

AUDITORÍA DE CARÁCTER ESPECIAL SOBRE APO01 GESTIONAR EL MARCO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN (TI)

IA-031-2024
30 DE JULIO DE 2024



RESUMEN EJECUTIVO

Como parte del programa Marco de Gestión del Uso de Tecnologías de Información (MGETI), el cual tenía como objetivo principal instaurar dentro del INS un marco de gestión empresarial del uso de las tecnologías de información, se realizó la implementación del proceso “APO01 Gestionar el Sistema de Gestión de Tecnología de Información”.

En esta revisión, se evaluaron los procedimientos de gestión, la documentación y las prácticas implementadas para el proceso mencionado, y se encontró que, si bien la gestión del proceso se ha alineado con el marco de referencia COBIT, existen áreas de mejora.

La evaluación reveló la adecuada conformación de estructuras organizativas en la gestión de TI, al revisar funciones, roles y responsabilidades que garantizan una toma de decisiones eficiente, la asignación adecuada de recursos y la rendición de cuentas. No obstante, la falta de capacitación del personal puede obstaculizar la efectiva administración del proceso y generar situaciones de falta de control.

Otro aspecto que se detectó fue una inconsistencia en la definición de la responsabilidad de la comunicación de objetivos, dirección y decisiones tomadas, lo que puede afectar la efectividad de las comunicaciones internas.

En general, se resalta la necesidad de mejorar la formación del personal y la comunicación interna para garantizar una gestión eficaz de las Tecnologías de la Información en la organización.

Contenido

I.	INTRODUCCIÓN	1
A.	Origen del Estudio	1
B.	Antecedentes o Generalidades	1
C.	Objetivo General.....	1
D.	Objetivos Específicos	2
E.	Naturaleza y Alcance	2
F.	Metodología	2
G.	Marco Normativo	2
H.	Comunicación de Resultados.....	3
II.	RESULTADOS	3
A.	Gestión de la comunicación de objetivos, dirección y decisiones tomadas (APO01.02 y APO01.09).....	3
B.	Gestión de las competencias, habilidades, propiedad de la información, políticas, procedimientos y aplicaciones adecuadas que respalden el sistema de gobierno y gestión (APO01.07, APO01.08 y APO01.10).....	4
III.	CONCLUSIONES.....	5
IV.	RECOMENDACIONES	6
A.	Recomendaciones para la Dirección de Planificación	6
V.	APÉNDICE 1“ACTA DE COMUNICACIÓN DE RESULTADOS”	6

I. INTRODUCCIÓN

A. Origen del Estudio

Este estudio se efectúa con fundamento en las competencias que le confiere el artículo 22 de la Ley General de Control Interno a las Auditorías Internas y en cumplimiento al Plan Anual de Trabajo del año 2024.

B. Antecedentes o Generalidades

Mediante el Acuerdo 5-17 del Consejo Nacional de Supervisión de Sistema Financiero (CONASSIF) se estableció que:

“Las entidades deben implementar los procesos de su marco de gestión de TI gradualmente como máximo durante los primeros 3 años para las entidades supervisadas por SUGEF y 5 años para el resto de las entidades supervisadas por las otras Superintendencias, contados a partir de la entrada en vigencia del reglamento”.

Por esta razón, durante el año 2019, se inició el programa Marco de Gestión del Uso de Tecnologías de Información (en adelante MGETI) el cual tenía como objetivo principal: *“Instaurar dentro del INS un marco de gestión empresarial del uso de las tecnologías de información que genere valor mediante la optimización de riesgos, entrega de beneficios y uso adecuado de los recursos, cumpliendo a su vez con el Reglamento General de Gestión de Tecnología de Información (conocido como Acuerdo CONASSIF 5-17), mediante la implementación de 38 procesos basados en la mejor práctica de COBIT 2019¹”.*

Dentro de los 38 procesos implementados en el marco de referencia COBIT 2019 se encuentra el proceso “Gestionar el Sistema de Gestión de Tecnología de Información”, que tiene como objetivo garantizar un enfoque estándar para los procesos relacionados con la tecnología de información institucional, en cumplimiento de las pautas del gobierno corporativo. Asimismo, establece para el proceso del marco de gestión de TI una serie de prácticas que permiten alcanzar los objetivos y generar resultados que contribuyen a la consecución de los objetivos relacionados con las Tecnologías de Información.

