

GRUPO DE TRABAJO DE TURISMO Y HOTELERIA

La inteligencia artificial en Turismo y Hotelería: retos sectoriales, marco regulatorio comparado y cláusula modelo

21 de septiembre de 2026

© Madrid (España), septiembre de 2026

PRESIDENTES:

[David Vich Comas](#)

Socio, Garrigues

[Alejandra Aguad Deik](#)

Socia, Aguad Bañados Izquierdo Abogados

SECRETARIA:

[Lisette Hernández Del Olmo](#)

Abogada, Garrigues

Este documento es fruto del trabajo del Grupo de Trabajo de Turismo y Hoteles y no representa la posición de CIAM. No constituye, tampoco, asesoramiento jurídico de ningún tipo respecto de una disputa específica.

TABLA DE CONTENIDO

I.	PRÓLOGO.....	4
II.	PRESENTACIÓN DEL TRABAJO.....	6
III.	OBJETO Y ALCANCE	7
IV.	LA IA EN TURISMO Y HOTELERÍA: TRANSFORMACIÓN, APLICACIONES Y RETOS.....	7
1.	LA IA COMO MOTOR DE TRANSFORMACIÓN PRODUCTIVA EN EL SECTOR..	7
2.	LOS TRES NIVELES DE ACTUACIÓN DE LA IA EN EL SECTOR.....	8
3.	UN CAMBIO DE ESCENARIO	8
4.	PRINCIPALES LÍNEAS DE APLICACIÓN EN TURISMO Y HOTELERÍA.....	9
4.1.	<i>Front-office</i> y experiencia del huésped.....	9
4.2.	<i>Back-office</i> y operaciones internas.....	10
5.	RETOS DEL SECTOR: DATOS, CAPACIDADES Y ECONOMÍA.....	11
5.1.	Retos de datos.....	11
5.2.	Retos de capacidades.....	11
5.3.	Retos económicos	11
V.	MARCO REGULATORIO COMPARADO	12
1.	Unión Europea.....	12
2.	Chile	13
3.	México.....	14
4.	Brasil.....	14
5.	Colombia.....	14
6.	Argentina	15
VI.	CHILE: LINEAMIENTOS ACTUALES Y VACÍOS NORMATIVOS	15
1.	Revisión del Proyecto de Ley que regula los Sistemas de Inteligencia Artificial	16
1.1.	Objeto, justificación normativa y ámbito de aplicación	16
1.2.	Definiciones y roles en la cadena de suministro.....	16
1.3.	Principios rectores y estándar transversal de conducta.....	16
1.4.	Modelo basado en riesgos	16
1.5.	Sanciones y responsabilidad civil.....	17
1.6.	Mecanismos de fomento: espacios controlados de prueba y apoyo a empresas.	17
1.7.	Convergencia con datos personales y ciberseguridad	17

2.	Análisis del Proyecto de Ley respecto de la industria del turismo y hotelería ...	18
2.1.	Relevancia sectorial e impacto operativo	18
2.2.	Sujetos obligados y tensión contractual con proveedores internacionales	18
2.3.	Clasificación de riesgos aplicada a usos típicos del sector	18
2.4.	Vacíos normativos y zonas grises	18
2.5.	Perfil de riesgo agregado: sanciones, responsabilidad y reputación	19
VII.	BUENAS PRÁCTICAS EMPRESARIALES Y AUTORREGULACIÓN	19
1.	Estándares internacionales como línea base sectorial	19
2.	Gobernanza digital hotelera: estructura, roles y convergencia con compliance y ESG 20	
3.	Instrumentos mínimos de autorregulación.....	20
4.	Supervisión humana y control de decisiones automatizadas relevantes.	20
5.	Transparencia y deberes frente al consumidor	21
6.	Gestión de terceros, auditoría y evidencia.....	21
VIII.	GESTIÓN CONTRACTUAL, CADENA SUMINISTRO Y RESOLUCIÓN DE CONTROVERSIAS.....	21
1.	El ecosistema de terceros como punto duro del sector	21
2.	Checklist mínimo multi-país para uso de IA y datos personales.....	22
3.	Riesgos de litigiosidad y responsabilidad civil	22
4.	Arbitraje comercial como mecanismo idóneo	22
5.	Aterrizaje contractual: cláusula modelo de cumplimiento y uso de IA.....	23
IX.	CONCLUSIONES.....	24
	ANEXO A. MATRIZ COMPARADA POR JURISDICCIÓN (NORMATIVA VIGENTE)	25
	ANEXO B. MATRIZ OPERATIVA CASO DE USO TÍPICO EN TURISMO Y HOTELERÍA .	36
	ANEXO C. CLÁUSULA MODELO: INTELIGENCIA ARTIFICIAL	39

I. PRÓLOGO

La irrupción de la inteligencia artificial (IA en adelante) ha supuesto una transformación en todos los aspectos de la vida humana, introduciendo cambios sustanciales en todas las actividades productivas, desde su generación hasta las decisiones esenciales sobre las mismas. El turismo, no es ajeno a esta ola, como demuestra su empleo para la anticipación de tendencias, optimización de procesos o la generación de nuevas oportunidades en un sector estratégico a nivel global, conllevando que ONU Turismo, como organismo internacional que promueve un turismo sostenible e inclusivo juegue un papel esencial para todos los operadores del sector.

Sin embargo, el verdadero potencial de la inteligencia artificial no reside únicamente en la disponibilidad de nuevas herramientas, sino en la capacidad de empresas, destinos y administraciones públicas para incorporarlas de manera estratégica y responsable. Ello requiere fortalecer las competencias digitales y el talento, impulsar ecosistemas de innovación que conecten al sector turístico con empresas tecnológicas y startups, y facilitar las condiciones necesarias para que la inversión en tecnología se traduzca en mayor productividad, competitividad y valor para los destinos y sus comunidades.

Este contexto implica igualmente un enorme desafío para el derecho de turismo, tal y como demuestra el presente trabajo que, a través de un excelente análisis desentraña algunas de las cuestiones a las que habremos de enfrentarnos en los próximos años. El uso de la IA, la incorporación de sistemas inteligentes, en ámbitos como el derecho de la contratación, la protección de datos o la gestión de destinos conlleva necesariamente que se deban afrontar cambios legislativos que permitan ajustar la normativa a la realidad económica y social del mundo.

De este modo, al igual que se hace en este trabajo, ONU Turismo viene desarrollando acciones que ponen a la IA en el centro y, más concretamente, en lo relativo al derecho se desarrolló en el III Seminario Internacional de Derecho del Turismo celebrado en La Habana, Cuba en diciembre de 2025, una mesa redonda que tuvo por título “Regulación de la Inteligencia Artificial en el Sector Turístico: Desafíos y Nuevos Horizontes Jurídicos”, en la que expertos de distintas nacionalidades tuvieron la oportunidad de disertar sobre esta cuestión, analizando su actual desarrollo y buscando soluciones para los retos ante los que el sector jurídico se encuentra y que están también reflejados en el presente trabajo.

Esta reflexión forma parte de un trabajo más amplio de ONU Turismo sobre la adopción responsable de la inteligencia artificial en el sector. En este contexto, la publicación *Artificial Intelligence Adoption in Tourism: Key Considerations for Sector Stakeholders* (2025) aborda las oportunidades que ofrece esta tecnología y las principales consideraciones para su adopción por parte de los actores del sector turístico. A esta línea de trabajo se suma *AI Impact Analysis on Tourism Jobs and the Future of Tourism*, que analiza el impacto de la inteligencia artificial sobre el empleo turístico y la evolución futura del sector, prestando especial atención a la transformación de las competencias y capacidades profesionales que requiere la creciente incorporación de estas tecnologías. Asimismo, *Implementing Artificial Intelligence in Tourism: Guidelines and Recommendations for the Public Sector*, vinculada al *UN Tourism AI Readiness and Maturity Framework*, aborda la implementación de la IA desde la perspectiva de las administraciones públicas y ofrece directrices y recomendaciones para orientar su adopción. Este marco permite, además, analizar el grado de preparación y madurez de los países para la implementación de la inteligencia artificial en el turismo, proporcionando una referencia para identificar necesidades, orientar políticas públicas y avanzar hacia una adopción estratégica y responsable de estas tecnologías. El

presente informe toma estas publicaciones como referencias internacionales para orientar la adopción de la IA y la gestión de sus riesgos en el turismo.

En el mismo sentido, en el marco del Plan de Trabajo del Observatorio del Derecho del Turismo para América Latina y el Caribe para los ejercicios 2026/2027, las nuevas tecnologías y la IA son objeto de estudio, pues así lo han querido los Estados miembros de la zona, quienes lo han establecido como uno de los elementos sobre los que debiera de pivotar la acción que se desarrolla a través de esta herramienta que ONU Turismo ha creado con la misión de impulsar el desarrollo, la armonización y la modernización del marco jurídico del turismo en la región, promoviendo políticas públicas basadas en evidencia, el fortalecimiento institucional y la protección de los derechos de turistas, comunidades y actores del sector.

En consecuencia, en un momento en el que el turismo se enfrenta a una importante transformación este trabajo se presenta como una guía que permite a profesionales y académicos conocer de manera sencilla pero rigurosa los desafíos existentes y avanzar hacia una adopción de la inteligencia artificial que combine innovación, competitividad y responsabilidad.

En este contexto, innovación y regulación no deben entenderse como fuerzas contrapuestas, sino como elementos complementarios. Unos marcos éticos y jurídicos sólidos, acompañados del desarrollo de las capacidades necesarias, pueden generar la confianza necesaria para impulsar la inversión y facilitar el desarrollo y la adopción responsable de soluciones innovadoras en el sector turístico.

Dña. Alicia Gómez

Directora del Departamento de Asuntos Jurídicos y Estándares Internacionales
ONU Turismo

II. PRESENTACIÓN DEL TRABAJO

Con la satisfacción renovada de quien ve crecer un proyecto colectivo, presentamos el tercer entregable fruto de la labor del Grupo de Trabajo de Turismo y Hoteles de CIIAM. Si el año pasado la temática escogida fueron los criterios ESG y su reflejo en las cláusulas contractuales de la operación hotelera, este año el Grupo de Trabajo ha decidido abordar uno de los fenómenos que con mayor intensidad y velocidad está transformando la industria del turismo y la hotelería: la inteligencia artificial.

Mucho se habla de la inteligencia artificial, pero, en muchas ocasiones, se hace desde una perspectiva general o abstracta que dificulta aterrizar su impacto en una industria en concreto o, lo que aquí nos trae, a la operativa contractual y regulatoria del sector hotelero. Los titulares sobre modelos generativos, automatización y algoritmos predictivos se suceden a diario; sin embargo, la reflexión sobre qué significa todo ello para quien negocia un contrato de gestión hotelera, para quien despliega un *chatbot* en la recepción de un hotel o para quien debe cumplir simultáneamente con normativas de protección de datos, ciberseguridad e inteligencia artificial en múltiples jurisdicciones, resulta todavía escasa y fragmentaria.

Por ello, el Grupo de Trabajo de Turismo y Hoteles de CIIAM decidió debatir, trabajar y proponer un análisis integral que, partiendo del denominador común de la inteligencia artificial aplicada al sector, ofrezca orientación práctica a los distintos actores involucrados. En concreto, los ámbitos de trabajo se han centrado en:

1. Una mirada sectorial y estratégica sobre la adopción de la IA en el turismo y hotelería, sus principales líneas de aplicación —tanto en el *front-office* y la experiencia del huésped como en el *back-office* y las operaciones internas— y los retos que el sector afronta en materia de datos, capacidades y economía.
2. Un análisis jurídico comparado del marco regulatorio de la inteligencia artificial en la Unión Europea, Chile, México, Brasil, Colombia y Argentina, con una revisión específica del caso chileno —sus lineamientos actuales, el proyecto de ley sobre sistemas de inteligencia artificial y los vacíos normativos que persisten—, así como un estándar mínimo de buenas prácticas empresariales y autorregulación para la gobernanza digital hotelera.
3. Una propuesta de aterrizaje contractual mediante una cláusula modelo de cumplimiento y uso de inteligencia artificial en la gestión hotelera, estructurada sobre una lógica de roles, cadena de suministro y responsabilidad entre las partes, que aspira a servir como base de negociación y adaptación para contratos de gestión, operación o servicios hoteleros intensivos en tecnología.

Como en los anteriores trabajos, éste no desea ser ejemplo de nada, ni aspira a ser leído como una guía de referencia definitiva sobre la materia. Su única finalidad es la de ser el principio de un debate, ganar el reto de la hoja en blanco e inspirar en la negociación y la gobernanza de la inteligencia artificial en contratos de operación hotelera. En el fondo, es predicar con el ejemplo y pretende ser un ejercicio de responsabilidad, buscando que las reuniones del Grupo de Trabajo tengan un impacto positivo hacia la colectividad. Gracias por su lectura y consideración.

Dña. Alejandra Agud

D. David Vich Comas

Co-Presidentes del Grupo de Trabajo

III. OBJETO Y ALCANCE

El presente informe tiene por objeto exponer, de manera sistemática y articulada, los principales desafíos, oportunidades, tendencias y lineamientos asociados al uso, adopción y gobernanza de la inteligencia artificial en la industria del turismo y la hotelería. Se trata de un trabajo elaborado por el Grupo de Trabajo de Turismo y Hoteles del CIAM, con el propósito de ofrecer una visión integral sobre el impacto de estas tecnologías en el sector, así como de identificar criterios, buenas prácticas y recomendaciones útiles para los distintos actores involucrados.

En cuanto a su alcance, el informe aborda la aplicación de herramientas de inteligencia artificial en ámbitos tales como la experiencia del cliente, la personalización de servicios, la eficiencia operativa, la analítica de datos, la comercialización, la gestión reputacional, la ciberseguridad, el cumplimiento normativo y la gobernanza tecnológica. Asimismo, examina los principales riesgos jurídicos, éticos, regulatorios y operacionales asociados a su implementación, proponiendo orientaciones para una adopción responsable, segura y alineada con los objetivos estratégicos de la industria.

Con ese propósito, el documento combina una mirada sectorial y estratégica sobre la adopción de la IA, un análisis jurídico comparado, una revisión específica del caso chileno, un estándar mínimo de buenas prácticas empresariales y una propuesta de aterrizaje contractual mediante una cláusula modelo para la gestión hotelera.

IV. LA IA EN TURISMO Y HOTELERÍA: TRANSFORMACIÓN, APLICACIONES Y RETOS

1. LA IA COMO MOTOR DE TRANSFORMACIÓN PRODUCTIVA EN EL SECTOR

Durante los últimos años, la inteligencia artificial se ha consolidado como uno de los ejes centrales de la transformación productiva a escala global¹. Más que una tecnología emergente, constituye una infraestructura que reconfigura la manera en que las organizaciones generan, procesan y aprovechan la información. Ello resulta especialmente visible en turismo y hotelería, donde la ventaja competitiva depende cada vez más de la capacidad para anticipar comportamientos, optimizar recursos y personalizar interacciones a gran escala.

