

Desafíos para la gestión de riesgos de terceros: ¿Cómo construir un modelo eficiente en el liderazgo de las relaciones?

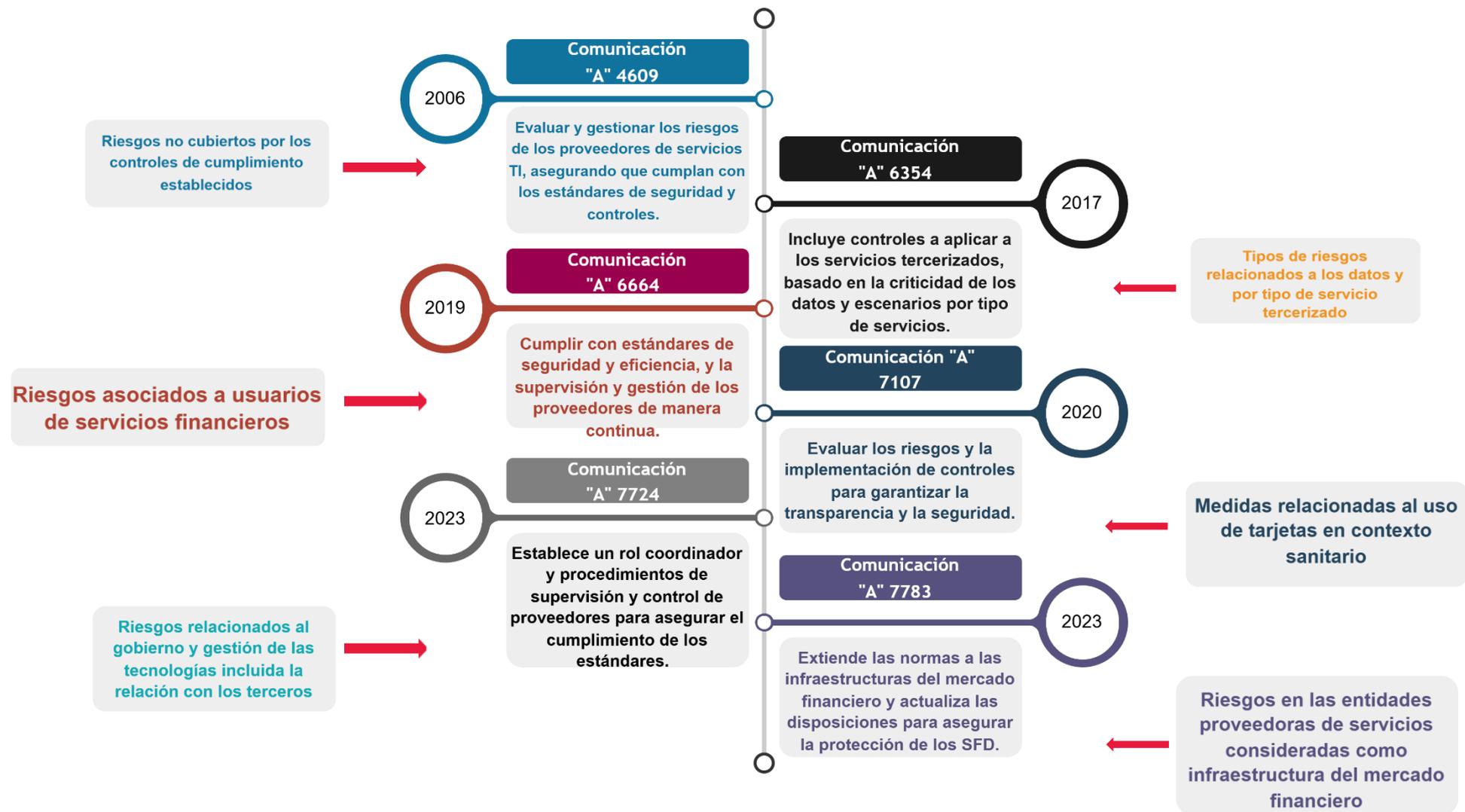
- ▶ Lorena Almirón, BDO en Argentina
- ▶ Mariana Martinez Brizuela, BDO en Argentina
- ▶ Jesús Briceño, BDO en Perú

