraude, y asumir que la responsabilidad del error es de la empresa.

Datos, regulación, sesgo y fraude: lo que se firma cuando se activa una herramienta

Este tema es el más incómodo del curso porque no habla de eficiencia. Habla de lo que la empresa entrega sin cotizarlo: la información de sus clientes, la de su gente, el criterio con el que decide a quién llama y a quién no, y el dinero que puede salir por una orden que alguien no dio.

El riesgo más grande que trae la adopción de inteligencia artificial en una PyME no es técnico ni legal: es que la empresa empezó a tratar información que no era suya —la de sus clientes y la de su propio personal— como si fuera un insumo gratis para configurar una herramienta de otra persona.

Ficha del objeto · Lumbre

Curso: Empresarios e IA (2026-2034) · Ruta: Ruta del empresario aumentado · Etapa: Personas, datos y riesgo · Tema 6 de 8 · Dificultad: intermedia · Duración sugerida: una hora veinte con cuatro videos, cuatro diagramas propios y reactivos con evidencia · Prerrequisito: tema 5 de esta ruta (equipo y conocimiento) y tema 3 (datos del cliente en la venta) · Autoría: Roadwise Consulting.

1. Qué es un activo y qué es un pasivo

La base de clientes es el activo que menos se puede reponer y el más fácil de entregar. Subir correos, teléfonos, domicilios e historiales de compra a una herramienta gratuita no cuesta dinero: cuesta control, y el control es lo único que hace que esa base siga siendo un activo y no un producto que alguien más está entrenando.

Hay un criterio que resuelve la mitad de los casos sin consultar a ningún abogado: no subir lo que la herramienta no necesita. Para pedir un pronóstico de reposición no hace falta el nombre del cliente ni su teléfono; alcanza con producto, cantidad y fecha. El dato que no sale de la empresa no puede filtrarse, entrenar a un tercero ni violar una ley.

Una confusión frecuente: creer que el dato es propio porque la empresa lo recopiló. Buena parte de lo que hay en el archivo de clientes es información personal que se entregó para comprar, no para entrenar un modelo ni para que otra empresa la use con fines que nadie declaró. La diferencia entre activo y pasivo está en el consentimiento y en el uso, no en la propiedad de la base.

Dónde se rompe el riesgo de subir los datos a una herramienta

Cuatro capas que hay que cerrar antes de pegar el primer archivo

Lumbre · Empresa

CUATRO CAPAS

Qué dato sale

Datos personales, de nómina, de salud o secretos de producción: no todos viajan.

Quién lo puede ver

Acceso por rol y registro de quién consultó qué: sin esto no hay control posible.

Con qué finalidad

Si el proveedor entrena con la base de clientes, está cobrando de otra manera.

Con qué contrato

Encargo de tratamiento, plazo de borrado, responsabilidad ante fuga y jurisdicción.

La base de clientes es el activo más difícil de reconstruir y el más fácil de entregar sin contrato.

El error habitual es empezar por la última capa: sin saber qué dato sale, el contrato no protege de nada.

Lo que se juega una empresa al usar modelos sin reglas

Cuatro exposiciones con dueños distintos y un mismo origen

Lumbre · Empresa

CUATRO RIESGOS



Base de clientes en una app gratuita

Datos personales de terceros tratados sin contrato ni finalidad declarada.



Receta, diseño o proceso subido a un chat

Secreto industrial entregado a un proveedor que lo usa para entrenar.



Respuesta automática que promete de más

El asistente compromete precio, entrega o garantía que la empresa no puede cumplir.



Selección de personal con un modelo

Descarta por patrón de currícula y reproduce sesgo sin que nadie lo firme.

El costo no es la multa: es el cliente que se entera y se va.

Los cuatro riesgos comparten remedio: decir qué datos salen de la empresa, quién responde por lo que se promete y quién revisa lo que se decide.