La IA transforma no solo la operación diaria, sino también la estrategia de las empresas. En el plano operativo, permite automatizar tareas, reducir costos y liberar recursos para actividades de mayor valor. En el plano estratégico, al analizar grandes volúmenes de datos —historiales, patrones de búsqueda, comportamientos de reserva, clima, eventos locales y variables económicas— la IA puede anticipar escenarios futuros con una precisión que supera con creces los métodos tradicionales. Esto ofrece a las compañías una ventaja competitiva clara, habilitando decisiones más rápidas y mejor informadas sobre demanda, precios, ocupación y asignación de recursos.

En mercados altamente digitalizados como el español —donde el turismo representa uno de los pilares del PIB y del empleo—, la adopción de IA ha dejado de ser una herramienta opcional de mejora para convertirse progresivamente en una condición de competitividad. La estructura del mercado turístico, con fuerte presencia de plataformas digitales, concentración de demanda en determinados destinos y competencia internacional intensa, exige una sofisticación tecnológica creciente.

¹ KPMG (2025), *Perspectivas España 2025: IA y Transformación*, p. 4.

De acuerdo con un estudio reciente de Skift Research y McKinsey & Company (2025)², basado en encuestas a 1.002 viajeros y 86 ejecutivos del sector, el 59% de los directivos turísticos afirma que la IA ha incrementado la productividad de sus empleados, el 33% señala mejoras en la personalización y el 36% destaca un aumento en la calidad de los resultados. La mayoría de los encuestados indica que la adopción de IA ha generado, en los últimos tres años, un crecimiento anual de ingresos superior al 6% y ahorros de costes también por encima del 6%.

2. LOS TRES NIVELES DE ACTUACIÓN DE LA IA EN EL SECTOR

La IA opera en el sector turístico y hotelero a través de tres niveles interrelacionados. En un primer nivel, de automatización operativa, sustituye o complementa tareas humanas mediante sistemas que ejecutan procesos con mayor rapidez y menor margen de error, como reservas, atención primaria, inventarios, turnos de personal o mantenimiento predictivo de instalaciones, entre otros.

En un segundo nivel, de personalización de la experiencia, la IA permite evolucionar desde una oferta homogénea hacia una hiperpersonalización basada en perfiles conductuales. Mediante técnicas de aprendizaje automático, se analizan variables como el historial de consumo, las preferencias implícitas, las interacciones digitales previas, los patrones de movilidad y las valoraciones del huésped, generando recomendaciones, mejoras de categoría y ofertas individualizadas, lo cual repercute de manera directa en indicadores clave como la tasa de conversión, el *ticket* promedio, la fidelización del cliente y la reputación en línea.

El tercer nivel es el más transformador: la IA como herramienta de decisión estratégica. Gracias a modelos predictivos avanzados, es posible proyectar demanda futura, estimar elasticidad precio-demanda, identificar segmentos de mercado emergentes, anticipar el impacto de eventos externos —geopolíticos, sanitarios o climáticos— y simular distintos escenarios de inversión y expansión. En este plano, la IA deja de ser solo una herramienta de eficiencia y pasa a convertirse en una tecnología de gobernanza corporativa.

En consecuencia, la cuestión ya no es si la IA transformará el sector, sino qué actores serán capaces de integrarla de manera estratégica, ética y conforme al marco regulatorio, y cuáles quedarán rezagados en un entorno crecientemente algorítmico.

3. UN CAMBIO DE ESCENARIO

La importancia de la IA no radica únicamente en la mejora incremental de la eficiencia. Su impacto es estructural porque altera dimensiones fundamentales del negocio: la cadena de valor, la relación con los intermediarios, la estructura de costos, la estrategia de precios, la interacción con el cliente y la gobernanza de datos.

El hotel deja de ser un mero proveedor de alojamiento para convertirse en un nodo dentro de un ecosistema digital interconectado. Los datos pasan a constituir un activo estratégico equiparable a la ubicación física o al valor de la marca. De igual modo, la frontera entre empresa tecnológica y empresa hotelera se desdibuja: la ventaja competitiva ya no depende exclusivamente de activos tangibles, sino también de las capacidades analíticas y del dominio de las infraestructuras digitales.

Así, la IA no representa una innovación marginal para el turismo y la hotelería, sino un cambio sustancial. Permite reducir la incertidumbre en un sector históricamente

² Skift Research y McKinsey & Company, *Remapping Travel with Agentic AI* (2025), p. 8.

expuesto a la volatilidad, optimizar márgenes en entornos de competencia intensa y ofrecer experiencias individualizadas a escala global.

La cuestión, por tanto, ya no es si la IA transformará el sector, sino qué actores serán capaces de integrarla de manera estratégica, ética y conforme al marco regulatorio, y cuáles quedarán rezagados en un entorno crecientemente algorítmico.

4. PRINCIPALES LÍNEAS DE APLICACIÓN EN TURISMO Y HOTELERÍA

4.1. *Front-office* y experiencia del huésped

El *front-office* constituye el espacio más visible del negocio hotelero y el punto donde se materializa la propuesta de valor. En un entorno fuertemente mediado por plataformas tecnológicas y valoraciones en línea, la experiencia del huésped repercute no solo en la satisfacción individual, sino también impacta en la demanda futura agregada. La IA permite transformar ese *front-office*, pasando de un modelo reactivo a uno predictivo y proactivo en el que la interacción con el cliente se anticipa y optimiza en tiempo real.

Una primera línea de aplicación es la personalización predictiva. A partir del historial de reservas, las preferencias implícitas, el comportamiento de navegación, las interacciones previas y los patrones de gasto, los algoritmos construyen perfiles dinámicos capaces de anticipar necesidades futuras: desde ofrecer una habitación en planta alta a un cliente que evita el ruido, hasta proponer servicios de spa o experiencias locales ajustadas a su comportamiento anterior. Ello permite desplegar estrategias de *cross-selling* y *upselling* más eficaces, reducir fricciones y elevar el ingreso por huésped³.

Una segunda línea es el uso de *chatbots* y asistentes virtuales. La atención ininterrumpida se ha convertido en un estándar competitivo, y los sistemas basados en procesamiento de lenguaje natural⁴ permiten resolver consultas frecuentes, gestionar reservas, modificar fechas o servicios, proporcionar información local y operar en múltiples idiomas⁵. El efecto operativo suele traducirse en menor carga administrativa, menores tiempos de respuesta y una mejor percepción de disponibilidad del servicio. Desde una perspectiva estratégica, los *chatbots* permiten además capturar datos adicionales sobre preferencias y comportamiento del cliente, lo que retroalimenta de forma continua los sistemas predictivos.

³ Véase Skift Research y McKinsey & Company, *Remapping Travel with Agentic AI* (2025), pp. 13-14. El informe ilustra esta capacidad con el caso de una viajera corporativa cuyo agente de IA es capaz de recordar preferencias acumuladas en múltiples interacciones —asiento de pasillo, aerolínea preferida por puntos de fidelidad, habitaciones con dos camas queen y evitación de plantas altas— y coordinar automáticamente vuelo, hotel y transporte terrestre en una única acción. Según el informe, la IA agente puede combinar datos estructurados (tarifas, horarios, registros de reserva) con datos no estructurados (reseñas, transcripciones de atención al cliente, blogs de viaje) para lograr una personalización de extremo a extremo a escala.

⁴ Los modelos basados en procesamiento de lenguaje natural pueden interpretar la intención, el contexto y el tono del usuario, superando la lógica rígida de los sistemas automatizados tradicionales.

⁵ Phocuswright, *Travel Forward: Data, Insights & Trends for 2026* (2025), disponible en <https://www.phocuswright.com/Travel-Research/Research-Updates/2026/Travel-Forward-Data-Insights-and-Trends-for-2026>. Según el estudio, el 31% de la industria está utilizando IA (chatbots o respuestas automáticas) para comunicaciones con el huésped.

Una tercera aplicación es el *revenue management* dinámico. Los modelos algorítmicos integran variables como ocupación histórica, anticipación promedio de reservas, precios de la competencia, eventos locales, factores climáticos y elasticidad de la demanda, ajustando tarifas en tiempo real para maximizar ingresos. Se trata de uno de los ámbitos con mayor impacto económico directo. El impacto documentado incluye incrementos del RevPAR de aproximadamente un 10%⁶. Según el informe de Skift y McKinsey, en el ámbito de la *menu engineering*, la IA convencional genera actualmente entre un 2% y un 5% de mejora en el beneficio neto mediante análisis básico de datos y previsión de demanda. Con la IA agente, capaz de personalizar ofertas en tiempo real e integrar sistemas de forma autónoma, dicha mejora podría alcanzar entre el 5% y el 15%⁷.

Sin embargo, la aplicación de IA en el *revenue management* dinámico es también uno de los más sensibles desde la perspectiva regulatoria y de competencia, en particular por la posibilidad de que el uso de algoritmos de fijación o ajuste automatizado (p. ej., precios o disponibilidad) termine alineando indirectamente las conductas de distintos actores del mercado, aun sin un acuerdo expreso entre ellos.

Finalmente, destacan el reconocimiento biométrico y el *check-in* automatizado. El uso de validación biométrica de identidad, llaves digitales y quioscos inteligentes reduce tiempos de espera y minimiza fricciones en un momento crítico de la experiencia del huésped⁸. Sin embargo, esta línea de innovación exige un escrutinio especialmente riguroso en materia de protección de datos personales, proporcionalidad y clasificación de riesgo del sistema utilizado.

4.2. Back-office y operaciones internas

Si bien el *front-office* concentra la visibilidad, es en las operaciones internas donde la IA genera algunos de los retornos de inversión más inmediatos y medibles. En *housekeeping*, por ejemplo, la combinación de patrones de *check-out*, duración de la estancia, tipo de huésped y sensores IoT permite optimizar rutas, prioridades y asignación de tareas, reduciendo tiempos muertos y acortando la ventana entre la salida de un huésped y la disponibilidad comercial de la habitación⁹.

⁶ Hotel Technology News, *How AI Is Reshaping Every Corner of Hotel Operations and the Guest Experience* (2025), disponible en <https://hoteltechnologynews.com/2025/02/how-ai-is-reshaping-every-corner-of-hotel-operations-and-the-guest-experience/>

⁷ Skift Research y McKinsey & Company, *Remapping Travel with Agentic AI* (2025), p. 21.

⁸ Véase Skift Research y McKinsey & Company, *Remapping Travel with Agentic AI* (2025), p. 21. Los sistemas de IA aplicados a la asignación automatizada de habitaciones generan recomendaciones que permiten ahorrar aproximadamente 30 minutos diarios al personal de recepción. Con la implementación de IA agente, capaz de ejecutar asignaciones en tiempo real, gestionar reasignaciones y comunicarse directamente con los huéspedes, el ahorro podría alcanzar entre 1 y 2 horas diarias.

⁹ Véase Skift Research y McKinsey & Company, *Remapping Travel with Agentic AI* (2025), pp. 21-22. Actualmente la IA convencional ya consigue reducir las horas de limpieza entre un 5% y un 15% mediante la agrupación de habitaciones y la programación optimizada de turnos. Sin embargo, con sistemas agénticos —capaces de asignar tareas autónomamente según la disponibilidad en tiempo real, el estado de cada habitación y la ubicación del personal de limpieza— esa reducción podría alcanzar entre el 10% y el 30%. A esto se suma la asignación automatizada de habitaciones: mientras la IA actual ahorra aproximadamente 30 minutos diarios de trabajo en recepción mediante recomendaciones básicas, la IA agéntica podría ahorrar entre

En mantenimiento, los modelos de aprendizaje automático pueden detectar patrones anormales en climatización, fontanería, ascensores o sistemas eléctricos antes de que se produzcan averías, reduciendo costos y evitando interrupciones operacionales. En alimentación y bebidas, la IA optimiza compras, predice demanda por producto y reduce desperdicio alimentario. En recursos humanos, los algoritmos de planificación integran previsiones de ocupación, eventos, estacionalidad y normativa laboral para construir turnos más eficientes. Esto resulta especialmente relevante en un sector con alta rotación de personal y costes laborales que representan un porcentaje relevante de los gastos totales.

5. RETOS DEL SECTOR: DATOS, CAPACIDADES Y ECONOMÍA

La narrativa dominante en torno a la IA suele poner el acento en su potencial transformador; sin embargo, existe una brecha significativa entre la promesa tecnológica y la adopción real. Esa distancia no responde solo a limitaciones presupuestarias, sino a obstáculos estructurales vinculados con la calidad de los datos, las capacidades organizacionales y la sostenibilidad económica del modelo. En muchos casos, el problema no reside en la ausencia de tecnología disponible, sino en la falta de condiciones habilitantes para una implementación eficiente, conforme y estratégica.

5.1. Retos de datos

La IA es tan eficaz como los datos que la alimentan. En el sector hotelero, uno de los principales problemas reside en la fragmentación de sistemas: PMS, *channel managers*, plataformas de CRM, motores de reserva, plataformas externas y soluciones contables que muchas veces carecen de interoperabilidad. Ello genera silos de información, duplica registros y reduce la coherencia de los modelos predictivos.

A esa fragmentación se suman problemas de calidad e integridad de datos: formatos inconsistentes, duplicidades, errores de carga manual e información desactualizada. Los algoritmos amplifican esos defectos; un modelo entrenado con datos sesgados o incompletos no solo será ineficiente, sino que puede generar resultados discriminatorios o económicamente perjudiciales. La gobernanza de datos, por tanto, no es un elemento accesorio, sino una condición previa para cualquier despliegue serio de IA.

5.2. Retos de capacidades

La transformación tecnológica exige una transformación organizacional paralela. La implementación efectiva de IA requiere perfiles especializados —ciencia de datos, ingeniería de sistemas, ciberseguridad, cumplimiento digital— que no siempre están disponibles, especialmente en establecimientos de menor escala. Sin liderazgo de la alta dirección, formación continua, rediseño de procesos internos y métricas precisas de desempeño tecnológico, la inversión en IA tiende a fragmentarse en proyectos aislados y de impacto limitado.

5.3. Retos económicos

La adopción de IA también enfrenta desafíos económicos relevantes. Su puesta en marcha exige inversión en licencias, integración con sistemas existentes, infraestructura, consultoría, formación y cumplimiento regulatorio. Además, los retornos suelen ser menos lineales y más difíciles de cuantificar que en inversiones

1 y 2 horas al día al ejecutar reasignaciones y comunicaciones con los huéspedes de forma autónoma.

tradicionales. A ello se suma el riesgo de dependencia respecto del proveedor tecnológico, con potencial pérdida de control sobre datos, altos costos de migración y exposición frente a fallas del servicio.