19 de febrero



Regulaciones en Argentina

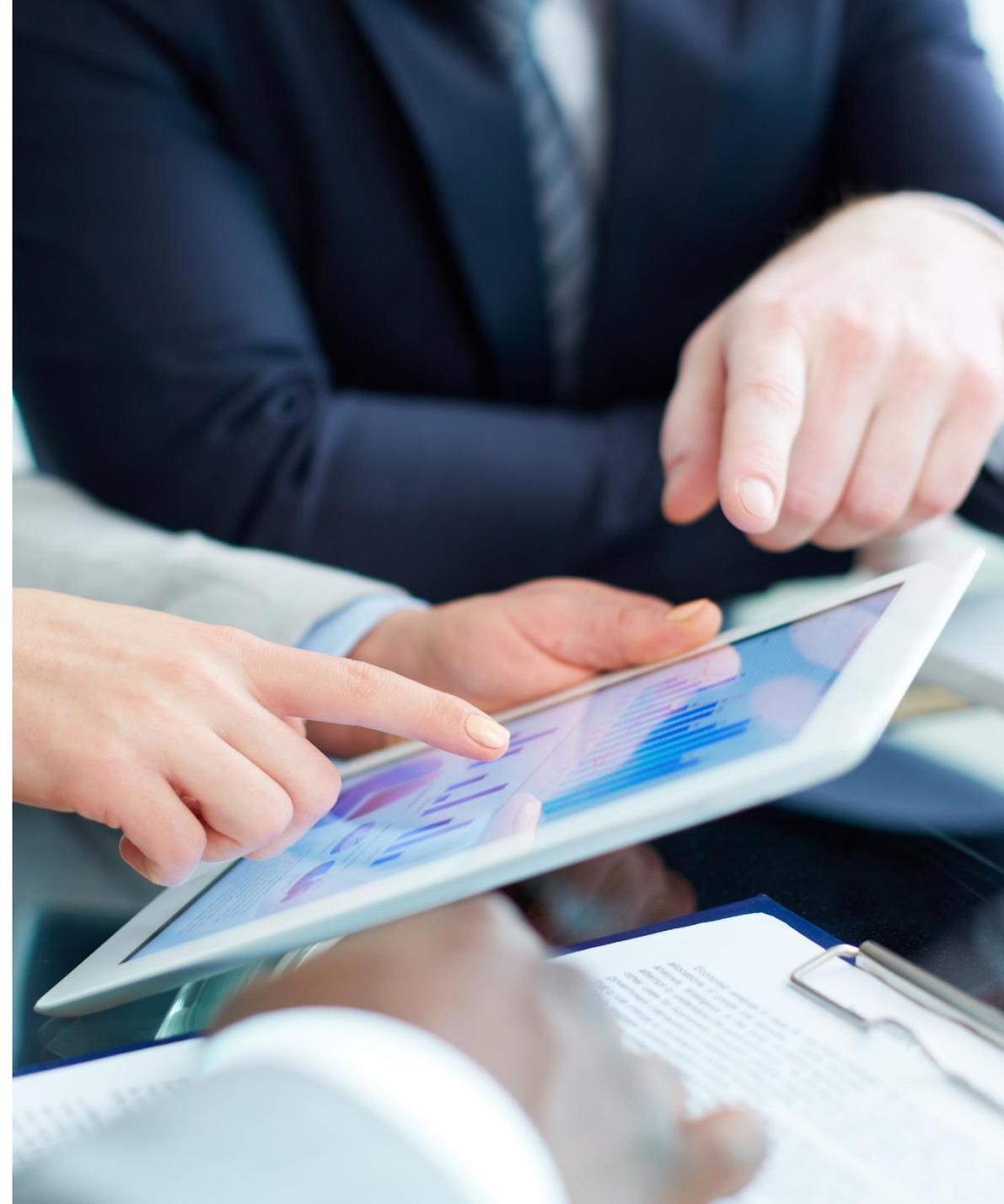
Proceso de maduración de la regulación en Argentina



Lecciones aprendidas:

La importancia de:

- ▶ Definir el rol que deberá encargarse de la tarea de coordinación.
- ▶ Cláusulas mínimas que deberán considerarse al momento de contratar.
- ▶ Tener bien delimitado el alcance en relación con el objeto de contratación y plazos establecidos.
- ▶ Considerar cuestiones de continuidad y ciberseguridad.
- ▶ Tener presente los modelos de contratación con las responsabilidades del manejo de datos.
- ▶ Confidencialidad y cumplimiento de marco legal y regulatorio.
- ▶ Si es un proveedor de tecnología y seguridad de la información, tener en cuenta sus particularidades.