A nivel institucional, la Dirección de Planificación Corporativa tiene a cargo este proceso, bajo la dirección de la MDE Dayana Esquivel Arce.

C. Objetivo General

Verificar el proceso de gestión de las tecnologías de información para determinar si está alineado con las metas empresariales y da los resultados esperados por la Alta administración.

¹ Marco de gobierno de TI denominado “Objetivos de Control para Información y Tecnologías Relacionadas” (COBIT, por sus siglas en inglés)

D. Objetivos Específicos

1. Determinar la alineación del diseño e implementación del proceso de gestión de TI con los objetivos estratégicos de la Institución y verificar la comunicación de los objetivos organizativos, la dirección estratégica y las decisiones tomadas en la gestión mediante de la revisión del proceso, para asegurar que exista una conexión clara entre las actividades de la gestión de TI con los objetivos y estrategias del INS y constatar el cumplimiento de la práctica.
2. Determinar las estructuras organizativas requeridas en la gestión de TI mediante la revisión de las funciones de cada estructura, los roles y responsabilidades para garantizar la toma de decisiones eficiente, la asignación adecuada de recursos y la rendición de cuentas en todos los niveles.
3. Identificar el desarrollo y aplicación de habilidades, competencias, políticas, procedimientos, responsabilidades de propiedad de información (datos) y sistemas de información, así como la implementación de una infraestructura tecnológica sólida con la finalidad de garantizar la idoneidad del proceso APO01 y verificar la gestión de la mejora continua del proceso, mediante la identificación de las prácticas de calidad utilizadas para garantizar el cumplimiento de los objetivos de gobierno y gestión.

E. Naturaleza y Alcance

Esta auditoría es de carácter especial. Se realiza un proceso sistemático para la planificación de la actividad de auditoría interna, de conformidad con lo establecido en las Normas para el Ejercicio de la Auditoría Interna y las Normas Generales de Auditoría Interna para el Sector Público.

La revisión comprendió aspectos relacionados con la gestión del marco de gestión de TI y abarcó las operaciones comprendidas y la documentación generada entre el 1 de enero de 2023 y el 31 de enero de 2024.

F. Metodología

Las actividades ejecutadas en el presente estudio fueron realizadas de acuerdo con las Normas Generales de Auditoría para el Sector Público y demás normativa aplicable al ejercicio de la auditoría interna.

La metodología aplicada involucró el uso de prácticas, técnicas y procedimientos de auditoría, tales como: a) sesiones de trabajo con personal técnico y administrativo de la Dirección de Planificación, y b) inspección documental técnica y usuaria relevante.

G. Marco Normativo

1. Ley General de Control Interno, Ley N° 8292.
2. Marco de referencia COBIT 2019: objetivos de gobierno y gestión de las Tecnologías de Información.

3. Documentación vigente (GOB-MAT-0010 Manual del Sistema de Gestión de la Tecnología de Información Institucional).
4. Normas técnicas para la gestión y el control de las Tecnologías de Información emitido por el Ministerio de Ciencia Innovación, Tecnología y Telecomunicaciones (MICCIT).
5. Reglamento general de gestión de la Tecnología de Información, CONASIFF 5-17.

H. Comunicación de Resultados

En cumplimiento de lo establecido en la norma 205.08 de las “Normas Generales de Auditoría para el Sector Público las debilidades de control o situaciones sujetas a mejora que se exponen en este informe fueron presentadas en reunión celebrada mediante videoconferencia a través de la herramienta Teams el 18 de julio de 2024 a las señoras Dayana Esquivel Arce (jefa a.i de la Dirección de Planificación) e Ivonne Gutierrez Carvajal (funcionaria del Departamento de Normas y Estudios Administrativos de la Dirección de Planificación), quienes manifestaron mediante el oficio NEA-00265-2024 del 18 de julio de 2024 sus observaciones al borrador del informe. En los casos procedentes, los comentarios de la Administración fueron incorporados en el presente informe, lo cual quedó consignado en el Apéndice 1 “Acta de comunicación de resultados”.