V. MARCO REGULATORIO COMPARADO

La digitalización del turismo y la hotelería avanza en América Latina en un entorno regulatorio fragmentado y con distintos niveles de madurez institucional. A diferencia de lo que ocurre en la Unión Europea —que hoy constituye el referente regulatorio más desarrollado en materia de inteligencia artificial, dentro de un ecosistema normativo más amplio que comprende, entre otros, el Reglamento General de Protección de Datos (GDPR), el Digital Services Act (DSA) y el Reglamento Europeo de Inteligencia Artificial (AI Act)—, la región no cuenta todavía con un marco uniforme, transversal y plenamente vigente sobre IA de alcance comparable.

En el caso europeo, el AI Act establece un marco armonizado y horizontal, basado en un enfoque de riesgo, que distingue entre usos prohibidos, sistemas de alto riesgo, obligaciones de transparencia y reglas específicas para modelos de propósito general, todo ello con una lógica preventiva orientada a resguardar derechos fundamentales, seguridad, transparencia y confianza en el entorno digital.

En América Latina, en cambio, el cumplimiento regulatorio aplicable a la IA se estructura principalmente a partir de normas de protección de datos personales, derecho del consumidor, ciberseguridad, comercio digital y, en ciertos casos, proyectos de ley sobre inteligencia artificial que aún no han entrado en vigor.

En este contexto, a continuación se sintetizan resumidamente los principales ejes regulatorios relevantes para el sector en la Unión Europea, Chile, México, Brasil, Colombia y Argentina, atendiendo especialmente a su impacto operativo en la actividad turística y hotelera¹⁰.

1. Unión Europea

En la Unión Europea, el marco aplicable a inteligencia artificial, datos personales y plataformas digitales se articula principalmente sobre tres normas generales: el Reglamento (UE) 2024/1689, conocido como AI Act¹¹; el Reglamento (UE) 2016/679, conocido como GDPR¹²; y el Reglamento (UE) 2022/2065, conocido como DSA¹³. El AI Act introduce un enfoque preventivo y basado en riesgos para el diseño, comercialización y uso de sistemas de IA; el GDPR establece estándares elevados de licitud, transparencia, minimización, seguridad y transferencias; y el DSA impone deberes de diligencia y transparencia a intermediarios y plataformas digitales.

Para hotelería y turismo, este triángulo regulatorio resulta especialmente relevante en biometría, videovigilancia inteligente, decisiones automatizadas sobre reservas o pagos, personalización, chatbots, publicidad segmentada y operación de OTAs o

¹⁰ Véanse los Anexos A y B.

¹¹ Unión Europea, Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, disponible en EUR-Lex.

¹² Unión Europea, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (GDPR), disponible en EUR-Lex y en el BOE.

¹³ Unión Europea, Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo (DSA), disponible en EUR-Lex y en el BOE.

marketplaces. En la práctica, el estándar europeo opera como referencia contractual y reputacional incluso para actores no europeos que utilizan proveedores, plataformas o canales de distribución vinculados a ese mercado.

Adicionalmente, en lo que respecta a los modelos de inteligencia artificial de propósito general, la Comisión Europea ha publicado instrumentos de apoyo interpretativo y de cumplimiento. Por una parte, el *“General-Purpose AI Code of Practice”*¹⁴ constituye un instrumento voluntario elaborado en un proceso multiactor para facilitar el cumplimiento de obligaciones del AI Act en materias como seguridad, transparencia y derechos de autor por parte de los proveedores de modelos de propósito general. Por otra, la Comisión ha publicado las *“Guidelines on the scope of the obligations for providers of general-purpose AI models under the AI Act”*¹⁵, orientadas a clarificar el alcance subjetivo y material de dichas obligaciones, en atención a su entrada en aplicación.

Para la industria turística y hotelera, estos instrumentos resultan relevantes en la contratación de soluciones basadas en modelos de propósito general ofrecidas por terceros, en tanto permiten orientar exigencias contractuales mínimas de documentación, transparencia y gestión de riesgos hacia proveedores tecnológicos.

2. Chile

En Chile, la normativa vigente que ordena los riesgos de datos, automatización y prácticas digitales en hotelería se organiza por capas: la Ley 19.628 sobre protección de datos personales¹⁶, la Ley 19.496 sobre protección de los derechos de los consumidores¹⁷ y la Ley 21.663, Ley Marco de Ciberseguridad¹⁸. A ello se suma la Ley 21.719, publicada en 2024¹⁹, que crea la Agencia de Protección de Datos Personales y entra en vigor el 1 de diciembre de 2026, trazando el estándar futuro de gobernanza de datos.

Aunque aún no existe una ley de inteligencia artificial vigente, el Congreso tramita un proyecto específico sobre la materia, sin perjuicio de que Chile cuenta con una Política Nacional de Inteligencia Artificial²⁰, la cual ha sido actualizada por el Decreto N°12 del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, publicado en enero de 2025²¹. En consecuencia, el cumplimiento en el sector ya exige integrar datos personales, consumo y ciberseguridad, y proyectar desde ahora los ajustes necesarios

¹⁴ Comisión Europea, *General-Purpose AI Code of Practice*, disponible en el portal oficial de la Comisión Europea sobre política digital.

¹⁵ Comisión Europea, *Guidelines for providers of general-purpose AI models*, disponible en la biblioteca oficial de la Comisión Europea.

¹⁶ Chile, Ley N° 19.628, sobre protección de la vida privada, texto disponible en LeyChile/BCN.

¹⁷ Chile, Ley N° 19.496, que establece normas sobre protección de los derechos de los consumidores, texto disponible en LeyChile/BCN.

¹⁸ Chile, Ley N° 21.663, Ley Marco de Ciberseguridad, texto disponible en LeyChile/BCN.

¹⁹ Chile, Ley N° 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, texto disponible en LeyChile/BCN.

²⁰ La Política Nacional de Inteligencia Artificial se estructura en tres ejes: factores habilitantes; desarrollo y adopción; y gobernanza y ética.

²¹ Chile, Decreto N° 12 del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, publicado el 28 de enero de 2025, texto disponible en LeyChile/BCN.

para converger hacia un régimen más exigente de transparencia, trazabilidad y supervisión humana.

3. México

En México, el cumplimiento relevante para hotelería digital se apoya principalmente en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, conocida como LFPDPPP²² y su Reglamento²³. El artículo 112 del Reglamento de la LFPDPPP cobra especial importancia cuando existen decisiones basadas en tratamiento automatizado de datos sin intervención humana valorativa, escenario típico en *scoring* antifraude, denegación automatizada de reservas o segmentación que incide en condiciones esenciales. En materia de consumidor, el marco general está contenido en la Ley Federal de Protección al Consumidor de 1992, conocida como LFPC²⁴, particularmente determinante en transparencia de precios, cargos obligatorios, publicidad y condiciones de cancelación o reembolso.

4. Brasil

Brasil cuenta con un marco particularmente estructurado para gobernar tratamientos intensivos en datos y perfiles comerciales: la Lei n.º 13.709/2018, conocida como LGPD (*Lei Geral de Proteção de Dados Pessoais*)²⁵, complementada por la Lei n.º 12.965/2014, conocida como Marco Civil da Internet o MCI²⁶, que fija reglas y principios del entorno digital, relevantes para operaciones online basadas en registros y para la interacción con plataformas; y la Lei n.º 8.078/1990, conocida como CDC (Código de Defesa do Consumidor)²⁷, que opera como límite frente a prácticas comerciales opacas o abusivas, fija un estándar robusto de licitud, transparencia, seguridad y control de prácticas comerciales automatizadas.

Para hotelería y turismo, ello impacta especialmente en personalización, marketing, *scoring* antifraude, biometría, videovigilancia inteligente, operación online y uso de estímulos conductuales en el embudo de compra.

5. Colombia

En Colombia, el marco base está dado por la Ley Estatutaria 1581 de 2012²⁸, complementada por el Decreto 1377 de 2013²⁹, que aterriza obligaciones operativas como políticas de tratamiento, deberes de información, autorizaciones, medidas de seguridad y procedimientos para consultas y reclamos. Este régimen es directamente

²² México, Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), texto disponible en el portal oficial del Gobierno de México.

²³ México, Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, incluido su artículo 112, texto disponible en la Cámara de Diputados.

²⁴ México, Ley Federal de Protección al Consumidor (LFPC), texto disponible en la Cámara de Diputados.

²⁵ Brasil, Lei n.º 13.709/2018 (*Lei Geral de Proteção de Dados Pessoais* - LGPD), texto disponible en Planalto.

²⁶ Brasil, Lei n.º 12.965/2014 (Marco Civil da Internet), texto disponible en Planalto.

²⁷ Brasil, Lei n.º 8.078/1990 (Código de Defesa do Consumidor), texto disponible en Planalto.

²⁸ Colombia, Ley Estatutaria 1581 de 2012, texto disponible en el Gestor Normativo de Función Pública.

²⁹ Colombia, Decreto 1377 de 2013, texto disponible en el Gestor Normativo de Función Pública.

aplicable a hotelería por el tratamiento masivo en sistemas de fidelización, marketing, analítica y gestión de huéspedes, así como por las transferencias a encargados tecnológicos y plataformas. Además, cuando los modelos de fraude o verificación tratan información financiera o comercial proveniente de bases de terceros, puede resultar aplicable la Ley 1266 de 2008³⁰, que regula el habeas data financiero y comercial, relevante para proveedores de screening de fraude que operan con datos de esa naturaleza.

En materia de derecho del consumidor, la norma general es la Ley 1480 de 2011³¹, conocida como Estatuto del Consumidor, que resulta crítica para exigir información suficiente y control de prácticas que generen asimetrías, especialmente en *pricing*, cargos, cancelaciones y reembolsos cuando se automatizan.

La centralidad de la Superintendencia de Industria y Comercio en datos personales y, en gran medida, en consumo, vuelve particularmente estratégico contar con políticas, evidencia y trazabilidad suficientes respecto del tratamiento y de las decisiones automatizadas.

6. Argentina

En Argentina, el eje regulatorio descansa principalmente en la Ley 25.326 de Protección de los Datos Personales y la Ley 24.240 de Defensa del Consumidor³². Aunque no exista una ley específica vigente sobre IA, el efecto regulatorio sobre automatización se produce por la vía del dato personal, las cesiones y transferencias, los deberes de seguridad y la transparencia de prácticas comerciales.

En materia de derecho del consumidor, el marco general aplicable es la Ley 24.240 de 1993³³, conocida como Ley de Defensa del Consumidor, que controla información, publicidad, cargos y condiciones, especialmente sensible en turismo por intermediación y multiplicidad de canales. En términos operativos, el punto decisivo para reducir riesgo suele estar menos en la discusión abstracta sobre la tecnología utilizada y más en la coherencia documental y contractual: finalidades claras, trazabilidad de transferencias, controles de seguridad y consistencia entre la promesa comercial y la operación automatizada.

VI. CHILE: LINEAMIENTOS ACTUALES Y VACÍOS NORMATIVOS

Chile constituye un caso paradigmático de transición regulatoria regional. La operación hotelera digital ya se encuentra disciplinada por capas normativas vigentes en materia de datos personales, consumo y ciberseguridad, pero al mismo tiempo enfrenta un proceso de densificación regulatoria derivado de la entrada en vigor de la Ley 21.719 y de la eventual aprobación del proyecto de ley sobre sistemas de inteligencia artificial.

En ese contexto, la discusión ya no gira únicamente en torno a si los programas de cumplimiento tradicionales son suficientes, sino a si el sector requiere una verdadera gobernanza digital específica capaz de integrar ética, cumplimiento normativo, gestión tecnológica y relaciones contractuales con terceros.

³⁰ Colombia, Ley 1266 de 2008, texto disponible en el Gestor Normativo de Función Pública.

³¹ Colombia, Ley 1480 de 2011 (Estatuto del Consumidor), texto disponible en el Gestor Normativo de Función Pública.

³² Argentina, Ley 25.326 de Protección de los Datos Personales, texto disponible en InfoLEG.

³³ Argentina, Ley 24.240 de Defensa del Consumidor, texto disponible en InfoLEG.

1. Revisión del Proyecto de Ley que regula los Sistemas de Inteligencia Artificial

1.1. Objeto, justificación normativa y ámbito de aplicación

El proyecto, contenido en el Boletín N°16.821-19, refundido con Boletín N°15.869-19³⁴, declara como finalidad regular los usos de sistemas de inteligencia artificial equilibrando el fomento de la innovación con la protección de derechos fundamentales, promoviendo un despliegue responsable y alineado con el Estado de Derecho. Esta formulación no es meramente programática: introduce un estándar interpretativo que, previsiblemente, orientará tanto la fiscalización administrativa como la construcción de criterios jurisprudenciales, especialmente en materias que el texto formula con conceptos abiertos, tales como “riesgo significativo” y el alcance operacional de la “supervisión humana”.

Su ámbito de aplicación es amplio e incluye hipótesis de extraterritorialidad, sujetando no solo a proveedores e implementadores domiciliados en Chile, sino también a proveedores o implementadores extranjeros cuando los resultados del sistema se utilicen en el país.

1.2. Definiciones y roles en la cadena de suministro

El texto incorpora definiciones clave —sistema de inteligencia artificial, proveedor, implementador, sistema de uso general, identificación biométrica, riesgo significativo, entre otras— con el propósito de distribuir obligaciones a lo largo de toda la cadena de valor. Esta lógica resulta especialmente exigente en industrias como la hotelería, donde buena parte de la tecnología se adquiere a proveedores internacionales bajo modalidad de *software* como servicio, lo que puede desplazar obligaciones hacia el implementador local incluso cuando el control del sistema y su documentación permanezcan en manos del proveedor internacional.

1.3. Principios rectores y estándar transversal de conducta

El proyecto consagra principios rectores de aplicación transversal, tales como supervisión humana, solidez y seguridad técnica, privacidad y gobernanza de datos, transparencia, diversidad, equidad social, bienestar social y medioambiental, rendición de cuentas, protección del consumidor, derechos de autor y explicabilidad. Su importancia radica en que operan como un estándar de diligencia exigible incluso más allá del cumplimiento formal de una obligación específica, y por tanto pueden orientar la fiscalización incluso cuando el cumplimiento “formal” de una obligación no neutraliza efectos materialmente lesivos o discriminatorios.

El proyecto anticipa una fiscalización que involucra a diversas entidades públicas, mencionando al Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, a la futura Agencia de Protección de Datos Personales y a la Agencia Nacional de Ciberseguridad. Ello sugiere un esquema de cumplimiento que deberá coordinar exigencias provenientes de ámbitos distintos, especialmente cuando un mismo caso de uso involucre tratamiento intensivo de datos personales y riesgos de ciberseguridad.