VIDEO

Inteligencia Artificial y Marco Legal: Riesgos, Regulación y Oportunidades para las Empresas

Anota qué responsabilidades se mencionan como ya exigibles para una empresa mediana y cuáles dependen de una ley que todavía no está vigente: la lista de las primeras es la que hay que atender.



Escanea para verlo en Lumbre

<https://www.youtube.com/watch?v=hLJuz1yzCLU>

VIDEO

Privacidad y gobernanza de datos en 2026: retos globales RGPD, IA y Latinoamérica

Escucha qué parte de la gobernanza es tecnológica y qué parte es organizativa: en una PyME el hueco casi siempre está en la segunda y se disfraza comprando la primera.



Escanea para verlo en Lumbre

<https://www.youtube.com/watch?v=GhhbwccawnM>

1. Una empresa quiere usar un asistente que redacta respuestas con el historial de sus clientes. ¿Cuál es el primer paso de la política de datos?

- ☐ Pedir a todos los clientes un nuevo consentimiento general por correo
- ☐ Definir qué campos mínimos necesita el asistente y qué datos personales quedan fuera
- ☐ Contratar un servicio de cifrado para la base de clientes
- ☐ Prohibir el uso de cualquier herramienta externa mientras exista duda legal

2. Subir la base de clientes a una herramienta gratuita no tiene consecuencias porque no se pagó por ella.

- ☐ Verdadero
- ☐ Falso

Qué información puede compartirse con una herramienta, bajo qué condición y cuánto cuesta perderla

Dato	Puede salir de la empresa	Nunca sale sin contrato	Costo si se filtra
Catálogo público y precios	Sí, sin problema	No aplica	Bajo
Volúmenes de venta por producto	Sí, agregado y sin cliente	Con nombre de cliente	Medio
Correo y teléfono del cliente	No	Finalidad y plazo declarados	Alto
Domicilios y RFC	No	Tratamiento con encargado formal	Muy alto
Datos de salud o nómina del personal	No	Requiere base legal específica	Muy alto

Dato	Puede salir de la empresa	Nunca sale sin contrato	Costo si se filtra
Recetas, claves y método de producción	No	Secreto industrial por escrito	Irrecuperable

2. Regulación: qué aplica hoy y qué viene

La regulación avanza más lento que la adopción y por eso casi nunca llega a tiempo para proteger a quien se confió. En la Unión Europea ya hay obligaciones con fechas para los sistemas de riesgo, y en América Latina el piso es la legislación de datos personales, que sí aplica hoy a la empresa que sube una base de clientes a un servidor ajeno.

Conviene tomar una decisión práctica: trabajar como si la regulación avanzada ya aplicara. No porque la multa llegue, sino porque las obligaciones que esas leyes imponen —minimización, registro, consentimiento verificable, borrado cuando el cliente lo pide— son las mismas que evitan la filtración que sí cuesta dinero y clientes hoy. Y conviene quitarse de encima una idea falsa que circula en los cursos cortos: nadie está protegido por la convicción de que el aviso de privacidad basta para hacer cualquier cosa con el dato que otro le entregó.

Cuatro preguntas por escrito antes de subir un archivo: qué datos se tratan y con qué finalidad, quién tiene acceso dentro de la empresa, cuánto tiempo se guardan y qué pasa con ellos al terminar el contrato. Si el proveedor no contesta las cuatro en un documento, no hay acuerdo: hay una caja de texto.

Ese documento no es un trámite legal mayor: en una empresa de veinte personas cabe en dos páginas y es lo que convierte una suscripción en una relación revisable. Sin él, cualquier discusión posterior sobre quién usó qué, con qué fin y durante cuánto tiempo se cierra con un copy-paste de los términos del servicio, que no fueron escritos para proteger a la empresa que paga la mensualidad.

Cuatro prácticas de riesgo y lo que cuestan

Qué se expone cuando la empresa adopta modelos sin reglas de datos

Lumbre · Empresa

EXPOSICION

Subir la base de clientes sin contrato

ALTA

Exposición alta y permanente: el activo se usa para entrenar a alguien más.



