Estándar / Normativa	Numeral / Referencia	Descripción del Requisito	Cumplimiento (Cumple/Parcial/No cumple)	Evidencia Documental	Observaciones Técnicas	Brecha / Debilidad Identificada
NTC-ISO/IEC 42001:2024	4.2 Partes interesadas	Comprensión de las necesidades y expectativas de las partes interesadas en el sistema de gestión de IA.				Falta definir stakeholders específicos para el uso de Gemini.
NTC-ISO/IEC 42001:2024	6.1 Riesgos y Oportunidades	Evaluación de impactos y riesgos específicos de la IA (exfiltración, sesgos).				Se requiere una matriz de riesgos específica para modelos generativos.
ISO/IEC 27001:2022	A.5.1 Políticas	Políticas para la seguridad de la información revisadas periódicamente.				La política actual no contempla explícitamente el uso de LLMs externos.
ISO/IEC 27001:2022	A.8.10 Prevención de fuga de datos	Controles aplicados para evitar la divulgación no autorizada de información.				Ausencia de filtros DLP específicos para prompts de IA.
Circular Externa 007 de 2023 (SFC)	Seguridad y Calidad	Requerimientos mínimos de seguridad y calidad en el manejo de la información.				Necesidad de alinear el uso de IA con el SARO y SARM.
Ley 1581 de 2012	Protección de Datos	Garantizar que los datos personales no sean procesados sin autorización o en entornos inseguros.				Riesgo de procesar datos sensibles de clientes en versiones públicas de Gemini.
NTC-ISO/IEC 42001:2023	8.2 Evaluación de impacto	Realización de evaluaciones de impacto sobre la privacidad y ética de la IA.				Pendiente por implementar antes del despliegue de soluciones basadas en Gemini.
ISO/IEC 27001:2022	A.5.33 Protección de registros	Protección de registros contra pérdida, destrucción y falsificación.				Se debe asegurar la trazabilidad de los logs de interacción con la IA.
Circular Externa 007 de 2023 (SFC)	Gestión de Riesgo Tecnológico	Considerar la IA como un factor de riesgo tecnológico dentro de la estructura de control.				Falta integrar la gobernanza de IA en el Sistema de Gestión de Riesgo (SARLAFT).