1.4. Modelo basado en riesgos

El eje estructural del proyecto es la clasificación de los sistemas en categorías de riesgo: riesgo inaceptable, alto riesgo, riesgo limitado y riesgo mínimo o sin riesgo evidente.

³⁴ Chile, Boletín N° 16.821-19, refundido con Boletín N° 15.869-19, proyecto de ley que regula los sistemas de inteligencia artificial, texto disponible en el Congreso Nacional.

Esta arquitectura ordena el estatuto porque define qué conductas se prohíben, qué usos se permiten bajo obligaciones estrictas y qué implementaciones quedan sujetas principalmente a transparencia. Así, en riesgo inaceptable se prohíben prácticas como la manipulación subliminal con daño, la explotación de vulnerabilidades, ciertas formas de categorización biométrica discriminatoria, el *social scoring* y determinados usos de biometría remota en tiempo real. En hotelería y turismo, estas prohibiciones pueden impactar especialmente en sistemas de seguridad basados en biometría o en prácticas de perfilamiento que terminen operando como una forma de “puntaje” de huéspedes con efectos excluyentes.

En riesgo alto se exige gobernanza reforzada durante todo el ciclo de vida del sistema. Se contemplan deberes de gestión continua de riesgos, gobernanza de datos, documentación técnica, registros de funcionamiento, supervisión humana y estándares elevados de precisión, solidez y ciberseguridad. Se prevén, además, obligaciones de reacción frente a incumplimientos, incluyendo la desactivación o retiro del sistema cuando corresponda.

En riesgo limitado, el núcleo es la transparencia frente al usuario: informar al usuario que interactúa con inteligencia artificial y asegurar identificabilidad del contenido sintético, obligaciones especialmente relevantes para *chatbots* y herramientas de generación de contenido usadas en marketing.

1.5. Sanciones y responsabilidad civil

El Proyecto estructura su régimen sancionatorio de manera coherente con el modelo de riesgos. Distingue infracciones leves, graves y gravísimas, asociando su calificación a la naturaleza del deber incumplido: las faltas de transparencia propias de sistemas de riesgo limitado tienden a calificarse como infracciones leves; el incumplimiento de obligaciones reforzadas aplicables a sistemas de alto riesgo se califica como infracción grave; y el desarrollo o utilización de sistemas o prácticas expresamente prohibidas por la categoría de riesgo inaceptable se configura como infracción gravísima. En consecuencia, la clasificación del sistema no sólo ordena los controles *ex ante*, sino que determina el “techo” de exposición sancionatoria *ex post*. En materia de multas, el proyecto contempla sanciones monetarias máximas diferenciadas por categoría, estableciendo topes de hasta 5.000 unidades tributarias mensuales para infracciones leves, de hasta 10.000 unidades tributarias mensuales para infracciones graves, y de hasta 20.000 unidades tributarias mensuales para infracciones gravísimas, y se reconoce expresamente la procedencia de responsabilidad civil por daños causados mediante sistemas de inteligencia artificial.

1.6. Mecanismos de fomento: espacios controlados de prueba y apoyo a empresas.

El proyecto incorpora instrumentos orientados a habilitar innovación bajo supervisión, creando espacios controlados de prueba, conocidos como *sandboxes*. Estos permiten experimentar y validar sistemas en condiciones reguladas, con mecanismos de supervisión y con incentivos en materia sancionatoria si se cumplen los requisitos de operación del espacio de prueba. El texto también contempla medidas de apoyo y formación, con atención a empresas de menor tamaño y organizaciones de la sociedad civil, lo que puede ser relevante en turismo por la atomización de actores, especialmente fuera de grandes cadenas hoteleras.

1.7. Convergencia con datos personales y ciberseguridad

El proyecto reconoce que la IA no puede gestionarse de forma aislada. Su despliegue converge con el régimen de protección de datos personales y con la institucionalidad

de ciberseguridad, especialmente en perfilamiento, decisiones automatizadas, evaluaciones de impacto, trazabilidad, continuidad y gestión de incidentes. En la práctica, ello obliga a construir una arquitectura de cumplimiento integrada y no compartimentos separados.

2. Análisis del Proyecto de Ley respecto de la industria del turismo y hotelería

2.1. Relevancia sectorial e impacto operativo

La industria turística y hotelera opera como un ecosistema intensivo en datos personales y dependiente de plataformas y proveedores tecnológicos. La eventual entrada en vigor del proyecto implicaría que muchas decisiones tecnológicas y comerciales pasen a requerir clasificación de riesgo, documentación, transparencia, trazabilidad y, en determinados casos, gobernanza reforzada.

2.2. Sujetos obligados y tensión contractual con proveedores internacionales

En el sector, el sujeto obligado más frecuente será el implementador, esto es, la organización que utiliza el sistema en su operación. Sin embargo, la extraterritorialidad del proyecto y la lógica de cadena de suministro generan una tensión práctica: el operador local puede quedar compelido a cumplir obligaciones que dependen de la cooperación del proveedor extranjero, como documentación técnica, registros de funcionamiento o garantías de ciberseguridad. De allí la centralidad de las cláusulas contractuales *back-to-back*, el derecho de auditoría y las obligaciones de cooperación.

2.3. Clasificación de riesgos aplicada a usos típicos del sector

Un número importante de aplicaciones sectoriales podría ubicarse en riesgo limitado, especialmente *chatbots*, asistentes virtuales y ciertas herramientas de generación de contenidos para marketing, cuyo eje es informar al usuario que interactúa con inteligencia artificial y asegurar identificabilidad del contenido generado. No obstante, incluso en estos supuestos, el cumplimiento de la obligación de transparencia que contempla el proyecto no sustituye las exigidas por el régimen de datos personales ni por el estándar de protección al consumidor, por lo que el cumplimiento debe construirse en capas y con coherencia comunicacional.

En el otro extremo, podrían aproximarse a categorías más sensibles los sistemas de *scoring* de huéspedes, las decisiones automatizadas sobre acceso a servicios o beneficios, las herramientas de seguridad con analítica avanzada y las soluciones biométricas en espacios de acceso público. En estos casos, el proyecto exige institucionalizar procesos de gestión de riesgos, supervisión humana trazable, documentación y ciberseguridad reforzada, con capacidad de auditoría.

2.4. Vacíos normativos y zonas grises

Persisten vacíos interpretativos relevantes. Entre ellos destacan la ausencia de un catálogo cerrado para determinar qué constituye “riesgo significativo”; la frontera difusa entre fidelización legítima y social *scoring* prohibido cuando la segmentación derive en exclusiones o encarecimientos o trato desfavorable basado en perfiles automatizados; y la dependencia tecnológica del sector, que unida a la extraterritorialidad regulatoria, crean una zona de riesgo estructural: la obligación jurídica puede recaer en quien no controla plenamente la tecnología ni su evidencia documental, lo que obliga a rediseñar contratos y modelos de aprovisionamiento.

Un punto adicional, especialmente sensible es la tensión derivada del uso de datos históricos para entrenamiento o mejora de sistemas, especialmente cuando hay transferencias internacionales o combinación con información de terceros.

Dado que estos vacíos se podrían revolver progresivamente mediante reglamentos y jurisprudencia administrativa y judicial, el sector deberá asumir un enfoque de cumplimiento dinámico y de actualización continua

2.5. Perfil de riesgo agregado: sanciones, responsabilidad y reputación

En hotelería, el riesgo agregado aumenta por la interacción con regímenes de datos personales, ciberseguridad y consumo, por lo que la exposición es múltiple: fiscalización, reclamos de consumidores, acciones civiles, suspensión de integraciones críticas, disrupción operativa y daño reputacional. Por ello, la clave pasa por controles preventivos, evidencia trazable, claridad contractual y capacidad real de reacción frente a incidentes o fallas del sistema.

VII. BUENAS PRÁCTICAS EMPRESARIALES Y AUTORREGULACIÓN

La autorregulación empresarial en hotelería y turismo debe comprenderse como una extensión funcional de la ética corporativa tradicional. Si bien los códigos de conducta históricos han tratado materias como integridad, trato digno, no discriminación y protección del consumidor, fueron diseñados antes de la masificación del tratamiento automatizado de datos personales y de la incorporación sistemática de sistemas algorítmicos en decisiones comerciales y operativas.

En este escenario, la ética digital y la ética algorítmica se proyectan como marcos necesarios para orientar el diseño y uso responsable de tecnologías que inciden sobre derechos, autonomía individual y bienestar social y se conecta crecientemente con obligaciones jurídicas, estándares ESG. En hotelería, ello se expresa en prácticas como *pricing* dinámico personalizado, segmentación por perfiles de consumo, priorización automatizada de reclamos y detección algorítmica de fraude.

1. Estándares internacionales como línea base sectorial

Como punto de partida, resulta recomendable que la autorregulación sectorial adopte expresamente los Principios sobre Inteligencia Artificial de la OCDE³⁵, que promueven una inteligencia artificial innovadora y confiable, centrada en el ser humano, transparente, robusta y responsable, y que han influido en desarrollos regulatorios posteriores.

A estos estándares conviene añadir la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO³⁶, como instrumento normativo global que organiza principios y políticas públicas para una inteligencia artificial alineada con derechos humanos, dignidad y supervisión humana, y las consideraciones de ONU Turismo sobre adopción de IA en turismo³⁷, en cuanto sistematiza consideraciones de adopción y riesgos operativos en turismo, útiles para orientar prácticas empresariales y exigencias a

³⁵ OECD, *OECD Principles on Artificial Intelligence* (2024).

³⁶ UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021), disponible en UNESDOC.

³⁷ UN Tourism, *Artificial Intelligence Adoption in Tourism: Key Considerations for Sector Stakeholders* (2025).

proveedores tecnológicos. Estos instrumentos permiten traducir principios generales en exigencias internas auditables.

- Identificación de finalidades legítimas y proporcionalidad del uso de modelos.
- Medidas para prevenir sesgos y efectos discriminatorios.
- Transparencia hacia el huésped cuando exista interacción automatizada o toma de decisiones relevante.
- Robustez, seguridad y trazabilidad durante todo el ciclo de vida del sistema.
- Rendición de cuentas institucional, evitando que la decisión quede atribuida a un "sistema" sin responsable.

2. Gobernanza digital hotelera: estructura, roles y convergencia con compliance y ESG

La gobernanza digital puede definirse como el conjunto de estructuras, políticas, procesos y mecanismos de control destinados a dirigir y supervisar el uso de tecnologías digitales y datos dentro de una organización, vinculando tecnología con objetivos corporativos, gestión de riesgos y rendición de cuentas. Sus elementos esenciales incluyen definición clara de roles y responsabilidades, políticas internas coherentes, mecanismos de evaluación de riesgos, supervisión y auditoría, y procesos de mejora continua. En sectores intensivos en tratamiento de datos, como la hotelería, esta gobernanza resulta instrumental para articular cumplimiento normativo, ética corporativa, seguridad y sostenibilidad reputacional.

Para que esta convergencia sea operativa, el sector debiera adoptar un esquema de tres niveles: uno estratégico, radicado en directorio y comités; uno táctico, donde confluyan cumplimiento, protección de datos, seguridad y responsables de IA; y uno operativo, compuesto por procedimientos, auditoría, gestión de incidentes, capacitación y revisión de decisiones automatizadas.

3. Instrumentos mínimos de autorregulación

Un programa mínimo de autorregulación debiera incluir, a lo menos, una política de uso responsable de inteligencia artificial aprobada por la alta dirección; un inventario de sistemas y casos de uso; una clasificación interna por nivel de riesgo; evaluaciones de impacto para usos de riesgo medio o alto; protocolos de supervisión humana; procedimientos de reclamación y revisión; y criterios de contratación y control de proveedores tecnológicos.

4. Supervisión humana y control de decisiones automatizadas relevantes.

Una exigencia transversal, especialmente relevante en turismo y hotelería, consiste en evitar automatizaciones opacas en decisiones críticas. En particular, decisiones como rechazo de reservas, bloqueo de transacciones, penalidades, restricciones de reembolso, asignación de condiciones individualizadas o priorización de reclamos no debieran quedar exclusivamente entregadas a un proceso automatizado sin instancias de revisión humana y sin vías de reclamación efectivas.

Operativamente, lo anterior exige definir responsables internos de revisión, criterios mínimos de reconsideración y estándares de trazabilidad para comprender qué variables condujeron al resultado, sin que ello implique revelar secretos comerciales. La finalidad es garantizar decisiones razonables, no arbitrarias, y reducir conflictos con

consumidores y fiscalizaciones derivadas de prácticas comerciales percibidas como injustas u opacas.

5. Transparencia y deberes frente al consumidor

En turismo, una fracción relevante de los problemas se suscitan en controversias de consumo: información insuficiente, publicidad engañosa, cargos obligatorios no transparentados, condiciones de cancelación opacas o atención automatizada ineficaz. Por ello, la autorregulación debe exigir consistencia documental entre el sitio o aplicación, los términos y condiciones, las comunicaciones comerciales, la postventa y los canales de atención.

6. Gestión de terceros, auditoría y evidencia

La hotelería digital depende estructuralmente de terceros: PMS, CRM, *channel managers*, OTAs, pasarelas de pago, servicios antifraude, *contact centers* y nube. Esto multiplica flujos y copias de datos, y difumina responsabilidades si no existe una gobernanza contractual robusta. En consecuencia, la autorregulación debe incluir diligencia debida previa, definición clara de roles, anexos de tratamiento de datos, reglas sobre subcontratación, transferencias internacionales, retención y borrado, compromisos de continuidad y derechos razonables de auditoría.

Finalmente, la utilidad jurídica de la autorregulación depende de la evidencia. Ello supone contar con inventarios de sistemas, mapas de datos, registros de actividades de tratamiento, versiones de avisos y términos, procedimientos de revisión humana, bitácoras de incidentes, pruebas de restauración y documentación contractual suficiente. Sin evidencia, el cumplimiento no es auditable.

VIII. GESTIÓN CONTRACTUAL, CADENA DE SUMINISTRO Y RESOLUCIÓN DE CONTROVERSIAS

1. El ecosistema de terceros como punto duro del sector

En turismo y hotelería, la mayoría de los casos de uso de IA y de datos personales no operan dentro de un único sistema ni bajo el control exclusivo de un solo actor. La operación digital típica se sostiene sobre una arquitectura distribuida: PMS, CRM, *channel manager*, OTAs, *marketplaces*, pasarelas de pago, servicios antifraude, *contact centers*, herramientas de analítica y servicios en la nube. En ese ecosistema, la IA suele aparecer “integrada”, pero el riesgo regulatorio y operativo raramente se origina en el modelo por sí mismo; se concentra, más bien, en la circulación y replicación de datos, la opacidad de roles y la falta de trazabilidad sobre la cadena de subcontratación.