II. RESULTADOS

A. Gestión de la comunicación de objetivos, dirección y decisiones tomadas (APO01.02 y APO01.09).

El Manual del Sistema de Gestión de la Tecnología de Información Institucional (GOB-MAT-0010, aprobado el 23 de diciembre de 2022) establece que el Plan de Comunicación correspondiente a los procesos del Sistema de Gestión de TI lo debe administrar la Dirección de Planificación, no obstante, las Disposiciones complementarias a la Política de Comunicaciones y Reputación del Grupo INS (aprobadas el 08 de noviembre de 2023) establecen que esta tarea le corresponde a la Subdirección de Relaciones Corporativas.

Esto se origina en que, al momento de aprobar las Disposiciones complementarias a la Política de Comunicaciones y Reputación del Grupo INS la Dirección de Planificación omitió coordinar con las dependencias involucradas la actualización del Manual del Sistema de Gestión de la Tecnología de Información Institucional, según lo establecido en el procedimiento GOB-PST-0003 Trámite para Aprobación de Normativa Interna y/o Corporativa.

Esta discrepancia podría generar confusión en la implementación y seguimiento de las comunicaciones dentro de la organización, aumentando la posibilidad de la materialización del riesgo “Falta de comunicación efectiva”.

Adicionalmente, se presenta una oportunidad para revisar y actualizar otras normativas institucionales que sean afectadas por las Disposiciones complementarias a la Política de Comunicaciones y Reputación del Grupo INS. Este proceso de actualización contribuirá a eliminar cualquier posible confusión, asegurando una comunicación más clara y efectiva.

Esto contraviene lo establecido en el punto 2.5.1 “Delegación de Funciones” del Capítulo II de las Normas de control interno para el Sector Público (N-2-2009-CO-DFOE), que indica:

“El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que la delegación de funciones se realice de conformidad con el bloque de legalidad, y de que conlleve la exigencia de la responsabilidad correspondiente y la asignación de la autoridad necesaria para que los funcionarios puedan tomar las decisiones y emprender las acciones pertinentes”.

B. Gestión de las competencias, habilidades, propiedad de la información, políticas, procedimientos y aplicaciones adecuadas que respalden el Sistema de Gobierno y Gestión (APO01.07, APO01.08 y APO01.10).

Los funcionarios del Departamento de Normas y Estudios Administrativos a cargo de la gestión del proceso APO01 no cuentan con formación específica sobre el marco normativo para el gobierno y la gestión de las tecnologías de la información (COBIT).

Adicionalmente, la administración del proceso APO01 “Gestionar el marco de gestión de TI” se realiza por un único funcionario quien no se encuentra dedicado únicamente a las labores propias del proceso, por lo que las actividades que se ejecutan pueden perder prioridad dentro del marco del proceso.

Esto se debe a que la implementación del proceso, producto del programa MGETI, no contempló la dotación de personal, capacitación o un análisis de cargas de trabajo que determinara la suficiencia y capacidad de la Dirección de Planificación para la atención del proceso APO01, por lo que se asumió como recargo de funciones.

Cabe mencionar que la falta de formación en el marco COBIT del personal puede aumentar el riesgo de errores, incumplimiento de políticas, falta de conciencia sobre las amenazas y respuestas inadecuadas a los incidentes del proceso APO01.

Asimismo, la falta de personal aumenta la carga de trabajo para los empleados existentes, lo que puede llevar a una disminución en la calidad, así como resultar en errores y omisiones.

Lo anterior contraviene lo establecido en el punto 2.4 “Idoneidad del personal” del Capítulo II de las Normas de control interno para el Sector Público (N-2-2009-CO-DFOE), que indica:

“El personal debe reunir las competencias y valores requeridos, de conformidad con los manuales de puestos institucionales, para el desempeño de los puestos y la operación de las actividades de control respectivas. Con ese propósito, las políticas y actividades de planificación, reclutamiento, selección, motivación, promoción, evaluación del desempeño, capacitación y otras relacionadas con la gestión de recursos humanos, deben dirigirse técnica y profesionalmente con miras a la contratación, la retención y la

actualización de personal idóneo en la cantidad que se estime suficiente para el logro de los objetivos institucionales.” (Se provee el resaltado.)

