

el
Respaldo
de los que
sueñan



100
Años **INS**

Auditoría especial

2025-AI003

Gestión del riesgo tecnológico - EDM03 APO12

Auditoría Interna INS

Informe parcial

IA-018-2025

Plan Anual 2025



Objetivos Específicos de la revisión

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 y oportunidades de TI sean adecuadamente analizados.

Conclusiones:

La revisión de esta Auditoría evidenció que la información de los expedientes de riesgos en el sistema SRERM se mantiene precisa y confiable, contribuyendo a una gestión eficiente y segura. Esto fortalece la calidad de los datos y respalda la toma de decisiones fundamentadas.

Los resultados permitieron evaluar que 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.

Se identificó que 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).

Por otra parte, se desprende una oportunidad de mejora para el proceso de valoración de riesgos tecnológicos, en la cual se contemplen los procesos COBIT gestionados por la institución.

Aspectos positivos

La revisión de los expedientes de riesgos ha sido exitosa, garantizando la precisión y confiabilidad de la información.

Además, se identificaron áreas clave para la mejora continua, la actualización de metodologías, lo que refuerza la resiliencia y eficiencia operativa de la Institución.

Dirigido a: Dirección de Riesgos Corporativa

Con copia a: Gerencia General

Objetivo estratégico INS

OE.10 Aplicar las mejores prácticas y estándares globales para fortalecer el Gobierno Corporativo.

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 abarca la documentación y las operaciones comprendidas entre el 1 de enero de 2024 y el 31 de enero de 2025.

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

A. Metodología general para la gestión de riesgos operativos desactualizada.

Condición:

La última actualización de la Metodología general para la gestión integral de riesgos operativos se realizó en octubre del 2021.

Causa:

La causa de esta deficiencia radica en la falta de actualización, debido a la ausencia de una revisión periódica a la metodología general para la gestión de riesgos operativos.

Efecto:

La desactualización de la metodología puede provocar una desalineación con las mejores prácticas actuales y las normativas vigentes en la Institución, debilitando su capacidad para gestionar riesgos operativos de manera más efectiva y proactiva.

Criterio:

La Metodología general para la gestión integral de riesgos operativos, acota en el siguiente punto:
“Revisión periódica La presente metodología deberá ser objeto de una revisión y actualización por lo menos una vez al año.”.

Recomendaciones

Para Dirección de Riegos Corporativa

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

Prioridad: Media.

Riesgos asociados

En ausencia de una actualización periódica de la Metodología, la condición detectada podría materializar el riesgo de Procesos/ productos diseñados o implementados de forma incorrecta o inadecuada.

B. Procesos COBIT no integrados en la valoración de riesgo tecnológico.

Condición:

Se ha identificado una situación de mejora en implementar valoraciones de riesgos en los procesos COBIT.

Causa:

La valoración de los riesgos tecnológicos correspondientes al año 2024 se realizó producto de una solicitud de la Contraloría General de la República (Oficio DFOE-CAP-2125), razón por la que se centró en la evaluación de algunos riesgos específicos del negocio. No obstante, es necesario cumplir con las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información del MICITT para abordar de manera integral los riesgos tecnológicos.

Efecto:

La ausencia de una evaluación del riesgo operativo asociado a los procesos de gestión y gobernabilidad de la tecnología puede llevar a una organización a operar con procesos ineficientes, una gobernanza débil, una gestión de riesgos ineficaz, un mayor riesgo de incumplimiento normativo, la pérdida de oportunidades de mejora e innovación, y una asignación ineficiente de recursos.

Criterio:

Las “Normas Técnicas para la Gestión y el Control de las Tecnologías de Información del MICITT”, en la sección del Perfil del proceso detalla elementos que contribuyen a una gestión de riesgos efectiva, asimismo al respecto acota:

“Capítulo Procesos del marco de gestión de TI, Sección IV. Gestión de riesgos tecnológicos
La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el Marco de Gestión de TI que le resulte aplicable.”.

Recomendaciones

Para la Dirección de Riesgos Corporativa:

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.

Prioridad: Media.

Riesgos Asociados

Esta situación puede materializar el riesgo de desviaciones en el análisis de riesgos, debido a que la gestión de riesgos puede ser establecida e implementada de forma inadecuada.



Jefatura del estudio

Johnny Muñoz Paniagua



Equipo de trabajo

Amalia Chinchilla Monge
José Alejandro Álvarez Delgado
Ricardo Luna Álvarez

Fecha del informe: 24/03/2025

Apéndices y/o anexos

Tipo de documento	Descripción corta	Adjunto
Acta	Acta de presentación	

El presente informe se encuentra firmado digitalmente mediante agente GAUDI.