El primer problema recurrente es la falta de claridad sobre roles. Cuando no se distingue si un proveedor procesa datos por cuenta del hotel o si actúa como un tercero que define fines propios, surgen brechas estructurales: contratos sin anexos de tratamiento, cláusulas de seguridad genéricas, ausencia de compromisos de borrado y responsabilidad diluida ante incidentes. El segundo problema es la proliferación de copias y ambientes paralelos —logs, respaldos, repositorios, entornos de prueba o *staging*— que multiplican el riesgo de exposición. El tercero es la gestión de incidentes y continuidad: si el contrato no fija plazos, cooperación forense, acceso a evidencias y compromisos de restauración, el operador queda sin capacidad real de contener el daño.

2. Checklist mínimo multi-país para uso de IA y datos personales

Para operar IA y datos personales con bajo riesgo regulatorio en un entorno multi-país, el objetivo no es construir un manual infinito, sino establecer un estándar mínimo verificable que sirva tanto para auditoría como para operación diaria. Ese estándar debiera cubrir, al menos, los siguientes componentes:

- Inventario de casos de uso y sistemas que incorporan IA o automatización relevante.
- Mapa de datos o registro de actividades de tratamiento, con origen, finalidad, retención y transferencias.
- Textos de transparencia coherentes a lo largo del *funnel* de compra, contratación y postventa.
- Gobernanza de decisiones automatizadas con efectos relevantes, incluyendo revisión humana y canal de reconsideración.
- Paquete mínimo de gobernanza para terceros críticos: tratamiento de datos, seguridad, continuidad, subprocesadores, borrado y evidencia de controles.
- Capacidades transversales de seguridad, continuidad y prueba de restauración.
- Evidencia suficiente para auditoría y para defensa frente a reclamos regulatorios o contractuales.

3. Riesgos de litigiosidad y responsabilidad civil

La incorporación de IA en hotelería no solo transforma las operaciones y la experiencia del cliente, sino que introduce nuevas fuentes de litigiosidad. Los modelos de *pricing* dinámico o segmentación conductual pueden generar, inadvertidamente, diferencias de trato basadas en edad, nacionalidad, género o perfil de gasto, configurando supuestos de discriminación algorítmica. Las cancelaciones automáticas, bloqueos de reservas, restricciones de reembolso o decisiones de *scoring* sin intervención humana suficiente pueden dar lugar a responsabilidad contractual o extracontractual.

A ello se añaden vulnerabilidades contractuales derivadas de fallos de *software*, duplicidad de reservas, errores de disponibilidad, *overbooking* algorítmico, interrupciones operativas, ambigüedad sobre la propiedad de los datos generados por los sistemas o incumplimientos de niveles de servicio. El riesgo se agrava cuando los contratos carecen de cláusulas específicas sobre responsabilidad frente a decisiones automatizadas, cumplimiento normativo, escalamiento técnico, supervisión humana o cooperación ante incidentes.

4. Arbitraje comercial como mecanismo idóneo

La complejidad técnica y el carácter transfronterizo de estos conflictos hacen del arbitraje comercial un mecanismo especialmente idóneo para su resolución. La denominada prueba digital especializada —peritajes sobre algoritmos, trazabilidad de datos, registros de decisiones automatizadas, ciberseguridad y continuidad— exige procedimientos flexibles y árbitros con conocimientos suficientes en tecnología y contratación compleja. Además, la presencia de proveedores SaaS, plataformas globales e intermediarios internacionales favorece la conveniencia de un foro neutral.

Con todo, el análisis debe diferenciar según la naturaleza de la relación jurídica comprometida. Cuando se trata de reclamos de consumidores o huéspedes, la utilidad

de la IA puede manifestarse sobre todo en mecanismos de prevención y solución temprana de controversias, como sistemas de detección de reclamos, compensaciones automatizadas u otros esquemas de *online dispute resolution*. Sin embargo, en este ámbito tales mecanismos deben diseñarse con cautela, como vías complementarias de gestión y no como instrumentos que restrinjan, dificulten o sustituyan indebidamente el acceso del consumidor a los tribunales u otros remedios que le confiere la ley.

En España, por ejemplo, la Ley 7/2017 sobre resolución alternativa de litigios de consumo exige, para que un procedimiento con decisión vinculante obligue al consumidor, la existencia de un acuerdo posterior al surgimiento del litigio y la aceptación expresa e informada de sus efectos; además, incluso en supuestos de participación obligatoria, la decisión vinculante no puede impedir el acceso a la vía judicial. Asimismo, en el ordenamiento chileno estos mecanismos no pueden diseñarse como sustitutos obligatorios ni como renunciaciones anticipadas al acceso a la justicia. Por el contrario, la Ley N.º 19.496 reconoce al consumidor el derecho a acudir siempre al tribunal competente, declara ineficaz toda estipulación en contrario y permite someter la controversia a mediación, conciliación o arbitraje solo una vez surgido el conflicto, por voluntad expresa y escrita del consumidor.

En consecuencia, tratándose de controversias B2C en turismo y hotelería, el arbitraje o los sistemas de resolución apoyados en IA debieran concebirse, por regla general, como mecanismos voluntarios, complementarios y posteriores al conflicto, orientados a facilitar soluciones rápidas, pero sin desplazar ni restringir los remedios judiciales que la ley confiere al consumidor.

Distinto es el caso de las disputas entre propietario, operador y/o proveedores tecnológicos, donde existe mayor simetría entre las partes y, por ende, un margen mucho más amplio para distribuir riesgos y pactar mecanismos privados de solución de controversias. En este plano B2B, el arbitraje aparece como una herramienta particularmente adecuada, no solo por la neutralidad del foro y la especialización técnica de los árbitros, sino también porque permite articular remedios procesales y contractuales ajustados a la realidad del negocio: cláusulas escalonadas de negociación y mediación previa, peritajes técnicos, determinaciones por experto, medidas conservativas urgentes, deberes reforzados de conservación y exhibición de logs o evidencias digitales, y reglas específicas sobre auditoría, continuidad operacional y cooperación frente a incidentes. En este ámbito, la IA no solo puede ser objeto del litigio, sino también un medio útil para su administración y esclarecimiento, siempre bajo supervisión humana y con resguardo de las garantías básicas del debido proceso.

5. Aterrizaje contractual: cláusula modelo de cumplimiento y uso de IA

Como mecanismo de aterrizaje contractual, este documento incorpora en el **Anexo C** una cláusula modelo de cumplimiento y uso de inteligencia artificial en la gestión hotelera. La cláusula está estructurada sobre una lógica de roles, cadena de suministro y responsabilidad interna entre las partes, sin desconocer el régimen imperativo aplicable frente a autoridades y terceros.

En términos sustantivos, la cláusula se organiza en torno a los siguientes ejes: objeto, ámbito y principios; gobierno, roles y cadena de valor; conformidad regulatoria y clasificación de riesgos; privacidad, datos y no discriminación; seguridad y continuidad; gestión de incidentes y notificaciones; propiedad intelectual y uso de contenidos; tratamiento de casos sensibles; auditoría, formación y evidencia; responsabilidades, garantías e indemnidades; y coordinación con el resto del contrato. Su función práctica

es servir como base de negociación y adaptación para contratos de gestión, operación o servicios hoteleros intensivos en tecnología.

IX. CONCLUSIONES

La transformación digital de la hotelería y el turismo ha convertido al sector en un modelo de negocio intensivo en tratamiento de datos personales y automatización, con impacto directo tanto en la experiencia del huésped como en la operación. La IA ya no constituye una innovación marginal, sino un factor estructural de competitividad.

El derecho comparado muestra que, mientras la Unión Europea ha construido un marco integrado y basado en riesgos, América Latina avanza en un entorno más fragmentado y con madurez institucional dispar. Esa diferencia refuerza la importancia de adoptar políticas internas comunes y verificables que permitan operar con un estándar razonable de diligencia en múltiples jurisdicciones.

Chile aparece como un caso especialmente relevante de transición regulatoria. La coexistencia entre normativa vigente de datos personales, consumo y ciberseguridad, la entrada en vigor futura de la Ley 21.719 y la discusión legislativa sobre IA proyectan un escenario de mayor exigencia, donde la gobernanza digital específica deja de ser una opción y pasa a ser una necesidad organizacional.

En el plano sectorial, el principal riesgo no proviene solo del modelo algorítmico, sino de la cadena de suministro digital que sostiene la operación. La reducción del riesgo depende, en gran medida, de claridad documental y contractual, definición de roles, trazabilidad de flujos, controles de seguridad, disciplina de entornos y capacidad real de respuesta frente a incidentes.

La autorregulación útil para el sector no puede consistir únicamente en declaraciones de principios. Debe traducirse en instrumentos internos auditables: inventarios, clasificación de riesgos, evaluaciones de impacto, protocolos de revisión humana, criterios de contratación de terceros, manuales de incidentes y evidencia verificable.

Finalmente, la adopción responsable de inteligencia artificial en hotelería y turismo exige una aproximación convergente: estrategia de negocio, regulación, ética, gobernanza de datos, ciberseguridad y contratación deben operar como un solo sistema de gestión. Solo así la IA puede transformarse en una ventaja competitiva sostenible y no en una fuente creciente de contingencias regulatorias, contractuales y reputacionales.

ANEXO A. MATRIZ COMPARADA POR JURISDICCIÓN (NORMATIVA VIGENTE)

Unión Europea (UE)					
Eje regulatorio	Norma vigente	Materias que aborda	Limitaciones / obligaciones clave	Impacto específico en turismo y hotelería	Referencia oficial
IA (marco principal)	Reglamento de Inteligencia Artificial (UE) 2024/1689 (Artificial Intelligence Act - "AI Act")	Reglas armonizadas para puesta en el mercado y uso de IA; prohibiciones; requisitos y obligaciones para IA de alto riesgo; transparencia para ciertos usos; reglas para modelos de IA de uso general; gobernanza y vigilancia de mercado.	Entra en vigor a los 20 días desde su publicación y aplica por etapas: capítulos I-II desde el 2 de febrero de 2025; parte relevante desde el 2 de agosto de 2025; aplicación general desde el 2 de agosto de 2026. Establece sanciones administrativas pueden llegar (p. ej. por prácticas prohibidas) a 35.000.000 EUR o 7% del volumen de negocios mundial (lo que sea mayor).	Casos típicos: 1) Biometría / reconocimiento facial en accesos, check-in o seguridad; 2) Perfilamiento para precios dinámicos y personalización; 3) Selección / reclutamiento y analítica laboral; 4) Chatbots y asistentes (obligaciones de transparencia); 5) Uso de IA por OTAs / plataformas con obligaciones complementarias (ver DSA).	Texto en EUR-Lex del Reglamento (UE) 2024/1689.
Datos personales / perfilamiento	Reglamento General de Protección de Datos - Reglamento (UE) 2016/679 (GDPR)	Principios, bases legales, derechos (acceso, rectificación, cancelación o supresión, y	Relevancia alta para IA por: 1) Minimización, 2) Limitación de finalidad, 3) DPIA en tratamientos de alto riesgo, y 4) reglas sobre decisiones	Fidelización, personalización, marketing conductual, prevención de fraude, analítica de huéspedes, videovigilancia con	Texto en EUR-Lex del GDPR. / Agencia Estatal Boletín Oficial del Estado (España).

Unión Europea (UE)					
Eje regulatorio	Norma vigente	Materias que aborda	Limitaciones / obligaciones clave	Impacto específico en turismo y hotelería	Referencia oficial
Plataformas y servicios digitales	Ley de Servicios Digitales - Reglamento (UE) 2022/2065 (Digital Services Act – “DSA”)	oposición -ARCO-; y portabilidad, limitación del tratamiento y a no ser objeto de decisiones automatizadas), seguridad, transferencias internacionales, DPIA, etc.	automatizadas / perfilamiento (según interpretación y guías de autoridades).	analítica, data sharing hotel-OTA-proveedores.	Texto en EUR-Lex de DSA. / Agencia Estatal Boletín Oficial del Estado (España).
		Deberes de diligencia para intermediarios y plataformas; transparencia; gestión de riesgos (especialmente VLOPs / VLOSEs).	Impacta a OTAs / marketplaces cuando califiquen como plataforma; obligaciones de transparencia en sistemas de recomendación / ads (advertisements, es decir, anuncios publicitarios) y mitigación de riesgos sistémicos (según clasificación).	Relevante para OTAs y marketplaces de tours / experiencias: anuncios segmentados, rankings, reseñas, moderación, transparencia.	

Chile					
Eje regulatorio	Norma vigente	Materias que aborda	Limitaciones / obligaciones clave	Impacto específico en turismo y hotelería	Referencia oficial
Protección de datos personales (base)	Ley 19.628 sobre Protección de la Vida Privada (y sus modificaciones)	Tratamiento de datos personales; obligaciones y derechos del titular (según texto vigente consolidado).	El cumplimiento en IA se expresa vía: bases y/o justificación del tratamiento, proporcionalidad, seguridad, contratos con terceros, transferencias, y control de acceso interno.	Programas de fidelización, CRM, historial de consumo y preferencias, validación de identidad, marketing directo, intercambio de datos con OTAs y proveedores.	Texto en LeyChile / BCN de Ley 19.628.
Reforma / modernización (datos personales)	Ley 21.719 que Regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales	Modifica la Ley 19.628 y establece marco institucional por medio de la Agencia de Protección de Datos Personales.	Entra a regir el 01 de diciembre de 2026. Eleva exigencias y gobernanza (en particular, refuerzos institucionales) relevantes para cumplimiento de IA basada en datos personales. Contempla multas de hasta 20.000 UTM, o hasta el 2% o 4% de sus ingresos anuales del último año. Se establece la posibilidad de que los responsables de datos adopten voluntariamente un Modelo de prevención de infracciones.	Afecta gobierno de datos para personalización, analítica y automatización en operación hotelera y marketing.	Texto en LeyChile / BCN de Ley 21.719.

