Edición de lectura | 2026-11-20

IA práctica para los servicios financieros — Tecnología de la información

Harbour Think Tank, Caribbean AI Association, under the leadership of Adrian Dunkley | 2026-11-11

Edición de lectura abreviada del documento preparado por el Harbour Think Tank de la Caribbean AI Association bajo la dirección de Adrian Dunkley. Incorpora la revisión del 11 de noviembre de 2026, las diez propuestas y sus límites de actuación.

Edición de lectura abreviada del documento preparado por el Harbour Think Tank de la Caribbean AI Association bajo la dirección de Adrian Dunkley. Incorpora la revisión del 11 de noviembre de 2026, las diez propuestas y sus límites de actuación.

Quién decide

Los equipos de servicio y los dueños de aplicaciones documentan solicitudes y cambios antes de tocar sistemas bancarios en producción. Los ingenieros conservan la decisión sobre versiones, acceso y recuperación.

Diez usos y sus controles

01. Solicitudes de soporte. Proponga una ruta con el texto del ticket. Un analista comprueba urgencia y escala los casos dudosos. Nivel 1.

02. Preguntas operativas. Recupere instrucciones con enlace y versión vigentes. Si falta una fuente accesible y válida, remita la consulta al responsable. Nivel 0.

03. Cambios de código. Señale líneas que necesitan revisión y documente la conducta esperada. El ingeniero evalúa los hallazgos y autoriza cualquier cambio. Nivel 1.

04. Pruebas de reglas de negocio. Proponga casos normales, límites y fallos previstos. El responsable fija el resultado esperado antes de ejecutar pruebas controladas. Nivel 0.

05. Impacto de cambios. Mapee un cambio propuesto a servicios y dependencias. Los responsables comprueban el alcance y las condiciones de reversión. Nivel 1.

06. Documentación de operaciones. Proponga correcciones a partir de una versión aceptada. El dueño del documento revisa los cambios y conserva el historial. Nivel 1.

07. Interfaces antes de automatizar. Relacione campos y sistemas e indique los vínculos no comprobados. Los dueños de cada conexión confirman compatibilidad y permisos. Nivel 0.

08. Expedientes de acceso. Compare permisos existentes con requisitos de la función y señale excepciones. Solo el responsable autorizado modifica el acceso. Nivel 0.

09. Demanda de servicio. Compare volúmenes y medidas agregadas con períodos equivalentes. El analista comprueba causas antes de solicitar capacidad adicional. Nivel 1.

10. Manual de recuperación. Señale pasos ausentes, requisitos previos y decisiones sin dueño. El responsable de continuidad los prueba en un ejercicio autorizado. Nivel 0.

Cómo preparar y validar una prueba

En el nivel 0, el asistente responde a una solicitud y una persona ejecuta cada paso. En el nivel 1, reúne entradas aprobadas y prepara un borrador. No envía mensajes ni modifica sistemas. El expediente de prueba debe identificar fuente, versión de la instrucción, permisos, revisor y condición de parada.

Limite la recuperación de instrucciones a una colección autorizada con versiones y vencimientos. Pruebe una pregunta bien documentada, otra sin respuesta, otra con una guía caducada y otra que pide acceso restringido. Registre errores graves no detectados, sugerencias dañinas y retrabajo. Suspenda ante una acción en producción sin aprobación.

Medición y límites

Compare tareas equivalentes con el proceso actual. Registre tamaño de la muestra, tiempo de preparación, verificación y corrección, fallos relevantes, permisos y problemas de confidencialidad. Incluya licencia, integración, formación, supervisión y costo por ejecución cuando corresponda. Las puntuaciones orientan la selección de pruebas. La publicación no presenta rendimientos medidos en una entidad. El documento íntegro describe la instrucción inicial, herramientas de ejemplo, habilidades y método de cada caso.

Referencias

[1] International Telecommunication Union. Global Cybersecurity Index 2024. Americas tier table, printed page 27. Jamaica appears in Tier 3, Establishing. National commitments, not firm-level operational performance.

[2] Office of the Information Commissioner, Jamaica. Data Protection Standards. Official guidance, inspected 26 October 2026; relevant sections cover purpose, minimisation, security and transfers.

[3] National Institute of Standards and Technology. Secure Software Development Framework version 1.1, Special Publication 800-218. February 2022.

[4] National Institute of Standards and Technology. Cybersecurity Framework 2.0. Official framework resource page, inspected 26 October 2026.

[5] Agent Skills. Agent Skills Overview. Accessed 10 November 2026.

Esta edición abreviada acompaña al original completo en inglés.

Edición en inglés (PDF)