Automatizar el dato de nómina

ALTA

Exposición alta: datos personales sensibles, con derecho de reclamo individual.



Dejar que el bot conteste reclamos

MEDIA

Exposición media: genera compromiso escrito y prueba contra la empresa.



Pedirle al modelo que despida

MEDIA

Exposición media y silenciosa: sesgo del historial convertido en decisión.



La regulación avanza más lento que la adopción: conviene actuar como si ya aplicara.

Ninguna de las cuatro es ilegal por sí misma: el problema es hacerlas sin reglas escritas y sin saber que se están haciendo.

VIDEO

Reglamento Europeo de IA: qué ha cambiado el 2 de agosto de 2026 y qué debe hacer tu empresa

Identifica qué exige el reglamento a quien usa la herramienta y qué exige a quien la construye: en una PyME casi todo cae del primer lado y casi nadie lo sabe.



Escanea para verlo en Lumbre

<https://www.youtube.com/watch?v=K1zFfT1xd4Q>

ACTIVIDAD INTERACTIVA
DISPONIBLE EN LUMBRE

3. Una de estas afirmaciones sobre datos y regulación es incorrecta. ¿Cuál?



4. Clasifica cada uso cotidiano de una herramienta según el riesgo del dato que se le entrega.

Elementos:

- Preguntar al modelo por el clima de la ciudad
- Subir el catálogo y los precios para generar publicidades
- Pegar un texto de un cliente para redactar la respuesta
- Cargar ventas por producto sin nombre de cliente
- Exportar la base de clientes al panel del proveedor
- Subir nómina y datos de salud a una app sin contrato
- Compartir la fórmula del producto con un servicio externo

Sin riesgo	. . .
Riesgo medio	. . .
Riesgo alto	. . .

ACTIVIDAD
INTERACTIVA
DISPONIBLE EN
LUMBRE

5. ¿Tienes por escrito qué hace tu proveedor de software con los datos de tus clientes?



3. Sesgo: la decisión que hereda el prejuicio

El sesgo en una empresa pequeña no se ve como en los documentales: no hay un sistema que rechace candidatos por apellido. Se ve como una lista de prospectos donde nunca aparece cierto barrio, un puntaje de crédito que castiga a quien paga distinto, o una hoja de vida descartada porque no coincide con el perfil que la empresa ya contrató diez veces.

La razón por la que esto importa en una empresa y no solo en una multinacional es que aquí el sesgo decide a quién se llama, a quién se le da crédito y a quién se contrata. Son tres decisiones que valen dinero y que afectan a personas concretas, y se toman cada vez más rápido con una recomendación que llega redactada como si fuera un cálculo neutro.

El control del sesgo es aburrido y es posible: mirar de vez en cuando la lista de lo que el sistema descartó. Quién quedó fuera, con qué criterio y si alguien valioso habría estado ahí. Cinco minutos al mes, con una persona que conozca el negocio, y no con la hoja de métricas del proveedor.

Qué pasa cuando el modelo se equivoca con un cliente

Recorrido del error automático, desde el mensaje hasta la responsabilidad

Lumbre · Empresa

UN ERROR



La defensa no es un mejor modelo: es la lista de lo que no puede decir y el registro de revisiones.

Toda automatización comercial sin reglas escritas convierte un error de software en un compromiso de la empresa.

VIDEO

Lorena Fernández: Sesgo de la IA, ¿deciden los algoritmos por ti?

Fíjate en qué parte del sesgo viene del dato histórico y qué parte del diseño del sistema: en una PyME, la primera es la que reproduce lo que la empresa ya hacía a ojo.



Escanea para verlo en Lumbre

<https://www.youtube.com/watch?v=-0maheBivaM>

6. Una empresa usa un modelo para priorizar qué prospectos llamar, entrenado con los cierres de los últimos tres años. Antes de ver el efecto, ¿qué es lo más probable que ocurra con la cartera?