Chile					
Eje regulatorio	Norma vigente	Materias que aborda	Limitaciones / obligaciones clave	Impacto específico en turismo y hotelería	Referencia oficial
Ciberseguridad (marco transversal)	Ley 21.663 (Ley Marco de Ciberseguridad)	Institucionalidad y normativa general de ciberseguridad; requisitos mínimos; deberes de notificación y gestión de incidentes para sujetos obligados (según alcance legal). Se crea la Agencia Nacional de Ciberseguridad (ANCI), cuyo principal objeto es asesorar al Presidente de la República en materias propias de ciberseguridad.	Entró a regir el 1 de enero de 2025 para sus disposiciones generales y el 1 de marzo de 2025 para las normas más críticas, como la calificación de Operadores de Importancia Vital (OIV), deberes específicos de estos, y la obligación de reportar incidentes significativos, sin perjuicio de la dictación de reglamentos y demás actos administrativos que indica. Impacta al uso de IA por dependencia de proveedores, nube, integraciones y tratamiento masivo de datos; obliga a fortalecer gestión de incidentes, continuidad y controles.	Hotelería y turismo no se consideran, para efectos de esta ley, servicios esenciales y operadores de importancia vital. Sin embargo, eventual e indirectamente, podrían verse comprometidos operadores con servicios digitales críticos, integraciones PMS / CRM / channel manager, pagos, OTAs; mayor exigencia ante incidentes. (ransomware, filtraciones).	Texto en LeyChile / BCN de Ley 21.663.
Consumo (relación con clientes)	Ley 19.496 que Establece Normas sobre Protección de los Derechos de los	Derechos del consumidor; deberes de información;	Relevante para IA en publicidad, pricing, "dark patterns", términos y condiciones,	Precios dinámicos, ofertas personalizadas, cancelaciones y reembolsos	Texto en LeyChile / BCN de Ley 19.496.

Chile					
Eje regulatorio	Norma vigente	Materias que aborda	Limitaciones / obligaciones clave	Impacto específico en turismo y hotelería	Referencia oficial
	Consumidores (texto refundido, coordinado y sistematizado)	procedimientos y sanciones.	y transparencia en ofertas automatizadas.	automatizados, chatbots de atención al cliente.	
IA (No se trata de una norma vigente, sin embargo, en la preparación del presente informe se tuvo a la vista el proyecto de ley que se indica, el cual actualmente se encuentra en su segundo trámite constitucional en el Senado)	Proyecto de Ley: Regula los sistemas de inteligencia artificial	Disposiciones generales; Usos de riesgo inaceptable, alto riesgo y riesgo limitado de sistemas de inteligencia artificial; Medidas de apoyo a la innovación; y Confidencialidad, infracciones y sanciones.			Texto en Proyecto de Ley del Congreso Nacional (Boletín N°16821-19. Refundido con: N°15869-19).

México					
Eje regulatorio	Norma vigente	Materias que aborda	Limitaciones / obligaciones clave	Impacto específico en turismo y hotelería	Referencia oficial
Datos personales (sector privado)	Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)	Principios, aviso de privacidad, consentimiento, derechos ARCO, seguridad, transferencias, encargados.	Marco base para IA en empresas privadas (hoteles, OTAs, operadores): obligaciones de información, seguridad y responsabilidad por terceros.	CRM, fidelización, analítica de huéspedes, campañas segmentadas, antifraude, identidad para check-in.	Texto en Gobierno de México - LFPDPPP.
Decisiones automatizadas (regla explícita)	Reglamento de la LFPDPPP (DOF 21-12-2011)	Desarrollo operativo de obligaciones, seguridad, procedimientos, reglas específicas.	Artículo 112: Si hay tratamiento de datos en decisiones sin intervención humana valorativa, el responsable debe informar al titular; el titular puede ejercer acceso para conocer datos usados y, en su caso, rectificación para solicitar reconsideración de la decisión.	Muy relevante para: denegación automatizada de reservas, antifraude que bloquea transacciones, segmentación que excluye ofertas, priorización automática de atención / reclamos.	Texto en Cámara de Diputados de México - Reglamento LFPDPPP y Art. 112.
Consumo / prácticas comerciales	Ley Federal de Protección al Consumidor (LFPC)	Derechos del consumidor, información, publicidad, cláusulas abusivas, competencias de	Riesgo regulatorio por publicidad engañosa, condiciones opacas o ambiguas, cargos automáticos, y personalización que no	Pricing dinámico, "resort fees", upselling automatizado, chatbots de atención y reclamaciones.	Texto en Cámara de Diputados de México - LFPC.

México					
Eje regulatorio	Norma vigente	Materias que aborda	Limitaciones / obligaciones clave	Impacto específico en turismo y hotelería	Referencia oficial
		Procuraduría Federal del Consumidor (PROFECO).	respete deberes de información.		

Brasil					
Eje regulatorio	Norma vigente	Materias que aborda	Limitaciones / obligaciones clave	Impacto específico en turismo y hotelería	Referencia oficial
Datos personales	Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018)	Principios, bases legales, derechos, seguridad, transferencias, encargados, autoridad (ANPD).	Marco base para IA: gobernanza, minimización, transparencia, seguridad, gestión de terceros y proveedores y derechos del titular (incluida la lógica de decisiones cuando corresponda según interpretación y guías).	Personalización, marketing, scoring antifraude, analítica de comportamiento, biometría, videovigilancia inteligente.	Texto legal (Planalto - Lei nº 13.709/2018).
Internet y plataformas	Marco Civil da Internet (Lei nº 12.965/2014)	Principios, derechos y deberes en el uso de internet; responsabilidad y directrices.	Relevante para servicios turísticos digitales (apps / sitios), registros, gobernanza y deberes en el ecosistema online.	OTAs, apps de reservas, marketplaces y canales de atención digital integrados a IA.	Texto legal (Planalto - Lei nº 12.965/2014).
Consumo / e-commerce	Código de Defesa do Consumidor (Lei nº 8.078/1990) (y normativa relacionada)	Derechos del consumidor; prácticas abusivas; información.	Riesgo por prácticas automatizadas de pricing / ads que resulten abusivas o engañosas.	Precios dinámicos y personalización; condiciones automatizadas de cancelación; "nudges" en funnels de compra.	Texto legal (Planalto - Lei nº 8.078/1990).

Colombia					
Eje regulatorio	Norma vigente	Materias que aborda	Limitaciones / obligaciones clave	Impacto específico en turismo y hotelería	Referencia oficial
Datos personales (régimen general)	Ley Estatutaria 1581 de 2012	Disposiciones generales de protección de datos personales.	Exige autorización / bases, información, medidas de seguridad, gestión de encargados y derechos del titular (en el marco de la Superintendencia de Industria y Comercio -SIC- como autoridad).	Programas de fidelización, analítica de huéspedes, perfiles de consumo, marketing y transferencias con OTAs / proveedores.	Texto en Gestor Normativo de Función Pública - Ley 1581.
Reglamentación sobre protección de datos personales	Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 (aspectos operativos).	Reglas operativas de tratamiento y cumplimiento; relevante para contratos y flujos con terceros y políticas.	Estandarización de avisos, autorizaciones y procedimientos para operaciones con terceros.	Texto en Gestor Normativo de Función Pública - Decreto 1377.
Habeas data financiero / comercial	Ley 1266 de 2008	Régimen de habeas data para información financiera, crediticia, comercial y de servicios.	Puede incidir en modelos de IA que consuman fuentes crediticias o comerciales (p. ej., antifraude, garantías, depósitos).	Screening de fraude, garantías y depósitos, evaluación de riesgo de transacción (según uso de fuentes).	Texto en Gestor Normativo de Función Pública - Ley 1266.
Consumo	Ley 1480 de 2011 (Estatuto del Consumidor)	Derechos del consumidor y obligaciones de	Relevante para ofertas y decisiones automatizadas que afecten información, publicidad y condiciones.	Pricing dinámico, condiciones de cancelación y reembolso,	Texto en Gestor Normativo de Función Pública - Ley 1480.

Colombia

Eje regulatorio	Norma vigente	Materias que aborda	Limitaciones / obligaciones clave	Impacto específico en turismo y hotelería	Referencia oficial
		productores y proveedores.		atención automatizada de quejas.	

Argentina

Eje regulatorio	Norma vigente	Materias que aborda	Limitaciones / obligaciones clave	Impacto específico en turismo y hotelería	Referencia oficial
Datos personales (base)	Ley 25.326 (Protección de los Datos Personales)	Principios generales relativos a la protección de datos; derechos de los titulares de datos; usuarios y responsables de archivos, registros y bancos de datos; control; sanciones; y acción de protección de los datos personales.	Marco base para IA: finalidad, calidad de datos, seguridad, cesiones y transferencias, derechos del titular y cumplimiento documental.	Fidelización, CRM, perfiles de consumo, analítica de huéspedes, campañas segmentadas, intercambio hotel-OTA-proveedores.	Texto en InfoLEG - Ley 25.326.
Consumo	Ley 24.240 (Defensa del Consumidor)	Normas de protección y defensa de los consumidores;	Riesgo por automatización de ofertas y publicidad; cargos y condiciones no	Pricing dinámico, fees, upselling automatizado,	Texto en InfoLEG - Ley 24.240.

Argentina					
Eje regulatorio	Norma vigente	Materias que aborda	Limitaciones / obligaciones clave	Impacto específico en turismo y hotelería	Referencia oficial
		autoridad aplicación; procedimiento sanciones.	de informadas; abusivas. y	prácticas chatbots para reclamos y devoluciones.	

ANEXO B. MATRIZ OPERATIVA POR CASO DE USO TÍPICO EN TURISMO Y HOTELERÍA

La siguiente matriz identifica el foco principal de cumplimiento por caso de uso de IA y/o datos personales en cada una de las legislaciones revisadas.

Caso de uso de IA y/o datos personales en turismo / hotelería	UE	Chile	México	Brasil	Colombia	Argentina
Check-in biométrico / reconocimiento facial	Alto riesgo potencial y/o prohibiciones según contexto; además aplica RGPD (datos biométricos) y exigencias de transparencia. AI Act tiene vigencia diferida.	Aplica principalmente normativa sobre datos personales (Ley 19.628 y reformas) y ciberseguridad.	LFPDPPP (datos sensibles, aviso / consentimiento según cada caso) y seguridad; especial cuidado por tratamiento intensivo.	LGPD (biométricos como datos sensibles) y gobernanza.	Ley 1581 y Decreto 1377 (autorización, seguridad; datos sensibles).	Ley 25.326 (calidad, finalidad, consentimiento según estructura del tratamiento; seguridad).
Precios dinámicos y personalización por perfil (IA / ML)	RGPD (perfilamiento), reglas de consumo; aplica DSA si es plataforma (OTAs).	Ley 19.496 y Ley 19.628 sobre datos personales.	LFPC (publicidad y condiciones), y aplica LFPDPPP si hay perfilamiento con datos personales.	Código de Defensa del Consumidor y LGPD (transparencia y derechos).	Estatuto del Consumidor y Ley 1581.	Ley 24.240 y Ley 25.326.

Caso de uso de IA y/o datos personales en turismo / hotelería	UE	Chile	México	Brasil	Colombia	Argentina
Antifraude / denegación automática de transacciones o reservas	RGPD (según diseño) y AI Act si califica como alto riesgo por ámbito / uso; obligaciones de transparencia y gestión.	Aplica principalmente normativa sobre datos personales (Ley 19.628 y reformas) y ciberseguridad.	Regla explícita: Art. 112 del Reglamento LFPDPPP (informar decisión automatizada; acceso / rectificación para reconsideración).	LGPD (derechos / transparencia) y gestión de seguridad.	Ley 1581 (derechos; procedimientos) y, si se usa data crediticia o comercial, aplica Ley 1266.	Ley 25.326 (calidad / actualización; derechos) y aplica Ley 24.240 si afecta al consumidor.
Chatbots / voicebots para atención y ventas	AI Act: transparencia para ciertos sistemas; aplica RGPD si tratan datos; y aplica DSA si se utiliza plataforma.	Aplica normativa de derecho del consumidor (información veraz; no inducir a error) y de datos personales.	Aplica normativa de derecho del consumidor y datos personales; cuidado con grabaciones y análisis.	Aplica normativa de derecho del consumidor, LGPD, y Marco Civil si se trata de servicio online intensivo.	Aplica normativa de derecho del consumidor y Ley 1581 junto con Decreto 1377.	Aplica normativa de derecho del consumidor y Ley 25.326.
IA para RR.HH. (reclutamiento, turnos, scoring de desempeño)	Puede calificar como alto riesgo bajo AI Act (ámbito laboral) y RGPD	Datos personales y laboral (riesgo reputacional y de cumplimiento	Datos personales; además trazabilidad de decisiones automatizadas	LGPD (bases, transparencia y seguridad) y controles internos.	Ley 1581 y Decreto 1377 (autorización, finalidad, seguridad).	Ley 25.326 (finalidad/calidad; seguridad; derechos).

Caso de uso de IA y/o datos personales en turismo / hotelería	UE	Chile	México	Brasil	Colombia	Argentina
	(datos, evaluaciones).	por tratamiento intensivo).	si aplicara Art. 112 cuando el proceso sea sin intervención humana valorativa.			

ANEXO C. CLÁUSULA MODELO DE CUMPLIMIENTO Y USO DE INTELIGENCIA ARTIFICIAL

1. Objeto, ámbito y principios

- 1.1. La presente cláusula regula el diseño, aprovisionamiento, integración, despliegue, uso, supervisión y retiro de sistemas de inteligencia artificial ("IA") y de modelos de IA de propósito general ("GPAI") empleados en la operación y gestión del Hotel, incluyendo, a título enunciativo, herramientas de atención al cliente, recomendación y personalización, fijación dinámica de precios, marketing y generación de contenidos, análisis de demanda, mantenimiento predictivo, prevención de fraude, gestión de quejas, y cualesquiera otros casos de uso análogos en el ámbito hotelero.
- 1.2. El GESTOR utilizará la IA exclusivamente para la mejor prestación de los servicios que le correspondan como gestor, dentro del ámbito, alcance y fines del Contrato, sin emplearla para finalidades ajenas o incompatibles, ni para beneficiar directa o indirectamente a otros establecimientos hoteleros salvo en la medida permitida en esta cláusula mediante datos agregados o debidamente desidentificados.
- 1.3. A los efectos de esta cláusula, conceptos como "Proveedor", "Responsable del Despliegue", "Modelo de IA de uso general", "Sistema de IA de uso general", "Incidente grave", "Sistema de IA de alto riesgo" u otros conceptos específicos sobre la materia, tendrán el significado que les confiere el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 *por el que se establecen normas armonizadas en materia de inteligencia artificial ("Reglamento UE IA")*, según se modifiquen, desarrollen o sustituyan por normas posteriores, actos de ejecución o directrices interpretativas aplicables

Sin perjuicio de lo anterior, cualquier cambio normativo o interpretativo posterior que altere de forma sustancial la distribución de obligaciones, riesgos, responsabilidades o cargas entre las Partes de tal forma que modifique materialmente el equilibrio del Contrato, no se aplicará automáticamente. En tal caso, las Partes se comprometen a negociar de buena fe las modificaciones contractuales estrictamente necesarias a fin de (i) asegurar el cumplimiento de la normativa vigente y (ii) preservar, en la medida de lo legalmente posible, el equilibrio económico y de riesgos originalmente pactado. Hasta que dichas modificaciones se acuerden por escrito, cada Parte seguirá cumpliendo sus obligaciones contractuales vigentes en la medida en que no contradigan la normativa aplicable y adoptará las medidas razonables necesarias para mitigar impactos regulatorios inmediatos.