Regulaciones en Perú

Actualizaciones de la SBS sobre requerimientos para la Gestión de Terceros

La Superintendencia de Banca y Seguros (SBS) en consonancia con los reguladores de la región, ha venido evolucionando en un marco normativo más riguroso para la gestión de terceros.

- ▶ Este marco tiene como objetivo principal asegurar que los procesos adecuados para seleccionar, supervisar y monitorear a los proveedores de servicios
- ▶ Mitigar los riesgos asociados a la externalización de funciones críticas promoviendo las siguientes prácticas:

Resolución S.B.S. N° 272-2017

Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos

Resolución S.B.S. N° 2116-2009

Reglamento para la Gestión del Riesgo Operacional

Resolución S.B.S. N° 504-2021

Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad/**Disposiciones Complementarias Finales**

Gobierno Corporativo y de la Gestión Integral de Riesgos



- La subcontratación ocurre cuando la empresa solicita a un tercero bienes o servicios que podría desarrollar internamente.
- Bienes y servicios significativos de terceros pueden afectar gravemente a la empresa si
 - Fallan impactando ingresos, solvencia, continuidad y reputación.
- Un proveedor es significativo si provee servicios críticos, sin importar la modalidad de subcontratación.

Gestión del Riesgo Operacional:



- Evaluar amenazas y vulnerabilidades de seguridad e implementar medidas adecuadas.
- Asegurar que el contrato permita cumplir con el reglamento.
- Definir roles y responsabilidades sobre la seguridad de la información.
- Implementar procedimientos para identificar proveedores significativos y contar con un proceso de selección del proveedor.
- Monitorear y gestionar los riesgos de los servicios de terceros y mantener un registro detallado de los proveedores y sus servicios.

Actualizaciones de la SBS sobre requerimientos para la Gestión de Terceros

Resolución S.B.S. N° 504-2021

Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad/**Disposiciones Complementarias Finales**

Resolución S.B.S. N°877-2020

Reglamento para la Gestión de la Continuidad del Negocio

Resolución S.B.S. N°3601-2021

Modificatoria del Reglamento para la Gestión de la Continuidad del Negocio

Resolución S.B.S. N° 11699-2008

Reglamento de Auditoría Interna

Seguridad de la Información y Ciberseguridad:



- Evaluar las amenazas y vulnerabilidades de seguridad e implementar medidas adecuadas.
- Asegurar que el contrato con el proveedor permita cumplir con este Reglamento.
- Definir roles y responsabilidades sobre la seguridad de la información y asegurar que se implementen las medidas complementarias necesarias.

Continuidad de Negocio:



- Estimación de recursos necesarios (propios y/o de terceros) para productos y servicios priorizados
- Identificación de puntos únicos de falla.
- Escenarios con indisponibilidad de recursos necesarios
- Exposición a riesgos según ubicación, instalaciones y proveedores críticos.
- Análisis de escenarios con falla o indisponibilidad de bienes o servicios

Auditoría Interna:

Revisión de la gestión del riesgo operacional.

Cumplimiento de los procedimientos para la administración de los riesgos de operación.

Verificación de la normativa vigente sobre gestión de continuidad del negocio.

Evaluación de la seguridad de la información y ciberseguridad.



Riesgos y desafíos

Gobierno y gestión de los servicios

Implica:

Toma de decisiones de la calidad de los servicios que espera recibir.

Esquema de control y monitoreo continuo de los procesos, servicios y/o actividades delegadas en las terceras partes.



Será necesario:

Análisis de riesgos propio de la delegación.

Los mitigantes de riesgos previo y en la formalización, registrarán en toda la prestación del servicio y será un esfuerzo en conjunto con el tercero.

Para los casos en donde se aceptan riesgos derivados de la delegación, se deberán establecer mitigantes internos.

Cuestiones relevantes:

-
- ▶ Delimitar el proceso de subcontratación.
 - ▶ Definir claramente el alcance y responsabilidades.
 - ▶ Dictamen jurídico/legal.
 - ▶ Monitoreo de consensos.
 - ▶ Gestionar de acuerdo a la criticidad y los riesgos de los proveedores.

