



Política de Uso Responsable de Inteligencia Artificial

Esta Política establece los principios y lineamientos para promover el uso responsable de la inteligencia artificial en el Banco. Su propósito es impulsar la innovación de manera segura, ética y alineada con la normativa aplicable.

Área responsable: VP DATA & AI

MANUAL DE
POLÍTICAS

Descripción del documento

Información del documento	Detalle
Versión	1.0
Clasificación	Uso Interno
Propietario	VP DATA & AI
Instancia de aprobación	Directorio
Fecha de entrada en vigor	17/07/2026
Frecuencia de revisión	Ante cambios normativos o tecnológicos relevantes

Control de versiones

Versión	Fecha	Elaborado por	Descripción del cambio
9/6/2026	1	VP DATA & AI	Versión inicial de la Política

Elaboración, revisión y aprobación

Etapa	Nombre	Cargo/Área	Fecha
Elaborado por	Gisele Salinas	Frente RAI	23/06/2026
Revisado por	Eduardo Guardia	Ética y Cumplimiento	23/06/2026
Revisado por	Adriana Ñañez	Ética y Cumplimiento	23/06/2026
Revisado por	Laura Cerna	Legal	23/06/2026
Revisado por	David Tito	Arquitectura	23/06/2026
Revisado por	Pamela Paredes	Ciberseguridad	23/06/2026
Revisado por	Leslie Tamayo	Ciberseguridad	23/06/2026
Revisado por	Miguel Jinez	Frente RAI	23/06/2026
Revisado por	Castro Joshimar	Ciberseguridad	23/06/2026
Revisado por	Gomez Jesus	Ciberseguridad	23/06/2026
Revisado por	Adriana Cuadros	Frente RAI	23/06/2026
Revisado por	Sheilla Bustamante	Riesgo Operacional	23/06/2026
Revisado por	Andaluz Malaga, Alvaro Daniel	Auditoria	23/06/2026

Revisado por	Murguía Jara, Luis	Auditoría	23/06/2026
Revisado por	Salcedo Salazar, Jaqueline	Conducta de Mercado	23/06/2026
Revisado por	Rocio Tinoco	Prevención de Fraude	23/06/2026
Aprobador	Pamela Griffith	Líder AI	23/06/2026

La información contenida en este documento y sus anexos son propiedad de Interbank, es de uso privilegiado, confidencial y solo puede ser utilizado por sus colaboradores y/o entes reguladores. Si usted no se considera de ninguno de los grupos de interés antes mencionados no deberá examinar, usar, copiar o distribuir parcial o totalmente este documento o la información que contiene. Si llegó a su poder por error, por favor elimínelo. Cualquier retención o distribución total o parcial no autorizada de este documento está estrictamente prohibida y sancionada por ley.

Índice

1.Propósito	5
2.Alcance	5
3.Marco Normativo	6
4.Definiciones	7
5.Principios de uso responsable.....	8
5.1. Robustez, seguridad y ciberseguridad	8
5.2. Responsabilidad y supervisión humana.....	8
5.3. Equidad y no discriminación	9
5.4. Transparencia y explicabilidad.....	9
5.5. Privacidad y gestión de datos	9
5.6. Bienestar ambiental y social.....	9
6.Gobierno y Roles de Inteligencia Artificial	9
7.Clasificación de sistemas por riesgo	10
8.Usos aceptables y usos prohibidos.....	11
8.1. Queda prohibido el uso de sistemas de IA en los siguientes supuestos, entre otros:.....	11
8.2 Uso de inteligencia artificial.....	12
9. Proceso de aprobación y gestión de riesgos del ciclo de vida	12
9.1 Documentación de sistema basado en IA	12
9.2 Evaluación de riesgo de sistema basado en IA	13
10. Derechos de los clientes y colaboradores frente a la inteligencia artificial.....	13
11. Gestión de proveedores y terceros	14
12. Incumplimientos y medidas aplicables	14
13. Vigencia, aprobación, revisión y documentos relacionados	15

1.Propósito

La presente Política establece los principios y responsabilidades que rigen el desarrollo, la adquisición, la implementación, el uso, el monitoreo y la supervisión de sistemas basados en inteligencia artificial en Interbank, con el fin de asegurar que dicha tecnología se utilice de manera segura, responsable, ética, transparente y conforme a la normativa vigente.