- ☐ Que el sistema encuentre clientes nuevos en segmentos que nadie probó
- ☐ Que se concentre en llamar al perfil que siempre compró y deje de contactar al resto
- ☐ Que la priorización no cambie nada porque todos los prospectos son iguales
- ☐ Que el modelo rechace funcionar sin un contrato de datos

Reflexiona: Si la estrategia de la empresa es crecer en un segmento nuevo, hay que decirlo en la regla de priorización, porque el histórico no lo va a proponer solo.

7. El control del sesgo es aburrido y es posible: mirar de vez en cuando la lista de lo que el sistema _____ .

4. Fraude con inteligencia artificial: el riesgo que llega por WhatsApp

Apareció un riesgo operativo que no existía hace cinco años y que golpea directo a la caja: la voz y la cara del dueño o del proveedor, generadas por máquina. Una orden de pago con la voz conocida, un cambio de cuenta con el tono habitual, una urgencia creíble a las nueve de la noche. La defensa no es detectar el audio: es una regla de segundo canal.

Los casos que más se repiten son simples de contar: una llamada del dueño pidiendo un pago urgente con su voz habitual, un correo del proveedor de siempre con la cuenta cambiada, un audio del familiar o del contador pidiendo un dato. Lo que cambió es la fábrica: antes se necesitaba parecer alguien; ahora basta una muestra de voz de treinta segundos.

Regla de segundo canal: ningún cambio de cuenta, ningún pago fuera de lo habitual y ningún dato sensible se ejecuta con lo que dijo un mensaje, una llamada o un video. Se confirma por otro medio, con un contacto que la empresa ya tenía, y se pregunta algo que solo la otra persona real sabe.

Para dimensionar el costo basta el caso base que se repite en las alertas: una empresa paga una factura de 340 000 pesos a una cuenta que el proveedor nunca cambió, y el seguro de fraude cubre apenas una parte. El fraude dejó de ser un evento excepcional para convertirse en un riesgo de procedimiento, y los procedimientos se arreglan con dos minutos de confirmación.

8. Una empresa paga una factura de 340 000 pesos a una cuenta que el proveedor nunca cambió. El seguro de fraude cubre 60 000 pesos. ¿Cuánto pierde la empresa? Redondea a miles.

Respuesta: (pesos)

9. Llega un audio del proveedor habitual: cambió de banco y pide depositar hoy la quincena. ¿Qué hace el encargado de pagos?

- ☐ Deposita: la voz es claramente la del proveedor y hay urgencia
- ☐ Confirma el cambio por un contacto que ya tenía, con una pregunta que solo el proveedor real sabe contestar
- ☐ Pide que envíen la factura otra vez por el mismo canal
- ☐ Guarda el audio como comprobante y procede con el pago

10. Detectar un audio falso escuchando si suena natural es un control confiable para autorizar un pago.

- ☐ Verdadero
- ☐ Falso

ACTIVIDAD INTERACTIVA
DISPONIBLE EN LUMBRE

11. Política de datos y pagos en una PyME, en seis movimientos



Qué se fue sumando al riesgo del dato, año por año

1. 2024-2025**Todo a la nube** Se sube sin preguntar: la comodidad era el argumento y el contrato no existía.
2. 2026**Llamada clonada** El fraude por voz pasa de caso raro a procedimiento de manual en PyMEs.
3. 2027-2028**Obligaciones de uso** Marcos con fechas y exigencias sobre sistemas de riesgo y sobre quién usa la herramienta.
4. 2029-2031**Datos o nada** El cliente empieza a condicionar: quién trata su información y para qué.
5. 2032-2034**Costo de la historia** Lo que se entregó sin contrato no se recupera: se renegocia o se reconstruye la base.

Cuando un modelo se equivoca con un cliente, la responsabilidad no es del modelo. La empresa prometió, la empresa respondió con su marca y la empresa paga: por eso toda automatización que habla con clientes necesita reglas escritas, un registro de revisiones y una persona que responda por lo que dijo.