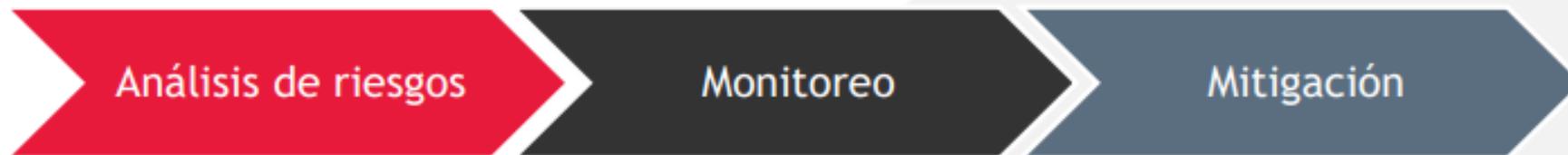
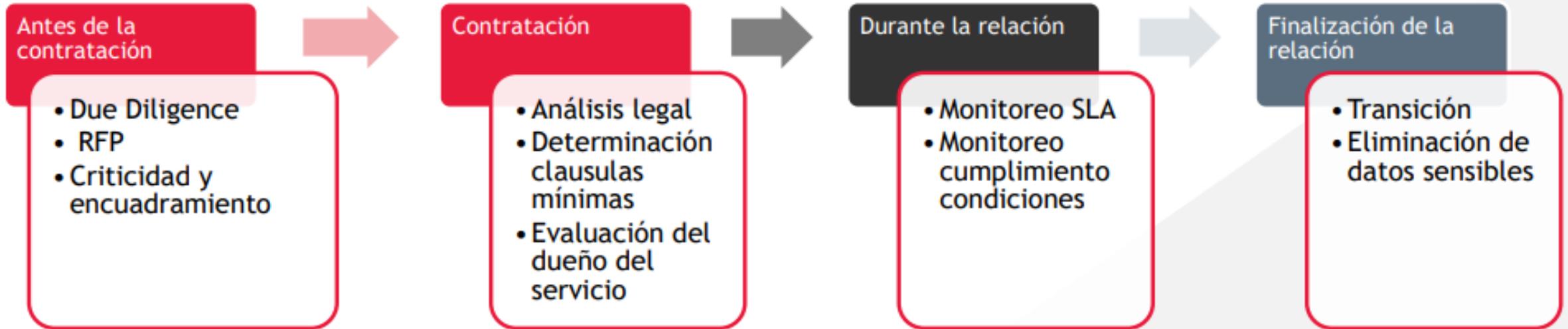