La finalidad de esta Política es proteger los derechos de los clientes, colaboradores y terceros, gestionando de forma adecuada los procesos involucrados para mitigar los riesgos asociados a la inteligencia artificial y habilitar la adopción responsable de herramientas de inteligencia artificial que genere valor para preservar la confianza en los clientes y colaboradores.

El presente documento constituye el marco de mayor jerarquía en Interbank en materia de inteligencia artificial. En ese sentido, los lineamientos, manuales, estándares, procedimientos y demás documentos internos que se emitan sobre la materia, deberán desarrollar y complementar sus disposiciones, asegurando su plena consistencia y alineamiento con lo descrito en ella, sin contradecirlo en ningún extremo.

2.Alcance

La presente Política es de cumplimiento obligatorio para todos los colaboradores de Interbank, cualquiera sea su modalidad de contratación, así como para los proveedores y terceros que desarrollen, integren, provean, mantengan, evalúen o utilicen sistemas basados en inteligencia artificial en beneficio, por encargo o en nombre de Interbank.

Su alcance aplica a todo sistema basado en inteligencia artificial, independientemente de que sea desarrollado internamente, adquirido por terceros o consumido a través de servicios o interfaces externas, y comprende todas las etapas de su ciclo de vida, desde la concepción hasta su retiro.

Para efectos de la presente Política, el uso de sistemas basados en inteligencia artificial se clasifica en:

(i) uso productivo,

- (ii) uso experimental o de prueba, y
- (iii) uso personal en entorno laboral.

Cada categoría estará sujeta a condiciones diferenciadas que serán desarrolladas en los lineamientos correspondientes, sin perjuicio de las restricciones mínimas establecidas en la presente Política.

3.Marco Normativo

Las disposiciones aquí establecidas se enmarcan y se interpretarán de conformidad con la normativa aplicable al régimen del sistema financiero en materia de inteligencia artificial, protección de datos personales y regulación financiera, en particular:

- Ley N.º 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país.
- Decreto Supremo N.º 115-2025-PCM, Reglamento de la Ley N.º 31814, que establece principios rectores, criterios de clasificación de riesgo y obligaciones para el sector privado.
- Ley N.º 29733, Ley de Protección de Datos Personales, y su Reglamento, así como las disposiciones complementarias emitidas por la Autoridad Nacional de Protección de Datos Personales.
- Normativa de la Superintendencia de Banca, Seguros (SBS) aplicable al Banco, en particular en materia de gestión de riesgos, seguridad de la información y ciberseguridad, continuidad del negocio, tercerización y demás materias relacionadas con el uso de sistemas de inteligencia artificial.

En caso de que la normativa aplicable establezca exigencias más estrictas que las previstas en este documento, prevalecerá la norma de mayor exigencia.

4. Definiciones

Para la interpretación y aplicación de la presente Política, los términos definidos a continuación deberán entenderse conforme al significado que se les asigna en este apartado.

- Inteligencia artificial (IA): Tecnología emergente de propósito general que tiene el potencial de mejorar el bienestar de las personas, contribuir a una actividad económica global sostenible positiva, aumentar la innovación y la productividad, y ayudar a responder a los desafíos globales clave.
- Sistema basado en IA. Sistema basado en máquina que, para objetivos de forma explícita o implícita, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenido, recomendaciones o toma de decisiones que puedan influir en la o los entornos físicos o digitales. Los diferentes sistemas basados en IA varían en sus niveles de autonomía y la capacidad de entendimiento y adaptación después del despliegue.
- Máquina: sistema tecnológico capaz de computar, procesar datos e inferir resultados sin intervención humana directa en cada paso. Cualquier sistema computacional que procese información automáticamente que incluye Software (algoritmos, modelos ML, LLMs), Sistemas en servidores, Aplicaciones, APIs, Plataformas en la nube, Equipos físicos (pero no es lo principal).
- Decisión automatizada: decisiones adoptadas por un sistema basado en inteligencia artificial sin intervención humana significativa, que inciden de manera significativa en los derechos, intereses o en el acceso a productos o servicios de una persona.
- Área responsable del sistema: unidad organizativa responsable de un caso de uso de IA y de su correcto funcionamiento conforme a la presente Política.
- Supervisión humana: mecanismo que permite a una persona comprender, vigilar y, cuando corresponda, intervenir, corregir, detener o revertir el funcionamiento o las decisiones de un sistema basado en IA.
- Datos personales: toda información sobre una persona natural que la identifica o la hace identificable, conforme a la Ley N.º 29733.
- Uso de sistemas basados en inteligencia artificial: toda acción de operar, interactuar con o aplicar un sistema basado en inteligencia artificial en el marco de las actividades de Interbank. Para efectos de la presente política se distinguen tres modalidades:

- Uso productivo: empleo de un sistema basado en IA en procesos, productos o servicios reales de Interbank, cuyos resultados tienen efecto sobre operaciones, decisiones del negocio o clientes.
- Uso experimental o de prueba: empleo de un sistema basado en IA en entornos controlados, pruebas de concepto o pilotos, sin efecto directo sobre operaciones, productos o clientes reales.
- Uso personal en entorno laboral: empleo de un sistema basado en IA por parte de un colaborador como apoyo a su trabajo individual, sin integrarse a procesos o sistemas institucionales.

5.Principios de uso responsable

El desarrollo, la implementación y el uso de inteligencia artificial en Interbank se rigen por los siguientes principios, que orientan la interpretación y aplicación de toda la presente Política:

5.1. Robustez, seguridad y ciberseguridad

Asegurar que los sistemas que contengan IA produzcan resultados precisos, seguros, reproducibles y resistentes a ataques, mediante la implementación de mecanismos de monitoreo continuo, pruebas rigurosas y procesos de validación de calidad a lo largo de su ciclo de vida. Asimismo, se deberá garantizar la protección de la información a través de controles de ciberseguridad que aseguren la confidencialidad, integridad y disponibilidad de los datos, incluyendo gestión de accesos, cifrado, trazabilidad y registro de actividades.

5.2. Responsabilidad y supervisión humana

Atribuir responsabilidad ética y jurídica a personas naturales o jurídicas involucradas en el ciclo de vida de los sistemas de IA, conforme a la normativa vigente que resulte aplicable, e incorporar supervisión humana (human-in-the-loop), evaluaciones de impacto, debida diligencia y auditoría en cada decisión y caso de uso. La supervisión humana será obligatoria en todos los sistemas de IA que influyan en clientes o colaboradores, y deberá permitir la revisión, intervención y, cuando corresponda, reversión de los resultados generados por el sistema.

5.3. Equidad y no discriminación

Asegurar el uso legítimo y ético de los datos personales, conforme a la regulación aplicable, y mitigar sesgos por grupos poblacionales presentes en los datos y outputs para evitar discriminación y garantizar resultados justos y equitativos.

5.4. Transparencia y explicabilidad

Documentar de forma exhaustiva el diseño, funcionamiento, datos y lógica de los sistemas con IA que sean auditables, asegurando que clientes y colaboradores sepan cuándo interactúan con sistemas de IA, comprendan su propósito, puedan interpretar resultados y accedan a atención humana cuando lo requieran.

5.5. Privacidad y gestión de datos

Garantizar la protección de datos personales y limitar su uso al principio de mínimo privilegio y necesidad de acceso por agente, sistema y caso de uso, previniendo fugas de información, memorización indebida e inferencia, y respetando los derechos de propiedad intelectual de terceros.

5.6. Bienestar ambiental y social

Considerar el impacto social, ambiental y ético en el despliegue de soluciones con IA, evitar la generación de contenido dañino, tóxico o inapropiado, y promover decisiones eficientes en consumo de cómputo optimizando el uso adecuado de los recursos y uso responsable de los datos a largo plazo.

Los principios establecidos en la presente sección son de cumplimiento obligatorio y constituyen criterios vinculantes para la evaluación, aprobación y supervisión de todos los sistemas basados en inteligencia artificial utilizados, desarrollados, adquiridos o implementados en Interbank.

6. Gobierno y Roles de Inteligencia Artificial

6.1 El Directorio aprueba la presente Política y ejerce la supervisión general de su cumplimiento y aplicación en Interbank.

6.2 Vicepresidencia de Data & IA: Responsable de velar por la aplicación de la presente política. Le corresponde proponer al Directorio las actualizaciones de la presente política, aprobar los lineamientos y procedimientos que de ella deriven y supervisar la clasificación de riesgos de los casos de uso.

6.3 El área de Ciberseguridad define los controles de seguridad aplicables a los sistemas basados en IA, evalúa los riesgos asociados antes de su puesta en producción, así como la evaluación de seguridad de proveedores cuyos productos o servicios incorporen capacidades de IA, garantizando el cumplimiento de los criterios y requisitos de seguridad establecidos.