- 1.4. Las Partes se obligan a garantizar que todos los sistemas de IA se ajustan a los principios de legalidad, necesidad y proporcionalidad, seguridad, privacidad y protección de datos, transparencia y trazabilidad, supervisión humana efectiva, no discriminación y accesibilidad. Las Partes evitarán prácticas prohibidas y mitigarán riesgos para la salud, la seguridad y los derechos fundamentales.
- 1.5. Esta cláusula se interpretará y aplicará conforme al Reglamento UE IA y, en lo que corresponda, conforme al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*.
- 1.6. Nada de lo dispuesto en el Contrato limitará, excluirá o alterará el régimen de responsabilidades que, frente a las autoridades competentes y a terceros, corresponda a cada Parte en su calidad de Proveedor o de Responsable del Despliegue, conforme a la

normativa imperativa, incluyendo, en particular, los requisitos para sistemas de alto riesgo, las prohibiciones de prácticas de IA y los deberes de vigilancia, suspensión y notificación de incidentes graves a autoridades competentes cuando proceda. Sin perjuicio de lo anterior, las Partes acuerdan que, en el marco de su relación contractual, podrán distribuir entre sí los riesgos, cargas y responsabilidades derivados del uso, implementación y despliegue de sistemas de IA de un modo distinto al previsto por la normativa aplicable, exclusivamente con efectos internos entre ellas. En consecuencia, dicha distribución contractual no afectará la responsabilidad de cada Parte frente a autoridades o terceros, pero sí dará lugar, entre las Partes, a las correspondientes acciones de indemnización, reembolso y/o repetición, conforme a lo pactado en el Contrato. Las Partes cooperarán de buena fe para permitir el cumplimiento de dichas obligaciones y adoptarán sin demora las medidas correctoras necesarias.

2. Gobierno, roles y cadena de valor

2.1. Salvo pacto escrito en contrario:

- a) El GESTOR actuará como Responsable del Despliegue respecto de los sistemas de IA utilizados en la operativa diaria del Hotel que él mismo administre, incluyendo aquellos sistemas integrados tanto en las plataformas del GESTOR como en las del Hotel; en este último caso cuando su utilización se refiera o esté vinculada, directa o indirectamente, a uno de sus servicios o áreas bajo su control y supervisión.
- b) El HOTELERO actuará como Responsable del Despliegue respecto de los sistemas de IA que utilice directamente, o instruya a utilizar a terceros bajo su autoridad, en el Hotel y que no se refieran a áreas bajo el control y supervisión del GESTOR.
- c) Quien modifique sustancialmente un sistema de IA o altere su finalidad prevista asume, en su caso, las obligaciones del Proveedor según la normativa aplicable, y garantizará la evaluación de conformidad y/o registro que proceda antes de su puesta en servicio.

2.2. El Responsable del Despliegue se obliga a celebrar y mantener vigentes, con todos los terceros que suministren componentes, herramientas, servicios o procesos de inteligencia artificial que se encuentren directa o indirectamente vinculados con la operación del Hotel, contratos de servicios u otros instrumentos jurídicos vinculantes que impongan a dichos terceros las obligaciones necesarias y suficientes para permitir el cumplimiento íntegro y oportuno del Reglamento (UE) sobre Inteligencia Artificial y demás normativa aplicable

2.3. Cuando un sistema de IA sea utilizado conjuntamente por HOTELERO y GESTOR, ambas Partes coordinarán sus obligaciones como Responsables del Despliegue y, en su caso, dejando constancia previamente por escrito de la asignación de responsabilidades, interfaces y flujos de información.

Para cada Sistema de IA identificado en el Inventario, las Partes formalizarán un Acuerdo de Asignación de Responsabilidades ("**Acuerdo de Asignación de Responsabilidades**" o "**AAR**") en el formato del **Anexo 1**, que contendrá, como mínimo: (i) identificación del sistema y alcance; (ii) roles regulatorios y contractuales; (iii) matriz RACI (*Responsible, Accountable, Consulted, Informed*) y (iv) aspectos de privacidad y datos.

El AAR se elaborará con enfoque proporcionado al nivel de riesgo del sistema. Cualquier modificación sustancial del sistema o de su finalidad exigirá actualizar el AAR con antelación razonable a su puesta en servicio. En caso de discrepancia entre el AAR y el

presente Contrato, prevalecerá este último; y, en todo caso, el AAR no limitará ni desplazará obligaciones imperativas establecidas por la normativa aplicable.

- 2.4. Las Partes confirman su compromiso con un uso de la IA que contribuya, cuando sea técnica y económicamente viable, a la mejora de la eficiencia operativa y ambiental del Hotel y su interacción con su entorno físico y social, en línea con principios internacionalmente reconocidos de IA responsable³⁸. Sin perjuicio de las obligaciones imperativas y del resto de prioridades de cumplimiento, las Partes:
- a) Integrarán, en la medida razonable, criterios de sostenibilidad en la evaluación y selección de Sistemas de IA, priorizando soluciones que documenten prácticas de eficiencia energética, información sobre consumo de recursos y, cuando sea posible, opciones de despliegue en infraestructuras con eficiencia energética acreditada.
 - b) Garantizarán que la implementación de prácticas de eficiencia no compromete la seguridad, la transparencia, la supervisión humana ni los derechos de clientes, personas trabajadoras o terceros, y que cualquier tratamiento de datos personales necesario para medir o lograr tales eficiencias cumple la normativa aplicable y, cuando proceda, está cubierto por la DPIA correspondiente.

Este compromiso no constituye una obligación de resultado y su cumplimiento se realizará con criterios de proporcionalidad, sin afectar a los niveles de servicio pactados ni al reparto de responsabilidades legales.

- 2.5. Ninguna Parte podrá usar sistemas de IA, ni los datos o resultados derivados de su operación en el Hotel, para fines distintos de la ejecución del Contrato, salvo (i) obligación legal, (ii) autorización previa y por escrito de la otra Parte, (iii) análisis y *benchmarking* sectorial; (iv) desarrollo de nuevos productos o (v) uso interno para mejora de modelos. En todo caso, los usos permitidos deberán realizarse siempre mediante datos agregados y/o desidentificados conforme a la cláusula 7.4.
- 2.6. El Responsable del Despliegue sólo integrará modelos GPAI o sistemas de IA de terceros cuyos proveedores faciliten la documentación técnica y la información para integradores requerida por la normativa aplicable, incluyendo la relativa a capacidades, limitaciones, datos de entrenamiento (resumen público en su caso), parámetros de rendimiento, riesgos y salvaguardas.
- 2.7. El Responsable del Despliegue notificará a la otra Parte, con una antelación razonable y en todo caso antes de la puesta en servicio, cualquier despliegue inicial o cambio sustancial de un sistema de IA que pueda razonablemente afectar de forma material a clientes, empleados, seguridad del Hotel, imagen de marca o cumplimiento regulatorio. La notificación incluirá, al menos, la finalidad, clasificación de riesgo, principales salvaguardas, requisitos de transparencia al usuario y, cuando proceda, resultados resumidos de pruebas y evaluaciones de impacto.
- 2.8. El Responsable del Despliegue deberá disponer, y mantener actualizado, un inventario y matriz de riesgos de los sistemas de IA utilizados para la operación y gestión del Hotel, sus

³⁸ NOTA: *vid.*, entre otros, *OECD AI Principles* y *UNESCO Recommendation on the Ethics of Artificial Intelligence*

casos de uso, clasificación de riesgo, versión y proveedor, así como las medidas de control aplicadas; todo ello en forma razonable, proporcionada al tipo de sistema y al nivel de riesgo, evitando duplicidades con la documentación del proveedor y pudiéndose apoyar en plantillas y anexos normalizados (en “**Inventario**” y “**Matriz de Riesgos**”).

El inventario del GESTOR será accesible al HOTELERO a solicitud razonable y viceversa, con salvaguarda de la información confidencial.

Las Partes adjuntan como **Anexo 2.1** el formato de inventario y matriz de riesgos, y como **Anexo 2.2**, un formato simplificado para supuestos de no “alto riesgo”.

El Inventario y la Matriz de Riesgos tendrán carácter obligatorio y se actualizarán con las siguientes cadencias mínimas: (i) con periodicidad mensual para Sistemas de alto riesgo y para Sistemas de Alto Impacto; y (ii) con periodicidad trimestral para el resto de sistemas. A estos efectos, se entenderá por ‘Sistema de Alto Impacto’ aquel que, sin ser necesariamente de alto riesgo según el Reglamento (UE) 2024/1689, pueda afectar de forma material a clientes, trabajadores, seguridad del Hotel, imagen de marca o cumplimiento regulatorio.

- 2.9. Antes de integrar proveedores críticos de GPAI o de funciones de alto impacto, el Responsable del Despliegue informará a la otra Parte, en la medida razonablemente disponible y sin divulgar información confidencial del proveedor, sobre los criterios de selección, las garantías de cumplimiento del proveedor y los acuerdos de nivel de servicio relevantes. Esta información no retrasará indebidamente decisiones de aprovisionamiento urgentes y podrá satisfacerse mediante referencias a documentación pública o certificaciones del proveedor.
- 2.10. Cuando el GESTOR o el HOTELERO subcontraten servicios vinculados a IA, impondrán contractualmente obligaciones equivalentes a las previstas en esta cláusula, incluyendo el cumplimiento del Reglamento UE IA y la normativa aplicable en materia de protección de datos. La Parte que subcontrate seguirá siendo responsable frente a la otra por la actuación del subcontratista en el ámbito de los servicios.
- 2.11. Cuando un despliegue impacte en condiciones laborales o requiera medidas de información o consulta a trabajadores, los costes razonables asociados a dichas obligaciones regulatorias y a la supervisión humana operativa serán asumidos por el empleador del personal afectado.
- 2.12. Si el HOTELERO precisa asistencia para el cumplimiento de sus obligaciones en materia de IA derivadas del Contrato o de la normativa aplicable (incluyendo, a título enunciativo, la identificación y clasificación de sistemas de IA relevantes, actualización del inventario y matriz de riesgos, o preparación de documentación de soporte), las Partes negociarán de buena fe los términos de dicha asistencia por parte del GESTOR, incluyendo su alcance, entregables, plazos y la retribución adicional correspondiente.

3. Conformidad regulatoria y matriz de cumplimiento

- 3.1. Se prohíbe expresamente cualquier práctica de IA incompatible con la normativa aplicable en general, y con el Reglamento UE IA en particular; incluidas técnicas subliminales o deliberadamente manipuladoras, explotación de vulnerabilidades por edad o discapacidad, o sistemas de puntuación social.

- 3.2. En el Hotel queda prohibida la categorización biométrica y el reconocimiento de emociones con fines comerciales o de gestión del personal, salvo que sea legalmente permitido y conforme a esta cláusula.

- 3.3. Antes del despliegue de cualquier sistema, la Parte competente clasificará su caso de uso.

En caso de sistemas de alto riesgo (v.g., sistemas que incidan en selección/gestión de personal, identificación biométrica permitida, o con efectos significativos en derechos) o con impacto potencial significativamente adverso, se documentará: finalidad prevista, datos tratados, niveles de autonomía, impacto en clientes y empleados, probabilidad y gravedad de perjuicios, y posibles sesgos, con especial atención a colectivos vulnerables. Todo ello en forma razonable, proporcionada al tipo de sistema y al nivel de riesgo, evitando duplicidades con la documentación del proveedor.

Adicionalmente, para los sistemas potencialmente “alto riesgo” se implementará un sistema de gestión de riesgos a lo largo del ciclo de vida, con revisión humana periódica, pruebas y medidas de mitigación.

Para el resto de los sistemas, la Parte competente deberá elaborar una ficha ejecutiva que contemple de forma simplificada la información mínima contenida en el Anexo IV del Reglamento UE IA, pudiendo apoyarse en documentación del proveedor para evitar duplicidades. Esta obligación de documentación podrá cumplimentarse por medio del formulario simplificado de documentación técnica aprobados por la UE o la autoridad nacional competente.

- 3.4. En los supuestos en que un sistema sea de “alto riesgo”, el Proveedor y el Responsable del Despliegue velarán por: (a) la gobernanza y calidad de datos, (b) disponer de documentación técnica completa y actualizada, (c) mantenimiento de un registro de eventos/logs y trazabilidad, (d) transparencia e Instrucciones de Uso adecuadas, (e) supervisión humana efectiva, (f) precisión, robustez y ciberseguridad adecuadas, (g) evaluación de conformidad y, en su caso, marcado CE.
- 3.5. El Responsable del Despliegue utilizará los sistemas de IA conforme a sus Instrucciones de Uso, vigilará su funcionamiento y formará al personal encargado.
- 3.6. Cuando se integren modelos GPAI, el Responsable del Despliegue exigirá al proveedor del modelo: documentación técnica precisa, información para integradores, política de cumplimiento en materia de derechos de autor (incluida la observancia de reservas de derechos), y resumen público suficiente de contenidos de entrenamiento. Si el modelo GPAI fuese clasificado con riesgo sistémico, el proveedor deberá acreditar evaluaciones, pruebas de equipos rojos, gestión de riesgos sistémicos, ciberseguridad reforzada y notificación de incidentes graves, todo ello conforme a la normativa aplicable o a los códigos de práctica comúnmente aceptados.
- 3.7. En sistemas que interactúen con personas físicas (*chatbots*, asistentes, kioscos), se informará claramente al usuario de que interactúa con IA. En contenidos sintéticos (texto, audio, imagen o vídeo) generados o manipulados por IA que puedan inducir a error (ultrasuplantaciones), se aplicarán medidas técnicas de marcación/procedencia legibles por máquina y etiquetado visible conforme a la normativa, sin perjuicio de las excepciones legalmente previstas para obras creativas.

- 3.8. El Responsable del Despliegue implementará filtros y políticas de uso aceptable para evitar que los sistemas generen o difundan contenidos ilícitos, discriminatorios, difamatorios o que vulneren derechos de terceros, con procedimientos de retirada y corrección expeditos.
- 3.9. Antes de poner en servicio un sistema de alto riesgo en el Hotel o de desplegar sistemas de IA que impacten significativamente en condiciones laborales, se informará a los trabajadores y a sus representantes y, cuando proceda, se realizará una evaluación de impacto en derechos fundamentales y/o en protección de datos.
- 3.10. El GESTOR informará al HOTELERO, de forma clara y previa a su puesta en servicio, de los sistemas de IA que afecten a la experiencia del cliente, marca, tarificación o canales de venta del Hotel, incluyendo las medidas de transparencia que se aplicarán frente a los huéspedes y las opciones de oposición cuando proceda. De forma recíproca, el HOTELERO informará al GESTOR cuando despliegue o instruya el uso de IA que impacte en procesos operados por el GESTOR.