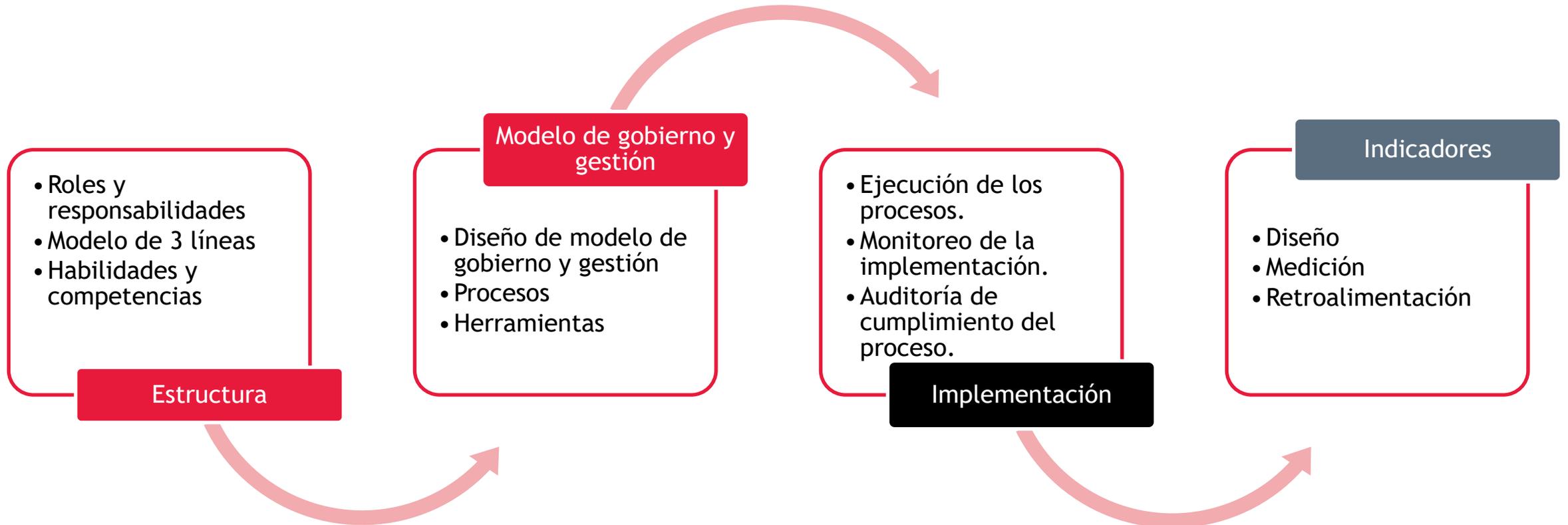
Modelo BDO



MODELO DE SOLUCIÓN BDO PARA EL CICLO DE VIDA DEL PROVEEDOR



MODELO DE IMPLEMENTACIÓN DE BDO PARA EL CICLO DE VIDA DEL PROVEEDOR



Gestión de Riesgos

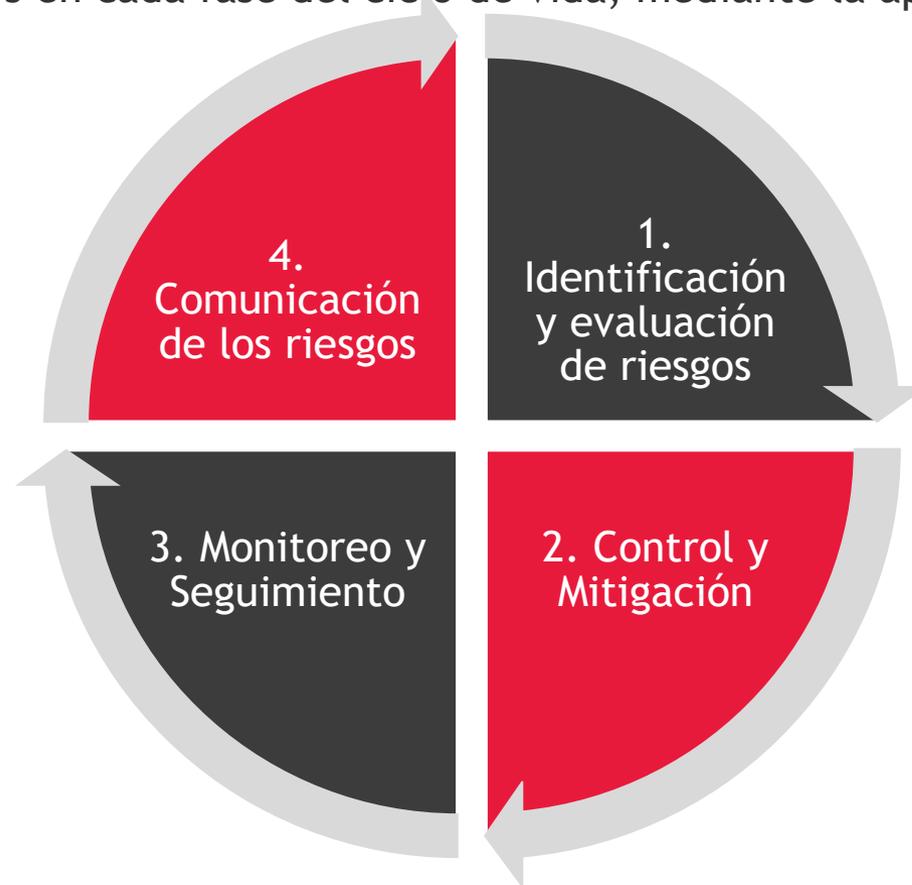
Identificación y evaluación de riesgos en cada fase del ciclo de vida, mediante la aplicación de bases específicas de amenazas y controles:

Previo a Contratación

- Controles de los procesos a delegar.
- Due Diligence (proceso - proveedores)

Contratación

- Instrumento jurídico.
- Plazos para formalización.



Durante la Relación

- Monitoreo de acciones de mitigación
- Pautas de cumplimiento
- Cambios en el contexto

Finalización de la relación

- Cumplimiento del proceso de fin de relación.
- Eliminación de datos sensibles.

¡Gracias!