La parte cómoda de esta regla es que también es la más barata: un bot con reglas escritas, un registro de lo que dijo y un nombre responsable no requiere software adicional. Requiere que alguien decida qué puede prometer y que alguien firme lo que promete, dos cosas que casi ninguna PyME ha hecho antes de activar la herramienta.

ACTIVIDAD
INTERACTIVA
DISPONIBLE EN
LUMBRE

12. «Si cumplo la ley europea cuando me aplique, me alcanza: mientras no haya multa, el dato libre de mis clientes es mi ventaja competitiva.»



Regla de este tema: los datos de clientes y personal se tratan como algo prestado, no como material de trabajo; ninguna herramienta entra sin las cuatro respuestas por escrito; ninguna decisión sobre personas la toma el sistema sola; y ningún pago se mueve sin confirmación por un segundo canal.

13. Une cada control del riesgo con su definición operativa.

13.	Minimización	-----
13.	Encargo de tratamiento	-----
13.	Auditoría de descartes	-----
13.	Segundo canal	-----

Opciones: No entregar lo que el proceso no necesita · Contrato que dice qué hace el proveedor con el dato · Revisar quién quedó fuera de la lista del modelo · Confirmar por otra vía antes de mover dinero

Las tres reglas que valen más que cualquier política larga

El dato personal no sale si el proceso funciona sin él. Ninguna decisión sobre personas la toma el sistema sola. Ningún pago se ejecuta con lo que dijo un mensaje. Tres líneas, escritas y conocidas por todo el equipo, cubren la mayoría del riesgo de esta década.

La empresa no es dueña del dato de sus clientes: es custodio de una información que le prestó para comprarle. Esa frase cambia más decisiones que cualquier política de privacidad descargada de internet.

— Idea central del tema 6

14. Escribe qué datos de clientes tienes hoy, en dónde están y cuáles subirías a una herramienta si la necesitaras mañana. Después contesta la segunda parte: si esa información saliera en un periódico local esta semana, ¿qué cliente te dejaría de hablar?

La primera respuesta es un inventario; la segunda es el riesgo. Quien no puede contestar la segunda todavía no tiene una política de datos, tiene un archivo abierto.

ACTIVIDAD
INTERACTIVA
DISPONIBLE EN
LUMBRE

**15. Mi inventario de datos: qué hay /
dónde está / quién lo ve / qué no sale de
la empresa**



ACTIVIDAD INTERACTIVA DISPONIBLE EN LUMBRE

16. Tarjetas del tema 6



ACTIVIDAD INTERACTIVA
DISPONIBLE EN LUMBRE

**17. Memoria
del tema 6**

Une cada exposición
con su control.



ACTIVIDAD
INTERACTIVA
DISPONIBLE EN
LUMBRE

**18. Sopa de
letras del
tema 6**

Ocho términos del riesgo de datos,
en horizontal, en mayúsculas y sin
acentos.



Trazabilidad curricular del objeto

Dónde vive este objeto dentro de la ruta del curso

Campo	Valor
Categoría	Administración y Dirección
Curso	Empresarios e IA (2026-2034)
Ruta	Ruta del empresario aumentado
Etapas	Personas, datos y riesgo
Área de conocimiento	Gobernanza de datos, regulación y riesgo operativo
Tema	Datos, regulación, sesgo y fraude: lo que se firma al activar una herramienta
Objeto en la ruta	6 de 8
Dificultad	Intermedia
Modalidad	Autoestudio con video, diagrama propio y reactivos con evidencia
Prerrequisito	temas 3 y 5 de esta ruta
Autoría	Roadwise Consulting

Referencia curricular

Materia:	Administración y dirección
-----------------	----------------------------

Versión interactiva completa (con actividades, videos y autoevaluación):



<https://empresa.lumbre.lat/object/emp-06>

Material educativo generado desde Lumbre · lumbre.lat