

Auditoría de Carácter Especial

2025-AI003 - Gestión del riesgo tecnológico - EDM03 APO12

Auditoría Interna

Plan anual 2025

**Informe final
IA-029-2025**



Objetivos



Objetivo General:

Evaluar que el apetito y la tolerancia al riesgo tecnológico están alineados con los objetivos estratégicos del negocio y asegurar que estos sean comprendidos, comunicados y gestionados, mediante la revisión de la gestión de los procedimientos operativos, con el propósito de verificar que se cumpla con las actividades establecidas en el marco de gestión COBIT 2019.

Objetivos Específicos:

1

Evaluar que las actividades de la administración del riesgo se alinean con los objetivos empresariales, para asegurar su adecuada administración mediante la verificación del cumplimiento de los estándares establecidos en el marco de COBIT 2019.

2

Verificar que el proceso de gestión de riesgos incluya la identificación, análisis y reportes efectivos de los riesgos de TI, por medio de la revisión del registro de información y las valoraciones de riesgos implementados en la Institución, para asegurar que los riesgos de TI sean adecuadamente analizados.

3

Confirmar la implementación y efectividad de los planes de acción derivados de los análisis de riesgos, por medio de la revisión de la atención de estos, a fin de asegurar su efectividad.

Alcance

El alcance del estudio de auditoría está relacionado con el cumplimiento de los procesos COBIT APO12 “Gestionar el riesgo” y EDM03 “Asegurar la optimización del riesgo”. La auditoría abarcó la documentación y las operaciones comprendidas entre el 1 de enero de 2024 y se extendió al 31 de marzo de 2025 para contemplar las actividades realizadas con la Declaratoria de Apetito de Riesgo 2025.

Resumen ejecutivo



El estudio consistió en la evaluación de la “Gestión del riesgo tecnológico - EDM03 APO12” incluyendo la revisión de:

- Validación de información registrada.
- Valoraciones de riesgos de los procesos COBIT.
- Cumplimiento de identificación y comunicación de cambios en los objetivos estratégicos.
- Protección de información sensible y/o confidencial.
- Políticas y procedimientos de gestión de riesgos.
- Revisión de las evaluaciones periódicas del apetito de riesgos.
- Cumplimiento de los planes de acción de riesgos.
- Verificación de los informes de riesgos.

Se observaron las siguientes situaciones:

- La Metodología General para la Valoración de Riesgos Operativos se encontraba desactualizada de acuerdo con el acápite “Revisión y actualización periódica” (página 98 de la misma metodología).
- En el proceso de valoración de riesgos tecnológicos no se contemplan los procesos COBIT 2019 gestionados por la Institución.

Se considera que el estudio es importante para la Administración Superior, ya que el fin de los procesos son “Gestionar el riesgo” y “Asegurar la optimización del riesgo” de la Institución.

Principales Riesgos evaluados

- Procesos/ productos diseñados o implementados de forma incorrecta o inadecuada.
- Desviaciones en el análisis de riesgos, debido a que la gestión de riesgos puede ser establecida e implementada de forma inadecuada.

Para robustecer el Control Interno se emitieron las siguientes recomendaciones:

A.1. Revisar y actualizar la metodología general para la gestión integral de riesgos operativos según lo indicado por la normativa vigente.

B.1. Incorporar en el análisis y gestión de riesgos el marco de gestión de TI Institucional, esto permite a la Institución implementar un enfoque más amplio y robusto para la gestión de riesgos dentro del contexto de la gobernanza de TI proporcionada por COBIT 2019.

Conclusiones



Los cambios en los objetivos estratégicos Institucionales fueron comunicados e identificados adecuadamente, y se tomaron como base para la Declaratoria de Apetito del Riesgo del año 2025.

Las evaluaciones del cumplimiento de la Declaratoria de Apetito de Riesgo se llevaron a cabo de acuerdo con la periodicidad establecida, lo cual evidencia un adecuado seguimiento y control por parte de la Dirección de Riesgos Corporativa.

La evaluación de la efectividad del proceso de gestión del riesgos tecnológico ha permitido identificar áreas de mejora en la actualización de la Metodología General para la Valoración de Riesgos, así como la contemplación de la valoración de riesgos tecnológicos que indican los procesos COBIT 2019 que gestiona la Institución.

Los resultados derivados de los análisis de riesgos confirmaron que todos los riesgos identificados se encuentran en niveles bajos o muy bajos, en consecuencia, no se requirió la ejecución de planes de acción.

La revisión de la supervisión efectiva en la elaboración de informes para garantizar la satisfacción de la información transmitida reveló que la misma permite verificar la información relacionada con los riesgos tecnológicos, así como que la recepción y atención de las observaciones generadas por las partes interesadas se considera adecuada.

Las actividades ejecutadas fueron realizadas de acuerdo con las NGASP y demás normativa aplicable al ejercicio de la auditoría interna.

Resumen de recomendaciones



		Altas				Medias				Bajas					
Informe		Pendiente - Atendida		Pendiente - Atendida		Pendiente - Atendida		Pendiente - Atendida		Tarjeta de Seguimiento		Plan de acción			
IA-018-2025		00	00	02	00	00	00	00	00	TS-22470		Si			

Apéndices y/o anexos



Jefatura del estudio

Johnny Muñoz Paniagua



Equipo de trabajo

Amalia Chinchilla Monge
José Alejandro Álvarez Delgado
Ricardo Luna Álvarez

Tipo de documento	Descripción corta	Adjunto
Informe parcial Sprint 1	IA-018-2025 de fecha 24/03/2025	
Informe parcial Sprint 2	IA-024-2025 de fecha 29/04/2025	
Informe parcial Sprint 3	IA-028-2025 de fecha 16/05/2025	