6.4 El área de Ética y Cumplimiento es responsable de evaluar y supervisar de que toda la cadena de la IA (diseño → desarrollo → uso) cumpla con regulación, ética y gestión de riesgos.

6.5 El Área Legal Producto es responsable de brindar asesoramiento jurídico respecto de las iniciativas de inteligencia artificial, evaluando los aspectos legales, contractuales y regulatorios que resulten aplicables, así como los riesgos asociados a dichas iniciativas y al Banco.

6.6 El área responsable de cada sistema basado en IA deberá asegurar su uso conforme a la presente Política y al marco regulatorio aplicable, garantizando el cumplimiento de los estándares éticos, de control interno y de gestión de riesgos.

Todo colaborador y /o proveedor es responsable de utilizar los sistemas de inteligencia artificial conforme a la presente Política y de reportar los incidentes de seguridad y usos indebidos o cualquier incumplimiento que advierta.

7. Clasificación de sistemas por riesgo

El Banco adopta un enfoque de gestión de riesgos de Inteligencia Artificial basado en niveles de riesgo, conforme a la normativa vigente.

Los sistemas de IA serán clasificados como: prohibidos, de riesgo alto y de riesgo aceptable, clasificación que deberá realizarse de manera previa a su implementación. Esta clasificación considerará, entre otros aspectos, el impacto sobre los derechos de las personas, el tratamiento de datos personales, la existencia de decisiones automatizadas y la normativa aplicable vigente.

La clasificación del nivel de riesgo determinará el nivel de controles, validación, monitoreo y aprobación requeridos.

La definición detallada de los criterios de clasificación y de los controles asociados a cada nivel de riesgo se establecerá en los lineamientos internos y manuales que deriven de la presente Política.

8. Usos aceptables y usos prohibidos

Se considera uso aceptable aquel que se realiza mediante sistemas de Inteligencia Artificial autorizados por el Banco, conforme a la finalidad y alcance aprobados, en cumplimiento de la normativa aplicable, incluyendo la de protección de datos personales, y bajo los controles correspondientes a su nivel de riesgo.

8.1. Queda prohibido el uso de sistemas de IA en los siguientes supuestos, entre otros:

- El ingreso de datos personales, sensibles o confidenciales de clientes o de la organización en sistemas de IA no autorizados.
- El uso de herramientas o extensiones de IA no autorizadas para fines laborales.
- La adopción de decisiones que afecten los derechos de las personas sin la supervisión humana requerida
- La generación o uso de información engañosa, o con fines contrarios a la ley, la ética o los intereses del Banco, sus clientes o colaboradores
- Cualquier uso clasificado como prohibido por la normativa aplicable.

Está estrictamente prohibido:

- Ingresar datos personales, datos sensibles o información protegida por secreto bancario en herramientas no autorizadas.
- Utilizar resultados generados por IA sin debida validación humana previa.

El uso de herramientas de Inteligencia Artificial autorizadas por la organización deberá realizarse de acuerdo con la clasificación de la información y los controles de seguridad establecidos.

8.2 Uso de inteligencia artificial

El uso de herramientas de inteligencia artificial, incluyendo inteligencia artificial generativa externas, queda restringido a aquellas previamente autorizadas por Interbank.

9. Proceso de aprobación y gestión de riesgos del ciclo de vida

Todo nuevo sistema basado en IA, así como todo cambio significativo sobre uno existente, deberá ser evaluado y aprobado conforme al proceso definido por Interbank y con participación de las áreas de gobierno establecidas en la presente Política. El alcance de la evaluación y de los controles aplicables será proporcional al nivel de riesgo del sistema.

Ningún sistema basado en inteligencia artificial podrá ser puesto en producción sin contar con las aprobaciones previas requeridas de acuerdo con su clasificación de riesgo. Los sistemas clasificados como de alto riesgo deberán contar, adicionalmente, con evidencia documentada de su evaluación, gestión de riesgos, controles implementados y cumplimiento regulatorio aplicable, así como con las aprobaciones formales establecidas en Interbank.

La gestión de riesgos de los sistemas basados en Inteligencia artificial se sujetará a criterios de tolerancia al riesgo, aceptación y tratamiento del riesgo residual, diferenciados según la categoría de uso y la criticidad del sistema, conforme se establezca en los lineamientos correspondientes.