III. CONCLUSIONES

Durante la realización de este estudio fue posible determinar el alineamiento del diseño e implementación del proceso de gestión de TI con los objetivos estratégicos de la Institución, lo que aseguró que existe una conexión clara entre las actividades de la gestión de TI con los objetivos y estrategias del INS y permitió constatar el cumplimiento de la práctica.

No obstante, con respecto a la comunicación de objetivos, dirección y decisiones tomadas, se detectó un vacío en la atención de lo establecido en el Manual del Sistema de Gestión de la Tecnología de Información, debido a que, si bien las comunicaciones deben ser gestionadas por la Subdirección de Relaciones Corporativas (encargada de gestionar el Plan de Comunicaciones) debe existir un control por parte de la Dirección de Planificación para conocer si los encargados de procesos realizaron comunicaciones a las partes interesadas.

Por lo tanto, al verificar la forma en que se realiza la comunicación de objetivos, dirección y decisiones tomadas en el proceso APO01 “Gestionar el marco de Gestión de TI”, se puede concluir que la mitigación de los riesgos de cumplimiento y estratégicos se realiza de forma parcial, ya que las comunicaciones si se realizan, pero no existe un control por parte de los responsables del proceso APO01 que permita fiscalizar si todos los encargados de proceso realizan la comunicación de forma efectiva.

Asimismo, se revisaron las funciones de cada estructura organizativa requerida en la gestión de TI, sus roles y responsabilidades y se determinó que estas garantizan la toma de decisiones eficientes, la asignación adecuada de recursos y la rendición de cuentas en todos los niveles.

Con respecto a la identificación en el desarrollo y aplicación de habilidades, competencias, políticas, procedimientos, responsabilidades de propiedad de información (datos) y sistemas de información, así como la implementación de una infraestructura tecnológica sólida y la verificación de la gestión de la mejora continua del proceso, se determinó que existe falta de formación del personal sobre el proceso APO01, por lo cual se pueden presentar situaciones por falta de seguimientos o atenciones por parte de la Dirección de Planificación.

Adicionalmente, esto podría implicar disminuciones de la productividad, desmotivación y pérdida de empleados valiosos, así como falta de acciones para atender las tareas, entre otros.

Por lo anterior, al verificar las competencias, habilidades, propiedad de la información, políticas, procedimientos y aplicaciones adecuadas que respaldan el Sistema de Gobierno y gestión en el proceso APO01 “Gestionar el marco de Gestión de TI”, se puede concluir que la mitigación de los riesgos tecnológicos y operativos se realiza de forma parcial, ya que el recurso humano no se encuentra dedicado y no cuenta con capacitación suficiente, lo cual podría conllevar a falta de controles y que se obstaculice la administración gestión efectiva del proceso APO01.

IV. RECOMENDACIONES

A. Recomendaciones para la Dirección de Planificación

- A.1** Gestionar ante el Departamento Gestión de Calidad y Arquitectura Empresarial el análisis de cargas de trabajo de los procesos a ejecutar por el Departamento de Normas y Estudios Administrativos y establecer la cantidad de plazas y las características idóneas para asegurar la implementación efectiva del proceso APO01.

Una vez realizado lo anterior, tramitar las recomendaciones producto del análisis de cargas.

Prioridad: Media.

- A.2** De acuerdo con el análisis producto de la recomendación A.1, determinar las habilidades y conocimientos adicionales a COBIT necesarios para el personal que realiza labores relacionadas con el proceso APO01 “Gestionar el marco de gestión de TI” y coordinar con Capital Humano el desarrollo de un programa de capacitación que aborde las necesidades identificadas.

Prioridad: Media.

- A.3** Identificar y actualizar toda la normativa que pueda estar siendo afectada por las Disposiciones complementarias a la Política de Comunicaciones y Reputación del Grupo INS, a fin de evitar duplicidad e incompatibilidades entre la normativa vigente.

Prioridad: Baja.

- A.4** Instruir a los funcionarios encargados de atender las solicitudes de creación, modificación o derogatoria de normativa interna y/o corporativa sobre el acatamiento del procedimiento GOB-PST-0003 Trámite para Aprobación de Normativa Interna y/o Corporativa.

Prioridad: Baja.

V. APÉNDICE 1“ACTA DE COMUNICACIÓN DE RESULTADOS”

Se adjunta el acta de comunicación de resultados. 