

ID	Dimensión	Riesgo a evaluar	Pregunta de control	Evidencia esperada	Probabilidad	Impacto	Riesgo inherente	Nivel de control	Riesgo residual	Clasificación	Responsable	Plan de tratamiento	Fecha compromiso	Estado	Observaciones
R-01	Privacidad y datos personales	Uso de datos personales sin base jurídica o finalidad clara	¿Se documentó la finalidad, fundamento, categorías de datos y personas afectadas antes de usar IA? ¿Se realizó evaluación de impacto cuando la solución trata datos personales de forma intensiva o relevante?	Ficha de tratamiento, fundamento jurídico, aviso de privacidad o instrumento equivalente	Media	Medio		9 Definido		5 Medio				No iniciado	
R-02	Privacidad y datos personales	Tratamiento intensivo o relevante sin evaluación de impacto		Evaluación de impacto, dictamen, medidas de mitigación y autorización	Media	Medio		9 Definido		5 Medio				No iniciado	
R-03	Privacidad y datos personales	Exposición de datos sensibles en prompts, entrenamiento o registros	¿Existen reglas para impedir que datos sensibles se incorporen a prompts o servicios no autorizados?	Política de uso, filtros DLP, configuración, registros de pruebas	Media	Medio		9 Definido		5 Medio				No iniciado	
R-04	Minimización y retención	Recolección excesiva o conservación indefinida	¿Solo se utilizan los datos estrictamente necesarios y existe un plazo de conservación?	Inventario de datos, reglas de minimización y calendario de retención	Media	Medio		9 Definido		5 Medio				No iniciado	
R-05	Seguridad	Acceso no autorizado al sistema, modelos o datos	¿Se aplican controles de identidad, mínimo privilegio, MFA y segregación de funciones?	Matriz de accesos, configuración IAM, bitácoras y revisiones periódicas	Media	Medio		9 Definido		5 Medio				No iniciado	
R-06	Seguridad	Fuga de información por proveedor o servicio de IA	¿El contrato y la arquitectura limitan reutilización, transferencia y entrenamiento con datos institucionales?	Contrato, DPA, arquitectura, residencia de datos y configuración del proveedor	Media	Medio		9 Definido		5 Medio				No iniciado	
R-07	Seguridad	Ataques a prompts, manipulación de entradas o extracción de información	¿Se han probado ataques de prompt injection, exfiltración y entradas maliciosas?	Plan de pruebas, resultados, filtros de entrada/salida y controles compensatorios	Media	Medio		9 Definido		5 Medio				No iniciado	
R-08	Calidad y validez	Respuestas incorrectas, inventadas o desactualizadas	¿La solución valida fuentes, nivel de confianza y vigencia antes de presentar resultados?	Pruebas de precisión, referencias, umbrales y protocolo de validación	Media	Medio		9 Definido		5 Medio				No iniciado	
R-09	Supervisión humana	Automatización de decisiones que afectan derechos sin revisión humana	¿Las decisiones con impacto jurídico, económico o social requieren aprobación humana competente?	Fujo de aprobación, perfiles autorizados, registro de intervención y criterio de escalamiento	Media	Medio		9 Definido		5 Medio				No iniciado	
R-10	Supervisión humana	Dependencia excesiva del resultado de IA	¿Las personas usuarias están capacitadas para cuestionar, verificar y rechazar la recomendación?	Programa de capacitación, guías de validación y evaluación de competencias	Media	Medio		9 Definido		5 Medio				No iniciado	
R-11	Trazabilidad	Imposibilidad de reconstruir cómo se generó una respuesta o decisión	¿Se registran versión del modelo, datos de entrada, fuentes, reglas, salida, usuario y fecha?	Bitácoras, versionado, expediente de decisión y política de auditoría	Media	Medio		9 Definido		5 Medio				No iniciado	
R-12	Transparencia	La ciudadanía desconoce que interactúa con IA	¿Se informa claramente cuándo una respuesta o servicio utiliza IA y cuáles son sus límites?	Avisos al usuario, términos de uso, mensajes en interfaz y canal de aclaración	Media	Medio		9 Definido		5 Medio				No iniciado	
R-13	Explicabilidad	No se puede explicar una recomendación relevante	¿Existe una explicación comprensible y suficiente para el nivel de impacto del caso de uso?	Plantilla de explicación, factores utilizados, fuentes y limitaciones	Media	Medio		9 Definido		5 Medio				No iniciado	
R-14	Sesgos y no discriminación	Resultados diferenciados injustificadamente entre grupos	¿Se evalúa desempeño por grupos relevantes y se corrigen diferencias injustificadas?	Pruebas de sesgo, métricas por grupo, revisión legal y plan de mitigación	Media	Medio		9 Definido		5 Medio				No iniciado	
R-15	Accesibilidad e inclusión	El sistema excluye a personas por discapacidad, idioma o brecha digital	¿Se diseñaron canales alternos y criterios de accesibilidad e inclusión?	Pruebas de accesibilidad, canales no digitales, lenguaje claro y soporte	Media	Medio		9 Definido		5 Medio				No iniciado	
R-16	Gobernanza	Falta de propietario, comité o reglas de autorización	¿El caso de uso tiene dueño institucional, responsable técnico y órgano de aprobación?	RACI, acta de comité, inventario de sistemas de IA y política institucional	Media	Medio		9 Definido		5 Medio				No iniciado	
R-17	Proveedores	Dependencia tecnológica y falta de capacidad de salida	¿Se definieron portabilidad, exportación de datos, continuidad y terminación contractual?	Cláusulas de salida, respaldos, estándares abiertos y plan de transición	Media	Medio		9 Definido		5 Medio				No iniciado	
R-18	Monitoreo	Degradación del modelo o cambios no detectados	¿Se monitorean precisión, incidentes, deriva, seguridad y quejas durante la operación?	Tablero de indicadores, alertas, revisiones y calendario de reevaluación	Media	Medio		9 Definido		5 Medio				No iniciado	
R-19	Gestión de incidentes	No existe respuesta ante errores o daños causados por IA	¿Hay un procedimiento para contener, investigar, notificar, corregir y aprender de incidentes?	Plan de respuesta, responsables, niveles de severidad y registro de incidentes	Media	Medio		9 Definido		5 Medio				No iniciado	
R-20	Rendición de cuentas	No hay mecanismo de inconformidad, revisión o corrección	¿Las personas pueden solicitar revisión humana y corregir datos o resultados?	Canal de aclaración, SLA, procedimiento de revisión y evidencia de resolución	Media	Medio		9 Definido		5 Medio				No iniciado	