9.1 Documentación de sistema basado en IA

Todo sistema basado en IA, incluidos los desarrollados o provistos por terceros, deberá contar con documentación suficiente que permita garantizar su trazabilidad a lo largo de su ciclo de vida. Dicha documentación comprenderá, conforme a su nivel de riesgo, la finalidad del sistema, los datos utilizados, su diseño y lógica general de funcionamiento, los controles aplicados, así como la evidencia de su aprobación,

de la evaluación de riesgo realizada, del monitoreo de incidentes y de las decisiones humanas adoptadas en su operación. Esta custodia se conservará bajo custodia y por los plazos de retención que se establezcan en los lineamientos correspondientes.

Todo sistema basado en IA debe registrarse en un inventario de IA, con los atributos mínimos que se definan, incluyendo su propietario, finalidad y nivel de riesgo.

9.2 Evaluación de riesgo de sistema basado en IA

Los sistemas clasificados como de riesgo alto requieren, antes de su implementación, una evaluación de riesgos orientada a identificar y mitigar impactos, así como mecanismos de supervisión humana y de gestión de riesgos a lo largo de su ciclo de vida. La responsabilidad sobre dicha evaluación recaerá en el área responsable del sistema conforme a los roles y al detalle que establezcan los lineamientos correspondientes.

Interbank mantiene mecanismos de monitoreo, registro y trazabilidad que permitan auditar el funcionamiento de los sistemas basados en IA, especialmente aquellos de riesgo alto, a fin de detectar desviaciones, errores, sesgos o impactos no previstos, adoptar las medidas correctivas correspondientes y, cuando resulte necesario, restringir, suspender o retirar su uso ante riesgos significativos.

El retiro de un sistema deberá efectuarse mediante un proceso de baja segura de sus datos, accesos y componentes asociados.

10. Derechos de los clientes y colaboradores frente a la inteligencia artificial

Los clientes y colaboradores tienen derecho a ser informados, de manera previa y clara, cuando interactúan con un sistema basado en IA o cuando un servicio de Interbank utiliza inteligencia artificial de forma relevante para la decisión o interacción.

Los clientes y colaboradores tienen derecho a solicitar la intervención y revisión humana respecto de las decisiones automatizadas que les afecten, así como a que dicha revisión pueda modificar o dejar sin efecto la decisión cuando corresponda.

Interbank pone a disposición de los clientes y colaboradores canales accesibles y trazables para el ejercicio de estos derechos y para la prestación de consultas o reclamos relacionados con el uso de inteligencia artificial.

11. Gestión de proveedores y terceros

Los proveedores que desarrollen provean u operen sistemas basados en IA para Interbank, están sujetos a la presente Política y a las exigencias de seguridad, protección de datos personales y cumplimiento normativo que Interbank establezca conforme a los marcos de gestión de terceros vigentes. Estas exigencias comprenden la acreditación de los controles aplicables y el monitoreo del servicio durante toda su vigencia, conforme se establezca en dichos marcos.

La contratación de servicios de IA provistos por terceros requiere una evaluación previa de seguridad, cumplimiento normativo y posibles impactos sobre los derechos de las personas, proporcional al nivel de riesgo del servicio, conforme al proceso que se establezca para tal efecto.

Interbank definirá el procedimiento de debida diligencia para la evaluación de proveedores y terceros considerando su perfil de riesgo. Los contratos deberán incluir la cláusula del cumplimiento de la presente Política que contemple la posibilidad de auditar y/o solicitar información respecto a los servicios prestados, considerando también entrevistas en el proceso de debida diligencia y de rescindir el contrato o retener el pago en caso de incumplimiento.

12. Incumplimientos y medidas aplicables

El incumplimiento de la presente Política puede dar lugar a la aplicación de las medidas disciplinarias, contractuales o legales que correspondan, conforme al régimen aplicable a colaboradores, proveedores y terceros.

Los incidentes y usos indebidos de inteligencia artificial deben reportarse a través de los canales que Interbank establezca, los cuales son comunicados y difundidos a toda la organización.

13. Vigencia, aprobación, revisión y documentos relacionados

La presente Política entra en vigor a partir de su aprobación por el Directorio y se mantiene vigente hasta su modificación o derogación expresa.

La Política se revisa ante cambios normativos o tecnológicos relevantes. Las propuestas de actualización son elevadas por el Responsable de Gobierno de IA al Directorio para su aprobación.