4. Privacidad, datos y no discriminación

- 4.1. Cada Parte se obliga a cumplir la normativa de protección de datos que resulte de aplicación en cada momento. La IA se diseñará con minimización de datos, limitación de finalidad y seguridad desde el diseño. Si una funcionalidad implica tratamiento de datos personales, se evaluará la base jurídica y, cuando proceda, se efectuará una evaluación de impacto (FRIA / DPIA).

Los costes de evaluaciones de impacto (FRIA / DPIA), pruebas y controles de cumplimiento se imputarán conforme al plan de proyecto aprobado por las Partes y cualquier coste extraordinario no previsto se someterá a aprobación previa por escrito

- 4.2. Los conjuntos de datos de entrenamiento, validación y prueba (o, en su caso, los datos de entrada operativos controlados por el Responsable del Despliegue) serán pertinentes, suficientemente representativos, y, en la mayor medida posible, completos y libres de errores, con prácticas de documentación, depuración y control de sesgos.
- 4.3. El Responsable del Despliegue implementará mecanismos para ofrecer explicaciones claras y significativas del papel de la IA en decisiones que produzcan efectos jurídicos o afecten significativamente a clientes o empleados, cuando así lo exija la normativa. Se habilitarán canales para reclamaciones, revisión humana y rectificación.
- 4.4. Las Partes documentarán por escrito su respectiva condición en materia de protección de datos para cada caso de uso y firmarán los instrumentos necesarios. En todo lo relativo al tratamiento de datos personales, prevalecerán, en caso de conflicto con la presente cláusula de IA, los instrumentos de protección de datos suscritos entre las Partes, incluyendo: (i) el Acuerdo de Tratamiento de Datos (DPA) o, en su caso, el Acuerdo de Corresponsables; (ii) los anexos y mecanismos de transferencias internacionales (incluidas, cuando proceda, las Cláusulas Contractuales Tipo/IDTA y su correspondiente evaluación de impacto de transferencias –TIA–); y (iii) los Registros de Actividades de Tratamiento (ROPA) aplicables. Estos instrumentos se incorporan por referencia y regirán con carácter preferente en su ámbito material.

La puesta en producción del sistema quedará condicionada a la realización previa de la Evaluación de Impacto en Protección de Datos (DPIA) cuando sea exigible, o, en su defecto, a la documentación de la evaluación de riesgos que justifique su no necesidad

5. Seguridad y continuidad

- 5.1. Los sistemas de IA tendrán un nivel de ciberseguridad adecuado al riesgo, considerando envenenamiento de datos, ataques adversarios, inferencias, filtraciones de modelos y acceso no autorizado. Se aplicarán controles de acceso, cifrado, segmentación de redes, gestión de vulnerabilidades, registro de eventos y respuesta ante incidentes, así como se realizarán pruebas periódicas (incluido *'red teaming'* cuando proceda).
- 5.2. El Responsable del Despliegue establecerá medidas de supervisión humana, con capacidad de desactivación o parada segura del sistema en condiciones anómalas o de riesgo.
- 5.3. Los sistemas de IA que soporten procesos críticos del Hotel (p. ej., fijación de precios, asignación de habitaciones, atención al cliente 24/7) dispondrán de planes de continuidad, modos degradados o procedimientos manuales alternativos para mantener niveles mínimos de servicio en caso de caída, suspensión o retirada.
- 5.4. Las Partes acordarán métricas clave de desempeño y calidad (p. ej., precisión, latencia, tasa de errores, tasa de falsos positivos/negativos en detecciones) y umbrales de alerta. El GESTOR reportará al HOTELERO el desempeño relevante de los sistemas con una periodicidad razonable y propondrá medidas de mejora cuando se observen desviaciones materialmente adversas.
- 5.5. El GESTOR mantendrá, cuando sea razonable y proporcional, separación lógica y/o física entre entornos del Hotel y los de otros establecimientos hoteleros, evitando la mezcla no autorizada de datos y configuraciones, e implementará controles para prevenir fugas cruzadas de información o parámetros derivados.

6. Gestión de incidentes y notificaciones

- 6.1. Si el uso conforme a las Instrucciones de Uso pudiera generar un riesgo relevante, el Responsable del Despliegue suspenderá el uso y lo notificará sin demora al Proveedor afectado y a la autoridad competente cuando proceda.
- 6.2. Las Partes adoptarán un esquema de severidad con, al menos, los siguientes niveles: (i) Crítico; (ii) Alto; (iii) Medio; y (iv) Bajo. Se considerarán al menos 'Crítico' o 'Alto' los incidentes que impliquen: (a) riesgo para derechos de personas usuarias o personas trabajadoras; (b) exposición o pérdida de control de datos personales de alcance significativo; (c) potencial incumplimiento de requisitos aplicables a sistemas de alto riesgo; o (d) intrusión o vulneración relevante de seguridad.
- 6.3. Ante un incidente clasificado como Crítico o Alto, la Parte que lo detecte remitirá a la otra Parte: (a) una notificación preliminar dentro de las primeras veinticuatro (24) horas desde su detección razonable; y (b) un informe ampliado dentro de las setenta y dos (72) horas siguientes a la notificación preliminar, o antes si así lo exige la normativa aplicable. Para incidentes de severidad Media, se enviará notificación dentro de setenta y dos (72) horas y actualización en cinco (5) Días Hábiles si persiste el impacto. Los incidentes de severidad Baja se documentarán en el registro de eventos y se reportarán en el siguiente informe periódico, salvo que escalen de severidad.
- 6.4. La gestión de incidentes se coordinará con las obligaciones de notificación aplicables en materia de inteligencia artificial, protección de datos y ciberseguridad. Cuando concurren requisitos de notificación a autoridades o a interesados en virtud del RGPD, normativa de ciberseguridad o regulación sectorial, las Partes colaborarán para: (i) alinear plazos y contenidos; (ii) evitar duplicidades, pudiendo efectuar notificaciones coordinadas cuando la normativa lo permita; y (iii) designar un punto de contacto líder para cada incidente.

Lo anterior se entiende sin perjuicio de que cada Parte deba cumplir las notificaciones legales que le correspondan en su propio ámbito.

- 6.5. Se exigirá al Proveedor que coopere facilitando información técnica, acceso a registros y medidas correctoras. En todo caso el Responsable del Despliegue mantendrá registros proporcionales y conservará evidencia del uso y funcionamiento de los sistemas durante los plazos legalmente exigibles. Los registros se mantendrán en la medida exigida por la normativa y de forma proporcionada, pudiendo integrarse en herramientas existentes de registro y control del GESTOR.

7. Propiedad intelectual y contenidos

- 7.1. Los Proveedores de modelos GPAI deberán contar con políticas para cumplir la normativa aplicable en materia de derechos de autor y derechos afines.
- 7.2. Salvo pacto específico y derechos de terceros, los derechos sobre contenidos generados en el marco del Contrato pertenecerán a la Parte que haya encargado su creación y asumido su coste, con licencia a favor de la otra Parte en la medida necesaria para la ejecución del Contrato. Cada Parte garantiza que no instruirá a los sistemas para generar salidas que infrinjan derechos de terceros y que implementará salvaguardas para mitigar reproducciones no autorizadas de obras protegidas.
- 7.3. Si alguna Parte facilita datos propios para entrenar, ajustar o evaluar sistemas de IA usados en el Hotel: (i) garantizará que cuenta con la base jurídica y derechos necesarios para ello; (ii) no transferirá a la otra Parte la titularidad de dichos datos salvo pacto expreso; (iii) concederá únicamente una licencia no exclusiva para el uso estrictamente necesario para la prestación del servicio de gestión, con obligaciones de seguridad y confidencialidad equivalentes; (iv) no se permitirá su uso para beneficiar a otros establecimientos, salvo que los datos se utilicen de forma agregada y/o desidentificada de modo que no permitan la identificación, con técnicas y umbrales documentados; (v) el uso para mejora general de modelos por el GESTOR requerirá informar al HOTELERO e incorporar garantías de no reversibilidad y no extracción de información específica del Hotel; y (vi) se documentarán los conjuntos usados, finalidad, fechas y resultados principales a efectos de trazabilidad.
- 7.4. Cada Parte podrá utilizar, para entrenamiento o mejora de sus modelos propios de IA, datos agregados y/o desidentificados derivados de la ejecución del Contrato, siempre que: (i) no permitan la identificación directa ni indirecta del Hotel o de personas físicas; (ii) se apliquen técnicas documentadas de agregación/desidentificación con umbrales y pruebas de no reidentificación; (iii) se excluya información confidencial sensible del Hotel no susceptible de agregación; (iv) se respete la normativa de competencia; y (v) se prohíba su uso para beneficiar a otros establecimientos salvo en forma de modelos o *insights* agregados que no revelen información específica del Hotel.

8. Casos de uso sensibles

- 8.1. Identificación biométrica. Cualquier autenticación o verificación biométrica (p. ej., acceso a zonas restringidas) sólo se implementará cuando sea legalmente permitido, necesaria y proporcionada, con alternativas no biométricas razonables, medidas reforzadas de seguridad y evaluación de impacto previa. Queda prohibida la identificación biométrica remota “en tiempo real” en espacios de acceso público con fines comerciales, salvo los supuestos legales tasados.

- 8.2. Fijación dinámica de precios. Los algoritmos de *pricing* incorporarán salvaguardas para evitar discriminación injustificada por características protegidas. Se conservará evidencia de factores y reglas de negocio relevantes, con revisiones periódicas de sesgos.
- 8.3. Personalización y recomendación. Los motores de recomendación no realizarán perfilados que afecten desproporcionadamente a colectivos vulnerables ni condicionamientos manipuladores. El Responsable del Despliegue proporcionará información clara sobre la existencia de personalización y opciones para gestionarla.
- 8.4. Vigilancia y seguridad. Los sistemas de análisis de vídeo o audio no se usarán para reconocimiento de emociones ni categorización biométrica, salvo que concurra una base legal específica.

9. Auditoría, acceso a información y formación

- 9.1. Cada Parte permitirá auditorías razonables, con preaviso y en horario laboral, orientadas a verificar el cumplimiento de esta cláusula y de la normativa aplicable.
- 9.2. El Responsable del Despliegue garantizará que el personal que opere sistemas de IA recibe formación adecuada en alfabetización en IA, seguridad, sesgos, protección de datos, uso responsable y protocolos de incidente.

10. Responsabilidades y garantías

- 10.1. Las Partes exigirán a los Proveedores certificación y garantía de que, en el momento de la puesta a disposición, el sistema cumple los requisitos legales aplicables, que dispone de la documentación necesaria y que no incorpora funcionalidades prohibidas.
- 10.2. El Responsable del Despliegue garantiza el uso conforme a las Instrucciones de Uso, la implementación de controles organizativos y técnicos necesarios y la no alteración sustancial del sistema sin evaluación previa.

A los efectos del presente Contrato, las obligaciones del GESTOR como Responsable del Despliegue se limitan a las cuestiones y tareas bajo su control conforme el Contrato, y no será responsable frente al HOTELERO por incumplimientos del proveedor cuando haya actuado conforme a las Instrucciones de Uso y haya implementado medidas razonables.

- 10.3. En caso de incumplimiento del Reglamento UE IA u otra normativa aplicable imputable a una Parte en el ámbito de sus responsabilidades, ésta adoptará sin demora medidas correctoras, incluida desactivación o retirada del sistema afectado, y asumirá los daños directos acreditados causados a la otra Parte por dicho incumplimiento, con los límites de responsabilidad establecidos en el Contrato, salvo dolo o negligencia grave.
- 10.4. Cada Parte indemnizará a la otra por reclamaciones de terceros, sanciones o daños derivados de (i) uso de IA en contravención de la normativa aplicable o de esta cláusula, cuando sea imputable a la Parte infractora; (ii) infracción de derechos de propiedad intelectual de terceros causada por sus datos aportados o por Instrucciones de Uso; y (iii) incumplimiento de deberes de transparencia frente a usuarios cuando le fueran exigibles.

A efectos aclaratorios las Partes dejan constancia de que la responsabilidad derivada de la presente cláusula es exigible por incumplimientos imputables y culposos y dentro de los límites de responsabilidad previstos en el Contrato.

- 10.5. La Parte responsable del incumplimiento que haya dado lugar a la imposición de multas o sanciones administrativas indemnizará a la otra Parte por las cantidades que esta última

deba satisfacer por dicho concepto, más los costes razonables de defensa incurridos, siempre que tales multas sean consecuencia directa del incumplimiento de la Parte responsable. Esta obligación no será exigible cuando la normativa aplicable prohíba la transferencia o aseguramiento de las sanciones, ni alcanzará a sanciones debidas a actos u omisiones de la propia Parte sancionada.

- 10.6. La Parte que integre o contrate Proveedores de sistemas de IA para la ejecución del Contrato se obliga a: (i) imponer contractualmente obligaciones equivalentes (*back-to-back*) a las previstas en materia de cumplimiento, seguridad, transparencia, documentación e indemnidad, en un grado razonable y proporcionado al riesgo; (ii) procurar garantías y recursos contractuales adecuados del Proveedor, y (iii) mantener mecanismos de cooperación y auditoría razonables.

En caso de incumplimiento del Proveedor que cause o contribuya a un daño cubierto por el Contrato, la Parte que contrató al Proveedor: (i) ejercerá diligentemente los derechos y acciones disponibles para obtener la reparación; (ii) pondrá a disposición de la otra Parte, en la medida legalmente posible y a solicitud razonable, documentación necesaria para la defensa y para el eventual ejercicio coordinado de acciones; y (iii) transferirá o abonará a la otra Parte las cantidades finalmente recuperadas del Proveedor que correspondan a resarcir el daño sufrido por esta.

En ningún caso las previsiones contenidas en el presente apartado pueden interpretarse como una limitación, neutralización o retraso de la responsabilidad propia y exigible de la Parte que contrató al Proveedor frente a la otra Parte, quien podrá reclamarle el cumplimiento e indemnización sin demora conforme a este Contrato. Por ello, la obtención de reparaciones del Proveedor o la tramitación de acciones frente a este no constituirá condición previa para el pago de las cantidades debidas por la Parte que contrató al Proveedor.

11. Coordinación con el resto del Contrato

- 11.1. En caso de conflicto entre esta cláusula y otros apartados del Contrato en materia de tecnología, protección de datos, seguridad o cumplimiento, prevalecerá la previsión que otorgue mayor protección a los derechos fundamentales, a la seguridad y a la conformidad regulatoria, interpretada de forma armonizada con el resto del Contrato.
- 11.2. Las Partes se comprometen a negociar de buena fe las adaptaciones estrictamente necesarias de esta cláusula para reflejar cambios normativos que resulten imperativos y de aplicación directa, sin alterar el equilibrio económico del Contrato.

